



Guia de administração

# Amazon WorkSpaces Web



# Amazon WorkSpaces Web: Guia de administração

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

As marcas comerciais e imagens comerciais da Amazon não podem ser usadas no contexto de nenhum produto ou serviço que não seja da Amazon, nem de qualquer maneira que possa gerar confusão entre os clientes ou que deprecie ou desprestigie 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 Amazon WorkSpaces Web? .....	1
Termos para estar ciente ao usar os WorkSpaces Web .....	1
Serviços relacionados .....	3
Arquitetura .....	3
Acesso ao Amazon WorkSpaces Web .....	4
Configurando a Amazon WorkSpaces Web .....	5
Cadastrar e criar um usuário .....	5
Cadastrar-se em uma Conta da AWS .....	5
Criar um usuário administrativo .....	6
Conceder acesso programático .....	7
Redes e acesso .....	8
Requisitos da VPC .....	9
Recomendações de configuração da VPC .....	19
Zonas de disponibilidade compatíveis .....	21
Conexão de VPC .....	23
Conexão cliente/usuário .....	23
Começando com a Amazon WorkSpaces Web .....	26
Etapa 1: criar um portal da web .....	26
Definir configurações de rede .....	27
Definir configurações do portal .....	27
Definir as configurações do usuário .....	29
Configurar o provedor de identidades .....	30
Analisar e executar .....	40
Etapa 2: testar o portal da web .....	41
Etapa 3: distribuir o portal da web .....	41
Próximas etapas .....	42
Gerenciar seu portal da Web .....	43
Visualizar detalhes do portal da web .....	43
Editar um portal da web .....	43
Excluir um portal da web .....	44
Solicitar um aumento de cota de serviço .....	44
Controle o intervalo para autenticar novamente um token do IdP SAML .....	46
Configurar o registro de acesso do usuário .....	47
Logs de amostra .....	48

Definir ou editar a política de navegador .....	50
Definir uma política de navegador personalizada (exemplo) .....	50
Editar a política base do navegador .....	56
Configurar Editor de Método de Entrada (IME) .....	58
Configurar a localização na sessão .....	59
Configurar controles de acesso de IP (opcional) .....	62
Criar um grupo de controle de acesso de IP .....	63
Associar uma configuração de acesso de IP a um portal da web .....	63
Edite um grupo de controle de acesso de IP .....	64
Excluir um grupo de controle de acesso de IP .....	65
Habilitar extensão para autenticação única (opcional) .....	65
Configurar a filtragem de URL .....	67
Segurança .....	69
Proteção de dados .....	70
Criptografia de dados .....	71
Privacidade do tráfego entre redes .....	73
Registro em log do acesso do usuário .....	73
Identity and Access Management .....	73
Público .....	74
Autenticando com identidades .....	75
Como gerenciar acesso usando políticas .....	78
Como a Amazon WorkSpaces Web funciona com o IAM .....	81
Exemplos de políticas baseadas em identidade .....	89
Políticas gerenciadas pela AWS .....	92
Solução de problemas .....	99
Uso de funções vinculadas a serviço .....	101
Resposta a incidentes .....	105
Validação de compatibilidade .....	105
Resiliência .....	106
Segurança da infraestrutura .....	107
Análise de configuração e vulnerabilidade .....	108
Práticas recomendadas de segurança .....	108
Monitoramento .....	110
Monitoramento com CloudWatch .....	110
Logs do CloudTrail .....	112
Informações do Amazon WorkSpaces Web no CloudTrail .....	112

Noções básicas sobre entradas de arquivos de log do Amazon WorkSpaces Web .....	113
Registro em log do acesso do usuário .....	115
Orientação para usuários WorkSpaces da Amazon Web .....	116
Compatibilidade de navegadores e dispositivos .....	116
Acesso ao portal da web .....	117
Orientação da sessão .....	117
Iniciar uma sessão .....	117
Usar a barra de ferramentas .....	118
Usar o navegador .....	120
Encerrar uma sessão .....	120
Solução de problemas .....	121
Extensão de autenticação única .....	122
Compatibilidade .....	122
Instalação .....	123
Solução de problemas .....	123
Histórico do documento .....	124
.....	cxxviii

# O que é o Amazon WorkSpaces Web?

O Amazon WorkSpaces Web é um serviço sob demanda, totalmente gerenciado e baseado em Linux, projetado para facilitar o acesso seguro do navegador a sites internos e aplicações de software como serviço (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).

## Tópicos

- [Termos para estar ciente ao usar os WorkSpaces Web](#)
- [Serviços relacionados](#)
- [Arquitetura](#)
- [Acesso ao Amazon WorkSpaces Web](#)

## Termos para estar ciente ao usar os WorkSpaces Web

Para ajudar a começar a trabalhar com o WorkSpaces Web, você deve se familiarizar com os conceitos a seguir.

### Identity provider (IdP) (Provedor de identidade (IdP))

Um provedor de identidade verifica as credenciais de seus usuários. Em seguida, ele emite asserções de autenticação para fornecer acesso a um provedor de serviços. Você pode configurar seu IdP existente para funcionar com o WorkSpaces Web.

O processo de configuração do provedor de identidades (IdP) varia de acordo com o IdP.

Você deve carregar o arquivo de metadados do provedor de serviços no seu IdP. Caso contrário, os usuários não poderão fazer login. Você também deve conceder acesso para que os usuários usem o WorkSpaces Web em seu IdP.

### Documento de metadados do provedor de identidades (IdP)

O WorkSpaces Web exige metadados específicos do provedor de identidades (IdP) para estabelecer confiança. É possível adicionar esses metadados ao WorkSpaces Web carregando um arquivo de troca de metadados baixado do seu IdP.

## Provedor de serviço (SP)

Um provedor de serviços aceita declarações de autenticação e fornece um serviço ao usuário. O WorkSpaces Web atua como um provedor de serviços para usuários que foram autenticados por seu IdP.

## Documento de metadados do provedor do serviço (SP)

Você precisará adicionar os detalhes dos metadados do provedor de serviços à interface de configuração do provedor de identidades (IdP). Os detalhes desse processo de configuração variam entre os provedores.

## SAML 2.0

Um padrão para a troca de dados de autenticação e autorização entre um IdP e um provedor de serviços.

## Virtual Private Cloud (VPC)

Você pode usar uma VPC existente ou nova, sub-redes correspondentes e grupos de segurança para vincular seu conteúdo com o WorkSpaces Web.

As sub-redes devem ter uma conexão estável com a internet, e a VPC e as sub-redes também devem ter uma conexão estável com qualquer site interno e de software como serviço (SaaS) para que os usuários acessem esses recursos.

VPCs, sub-redes e grupos de segurança listados são obtidos da mesma região do console do WorkSpaces Web.

## Armazenamento de confiança

Se um usuário que acessa um site por meio do WorkSpaces Web receber um erro de privacidade, como `NET::ERR_CERT_INVALID`, esse site poderá estar usando um certificado assinado por uma autoridade de certificação privada (PCA). Talvez seja necessário adicionar ou alterar as PCAs em seu armazenamento confiável. Além disso, se o dispositivo do usuário exigir a instalação de um certificado específico para carregar um site, você precisará adicionar esse certificado ao armazenamento confiável para permitir que o usuário acesse esse site no WorkSpaces Web.

Os sites acessíveis ao público geralmente não exigem nenhuma alteração em um armazenamento confiável.

## Portal da web

Um portal da web fornece aos usuários acesso a sites internos e de SaaS por meio de navegadores. É possível criar um portal da web em qualquer região com suporte por conta. Para solicitar um aumento de limite para mais de um portal, entre em contato com o suporte.

## Endpoint do portal da web

O endpoint do portal da web é o ponto de acesso pelo qual os usuários iniciarão seu portal da web após fazerem login com o provedor de identidades configurado para o portal.

O endpoint está disponível publicamente na internet e pode ser incorporado à sua rede.

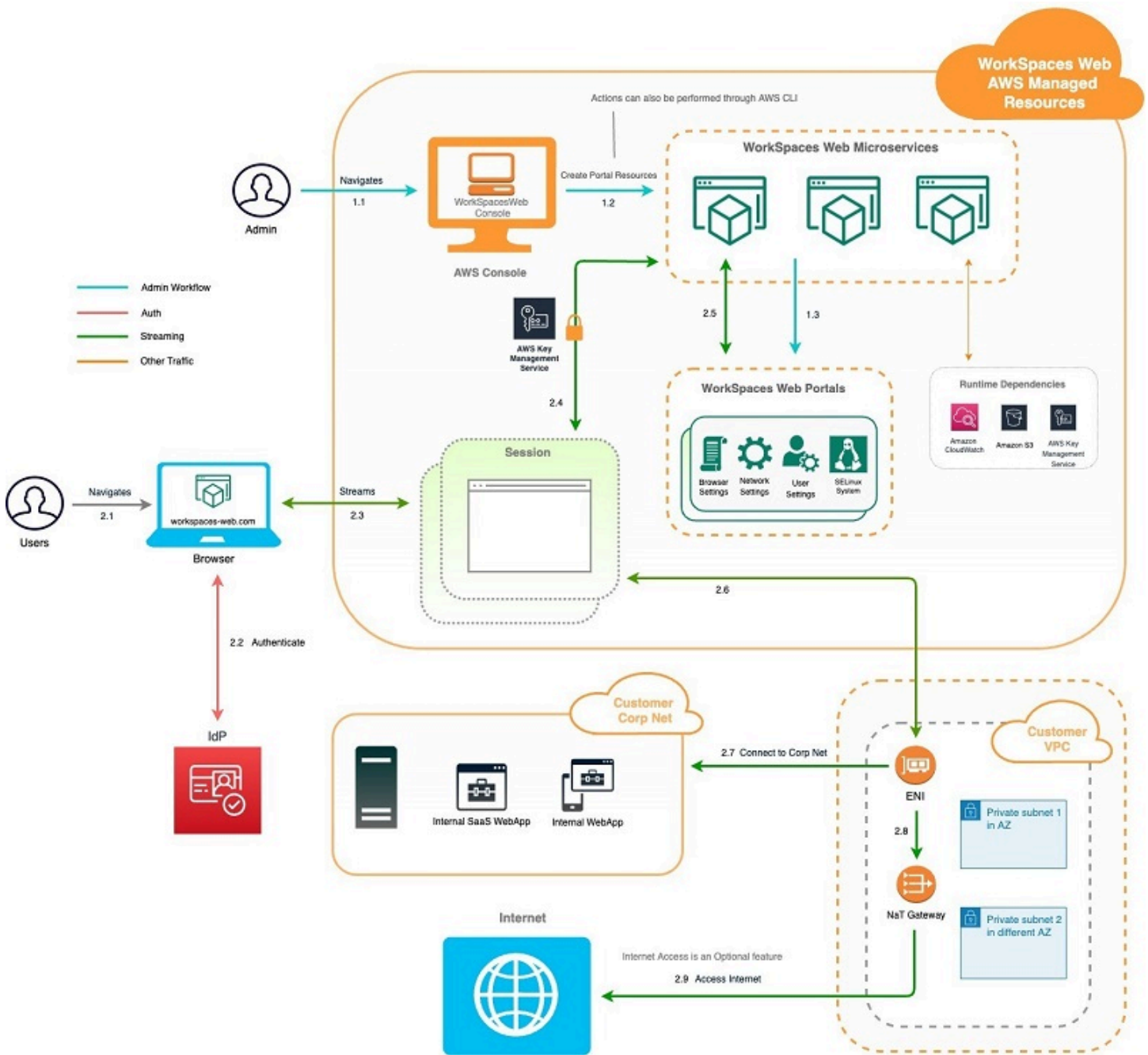
## Serviços relacionados

O WorkSpaces Web é um recurso do Amazon WorkSpaces no portfólio de computação do usuário final da AWS. Em comparação com o WorkSpaces e o AppStream 2.0, o WorkSpaces Web foi criado especificamente para facilitar workloads seguras e baseadas na web. O WorkSpaces Web é gerenciado automaticamente, com capacidade, escalabilidade e imagens provisionadas e atualizadas sob demanda pela AWS. Por exemplo, você pode optar por oferecer um Workspace Desktop persistente para seus desenvolvedores de software que precisam de acesso aos recursos de desktop e o Amazon WorkSpaces Web para os usuários da central de atendimento que só precisam acessar alguns sites internos e de SaaS (incluindo aqueles hospedados fora da sua rede) em computadores desktop.

## Arquitetura

O diagrama a seguir mostra a arquitetura do WorkSpaces Web.





## Acesso ao Amazon WorkSpaces Web

Os administradores acessam o Amazon WorkSpaces Web por meio do SDK, da CLI, da API ou do console do AWS WorkSpaces Web. Seus usuários o acessam por meio do endpoint do Amazon WorkSpaces Web.

# Configurando a Amazon WorkSpaces Web

Antes de configurar o Amazon WorkSpaces Web para acessar seus sites internos e aplicativos SaaS, você deve preencher os seguintes pré-requisitos.

## Tópicos

- [Cadastrar e criar um usuário](#)
- [Conceder acesso programático](#)
- [Redes e acesso](#)

## Cadastrar e criar um usuário

### Cadastrar-se em uma Conta da AWS

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

Para se cadastrar em uma Conta da AWS

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

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

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

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

## Criar um usuário administrativo

Depois de se inscrever em uma Conta da AWS, proteja seu Usuário raiz da conta da AWS, habilite o AWS IAM Identity Center e crie um usuário administrativo para não usar o usuário raiz em tarefas cotidianas.

### Proteger seu Usuário raiz da conta da AWS

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

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

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

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

### Criar um usuário administrativo

1. Habilitar o IAM Identity Center.

Para obter instruções, consulte [Enabling AWS IAM Identity Center](#) no Manual do Usuário do AWS IAM Identity Center.

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

Para ver um tutorial sobre como usar o Diretório do Centro de Identidade do IAM como fonte de identidade, consulte [Configure user access with the default Diretório do Centro de Identidade do IAM](#) no Manual do Usuário do AWS IAM Identity Center.

### Login como usuário administrativo

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

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

## Conceder acesso programático

Os usuários precisam de acesso programático se quiserem interagir com a AWS de fora do AWS Management Console. A forma de conceder acesso programático depende do tipo de usuário que está acessando a AWS.

Para conceder acesso programático aos usuários, selecione uma das seguintes opções:

Qual usuário precisa de acesso programático?	Para	Por
Identificação da força de trabalho  (Usuários gerenciados no Centro de Identidade do IAM)	Use credenciais temporárias para assinar solicitações programáticas para a AWS CLI, os SDKs da AWS ou as APIs da AWS.	Siga as instruções da interface que deseja utilizar. <ul style="list-style-type: none"> <li>Para a AWS CLI, consulte <a href="#">Configuração da AWS CLI para usar o AWS IAM Identity Center</a> no AWS Command Line Interface Guia do usuário da .</li> <li>Para os SDKs da AWS, ferramentas e APIs da AWS, consulte <a href="#">Autenticação do Centro de Identidade do IAM</a> no Guia de referência de ferramentas e SDKs da AWS.</li> </ul>
IAM	Use credenciais temporárias para assinar solicitações programáticas para a AWS CLI, os SDKs da AWS ou as APIs da AWS.	Siga as instruções em <a href="#">Como usar credenciais temporárias com recursos da AWS</a> no Guia do usuário do IAM.
IAM	(Não recomendado) Use credenciais de longo prazo para assinar solicitações programáticas para a	Siga as instruções da interface que deseja utilizar.

Qual usuário precisa de acesso programático?	Para	Por
	AWS CLI, os SDKs da AWS ou as APIs da AWS.	<ul style="list-style-type: none"><li>• Para a AWS CLI, consulte <a href="#">Autenticação usando as credenciais de usuário do IAM</a> no Guia do usuário da AWS Command Line Interface.</li><li>• Para as ferramentas e SDKs da AWS, consulte <a href="#">Autenticação usando as credenciais de longo prazo</a> no Guia de referência de ferramentas e SDKs da AWS.</li><li>• Para as APIs da AWS, consulte <a href="#">Gerenciamento de chaves de acesso de usuários do IAM</a> no Guia do usuário do IAM.</li></ul>

## Redes e acesso

Os tópicos a seguir explicam como configurar instâncias de streaming WorkSpaces da Web para que os usuários possam se conectar a elas. Também explica como permitir que suas instâncias de streaming WorkSpaces da Web acessem os recursos da VPC, bem como a Internet.

### Tópicos

- [Requisitos da VPC](#)
- [Recomendações de configuração da VPC](#)
- [Zonas de disponibilidade compatíveis](#)
- [Conexão de VPC](#)
- [Conexão cliente/usuário](#)

## Requisitos da VPC

Durante a criação do portal WorkSpaces da Web, você selecionará uma VPC em sua conta. Você também deverá escolher pelo menos duas sub-redes em duas zonas de disponibilidade diferentes. Essas VPCs e as sub-redes devem atender as seguintes requisitos:

- A VPC deve ter uma localização padrão. VPCs com localização dedicada não são compatíveis.
- Para considerar a disponibilidade, exigimos pelo menos duas sub-redes criadas em duas zonas de disponibilidade diferentes. Suas sub-redes devem ter endereços IP suficientes para suportar o tráfego esperado da WorkSpaces Web. Configure cada uma das sub-redes com uma máscara de sub-rede que permita endereços IP de cliente suficientes para contabilizar o número máximo de sessões simultâneas. Para ter mais informações, consulte [Criar e configurar uma nova VPC](#).
- Todas as sub-redes devem ter uma conexão estável com qualquer conteúdo interno, localizado no local Nuvem AWS ou no local, que os usuários acessarão com WorkSpaces a Web.

Recomendamos que você escolha três sub-redes em diferentes zonas de disponibilidade para considerar a disponibilidade e a escalabilidade. Para ter mais informações, consulte [Criar e configurar uma nova VPC](#).

WorkSpaces A Web não atribui nenhum endereço IP público às instâncias de streaming para permitir o acesso à Internet. Isso tornaria suas instâncias de streaming acessíveis pela internet. Portanto, qualquer instância de streaming conectada à sub-rede pública não terá acesso à internet. Se você quiser que seu portal WorkSpaces da Web tenha acesso ao conteúdo público da Internet e ao conteúdo privado da VPC, conclua as etapas em [Habilite a navegação irrestrita na internet \(recomendado\)](#)

### Criar e configurar uma nova VPC

Essa seção descreve como usar o assistente da VPC para criar uma VPC com uma sub-rede pública e uma sub-rede privada. Como parte desse processo, o assistente cria um gateway de Internet e um gateway NAT. Ele também cria uma tabela de rotas personalizada associada à sub-rede pública. Depois, ele atualiza a tabela de rotas principal associada à sub-rede privada. O gateway NAT é criado automaticamente na sub-rede pública da VPC.

Depois de usar o assistente para criar a configuração da VPC, você adicionará uma segunda sub-rede privada. Para obter mais informações sobre essa configuração, consulte [Exemplo: VPC com servidores em sub-redes privadas e NAT](#).

## Etapa 1: alocar um endereço IP elástico

Antes de criar sua VPC, você deve alocar um endereço IP elástico na sua WorkSpaces região da Web. Depois da alocação, associe o endereço IP elástico ao gateway NAT. Com um endereço IP elástico, você pode mascarar uma falha da instância de streaming fazendo rapidamente um novo mapeamento do endereço para outra instância de streaming na VPC. Para obter mais informações, consulte [Endereços IP elásticos](#).

### Note

Cobranças podem ser aplicadas aos endereços IP elásticos que você usa. Para obter mais informações, consulte a [Página de preços de Endereços IP elásticos](#).

Se você ainda não tiver um endereço IP elástico, conclua as etapas a seguir. Se desejar usar um endereço IP elástico existente, primeiro é necessário verificar se, no momento, ele não está associado a outra instância ou interface de rede.

Para alocar um endereço IP elástico

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, em Rede e segurança, selecione IPs elásticos.
3. Escolha Allocate New Address (Alocar novo endereço) e Allocate (Alocar).
4. Observe o endereço IP elástico mostrado no console.
5. No canto superior direito do painel IPs elásticos, clique no ícone × para fechar o painel.

## Etapa 2: criar uma VPC

Conclua as etapas a seguir para criar uma VPC com uma sub-rede pública e uma sub-rede privada.

Como criar uma nova VPC

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, escolha VPC Dashboard (Painel da VPC).
3. Selecione Launch VPC Wizard (Iniciar o assistente de VPC).
4. Em Step 1: Select a VPC Configuration (Etapa 1: selecionar uma configuração de VPC), escolha VPC with Public and Private Subnets (VPC com sub-redes públicas e privadas) e Select (Selecionar).

5. Em Step 2: VPC with Public and Private Subnets (VPC com sub-redes públicas e privadas), configure a VPC da seguinte forma:
- Em IPv4 CIDR block (Bloco CIDR IPv4), especifique um bloco CIDR IPv4 para sua VPC.
  - Em IPv6 CIDR block (Bloco CIDR IPv6), mantenha o valor padrão, No IPv6 CIDR Block (Nenhum bloco CIDR IPv6).
  - Em Nome da VPC, insira um nome exclusivo para a VPC.
  - Configure a sub-rede pública da seguinte forma:
    - Em Public subnet's IPv4 CIDR (CIDR IPv4 da sub-rede pública), especifique o bloco CIDR da sub-rede.
    - Em Availability Zone (Zona de disponibilidade), mantenha o valor padrão, No Preference (Sem preferência).
    - Em Nome da sub-rede pública, insira um nome para a sub-rede. Por exemplo, **WorkSpaces Web Public Subnet**.
  - Configure a primeira sub-rede privada da seguinte forma:
    - Em Private subnet's IPv4 CIDR (CIDR IPv4 da sub-rede privada), especifique o bloco CIDR para a sub-rede. Anote o valor especificado.
    - Em Availability Zone (Zona de disponibilidade), selecione uma zona específica e anote a zona selecionada.
    - Em Nome da sub-rede privada, insira um nome para a sub-rede. Por exemplo, **WorkSpaces Web Private Subnet1**.
  - Mantenha os valores padrão nos campos restantes, quando aplicável.
  - Em ID da alocação do IP elástico, insira o valor que corresponde ao endereço IP elástico que você criou. Esse endereço é então atribuído ao gateway NAT. Se você não tiver um endereço IP elástico, crie um usando o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
  - Em Endpoints de serviço, se um endpoint do Amazon S3 for necessário para seu ambiente, especifique um.

Para especificar um endpoint do Amazon S3, faça o seguinte:

1. Escolha Add Endpoint (Adicionar endpoint).
2. Em Serviço, selecione com.amazonaws.**Região**.s3, em que **Região** é a Região da AWS na qual você está criando a VPC.



4. Em Policy (Política), mantenha o valor padrão, Full Access (Acesso total).

  - Em Enable DNS hostnames (Habilitar nomes de host DNS), mantenha o valor padrão, Yes (Sim).
  - Em Hardware tenancy (Locação de hardware), mantenha o valor padrão, Default (Padrão).
  - Escolha Create VPC (Criar VPC).
  - A configuração da VPC leva vários minutos. Após a criação da VPC, escolha OK.

### Etapa 3: adicionar uma segunda sub-rede privada

Na etapa anterior, você criou uma VPC com uma sub-rede pública e uma sub-rede privada. Conclua as etapas a seguir para adicionar uma segunda sub-rede privada à VPC. Recomendamos que você adicione uma segunda sub-rede privada em uma zona de disponibilidade diferente da primeira sub-rede privada.

#### Para adicionar uma segunda sub-rede privada

1. No painel de navegação, escolha Sub-redes.
2. Selecione a primeira sub-rede privada que você criou na etapa anterior. Na guia Description (Descrição), abaixo da lista de sub-redes, anote a zona de disponibilidade dessa sub-rede.
3. No canto superior esquerdo do painel de sub-redes, escolha Create Subnet (Criar sub-rede).
4. Em Etiqueta de nome, insira um nome para a sub-rede privada. Por exemplo, **WorkSpaces Web Private Subnet2**.
5. Em VPC, selecione a VPC que você criou na etapa anterior.
6. Em Zona de disponibilidade, selecione uma zona de disponibilidade diferente da que você está usando para sua primeira sub-rede privada. Selecionar uma zona de disponibilidade diferente aumenta a tolerância a falhas e ajuda a evitar erros de capacidade insuficiente.
7. Em IPv4 CIDR block (Bloco CIDR IPv4), especifique um intervalo de blocos CIDR exclusivo para a nova sub-rede. Por exemplo, se a primeira sub-rede privada tiver um intervalo de blocos CIDR IPv4 de **10.0.1.0/24**, você poderá especificar um intervalo de blocos CIDR de **10.0.2.0/24** para a segunda sub-rede privada.
8. Escolha Criar.
9. Depois que a sub-rede for criada, selecione Close (Fechar).

## Etapa 4: verificar e nomear as tabelas de rota de sub-rede

Depois de criar e configurar a VPC, conclua as etapas a seguir para especificar um nome para as tabelas de rotas. Você precisará verificar se os detalhes a seguir estão corretos em sua tabela de rotas:

- A tabela de rotas associada à sub-rede em que reside o gateway NAT deve incluir uma rota que aponta o tráfego da internet para um gateway da Internet. Isso garante que seu gateway NAT possa acessar a Internet.
- As tabelas de rota associadas às sub-redes privadas devem ser configuradas para apontar o tráfego da internet para o gateway NAT. Isso permite que as instâncias de streaming nas sub-redes privadas se comuniquem com a Internet.

Para verificar e nomear as tabelas de rotas da sub-rede

1. No painel de navegação, escolha Sub-redes e selecione a sub-rede pública que você criou. Por exemplo, WorkSpaces Web 2.0 Public Subnet.
2. Na Tabela de rotas, escolha o ID da tabela de rotas. Por exemplo, rtb-12345678.
3. Selecione a tabela de rotas do . Em Nome, escolha o ícone de edição (lápiz) e insira um nome para a tabela. Por exemplo, insira o nome **workspacesweb-public-routetable**. Depois, selecione a marca de seleção para salvar o nome.
4. Com a tabela de rotas públicas ainda selecionada, na guia Rotas, verifique se há duas rotas: uma para o tráfego local e outra que envie todo o outro tráfego para o gateway da Internet da VPC. A tabela a seguir descreve essas duas rotas:

Destination (Destino)	Destino	Descrição
Bloco CIDR IPv4 de sub-rede pública (por exemplo, 10.0.0/20)	Local	Todo o tráfego dos recursos destinados a endereços IPv4 dentro do bloco CIDR IPv4 da sub-rede pública. Esse tráfego é roteado localmente dentro da VPC.
Tráfego destinado a todos os outros endereços IPv4 (por exemplo, 0.0.0.0/0)	Saída (igw-ID)	O tráfego destinado a todos os outros endereços IPv4 é roteado para o gateway da

Destination (Destino)	Destino	Descrição
		Internet (identificado por igw-ID) criado pelo assistente da VPC.

- No painel de navegação, escolha Sub-redes. Depois, selecione a primeira sub-rede privada que você criou (por exemplo, **WorkSpaces Web Private Subnet1**).
- Na guia Tabela de rotas, escolha o ID da tabela de rotas.
- Selecione a tabela de rotas do . Em Nome, escolha o ícone de edição (lápis) e insira um nome para a tabela. Por exemplo, insira o nome **workspacesweb-private-routetable**. Depois, selecione a marca de verificação para salvar o nome.
- Na guia Routes (Rotas), verifique se a tabela de rotas inclui as seguintes rotas:

Destination (Destino)	Destino	Descrição
Bloco CIDR IPv4 de sub-rede pública (por exemplo, 10.0.0/20)	Local	Todo o tráfego dos recursos destinados a endereços IPv4 dentro do bloco CIDR IPv4 da sub-rede pública é roteado localmente dentro da VPC.
Tráfego destinado a todos os outros endereços IPv4 (por exemplo, 0.0.0.0/0)	Saída (nat-ID)	O tráfego destinado a todos os outros endereços IPv4 é roteado para o gateway NAT (identificado por nat-ID).
Tráfego destinado a buckets do S3 (aplicável se você especificou um endpoint do S3) [pl-ID (com.amazonaws.region.s3)]	Armazenamento (vpce-ID)	O tráfego destinado aos buckets do S3 é roteado para o endpoint do S3 (identificado por vpce-ID).

- No painel de navegação, escolha Sub-redes. Depois, selecione a segunda sub-rede privada que você criou (por exemplo, **WorkSpaces Web Private Subnet2**).

10. Na guia Tabela de rotas, verifique se a tabela de rotas selecionada é a privada (por exemplo, **workspacesweb-private-routetable**). Se a tabela de rotas for diferente, escolha Editar e selecione sua tabela de rotas.

## Habilite a navegação irrestrita na internet (recomendado)

Siga estas etapas para configurar uma VPC com um gateway NAT para navegação irrestrita na internet. Isso concede acesso à WorkSpaces Web a sites na Internet pública e sites privados hospedados em ou com uma conexão com sua VPC.

Para configurar uma VPC com um gateway NAT para navegação irrestrita na internet

Se você quiser que seu portal WorkSpaces da Web tenha acesso tanto ao conteúdo público da Internet quanto ao conteúdo privado da VPC, siga estas etapas:

### Note

Se você já configurou uma VPC, conclua as etapas a seguir para adicionar um gateway NAT à VPC. Se você precisar criar uma nova VPC, consulte [Criar e configurar uma nova VPC](#).

1. Para criar o gateway NAT, conclua as etapas em [Create a NAT gateway](#). Certifique-se de que esse gateway NAT tenha conectividade pública e esteja em uma sub-rede pública na VPC.
2. Você deve especificar ao menos duas sub-redes privadas de zonas de disponibilidade diferentes. Atribuir suas sub-redes a diferentes zonas de disponibilidade ajuda a garantir melhor disponibilidade e tolerância a falhas. Para obter informações sobre como criar uma segunda sub-rede privada, consulte [the section called “Etapa 3: adicionar uma segunda sub-rede privada”](#).

### Note

Para garantir que todas as instâncias de streaming tenham acesso à Internet, não conecte uma sub-rede pública ao seu portal WorkSpaces da Web.

3. Atualize a tabela de rotas associada às sub-redes privadas para apontar o tráfego vinculado à internet para o gateway NAT. Isso permite que as instâncias de streaming nas sub-redes privadas se comuniquem com a Internet. Para obter informações sobre como associar uma tabela de rotas a uma sub-rede privada, conclua as etapas em [Configurar tabelas de rotas](#).

## Ativar navegação restrita na Internet (usando proxy HTTP de saída)

A configuração de rede recomendada de um portal WorkSpaces da Web é usar sub-redes privadas com o gateway NAT, para que o portal possa navegar pela Internet pública e pelo conteúdo privado. Para ter mais informações, consulte [the section called “Habilite a navegação irrestrita na internet \(recomendado\)”](#). No entanto, talvez seja necessário controlar a comunicação de saída de um portal WorkSpaces da Web para a Internet usando um proxy da Web. Por exemplo, se você usar um proxy da Web como porta de entrada para a Internet, poderá implementar controles preventivos de segurança, como lista de permissões de domínio e filtragem de conteúdo. Isso também pode reduzir o uso da largura de banda e melhorar o desempenho da rede armazenando em cache recursos acessados com frequência, como páginas da Web ou atualizações de software localmente. Para alguns casos de uso, você pode ter conteúdo privado que só pode ser acessado por meio de um proxy da web.

Talvez você já esteja familiarizado com a configuração de proxy em dispositivos gerenciados ou na imagem de seus ambientes virtuais. Mas isso representa desafios se você não estiver no controle do dispositivo (por exemplo, quando os usuários estão em dispositivos que não são de propriedade ou gerenciados pela empresa) ou se você precisa gerenciar a imagem em seu ambiente virtual. Com a WorkSpaces Web, você pode definir configurações de proxy usando as políticas do Chrome incorporadas ao navegador da Web. Você pode fazer isso configurando um proxy de saída HTTP para a WorkSpaces Web.

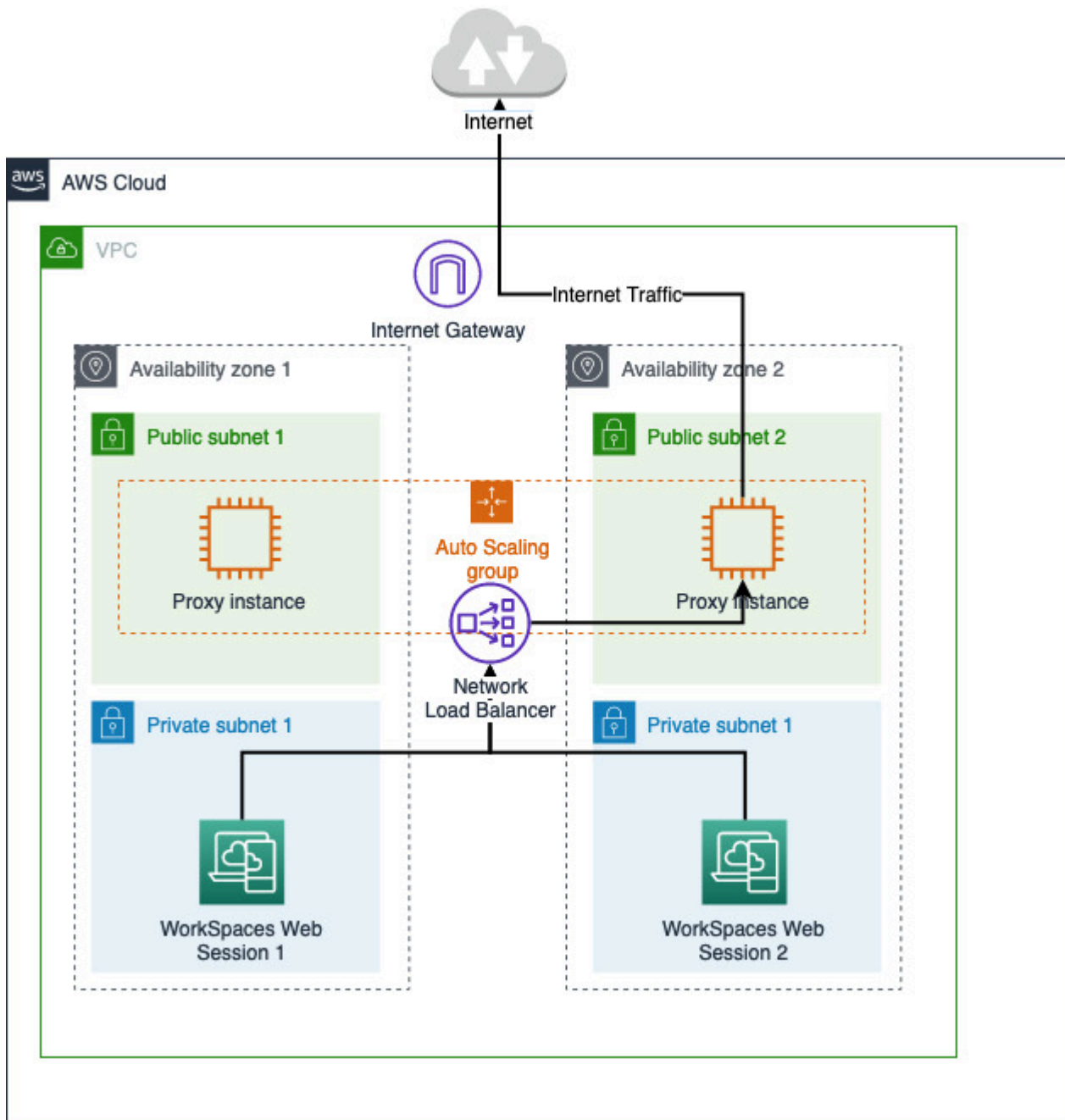
Essa solução é baseada em uma configuração recomendada de proxy VPC de saída. A solução de proxy é baseada no proxy HTTP de código aberto [Squid](#). Em seguida, ele usa as configurações do navegador WorkSpaces da Web para configurar o portal WorkSpaces da Web para se conectar ao endpoint do proxy. Para obter mais informações, consulte [Como configurar um proxy VPC de saída com lista branca de domínio e filtragem](#) de conteúdo.

Essa solução oferece os seguintes benefícios:

- Um proxy de saída que inclui um grupo de instâncias do Amazon EC2 com escalabilidade automática, hospedadas por um balanceador de carga de rede. As instâncias de proxy residem em uma sub-rede pública e cada uma delas é conectada com um IP elástico, para que possam ter acesso à Internet.
- Um portal WorkSpaces da Web implantado em sub-redes privadas. Você não precisa configurar o gateway NAT para habilitar o acesso à Internet. Em vez disso, você configura a política do seu navegador para que todo o tráfego da Internet passe pelo proxy de saída. Se você quiser usar seu próprio proxy, a configuração do portal WorkSpaces da Web será semelhante.

## Arquitetura

Veja a seguir um exemplo de uma configuração típica de proxy em sua VPC. A instância proxy do Amazon EC2 está em sub-redes públicas e associada ao Elastic IP, então elas têm acesso à Internet. Um balanceador de carga de rede hospeda um grupo de instâncias de proxy com escalabilidade automática. Isso garante que as instâncias de proxy possam ser escaladas automaticamente e que o balanceador de carga de rede seja o único endpoint de proxy, que pode ser consumido pelas sessões WorkSpaces da Web.



## Pré-requisitos

Antes de começar, verifique se você atende aos seguintes pré-requisitos:

- Você precisa de uma VPC já implantada, com sub-redes públicas e privadas espalhadas por várias zonas de disponibilidade (AZs). Para obter mais informações sobre como configurar seu ambiente de VPC, consulte VPCs [padrão](#).
- Você precisa de um único endpoint de proxy que seja acessível a partir de sub-redes privadas, onde as sessões WorkSpaces da Web estão localizadas (por exemplo, o nome DNS do balanceador de carga de rede). Se você quiser usar seu proxy existente, certifique-se de que ele também tenha um único endpoint acessível a partir de suas sub-redes privadas.

### Configurar um proxy de saída HTTP para WorkSpaces a Web

Para configurar um proxy de saída HTTP para a WorkSpaces Web, siga estas etapas.

1. Para implantar um exemplo de proxy de saída em sua VPC, siga as etapas [em Como configurar um proxy VPC de saída com lista branca de domínio e filtragem de conteúdo](#).
  - a. Siga as etapas em “Instalação (configuração única)” para implantar o CloudFormation modelo em sua conta. Certifique-se de escolher a VPC e as sub-redes corretas como parâmetros do modelo. CloudFormation
  - b. Após a implantação, encontre o parâmetro CloudFormation de saída OutboundProxyDomainOutboundProxyPorte. Esse é o nome e a porta DNS do seu proxy.
  - c. Se você já tem seu próprio proxy, pule esta etapa e use o nome e a porta DNS do seu proxy.
2. Na WorkSpaces Web, console, selecione seu portal e, em seguida, escolha Editar.
  - a. Nos detalhes da conexão de rede, escolha a VPC e as sub-redes privadas que têm acesso ao proxy.
  - b. Nas configurações de política, adicione a ProxySettings política a seguir usando um editor JSON. O ProxyServer campo deve ser o nome e a porta DNS do seu proxy. Para obter mais detalhes sobre a ProxySettings política, consulte [ProxySettings](#).

```
{
  "chromePolicies":
  {
    ...
    "ProxySettings": {
      "value": {
```

```
        "ProxyMode": "fixed_servers",
        "ProxyServer": "OutboundProxyLoadBalancer-0a01409a46943c47.elb.us-
west-2.amazonaws.com:3128",
        "ProxyBypassList": "https://www.example1.com,https://
www.example2.com,https://internalsite/"
    }
},
}
}
```

3. Em sua sessão na WorkSpaces Web, você verá que o proxy é aplicado à configuração do Chrome. O Chrome está usando as configurações de proxy do seu administrador.
4. Acesse `chrome://policy` e a guia Política do Chrome para confirmar se a política foi aplicada.
5. Verifique se sua sessão WorkSpaces da Web pode navegar com êxito pelo conteúdo da Internet sem o gateway NAT. Nos CloudWatch Registros, verifique se os registros de acesso ao proxy do Squid estão registrados.

## Solução de problemas

Depois que a política do Chrome for aplicada, se sua sessão WorkSpaces da Web ainda não conseguir acessar a Internet, siga estas etapas para tentar resolver o problema:

- Verifique se o endpoint do proxy está acessível a partir das sub-redes privadas em que seu portal WorkSpaces da Web reside. Para fazer isso, crie uma instância do EC2 na sub-rede privada e teste a conexão da instância privada do EC2 com seu endpoint de proxy.
- Verifique se o proxy tem acesso à Internet.
- Verifique se a política do Chrome está correta.
  - Confirme a seguinte formatação para o ProxyServer campo da política: `<Proxy DNS name>:<Proxy port>`. Não deve haver `http://` ou `https://` no prefixo.
  - Na sessão da WorkSpaces Web, use o Chrome para navegar até `chrome://policy` e verifique se a ProxySettings política foi aplicada com sucesso.

## Recomendações de configuração da VPC

As recomendações a seguir podem ajudá-lo a configurar sua VPC de forma mais eficaz e segura.

### Configuração geral da VPC



- Verifique se a configuração da VPC pode satisfazer suas necessidades de escalabilidade.
- Certifique-se de que suas cotas de serviços WorkSpaces da Web (também chamadas de limites) sejam suficientes para atender à demanda prevista. Para solicitar um aumento na cota, use o console do Service Quotas em <https://console.aws.amazon.com/servicequotas/>. Para obter informações sobre cotas padrão WorkSpaces da Web, consulte [the section called “Solicitar um aumento de cota de serviço”](#).
- Se você planeja fornecer às suas sessões de streaming acesso à Internet, recomendamos que você configure uma VPC com um gateway NAT em uma sub-rede pública.

## Interfaces de rede elástica

- Cada sessão WorkSpaces da Web requer sua própria interface de elastic network durante a duração do streaming. WorkSpaces A Web cria tantas [interfaces de rede elásticas](#) (ENIs) quanto a capacidade máxima desejada de sua frota. Por padrão, o limite de ENIs por região é de 5.000. Para obter mais informações, consulte [Interfaces de rede](#).

Ao planejar a capacidade para implantações muito grandes, por exemplo, milhares de sessões de streaming simultâneas, considere o número de ENIs que podem ser necessárias para seu uso máximo. Recomendamos que você mantenha seu limite de ENI igual ou superior ao limite máximo de uso simultâneo que você configura para seu portal da web.

## Subredes

- Ao desenvolver seu plano para aumentar a escala de usuários, lembre-se de que cada sessão WorkSpaces da Web exige um endereço IP de cliente exclusivo das sub-redes configuradas. Portanto, o tamanho do espaço de endereço IP do cliente configurado em suas sub-redes determina o número de usuários que podem fazer streaming simultaneamente.
- Recomendamos que cada sub-rede seja configurada com uma máscara de sub-rede que permita endereços IP de cliente suficientes para contabilizar o número máximo de usuários simultâneos esperados. Além disso, considere adicionar mais endereços IP para comportar o crescimento previsto. Para obter mais informações, consulte [Dimensionamento da VPC e da sub-rede para IPv4](#).
- Recomendamos que você configure uma sub-rede em cada zona de disponibilidade exclusiva que a WorkSpaces Web oferece suporte na região desejada para considerar a disponibilidade e a escalabilidade. Para ter mais informações, consulte [the section called “Criar e configurar uma nova VPC”](#).

- Verifique se os recursos de rede necessários para suas aplicações web podem ser acessados pelas sub-redes.

## Grupos de segurança

- Use grupos de segurança para fornecer controle de acesso adicional à sua VPC.

Os grupos de segurança que pertencem à sua VPC permitem que você controle o tráfego de rede entre as instâncias de streaming WorkSpaces da Web e os recursos de rede exigidos pelos aplicativos da Web. Verifique se os grupos de segurança fornecem acesso aos recursos de rede que as aplicações web exigem.

## Zonas de disponibilidade compatíveis

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

Uma zona de disponibilidade é representada por um código de região seguido por um identificador de letra, por exemplo, `us-east-1a`. Para garantir a distribuição de recursos entre as zonas de disponibilidade de uma região, mapeamos as zonas de disponibilidade de forma independente para os nomes de cada conta da AWS. Por exemplo, a zona de disponibilidade da `us-east-1a` para sua conta da AWS pode não ter o mesmo local que a `us-east-1a` de outra conta da AWS.

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

A visualização de IDs de AZs permite determinar o local de recursos em uma conta em relação aos recursos em outra conta. Por exemplo, se você compartilhar uma sub-rede na zona de disponibilidade com o ID de AZ `us-east-1-az2` com outra conta, essa sub-rede estará disponível para essa conta na zona de disponibilidade cujo ID de AZ também é `us-east-1-az2`. O ID da AZ de cada VPC e sub-rede é exibido no console da Amazon VPC.

WorkSpaces A Web está disponível em um subconjunto das zonas de disponibilidade para cada região suportada. A tabela a seguir lista os IDs de AZ que você pode usar para cada região. Para ver o mapeamento de IDs de AZ para zonas de disponibilidade em sua conta, consulte [AZ IDs for Your Resources](#) no Guia do usuário do AWS RAM.

Nome da região	Código da região	IDs de AZ compatíveis
Leste dos EUA (Norte da Virgínia)	us-east-1	use1-az1, use1-az2, use1-az4, use1-az5, use1-az6
Oeste dos EUA (Oregon)	us-west-2	usw2-az1, usw2-az2, usw2-az3
Asia Pacific (Mumbai)	ap-south-1	aps1-az1, aps1-az3
Ásia-Pacífico (Seul)	ap-northeast-2	apne2-az1 , apne2-az2 , apne2-az3
Ásia-Pacífico (Singapura)	ap-southeast-1	apse1-az1 , apse1-az2 , apse1-az3
Ásia-Pacífico (Sydney)	ap-southeast-2	apse2-az1 , apse2-az2 , apse2-az3
Ásia-Pacífico (Tóquio)	ap-northeast-1	apne1-az1 , apne1-az2 , apne1-az4
Canadá (Central)	ca-central-1	cac1-az1, cac1-az2, cac1-az4
Europa (Frankfurt)	eu-central-1	euc1-az2, euc1-az2, euc1-az3
Europa (Irlanda)	eu-west-1	euw1-az1, euw1-az2, euw1-az3
Europa (Londres)	eu-west-2	euw2-az1, euw2-az2

Para obter mais informações sobre zonas de disponibilidade e IDs de AZ, consulte [Regiões, zonas de disponibilidade e Local Zones](#) no Guia do usuário do Amazon EC2 para instâncias do Linux.

## Conexão de VPC

Cada instância de streaming WorkSpaces da Web tem uma interface de rede do cliente que fornece conectividade aos recursos em sua VPC, bem como à Internet, se sub-redes privadas com gateway NAT estiverem configuradas.

Para conectividade com a Internet, as portas a seguir devem ser abertas para todos os destinos. Se você estiver usando um grupo de segurança personalizado ou modificado, será necessário adicionar as regras exigidas manualmente. Para obter mais informações, consulte [Regras de grupos de segurança](#).

### Note

Isso se aplica ao tráfego de saída.

- TCP 80 (HTTP)
- TCP 443 (HTTPS)
- UDP 8433

## Conexão cliente/usuário

WorkSpaces A Web está configurada para rotear conexões de streaming pela Internet pública. A conectividade com a Internet é necessária para autenticar os usuários e fornecer os ativos da Web que a WorkSpaces Web requer para funcionar. Para permitir esse tráfego, você deve inserir os domínios listados em [Domínios permitidos](#).

Os tópicos a seguir fornecem informações sobre como habilitar conexões de usuário com a WorkSpaces Web.

### Tópicos

- [Requisitos de endereço IP e porta](#)
- [Domínios permitidos](#)

## Requisitos de endereço IP e porta

Para acessar instâncias WorkSpaces da Web, os dispositivos do usuário exigem acesso de saída nas seguintes portas:

- Porta 443 (TCP)
  - A porta 443 é usada para comunicação HTTPS entre dispositivos de usuário e instâncias de streaming ao usar os endpoints de internet. Normalmente, quando os usuários finais navegam na web durante sessões de streaming, o navegador da web seleciona aleatoriamente uma porta de origem no intervalo para streaming de tráfego. Você deve garantir que o tráfego de retorno para essa porta seja permitido.
  - Essa porta deve estar aberta para os domínios exigidos listados em [Domínios permitidos](#).
  - AWS publica seus intervalos de endereços IP atuais, incluindo os intervalos para os quais o Session Gateway e CloudFront os domínios podem resolver, no formato JSON. Para obter informações sobre como baixar o arquivo.json e visualizar os intervalos atuais, consulte [Intervalos de endereços IP da AWS](#). Ou, se estiver usando AWS Tools for Windows PowerShell, você pode acessar as mesmas informações usando o `Get-AWSPublicIpAddressRange` PowerShell comando. Para obter mais informações, consulte [Consultar intervalos de endereços IP públicos para a AWS](#).
- (Opcional) Porta 53 (UDP)
  - A porta 53 é usada para comunicação entre dispositivos de usuário e os servidores DNS.
  - Essa porta é opcional se você não estiver usando servidores DNS para resolução de nomes de domínio.
  - A porta deve estar aberta para os endereços IP dos seus servidores DNS, de forma que os nomes de domínio público possam ser resolvidos.

## Domínios permitidos

Para que o usuário possa acessar o serviço WorkSpaces Web a partir do navegador local, você deve adicionar os seguintes domínios e endereços IP à lista de permissões na rede a partir da qual o usuário está tentando acessar o serviço.

A *{Região}* abaixo deve ser substituída pelo nome da Região da AWS em operação. Por exemplo, `s3.{região}.amazonaws.com` deverá ser `s3.eu-west-1.amazonaws.com` se for para Europa (Irlanda) (eu-west-1).

Categoria	Domínio ou endereço IP
WorkSpaces Ativo de streaming na web	s3. <i>{região}</i> .amazonaws.com s3.amazonaws.com appstream2. <i>{região}</i> .aws.amazon.com *.amazonappstream.com *.shortbread.aws.dev
WorkSpaces WebApp Ativo da Web	*.workspaces-web.com
WorkSpaces Autenticação Web	*.auth. <i>{região}</i> .amazoncognito.com cognito-identity. <i>{região}</i> .amazonaws.com cognito-idp. <i>{região}</i> .amazonaws.com *.cloudfront.net
WorkSpaces Métricas e relatórios da Web	*.execute-api. <i>{região}</i> .amazonaws.com unagi-na.amazon.com

Dependendo do seu provedor de identidade configurado, talvez você também precise incluir domínios adicionais à lista de permissões. Revise a documentação do seu IdP para identificar quais domínios você precisa permitir a lista para que a WorkSpaces Web use esse provedor. Se você estiver usando o Centro de Identidade do IAM, consulte [IAM Identity Center prerequisites](#) para obter mais informações.

# Começando com a Amazon WorkSpaces Web

Siga estas etapas para criar um portal WorkSpaces da Web e fornecer aos usuários acesso a sites internos e SaaS a partir de seus navegadores existentes. É possível criar um portal da web em qualquer região com suporte por conta.

## Note

Para solicitar um aumento de limite para mais de um portal, entre em contato com o suporte com seu Conta da AWS ID, número de portais a serem solicitados e. Região da AWS

Esse processo normalmente leva cinco minutos com o assistente de criação do portal da web e até 15 minutos adicionais para que o portal se torne Ativo.

Não há custos associados à criação de um portal da web. WorkSpaces A Web oferece pay-as-you-go preços, incluindo um preço baixo mensal para usuários que usam ativamente o serviço. Não há custos antecipados, licenças nem compromissos de longo prazo.

## Important

Antes de começar, você deve atender aos pré-requisitos necessários para um portal da web. Para ter mais informações sobre os pré-requisitos do portal da web, consulte [Configurando a Amazon WorkSpaces Web](#).

## Tópicos

- [Etapa 1: criar um portal da web](#)
- [Etapa 2: testar o portal da web](#)
- [Etapa 3: distribuir o portal da web](#)
- [Próximas etapas](#)

## Etapa 1: criar um portal da web

Siga estas etapas para criar um portal da web.

## Tópicos

- [Definir configurações de rede](#)
- [Definir configurações do portal](#)
- [Definir as configurações do usuário](#)
- [Configurar o provedor de identidades](#)
- [Analisar e executar](#)

## Definir configurações de rede

1. Abra o console WorkSpaces da Web em <https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/>.
2. Escolha WorkSpaces Web, depois Portais da Web e escolha Criar portal da Web.
3. Na página Etapa 1: especificar conexão de rede, conclua as etapas a seguir para conectar a VPC ao portal da web e configurar a VPC e sub-redes.
  1. Para obter detalhes da rede, escolha uma VPC com uma conexão com o conteúdo que você deseja que seus usuários acessem com WorkSpaces a Web.
  2. Escolha até três sub-redes privadas que atendam aos requisitos a seguir. Para ter mais informações, consulte [Redes e acesso](#).
    - Escolha um mínimo de duas sub-redes privadas para criar um portal.
    - Para garantir a alta disponibilidade do portal da web, recomendamos que você forneça o número máximo de sub-redes privadas em zonas de disponibilidade exclusivas para a VPC.
  3. Escolha um grupo de segurança.

## Definir configurações do portal

Na página Etapa 2: definir configurações do portal da web, conclua as etapas a seguir para personalizar a experiência de navegação dos usuários quando eles iniciam uma sessão.

1. Em Detalhes do portal da Web, em Nome de exibição, insira um nome identificável para o seu portal da web.
2. Em Log de acesso do usuário, em ID de fluxo do Kinesis, selecione o fluxo de dados do Amazon Kinesis para o qual você deseja enviar seus dados. Para ter mais informações, consulte [the section called “Configurar o registro de acesso do usuário”](#).



### 3. Em Configurações de política, conclua o seguinte:

- Para Opções de política, selecione Editor visual ou Carregamento do arquivo JSON. Você pode usar qualquer um dos métodos para fornecer os detalhes da configuração da política para o portal da web. Para ter mais informações, consulte [the section called “Definir ou editar a política de navegador”](#).
- WorkSpaces A Web inclui suporte para as políticas corporativas do Chrome. É possível adicionar e gerenciar políticas com um editor visual ou um carregamento manual de arquivos de políticas. É possível alternar entre qualquer uma das opções a qualquer momento.
- Ao carregar um arquivo de política, você pode ver as políticas disponíveis no arquivo no console. No entanto, não é possível editar todas as políticas no editor visual. O console lista políticas no arquivo JSON que você não pode editar com o editor visual em Políticas JSON adicionais. Para fazer alterações nessas políticas, você deve editá-las manualmente.
- (Opcional) Em URL de inicialização – opcional, insira um domínio para usar como página inicial quando os usuários iniciarem o navegador. A VPC deve ter uma conexão estável com esse URL.
- Selecione ou desmarque a opção de Navegação privada e Exclusão do histórico para ativar ou desativar esses recursos durante a sessão de um usuário.

#### Note

Os URLs visitados durante a navegação privada ou antes de um usuário excluir o histórico do navegador não podem ser registrados no log de acesso do usuário. Para ter mais informações, consulte [the section called “Configurar o registro de acesso do usuário”](#).

- Em Filtragem de URL, você pode configurar quais URLs os usuários podem visitar durante uma sessão. Para ter mais informações, consulte [the section called “Configurar a filtragem de URL”](#).
- (Opcional) Em Marcadores do navegador – opcional, insira o Nome de exibição, o Domínio e a Pasta de favoritos que você deseja que os usuários vejam no navegador. Depois, escolha Adicionar marcador.

#### Note

Domínio é um campo obrigatório para os favoritos do navegador.

No Chrome, os usuários podem encontrar marcadores gerenciados na pasta Gerenciador de favoritos na barra de ferramentas de favoritos.

- (Opcional) Adicione Tags ao seu portal. Você pode usar tags para pesquisar ou filtrar seus AWS recursos. As tags consistem em uma chave e um valor opcional e estão associadas ao recurso do portal.
4. Em Controle de acesso de IP (opcional), escolha se deseja restringir o acesso a redes confiáveis. Para ter mais informações, consulte [the section called “Configurar controles de acesso de IP \(opcional\)”](#).
  5. Escolha Próximo para continuar.

## Definir as configurações do usuário

Na página Etapa 3: selecionar configurações do usuário, conclua as etapas a seguir para escolher quais recursos os usuários podem acessar na barra de navegação superior durante a sessão e escolha Próximo:

1. Em Permissões de usuário, escolha se deseja habilitar a extensão para login único. Para ter mais informações, consulte [the section called “Habilitar extensão para autenticação única \(opcional\)”](#).
2. Em Permissões da área de transferência, escolha Desabilitadas ou Habilitadas.
3. Em Transferência de arquivos, escolha Desabilitada ou Habilitada.
4. Em Imprimir no dispositivo local, escolha Permitido ou Não permitido.
5. Em Detalhes da sessão do usuário, especifique o seguinte:
  - Para Disconnect timeout in minutes (Tempo limite de desconexão em minutos), escolha a quantidade de tempo que uma sessão de streaming permanece ativa após os usuários se desconectarem. Se os usuários tentarem se reconectar à sessão de streaming após uma desconexão ou interrupção na rede dentro desse intervalo de tempo, eles serão conectados à sessão anterior. Caso contrário, eles serão conectados a uma nova sessão com uma nova instância de streaming.

Se um usuário encerrar a sessão, o tempo limite de desconexão não se aplicará. Em vez disso, o usuário é solicitado a salvar os documentos abertos e, depois, é desconectado imediatamente da instância de streaming. A instância que o usuário estava usando é encerrada.

- Para Idle disconnect timeout in minutes (Tempo limite de desconexão de inatividade em minutos), escolha a quantidade de tempo em que os usuários podem ficar ociosos (inativos) antes de serem desconectados de sua sessão de streaming e o início do intervalo de tempo de Disconnect timeout in minutes (Tempo limite de desconexão em minutos). Os usuários são notificados antes de serem desconectados devido à inatividade. Se eles tentarem reconectar-se à sessão de streaming antes do intervalo de tempo especificado em Disconnect timeout in minutes (Tempo limite de desconexão em minutos) terminar, eles são conectados à sessão anterior. Caso contrário, eles serão conectados a uma nova sessão com uma nova instância de streaming. Definir esse valor como 0 o desabilita. Quando esse valor estiver desabilitado, os usuários não serão desconectados devido à inatividade.

#### Note

Os usuários são considerados como ociosas quando param de fornecer entradas do mouse ou do teclado durante a sessão de streaming. Uploads e downloads de arquivos, entradas de áudio, saídas de áudio e alteração de pixels não são considerados atividade do usuário. Se os usuários permanecerem ociosos depois que o intervalo de tempo em Idle disconnect timeout in minutes (Limite de desconexão ociosa em minutos) terminar, eles serão desconectados.

## Configurar o provedor de identidades

Use as etapas a seguir para configurar seu provedor de identidade (IdP).

### Tópicos

- [Escolha o tipo de provedor de identidade](#)
- [Configurar o tipo de autenticação padrão](#)
- [Configurar o tipo de autenticação do IAM Identity Center](#)
- [Alterar o tipo de provedor de identidade](#)

### Escolha o tipo de provedor de identidade

WorkSpaces A Web oferece dois tipos de autenticação: Padrão AWS IAM Identity Center.

Você escolhe o tipo de autenticação para usar com seu portal na página Configurar provedor de identidade.

- Para Padrão (opção padrão), federe seu provedor de identidade SAML 2.0 de terceiros (como Okta ou Ping) diretamente com seu portal. Para ter mais informações, consulte [the section called “Configurar o tipo de autenticação padrão”](#). O tipo padrão é compatível com fluxos de autenticação iniciados pelo SP e iniciados pelo IdP.
- Para o IAM Identity Center (opção avançada), federe o IAM Identity Center com seu portal. Para usar esse tipo de autenticação, o IAM Identity Center e o portal WorkSpaces da Web devem residir no mesmo Região da AWS. Para ter mais informações, consulte [the section called “Configurar o tipo de autenticação do IAM Identity Center”](#).

## Configurar o tipo de autenticação padrão

Para Padrão (padrão), federe seu provedor de identidade SAML 2.0 de terceiros (como Okta ou Ping) diretamente com seu portal.


O tipo de identidade padrão pode suportar fluxos de login service-provider-initiated (iniciados pelo SP) e identity-provider-initiated (iniciados pelo IdP) com seu IdP compatível com SAML 2.0.

Etapa 1: Comece a configurar seu provedor de identidade na WorkSpaces Web

Conclua as etapas a seguir para configurar seu provedor de identidade:


1. Na página Configurar o provedor de identidade do assistente de criação, escolha Padrão.
2. Escolha Continuar com o IdP padrão.
3. Faça o download do arquivo de metadados do SP e mantenha a guia aberta para valores de metadados individuais.
  - Se o arquivo de metadados do SP estiver disponível, escolha Baixar arquivo de metadados para baixar o documento de metadados do provedor de serviços (SP) e faça o upload do arquivo de metadados do provedor de serviços para o seu IdP na próxima etapa. Sem isso, os usuários não conseguirão fazer login.
  - Se seu provedor não fizer upload dos arquivos de metadados do SP, insira manualmente os valores dos metadados.
4. Em Escolher tipo de login SAML, escolha entre asserções SAML iniciadas pelo SP e iniciadas pelo IdP, ou somente asserções SAML iniciadas pelo SP.
  - As asserções de SAML iniciadas pelo SP e iniciadas pelo IdP permitem que seu portal suporte os dois tipos de fluxos de entrada. Os portais que oferecem suporte a fluxos iniciados pelo IdP permitem que você apresente asserções de SAML ao endpoint da federação de identidade de serviço sem exigir que os usuários iniciem uma sessão visitando a URL do portal.

- Escolha essa opção para permitir que o portal aceite asserções SAML não solicitadas iniciadas pelo IDP.
- Essa opção exige que um estado de retransmissão padrão seja configurado em seu provedor de identidade SAML 2.0. O parâmetro de estado de retransmissão do seu portal está no console em login SAML iniciado por IdP, ou você pode copiá-lo do arquivo de metadados SP em. `<md:IdPInitRelayState>`
- Observação
  - A seguir está o formato do estado do relé: `redirect_uri=https%3A%2F%2Fportal-id.workspaces-web.com%2Fsso&response_type=code&client_id=1example23456789&identity_provider=Example-Identity-Provider.`
  - Se você copiar e colar o valor do arquivo de metadados do SP, certifique-se de alterar `&amp;` para `&`. `&` é um caractere de escape XML.
- Escolha somente asserções de SAML iniciadas pelo SP para que o portal ofereça suporte somente aos fluxos de login iniciados pelo SP. Essa opção rejeitará declarações SAML não solicitadas de fluxos de login iniciados pelo IDP.

 Note


Alguns terceiros IdPs permitem que você crie um aplicativo SAML personalizado que pode oferecer experiências de autenticação iniciadas pelo IdP aproveitando fluxos iniciados pelo SP. Consulte um exemplo em [Add an Okta bookmark application](#).

5. Escolha se você deseja ativar as solicitações do Sign SAML para esse provedor. A autenticação iniciada pelo SP permite que seu IdP valide se a solicitação de autenticação está vindo do portal, o que impede a aceitação de outras solicitações de terceiros.
  - a. Baixe o certificado de assinatura e faça o upload para o seu IdP. O mesmo certificado de assinatura pode ser usado para um único logout.
  - b. Ative a solicitação assinada em seu IdP. O nome pode ser diferente, dependendo do IdP.

 Note

O RSA-SHA256 é o único algoritmo de solicitação e assinatura de solicitação padrão suportado.

- Escolha se você deseja ativar Exigir asserções de SAML criptografadas. Isso permite que você criptografe a declaração SAML que vem do seu IdP. Isso pode impedir que os dados sejam interceptados em declarações SAML entre o IdP e a Web. WorkSpaces

 Note

O certificado de criptografia não está disponível nesta etapa. Ele será criado após o lançamento do seu portal. Depois de iniciar o portal, baixe o certificado de criptografia e faça o upload para o seu IdP. Em seguida, habilite a criptografia de asserção em seu IdP (o nome pode ser diferente, dependendo do IdP).

- Escolha se você deseja ativar o Logout Único. O logout único permite que seus usuários finais saiam do IdP WorkSpaces e da sessão da Web com uma única ação.
  - Baixe o certificado de assinatura da WorkSpaces Web e carregue-o em seu IdP. Esse é o mesmo certificado de assinatura usado para Assinatura de Solicitação na etapa anterior.
  - Usar o Logout Único exige que você configure uma URL de Logout Único no seu provedor de identidade SAML 2.0. Você pode encontrar a URL de Logout Único do seu portal no console em Detalhes do provedor de serviços (SP) - Mostrar valores de metadados individuais ou do arquivo de metadados SP em. `<md:SingleLogoutService>`
  - Ative o logout único em seu IdP. O nome pode ser diferente, dependendo do IdP.

Etapa 2: configure seu provedor de identidade em seu próprio IdP

Abra uma nova guia no navegador. Depois, conclua as seguintes etapas com seu IdP:

- Adicione os metadados do seu portal ao seu SAML IdP.

Faça upload do documento de metadados do SP que você baixou na etapa anterior para o seu IdP ou copie e cole os valores dos metadados nos campos corretos do seu IdP. Alguns provedores não permitem o upload de arquivos.

Os detalhes desse processo podem variar entre os fornecedores. Encontre a documentação do seu provedor [the section called “Orientação para fins específicos IdPs”](#) para obter ajuda sobre como adicionar os detalhes do portal à sua configuração de IdP.

- Confirme o nameID para sua declaração de SAML.

Certifique-se de que seu SAML IdP preencha nameID na declaração SAML com o campo de e-mail do usuário. NameID e e-mail do usuário são usados para identificar exclusivamente seu usuário federado SAML com o portal. Use o formato persistente de ID de nome SAML.

3. Opcional: configure o estado de retransmissão para a autenticação iniciada pelo IdP.


Se você escolheu Aceitar asserções SAML iniciadas pelo SP e iniciadas pelo IdP na etapa anterior, siga as etapas na etapa 2 de [the section called “Etapa 1: Comece a configurar seu provedor de identidade na WorkSpaces Web”](#) para definir o estado de retransmissão padrão para seu aplicativo de IdP.

4. Opcional: configure a assinatura da solicitação. Se você escolheu Assinar solicitações SAML para esse provedor na etapa anterior, siga as etapas na etapa 3 [the section called “Etapa 1: Comece a configurar seu provedor de identidade na WorkSpaces Web”](#) para carregar o certificado de assinatura no seu IdP e habilitar a assinatura da solicitação. Alguns IdPs, como o Okta, podem exigir que seu NameID pertença ao tipo “persistente” para usar a assinatura de solicitação. Certifique-se de confirmar seu NameID para sua declaração de SAML seguindo as etapas acima.
5. Opcional: configure a criptografia de asserção. Se você escolher Exigir asserções SAML criptografadas desse provedor, aguarde até que a criação do portal seja concluída e siga a etapa 4 em “Carregar metadados” abaixo para carregar o certificado de criptografia em seu IdP e habilitar a criptografia de asserção.
6. Opcional: configure o logout único. Se você escolheu Logout único, siga as etapas na etapa 5 [the section called “Etapa 1: Comece a configurar seu provedor de identidade na WorkSpaces Web”](#) para carregar o certificado de assinatura em seu IdP, preencher a URL de logout único e ativar o logout único.
7. Conceda acesso aos seus usuários em seu IdP para usar WorkSpaces a Web.
8. Baixe um arquivo de troca de metadados do seu IdP. Você fará o upload desses metadados para a WorkSpaces Web na próxima etapa.

### Etapa 3: Concluir a configuração do seu provedor de identidade na Web WorkSpaces

Retorne ao WorkSpaces console da Web. Na página Configurar provedor de identidade do assistente de criação, em Metadados do IdP, faça upload de um arquivo de metadados ou insira uma URL de metadados do seu IdP. O portal usa esses metadados do seu IdP para estabelecer confiança.

1. Para carregar um arquivo de metadados, em Documento de metadados do IdP, escolha Escolher arquivo. Carregue o arquivo de metadados no formato XML do IdP que você baixou na etapa anterior.
2. Para usar uma URL de metadados, acesse o IdP que você configurou na etapa anterior e obtenha a URL de metadados. Volte para o console WorkSpaces da Web e, em URL de metadados do IdP, insira o URL dos metadados que você obteve do seu IdP.
3. Quando concluir, escolha Next.
4. Para portais nos quais você habilitou a opção Exigir asserções SAML criptografadas deste provedor, você precisa baixar o certificado de criptografia da seção de detalhes do IdP do portal e carregá-lo no seu IdP. Em seguida, você pode ativar a opção lá.

 Note

WorkSpaces A Web exige que o assunto ou o nameID sejam mapeados e definidos na declaração SAML nas configurações do seu IdP. O IdP pode criar esses mapeamentos automaticamente. Se esses mapeamentos não estiverem configurados corretamente, os usuários não poderão fazer login no portal da web e iniciar uma sessão.

WorkSpaces A Web exige que as seguintes afirmações estejam presentes na resposta do SAML. Você pode encontrar <Your SP Entity ID>e <Your SP ACS URL>a partir do documento de metadados ou detalhes do provedor de serviços do seu portal, seja pelo console ou pela CLI.

- Uma AudienceRestriction declaração com um Audience valor que define seu ID de entidade SP como o destino da resposta. Exemplo:

```
<saml:AudienceRestriction>
  <saml:Audience><Your SP Entity ID></saml:Audience>
</saml:AudienceRestriction>
```

- Uma reivindicação Response com um valor de InResponseTo do ID da solicitação SAML original. Exemplo:

```
<samlp:Response ... InResponseTo="<originalSAMLrequestId">
```

- Uma SubjectConfirmationData declaração com o Recipient valor do URL do SP ACS e um InResponseTo valor que corresponda ao ID da solicitação SAML original. Exemplo:



```
<saml:SubjectConfirmation>
  <saml:SubjectConfirmationData ...
    Recipient="<Your SP ACS URL>"
    InResponseTo="<originalSAMLrequestId>"
  />
</saml:SubjectConfirmation>
```

WorkSpaces A Web valida seus parâmetros de solicitação e declarações de SAML. Para declarações SAML iniciadas pelo IdP, os detalhes da sua solicitação devem ser formatados como um RelayState parâmetro no corpo de uma solicitação HTTP POST. O corpo da solicitação também deve conter sua declaração de SAML como parâmetro. SAMLResponse Ambos devem estar presentes se você tiver seguido a etapa anterior. Veja a seguir um exemplo de POST corpo para um provedor de SAML iniciado pelo IdP.

```
SAMLResponse=<Base64-encoded SAML assertion>&RelayState=<RelayState>
```

## Orientação para fins específicos IdPs

Para garantir que você configure corretamente a federação SAML para seu portal, consulte os links abaixo para obter a documentação dos mais usados IdPs.

IdP	Configuração do aplicativo SAML	Gerenciamento de usuários	Autenticação iniciada pelo IDP	Solicitar assinatura	Criptografia de asserção	Sessão única
Okta	<a href="#">Crie integrações de aplicativos SAML</a>	<a href="#">Gerenciamento de usuários</a>	<a href="#">Referência de campo SAML do Application Integration Wizard</a>	<a href="#">Referência de campo SAML do Application Integration Wizard</a>	<a href="#">Referência de campo SAML do Application Integration Wizard</a>	<a href="#">Referência de campo SAML do Application Integration Wizard</a>
Entrar	<a href="#">Crie seu próprio aplicativo</a>	<a href="#">Início rápido: criar e atribuir</a>	<a href="#">Habilite o login único para um</a>	<a href="#">Verificação da assinatura</a>	<a href="#">Configurar a criptografia de token</a>	<a href="#">Protocolo SAML de saída única</a>

IdP	Configuração do aplicativo SAML	Gerenciamento de usuários	Autenticação iniciada pelo IDP	Solicitar assinatura	Criptografia de asserção	Sessão única
		<a href="#">uma conta de usuário</a>	<a href="#">aplicativo corporativo</a>	<a href="#">da solicitação SAML</a>	<a href="#">SAML do Microsoft Entra</a>	
Ping	<a href="#">Adicionar um aplicativo SAML</a>	<a href="#">Usuários</a>	<a href="#">Habilitando o SSO iniciado pelo IdP</a>	<a href="#">Configurando o login da solicitação de autenticação PingOne para Enterprise</a>	<a href="#">O PingOne for Enterprise e oferece suporte à criptografia?</a>	<a href="#">Logout único do SAML 2.0</a>
Um login	<a href="#">Conector personalizado SAML (avançado) (4266907)</a>	<a href="#">Adicionar usuários OneLogin manualmente</a>	<a href="#">Conector personalizado SAML (avançado) (4266907)</a>	<a href="#">Conector personalizado SAML (avançado) (4266907)</a>	<a href="#">Conector personalizado SAML (avançado) (4266907)</a>	<a href="#">Conector personalizado SAML (avançado) (4266907)</a>
IAM Identity Center	<a href="#">Configure seu próprio aplicativo SAML 2.0</a>	<a href="#">Configure seu próprio aplicativo SAML 2.0</a>	<a href="#">Configure seu próprio aplicativo SAML 2.0</a>	N/D	N/D	N/D

## Configurar o tipo de autenticação do IAM Identity Center

Para o tipo IAM Identity Center (avançado), você federa o IAM Identity Center com seu portal. Selecione essa opção somente se o seguinte se aplicar a você:

- Seu IAM Identity Center está configurado no mesmo portal da web Conta da AWS e Região da AWS no mesmo.

- Se você estiver usando AWS Organizations, você está usando uma conta de gerenciamento.

Antes de criar um portal da web com o tipo de autenticação do IAM Identity Center, você deve configurar o IAM Identity Center como um provedor independente. Para obter mais informações, consulte [Comece a usar tarefas comuns no IAM Identity Center](#). Ou você pode conectar seu IdP do SAML 2.0 ao IAM Identity Center. Para obter mais informações, consulte [Conectar-se a um provedor de identidade externo](#). Caso contrário, você não terá nenhum usuário ou grupo para atribuir ao portal da web.

Se você já usa o IAM Identity Center, pode escolher o IAM Identity Center como um tipo de provedor e seguir as etapas abaixo para adicionar, visualizar ou remover usuários ou grupos do seu portal da web.

#### Note

Para usar esse tipo de autenticação, seu IAM Identity Center precisa estar no mesmo Conta da AWS e no Região da AWS mesmo portal WorkSpaces da Web. Se o seu IAM Identity Center estiver em um local separado Conta da AWS ou Região da AWS, siga as instruções para o tipo de autenticação padrão. Para ter mais informações, consulte [the section called “Configurar o tipo de autenticação padrão”](#).

Se você estiver usando AWS Organizations, só poderá criar portais WorkSpaces da Web integrados ao IAM Identity Center usando uma conta de gerenciamento.

Para criar um portal da web com o Centro de Identidade do IAM

1. Durante a criação do portal na Etapa 4: Configurar provedor de identidade, escolha AWS IAM Identity Center.
2. Escolha Continuar com o IAM Identity Center.
3. Na página Atribuir usuários e grupos, escolha a guia Usuários e/ou grupos.
4. Marque a caixa ao lado do (s) usuário (s) ou grupo (s) que você deseja adicionar no portal.
5. Depois de criar seu portal, os usuários que você associou podem entrar na WorkSpaces Web com seu nome de usuário e senha do IAM Identity Center.

## Para gerenciar o portal da web com o Centro de Identidade do IAM

1. Depois de criar seu portal, ele é listado no console do IAM Identity Center como um aplicativo configurado.
2. Para acessar a configuração dessa aplicação, escolha Aplicações na barra lateral e procure uma aplicação configurada com um nome que corresponda ao nome de exibição do seu portal da web.

### Note

Se você não inseriu um nome de exibição, o GUID do portal será exibido em vez disso. O GUID é o ID prefixado ao URL do endpoint do seu portal da web.

## Para adicionar mais usuários e grupos a um portal da web existente

1. Abra o console WorkSpaces da Web em <https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/>.
2. Escolha WorkSpaces Web, Portais da Web, escolha seu portal da Web e, em seguida, escolha Editar.
3. Escolha Configurações do provedor de identidade e Atribuir usuários e grupos adicionais. Agora você pode adicionar usuários e grupos ao seu portal da web.

### Note

Não é possível adicionar usuários ou grupos pelo console do Centro de Identidade do IAM. Você deve fazer isso na página de edição do seu portal WorkSpaces da Web.

## Para visualizar ou remover usuários e grupos do seu portal da web

- Você pode visualizar ou remover o acesso do usuário a esse aplicativo usando as ações disponíveis na tabela Usuários atribuídos. Para obter mais informações, consulte [Gerenciar o acesso aos aplicativos](#).

**Note**

Você não pode visualizar ou remover usuários e grupos da página de edição do WorkSpaces portal da Web. Você deve fazer isso na página de edição do console do Centro de Identidade do IAM.

## Alterar o tipo de provedor de identidade

Siga estas etapas para alterar o tipo de autenticação do seu portal a qualquer momento:

- Para mudar do IAM Identity Center para o Standard, siga as etapas em [the section called “Configurar o tipo de autenticação padrão”](#).
- Para mudar do Standard para o IAM Identity Center, siga as etapas em [the section called “Configurar o tipo de autenticação do IAM Identity Center”](#).

As alterações no tipo de provedor de identidade podem levar até 15 minutos para serem implantadas e não encerrarão automaticamente as sessões em andamento.

Você pode visualizar as alterações do tipo de provedor de identidade em seu portal AWS CloudTrail inspecionando `UpdatePortal` eventos. O tipo é visível nas cargas de solicitação e resposta do evento.

## Analisar e executar

1. Na página Etapa 5: analisar e executar, revise as configurações que você selecionou para o seu portal da web. Você pode selecionar Editar para alterar as configurações de determinada seção. Também é possível alterar essas configurações posteriormente na guia Portais da Web do console.
2. Quando terminar, escolha Iniciar o portal da Web.
3. Para visualizar o status do seu portal da web, selecione Portais da Web, escolha seu portal e Visualizar detalhes.

Um portal da web tem um dos seguintes status:

- Incompleto: faltam configurações necessárias do provedor de identidades no portal da web.
- Pendente: o portal da web está aplicando alterações em suas configurações.

- Ativo: o portal da web está pronto e disponível para uso.
4. Aguarde até 15 minutos para que o portal se torne Ativo.

## Etapa 2: testar o portal da web

Depois de criar um portal da web, você pode entrar no endpoint WorkSpaces da Web para navegar pelos sites conectados como um usuário final faria.

Se você já concluiu essas etapas em [the section called “Configurar o provedor de identidades”](#), ignore esta seção e vá para [Etapa 3: distribuir o portal da web](#).

1. Abra o console WorkSpaces da Web em [https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#](https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/).
2. Escolha WorkSpaces Web, Portais da Web, escolha seu portal da Web e, em seguida, escolha Exibir detalhes
3. Em Endpoint do portal da Web, vá até o URL especificada para seu portal. O endpoint do portal da web é o ponto de acesso pelo qual os usuários iniciarão seu portal da web após fazerem login com o provedor de identidades configurado para o portal. Ele está disponível publicamente na internet e pode ser incorporado à sua rede.
4. Na página de login na WorkSpaces Web, escolha Entrar, SAML e insira suas credenciais do SAML.
5. Quando você vê a página Sua sessão está sendo preparada, sua sessão WorkSpaces na Web está sendo iniciada. Não feche nem saia dessa página.
6. O navegador da web é iniciado, exibindo o URL de inicialização e qualquer outro comportamento adicional definido por meio das configurações de política do navegador.
7. Agora, é possível navegar até sites conectados escolhendo links ou inserindo URLs na barra de endereço.

## Etapa 3: distribuir o portal da web

Quando você estiver pronto para que seus usuários comecem a usar a WorkSpaces Web, você escolhe entre as seguintes opções para distribuir o portal:

- Adicione o portal ao gateway da aplicação de SAML para que os usuários iniciem uma sessão diretamente de seu IdP. Por exemplo, consulte [Create a Bookmark App integration](#).

- Adicione o URL do portal a um site de sua propriedade e use um redirecionamento de navegador para direcionar os usuários ao portal da web.
- Envie por e-mail o URL do portal para seus usuários ou envie para um dispositivo que você gerencia como página inicial ou marcador do navegador.

## Próximas etapas

Depois de criar o primeiro portal da web, é possível visualizar detalhes, editar detalhes ou excluir o portal da web a qualquer momento. Para ter mais informações, consulte [Gerenciar seu portal da Web](#).

Você Conta da AWS pode criar um portal da web em cada um em Região da AWS que a WorkSpaces Web esteja disponível. Cada portal da web pode suportar até 25 conexões de usuários a qualquer momento. Para aumentar o número de portais que você pode criar em uma região ou para suportar mais sessões simultâneas para um portal, consulte [the section called “Solicitar um aumento de cota de serviço”](#).

# Gerenciar seu portal da Web

Depois de configurar seu portal da web, você pode visualizar ou editar seus detalhes, bem como excluir o portal se ele não for mais necessário.

## Tópicos

- [Visualizar detalhes do portal da web](#)
- [Editar um portal da web](#)
- [Excluir um portal da web](#)
- [Solicitar um aumento de cota de serviço](#)
- [Controle o intervalo para autenticar novamente um token do IdP SAML](#)
- [Configurar o registro de acesso do usuário](#)
- [Definir ou editar a política de navegador](#)
- [Configurar Editor de Método de Entrada \(IME\)](#)
- [Configurar a localização na sessão](#)
- [Configurar controles de acesso de IP \(opcional\)](#)
- [Habilitar extensão para autenticação única \(opcional\)](#)
- [Configurar a filtragem de URL](#)

## Visualizar detalhes do portal da web

Para visualizar detalhes do portal da web

1. Abra o console WorkSpaces da Web em [https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#](https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/).
2. Escolha WorkSpaces Web, Portais da Web, escolha seu portal da Web e, em seguida, escolha Exibir detalhes.

## Editar um portal da web

Para editar um portal da web



1. Abra o console WorkSpaces da Web em <https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/>.
2. Escolha WorkSpaces Web, Portais da Web, escolha seu portal da Web e, em seguida, escolha Editar.

#### Note

Alterações nas configurações de rede ou nas configurações de tempo limite encerram imediatamente qualquer sessão ativa do portal. Os usuários são desconectados e precisam se reconectar para iniciar uma nova sessão. As alterações nas Permissões da área de transferência, nas Permissões de transferência de arquivos ou em Imprimir no dispositivo local são aplicadas a partir da primeira nova sessão. As sessões que estão ativas não são desconectadas. Os usuários conectados às sessões ativas não são afetados pelas alterações até que se desconectem e se conectem a uma nova sessão.

## Excluir um portal da web

Para excluir um portal da web

1. Abra o console WorkSpaces da Web em <https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/>.
2. Escolha WorkSpaces Web, Portais da Web, escolha seu portal da Web e, em seguida, escolha Excluir.

## Solicitar um aumento de cota de serviço

Quando você cria sua AWS conta, definimos automaticamente cotas de serviço padrão (também chamadas de limites) para o uso de recursos com os AWS Serviços. WorkSpaces A Web define cotas em dois tipos de recursos: portais da web (por região) e sessões simultâneas máximas (por portal da web). WorkSpaces Atualmente, a Web tem os seguintes limites de cotas de serviço:

Cotas padrão em uma conta Região da AWS por	Valor
Portais da web	1

Cotas padrão em uma conta Região da AWS por	Valor
Máximo de sessões simultâneas	25

Um portal da web é o recurso fundamental dentro WorkSpaces da Web. É uma associação entre seu provedor de identidades SAML 2.0 e sua conexão de rede com a internet e seu conteúdo. Você pode criar um portal da web em qualquer Região da AWS lugar onde a WorkSpaces Web esteja disponível. Consulte a disponibilidade atual na tabela de regiões.


O máximo de sessões simultâneas é a maior quantidade de usuários que serão conectados ao mesmo tempo a determinado portal da web. Se o limite de cota de serviço para o máximo de sessões simultâneas não for definido adequadamente, os usuários poderão descobrir que a sessão não está disponível quando entrarem na Web. WorkSpaces Você também deve garantir que a VPC e as sub-redes tenham espaço de IP suficiente para suportar o máximo de sessões simultâneas, ou os usuários talvez não consigam se conectar a uma sessão.

Por exemplo, um cliente tem dois portais da web na região Leste dos EUA (Norte da Virgínia) e 125 usuários. O primeiro portal da web (portal A) tem 25 usuários e não exige um aumento da cota de serviço. O segundo portal da web (portal B) precisa estar disponível para até 100 usuários. Esses usuários estão distribuídos em dois turnos e suas horas de trabalho não se sobrepõem. Portanto, o cliente precisaria solicitar um aumento da cota de serviço do Portal B para um máximo de sessões simultâneas de 50 usuários.

É possível solicitar o aumento de qualquer um desses limites de cota de serviço. Consulte [Requesting a quota increase](#) (Como solicitar um aumento de cota) para obter mais informações.

Para solicitar um aumento de cota de serviço

1. Abra o [painel do AWS Support](#).
2. Escolha Aumento do limite de serviço.

 Important

WorkSpaces As cotas de serviços da Web afetam uma região por vez. Você deve solicitar aumentos de cota de serviço em cada região da AWS em que precisa de mais recursos. Para obter mais informações, consulte os [Endpoints de serviço da AWS](#).

3. Em Descrição do caso de uso, insira as seguintes informações:
  - Se você estiver solicitando um aumento no número de portais da web, especifique esse tipo de recurso e inclua o ID da sua conta da AWS, a região em que você gostaria de aumentar e o novo valor de limite.
  - Se você estiver solicitando um aumento para o máximo de sessões simultâneas, especifique esse tipo de recurso e inclua o ID da sua conta da AWS, a região em que você gostaria de aumentar, o ARN do portal da web e o novo valor de limite.
4. (Opcional) Para solicitar vários aumentos de cota de serviço ao mesmo tempo, conclua uma solicitação de aumento de cota na seção Solicitações e escolha Adicionar outra solicitação.

## Controle o intervalo para autenticar novamente um token do IdP SAML


Quando um usuário visita um portal WorkSpaces da Web, ele pode entrar para iniciar uma sessão de streaming. Todas as sessões começam na página inicial, a menos que eles tenham feito login há menos de cinco minutos. O portal verifica os tokens do provedor de identidades (IdP) para determinar se as credenciais do usuário devem ser solicitadas ao iniciar uma sessão. Um usuário sem um token de IdP válido deve inserir um nome de usuário, uma senha e, opcionalmente, a autenticação multifator (MFA) para iniciar uma sessão de streaming. Se um usuário já tiver gerado um token do IdP SAML fazendo login em seu IdP ou em uma aplicação protegida pelo mesmo IdP, as credenciais de login não serão solicitadas a ele.

Se um usuário tiver um token SAML IdP válido, ele poderá WorkSpaces acessar a Web. É possível controlar o intervalo necessário para autenticar novamente um token do IdP SAML.

Para controlar o intervalo para autenticar novamente um token do IdP SAML

1. Defina a duração do tempo limite do IdP com seu provedor de IdP SAML. Recomendamos configurar a duração do tempo limite do IdP com o menor tempo necessário para que o usuário conclua suas tarefas.
  - Para obter mais informações sobre o Okta, consulte [Impor uma vida útil de sessão limitada para todas as políticas](#).
  - Para obter mais informações sobre o Azure AD, consulte [Configurar controles da sessão de autenticação](#).
  - Para obter mais informações sobre Ping, consulte [Sessões](#).

- Para obter mais informações sobre AWS IAM Identity Center, consulte [Definir a duração da sessão](#).
2. Defina os valores de inatividade e tempo limite de inatividade do seu portal da WorkSpaces Web. Esses valores controlam a quantidade de tempo entre a última interação do usuário e o término de uma sessão WorkSpaces na Web devido à inatividade. Quando uma sessão termina, o usuário perde o estado da sessão (incluindo guias abertas, conteúdo da web não salvo e histórico) e retorna a um novo estado no início da próxima sessão. Para obter mais informações, consulte a etapa 5 em [the section called “Etapa 1: criar um portal da web”](#).


 Note

Se a sessão de um usuário expirar, mas o usuário ainda tiver um token SAML IdP válido, ele não precisará inserir seu nome de usuário e senha para iniciar uma WorkSpaces nova sessão na Web. Para controlar como os tokens são autenticados novamente, siga os guias na etapa anterior.

## Configurar o registro de acesso do usuário

É possível configurar o log de acesso do usuário para registrar os seguintes eventos do usuário:

- Início da sessão - Marca o início de uma sessão WorkSpaces na Web.
- Fim da sessão - marca o fim de uma sessão WorkSpaces na Web.
- Navegação por URL: registra o URL que um usuário carrega.

 Note

Os logs de navegação por URL são registrados no histórico do navegador. URLs não registrados no histórico do navegador (acessados no modo de navegação anônima ou excluídos do histórico do navegador) não são registrados nos logs. Cabe aos clientes determinar se devem desativar o modo de navegação anônima ou a exclusão do histórico com a política do navegador.

Além disso, as seguintes informações estão incluídas para cada evento:

- Hora do evento

- Nome de usuário
- ARN do portal da web

Os clientes são responsáveis por compreender os possíveis problemas legais que surgem com o uso da WorkSpaces Web e garantir que o uso da WorkSpaces Web esteja em conformidade com todas as leis e regulamentos aplicáveis. Isso inclui leis que regulam a capacidade do empregador de monitorar o uso da WorkSpaces Web por um funcionário, incluindo atividades realizadas dentro do aplicativo.

A ativação dos registros de acesso do usuário em seu portal WorkSpaces da Web pode resultar em cobranças do Amazon Kinesis Data Streams. Para obter detalhes de preço, consulte [Preços do Amazon Kinesis Data Streams](#).

Para ativar o registro de acesso do usuário no console WorkSpaces Web, em Registro de acesso do usuário, selecione o Kinesis Stream ID que você deseja usar para receber dados. Os dados gravados serão entregues diretamente para esse fluxo.

Para obter mais informações sobre como criar um Amazon Kinesis Data Stream, consulte [What Is Amazon Kinesis Data Streams?](#).

#### Note

Para receber registros da WorkSpaces Web, você deve ter um Amazon Kinesis Data Stream que comece com "amazon-workspaces-web-\*". Seu stream de dados do Amazon Kinesis deve ter a criptografia do lado do servidor desativada ou deve ser usada para criptografia do lado do servidor. Chaves gerenciadas pela AWS

Para obter mais informações sobre a configuração da criptografia do lado do servidor no Amazon Kinesis, consulte [How Do I Get Started with Server-Side Encryption?](#).

## Logs de amostra

Abaixo está um exemplo de cada evento disponível, incluindo Validação StartSessionVisitPage,, EndSessione.

Os campos a seguir estão sempre incluídos em cada evento:

- timestamp é incluído como tempo epoch em milissegundos.

- `eventType` é incluído como uma string.
- `details` é incluído como outro objeto json.
- `portalArn` e `userName` são incluídos em todos os eventos, exceto em `Validation`.

```
{
  "timestamp": "1665430373875",
  "eventType": "Validation",
  "details": {
    "permission": "Kinesis:PutRecord",
    "userArn": "userArn",
    "operation": "AssociateUserAccessLoggingSettings",
    "userAccessLoggingSettingsArn": "userAccessLoggingSettingsArn"
  }
}

{
  "timestamp": "1665179071723",
  "eventType": "StartSession",
  "details": {},
  "portalArn": "portalArn",
  "userName": "userName"
}

{
  "timestamp": "1665179084578",
  "eventType": "VisitPage",
  "details": {
    "title": "Amazon",
    "url": "https://www.amazon.com/"
  },
  "portalArn": "portalArn",
  "userName": "userName"
}

{
  "timestamp": "1665179155953",
  "eventType": "EndSession",
  "details": {},
  "portalArn": "portalArn",
  "userName": "userName"
}
```

## Definir ou editar a política de navegador

Com a WorkSpaces Web, você pode definir uma política de navegador personalizada usando as políticas do Chrome disponíveis para a versão estável mais recente. Há mais de 300 políticas que você pode aplicar a um portal da web. Para obter mais informações, consulte [the section called “Definir uma política de navegador personalizada \(exemplo\)”](#) e [Lista de políticas do Chrome Enterprise](#).

Ao usar a visualização do console para criar um portal da web, você pode aplicar as seguintes políticas:

- StartURL
- Favoritos e pastas de favoritos
- Ativar e desativar a navegação privada
- Exclusão do histórico
- Filtro de URL com AllowURL e BlockURL

Para obter mais informações sobre como usar políticas de visualização do console, consulte [Começando com a Amazon WorkSpaces Web](#).

WorkSpaces A Web aplica uma configuração básica da política do navegador a todos os portais junto com todas as políticas que você especificar. Você pode editar algumas dessas políticas com seu arquivo JSON personalizado. Para ter mais informações, consulte [the section called “Editar a política base do navegador”](#).

### Tópicos

- [Definir uma política de navegador personalizada \(exemplo\)](#)
- [Editar a política base do navegador](#)

## Definir uma política de navegador personalizada (exemplo)

É possível definir qualquer política compatível do Chrome para Linux carregando um arquivo JSON. Para saber mais sobre as políticas do Chrome, consulte a [Lista de políticas do Chrome Enterprise](#) e selecione a plataforma Linux. Depois, pesquise e revise as políticas da versão estável mais recente.

No exemplo a seguir, você cria um portal da web com os seguintes controles de política:

- Configurar favoritos
- Configurar páginas de inicialização padrão
- Impedir que o usuário instale outras extensões
- Impedir que o usuário exclua o histórico
- Impedir que o usuário acesse o modo de navegação anônima
- Pré-instale a extensão do [plug-in Okta](#) para todas as sessões.

## Tópicos

- [Etapa 1: criar um portal da web](#)
- [Etapa 2: reunir políticas](#)
- [Etapa 3: criar um arquivo de política JSON personalizado](#)
- [Etapa 4: adicionar políticas ao modelo](#)
- [Etapa 5: carregue o arquivo JSON de política em seu portal da web](#)

## Etapa 1: criar um portal da web

Para fazer o upload do arquivo JSON da política do Chrome, você deve criar um portal WorkSpaces da Web. Para ter mais informações, consulte [the section called “Etapa 1: criar um portal da web”](#).

## Etapa 2: reunir políticas

Pesquise e localize as políticas que você deseja na Política do Chrome. Depois, use as políticas para criar um arquivo JSON na próxima etapa.

1. Acesse a [Lista de políticas do Chrome Enterprise](#).
2. Escolha a plataforma Linux e selecione a versão mais recente do Chrome.
3. Pesquise as políticas que você deseja definir. Neste exemplo, pesquise extensões para encontrar políticas para gerenciá-las. Cada política inclui uma descrição, nome de preferência do Linux e valor de amostra.
4. Nos resultados da pesquisa, há três políticas que atendem aos requisitos empresariais se usadas em conjunto:
  - ExtensionSettings: instala uma extensão na inicialização do navegador.
  - ExtensionInstallBlocklist: impede que extensões específicas sejam instaladas.
  - ExtensionInstallAllowlist— Permite que determinadas extensões sejam instaladas.



## 5. Políticas adicionais atendem aos requisitos restantes:

- **ManagedBookmarks**— Adiciona marcadores às páginas da web.
- **RestoreOnStartupURLs** — Configura quais páginas da Web são abertas sempre que uma nova janela do navegador é aberta.
- **AllowDeletingBrowserHistory**— Configura se os usuários podem excluir seu histórico de navegação.
- **IncognitoModeAvailability**— Configura se os usuários podem acessar o modo de navegação anônima.

## Etapa 3: criar um arquivo de política JSON personalizado

Crie um arquivo JSON usando um editor de texto, um modelo e as políticas encontradas na etapa anterior.

1. Abra um editor de texto.
2. Copie e cole o seguinte modelo em seu editor de texto:

```
{
  "chromePolicies":
  {
    "ManagedBookmarks":
    {
      "value":
      [
        {
          "name": "Bookmark 1",
          "url": "bookmark-url-1"
        },
        {
          "name": "Bookmark 2",
          "url": "bookmark-url-2"
        }
      ]
    },
    "RestoreOnStartup":
    {
      "value": 4
    },
    "RestoreOnStartupURLs":
```

```
{
  "value":
  [
    "startup-url"
  ]
},
"ExtensionInstallBlocklist": {
  "value": [
    "insert-extensions-value-to-block",
  ]
},
"ExtensionInstallAllowlist": {
  "value": [
    "insert-extensions-value-to-allow",
  ]
},
"ExtensionSettings":
{
  "value":
  {
    "insert-extension-value-to-force-install":
    {
      "installation_mode": "force_installed",
      "update_url": "https://clients2.google.com/service/update2/crx",
      "toolbar_pin": "force_pinned"
    },
  }
},
"AllowDeletingBrowserHistory":
{
  "value": should-allow-history-deletion
},
"IncognitoModeAvailability":
{
  "value": incognito-mode-availability
}
}
}
```

## Etapa 4: adicionar políticas ao modelo

Adicione suas políticas personalizadas ao modelo para cada requisito empresarial.

### 1. Configure URLs de favoritos.

- a. Abaixo da chave `value`, adicione pares de chaves `name` e `url` para cada marcador que você deseja adicionar.
- b. Defina `bookmark-url-1` como `https://www.amazon.com`.
- c. Defina `bookmark-url-2` como `https://docs.aws.amazon.com/workspaces-web/latest/adminguide/`.

```
"ManagedBookmarks":
  {
    "value":
      [
        {
          "name": "Amazon",
          "url": "https://www.amazon.com"
        },
        {
          "name": "Bookmark 2",
          "url": "https://docs.aws.amazon.com/workspaces-web/latest/
adminguide/"
        }
      ]
  },
```

### 2. Configure os URLs de inicialização. Essa política permite que os administradores definam os sites exibidos quando um usuário abre uma nova janela do navegador.

- a. Defina `RestoreOnStartup` como `4`. Isso define a ação `RestoreOnStartup` para abrir uma lista de URLs. Você também pode usar outras ações nos URLs de inicialização. Para obter mais informações, consulte [Lista de políticas do Chrome Enterprise](#).
- b. Defina `RestoreOnStartupURLs` como `https://www.aboutamazon.com/news`.

```
"RestoreOnStartup":
  {
    "value": 4
```

```
    },
    "RestoreOnStartupURLs":
    {
        "value":
        [
            "https://www.aboutamazon.com/news"
        ]
    },
    },
```

3. Para evitar que o usuário exclua o histórico do navegador, defina `AllowDeletingBrowserHistory` como `false`.

```
"AllowDeletingBrowserHistory":
{
    "value": false
},
```

4. Para desativar o acesso ao modo de navegação anônima para os usuários, defina `IncognitoModeAvailability` como `1`.

```
"IncognitoModeAvailability":
{
    "value": 1
}
```

5. Defina e aplique o [plug-in Okta](#) com as seguintes políticas:

- `ExtensionSettings`: instala uma extensão na inicialização do navegador. O valor da extensão está disponível na página de ajuda do plug-in Okta.
- `ExtensionInstallBlocklist`: impede que extensões específicas sejam instaladas. Use um valor `*` para evitar todas as extensões por padrão. Os administradores podem controlar quais extensões permitir em `ExtensionInstallAllowlist`.
- `ExtensionInstallAllowlist` permite que você instale determinadas extensões. Já que `ExtensionInstallBlocklist` está definido como `*`, adicione o valor do plug-in Okta aqui para permiti-lo.

Veja a seguir um exemplo de política para ativar o plug-in Okta:

```
"ExtensionInstallBlocklist": {
  "value": [
    "*"
  ],
},
"ExtensionInstallAllowlist": {
  "value": [
    "glnpjglilkicbckjpbgcfkogebgllemb",
  ]
},
"ExtensionSettings": {
  "value": {
    "glnpjglilkicbckjpbgcfkogebgllemb": {
      "installation_mode": "force_installed",
      "update_url": "https://clients2.google.com/service/update2/crx",
      "toolbar_pin": "force_pinned"
    }
  }
}
```

## Etapa 5: carregue o arquivo JSON de política em seu portal da web

1. Abra o console WorkSpaces da Web em [https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.](https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/)
2. Escolha WorkSpaces Web e, em seguida, escolha Portais da Web.
3. Selecione seu portal da web e escolha Editar.
4. Escolha Configurações da política e Carregamento do arquivo JSON.
5. Selecione Escolher arquivo. Navegue até o arquivo JSON, selecione-o e carregue-o.
6. Escolha Salvar.

## Editar a política base do navegador

Para fornecer o serviço, a WorkSpaces Web aplica uma política básica de navegador a todos os portais. Essa política base é aplicada além das que você especifica na visualização do console ou no carregamento do JSON. Veja a seguir a lista de políticas aplicadas pelo serviço no formato JSON:

```
{
  "chromePolicies":
  {
    "DefaultDownloadDirectory": {
      "value": "/home/as2-streaming-user/MyFiles/TemporaryFiles"
    },
    "DownloadDirectory": {
      "value": "/home/as2-streaming-user/MyFiles/TemporaryFiles"
    },
    "DownloadRestrictions": {
      "value": 1
    },
    "URLBlocklist": {
      "value": [
        "file://",
        "http://169.254.169.254",
        "http://[fd00:ec2::254]",
      ]
    },
    "URLAllowlist": {
      "value": [
        "file:///home/as2-streaming-user/MyFiles/TemporaryFiles",
        "file:///opt/appstream/tmp/TemporaryFiles",
      ]
    }
  }
}
```

Os clientes não podem fazer alterações nas seguintes políticas:

- `DefaultDownloadDirectory`: essa política não pode ser editada. O serviço substitui todas as alterações nessa política.
- `DownloadDirectory`: essa política não pode ser editada. O serviço substitui todas as alterações nessa política.

Os clientes podem atualizar as seguintes políticas em seu portal da web:

- `DownloadRestrictions`: o padrão é definido como 1 para evitar downloads identificados como mal-intencionados pela Navegação segura do Chrome. Para obter mais informações, consulte [Bloquear o download de arquivos nocivos pelos usuários](#). É possível definir o valor de 0 para 4.

- As políticas `URLAllowlist` e `URLBlocklist` podem ser estendidas usando o recurso de filtragem de URL da visualização do console ou o carregamento de JSON. No entanto, os URLs de base não podem ser substituídos. Essas políticas não são visíveis de um arquivo JSON baixado do seu portal da web. No entanto, se você acessar “chrome://policy” durante uma sessão, o navegador remoto exibirá as políticas aplicadas.

## Configurar Editor de Método de Entrada (IME)

Um editor de método de entrada (IME) é um utilitário que fornece opções ao usuário final para inserir texto em idiomas que usam um layout de teclado diferente do teclado QWERTY. Os IMEs ajudam os usuários a inserir texto em idiomas com conjuntos de idiomas maiores e mais complexos, como japonês, chinês e coreano. WorkSpaces As sessões da Web incluem suporte a IME por padrão. Os usuários podem selecionar idiomas alternativos na barra de ferramentas do IME na sessão ou usando atalhos de teclado.

Atualmente, os seguintes idiomas são suportados pelo IME da WorkSpaces Web:

- Inglês
- Chinês simplificado (pinyin)
- Chinês tradicional (bopomofo)
- Japonês
- Coreano

Para selecionar um idioma na barra de ferramentas do IME, faça o seguinte:

1. Selecione o menu suspenso do seletor de idiomas localizado no lado direito da barra preta do painel superior. Por padrão, o seletor mostrará en, para inglês.
2. No menu suspenso, escolha o idioma desejado.
3. No submenu exibido após a escolha de um idioma, selecione detalhes adicionais do idioma.

Para selecionar um idioma usando atalhos de teclado, faça o seguinte:

- Todos os IMEs
  - Para avançar o IME (ou mover para o layout direito do teclado), pressione Shift+Control+Left Alt.
- Japonês

- Para escolher hiragana, pressione F6.
- Para escolher katakana, pressione F7.
- Para escolher latim, pressione F10.
- Para escolher latim estendido, pressione F9.
- Para escolher Entrada direta, pressione ALT +, ALT+@, Zenkaku Hankaku.
- Coreano
  - Para escolher hangul, pressione Shift+Space.
  - Para escolher hanja, pressione F9.

Para remover a barra de ferramentas e o menu do IME, ou para desativar o teclado virtual de suas sessões da WorkSpaces Web, entre em contato com. AWS Support

## Configurar a localização na sessão

Quando um usuário inicia uma sessão, a WorkSpaces Web detecta as configurações de idioma e fuso horário do navegador local do usuário e as aplica à sessão. Isso afeta o idioma de exibição durante a sessão e ajuda a garantir que a hora exibida corresponda à hora atual na localização do usuário.

A lista a seguir mostra os códigos de idioma atualmente suportados pela WorkSpaces Web. Se o navegador local do usuário estiver configurado para usar um código de idioma que não é compatível, o padrão da sessão será inglês (en-US).

- Alemão
  - de: alemão
  - de-AT: alemão (Áustria)
  - de-DE: alemão (Alemanha)
  - de-CH: alemão (Suíça)
  - De-LI: alemão (Liechtenstein)
- Inglês
  - en: inglês
  - en-AU: inglês (Austrália)
  - en-CA: inglês (Canadá)



- en-IN: inglês (Índia)
- en-NZ: inglês (Nova Zelândia)
- en-ZA: inglês (África Meridional)
- en-GB – Inglês (Reino Unido)
- en-US – Inglês (Estados Unidos)
- Espanhol
  - es: espanhol
  - es-AR: espanhol (Argentina)
  - es-CL: espanhol (Chile)
  - es-CO: espanhol (Colômbia)
  - es-CR: espanhol (Costa Rica)
  - es-HN: espanhol (Honduras)
  - es-419: espanhol (América Latina)
  - es-MX: espanhol (México)
  - es-PE: espanhol (Peru)
  - es-ES: espanhol (Espanha)
  - es-US: espanhol (Estados Unidos)
  - es-UY: espanhol (Uruguai)
  - es-VE: espanhol (Venezuela)
- Francês
  - fr: francês
  - fr-CA: francês (Canadá)
  - fr-FR: francês (França)
  - fr-CH: francês (Suíça)
- Indonésio
  - id: indonésio
  - id-ID: indonésio (Indonésia)
- Italiano
  - it: italiano
  - it-IT: italiano (Itália)

- it-CH: italiano (Suíça)
- Japonês
  - ja: japonês
  - Ja-JP: japonês (Japão)
- Coreano
  - ko: coreano
  - ko-KR: coreano (Coreia)
- Português
  - pt: português
  - pt-BR: português (Brasil)
  - pt-PT: português (Portugal)
- Chinês
  - zh: chinês
  - zh-CN: chinês (China)
  - zh-HK: chinês (Hong Kong)
  - zh-TW: chinês (Taiwan)

O idioma da sessão é determinado na seguinte ordem de prioridade:

1. A `ForcedLanguages` política nas configurações do navegador do portal da web. Para obter mais informações, consulte [ForcedLanguages](#).
2. A configuração do idioma do navegador local do usuário final.
3. O valor padrão, inglês (en-US).

O fuso horário é determinado pelas configurações de fuso horário local especificadas no navegador do usuário final. Se a configuração do fuso horário não for válida, o UTC será usado.

Os seguintes componentes na WorkSpaces Web oferecem suporte à localização:

- WorkSpaces Página de login na web
- WorkSpaces Mensagens de status do portal da Web (incluindo mensagens de carregamento e erros)
- Navegador Chrome

- Menu de Contexto do sistema e janela Salvar como

Para definir as configurações do navegador local do usuário, siga um destes procedimentos:

- No Chrome, escolha Configurações, Idiomas e, ordene os idiomas com base na preferência.
- No Firefox, escolha Configurações, Geral, Idioma e selecione o idioma no menu suspenso.
- No Edge, escolha Configurações, escolha Idiomas e ordene os idiomas com base na preferência.

## Configurar controles de acesso de IP (opcional)

WorkSpaces A Web permite que você controle de quais endereços IP seu portal da web pode ser acessado. Ao usar as configurações de acesso de IP, é possível definir e gerenciar grupos de endereços IP confiáveis e só permitir que os usuários acessem seu portal quando estiverem conectados a uma rede confiável.

Por padrão, a WorkSpaces Web permite que os usuários acessem seu portal da web de qualquer lugar. Um grupo de controle de acesso de IP atua como um firewall virtual que filtra o endereço IP que um usuário pode usar para se conectar ao portal da web. Quando associadas ao seu portal da web, as configurações de acesso de IP detectarão o IP do usuário antes da autenticação para determinar se ele está qualificado a se conectar. Uma vez conectado, o WorkSpaces Web monitora continuamente o endereço IP do usuário para garantir que ele permaneça conectado a partir de uma rede confiável. Se o IP de um usuário mudar, a WorkSpaces Web detectará e encerrará a sessão.

Para especificar os intervalos de endereços CIDR, adicione regras ao seu grupo de controle de acesso de IP e, depois, associe o grupo ao seu portal da web. É possível associar cada configuração de acesso de IP a um ou mais portais da web. Para especificar os endereços IP públicos e intervalos de endereços IP para suas redes confiáveis, adicione regras para seus grupos de controle de acesso IP. Se os usuários acessam o portal da web por meio de um gateway NAT ou uma VPN, você deverá criar regras que permitam o tráfego de endereços IP públicos para o gateway NAT ou a VPN.

### Note

Os clientes são responsáveis por compreender os possíveis problemas legais que surgem com o uso da WorkSpaces Web e devem garantir que o uso da WorkSpaces Web esteja em conformidade com todas as leis e regulamentos aplicáveis. Isso inclui leis que regulam

a capacidade do empregador de monitorar o uso da WorkSpaces Web por um funcionário, incluindo atividades realizadas dentro do aplicativo.

## Criar um grupo de controle de acesso de IP

Para criar um grupo de controle de acesso de IP, siga estas etapas.

1. Abra o console WorkSpaces da Web em [https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#](https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/).
2. No painel de navegação, selecione Controles de acesso a IP.
3. Selecione Criar grupo de controle de acesso IP.
4. Na caixa de diálogo Criar grupo de controle de acesso IP, insira um nome (obrigatório) e uma descrição (opcional) para o grupo.
5. Insira o endereço IP ou o intervalo de IP CIDR que será associado à Origem e uma Descrição (opcional).
6. Em Tags, escolha se deseja marcar um par de chave-valor para cada grupo de controle de acesso de IP.
7. Quando terminar de adicionar regras e tags, escolha Salvar.

## Associar uma configuração de acesso de IP a um portal da web

Para associar um grupo de controle de acesso de IP a um portal da web existente, siga estas etapas.

1. Abra o console WorkSpaces da Web em [https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#](https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/).
2. No painel de navegação, selecione Portais da Web.
3. Selecione o portal da web e escolha Editar.
4. Em Grupo de controle de acesso de IP, selecione os grupos de controle de acesso de IP para o portal da web.
5. Escolha Salvar.

Para associar um grupo de controle de acesso de IP ao criar um portal da web, siga estas etapas.

1. Conclua as etapas de 1 a 4 em [the section called “Definir configurações do portal”](#) para acessar Controle de acesso de IP (opcional).
2. Escolha Criar controles de acesso de IP.
3. Na caixa de diálogo Criar grupo de IP, insira um nome (obrigatório) e uma descrição (opcional) para o grupo.
4. Insira o endereço IP ou o intervalo de IP CIDR que será associado à Origem e uma Descrição (opcional).
5. Em Tags, escolha se deseja marcar um par de chave-valor para cada grupo de controle de acesso de IP.
6. Quando terminar de adicionar regras e tags, escolha Criar controle de acesso de IP.
7. O grupo de controle de acesso IP será associado a esse portal da web quando iniciado.

## Edite um grupo de controle de acesso de IP

Você pode excluir uma regra de uma configuração de acesso de IP a qualquer momento. Se você remover uma regra que foi usada para permitir uma conexão com um portal da web, todos os usuários com uma sessão atual serão desconectados do portal da web.

Para editar um grupo de controle de acesso de IP, siga estas etapas.

1. Abra o console WorkSpaces da Web em [https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#](https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/).
2. No painel de navegação, selecione Controles de acesso a IP.
3. Selecione o grupo e escolha Edit (Editar).
4. Edite a Origem e a Descrição (opcional) das regras existentes ou adicione outras regras.
5. Em Tags, escolha se deseja marcar um par de chave-valor para cada grupo de controle de acesso de IP.
6. Quando terminar de adicionar regras e tags, escolha Salvar.
7. Se você atualizou uma configuração de acesso de IP existente, aguarde até 15 minutos para que a regra nova ou editada entre em vigor.

## Excluir um grupo de controle de acesso de IP

Você pode excluir uma regra de um grupo de controle de acesso IP a qualquer momento. Se você remover uma regra que foi usada para permitir uma conexão com um portal da web, todos os usuários com uma sessão atual serão desconectados do portal da web.

Para excluir um grupo de controle de acesso de IP, siga estas etapas.

1. Abra o console WorkSpaces da Web em [https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#](https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/).
2. No painel de navegação, selecione Grupo de controle de acesso de IP.
3. Selecione o grupo e escolha Excluir.

## Habilitar extensão para autenticação única (opcional)

É possível habilitar uma extensão para que os usuários finais tenham uma melhor experiência de login no portal. Por exemplo, se você usar o Okta como provedor de identidades (IdP) SAML 2.0 do seu portal e também usá-lo como o IdP dos sites que você deseja que os usuários acessem durante uma sessão, será possível passar o cookie de login do Okta para a sessão com a extensão. Posteriormente, quando os usuários acessarem um site que requer o cookie de domínio Okta, eles não precisarão fazer login durante a sessão.

A extensão é compatível com os navegadores Chrome e Firefox. A extensão permite a sincronização de cookies para os domínios permitidos pelo login dos usuários na sessão. A extensão não exige que o usuário faça login e funciona nos bastidores para permitir a sincronização de cookies sem exigir que o usuário execute nenhuma ação após a instalação. Nenhum dado é armazenado pela extensão.

Os usuários podem adicionar a extensão ao navegador Chrome na loja virtual do Chrome ou ao Firefox navegador a partir de complementos para Firefox.

As extensões não estão habilitadas no Chrome no InCognito Windows. O Firefox tem uma configuração para permitir extensões durante a navegação privada. Para obter mais informações, consulte [Extensões na navegação privada](#).

É possível atualizar a configuração de usuário existente de um portal ou ao criar um portal da web pela primeira vez. Primeiro, determine quais domínios você precisa para o IdP SAML e sites. É possível adicionar até 10 domínios.

Você é responsável por testar e identificar o domínio apropriado para que os cookies sejam sincronizados. Pode ser necessário fazer alterações no nível de autenticação do IdP ou do site para garantir que a autenticação única funcione conforme o esperado.

Para ver quais domínios usar com o IdP mais comum, consulte a tabela a seguir:

#### IdP e domínios

IdP	Domínio
Okta	okta.com
Anúncio do Azure	microsoftonline.com
Centro de Identidade da AWS	awsapps.com
Um login	onelogin.com
Duo	duosecurity.com

Depois, acesse seu portal da web no console. Então, permita a extensão e adicione os cookies dos domínios que devem ser sincronizados. Siga as etapas abaixo para criar um portal com a extensão permitida ou para atualizar um portal existente.

Para permitir a extensão ao criar um portal da web, siga estas etapas:

1. Siga as etapas em [the section called “Etapa 1: criar um portal da web”](#) até chegar a [the section called “Definir as configurações do usuário”](#).
2. Para a etapa 1 de [the section called “Definir as configurações do usuário”](#), em Permissões do usuário, escolha Permitido para habilitar a extensão para seu portal da web.
3. Insira o domínio para sincronização de cookies e escolha Adicionar novo domínio.
4. Conclua as etapas em [the section called “Definir as configurações do usuário”](#) e as seções restantes em [the section called “Etapa 1: criar um portal da web”](#) para criar seu portal da web.

Para adicionar a extensão a um portal da web existente, siga estas etapas:

1. Abra o console WorkSpaces da Web em <https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/>.
2. Selecione o portal da web a ser editado.

3. Escolha Configurações do usuário, Permissões do usuário e Permitido para habilitar a extensão para seu portal da web.
4. Insira o domínio para sincronização de cookies e escolha Adicionar novo domínio.
5. Salve as alterações do portal. Os portais solicitarão que os usuários instalem a extensão em até 15 minutos.

Para editar domínios ou remover a extensão, siga estas etapas:

1. Abra o console WorkSpaces da Web em [https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#](https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/).
2. Selecione o portal da web a ser editado.
3. Escolha Configurações do usuário, Permissões do usuário e Não permitido para remover a extensão do seu portal da web.
4. Remova ou edite domínios individuais.
5. Depois de removidas, as sessões não sincronizarão mais os cookies, mesmo que o usuário tenha a extensão WorkSpaces da Web instalada em seu navegador.

Para obter detalhes sobre a experiência do usuário com a extensão, consulte [the section called “Extensão de autenticação única”](#).

## Configurar a filtragem de URL

Você pode usar a Política do Chrome para filtrar quais URLs os usuários podem acessar a partir do navegador remoto. A Política do Chrome fornece dois mecanismos para filtrar URLs: URLAllowlist e URLBlocklist. Você pode usar a interface do console WorkSpaces Web para configurar a filtragem de URL como uma configuração do portal ou adicioná-la como parte de sua instrução JSON personalizada (no editor embutido ou como um upload de arquivo JSON).

Para configurar a filtragem de URL usando o console

1. Abra o console WorkSpaces da Web em [https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#](https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/).
2. Escolha WorkSpaces Web, Portais da Web, escolha seu portal da Web e, em seguida, escolha Exibir detalhes.
3. Para filtragem de URL, escolha entre as seguintes opções:



- Permitir acesso a todos os URLs: por padrão, um portal da web permite acesso a todos os URLs. Você pode adicionar sites específicos à lista BlockURL para impedir que os usuários visitem esses sites durante uma sessão. Por exemplo, adicionar `www.anycorp.com` à lista BlockURL impedirá que o usuário navegue até `www.anycorp.com` durante a sessão.
- Bloquear o acesso a todos os URLs: por padrão, o portal da web bloqueia o acesso a todos os URLs. Você pode adicionar sites específicos à lista de URLs permitidos para organizar uma lista de sites que os usuários podem visitar e bloquear o tráfego para outros sites. Considere adicionar cada URL como um marcador para permitir o acesso com um clique para os usuários durante a sessão.
- Configuração avançada: escolha essa opção para criar listas allowURL e blockURL em paralelo. A lista de permissões de URL tem prioridade sobre a lista de bloqueio de URL. Essa opção ativa a filtragem de URL por caminho. Por exemplo, você pode adicionar `www.anycorp.com` à lista de bloqueio e, em seguida, adicionar `www.anycorp.com/hr` à lista de permissões. Isso permite que os usuários acessem `www.anycorp.com/hr`, mas não conseguirão acessar outros caminhos de URL, como `www.anycorp.com/finance`.

Para obter mais orientações sobre como bloquear e permitir URLs, consulte [Permitir ou bloquear o acesso a sites](#). Adicione URLs a essas listas seguindo o formato de filtro de lista de bloqueio do Chrome para obter os melhores resultados. Para obter mais informações, consulte [Formato do filtro da lista de bloqueio de URL](#).

Para configurar a filtragem de URL usando o editor JSON ou o upload de arquivo

1. No módulo de configurações de política, escolha Editor JSON e ignore o módulo de interface do usuário do console para a visualização Editor ou Upload de arquivo.
  - O editor permite que os clientes criem declarações de políticas personalizadas em linha no console. O editor destaca os erros na instrução JSON durante a criação da política.
  - O upload de arquivos permite que os clientes adicionem um arquivo JSON criado fora do console (como exportado de um navegador Chrome existente).
2. Consulte os detalhes da Política do Chrome para URLAllowlist e URLBlocklist para formatar adequadamente uma lista de permissão/negação de URL para seu portal da web. [Para obter mais informações, consulte URLAllowlist e URLBlocklist](#).

# Segurança no Amazon WorkSpaces Web

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

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

- **Segurança da nuvem:** a AWS é responsável pela proteção da infraestrutura que executa produtos da AWS na Nuvem AWS. A AWS também fornece serviços que podem ser usados com segurança. Auditores de terceiros testam e verificam regularmente a eficácia da nossa segurança como parte dos [Programas de conformidade da AWS](#). Para saber mais sobre os programas de conformidade que se aplicam ao Amazon WorkSpaces Web, consulte [Serviços da AWS no escopo por programa de conformidade](#).
- **Segurança na nuvem:** sua responsabilidade é determinada pelo serviço da AWS que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade dos dados, os requisitos da empresa e quaisquer leis e regulamentos aplicáveis aos seus dados.

Esta documentação ajuda você a entender como aplicar o modelo de responsabilidade compartilhada ao usar o Amazon WorkSpaces Web. Ela mostra como configurar o Amazon WorkSpaces Web para atender aos objetivos de segurança e conformidade. Saiba também como usar outros serviços da AWS que ajudam você a monitorar e proteger os recursos do Amazon WorkSpaces Web.

## Índice

- [Proteção de dados na Amazon WorkSpaces Web](#)
- [Identity and Access Management para Amazon WorkSpaces Web](#)
- [Resposta a incidentes no Amazon WorkSpaces Web](#)
- [Validação de conformidade para Amazon WorkSpaces Web](#)
- [Resiliência no Amazon WorkSpaces Web](#)
- [Segurança da infraestrutura no Amazon WorkSpaces Web](#)
- [Análise de configuração e vulnerabilidade no Amazon WorkSpaces Web](#)

- [Práticas recomendadas de segurança para o Amazon WorkSpaces Web](#)

## Proteção de dados na Amazon WorkSpaces Web

O [modelo de responsabilidade AWS compartilhada](#) de se aplica à proteção de dados na Amazon WorkSpaces Web. Conforme descrito nesse modelo, a AWS é responsável por proteger a infraestrutura global que executa toda a Nuvem AWS. Você é responsável por manter o controle sobre seu conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para obter mais informações sobre a privacidade de dados, consulte as [Perguntas frequentes sobre privacidade de dados](#). Para mais informações sobre a proteção de dados na Europa, consulte o artigo [AWS Shared Responsibility Model and GDPR](#) no Blog de segurança da AWS.

Para fins de proteção de dados, recomendamos que você proteja as Conta da AWS credenciais da e configure as contas de usuário individuais com o AWS IAM Identity Center ou o 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 [multi-factor authentication]) com cada conta.
- Use SSL/TLS para se comunicar com os atributos da AWS. Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure o registro em log das atividades da API e do usuário com o .AWS CloudTrail
- Use AWS as soluções de criptografia da , juntamente com todos os controles de segurança padrão dos 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 a AWS por meio de uma interface de linha de comandos ou uma API, use um endpoint do 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 Name (Nome). Isso inclui quando você trabalha com a WorkSpaces Web ou outros 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.

## Criptografia de dados

A Amazon WorkSpaces Web coleta dados de personalização do portal, como configurações do navegador, configurações do usuário, configurações de rede, informações do provedor de identidade, dados da loja confiável e dados do certificado da loja confiável. WorkSpaces A Web também coleta dados de políticas do navegador, preferências do usuário (para configurações do navegador) e registros de sessão. Os dados coletados são armazenados no Amazon DynamoDB e no Amazon S3. WorkSpaces Usos da web AWS Key Management Service para criptografia.

Para proteger seu conteúdo, siga estas diretrizes:

- Implemente o acesso com privilégios mínimos e crie funções específicas para serem usadas em ações WorkSpaces da Web. Use modelos do IAM para criar um perfil de acesso total ou somente leitura. Para ter mais informações, consulte [Políticas gerenciadas pela AWS para o WorkSpaces Web](#).
- Proteja os dados de ponta a ponta fornecendo uma chave gerenciada pelo cliente, para que a WorkSpaces Web possa criptografar seus dados em repouso com as chaves que você fornece.
- Tenha cuidado ao compartilhar domínios do portal e credenciais do usuário:
  - Os administradores devem fazer login no WorkSpaces console da Amazon e os usuários devem fazer login no portal da WorkSpaces Web.
  - Qualquer pessoa na internet pode acessar o portal da web, mas não pode iniciar uma sessão a menos que tenha credenciais de usuário válidas no portal.
- Os usuários podem encerrar suas sessões explicitamente escolhendo Encerrar sessão. Isso descarta a instância que hospeda a sessão do navegador e resulta no isolamento do navegador.

WorkSpaces A Web protege conteúdo e metadados por padrão, criptografando todos os dados confidenciais com o. AWS KMS Ele coleta a política do navegador e as preferências do usuário para aplicar políticas e configurações durante as sessões WorkSpaces da Web. Se ocorrer um erro ao aplicar as configurações existentes, o usuário não poderá acessar novas sessões nem acessar os sites internos e as aplicações de SaaS da empresa.

## Criptografia inativa

A criptografia em repouso é configurada por padrão. Os dados específicos do cliente usados na WorkSpaces Web são criptografados usando AWS KMS WorkSpaces A Web fornece criptografia em repouso para os recursos que você cria. O serviço aceita uma chave gerenciada pelo cliente do AWS KMS na criação de recursos e, se não for fornecida, uma chave própria da AWS será usada para criptografar os recursos em repouso. O serviço criptografa o documento da Política do navegador que você pode fornecer para personalizar as sessões do navegador, bem como a configuração do provedor de identidades e os nomes de exibição dos seus portais. Essas informações permanecerão criptografadas usando a chave gerenciada pelo cliente ou a chave própria da AWS, enquanto estiverem armazenadas em nosso back-end.

Você pode decidir qual chave será usada ao criar um recurso WorkSpaces da Web. Se os dados que fazem parte desse recurso forem criptografados, a WorkSpaces Web `customerManagedKeyArn` aceitará o campo como parte da `create` API. A chave fornecida deve ser uma chave simétrica do AWS KMS, e o administrador que cria o recurso usando essa chave deve ter as permissões `kms:Decrypt`, `kms:GenerateDataKey` e `kms:CreateGrant`. Depois que um recurso é criado com a chave, ela não pode ser removida nem alterada. Se você usou uma chave gerenciada pelo cliente, o administrador que acessa o recurso deve ter as permissões `kms:Decrypt` e `kms:GenerateDataKey`. Caso veja um erro sobre o acesso ser negado ao usar o console, verifique se o usuário que está utilizando-o tem essas permissões com a chave que foi usada.

É possível solucionar problemas e auditar o uso da chave verificando o status das concessões do AWS KMS. Para obter mais informações, consulte [Managing grants](#). Durante a criação do portal, a WorkSpaces Web cria uma concessão para permitir que o serviço acesse a chave de forma assíncrona. Você pode verificar o status do uso da nossa chave verificando a concessão, bem como o contexto de criptografia fornecido quando a concessão é usada. O contexto de criptografia sempre contém uma entrada com a chave `aws:workspaces-web:portal:id` e um valor igual ao ID do portal. Para outros recursos, o contexto de criptografia sempre conterá uma entrada no formato `aws:workspaces-web:RESOURCE_TYPE:id` e o ID do recurso correspondente.

## Criptografia em trânsito

WorkSpaces A Web criptografa dados em trânsito por HTTPS e TLS 1.2. Você pode enviar uma solicitação WorkSpaces usando o console ou chamadas diretas de API. Os dados da solicitação transferidos são criptografados enviando tudo por meio de uma conexão HTTPS ou TLS. Os dados da solicitação podem ser transferidos do AWS console ou do AWS SDK para a WorkSpaces Web. AWS Command Line Interface

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 do AWS KMS gerenciada pelo cliente para criptografar as informações do cliente. Se você não fornecer uma, a WorkSpaces Web usará uma AWS chave própria. É possível definir sua chave usando o SDK da AWS.

## Privacidade do tráfego entre redes

Para proteger as conexões entre aplicativos WorkSpaces da Web e locais, você usa a WorkSpaces Web para iniciar sessões de navegador dentro da sua própria VPC. A conexão com aplicativos locais é configurada em sua própria VPC e não é controlada pela Web. WorkSpaces

Para proteger as conexões entre contas, a WorkSpaces Web usa uma função vinculada ao serviço para se conectar com segurança às contas dos clientes e executar operações em nome do cliente. Para ter mais informações, consulte [Usar perfis vinculados ao serviço para o WorkSpaces Web](#).

## Registro em log do acesso do usuário

Os administradores podem registrar eventos de sessões WorkSpaces da Web, incluindo visitas de início, término e URL. Esses logs são criptografados e entregues com segurança aos clientes por meio de um Amazon Kinesis Data Stream. As informações de navegação do registro em log de acesso do usuário não são armazenadas pela AWS nem estão disponíveis nas sessões sem o registro configurado. Visitas de URL no modo de navegação anônima ou URLs excluídos do histórico do navegador não são registrados no log de acesso do usuário.

## Identity and Access Management para Amazon WorkSpaces Web

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

### Tópicos

- [Público](#)
- [Autenticando com identidades](#)
- [Como gerenciar acesso usando políticas](#)
- [Como a Amazon WorkSpaces Web funciona com o IAM](#)
- [Exemplos de políticas baseadas em identidade para a Amazon Web WorkSpaces](#)
- [Políticas gerenciadas pela AWS para o WorkSpaces Web](#)
- [Solução de problemas de identidade e acesso à Amazon WorkSpaces Web](#)
- [Usar perfis vinculados ao serviço para o WorkSpaces Web](#)

## Público

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

**Usuário do serviço** — Se você usa o serviço WorkSpaces Web para realizar seu trabalho, seu administrador fornecerá as credenciais e as permissões necessárias. À medida que você usa mais recursos WorkSpaces da Web 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 na WorkSpaces Web, consulte [Solução de problemas de identidade e acesso à Amazon WorkSpaces Web](#).

**Administrador de serviços** — Se você é responsável pelos recursos da WorkSpaces Web em sua empresa, provavelmente tem acesso total à WorkSpaces Web. É seu trabalho determinar quais recursos e recursos WorkSpaces da Web 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 a WorkSpaces Web, consulte [Como a Amazon WorkSpaces Web 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 à WorkSpaces Web. Para ver exemplos de políticas baseadas em identidade WorkSpaces da Web que você pode usar no IAM, consulte. [Exemplos de políticas baseadas em identidade para a Amazon Web WorkSpaces](#)



## Autenticando com identidades

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

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

É possível fazer login no AWS Management Console ou no de acesso da AWS dependendo do tipo de usuário que você é. Para obter mais informações sobre como fazer login na AWS, consulte [Como fazer login na conta da Conta da AWS](#) no Guia do usuário do Início de Sessão da AWS.

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

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

### Usuário raiz da Conta da AWS

Ao criar uma Conta da AWS, você começa com uma identidade de login que tem acesso completo a todos os atributos e Serviços da AWS na conta. Essa identidade, denominada usuário raiz da Conta da AWS, é acessada por login com o endereço de e-mail e a senha que você usou para criar a conta. É altamente recomendável não utilizar o usuário raiz para tarefas diárias. Proteja as credenciais do usuário raiz e use-as para executar as tarefas que somente ele puder 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 os usuários, inclusive os que precisam de acesso de administrador, usem a federação com um provedor de identidades para acessar Serviços da AWS usando credenciais temporárias.

Identidade federada é um usuário de seu diretório de usuários corporativos, um provedor de identidades da web AWS Directory Service, o , o diretório do Centro de Identidade ou qualquer usuário que acesse os Serviços da AWS usando credenciais fornecidas por meio de uma fonte de identidade. Quando as identidades federadas acessam Contas da AWS, elas assumem perfis que fornecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, recomendamos usar o .AWS IAM Identity Center. Você pode criar usuários e grupos no Centro de Identidade do IAM ou se conectar e sincronizar com um conjunto de usuários e grupos em sua própria fonte de identidade para uso em todas as suas Contas da AWS e aplicações. 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.

## Usuários e grupos do IAM

Um [usuário do IAM](#) é uma identidade dentro da Conta da AWS que tem permissões específicas para uma única pessoa ou aplicação. Sempre que possível, recomendamos contar com credenciais temporárias em vez de criar usuários do IAM com credenciais de longo prazo, como senhas e chaves de acesso. No entanto, se você tiver casos de utilização 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 utilizar 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 atributos 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

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

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 Centro de identidade do IAM correlaciona o conjunto de permissões a um perfil no IAM. Para obter informações sobre conjuntos de permissões, consulte [Conjuntos de permissões](#) no Guia do usuário do AWS IAM Identity Center.
- **Permissões temporárias para usuários do IAM:** um usuário ou um perfil do IAM pode 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, alguns Serviços da AWS permitem que você anexe uma política diretamente a um atributo (em vez de usar um perfil como proxy). Para saber a diferença entre perfis e políticas baseadas em atributo para acesso entre contas, consulte [Como os perfis do IAM diferem das políticas baseadas em atributo](#) no Guia do usuário do IAM.
- **Acesso entre serviços:** alguns Serviços da AWS usam atributos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicações no Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões do principal de chamada, usando um perfil de serviço ou uma função vinculada ao serviço.
  - **Encaminhamento de sessões de acesso (FAS):** qualquer pessoa que utilizar uma função ou usuário do IAM para realizar ações na AWS é considerada uma entidade principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O recurso FAS utiliza as permissões da entidade principal que chama um AWS service (Serviço da

AWS), combinadas às permissões do AWS service (Serviço da AWS) solicitante, para realizar solicitações para serviços downstream. As solicitações de FAS só são feitas quando um serviço recebe uma solicitação que exige interações com outros Serviços da AWS ou com recursos para serem concluídas. 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: um 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 um perfil para delegar permissões a um AWS service \(Serviço da AWS\)](#) no Guia do usuário do IAM.
- Função vinculada ao serviço: uma função vinculada a 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. Os perfis vinculados ao serviço aparecem em sua 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.
- Aplicações em execução no Amazon EC2: é possível usar um perfil do IAM para gerenciar credenciais temporárias para aplicações em execução em uma instância do EC2 e fazer solicitações da AWS CLI ou da AWS API. É preferível fazer isso a armazenar chaves de acesso na instância do EC2. Para atribuir um perfil da AWS a uma instância do EC2 e disponibilizá-la para todas as suas aplicações, crie um perfil de instância que esteja anexado a ela. Um perfil de instância contém a 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 os perfis do IAM, consulte [Quando criar um perfil do IAM \(em vez de um usuário\)](#) no Guia do usuário do IAM.

## Como gerenciar acesso usando políticas

Você controla o acesso na AWS criando políticas e anexando-as a identidades ou atributos da AWS. Uma política é um objeto na AWS que, quando associado a uma identidade ou atributo, define suas permissões. A AWS avalia essas políticas quando uma entidade principal (usuário, usuário raiz ou sessão de perfil) faz uma solicitação. As permissões nas políticas determinam se a solicitação será permitida ou negada. A maioria das políticas são armazenadas na AWS como documentos JSON.

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

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

Por padrão, usuários e 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 independente 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 perfil do AWS Management Console, da AWS CLI 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 [Criar políticas do IAM](#) no Guia do usuário do IAM.

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

## Políticas baseadas em recurso

Políticas baseadas em atributos são documentos de políticas JSON que você anexa a um atributo. 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

especificado pode executar nesse recurso e em que condições. Você precisa [especificar uma entidade principal](#) em uma política baseada em recurso. As entidades principais podem incluir contas, usuários, perfis, usuários federados ou Serviços da AWS.

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

## Listas de controle de acesso (ACLs)

As listas de controle de acesso (ACLs) controlam quais entidades principais (membros, usuários ou funções 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.

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

## Outros tipos de política

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

- **Limites de permissões:** um limite de permissões é um 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 com 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 (UO) no AWS Organizations. O AWS Organizations é um serviço para agrupar e gerenciar centralmente várias Contas da AWS pertencentes à sua empresa. Se você habilitar todos os 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 em contas-membro, incluindo cada `.Usuário raiz` da conta da AWS. Para obter mais informações sobre o Organizações e SCPs, consulte [How SCPs work \(Como os SCPs funcionam\)](#) no AWS Organizations Guia do usuário do .

- Políticas de sessão: são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para um perfil ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do usuário ou do perfil e das políticas de sessão. As permissões também podem ser provenientes de uma política baseada em atributo. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações, consulte [Políticas de sessão](#) no Guia 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 a AWS determina se deve permitir uma solicitação quando há vários tipos de política envolvidos, consulte [Lógica da avaliação](#) de políticas no Guia do usuário do IAM.

## Como a Amazon WorkSpaces Web funciona com o IAM

Antes de usar o IAM para gerenciar o acesso à WorkSpaces Web, saiba quais recursos do IAM estão disponíveis para uso com a WorkSpaces Web.

Recursos do IAM que você pode usar com a Amazon WorkSpaces Web

atributo do IAM	WorkSpaces Suporte na web
<a href="#">Políticas baseadas em identidade</a>	Sim
<a href="#">Políticas baseadas em recurso</a>	Não
<a href="#">Ações de políticas</a>	Sim
<a href="#">atributos de políticas</a>	Sim
<a href="#">Chaves de condição de políticas</a>	Sim
<a href="#">ACLs</a>	Não
<a href="#">ABAC (tags em políticas)</a>	Parcial
<a href="#">Credenciais temporárias</a>	Sim

atributo do IAM	WorkSpaces Suporte na web
<a href="#">Permissões de entidade principal</a>	Sim
<a href="#">Perfis de serviço</a>	Não
<a href="#">Funções vinculadas ao serviço</a>	Sim

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

## Políticas baseadas em identidade para a Web WorkSpaces

Suporta 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 do IAM, grupo de usuários ou perfil. 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 atributos 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 a Web WorkSpaces

Para ver exemplos de políticas baseadas em identidade WorkSpaces da Web, consulte. [Exemplos de políticas baseadas em identidade para a Amazon Web WorkSpaces](#)



## Políticas baseadas em recursos na Web WorkSpaces

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

Políticas baseadas em atributos são documentos de políticas JSON que você anexa a um atributo. 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 especificado pode executar nesse recurso e em que condições. Você precisa [especificar uma entidade principal](#) em uma política baseada em recurso. As entidades principais podem incluir contas, usuários, perfis, 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 atributo. Adicionar uma entidade principal entre contas à política baseada em recurso é apenas metade da tarefa de estabelecimento da relação de confiança. Quando a entidade principal e o atributo estão em diferentes Contas da AWS, um administrador do IAM da conta confiável também deve conceder à entidade principal (usuário ou perfil) permissão para acessar o atributo. 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 as funções do IAM diferem de políticas baseadas em recurso](#) no Guia do usuário do IAM.

## Ações políticas para a WorkSpaces Web

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

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

O elemento `Action` de uma política JSON descreve as ações que você pode usar para permitir ou negar acesso em uma política. As ações de política geralmente têm o mesmo nome que a operação de API da AWS associada. Existem algumas exceções, como ações somente de permissão, que não



têm uma operação de API correspondente. Algumas operações também exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

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

Para ver uma lista de ações WorkSpaces da Web, consulte [Ações definidas pela Amazon WorkSpaces Web](#) na Referência de Autorização de Serviço.

As ações de política na WorkSpaces Web usam o seguinte prefixo antes da ação:

```
workspaces-web
```

Para especificar várias ações em uma única instrução, separe-as com vírgulas.

```
"Action": [  
  "workspaces-web:action1",  
  "workspaces-web:action2"  
]
```

Para ver exemplos de políticas baseadas em identidade WorkSpaces da Web, consulte. [Exemplos de políticas baseadas em identidade para a Amazon Web WorkSpaces](#)

## Recursos de políticas para a WorkSpaces Web

Oferece suporte a atributos de políticas	Sim
--	-----

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

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 atributo usando seu [Nome do atributo da Amazon \(ARN\)](#). Isso pode ser feito para ações que oferecem suporte a um tipo de atributo específico, conhecido como permissões em nível de atributo.

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 WorkSpaces da Web e seus ARNs, consulte [Recursos definidos pela Amazon WorkSpaces Web](#) na Referência de autorização de serviço. Para saber com quais ações você pode especificar o ARN de cada recurso, consulte [Ações definidas pela Amazon WorkSpaces Web](#).

Para ver exemplos de políticas baseadas em identidade WorkSpaces da Web, consulte [Exemplos de políticas baseadas em identidade para a Amazon Web WorkSpaces](#)

## Chaves de condição de política para a WorkSpaces Web

Suporta chaves de condição de política específicas de serviço	Sim
---	-----

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

O elemento `Condition` (ou `Condition` bloco de) 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 `Condition` elemento, a AWS os avaliará usando uma operação lógica AND. Se você especificar vários valores para uma única chave de condição, a AWS avaliará a condição usando uma operação lógica OR. Todas as condições devem ser atendidas antes que as permissões da instrução sejam concedidas.

Você também pode utilizar variáveis de espaço reservado ao especificar as condições. Por exemplo, é possível conceder a um usuário do IAM permissão para acessar um atributo 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.

A AWS oferece suporte a chaves de condição globais e chaves de condição específicas do serviço. Para ver todas as AWS chaves de condição globais da , consulte [AWSChaves de contexto de condição globais da](#) no Guia do usuário do IAM.

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

Para ver exemplos de políticas baseadas em identidade WorkSpaces da Web, consulte. [Exemplos de políticas baseadas em identidade para a Amazon Web WorkSpaces](#)

## Listas de controle de acesso (ACLs) na Web WorkSpaces

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.

## Controle de acesso baseado em atributos (ABAC) com Web WorkSpaces

Oferece suporte a ABAC (tags em políticas)

Parcial

O controle de acesso baseado em atributo (ABAC) é uma estratégia de autorização que define permissões com base em atributos. Na AWS, esses atributos são chamados de tags. É possível anexar tags a entidades do IAM (usuários ou perfis) e a muitos atributos da AWS. A marcação de entidades e atributos 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 atributo que ela está tentando acessar.

O ABAC é útil em ambientes que estão crescendo rapidamente e ajuda em situações onde 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 a Web WorkSpaces

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 que funcionam com o IAM](#) no Guia do usuário do IAM.

Você está usando credenciais temporárias se faz login no AWS Management Console usando qualquer método, exceto um nome de usuário e uma senha. Por exemplo, quando você acessa a AWS usando o link de autenticação única (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 um perfil \(console\)](#) no Guia do usuário do IAM.

Você pode criar credenciais temporárias manualmente usando a AWS CLI ou a API da AWS. Em seguida, você pode usar essas credenciais temporárias para acessar a AWS. A 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 a Web WorkSpaces

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

Quando você usa um usuário ou perfil do IAM para executar ações na AWS, você é considerado uma entidade principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O recurso FAS utiliza as permissões da entidade principal que chama um AWS service (Serviço da AWS), combinadas às permissões do AWS service (Serviço da AWS) solicitante, para realizar solicitações para serviços downstream. As solicitações de FAS só são feitas

quando um serviço recebe uma solicitação que exige interações com outros Serviços da AWS ou com recursos para serem concluídas. 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 a WorkSpaces Web

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 um perfil 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 prejudicar a funcionalidade da WorkSpaces Web. Edite funções de serviço somente quando a WorkSpaces Web fornecer orientação para fazer isso.

## Funções vinculadas a serviços para a Web WorkSpaces

Oferece suporte a perfis vinculados ao serviço	Sim
--	-----

Um perfil vinculado ao serviço é um tipo de perfil de serviço vinculado a um AWS service (Serviço da AWS). O serviço pode presumir a função de executar uma ação em seu nome. Os perfis vinculados ao serviço aparecem em sua Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não pode editar as permissões para 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 Função vinculada ao serviço. Escolha o link Sim para visualizar a documentação do perfil vinculado a esse serviço .

## Exemplos de políticas baseadas em identidade para a Amazon Web WorkSpaces

Por padrão, usuários e funções não têm permissão para criar ou modificar recursos WorkSpaces da Web. Eles também não podem executar tarefas usando o AWS Management Console, a AWS Command Line Interface (AWS CLI) ou a API AWS. Para conceder aos usuários permissão para executar ações nos recursos de que 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 pela WorkSpaces Web, incluindo o formato dos ARNs para cada um dos tipos de recursos, consulte [Ações, recursos e chaves de condição para a Amazon WorkSpaces Web](#) na Referência de Autorização de Serviço.

### Tópicos

- [Melhores práticas de políticas](#)
- [Usando o console WorkSpaces da Web](#)
- [Permitir que usuários visualizem suas próprias permissões](#)

### Melhores práticas de políticas

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir recursos WorkSpaces da Web 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 AWS as políticas gerenciadas pela e avance para as permissões de privilégio mínimo: para começar a conceder permissões a seus usuários e workloads, use as AWS políticas gerenciadas pela que concedem permissões para muitos casos de uso comuns. Elas estão disponíveis na sua Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo cliente da AWS específicas para seus casos de uso. Para obter mais informações, consulte [Políticas gerenciadas pela AWS](#) ou [Políticas gerenciadas pela AWS para 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 atributos 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 atributos. Por exemplo, você pode escrever uma condição de política para especificar que todas as solicitações devem ser enviadas usando SSL. Você também pode usar condições para conceder acesso a ações de serviço, se elas forem usadas por meio de um AWS service (Serviço da AWS) específico, como o AWS CloudFormation. Para obter mais informações, consulte [Elementos de política JSON do IAM: Condition](#) no 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 100 verificações de política e recomendações acionáveis para ajudá-lo 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 houver um cenário que exija usuários do IAM ou um usuário raiz em sua Conta da AWS, ative a MFA para obter segurança adicional. Para exigir 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 da Web

Para acessar o console WorkSpaces da Amazon Web, você deve ter um conjunto mínimo de permissões. Essas permissões devem permitir que você liste e visualize detalhes sobre os recursos WorkSpaces da Web em sua 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.

Não é necessário conceder permissões mínimas do console para usuários que fazem chamadas somente à AWS CLI ou à AWS API. Em vez disso, permita o acesso somente a ações que correspondam a operação de API que estiverem tentando executar.

Para garantir que usuários e funções ainda possam usar o console WorkSpaces Web, anexe também a política ReadOnly AWS gerenciada ConsoleAccess ou a WorkSpaces Web às entidades. Para obter mais informações, consulte [Adicionando Permissões a um Usuário](#) no Guia do Usuário do IAM.

## Permitir que usuários visualizem suas próprias permissões

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

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



```
]
}
```

## Políticas gerenciadas pela AWS para o WorkSpaces Web

Para adicionar permissões a usuários, grupos e funções, é mais fácil usar políticas gerenciadas pela AWS do que gravar políticas por conta própria. É necessário tempo e experiência para [criar políticas gerenciadas pelo cliente do IAM](#) que fornecem à sua equipe apenas as permissões de que precisam. Para começar rapidamente, é possível usar nossas políticas gerenciadas pela AWS. Essas políticas abrangem casos de uso comuns e estão disponíveis na sua conta da AWS. Para obter mais informações sobre políticas gerenciadas pela AWS, consulte [Políticas gerenciadas pela AWS](#) no Guia do usuário do IAM.

Os serviços da AWS mantêm e atualizam políticas gerenciadas pela AWS. Não é possível alterar as permissões em políticas gerenciadas pela AWS. Os serviços podem ocasionalmente acrescentar permissões adicionais a uma política gerenciada pela AWS para oferecer suporte a novos recursos. Esse tipo de atualização afeta todas as identidades (usuários, grupos e funções) em que a política está anexada. É mais provável que os serviços atualizem uma política gerenciada pela AWS quando um novo recurso for iniciado ou novas operações se tornarem disponíveis. Os serviços não removem permissões de uma política gerenciada pela AWS, portanto, as atualizações de políticas não suspendem suas permissões existentes.

Além disso, a AWS oferece suporte a políticas gerenciadas para funções de trabalho que abrangem vários serviços. Por exemplo, a política `ReadOnlyAccess` gerenciada pela AWS concede acesso somente leitura a todos os recursos e serviços da AWS. Quando um serviço executa um novo recurso, a AWS adiciona permissões somente leitura para novas operações e recursos. Para obter uma lista e descrições das políticas de funções de trabalho, consulte [Políticas gerenciadas pela AWS para funções de trabalho](#) no Guia do usuário do IAM.

### Política gerenciada pela AWS: `AmazonWorkSpacesWebServiceRolePolicy`

Não é possível anexar a política `AmazonWorkSpacesWebServiceRolePolicy` às suas entidades do IAM. Essa política é anexada a um perfil vinculado ao serviço que permite que o WorkSpaces Web realize ações em seu nome. Para obter mais informações, consulte [the section called “Uso de funções vinculadas a serviço”](#).

Essa política concede permissões administrativas que concedem acesso aos serviços e recursos da AWS usados ou gerenciados pelo Amazon WorkSpaces Web.

### Detalhes da permissão

Esta política inclui as seguintes permissões:

- `WorkSpaces Web`: permite acesso a serviços e recursos da AWS usados ou gerenciados pelo Amazon WorkSpaces Web.
- `ec2`: permite que as entidades principais descrevam VPCs, sub-redes e zonas de disponibilidade; criem, marquem, descrevam e excluam interfaces de rede; associem ou desassociem um endereço; e descrevam tabelas de rotas, grupos de segurança e endpoints da VPC.
- `CloudWatch`: permite que as entidades principais coloquem dados de métricas.
- `Kinesis`: permite que as entidades principais descrevam um resumo dos fluxos de dados do Kinesis e coloquem registros nos fluxos de dados do Kinesis para registro em log de acesso do usuário. Para obter mais informações, consulte [the section called “Configurar o registro de acesso do usuário”](#).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeNetworkInterfaces",
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
```

```

        "ec2:DescribeVpcEndpoints"
    ],
    "Resource": "*"
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:CreateNetworkInterface"
    ],
    "Resource": [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:CreateNetworkInterface"
    ],
    "Resource": "arn:aws:ec2:*:*:network-interface/*",
    "Condition": {
        "StringEquals": {
            "aws:RequestTag/WorkSpacesWebManaged": "true"
        }
    }
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:CreateTags"
    ],
    "Resource": "arn:aws:ec2:*:*:network-interface/*",
    "Condition": {
        "StringEquals": {
            "ec2:CreateAction": "CreateNetworkInterface"
        },
        "ForAllValues:StringEquals": {
            "aws:TagKeys": [
                "WorkSpacesWebManaged"
            ]
        }
    }
},
{

```

```

    "Effect": "Allow",
    "Action": [
      "ec2:DeleteNetworkInterface"
    ],
    "Resource": "arn:aws:ec2:*:*:network-interface/*",
    "Condition": {
      "StringEquals": {
        "aws:ResourceTag/WorkSpacesWebManaged": "true"
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "cloudwatch:PutMetricData"
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "cloudwatch:namespace": [
          "AWS/WorkSpacesWeb",
          "AWS/Usage"
        ]
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "kinesis:PutRecord",
      "kinesis:PutRecords",
      "kinesis:DescribeStreamSummary"
    ],
    "Resource": "arn:aws:kinesis:*:*:stream/amazon-workspaces-web-*"
  }
]
}

```

## Política gerenciada pela AWS: AmazonWorkSpacesWebReadOnly

É possível anexar a política AmazonWorkSpacesWebReadOnly a suas identidades do IAM.

Essa política concede permissões somente leitura que permitem acesso ao WorkSpaces Web e suas dependências por meio do SDK, da CLI e do Console de Gerenciamento da AWS. Essa política não inclui as permissões necessárias para interagir com portais usando o IAM\_Identity\_Center como tipo de autenticação. Para obter essas permissões, combine essa política com AWSSSOReadOnly.

## Detalhes da permissão

Esta política inclui as seguintes permissões.

- **WorkSpaces Web**: concede acesso somente leitura ao Amazon WorkSpaces Web e suas dependências por meio do SDK, da CLI e do Console de Gerenciamento da AWS.
- **ec2**: permite que as entidades principais descrevam VPCs, sub-redes e grupos de segurança. Isso é usado no Console de Gerenciamento da AWS no WorkSpaces Web para mostrar suas VPCs, sub-redes e grupos de segurança que estão disponíveis para uso com o serviço.
- **Kinesis**: permite que as entidades principais listem fluxos de dados do Kinesis. Isso é usado no Console de Gerenciamento da AWS no WorkSpaces Web para mostrar fluxos de dados do Kinesis que estão disponíveis para uso com o serviço.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces-web:GetBrowserSettings",
        "workspaces-web:GetIdentityProvider",
        "workspaces-web:GetNetworkSettings",
        "workspaces-web:GetPortal",
        "workspaces-web:GetPortalServiceProviderMetadata",
        "workspaces-web:GetTrustStore",
        "workspaces-web:GetTrustStoreCertificate",
        "workspaces-web:GetUserSettings",
        "workspaces-web:GetUserAccessLoggingSettings",
        "workspaces-web:ListBrowserSettings",
        "workspaces-web:ListIdentityProviders",
        "workspaces-web:ListNetworkSettings",
        "workspaces-web:ListPortals",

```

```

        "workspaces-web:ListTagsForResource",
        "workspaces-web:ListTrustStoreCertificates",
        "workspaces-web:ListTrustStores",
        "workspaces-web:ListUserSettings",
        "workspaces-web:ListUserAccessLoggingSettings"
    ],
    "Resource": "arn:aws:workspaces-web:*:*:*"
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "kinesis:ListStreams"
    ],
    "Resource": "*"
}
]
}

```

## Atualizações do WorkSpaces Web para políticas gerenciadas pela AWS

Visualize detalhes sobre atualizações em políticas gerenciadas pela AWS para o WorkSpaces Web desde que esse serviço começou a rastrear essas alterações. Para obter alertas automáticos sobre alterações feitas nesta página, inscreva-se no feed RSS na página [Histórico do documento](#).

Alteração	Descrição	Data
<a href="#">AmazonWorkSpacesWebServiceRolePolicy</a> – Política atualizada	O WorkSpaces Web atualizou a política para restringir <code>CreateNetworkInterface</code> à marcação com <code>aws:RequestTag/WorkSpacesWebManaged: true</code> e agir nos recursos da sub-rede e do grupo de segurança, bem como restringir a <code>DeleteNet</code>	15 de dezembro de 2022

Alteração	Descrição	Data
	workInterface às ENIs marcadas com aws:ResourceTag/WorkSpacesWebManaged: true.	
<a href="#">AmazonWorkSpacesWebReadOnly</a> – Política atualizada	<p>O WorkSpaces Web atualizou a política para incluir permissões de leitura para o registro em log de acesso do usuário e para listar fluxos de dados do Kinesis. Para obter mais informações, consulte <a href="#">the section called “Configurar o registro de acesso do usuário”</a>.</p>	2 de novembro de 2022
<a href="#">AmazonWorkSpacesWebServiceRolePolicy</a> – Política atualizada	<p>O WorkSpaces Web atualizou a política para descrever um resumo dos fluxos de dados do Kinesis e colocar registros nos fluxos de dados do Kinesis para registro em log de acesso do usuário. Para obter mais informações, consulte <a href="#">the section called “Configurar o registro de acesso do usuário”</a>.</p>	17 de outubro de 2022
<a href="#">AmazonWorkSpacesWebServiceRolePolicy</a> – Política atualizada	<p>O WorkSpaces Web atualizou a política para criar tags durante a criação da ENI.</p>	6 de setembro de 2022

Alteração	Descrição	Data
<a href="#">AmazonWorkSpacesWebServiceRolePolicy</a> – Política atualizada	O WorkSpaces Web atualizou a política para adicionar o namespace AWS/Usage às permissões da API PutMetric Data.	6 de abril de 2022
<a href="#">AmazonWorkSpacesWebReadOnly</a> – Nova política	O WorkSpaces Web adicionou uma nova política para fornecer acesso somente leitura ao Amazon WorkSpaces Web e suas dependências por meio do SDK, da CLI e do Console de Gerenciamento da AWS.	30 de novembro de 2021
<a href="#">AmazonWorkSpacesWebServiceRolePolicy</a> – Nova política	O WorkSpaces Web adicionou uma nova política para permitir o acesso aos serviços e recursos da AWS usados ou gerenciados pelo Amazon WorkSpaces Web.	30 de novembro de 2021
O WorkSpaces Web começou a monitorar alterações	O WorkSpaces Web começou a monitorar as alterações para as políticas gerenciadas pela AWS.	30 de novembro de 2021

## Solução de problemas de identidade e acesso à Amazon WorkSpaces Web

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

### Tópicos

- [Não estou autorizado a realizar uma ação na WorkSpaces Web](#)
- [Não estou autorizado a realizar iam: PassRole](#)



- [Quero permitir que pessoas fora da minha AWS conta acessem meus recursos WorkSpaces da Web](#)

## Não estou autorizado a realizar uma ação na WorkSpaces Web

Se você receber uma mensagem de erro informando que não tem autorização para executar uma ação, suas políticas deverão ser atualizadas para permitir que você realize a ação.

O erro do exemplo a seguir ocorre quando o usuário do IAM `mateojackson` tenta usar o console para visualizar detalhes sobre um atributo `my-example-widget` fictício, mas não tem as permissões `workspaces-web: GetWidget` fictícias.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
workspaces-web: GetWidget on resource: my-example-widget
```

Nesse caso, a política do usuário `mateojackson` deve ser atualizada para permitir o acesso ao atributo `my-example-widget` usando a ação `workspaces-web: GetWidget`.

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

## Não estou autorizado a realizar iam: PassRole

Se você receber um erro informando que não está autorizado a realizar a `iam:PassRole` ação, suas políticas devem ser atualizadas para permitir que você passe uma função para a WorkSpaces Web.

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

O exemplo de erro a seguir ocorre quando um usuário do IAM chamado `marymajor` tenta usar o console para realizar uma ação na WorkSpaces Web. No entanto, a ação exige que o serviço tenha permissões concedidas por um perfil de serviço. Mary não tem permissões para passar o perfil para o serviço.

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

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

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

## Quero permitir que pessoas fora da minha AWS conta acessem meus recursos WorkSpaces da Web

Você pode criar um perfil que os usuários de outras contas ou pessoas fora da sua organização possam 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 a WorkSpaces Web oferece suporte a esses recursos, consulte [Como a Amazon WorkSpaces Web funciona com o IAM](#).
- Para saber como conceder acesso a seus atributos em todas as Contas da AWS pertencentes a você, consulte [Fornecimento de acesso a um usuário do IAM em outra Conta da AWS pertencente a você](#) no Guia de usuário do IAM.
- Para saber como conceder acesso a seus recursos para Contas da AWS terceirizadas, consulte [Fornecimento de acesso a Contas da AWS pertencentes a terceiros](#) no Guia do usuário do IAM.
- Para saber como conceder acesso por meio da federação de identidades, consulte [Conceder acesso a usuários autenticados externamente \(federação de identidades\)](#) no Guia do usuário do IAM.
- Para saber a diferença entre usar perfis e políticas baseadas em atributos para acesso entre contas, consulte [Como os perfis do IAM diferem de políticas baseadas em atributos](#) no Guia do usuário do IAM.

## Usar perfis vinculados ao serviço para o WorkSpaces Web

O WorkSpaces Web usa [perfis vinculados ao serviço](#) do AWS Identity and Access Management (IAM). O perfil vinculado ao serviço é um tipo exclusivo de perfil do IAM vinculado diretamente ao WorkSpaces Web. Os perfis vinculadas ao serviço são predefinidos pelo WorkSpaces Web e incluem todas as permissões que o serviço requer para chamar outros serviços da AWS em seu nome.

Um perfil vinculado ao serviço facilita a configuração do WorkSpaces Web porque você não precisa adicionar as permissões necessárias manualmente. O WorkSpaces Web define as permissões dos perfis vinculados ao serviço e, exceto se definido de outra forma, somente o WorkSpaces Web pode assumir seus perfis. As permissões definidas incluem as políticas de confiança e de permissões. A política de permissões não pode ser anexada a nenhuma outra entidade do IAM.

Você pode excluir uma função vinculada ao serviço somente depois de primeiro excluir seus recursos relacionados. Isso protege seus recursos do WorkSpaces Web, pois você não pode remover por engano as permissões para acessar os recursos.

Para obter informações sobre outros serviços compatíveis com funções vinculadas a serviços, consulte [Serviços da AWS compatíveis com o IAM](#) e procure os serviços que contenham Yes (Sim) na coluna Service-Linked Role (Função vinculada a serviço). Escolha um Sim com um link para visualizar a documentação da função vinculada a esse serviço.

## Permissões de perfil vinculado ao serviço para o WorkSpaces Web

O WorkSpaces Web usa o perfil vinculado ao serviço chamado `AWSServiceRoleForAmazonWorkSpacesWeb`: o WorkSpaces Web usa esse perfil vinculado ao serviço para acessar os recursos do Amazon EC2 de contas de clientes para instâncias de streaming e métricas do CloudWatch.

A função vinculada ao serviço `AWSServiceRoleForAmazonWorkSpacesWeb` confia nos seguintes serviços para assumir a função:

- `workspaces-web.amazonaws.com`

A política de permissões do perfil chamada `AmazonWorkSpacesWebServiceRolePolicy` permite que o WorkSpaces Web conclua as ações a seguir nos recursos especificados. Para obter mais informações, consulte [the section called “AmazonWorkSpacesWebServiceRolePolicy”](#).

- Ação: `ec2:DescribeVpcs` em all AWS resources
- Ação: `ec2:DescribeSubnets` em all AWS resources
- Ação: `ec2:DescribeAvailabilityZones` em all AWS resources
- Ação: `ec2:CreateNetworkInterface` com `aws:RequestTag/WorkSpacesWebManaged: true` em recursos de sub-rede e grupo de segurança
- Ação: `ec2:DescribeNetworkInterfaces` em all AWS resources

- Ação: `ec2:DeleteNetworkInterface` em interfaces de rede com `aws:ResourceTag/WorkSpacesWebManaged: true`
- Ação: `ec2:DescribeSubnets` em all AWS resources
- Ação: `ec2:AssociateAddress` em all AWS resources
- Ação: `ec2:DisassociateAddress` em all AWS resources
- Ação: `ec2:DescribeRouteTables` em all AWS resources
- Ação: `ec2:DescribeSecurityGroups` em all AWS resources
- Ação: `ec2:DescribeVpcEndpoints` em all AWS resources
- Ação: `ec2:CreateTags` na operação `ec2:CreateNetworkInterface` com `aws:TagKeys: ["WorkSpacesWebManaged"]`
- Ação: `cloudwatch:PutMetricData` em all AWS resources
- Ação: `kinesis:PutRecord` em fluxos de dados do Kinesis com nomes que começam com `amazon-workspaces-web-`
- Ação: `kinesis:PutRecords` em fluxos de dados do Kinesis com nomes que começam com `amazon-workspaces-web-`
- Ação: `kinesis:DescribeStreamSummary` em fluxos de dados do Kinesis com nomes que começam com `amazon-workspaces-web-`

Você deve configurar permissões para que uma entidade do IAM (por exemplo, um usuário, grupo ou função) crie, edite ou exclua uma função vinculada ao serviço. Para obter mais informações, consulte [Permissões de função vinculada ao serviço](#) no Guia do usuário do IAM.

## Criar um perfil vinculado ao serviço para o WorkSpaces Web

Não é necessário criar manualmente uma função vinculada ao serviço. Ao criar seu primeiro portal no AWS Management Console, na AWS CLI ou na API da AWS, o WorkSpaces Web cria o perfil vinculado ao serviço para você.

### Important

Essa função vinculada ao serviço pode aparecer em sua conta se você concluiu uma ação em outro serviço que usa os recursos compatíveis com essa função.

Se excluir esse perfil vinculado ao serviço e precisar criá-lo novamente, você poderá usar esse mesmo processo para recriar o perfil em sua conta. Quando você cria seu primeiro portal, o WorkSpaces Web cria um perfil vinculado ao serviço novamente.

Você também pode usar o console do IAM para criar um perfil vinculado ao serviço com o caso de uso do WorkSpaces Web. Na AWS CLI ou na API do AWS, crie uma função vinculada ao serviço com o nome de serviço `workspaces-web.amazonaws.com`. Para obter mais informações, consulte [Criar uma função vinculada ao serviço](#) no Guia do usuário do IAM. Se você excluir essa função vinculada ao serviço, será possível usar esse mesmo processo para criar a função novamente.

## Editar um perfil vinculado ao serviço para o WorkSpaces Web

O WorkSpaces Web não permite que você edite a o perfil vinculado a serviço `AWSServiceRoleForAmazonWorkSpacesWeb`. Depois que você criar uma função vinculada a serviço, não poderá alterar o nome da função, pois várias entidades podem fazer referência à função. No entanto, você poderá editar a descrição da função usando o IAM. Para obter mais informações, consulte [Editar uma função vinculada ao serviço](#) no Guia do usuário do IAM.

## Excluir um perfil vinculado ao serviço do WorkSpaces Web

Se você não precisar mais usar um recurso ou serviço que requer uma função vinculada a serviço, é recomendável excluí-la. Dessa forma, você não tem uma entidade não utilizada que não seja monitorada ativamente ou mantida. No entanto, você deve limpar os recursos de sua função vinculada ao serviço antes de excluí-la manualmente.

### Note

Se o serviço WorkSpaces Web estiver usando o perfil quando você tenta excluir os recursos, a exclusão poderá falhar. Se isso acontecer, espere alguns minutos e tente a operação novamente.

Para excluir os recursos do WorkSpaces Web usados por `AWSServiceRoleForAmazonWorkSpacesWeb`

- Escolha uma das seguintes opções:
  - Se você usa o console, exclua todos os seus portais no console.

- Se você usa a CLI ou a API, desassocie todos os seus recursos (incluindo configurações do navegador, configurações de rede, configurações do usuário, armazenamentos confiáveis e configurações de registro de acesso do usuário) dos seus portais, exclua esses recursos e exclua os portais.

Como excluir manualmente a função vinculada ao serviço usando o IAM

Use o console do IAM, a AWS CLI ou a API da AWS para excluir o perfil vinculado ao serviço `AWSServiceRoleForAmazonWorkSpacesWeb`. Para obter mais informações, consulte [Excluir uma função vinculada ao serviço](#) no Guia do usuário do IAM.

Regiões compatíveis com perfis vinculadas ao serviço do WorkSpaces Web

O WorkSpaces Web é compatível com perfis vinculados ao serviço em todas as regiões em que o serviço está disponível. Para obter mais informações, consulte [Regiões e endpoints do AWS](#).

## Resposta a incidentes no Amazon WorkSpaces Web

É possível detectar incidentes monitorando a métrica `SessionFailure` do Amazon CloudWatch. Para receber alertas de incidentes, use um alarme do CloudWatch para a métrica `SessionFailure`. Para obter mais informações, consulte [Monitorando a Amazon WorkSpaces Web com a Amazon CloudWatch](#).


## Validação de conformidade para Amazon WorkSpaces Web

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

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

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

- [Guias de referência rápida de conformidade e segurança](#) - estes guias de implantação discutem considerações sobre arquitetura e fornecem as etapas para a implantação de ambientes de linha de base focados em segurança e conformidade na AWS.
- [Arquitetura para segurança e conformidade com HIPAA no Amazon Web Services](#): esse whitepaper descreve como as empresas podem usar a AWS para criar aplicações adequadas aos padrões HIPAA.

 Note

Nem todos os Serviços da AWS estão qualificados pela HIPAA. Para obter mais informações, consulte a [Referência dos serviços qualificados pela HIPAA](#).

- [atributos de conformidade da AWS](#): essa coleção de manuais e guias pode ser aplicada a seu setor e local.
- [Guias de conformidade do cliente da AWS](#): entenda o modelo de responsabilidade compartilhada sob a ótica da conformidade. Os guias resumem as práticas recomendadas para proteção de Serviços da AWS e mapeiam as diretrizes para controles de segurança em várias estruturas (incluindo o Instituto Nacional de Padrões e Tecnologia (NIST), o Conselho de Padrões de Segurança do Setor de Cartões de Pagamento (PCI) e a Organização Internacional de Padronização (ISO)).
- [Avaliar atributos com regras](#) no AWS Config Guia do desenvolvedor: o serviço AWS Config avalia como as configurações de atributos estão em conformidade com práticas internas, diretrizes do setor e regulamentos.
- [AWS Security Hub](#): este AWS service (Serviço da AWS) fornece uma visão abrangente do seu estado de segurança na AWS. O Security Hub usa controles de segurança para avaliar os atributos da AWS e verificar a conformidade com os padrões e as práticas recomendadas do setor de segurança. Para obter uma lista dos serviços e controles aceitos, consulte a [Referência de controles do Security Hub](#).
- [AWS Audit Manager](#) – Esse AWS service (Serviço da AWS) ajuda a auditar continuamente seu uso da AWS para simplificar a forma como você gerencia os riscos e a conformidade com regulamentos e padrões do setor.

## Resiliência no Amazon WorkSpaces Web

A infraestrutura global da AWS se baseia em Regiões da AWS e zonas de disponibilidade. A Regiões da AWS oferece várias zonas de disponibilidade separadas e isoladas fisicamente que

são conectadas com baixa latência, throughputs elevadas e em redes altamente redundantes. Com as zonas de disponibilidade, é possível projetar e operar aplicações e bancos de dados que automaticamente executam o failover entre as zonas sem interrupção. As zonas de disponibilidade são mais altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de data center tradicionais.

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

Os itens a seguir não são compatíveis com o WorkSpaces Web no momento:

- Backup de conteúdo em AZs ou regiões
- Backups criptografados
- Criptografia de conteúdo em trânsito entre AZs ou regiões
- Backups padrão ou automáticos

Para configurar a alta disponibilidade da internet, é possível ajustar a configuração da VPC. Para alta disponibilidade da API, você pode solicitar a quantidade certa de TPS.

## Segurança da infraestrutura no Amazon WorkSpaces Web

Como um serviço gerenciado, o Amazon WorkSpaces Web é protegido pela segurança da rede global da AWS. Para obter informações sobre serviços de segurança da AWS e como a AWS protege a infraestrutura, consulte [Segurança na Nuvem AWS](#). Para projetar seu ambiente da AWS usando as práticas recomendadas de segurança de infraestrutura, consulte [Proteção de infraestrutura](#) em Pilar segurança: AWS Well-Architected Framework.

Você usa chamadas de API publicadas pela AWS para acessar o Amazon WorkSpaces Web por meio da rede. Os clientes devem oferecer suporte para:

- Transport Layer Security (TLS). Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Conjuntos de criptografia com perfect forward secrecy (PFS) como DHE (Ephemeral Diffie-Hellman) ou ECDHE (Ephemeral Elliptic Curve Diffie-Hellman). A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

Além disso, as solicitações devem ser assinadas usando um ID da chave de acesso e uma chave de acesso secreta associada a uma entidade principal do IAM. Ou você pode usar o [AWS](#)



[Security Token Service](#) (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

O WorkSpaces Web isola o tráfego de serviços aplicando a autenticação e autorização SigV4 AWS padrão a todos os serviços. O endpoint de recursos do cliente (ou endpoint do portal da web) é protegido pelo seu provedor de identidades. Você pode isolar ainda mais o tráfego usando a autorização multifator e outros mecanismos de segurança em seu provedor de identidades (IdP).

Todo o acesso à internet pode ser controlado definindo configurações de rede, como VPC, sub-rede ou grupo de segurança. Atualmente, não há suporte para multilocação e endpoints da VPC (PrivateLink).

## Análise de configuração e vulnerabilidade no Amazon WorkSpaces Web

O WorkSpaces Web atualiza e corrige aplicações e plataformas conforme necessário em seu nome, incluindo Chrome e Linux. Você não precisa corrigir nem recriar. No entanto, é sua responsabilidade configurar o WorkSpaces Web de acordo com as especificações e diretrizes e monitorar o uso do WorkSpaces Web por seus usuários. Todas as configurações relacionadas ao serviço e a análise de vulnerabilidades são de responsabilidade do WorkSpaces Web.

Você pode solicitar um aumento de limite para os recursos do WorkSpaces Web, como o número de portais da web e o número de usuários. O WorkSpaces Web garante a disponibilidade do serviço e do SLA.

## Práticas recomendadas de segurança para o Amazon WorkSpaces Web

O Amazon WorkSpaces Web fornece uma série de recursos de segurança que você pode usar no desenvolvimento e na implementação das suas próprias políticas de segurança. As práticas recomendadas a seguir são diretrizes gerais e não representam uma solução completa de segurança. Como essas práticas recomendadas podem não ser adequadas ou suficientes no seu ambiente, trate-as como considerações úteis em vez de requisitos.

As práticas recomendadas para o Amazon WorkSpaces Web incluem o seguinte:

- Para detectar possíveis eventos de segurança associados ao seu uso do WorkSpaces Web, use o AWS CloudTrail ou o Amazon CloudWatch para detectar e rastrear o histórico de acesso e os logs

de processos. Para obter mais informações, consulte [Monitorando a Amazon WorkSpaces Web com a Amazon CloudWatch](#) e [Log de chamadas de API do Amazon WorkSpaces Web usando o AWS CloudTrail](#).

- Para implementar controles de detecção e identificar anomalias, use os logs do CloudTrail e as métricas do CloudWatch. Para obter mais informações, consulte [Monitorando a Amazon WorkSpaces Web com a Amazon CloudWatch](#) e [Log de chamadas de API do Amazon WorkSpaces Web usando o AWS CloudTrail](#).
- É possível configurar o registro em log de acesso do usuário para registrar os eventos do usuário. Para obter mais informações, consulte [the section called “Configurar o registro de acesso do usuário”](#).

Para evitar possíveis eventos de segurança associados ao seu uso do WorkSpaces Web, siga estas práticas recomendadas:

- Implemente o acesso de privilégio mínimo e crie perfis específicos para serem usados nas ações do WorkSpaces Web. Use modelos do IAM para criar um perfil de acesso total ou somente leitura. Para obter mais informações, consulte [Políticas gerenciadas pela AWS para o WorkSpaces Web](#).
- Tenha cuidado ao compartilhar domínios do portal e credenciais do usuário. Qualquer pessoa na internet pode acessar o portal da web, mas não pode iniciar uma sessão a menos que tenha uma credencial de usuário válida para o portal. Tenha cuidado sobre como, quando e com quem você compartilha as credenciais do portal da web.

# Monitoramento da Amazon WorkSpaces Web

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

- A Amazon CloudWatch monitora seus AWS recursos e os aplicativos em que você executa AWS em tempo real. É possível coletar e rastrear métricas, criar painéis personalizados e definir alarmes que o notificam ou que realizam ações quando uma métrica especificada atinge um limite especificado. Por exemplo, você pode CloudWatch rastrear o uso da CPU ou outras métricas para suas instâncias do Amazon EC2 e iniciar automaticamente novas instâncias quando necessário. Para obter mais informações, consulte o [Guia CloudWatch do usuário da Amazon](#).
- O Amazon CloudWatch Logs permite monitorar, armazenar e acessar seus arquivos de log a partir de instâncias do Amazon EC2 e de outras fontes. CloudTrail CloudWatch Os registros podem monitorar as informações nos arquivos de log e notificá-lo quando determinados limites forem atingidos. É possível também arquivar seus dados de log em armazenamento resiliente. Para obter mais informações, consulte o [Guia do usuário do Amazon CloudWatch Logs](#).
- 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 um bucket do Amazon S3 que você especificar. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem a partir do qual as chamadas foram feitas e quando elas ocorreram. Para obter mais informações, consulte o [AWS CloudTrail Guia do Usuário](#).

## Tópicos

- [Monitorando a Amazon WorkSpaces Web com a Amazon CloudWatch](#)
- [Log de chamadas de API do Amazon WorkSpaces Web usando o AWS CloudTrail](#)
- [Registro em log do acesso do usuário](#)

## Monitorando a Amazon WorkSpaces Web com a Amazon CloudWatch

Você pode monitorar o Amazon WorkSpaces Web usando CloudWatch, que coleta dados brutos e os processa em métricas legíveis, quase em tempo real. Essas estatísticas são mantidas por 15

meses, de maneira que você possa acessar informações históricas e ter uma perspectiva melhor de como o aplicativo web ou o serviço está se saindo. Você também pode definir alarmes que observam determinados limites e enviam notificações ou realizam ações quando esses limites são atingidos. Para obter mais informações, consulte o [Guia CloudWatch do usuário da Amazon](#).

O namespace `AWS/WorkSpacesWeb` inclui as métricas a seguir.

#### CloudWatch métricas para Amazon WorkSpaces Web

Métrica	Descrição	Dimensões	Estatísticas	Unidades
<code>SessionAttempt</code>	O número de tentativas de sessões WorkSpaces da Amazon Web.	<code>PortalId</code>	Média, Soma, Máximo, Mínimo	Contagem
<code>SessionSuccess</code>	O número de sessões bem-sucedidas WorkSpaces da Amazon Web começa.	<code>PortalId</code>	Média, Soma, Máximo, Mínimo	Contagem
<code>SessionFailure</code>	O número de sessões fracassadas WorkSpaces da Amazon Web iniciadas.	<code>PortalId</code>	Média, Soma, Máximo, Mínimo	Contagem
<code>GlobalCpuPercent</code>	O uso da CPU da instância de sessão WorkSpaces da Amazon Web.	<code>PortalId</code>	Média, Soma, Máximo, Mínimo	Percentual
<code>GlobalMemoryPercent</code>	O uso da memória (RAM)	<code>PortalId</code>	Média, Soma, Máximo, Mínimo	Percentual

Métrica	Descrição	Dimensões	Estatísticas	Unidades
	da instância de sessão WorkSpaces da Amazon Web.			

### Note

Você pode visualizar a estatística métrica “SampleCount” `GlobalMemoryPercent` para `GlobalCpuPercent` ou determinar o número de sessões simultâneas ativas no seu portal. Os pontos de dados são emitidos por cada sessão uma vez por minuto.

## Log de chamadas de API do Amazon WorkSpaces Web usando o AWS CloudTrail

O Amazon WorkSpaces Web é integrado ao AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, um perfil ou um serviço da AWS no Amazon WorkSpaces Web. O CloudTrail captura todas as chamadas de API para o Amazon WorkSpaces Web como eventos. Isso inclui as chamadas do console do Amazon WorkSpaces Web e as chamadas de código para as operações da API do Amazon WorkSpaces Web. Se você criar uma trilha, poderá habilitar a entrega contínua de eventos do CloudTrail para um bucket do Amazon S3, incluindo eventos para o Amazon WorkSpaces Web. Se você não configurar uma trilha, ainda poderá visualizar os eventos mais recentes no console do CloudTrail em Event history (Histórico de eventos). Usando as informações coletadas pelo CloudTrail, é possível identificar a solicitação feita ao Amazon WorkSpaces Web, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita, bem como detalhes adicionais.

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

### Informações do Amazon WorkSpaces Web no CloudTrail

O CloudTrail é habilitado em sua conta da AWS quando ela é criada. Quando ocorre uma atividade no Amazon WorkSpaces Web, ela é registrada em um evento do CloudTrail junto com outros eventos de serviço da AWS no Histórico de eventos. Em Histórico de eventos, é possível visualizar, pesquisar e baixar eventos recentes em sua conta da AWS. Para obter mais informações, consulte

[Viewing events with CloudTrail Event history](#) (Como visualizar eventos com o histórico de eventos do CloudTrail).

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

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

Todas as ações do Amazon WorkSpaces Web são registradas pelo CloudTrail e documentadas na Referência de API do Amazon WorkSpaces Web. Por exemplo, as chamadas para as ações `CreatePortal`, `DeleteUserSettings` e `ListBrowserSettings` geram entradas nos arquivos de log do CloudTrail.

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

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

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

## Noções básicas sobre entradas de arquivos de log do Amazon WorkSpaces Web

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log a um bucket do Amazon S3 especificado. Os arquivos de log do CloudTrail contêm uma ou mais entradas de log.

Um evento representa uma única solicitação de qualquer origem e inclui informações sobre a ação solicitada, a data e a hora da ação, os parâmetros de solicitação e outros detalhes. Os arquivos de log do CloudTrail não são um rastreamento de pilha ordenada de chamadas de API pública. Dessa forma, eles não são exibidos em uma ordem específica.

O exemplo a seguir mostra uma entrada de log do CloudTrail que demonstra a ação `ListBrowserSettings`.

```
{
  "Records": [{
    "eventVersion": "1.08",
    "userIdentity": {
      "type": "IAMUser",
      "principalId": "111122223333",
      "arn": "arn:aws:iam::111122223333:user/myUserName",
      "accountId": "111122223333",
      "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
      "userName": "myUserName"
    },
    "eventTime": "2021-11-17T23:44:51Z",
    "eventSource": "workspaces-web.amazonaws.com",
    "eventName": "ListBrowserSettings",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "127.0.0.1",
    "userAgent": "[]",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "159d5c4f-c8c8-41f1-9aee-b5b1b632e8b2",
    "eventID": "d8237248-0090-4c1e-b8f0-a6e8b18d63cb",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
  },
  {
    "eventVersion": "1.08",
    "userIdentity": {
      "type": "IAMUser",
      "principalId": "111122223333",
      "arn": "arn:aws:iam::111122223333:user/myUserName",
      "accountId": "111122223333",
```

```
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "myUserName"
  },
  "eventTime": "2021-11-17T23:55:51Z",
  "eventSource": "workspaces-web.amazonaws.com",
  "eventName": "CreateUserSettings",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "5127.0.0.1",
  "userAgent": "[]",
  "requestParameters": {
    "clientToken": "some-token",
    "copyAllowed": "Enabled",
    "downloadAllowed": "Enabled",
    "pasteAllowed": "Enabled",
    "printAllowed": "Enabled",
    "uploadAllowed": "Enabled"
  },
  "responseElements": "arn:aws:workspaces-web:us-
west-2:111122223333:userSettings/04a35a2d-f7f9-4b22-af08-8ec72da9c2e2",
  "requestID": "6a4aa162-7c1b-4cf9-a7ac-e0c8c4622117",
  "eventID": "56f1fbee-6a1d-4fc6-bf35-a3a71f016fcb",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "111122223333",
  "eventCategory": "Management"
}]
}
```

## Registro em log do acesso do usuário

A Amazon WorkSpaces Web permite que os clientes registrem eventos da sessão, incluindo visitas de início, parada e URL. Esses logs são entregues a um Amazon Kinesis Data Stream que você especifica para o seu portal da web. Para ter mais informações, consulte [the section called “Configurar o registro de acesso do usuário”](#).



# Orientação para usuários WorkSpaces da Amazon Web

Os administradores usam a Amazon WorkSpaces Web para criar portais web que se conectam aos sites da empresa, como sites internos, aplicativos web software-as-a-service (SAAS) ou à Internet. Os usuários finais usam os navegadores da web existentes para acessar esses portais da web a fim de iniciar uma sessão e acessar o conteúdo.

O conteúdo a seguir ajuda a orientar os usuários finais que desejam saber mais sobre como acessar a Amazon WorkSpaces Web, iniciar e configurar uma sessão e usar a barra de ferramentas e o navegador da web.

## Tópicos

- [Compatibilidade de navegadores e dispositivos](#)
- [Acesso ao portal da web](#)
- [Orientação da sessão](#)
- [Solução de problemas](#)
- [Extensão de autenticação única](#)

## Compatibilidade de navegadores e dispositivos

O Amazon WorkSpaces Web é alimentado pelo cliente de navegador NICE DCV, que é executado dentro de um navegador da web, portanto, nenhuma instalação é necessária. O cliente do navegador da web é compatível com navegadores comuns, como Chrome e Firefox, e com os principais sistemas operacionais de desktop, como Windows, macOS e Linux.

Para up-to-date obter mais detalhes sobre o suporte ao cliente do navegador da Web, consulte [Cliente do navegador da Web](#).

### Note

Atualmente, o suporte para webcam está disponível apenas em navegadores baseados em Chromium, como Google Chrome e Microsoft Edge. Atualmente, o Apple Safari e o Mozilla FireFox não suportam webcam.

## Acesso ao portal da web

Seu administrador pode fornecer acesso ao portal da web com as seguintes opções:

- Você pode selecionar um link de um e-mail ou site e entrar com suas credenciais de identidade SAML.
- É possível entrar no seu provedor de identidade SAML (como Okta, Ping ou Azure) e iniciar uma sessão com um clique na página inicial da aplicação do provedor de SAML (como o Painel do Usuário Final do Okta ou o portal Myapps do Azure).

## Orientação da sessão

Depois de entrar no portal da web, você pode iniciar uma sessão e realizar várias ações durante sua sessão.

Tópicos

- [Iniciar uma sessão](#)
- [Usar a barra de ferramentas](#)
- [Usar o navegador](#)
- [Encerrar uma sessão](#)

## Iniciar uma sessão

Depois de entrar para iniciar uma sessão, você verá a mensagem de Inicialização da sessão e a barra de progresso. Isso indica que a Amazon WorkSpaces Web está criando uma sessão para você. Nos bastidores, a Amazon WorkSpaces Web está criando a instância, iniciando o navegador gerenciado e aplicando as configurações do administrador e as políticas do navegador.

Se essa é a primeira vez que você faz login no portal da web, você verá ícones azuis + na barra de ferramentas. Esse ícone indica que um tutorial está disponível, que orientará os recursos disponíveis na barra de ferramentas. Você pode usar esses ícones para aprender a:

- Conceder permissões do navegador para o microfone, a webcam e a área de transferência selecionando o ícone de cadeado ao lado do navegador local e configurando o botão para Ativado ao lado da área de transferência, do microfone e da câmera.

**Note**

Quando você habilita as permissões da webcam no início da primeira sessão, a webcam é ativada brevemente e uma luz no computador pisca. Isso concede acesso do navegador local à sua webcam.

- Permita que a Amazon WorkSpaces Web abra janelas de monitor adicionais, selecionando o ícone de cadeado no seu navegador e a configuração Sempre permitir pop-ups.

Se quiser reiniciar um tutorial, você pode escolher Perfil na barra de ferramentas, Ajuda e Iniciar tutorial.










## Usar a barra de ferramentas

Para mover a barra de ferramentas, selecione a barra mais clara na parte superior da barra de ferramentas, arraste-a até o local desejado e solte-a.

Para contrair a barra de ferramentas, passe o mouse sobre ela e selecione o botão de seta para cima ou clique duas vezes na barra mais clara na seção superior. A visualização reduzida fornece mais espaço na tela e acesso com um clique aos ícones mais usados.

Para encaixar a barra de ferramentas na parte superior da tela, escolha Preferências, Geral e Encaixado no modo Barra de ferramentas.

A tabela a seguir inclui uma descrição de todos os ícones disponíveis na barra de ferramentas:

Icon	Title	Description
	<b>Windows</b>	Move between windows or launch additional browser windows.
	<b>Launch additional monitor window</b>	Launch an additional monitor window with a separate browser window. Then drag to your secondary monitor.
	<b>Full screen</b>	Launch a full screen experience view.
	<b>Microphone</b>	Activate mic input for the session.
	<b>Preferences</b>	Access the <b>General</b> and <b>Keyboard</b> menus. From the <b>General</b> menu, toggle between light and dark mode, activate the keyboard input selector (for changing the keyboard language), and switch between streaming mode or display resolution. From the <b>Keyboard</b> menu, change the option and command key settings (on Mac devices), or activate <b>Functions</b> (see below).
	<b>Profile</b>	<p>End your session, view performance metrics, access <b>Feedback</b> and <b>Help</b>, and learn about Amazon WorkSpaces Web. <b>End Session</b> ends the Amazon WorkSpaces Web session.</p> <p><b>Performance metrics</b> displays the frame rate, network latency, and bandwidth usage graph. This information is useful for administrators when investigating issues with the service.</p> <p><b>Feedback</b> provides you with an email address to share feedback to the Amazon WorkSpaces Web team.</p> <p><b>Help</b> provides you with access to Frequently Asked Questions, such as how to use the clipboard, microphone, and webcam during the session, or how to troubleshoot launching an additional monitor window. From help, you can also launch the tutorial or user guide.</p> <p><b>About</b> provides more information about Amazon WorkSpaces Web.</p>
	<b>Notifications</b>	Get one-click access to session notifications.
	<b>Clipboard</b>	Access clipboard shortcut descriptions, links to set the command key preference, and troubleshoot clipboard permissions from the local web browser. You can use the content preview text box to test clipboard functionality. This icon only displays if clipboard permission is granted by your administrator.
	<b>Files</b>	From the files menu, you can upload content to the remote browser. Once uploaded, you can rename, download, or delete, as well as create folders in the temporary file menu. All files and data in <b>Files</b> are deleted at the end of the session. This icon only displays if <b>Files</b> permission is granted by your administrator.

**Note**

Os ícones da Área de transferência e Arquivos ficam ocultos por padrão, a menos que o administrador conceda essas permissões. Somente administradores podem habilitar ou desabilitar a área de transferência e os arquivos em um portal da web. Se esses ícones estiverem ocultos e você precisar acessá-los, entre em contato com o administrador.

## Usar o navegador

Quando você inicia sua sessão, o navegador exibe o URL de inicialização, que é um URL escolhido pelo administrador. Se o administrador não tiver escolhido um URL de inicialização, você verá a experiência padrão da nova guia do Google Chrome.

No navegador, é possível abrir guias, abrir janelas adicionais do navegador (no ícone da barra de ferramentas do Windows ou no menu de três pontos do navegador), inserir um URL ou pesquisar na barra de URL ou acessar sites a partir dos favoritos gerenciados. Para acessar os favoritos do portal da web, abra a pasta Marcadores gerenciados na barra de favoritos (abaixo da barra de URL) ou abra o gerenciador de favoritos no menu de três pontos no lado direito da barra de URL.

Para redimensionar ou mover a janela do navegador, arraste para baixo a barra de guias do Chrome. Essa ação libera mais espaço na tela para várias janelas do navegador durante a sessão.

**Note**

Os recursos do navegador, como o modo de navegação anônima, podem não estar disponíveis durante a sessão se o administrador os tiver desativado.

## Encerrar uma sessão

Para encerrar uma sessão, escolha Perfil e Encerrar sessão. Após o término de uma sessão, a Amazon WorkSpaces Web exclui todos os dados da sessão. Nenhum dado do navegador, como sites abertos ou histórico, ou arquivos ou dados do Explorador de Arquivos, fica disponível após o término da sessão.

Se você fechar uma guia durante uma sessão ativa, a sessão será encerrada após um período definido pelo administrador. Se você fechar a guia e revisitar o portal da web antes que esse tempo

limite entre em vigor, poderá ingressar na sessão atual e ver todos os dados da sessão anterior, como sites e arquivos abertos.

## Solução de problemas

Meu portal WorkSpaces da Amazon Web não permite que eu faça login. Recebi uma mensagem de erro que diz “Seu portal da web ainda não está configurado. Entre em contato com o administrador para obter ajuda.”

Seu administrador precisa concluir a criação do portal com um provedor de identidade SAML 2.0 para permitir que você faça login. Entre em contato com o administrador para obter ajuda.

Meu portal não inicia uma sessão. Recebi uma mensagem de erro que diz “Falha ao reservar a sessão. Ocorreu um erro interno. Tente novamente.”

Ocorreu um problema com a inicialização da sessão do portal da web. Tente inicializar a sessão novamente. Se isso continuar, entre em contato com seu administrador para obter ajuda.

Não consigo usar a área de transferência, o microfone ou a webcam.

Para permitir permissões do navegador, selecione o ícone de cadeado ao lado do URL e alterne o botão azul ao lado de Área de transferência, Microfone, Câmera e Pop-ups e redirecionamentos para ativar esses recursos.

### Note

Se o navegador não permitir entrada de vídeo ou áudio, essas opções não aparecerão na barra de ferramentas.

O áudio e vídeo (AV) em tempo real WorkSpaces da Amazon Web redireciona o vídeo da webcam local e a entrada de áudio do microfone para a sessão de streaming do navegador. Dessa forma, você pode usar seus dispositivos locais para videoconferência e audioconferência em sua sessão de streaming com navegadores da web baseados em Chromium, como o Google Chrome ou o Microsoft Edge. Atualmente, a webcam não é compatível com navegadores que não sejam Chromium.

Para obter informações sobre como configurar o Google Chrome, consulte [Usar a câmera e o microfone](#).

Meu portal da web não abre uma janela de monitor adicional.

Se você tentar iniciar dois monitores e ver um ícone de Pop-ups bloqueados no final da barra de endereço no navegador superior, selecione o ícone e o botão de opções ao lado de Sempre permitir pop-ups e redirecionamentos. Com os pop-ups permitidos, selecione o ícone de Monitor duplo na barra de ferramentas para abrir uma nova janela, reposicionar a janela no monitor e arrastar uma guia do navegador até a janela.

Quando tento baixar arquivos do painel Arquivos, nada acontece.

Se você tentar baixar arquivos do painel Arquivos e ver um ícone de Pop-ups bloqueados no final da barra de endereço no navegador superior, selecione o ícone e o botão de opção ao lado de Sempre permitir pop-ups e redirecionamentos. Com os pop-ups permitidos, tente baixar os arquivos novamente.

## Extensão de autenticação única

A Amazon WorkSpaces Web oferece uma extensão para login único com os navegadores Chrome e Firefox em computadores desktop. Se o administrador tiver habilitado a extensão, o portal da web solicitará que você instale a extensão ao fazer login.

A Amazon WorkSpaces Web criou a extensão para permitir o login único em sites durante sua sessão. Por exemplo, se você entrar no seu portal da web com um provedor de identidade SAML 2.0 (como Okta ou Ping) e acessar um site durante a sessão que usa o mesmo provedor de identidade, a extensão pode facilitar o acesso ao site removendo solicitações adicionais de login.

Não é necessário instalar a extensão para acessar seu portal da web, mas ela pode melhorar sua experiência ao reduzir o número de vezes que você precisa digitar o nome de usuário e senha.

Quando você faz login, a extensão localiza os cookies que seu administrador listou para sua sessão. Todos os dados que a extensão localiza são criptografados em repouso e durante o trânsito. Nenhum desses dados é armazenado no navegador local. Quando você encerra sua sessão, todos os dados da sessão (como guias abertas, arquivos baixados e cookies entregues ou criados durante a sessão) são excluídos.

## Compatibilidade

A extensão funciona com os seguintes dispositivos:

- Notebooks
- Computadores desktop

A extensão funciona com os seguintes navegadores:

- Chrome
- Firefox

## Instalação

Ao fazer login no portal, siga as instruções para instalar a extensão para seu navegador Chrome ou Firefox na loja virtual do navegador. Você só precisa fazer isso uma vez para cada navegador da web.

Se você trocar de dispositivo, alternar para um navegador diferente no mesmo dispositivo ou excluir a extensão do navegador local, verá uma solicitação para instalar a extensão ao iniciar a próxima sessão.

Para garantir que a extensão funcione conforme o esperado, use a extensão em uma guia de navegação normal, em vez de navegação anônima (Chrome) ou navegação privada (Firefox).

## Solução de problemas

Se você tiver a extensão instalada, mas ainda for solicitado que você faça login durante a sessão, siga estas etapas:

1. Certifique-se de ter a extensão Amazon WorkSpaces Web instalada em seu navegador. Se você excluiu os dados do navegador, talvez tenha removido a extensão acidentalmente.
2. Verifique se você não está navegando de forma anônima (Chrome) ou privada (Firefox). Esses modos podem causar problemas com extensões.
3. Se o problema persistir, entre em contato com o administrador do portal para obter ajuda adicional.



# Histórico de documentos do Amazon WorkSpaces Web User Guide

A tabela a seguir descreve os lançamentos da documentação WorkSpaces da Amazon Web.

Alteração	Descrição	Data
<a href="#">CloudWatch métricas</a>	Adicionado GlobalCpuPercent e GlobalMemoryPercent métricas.	26 de fevereiro de 2024
<a href="#">Configurar a filtragem de URL</a>	Você pode usar a Política do Chrome para filtrar quais URLs os usuários podem acessar a partir do navegador remoto.	21 de fevereiro de 2024
<a href="#">Tipos de autenticação IdP</a>	Você pode escolher o tipo de autenticação padrão ou o do IAM Identity Center.	5 de fevereiro de 2024
<a href="#">Habilitar extensão de autenticação única</a>	É possível habilitar uma extensão para que os usuários finais tenham uma melhor experiência de login no portal.	28 de agosto de 2023
<a href="#">Orientação para o usuário da Amazon WorkSpaces Web</a>	Conteúdo adicionado para ajudar a orientar os usuários finais que desejam saber mais sobre como acessar a Amazon WorkSpaces Web, iniciar e configurar uma sessão e usar a barra de ferramentas e o navegador da web.	17 de julho de 2023

<a href="#">Controles de acesso de IP</a>	WorkSpaces A Web permite que você controle de quais endereços IP seu portal da web pode ser acessado.	31 de maio de 2023
<a href="#">Atualização da política gerenciada</a>	Política AmazonWorkSpacesWebReadOnly gerenciada atualizada	15 de maio de 2023
<a href="#">Configurar a atualização do provedor de identidades</a>	WorkSpaces A Web oferece dois tipos de autenticação: padrão e AWS IAM Identity Center	15 de março de 2023
<a href="#">Atualização da política do navegador</a>	Seção de política do navegador atualizada e reestruturada	31 de janeiro de 2023
<a href="#">Atualização da política gerenciada</a>	Política AmazonWorkSpacesWebServiceRolePolicy gerenciada atualizada	15 de dezembro de 2022
<a href="#">Lista de permissões e lista de bloqueio</a>	Especifique a Lista de permissões e a Lista de bloqueios para especificar uma lista de domínios que seus usuários podem ou não acessar.	14 de novembro de 2022
<a href="#">Atualização da política gerenciada</a>	Política AmazonWorkSpacesWebReadOnly gerenciada atualizada	2 de novembro de 2022
<a href="#">Atualização da política gerenciada</a>	Política AmazonWorkSpacesWebServiceRolePolicy gerenciada atualizada	24 de outubro de 2022

<a href="#">Registro em log do acesso do usuário</a>	Configurar o registro em log de acesso do usuário para registrar eventos do usuário	17 de outubro de 2022
<a href="#">Atualizações de rede</a>	Várias atualizações na seção “Redes e acesso”	22 de setembro de 2022
<a href="#">Atualização da política gerenciada</a>	Política AmazonWorkSpacesWebServiceRolePolicy gerenciada atualizada	6 de setembro de 2022
<a href="#">Configurar sessões do usuário</a>	Configurar o Input Method Editor (IME) e a localização na sessão	28 de julho de 2022
<a href="#">Atualizações de rede</a>	Várias atualizações na seção “Redes e acesso”	7 de julho de 2022
<a href="#">Valores de tempo limite</a>	Especifique o Tempo limite de desconexão em minutos e o Tempo limite de desconexão de inatividade em minutos	16 de maio de 2022
<a href="#">Política gerenciada atualizada</a>	Atualizou a política AmazonWorkSpacesWebServiceRolePolicy gerenciada para adicionar o namespace AWS/Usage às permissões da API PutMetricData	6 de abril de 2022
<a href="#">Perfil vinculado ao serviço</a>	Nova função AWSServiceRoleForAmazonWorkSpacesWeb vinculada ao serviço	30 de novembro de 2021

---

<a href="#">Política gerenciada</a>	Nova política AmazonWorkSpacesWebReadOnly gerenciada	30 de novembro de 2021
<a href="#">Política gerenciada</a>	Nova política AmazonWorkSpacesWebServiceRolePolicy gerenciada	30 de novembro de 2021
<a href="#">Lançamento inicial</a>	Versão inicial do Guia de Administração WorkSpaces da Web	30 de novembro de 2021

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.