aws

Guia de administração

# WorkSpaces Navegador Amazon Secure

# WorkSpaces Navegador Amazon Secure: Guia de administração

# Table of Contents

# O que é o Amazon WorkSpaces Secure Browser?

> **Note**
>
> O Amazon WorkSpaces Secure Browser era conhecido anteriormente como Amazon WorkSpaces Web.

O Amazon WorkSpaces Secure Browser é um serviço de navegador hospedado, totalmente gerenciado e nativo da nuvem, usado para acessar com segurança sites privados e aplicativos web ( software-as-a-service SaaS), interagir com recursos on-line e navegar na Internet a partir de um contêiner descartável. WorkSpaces O Secure Browser funciona com os navegadores da Web existentes do usuário, sem sobrecarregar a TI com o gerenciamento de dispositivos, infraestrutura, software cliente especializado ou conexões de rede privada virtual (VPN). O conteúdo da Web é transmitido para o navegador da Web do usuário, enquanto o navegador real e o conteúdo da Web são isolados em AWS. Ao usar as mesmas tecnologias subjacentes que impulsionam os serviços de computação do usuário AWS final, como Amazon WorkSpaces e Amazon AppStream 2.0, o WorkSpaces Secure Browser pode ser mais econômico do que os desktops virtuais tradicionais e reduzir a complexidade em comparação com o fornecimento de software de gerenciamento aos dispositivos da empresa. WorkSpaces O Secure Browser reduz o risco de exfiltração de dados ao transmitir conteúdo da web. Nenhum HTML, modelo de objeto de documento (DOM) ou dados confidenciais da empresa são transmitidos para a máquina local. Ao isolar o dispositivo, a rede corporativa e a Internet um do outro, a superfície de ataque do navegador é praticamente eliminada.

Você pode aplicar a política do navegador corporativo (incluindo permissão/bloqueio de URL) em todas as sessões e incluir controles em nível de sessão para área de transferência, transferência de arquivos e impressora. Você também pode restringir o acesso a redes ou dispositivos confiáveis usando controles de acesso IP. WorkSpaces O Secure Browser é fácil de configurar e operar. Cada sessão é iniciada com uma versão nova e totalmente corrigida do navegador Chrome, com políticas e configurações da empresa aplicadas.

## Histórico de versões

Em 20 de maio de 2024, a Amazon WorkSpaces Web foi renomeada para Amazon WorkSpaces Secure Browser. Para os clientes existentes, não houve mudança na forma como eles gerenciam usuários ou recursos com o serviço. A lista a seguir descreve as atualizações aplicáveis que também ocorreram como resultado dessa renomeação.

O namespace da API workspaces-web permanece inalterado em termos de compatibilidade com versões anteriores. Como resultado, os seguintes recursos ainda são os mesmos:

- Comandos da CLI.
- CloudWatch Métricas da Amazon. Para ter mais informações, consulte the section called “Monitoramento com CloudWatch”.
- Pontos finais de serviço. Para obter mais informações, consulte os endpoints e cotas do Amazon WorkSpaces Secure Browser.
- AWS CloudFormation recursos. Para obter mais informações, consulte a referência do tipo de recurso do Amazon WorkSpaces Secure Browser.
- Função vinculada ao serviço contendo workspaces-web. Para ter mais informações, consulte the section called “Uso de perfis vinculadas ao serviço”.
- URLs do console contendo workspaces-web.
- URLs de documentação contendo workspaces-web. Para obter mais informações, consulte a documentação do Amazon WorkSpaces Secure Browser.
- Função ReadOnly gerenciada existente. Para ter mais informações, consulte the section called “AWS políticas gerenciadas”.
- Nome da concessão do KMS.
- Prefixo de stream do Kinesis UAL (User-Activity Logging).

Além disso, os URLs existentes do portal permanecem os mesmos. <UUID>Os URLs para portais criados antes de 20 de maio de 2024 usavam o formato .workspaces-web.com. WorkSpaces Os portais do Secure Browser continuam usando esse formato e o domínio workspaces-web.com.

# Termos a serem conhecidos ao usar o WorkSpaces Secure Browser

Para ajudá-lo a começar a usar o WorkSpaces Secure Browser, 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 Secure Browser.

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 seus usuários usem o Navegador WorkSpaces Seguro em seu IdP.

Documento de metadados do provedor de identidades (IdP)

WorkSpaces O Secure Browser exige metadados específicos do seu provedor de identidade (IdP) para estabelecer confiança. Você pode adicionar esses metadados ao WorkSpaces Secure Browser fazendo o upload de 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. WorkSpaces O Secure Browser 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.

Nuvem privada virtual (VPC)

Você pode usar uma VPC nova ou existente, sub-redes correspondentes e grupos de segurança para vincular seu conteúdo ao Secure Browser. WorkSpaces

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.

As VPCs, sub-redes e grupos de segurança listados são retirados da mesma região do console do WorkSpaces Secure Browser.

Armazenamento de confiança

Se um usuário acessando um site por meio do Navegador WorkSpaces Seguro receber um erro de privacidade, como NET: :ERR_CERT_INVALID, esse site pode 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 de um usuário exigir que você instale um certificado específico para carregar um site, você precisará adicionar esse certificado ao seu armazenamento confiável para permitir que o usuário acesse esse site no Navegador WorkSpaces Seguro.

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.

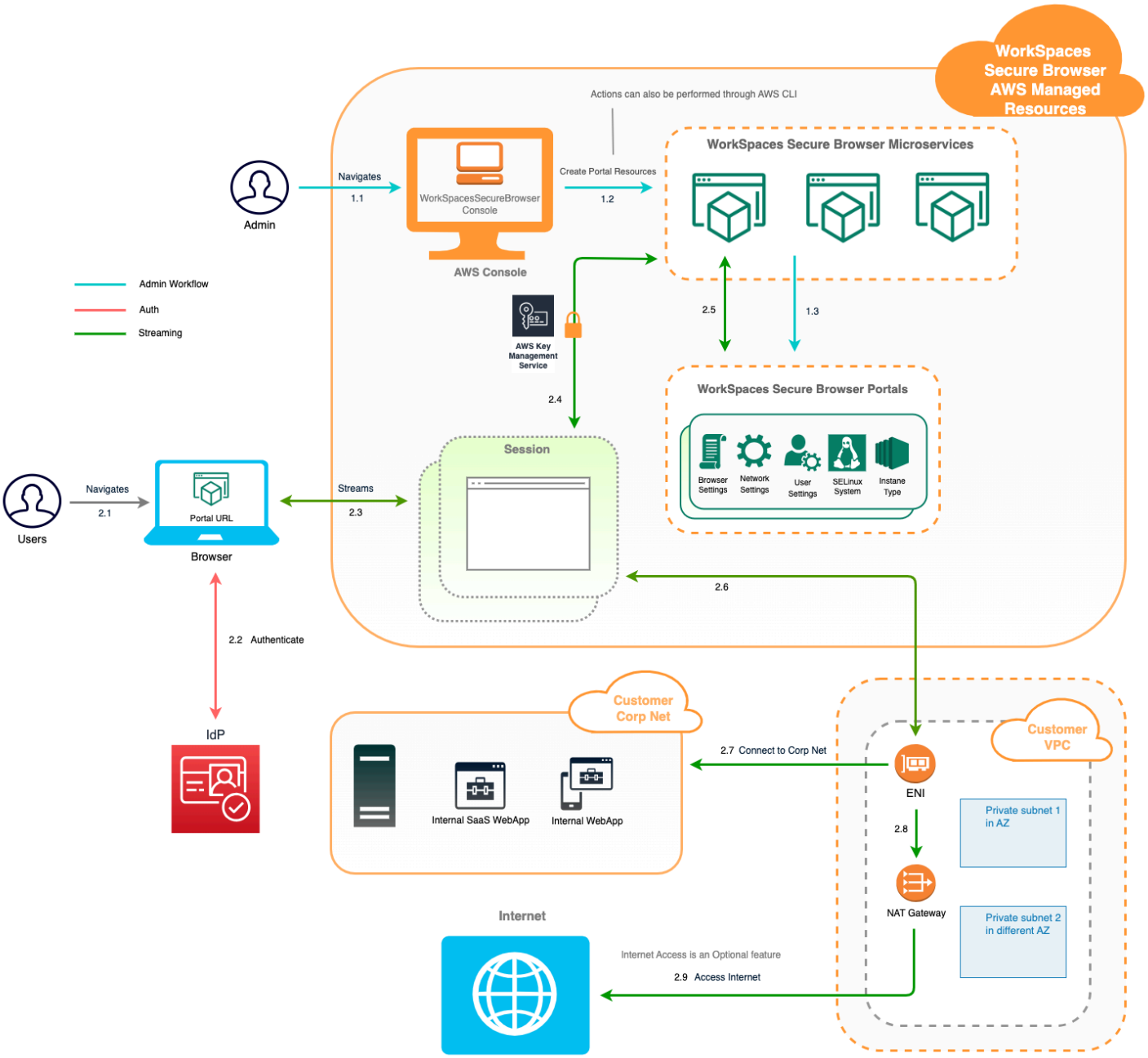
O endpoint está disponível publicamente na internet e pode ser incorporado à sua rede.

# Serviços relacionados

WorkSpaces O Secure Browser é um recurso da Amazon WorkSpaces no portfólio de computação para usuários finais da AWS. Comparado com o WorkSpaces e AppStream 2.0, o WorkSpaces Secure Browser foi desenvolvido especificamente para facilitar cargas de trabalho seguras baseadas na web. WorkSpaces O Secure Browser 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 acessar os recursos do desktop e o WorkSpaces Secure Browser para os usuários do contact center que precisam acessar apenas alguns sites internos e SaaS (incluindo aqueles hospedados fora da sua rede) em computadores desktop.

# Arquitetura

O diagrama a seguir mostra a arquitetura do WorkSpaces Secure Browser.




# Acessando o navegador WorkSpaces seguro

Os administradores acessam o WorkSpaces Secure Browser por meio do console do WorkSpaces Secure Browser, SDK, CLI ou API. Seus usuários o acessam por meio do endpoint do WorkSpaces Secure Browser.

# Configurando o WorkSpaces Navegador Seguro

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

Tópicos



## Cadastrar e criar um usuário

### Inscreva-se para um Conta da AWS

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

Para se inscrever em um Conta da AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga as instruções online.

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

   Quando você se inscreve em um Conta da AWS, um Usuário raiz da conta da AWSé criado. O usuário raiz tem acesso a todos os Serviços da AWS e atributos na conta. Como prática recomendada de segurança, atribua o acesso administrativo a um usuário e use somente o usuário-raiz para executar tarefas que exigem acesso de usuário-raiz.

AWS envia um e-mail de confirmação após a conclusão do processo de inscrição. A qualquer momento, é possível visualizar as atividades da conta atual e gerenciar sua conta acessando https://aws.amazon.com/ e selecionando Minha conta.

# Criar um usuário com acesso administrativo

Depois de se inscrever em um Conta da AWS, proteja seu Usuário raiz da conta da AWS AWS IAM Identity Center, habilite e crie um usuário administrativo para que você não use o usuário root nas tarefas diárias.

Proteja seu Usuário raiz da conta da AWS

1. Faça login AWS Management Consolecomo proprietário da conta escolhendo Usuário raiz e inserindo seu endereço de Conta da AWS e-mail. Na próxima página, insira 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. Habilite a autenticação multifator (MFA) para o usuário raiz.

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

Criar um usuário com acesso administrativo

1. Habilitar o IAM Identity Center.

   Para obter instruções, consulte Habilitar AWS IAM Identity Center no Guia do usuário do AWS IAM Identity Center .
2. No Centro de Identidade do IAM, conceda o acesso administrativo para um usuário.

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

Iniciar sessão como o usuário com acesso administrativo

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

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

Atribuir acesso a usuários adicionais

1. No Centro de Identidade do IAM, crie um conjunto de permissões que siga as práticas recomendadas de aplicação de permissões com privilégio mínimo.

   Para obter instruções, consulte Create a permission set no Guia do usuário do AWS IAM Identity Center .
2. Atribua usuários a um grupo e, em seguida, atribua o acesso de autenticação única ao grupo.

   Para obter instruções, consulte Add groups no Guia do usuário do AWS IAM Identity Center .

## Conceder acesso programático

Os usuários precisam de acesso programático se quiserem interagir com pessoas AWS fora do AWS Management Console. A forma de conceder acesso programático depende do tipo de usuário que está acessando 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<br><br>(Usuários gerenciados no Centro de Identidade do IAM) | Use credenciais temporári as para assinar solicitações programáticas para AWS SDKs ou APIs. AWS CLI AWS | Siga as instruções da interface que deseja utilizar.<br><br>• Para o AWS CLI, consulte Configurando o AWS CLI para uso AWS IAM Identity Center no Guia do AWS Command Line Interface usuário.<br>• Para AWS SDKs, ferrament as e AWS APIs, consulte a autenticação do IAM Identity Center no Guia de referência de AWS SDKs e ferramentas. |

| Qual usuário precisa de acesso programático? | Para | Por |
| --- | --- | --- |
| IAM | Use credenciais temporári as para assinar solicitações programáticas para AWS SDKs ou APIs. AWS CLI AWS | Siga as instruções em Como usar credenciais temporárias com AWS recursos no Guia do usuário do IAM. |
| IAM | (Não recomendado) Use credenciais de longo prazo para assinar solicitaç ões programáticas para AWS SDKs AWS CLI ou APIs. AWS | Siga as instruções da interface que deseja utilizar.<br>• Para isso AWS CLI, consulte Autenticação usando credenciais de usuário do IAM no Guia do AWS Command Line Interface usuário.<br>• Para AWS SDKs e ferramentas, consulte Autenticar usando credencia is de longo prazo no Guia de referência de AWS SDKs e ferramentas.<br>• Para AWS APIs, consulte Gerenciamento de chaves de acesso para usuários do IAM no Guia do usuário do IAM. |

# Redes e acesso

Os tópicos a seguir explicam como configurar instâncias de streaming do WorkSpaces Secure Browser para que os usuários possam se conectar a elas. Também explica como habilitar suas instâncias de streaming do WorkSpaces Secure Browser para acessar recursos de VPC, bem como a Internet.

Tópicos



## Requisitos da VPC

Durante a criação do portal do WorkSpaces Secure Browser, 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 locação padrão. VPCs com locação 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 do Navegador WorkSpaces Seguro. 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 o WorkSpaces Secure Browser.

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 O Secure Browser não atribui nenhum endereço IP público às instâncias de streaming para permitir o acesso à Internet. Essa ação tornaria suas instâncias de streaming acessíveis pela internet. Portanto, as instâncias de streaming conectadas à sub-rede pública não terão acesso à internet. Se você quiser que seu portal do WorkSpaces Secure Browser tenha acesso tanto ao conteúdo público da Internet quanto 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 região de navegador WorkSpaces seguro. 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 Secure Browser 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 Secure Browser 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. Entrada ***Region*** .s3, em que *Region* é a entrada em Região da AWS que você está criando sua VPC.
  3. Em Subnet (Sub-rede), escolha Private subnet (Sub-rede privada).
  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 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 Secure Browser 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 confirmar se as seguintes informações estão corretas 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 Secure Browser 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 (lápis) 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 Internet (identificado por igw-ID) criado pelo assistente da VPC. |

5. No painel de navegação, escolha Sub-redes. Depois, selecione a primeira sub-rede privada que você criou (por exemplo, **`WorkSpaces Secure Browser Private Subnet1`**).
6. Na guia Tabela de rotas, escolha o ID da tabela de rotas.
7. 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.
8. 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 |

| Destination (Destino) | Destino | Descrição |
| --- | --- | --- |
| | | 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). |

9. No painel de navegação, escolha Sub-redes. Depois, selecione a segunda sub-rede privada que você criou (por exemplo, **`WorkSpaces Secure Browser 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 ao WorkSpaces Secure Browser acesso 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 do WorkSpaces Secure Browser 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 portal do WorkSpaces Secure Browser.

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 do WorkSpaces Secure Browser 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 do Navegador WorkSpaces Seguro 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 o Navegador WorkSpaces Seguro, 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 o WorkSpaces Secure Browser.

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

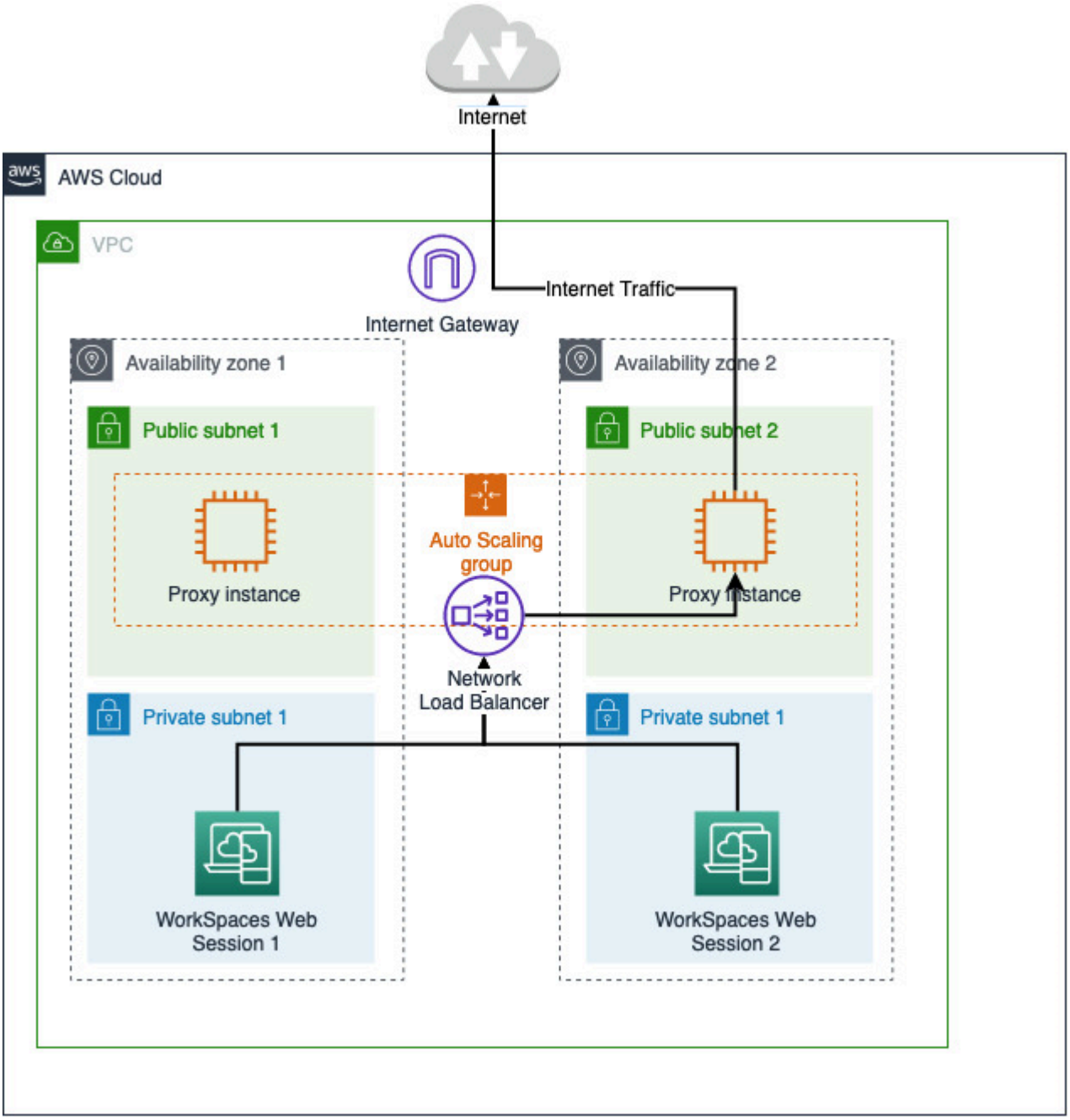
navegador WorkSpaces Secure Browser para configurar o portal do WorkSpaces Secure Browser para se conectar ao endpoint do proxy. Para obter mais informações, consulte Como configurar um proxy VPC de saída com lista branca de domínio e filtragem de conteúdo.

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 do WorkSpaces Secure Browser 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 do WorkSpaces Secure Browser 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 do WorkSpaces Secure Browser.




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 estão as sessões do WorkSpaces Secure Browser (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 o WorkSpaces Secure Browser

Para configurar um proxy de saída HTTP para o WorkSpaces Secure Browser, 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 OutboundProxyDomínio e OutboundProxyPorta. 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. No console do Navegador WorkSpaces Seguro, 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. Na sua sessão do Navegador WorkSpaces Seguro, 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 do WorkSpaces Secure Browser 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 do Navegador WorkSpaces Seguro 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 do WorkSpaces Secure Browser está localizado. 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 do Navegador WorkSpaces seguro, use o Chrome para navegar até chrome: //policy e certifique-se de que a ProxySettings política seja 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 as cotas do serviço WorkSpaces Secure Browser (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 as cotas padrão do WorkSpaces Secure Browser, consultethe section called “Gerencie cotas de serviço para seu portal”.

- 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 do WorkSpaces Secure Browser requer sua própria interface de elastic network durante a duração do streaming. WorkSpaces O Secure Browser 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 manter o limite de ENI igual ou superior ao limite máximo de uso simultâneo configurado para seu portal da web.

### Subredes

- Ao desenvolver seu plano para aumentar a escala de usuários, lembre-se de que cada sessão do WorkSpaces Secure Browser 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 define o número de usuários que podem fazer streaming de maneira simultânea.
- 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 o WorkSpaces Secure Browser suporta 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 do WorkSpaces Secure Browser e os recursos de rede exigidos pelos aplicativos 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 o WorkSpaces Secure Browser, as sub-redes da VPC devem residir em diferentes zonas de disponibilidade na região em que você está iniciando o Secure Browser. 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, `use1-az2` é uma ID AZ para a `us-east-1` região e tem a mesma localização em todas as AWS contas.

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

WorkSpaces O Navegador Seguro está disponível em um subconjunto das zonas de disponibilidade para cada região compatível. A tabela a seguir lista os IDs de AZ que você pode usar para cada região. Para ver o mapeamento de IDs de AZ para zonas de disponibilidade em sua conta, consulte IDs de AZ para seus recursos no Guia do usuário do AWS RAM .

| Nome da região | Código da região | IDs de AZ compatíveis |
|---|---|---|
| Leste dos EUA (Norte da Virgínia) | us-east-1 | use1-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 Zonas Locais no Guia do usuário do Amazon EC2.

# Conexão de VPC

Cada instância de streaming do WorkSpaces Secure Browser 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 O Secure Browser está configurado 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 o WorkSpaces Secure Browser exige 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 o WorkSpaces Secure Browser.

Tópicos

## Requisitos de endereço IP e porta

Para acessar as instâncias do WorkSpaces Secure Browser, os dispositivos do usuário precisam de 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 os usuários possam acessar portais da Web a partir do navegador local, você deve adicionar os seguintes domínios à lista de permissões na rede a partir da qual o usuário está tentando acessar o serviço.

Na tabela a seguir, substitua *{region}* pelo código da região do portal web operacional. Por exemplo, s3. *{region}* .amazonaws.com deve ser s3.eu-west-1.amazonaws.com para um portal da web na região da Europa (Irlanda). Para obter uma lista de códigos de região, consulte os endpoints e cotas do Amazon WorkSpaces Secure Browser.

| Categoria | Domínio ou endereço IP |
| --- | --- |
| WorkSpaces Recursos de streaming do Secure Browser | s3.*{região}*.amazonaws.com<br>s3.amazonaws.com<br>appstream2.*{região}*.aws.amazon.com<br>*.amazonappstream.com<br>*.shortbread.aws.dev |
| WorkSpaces Recursos estáticos do Secure Browser | *.workspaces-web.com<br>di5ry4hb4263e.cloudfront.net |
| WorkSpaces Autenticação de navegador seguro | *.auth.*{região}*.amazoncognito.com<br>cognito-identity.*{região}*.amazonaws.com<br>cognito-idp.*{região}*.amazonaws.com<br>*.cloudfront.net |
| WorkSpaces Métricas e relatórios do Secure Browser | *.execute-api.*{região}*.amazonaws.com<br>unagi-na.amazon.com |

Dependendo do provedor de identidade configurado, talvez seja preciso incluir domínios adicionais à lista de permissões. Revise a documentação do seu IdP para identificar quais domínios você precisa permitir na lista para que o WorkSpaces Secure Browser use esse provedor. Se você estiver usando o Centro de Identidade do IAM, consulte IAM Identity Center prerequisites para obter mais informações.

# Introdução ao WorkSpaces Secure Browser

Siga estas etapas para criar um portal web do WorkSpaces Secure Browser 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 O Secure Browser 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 o WorkSpaces Navegador Seguro.

Tópicos



## Etapa 1: criar um portal da web

Siga estas etapas para criar um portal da web.

Tópicos



## Definir configurações de rede

1. Abra o console do WorkSpaces Secure Browser em https://console.aws.amazon.com/workspaces-web/home.
2. Escolha Navegador WorkSpaces seguro, depois Portais da Web e, em seguida, 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 o WorkSpaces Secure Browser.
    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 Tipo de instância, selecione o tipo de instância para seu portal da web no menu suspenso. Em seguida, insira seu limite máximo de usuários simultâneos para o portal da web. Para ter mais informações, consulte the section called “Gerencie cotas de serviço para seu portal”.

> **Note**
>
> A seleção de um novo tipo de instância alterará o custo de cada usuário ativo mensal. Para obter mais informações, consulte os preços do Amazon WorkSpaces Secure Browser.

3. 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”.
4. 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 O Secure Browser 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.

5. 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)”.
6. 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 Permitir que os usuários imprimam em um dispositivo local a partir do portal da web, escolha Permitido ou Não permitido.
5. Em Permitir que os usuários façam um link direto para seu portal da web, escolha Permitido ou Não permitido. Para obter mais informações sobre links diretos, consultethe section called "Permitir links diretos (opcional)".
6. 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

WorkSpaces O Secure Browser oferece dois tipos de autenticação: Padrão AWS IAM Identity Centere. 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 do WorkSpaces Secure Browser 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 no WorkSpaces Secure Browser

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=ExIdentity-Provider`.
       - Se você copiar e colar o valor do arquivo de metadados do SP, certifique-se de alterar `&` 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.

6. 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 nas asserções do SAML entre o IdP e o Secure Browser. 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).

7. Escolha se você deseja ativar o Logout Único. O logout único permite que seus usuários finais saiam da sessão do IdP WorkSpaces e do Secure Browser com uma única ação.

a. Baixe o certificado de assinatura do WorkSpaces Secure Browser e carregue-o em seu IdP. Esse é o mesmo certificado de assinatura usado para Assinatura de Solicitação na etapa anterior.

b. 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>`

c. 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:

1. 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.

2. 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 no WorkSpaces Secure Browser” 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 no WorkSpaces Secure Browser” 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 no WorkSpaces Secure Browser” 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 o Navegador WorkSpaces Seguro.
8. Baixe um arquivo de troca de metadados do seu IdP. Você fará o upload desses metadados para o WorkSpaces Secure Browser na próxima etapa.

### Etapa 3: Concluir a configuração do seu provedor de identidade no WorkSpaces Secure Browser

Retorne ao console do WorkSpaces Secure Browser. 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 do WorkSpaces Secure Browser 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 O Secure Browser 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 O Secure Browser 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 O Secure Browser 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 | Crie integrações de aplicativos SAML | Gerenciamento de usuários | Referência de campo SAML do Application Integration Wizard | Referência de campo SAML do Application Integration Wizard | Referência de campo SAML do Application Integration Wizard | Referência de campo SAML do Application Integration Wizard |
| Entrar | Crie seu próprio aplicativo | Início rápido: criar e atribuir uma conta de usuário | Habilite o login único para um aplicativo corporativo | Verificação da assinatura da solicitação SAML | Configurar a criptografia de token SAML do Microsoft Entra | Protocolo SAML de saída única |
| Ping | Adicionar um aplicativo SAML | Usuários | Habilitando o SSO iniciado pelo IdP | Configurando o login da solicitação de autentica | O PingOne for Enterprise oferece suporte à | Logout único do SAML 2.0 |

| IdP | Configuração do aplicativo SAML | Gerenciamento de usuários | Autenticação iniciada pelo IDP | Solicitar assinatura | Criptografia de asserção | Sessão única |
|---|---|---|---|---|---|---|
| | | | | ção PingOne para Enterprise | criptografia? | |
| Um login | Conector personalizado SAML (avançado) (4266907) | Adicionar usuários OneLogin manualmente | Conector personalizado SAML (avançado) (4266907) | Conector personalizado SAML (avançado) (4266907) | Conector personalizado SAML (avançado) (4266907) | Conector personalizado SAML (avançado) (4266907) |
| IAM Identity Center | Configure seu próprio aplicativo SAML 2.0 | Configure seu próprio aplicativo SAML 2.0 | Configure seu próprio aplicativo SAML 2.0 | 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 estiver usando o IAM Identity Center, você 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 portal do WorkSpaces Secure Browser. Região da AWS 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 do WorkSpaces Secure Browser 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 no WorkSpaces Secure Browser 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 do WorkSpaces Secure Browser emhttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Escolha Navegador WorkSpaces seguro, 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 portal do WorkSpaces Secure Browser.

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 portal do Navegador WorkSpaces Seguro. 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 emthe section called "Configurar o tipo de autenticação padrão".
- Para mudar do Standard para o IAM Identity Center, siga as etapas emthe 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 do WorkSpaces Secure Browser para navegar nos 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 do WorkSpaces Secure Browser em https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Escolha Navegador WorkSpaces seguro, 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 do WorkSpaces Secure Browser, escolha Entrar, SAML e insira suas credenciais do SAML.
5. Quando você vê a página Sua sessão está sendo preparada, sua sessão do Navegador WorkSpaces Seguro 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 estiver pronto para que seus usuários comecem a usar o Navegador WorkSpaces Seguro, você escolhe entre as seguintes opções para distribuir o portal:

- Adicione seu portal ao gateway do aplicativo SAML para permitir que os usuários iniciem uma sessão diretamente de seu IdP. Você pode fazer isso por meio do fluxo de login iniciado pelo IdP com seu IdP compatível com SAML 2.0. Para obter mais informações, consulte Asserções de SAML iniciadas pelo SP e iniciadas pelo IdP em. the section called “Configurar o tipo de autenticação padrão” Como alternativa, você pode criar um aplicativo SAML personalizado que possa oferecer experiências de autenticação iniciadas pelo IdP usando fluxos iniciados pelo SP. Para obter mais informações, consulte Criar uma integração com o aplicativo Bookmark.
- 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 o Navegador WorkSpaces Seguro 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 “Gerencie cotas de serviço para seu portal”.

# 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

Para visualizar detalhes do portal da web

1. Abra o console do WorkSpaces Secure Browser emhttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Escolha Navegador WorkSpaces seguro, 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 do WorkSpaces Secure Browser emhttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Escolha Navegador WorkSpaces seguro, 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 do WorkSpaces Secure Browser emhttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Escolha Navegador WorkSpaces seguro, Portais da Web, escolha seu portal da Web e, em seguida, escolha Excluir.

## Gerencie cotas de serviço para seu portal

Quando você cria seu Conta da AWS, definimos automaticamente as cotas de serviço padrão (também chamadas de limites) para o uso de recursos com Serviços da AWS. Os administradores devem estar cientes de duas cotas que talvez precisem ser aumentadas para apoiar seu caso de uso. Essas duas cotas são o número de portais da web que você pode criar em cada região e o número máximo de sessões simultâneas que você pode suportar com cada tipo de instância disponível em cada região. Você pode solicitar um aumento para elas na página Service Quotas no AWS Console.

A tabela a seguir lista os limites de cotas de serviço padrão.

| Cotas padrão em uma conta Região da AWS por | Valor |
| --- | --- |
| Portais da web | 3 |
| Máximo de sessões simultâneas - standard.regular | 25 |
| Máximo de sessões simultâneas - standard.large | 10 |
| Máximo de sessões simultâneas - standard.xlarge | 5 |

> **Important**
>
> As cotas de serviço afetam uma Região da AWS de cada vez. Você deve solicitar aumentos de cota de serviço em cada um dos Região da AWS casos em que precisar de mais recursos. Para obter mais informações, endpoints e cotas do Amazon WorkSpaces Secure Browser.

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 do serviço Secure Browser 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.

## Solicite um aumento no portal

Um portal é o recurso fundamental do serviço. Cada portal é uma associação entre seu provedor de identidade SAML 2.0 e sua conexão de rede com a Internet e qualquer conteúdo privado da web. Cada portal pode ter uma política de navegador de portal e configurações de usuário separadas, portanto, os administradores geralmente criam vários portais na mesma região para tratar de diferentes casos de uso. Por exemplo, você pode fornecer ao Grupo A acesso a um site específico com políticas restritivas (por exemplo, área de transferência e transferência de arquivos desativadas) e ao Grupo B acesso à Internet geral sem filtragem de URL. Você pode criar um portal em qualquer um suportado Região da AWS. Para ver a disponibilidade atual do serviço, consulte Serviços da AWS por região.

Para solicitar um aumento de cota de serviço

1. Abra a página Service Quotas na região desejada.
2. Escolha Número de portais da Web.
3. Escolha Solicitar um aumento no nível da conta.
4. Em Aumentar valor da cota, insira o valor total que você deseja que a cota seja.

## Solicite um aumento máximo de sessões simultâneas

A cota máxima de sessões simultâneas é a maior quantidade de usuários que podem ser conectados ao mesmo tempo em um portal. Se o limite da cota de serviço para o máximo de sessões simultâneas não for definido adequadamente, os usuários poderão descobrir que uma sessão não está disponível quando entrarem. Além de aumentar essa cota de serviço, os clientes

também devem garantir que sua VPC e sub-redes tenham espaço IP suficiente para suportar o máximo de sessões simultâneas.

Para solicitar um aumento máximo de sessão simultânea

1. Abra a página Service Quotas na região desejada.
2. Escolha Número máximo de sessões simultâneas por portal para o tipo de instância que você deseja aumentar.
3. Escolha Solicitar um aumento no nível da conta.
4. Em Aumentar valor da cota, insira o valor total que você deseja que a cota seja.

> **Note**
>
> Para aumentos grandes ou urgentes, acesse sua página de histórico de Cotas de Serviço, selecione o link na coluna de status de sua solicitação, vincule seu caso de suporte e adicione uma resposta com detalhes sobre seu caso de uso e/ou a urgência. Essas informações ajudam a equipe de atendimento a priorizar as solicitações e garantir que a capacidade suficiente seja alocada para sua conta.

## Exemplo de limite

Por exemplo, suponha que um administrador esteja configurando dois portais da web no Leste dos EUA (Norte da Virgínia) para um total de 125 usuários. Antes de criar o portal da web, o administrador identifica que o primeiro portal da web (Portal A) suportará 100 usuários. Ao testar o fluxo de trabalho desses usuários, o administrador determina que eles precisarão do tipo de instância XL para oferecer suporte ao streaming de áudio e vídeo durante a sessão. O segundo portal da web (Portal B) precisa estar disponível para até 25 usuários para oferecer suporte ao acesso a uma única página da web estática hospedada na VPC do cliente. Ao testar esse caso de uso, o administrador determina que o tipo de instância padrão pode oferecer suporte a esse caso de uso.

Para o portal A, o administrador deve enviar uma solicitação de aumento da cota de serviço para aumentar o limite de instâncias XL do padrão da região (ou seja, 5) para 100. Depois de preenchido, o administrador pode alocar a capacidade editando o portal da web. Para o portal B, o administrador pode avançar sem solicitar um aumento de cota (ou seja, já que a região tem uma cota padrão de 25 para o tipo de instância padrão).

## Gerenciar cotas de serviço

Para ver as cotas de serviço alocadas à sua conta para cada região a qualquer momento, consulte a página Cotas de serviço.

## Outras cotas de serviços

Você pode visualizar e solicitar aumentos para outras cotas listadas na página Service Quotas. Na prática, a maioria dos clientes achará desnecessário solicitar aumentos desses limites. Essas cotas são amplamente agrupadas em dois tipos: Número e Taxa.

Para cotas numéricas, ao enviar um aumento de cota de serviço para Número de portais da web, você receberá automaticamente um aumento no número de sub-recursos necessários para criar um portal exclusivo. Isso será refletido na página de Cotas de Serviço. Por exemplo, se você solicitar um aumento nos portais de 3 para 5, receberá automaticamente um aumento na cota de serviço de 3 para 5 nas configurações do navegador e do usuário. Você tem a opção de reutilizar ou criar novos sub-recursos conforme desejado.

Em raras ocasiões, os clientes podem encontrar um caso de uso para aumentar o número ou a taxa de outras cotas de recursos. Por exemplo, os administradores podem querer aumentar o número de configurações do navegador para testar configurações adicionais do portal. Essas solicitações de cota de serviço serão analisadas e atendidas case-by-case com base nisso.

Para cotas de tarifas, os limites de taxa expostos nas Cotas de Serviço não precisam ser ajustados, independentemente do limite do portal da conta.

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

Quando um usuário visita um portal do WorkSpaces Secure Browser, 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 o Secure Browser. 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 portal do WorkSpaces Secure Browser. Esses valores controlam a quantidade de tempo entre a última interação do usuário e o término de uma sessão do Navegador WorkSpaces Seguro 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 o nome de usuário e a senha para iniciar uma WorkSpaces nova sessão do Navegador Seguro. 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 do Navegador WorkSpaces Seguro.
- Fim da sessão - marca o fim de uma sessão do Navegador WorkSpaces Seguro.

- 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 do WorkSpaces Secure Browser e garantir que o uso do WorkSpaces Secure Browser esteja em conformidade com todas as leis e regulamentos aplicáveis. Isso inclui leis que regulam a capacidade do empregador de monitorar o uso do Navegador WorkSpaces Seguro por um funcionário, incluindo atividades realizadas dentro do aplicativo.

A ativação dos registros de acesso do usuário no portal do WorkSpaces Secure Browser 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 do WorkSpaces Secure Browser, 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 do WorkSpaces Secure Browser, 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 o Navegador WorkSpaces Seguro, 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 Introdução ao WorkSpaces Secure Browser.

WorkSpaces O Secure Browser 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)

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

Para fazer o upload do arquivo JSON da política do Chrome, você deve criar um portal do Navegador WorkSpaces Seguro. 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 do WorkSpaces Secure Browser emhttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Escolha Navegador WorkSpaces seguro 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, o WorkSpaces Secure Browser 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 do Secure Browser 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 do WorkSpaces Secure Browser:

- 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 das sessões do Navegador WorkSpaces Seguro, entre em contato com. AWS Support

# Configurar a localização na sessão

Quando um usuário inicia uma sessão, o WorkSpaces Secure Browser 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 pelo WorkSpaces Secure Browser. 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 ForcedLanguagespolítica 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 no WorkSpaces Secure Browser oferecem suporte à localização:

- WorkSpaces Página de login do Secure Browser
- WorkSpaces Mensagens de status do portal do Secure Browser (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 O Navegador Seguro 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, o WorkSpaces Secure Browser 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 Secure Browser 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, o WorkSpaces Secure Browser 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 do WorkSpaces Secure Browser e devem garantir que o uso do WorkSpaces Secure Browser esteja em conformidade com todas as leis e regulamentos aplicáveis. Isso inclui leis que regulam a capacidade do empregador de monitorar o uso do Navegador WorkSpaces Seguro 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 do WorkSpaces Secure Browser emhttps://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 do WorkSpaces Secure Browser emhttps://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 do WorkSpaces Secure Browser emhttps://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 do WorkSpaces Secure Browser emhttps://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 são solicitados a instalar a extensão ao entrarem em um portal.

Por padrão, as extensões não estão habilitadas no Chrome nas janelas anônimas ou nas janelas de navegação privada do Firefox. Os usuários podem ativá-los manualmente. Para obter mais informações sobre o Chrome, consulte Extensões no modo de navegação anônima. Para obter mais informações sobre o Firefox, 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 |
| Inserir ID | microsoftonline.com |
| Centro de Identidade da AWS | awsapps.com |
| Um login | onelogin.com |
| Duo | duosecurity.com |

Em seguida, visite 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 do WorkSpaces Secure Browser em https://console.aws.amazon.com/workspaces-web/home.
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 do WorkSpaces Secure Browser em https://console.aws.amazon.com/workspaces-web/home.
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 Secure Browser 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 do WorkSpaces Secure Browser 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 do WorkSpaces Secure Browser emhttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Escolha Navegador WorkSpaces seguro, 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.

## Permitir links diretos (opcional)

Quando um usuário faz login no WorkSpaces Secure Browser, ele inicia a sessão em uma página inicial definida pelo administrador. Você também pode permitir que os portais recebam links diretos que conectam usuários a um site específico durante uma sessão. Quando um link direto é selecionado, o portal exibe a URL especificada no link direto. O link é exibido ao lado da (s) página (s) inicial (s) configurada (s) para o início da sessão ou por si só, se uma sessão já estiver em andamento. Esse recurso permite que os administradores criem experiências de usuário mais dinâmicas com o WorkSpaces Secure Browser. Para permitir a permissão para links diretos, escolha Permitido ao criar as configurações do usuário. Para ter mais informações, consulte the section called “Definir as configurações do usuário”.

Links diretos abrem páginas em uma sessão do WorkSpaces Secure Browser. Se uma sessão já estiver em execução, ela abrirá o link direto em uma nova guia. Se uma sessão ainda não estiver em execução, ela abrirá a URL do link direto em uma nova guia e a página inicial padrão do portal em uma guia separada. Se um link direto contiver mais de um URL, ele exibirá o URL do link direto listado primeiro em foco, com cada URL subsequente (incluindo a página inicial padrão) aberto em guias separadas.

Os links diretos devem atender aos seguintes requisitos:

- O portal deve ter permissões de link direto definidas como Permitido. Para ter mais informações, consulte the section called “Definir as configurações do usuário”.
- O site para o qual você deseja criar um link direto deve estar codificado em URL. Por exemplo, para vincular um usuário a “https://www.example.com/?query=true”, atualize o link para https%3A%2F%2Fwww.example.com%2F%3FQuery%3Dtrue.
- Anexe a URL a uma URL de portal com lista de permissões no seguinte formato, em que UUID é a ID do portal:

https://<uuid>.workspaces-web.com/? DeepLinks=https%3A%2F%2Fwww.example.com%2F%3FQuery%3Dtrue

- Um deeplink pode conter até 10 URLs, delineados por vírgula. Por exemplo: .

  https://<uuid>.workspaces-web.com/? deeplinks=https%3A%2F%2Fwww.example.com%2F%3Fquery%3Dtrue, https%3A%2F%2Fwww.example.com%2F%3Fquery%3DTrue2, https%3A%2F%2Fwww.example.com%2F%3Fquery%2Fwww.example.com%2F%3Fquery%2Fwww.example.com%2F%3Fquery%2Fwww.example.com%2F%3Fquery%2Fwww.example.com%2F%3Fquery%2Fwww.example.com%2F%3Fquery%2Fwww.example.com%2F%3Fquery%2Fwww.example.com3DTrue3, https%3A%2F%2Fwww.example.com%2F%3FQuery%3DTrue4

Qualquer usuário com quem você compartilhar este link do portal pode manipular o valor do link direto para visitar um site, se esse domínio estiver acessível a partir do portal e não estiver na lista de bloqueio de URL. Para criar uma lista restritiva de permissões ou lista de bloqueio para impedir que os usuários visitem domínios não intencionais com seu portal, utilize a filtragem de URL. A lista de permissões e a lista de bloqueio de um portal podem ser editadas com a filtragem de URL nas configurações do navegador do seu portal. Para obter mais informações, consulte the section called “Configurar a filtragem de URL” Permitir ou bloquear o acesso a sites.

# Segurança no Amazon WorkSpaces Secure Browser

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

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

- Segurança da nuvem — AWS é responsável por proteger a infraestrutura que executa AWS os serviços na AWS nuvem. AWS também fornece serviços que você pode usar com segurança. Auditores terceirizados testam e verificam regularmente a eficácia de nossa segurança como parte dos Programas de Conformidade Programas de AWS de . Para saber mais sobre os programas de conformidade que se aplicam ao Amazon WorkSpaces Secure Browser, consulte AWS Services in Scope by Compliance Program .
- Segurança na nuvem — Sua responsabilidade é determinada pelo AWS serviço 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.

Essa documentação ajuda você a entender como aplicar o modelo de responsabilidade compartilhada ao usar o Amazon WorkSpaces Secure Browser. Ele mostra como configurar o Amazon WorkSpaces Secure Browser para atender aos seus objetivos de segurança e conformidade. Você também aprende a usar outros AWS serviços que ajudam a monitorar e proteger seus recursos do Amazon WorkSpaces Secure Browser.

Conteúdo

- Melhores práticas de segurança para o Amazon WorkSpaces Secure Browser

# Proteção de dados no Amazon WorkSpaces Secure Browser

O modelo de responsabilidade AWS compartilhada se aplica à proteção de dados no Amazon WorkSpaces Secure Browser. Conforme descrito neste modelo, AWS é responsável por proteger a infraestrutura global que executa todos os Nuvem AWS. Você é responsável por manter o controle sobre seu conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para obter mais informações sobre privacidade de dados, consulte Privacidade de dados FAQ. Para obter informações sobre proteção de dados na Europa, consulte o Modelo de Responsabilidade AWS Compartilhada e GDPR a postagem no blog AWS de segurança.

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS as credenciais e configure usuários individuais com AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use a autenticação multifator (MFA) com cada conta.
- UseSSL/TLSpara se comunicar com AWS os recursos. Exigimos TLS 1,2 e recomendamos TLS 1,3.
- Configure API e registre as atividades do usuário com AWS CloudTrail.
- Use soluções de AWS criptografia, juntamente com todos os controles de segurança padrão Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados sigilosos armazenados no Amazon S3.
- Se você precisar de FIPS 140-3 módulos criptográficos validados ao acessar AWS por meio de uma interface de linha de comando ou umaAPI, use um endpoint. FIPS Para obter mais informações sobre os FIPS endpoints disponíveis, consulte Federal Information Processing Standard (FIPS) 140-3.

É altamente recomendável que nunca sejam colocadas informações de identificação confidenciais, como endereços de e-mail dos seus clientes, em marcações ou campos de formato livre, como um campo Nome. Isso inclui quando você trabalha com o WorkSpaces Secure Browser ou outro

Serviços da AWS usando o consoleAPI, AWS CLI,, ou AWS SDKs. 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, é altamente recomendável que você não inclua informações de credenciais no URL para validar sua solicitação para esse servidor.

## Criptografia de dados

O Amazon WorkSpaces Secure Browser coleta dados de personalização do portal, como configurações do navegador, configurações do usuário, configurações de rede, informações do provedor de identidade, dados do armazenamento confiável e dados do certificado do armazenamento confiável. WorkSpaces O Secure Browser 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 O Secure Browser usa 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 nas ações do Navegador WorkSpaces Seguro. Use IAM modelos para criar uma função de acesso total ou uma função somente leitura. Para obter mais informações, consulte AWS políticas gerenciadas para o WorkSpaces Secure Browser.
- Proteja os dados de ponta a ponta fornecendo uma chave gerenciada pelo cliente, para que o WorkSpaces Secure Browser 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 do WorkSpaces Secure Browser.
  - 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 O Secure Browser protege conteúdo e metadados por padrão, criptografando todos os dados confidenciais com. AWS KMS Ele coleta a política do navegador e as preferências do usuário para aplicar políticas e configurações durante as sessões do WorkSpaces Secure Browser. 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 em repouso

A criptografia em repouso é configurada por padrão. Os dados específicos do cliente usados no WorkSpaces Secure Browser são criptografados usando. AWS KMS WorkSpaces O Secure Browser fornece criptografia em repouso para os recursos que você cria. O serviço aceita uma chave gerenciada pelo AWS KMS cliente na criação de recursos e, se não for fornecida, uma AWS chave própria 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 AWS Própria, enquanto estiverem armazenadas em nosso back-end.

Você pode decidir qual chave será usada ao criar um recurso do Navegador WorkSpaces Seguro. Se os dados que fazem parte desse recurso forem criptografados, o WorkSpaces Secure Browser `customerManagedKeyArn` aceitará o campo como parte do `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.

Você pode solucionar problemas e auditar o uso da chave verificando o status das AWS KMS concessões. Para obter mais informações, consulte Managing grants. Durante a criação do portal, o WorkSpaces Secure Browser 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 O Secure Browser criptografa dados em trânsito acima HTTPS de TLS 1.2. Você pode enviar uma solicitação WorkSpaces usando o console ou API chamadas diretas. Os dados da

solicitação que são transferidos são criptografados enviando tudo por meio de uma TLS conexão HTTPS ou. Os dados da solicitação podem ser transferidos do AWS console ou AWS SDK para AWS Command Line Interface o WorkSpaces Secure Browser.

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

## Privacidade do tráfego entre redes

Para proteger as conexões entre o WorkSpaces Secure Browser e os aplicativos locais, você usa o WorkSpaces Secure Browser para iniciar sessões do navegador dentro das suas próprias. VPC A conexão com aplicativos locais é configurada por conta própria VPC e não é controlada pelo WorkSpaces Secure Browser.

Para proteger as conexões entre contas, o WorkSpaces Secure Browser usa uma função vinculada ao serviço para se conectar com segurança às contas dos clientes e executar operações em nome do cliente. Para obter mais informações, consulte Usando funções vinculadas ao serviço para WorkSpaces o Secure Browser.

## Registro em log do acesso do usuário

Os administradores podem registrar os eventos da sessão do WorkSpaces Secure Browser, incluindo início, parada e URL visitas. Esses logs são criptografados e entregues com segurança aos clientes por meio de um Amazon Kinesis Data Stream. As informações de navegação do registro de acesso do usuário não são AWS armazenadas nem estão disponíveis nas sessões sem o registro configurado. URLvisitas no modo de navegação anônima ou excluídas URLs do histórico do navegador não são registradas no registro de acesso do usuário.

# Identity and Access Management para o Amazon WorkSpaces Secure Browser

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

Tópicos



## Público

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

Usuário do serviço — Se você usa o serviço WorkSpaces Secure Browser para fazer seu trabalho, seu administrador fornecerá as credenciais e as permissões de que você precisa. À medida que você usa mais recursos do Navegador WorkSpaces Seguro para fazer seu trabalho, talvez precise de permissões adicionais. Entender como o acesso é gerenciado pode ajudar você a solicitar as permissões corretas ao seu administrador. Se você não conseguir acessar um recurso no WorkSpaces Secure Browser, consulteSolução de problemas de identidade e acesso ao Amazon WorkSpaces Secure Browser.

Administrador de serviços — Se você é responsável pelos recursos do Navegador WorkSpaces Seguro em sua empresa, provavelmente tem acesso total ao Navegador WorkSpaces Seguro. É seu trabalho determinar quais recursos e recursos do Navegador WorkSpaces Seguro seus usuários do serviço devem acessar. Em seguida, você deve enviar solicitações ao IAM administrador para alterar as permissões dos usuários do serviço. Revise as informações nesta página para entender os conceitos básicos doIAM. Para saber mais sobre como sua empresa pode usar o IAM WorkSpaces Secure Browser, consulteComo o Amazon WorkSpaces Secure Browser funciona com IAM.

IAMadministrador — Se você for IAM administrador, talvez queira saber detalhes sobre como criar políticas para gerenciar o acesso ao WorkSpaces Secure Browser. Para ver exemplos de políticas baseadas em identidade do WorkSpaces Secure Browser que você pode usar emIAM, consulte. Exemplos de políticas baseadas em identidade para o Amazon Secure WorkSpaces Browser

## Autenticando com identidades

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

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

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

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

Independente do método de autenticação usado, também pode ser exigido que você forneça informações adicionais de segurança. Por exemplo, AWS recomenda que você use a autenticação multifator (MFA) para aumentar a segurança da sua conta. Para saber mais, consulte Autenticação multifator no Guia AWS IAM Identity Center do usuário e Uso da autenticação multifator (MFA) AWS no Guia do IAMusuário.

### Conta da AWS usuário root

Ao criar uma Conta da AWS, você começa com uma identidade de login que tem acesso completo a todos Serviços da AWS os recursos da conta. Essa identidade é chamada de usuário Conta da AWS raiz e é acessada fazendo login com o endereço de e-mail e a senha que você usou para criar a conta. É altamente recomendável não usar o usuário raiz para tarefas diárias. Proteja as credenciais

do usuário raiz e use-as para executar as tarefas que somente ele puder executar. Para ver a lista completa de tarefas que exigem que você faça login como usuário raiz, consulte Tarefas que exigem credenciais de usuário raiz no Guia do IAM usuário.

## Identidade federada

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

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

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

## Grupos e usuários do IAM

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

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

Usuários são diferentes de perfis. Um usuário é exclusivamente associado a uma pessoa ou a uma aplicação, mas um perfil pode ser assumido por qualquer pessoa que precisar dele. Os usuários

têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias. Para saber mais, consulte Quando criar um IAM usuário (em vez de uma função) no Guia do IAM usuário.

## IAMfunções

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

IAMfunções com credenciais temporárias são úteis nas seguintes situações:

- Acesso de usuário federado: para atribuir permissões a identidades federadas, você pode criar um perfil e definir permissões para ele. Quando uma identidade federada é autenticada, essa identidade é associada ao perfil e recebe as permissões definidas pelo mesmo. Para obter informações sobre funções para federação, consulte Criação de uma função para um provedor de identidade terceirizado no Guia IAM do usuário. Se você usa o IAM Identity Center, configura um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o IAM Identity Center correlaciona o conjunto de permissões a uma função em. IAM Para obter informações sobre conjuntos de permissões, consulte Conjuntos de Permissões no Manual do Usuário do AWS IAM Identity Center .
- Permissões temporárias IAM de IAM usuário — Um usuário ou função pode assumir uma IAM função para assumir temporariamente permissões diferentes para uma tarefa específica.
- Acesso entre contas — Você pode usar uma IAM função para permitir que alguém (um diretor confiável) em uma conta diferente acesse recursos em sua conta. Os perfis são a principal forma de conceder acesso entre contas. No entanto, com alguns Serviços da AWS, você pode anexar uma política diretamente a um recurso (em vez de usar uma função como proxy). Para saber a diferença entre funções e políticas baseadas em recursos para acesso entre contas, consulte Acesso a recursos entre contas IAM no Guia do IAM usuário.
- Acesso entre serviços — Alguns Serviços da AWS usam recursos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicativos na Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões do principal de chamada, usando um perfil de serviço ou um perfil vinculado a serviço.

- Sessões de acesso direto (FAS) — Quando você usa um IAM usuário ou uma função para realizar ações em AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. FASusa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. FASas solicitações são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer FAS solicitações, consulte Encaminhar sessões de acesso.
- Função de serviço — Uma função de serviço é uma IAMfunção que um serviço assume para realizar ações em seu nome. Um IAM administrador pode criar, modificar e excluir uma função de serviço internamenteIAM. Para obter mais informações, consulte Criação de uma função para delegar permissões a uma AWS service (Serviço da AWS) no Guia do IAM usuário.
- Função vinculada ao serviço — Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode presumir a função de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um IAM administrador pode visualizar, mas não editar, as permissões das funções vinculadas ao serviço.

- Aplicativos em execução na Amazon EC2 — Você pode usar uma IAM função para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma EC2 instância e fazendo AWS CLI AWS API solicitações. Isso é preferível a armazenar chaves de acesso na EC2 instância. Para atribuir uma AWS função a uma EC2 instância e disponibilizá-la para todos os aplicativos, você cria um perfil de instância anexado à instância. Um perfil de instância contém a função e permite que os programas em execução na EC2 instância recebam credenciais temporárias. Para obter mais informações, consulte Como usar uma IAM função para conceder permissões a aplicativos executados em EC2 instâncias da Amazon no Guia IAM do usuário.

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

## Gerenciando acesso usando políticas

Você controla o acesso AWS criando políticas e anexando-as a AWS identidades ou recursos. Uma política é um objeto AWS que, quando associada a uma identidade ou recurso, define suas permissões. AWS avalia essas políticas quando um principal (usuário, usuário raiz ou sessão de função) faz uma solicitação. As permissões nas políticas determinam se a solicitação será permitida

ou negada. A maioria das políticas é armazenada AWS como JSON documentos. Para obter mais informações sobre a estrutura e o conteúdo dos documentos de JSON política, consulte Visão geral das JSON políticas no Guia IAM do usuário.

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

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

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

## Políticas baseadas em identidade

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

As políticas baseadas em identidade podem ser categorizadas ainda adicionalmente como políticas em linha ou políticas gerenciadas. As políticas em linha são anexadas diretamente a um único usuário, grupo ou perfil. As políticas gerenciadas são políticas autônomas que você pode associar a vários usuários, grupos e funções em seu Conta da AWS. As políticas AWS gerenciadas incluem políticas gerenciadas e políticas gerenciadas pelo cliente. Para saber como escolher entre uma política gerenciada ou uma política em linha, consulte Escolha entre políticas gerenciadas e políticas em linha no Guia do IAMusuário.

## Políticas baseadas no recurso

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

pode executar nesse recurso e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

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

### Listas de controle de acesso (ACLs)

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

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

### Outros tipos de política

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

- Limites de permissões — Um limite de permissões é um recurso avançado no qual você define as permissões máximas que uma política baseada em identidade pode conceder a uma IAM entidade (IAMusuário ou função). É possível definir um limite de permissões para uma entidade. As permissões resultantes são a interseção das políticas baseadas em identidade de uma entidade com seus limites de permissões. As políticas baseadas em recurso que especificam o usuário ou o perfil no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte Limites de permissões para IAM entidades no Guia IAM do usuário.
- Políticas de controle de serviço (SCPs) — SCPs são JSON políticas que especificam as permissões máximas para uma organização ou unidade organizacional (OU) em AWS Organizations. AWS Organizations é um serviço para agrupar e gerenciar centralmente vários Contas da AWS que sua empresa possui. Se você habilitar todos os recursos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as suas contas. Os SCP limites de permissões para entidades nas contas dos membros, incluindo cada uma Usuário raiz da conta da AWS. Para obter mais informações sobre Organizations eSCPs, consulte Políticas de controle de serviços no Guia AWS Organizations do Usuário.

- Políticas de sessão: são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para um perfil ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do usuário ou do perfil e das políticas de sessão. As permissões também podem ser provenientes de uma política baseada em atributo. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações, consulte Políticas de sessão no Guia IAM do usuário.

### Vários tipos de política

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

## Como o Amazon WorkSpaces Secure Browser funciona com IAM

Antes de usar IAM para gerenciar o acesso ao WorkSpaces Secure Browser, saiba quais IAM recursos estão disponíveis para uso com o WorkSpaces Secure Browser.

IAMrecursos que você pode usar com o Amazon WorkSpaces Secure Browser

| IAMrecurso | WorkSpaces Suporte ao Secure Browser |
|---|---|
| Políticas baseadas em identidade | Sim |
| Políticas baseadas em recursos | Não |
| Ações das políticas | Sim |
| Atributos de políticas | Sim |
| Chaves de condição de políticas | Sim |
| ACLs | Não |
| ABAC(tags nas políticas) | Parcial |
| Credenciais temporárias | Sim |

| IAMrecurso | WorkSpaces Suporte ao Secure Browser |
| --- | --- |
| Permissões de entidade principal | Sim |
| Perfis de serviço | Não |
| Funções vinculadas ao serviço | Sim |

Para obter uma visão geral de como o WorkSpaces Secure Browser e outros AWS serviços funcionam com a maioria dos IAM recursos, consulte AWS os serviços que funcionam com IAM no Guia do IAM Usuário.

## Políticas baseadas em identidade para WorkSpaces o Secure Browser

Compatível com políticas baseadas em identidade: Sim

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

Com políticas IAM baseadas em identidade, você pode especificar ações e recursos permitidos ou negados, bem como as condições sob as quais as ações são permitidas ou negadas. Você não pode especificar a entidade principal em uma política baseada em identidade porque ela se aplica ao usuário ou perfil ao qual ela está anexada. Para saber mais sobre todos os elementos que você pode usar em uma JSON política, consulte a referência IAM JSON de elementos de política no Guia IAM do usuário.

Exemplos de políticas baseadas em identidade para WorkSpaces o Secure Browser

Para ver exemplos de políticas baseadas em identidade do WorkSpaces Secure Browser, consulte. Exemplos de políticas baseadas em identidade para o Amazon Secure WorkSpaces Browser

## Políticas baseadas em recursos no Secure WorkSpaces Browser

Suporte a políticas baseadas em recursos: não

Políticas baseadas em recursos são documentos JSON de política que você anexa a um recurso. Exemplos de políticas baseadas em recursos são políticas de confiança de IAM funções e

políticas de bucket do Amazon S3. Em serviços que suportem políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações um principal especificado pode executar nesse recurso e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

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

## Ações de política para o WorkSpaces Secure Browser

Compatível com ações de políticas: Sim

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

O `Action` elemento de uma JSON política descreve as ações que você pode usar para permitir ou negar acesso em uma política. As ações de política geralmente têm o mesmo nome da AWS API operação associada. Há algumas exceções, como ações somente com permissão que não têm uma operação correspondente. API 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 do WorkSpaces Secure Browser, consulte Ações definidas pelo Amazon WorkSpaces Secure Browser na Referência de Autorização de Serviço.

As ações de política no WorkSpaces Secure Browser 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 do WorkSpaces Secure Browser, consulte. Exemplos de políticas baseadas em identidade para o Amazon Secure WorkSpaces Browser

## Recursos de política para o WorkSpaces Secure Browser

Compatível com recursos de políticas: Sim

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

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

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

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

Para ver uma lista dos tipos de recursos do Navegador WorkSpaces Seguro e seusARNs, consulte Recursos definidos pelo Amazon WorkSpaces Secure Browser na Referência de Autorização de Serviço. Para saber com quais ações você pode especificar cada recurso, consulte Ações definidas pelo Amazon WorkSpaces Secure Browser. ARN

Para ver exemplos de políticas baseadas em identidade do WorkSpaces Secure Browser, consulte. Exemplos de políticas baseadas em identidade para o Amazon Secure WorkSpaces Browser

## Chaves de condição de política para o WorkSpaces Secure Browser

Compatível com chaves de condição de política específicas de serviço: Sim

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

O elemento `Condition` (ou bloco `Condition`) permite que você especifique condições nas quais uma instrução estiver em vigor. O elemento `Condition` é opcional. É possível criar expressões condicionais que usem agentes 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, AWS avalia a condição usando uma `OR` operação lógica. Todas as condições devem ser atendidas antes que as permissões da instrução sejam concedidas.

Você também pode usar variáveis de espaço reservado ao especificar condições. Por exemplo, você pode conceder permissão a um IAM usuário para acessar um recurso somente se ele estiver marcado com o nome de IAM usuário. Para obter mais informações, consulte elementos de IAM política: variáveis e tags no Guia IAM do usuário.

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

Para ver uma lista das chaves de condição do WorkSpaces Secure Browser, consulte Chaves de condição do Amazon WorkSpaces Secure Browser na Referência de Autorização de Serviço. Para saber com quais ações e recursos você pode usar uma chave de condição, consulte Ações definidas pelo Amazon WorkSpaces Secure Browser.

Para ver exemplos de políticas baseadas em identidade do WorkSpaces Secure Browser, consulte. Exemplos de políticas baseadas em identidade para o Amazon Secure WorkSpaces Browser

## Listas de controle de acesso (ACLs) no WorkSpaces Secure Browser

SuportesACLs: Não

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

## Controle de acesso baseado em atributos (ABAC) com WorkSpaces o Secure Browser

Suportes ABAC (tags nas políticas): Parciais

O controle de acesso baseado em atributos (ABAC) é uma estratégia de autorização que define permissões com base em atributos. Em AWS, esses atributos são chamados de tags. Você pode anexar tags a IAM entidades (usuários ou funções) e a vários AWS recursos. Marcar entidades e recursos é a primeira etapa doABAC. Em seguida, você cria ABAC políticas para permitir operações quando a tag do diretor corresponde à tag do recurso que ele está tentando acessar.

ABACé útil em ambientes que estão crescendo rapidamente e ajuda em situações em que o gerenciamento de políticas se torna complicado.

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 chaves de condição `aws:TagKeys`.

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 sobreABAC, consulte O que éABAC? no Guia do IAM usuário. Para ver um tutorial com etapas de configuraçãoABAC, consulte Usar controle de acesso baseado em atributos (ABAC) no Guia do IAMusuário.

## Usando credenciais temporárias com o WorkSpaces Secure Browser

Compatível com 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 esse trabalho IAM no Guia do IAM usuário.

Você está usando credenciais temporárias se fizer login AWS Management Console usando qualquer método, exceto um nome de usuário e senha. Por exemplo, quando você acessa AWS usando o link de login único (SSO) da sua empresa, esse processo cria automaticamente credenciais temporárias. Você também cria automaticamente credenciais temporárias quando faz login no

console como usuário e, em seguida, alterna perfis. Para obter mais informações sobre a troca de funções, consulte Alternando para uma função (console) no Guia IAM do usuário.

Você pode criar manualmente credenciais temporárias usando o AWS CLI ou AWS API. Em seguida, você pode usar essas credenciais temporárias para acessar AWS. AWS recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para obter mais informações, consulte Credenciais de segurança temporárias emIAM.

## Permissões principais entre serviços para o WorkSpaces Secure Browser

Suporta sessões de acesso direto (FAS): Sim

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

## Funções de serviço para o WorkSpaces Secure Browser

Compatível com perfis de serviço: não

Uma função de serviço é uma IAMfunção que um serviço assume para realizar ações em seu nome. Um IAM administrador pode criar, modificar e excluir uma função de serviço internamenteIAM. Para obter mais informações, consulte Criação de uma função para delegar permissões a uma AWS service (Serviço da AWS) no Guia do IAM usuário.

> **Warning**
>
> Alterar as permissões de uma função de serviço pode interromper a funcionalidade do Navegador WorkSpaces Seguro. Edite as funções de serviço somente quando o WorkSpaces Secure Browser fornecer orientação para fazer isso.

## Funções vinculadas ao serviço para WorkSpaces o Secure Browser

Suporte a perfis vinculados a serviços: sim

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

Para obter detalhes sobre como criar ou gerenciar funções vinculadas a serviços, consulte AWS serviços que funcionam com. 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 serviço desse serviço.

# Exemplos de políticas baseadas em identidade para o Amazon Secure WorkSpaces Browser

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

Para saber como criar uma política IAM baseada em identidade usando esses exemplos de documentos de JSON política, consulte Criação de IAM políticas no Guia do IAMusuário.

Para obter detalhes sobre ações e tipos de recursos definidos pelo WorkSpaces Secure Browser, incluindo o formato de cada um dos tipos de recursos, consulte Ações, recursos e chaves de condição para o Amazon WorkSpaces Secure Browser na Referência de autorização de serviço. ARNs

Tópicos

- Melhores práticas de política
- Usando o console do WorkSpaces Secure Browser
- Permitir que usuários visualizem suas próprias permissões

## Melhores práticas de política

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir recursos do Navegador WorkSpaces Seguro em sua conta. Essas ações podem incorrer em custos para

seus Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com as políticas AWS gerenciadas e avance para as permissões de privilégios mínimos — Para começar a conceder permissões aos seus usuários e cargas de trabalho, use as políticas AWS gerenciadas que concedem permissões para muitos casos de uso comuns. Eles estão disponíveis no seu Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo AWS cliente que sejam específicas para seus casos de uso. Para obter mais informações, consulte políticas AWS gerenciadas ou políticas AWS gerenciadas para funções de trabalho no Guia IAM do usuário.
- Aplique permissões com privilégios mínimos — Ao definir permissões com IAM políticas, conceda somente as permissões necessárias para realizar uma tarefa. Você faz isso definindo as ações que podem ser executadas em atributos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para obter mais informações sobre IAM como usar para aplicar permissões, consulte Políticas e permissões IAM no Guia IAM do usuário.
- Use condições nas IAM políticas para restringir ainda mais o acesso — Você pode adicionar uma condição às suas políticas para limitar o acesso a ações e recursos. Por exemplo, você pode escrever uma condição de política para especificar que todas as solicitações devem ser enviadas usandoSSL. Você também pode usar condições para conceder acesso às ações de serviço se elas forem usadas por meio de uma ação específica AWS service (Serviço da AWS), como AWS CloudFormation. Para obter mais informações, consulte Elementos IAM JSON da política: Condição no Guia IAM do usuário.
- Use o IAM Access Analyzer para validar suas IAM políticas e garantir permissões seguras e funcionais — o IAM Access Analyzer valida políticas novas e existentes para que as políticas sigam a linguagem da IAM política (JSON) e as melhores práticas. IAM IAMO Access Analyzer fornece mais de 100 verificações de políticas e recomendações práticas para ajudá-lo a criar políticas seguras e funcionais. Para obter mais informações, consulte Validação da política do IAM Access Analyzer no Guia do IAM Usuário.
- Exigir autenticação multifatorial (MFA) — Se você tiver um cenário que exija IAM usuários ou um usuário root Conta da AWS, ative MFA para obter segurança adicional. Para exigir MFA quando API as operações são chamadas, adicione MFA condições às suas políticas. Para obter mais informações, consulte Configurando o API acesso MFA protegido no Guia do IAMusuário.

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

## Usando o console do WorkSpaces Secure Browser

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

Você não precisa permitir permissões mínimas do console para usuários que estão fazendo chamadas somente para AWS CLI o. ou AWS API o. Em vez disso, permita o acesso somente às ações que correspondam à API operação que eles estão tentando realizar.

Para garantir que usuários e funções ainda possam usar o console do Navegador WorkSpaces Seguro, anexe também o Navegador WorkSpaces Seguro `ConsoleAccess` ou a política `ReadOnly` AWS gerenciada às entidades. Para obter mais informações, consulte Adicionar permissões a um usuário no Guia do IAM usuário.

## Permitir que usuários visualizem suas próprias permissões

Este exemplo mostra como você pode criar uma política que permita IAM aos usuários visualizar as políticas embutidas e gerenciadas que estão anexadas à identidade do usuário. Essa política inclui permissões para concluir essa ação no console ou programaticamente usando o AWS CLI ou. AWS API

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

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

## AWS políticas gerenciadas para o WorkSpaces Secure Browser

Para adicionar permissões a usuários, grupos e funções, é mais fácil usar políticas AWS gerenciadas do que escrever políticas você mesmo. 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, você pode usar nossas políticas AWS gerenciadas. Essas políticas abrangem casos de uso comuns e estão disponíveis em sua AWS conta. Para obter mais informações sobre políticas AWS gerenciadas, consulte políticas AWS gerenciadas no Guia do usuário do IAM.

AWS os serviços mantêm e atualizam as políticas AWS gerenciadas. Você não pode alterar as permissões nas políticas AWS gerenciadas. Ocasionalmente, os serviços podem adicionar permissões adicionais a uma política AWS gerenciada 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 as permissões de uma política AWS gerenciada, portanto, as atualizações de políticas não violarão suas permissões existentes.

Além disso, AWS oferece suporte a políticas gerenciadas para funções de trabalho que abrangem vários serviços. Por exemplo, a política `ReadOnlyAccess` AWS gerenciada fornece acesso somente

de leitura a todos os AWS serviços e recursos. Quando um serviço lança um novo recurso, AWS adiciona permissões somente de 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.

## AWS política gerenciada: AmazonWorkSpacesWebServiceRolePolicy

Não é possível anexar a política `AmazonWorkSpacesWebServiceRolePolicy` às suas entidades do IAM. Essa política é anexada a uma função vinculada ao serviço que permite que o WorkSpaces Secure Browser execute ações em seu nome. Para ter mais informações, consulte the section called "Uso de perfis vinculadas ao serviço".

Essa política concede permissões administrativas que permitem acesso aos AWS serviços e recursos usados ou gerenciados pelo WorkSpaces Secure Browser.

Detalhes de permissão

Esta política inclui as seguintes permissões:

- `workspaces-web`— Permite acesso a AWS serviços e recursos usados ou gerenciados pelo WorkSpaces Secure Browser.
- `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 ter 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-*"
        }
    ]
}
```

## AWS política gerenciada: AmazonWorkSpacesSecureBrowserReadOnly

É possível anexar a política `AmazonWorkSpacesSecureBrowserReadOnly` a suas identidades do IAM.

Essa política concede permissões somente para leitura que permitem acesso ao WorkSpaces Secure Browser e suas dependências por meio do AWS Management Console, SDK e CLI. 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 das permissões

Esta política inclui as seguintes permissões:

- `workspaces-web`— Fornece acesso somente de leitura ao WorkSpaces Secure Browser e suas dependências por meio do console AWS de gerenciamento, SDK e CLI.
- `ec2`: permite que as entidades principais descrevam VPCs, sub-redes e grupos de segurança. Isso é usado no console AWS de gerenciamento do WorkSpaces Secure Browser 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 AWS de gerenciamento do WorkSpaces Secure Browser para mostrar os streams 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": "*"
        }
    ]
}
```

## AWS política gerenciada: AmazonWorkSpacesWebReadOnly

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

Essa política concede permissões somente para leitura que permitem acesso ao WorkSpaces Secure Browser e suas dependências por meio do AWS Management Console, SDK e CLI. 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`.

> **Note**
>
> Se você estiver usando essa política no momento, mude para a nova `AmazonWorkSpacesSecureBrowserReadOnly` política.

Detalhes das permissões

Esta política inclui as seguintes permissões:

- `workspaces-web`— Fornece acesso somente de leitura ao WorkSpaces Secure Browser e suas dependências por meio do console AWS de gerenciamento, SDK e CLI.
- `ec2`: permite que as entidades principais descrevam VPCs, sub-redes e grupos de segurança. Isso é usado no console AWS de gerenciamento do WorkSpaces Secure Browser 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 AWS de gerenciamento do WorkSpaces Secure Browser para mostrar os streams 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": "*"
        }
    ]
}
```

## WorkSpaces Atualizações do Secure Browser para políticas AWS gerenciadas

Veja detalhes sobre as atualizações das políticas AWS gerenciadas do WorkSpaces Secure Browser 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 |
| --- | --- | --- |
| AmazonWorkSpacesSecureBrowserReadOnly – Nova política | WorkSpaces O Secure Browser adicionou uma nova política para fornecer | 24 de junho de 2024 |

| Alteração | Descrição | Data |
| --- | --- | --- |
| | acesso somente de leitura ao WorkSpaces Secure Browser e suas dependências por meio do AWS Management Console, SDK e CLI. | |
| AmazonWorkSpacesWebServiceRolePolicy: política atualizada | WorkSpaces O Secure Browser atualizou a política CreateNetworkInterface para restringir a marcação com aws:RequestTag/WorkSpacesWebManaged: true e agir nos recursos da sub-rede e do grupo de segurança, bem como restringir DeleteNetworkInterface aos ENIs marcados com aws:ResourceTag/WorkSpacesWebManaged: true. | 15 de dezembro de 2022 |
| AmazonWorkSpacesWebReadOnly: política atualizada | WorkSpaces O Secure Browser atualizou a política para incluir permissões de leitura para o registro de acesso do usuário e para listar streams de dados do Kinesis. Para ter mais informações, consulte the section called “Configurar o registro de acesso do usuário”. | 2 de novembro de 2022 |

| Alteração | Descrição | Data |
| --- | --- | --- |
| AmazonWorkSpacesWebServiceRolePolicy: política atualizada | WorkSpaces O Secure Browser atualizou a política para descrever um resumo dos fluxos de dados do Kinesis e colocar registros nos fluxos de dados do Kinesis para registro de acesso do usuário. Para ter mais informações, consulte the section called “Configurar o registro de acesso do usuário”. | 17 de outubro de 2022 |
| AmazonWorkSpacesWebServiceRolePolicy: política atualizada | WorkSpaces O Secure Browser atualizou a política para criar tags durante a criação do ENI. | 6 de setembro de 2022 |
| AmazonWorkSpacesWebServiceRolePolicy: política atualizada | WorkSpaces O Secure Browser atualizou a política para adicionar o namespace AWS/Usage às permissões da API. PutMetricData | 6 de abril de 2022 |
| AmazonWorkSpacesWebReadOnly – Nova política | WorkSpaces O Secure Browser adicionou uma nova política para fornecer acesso somente de leitura ao WorkSpaces Secure Browser e suas dependências por meio do AWS Management Console, SDK e CLI. | 30 de novembro de 2021 |

| Alteração | Descrição | Data |
| --- | --- | --- |
| AmazonWorkSpacesWebServiceRolePolicy – Nova política | WorkSpaces O Secure Browser adicionou uma nova política para permitir o acesso aos serviços e recursos da AWS usados ou gerenciados pelo WorkSpaces Secure Browser. | 30 de novembro de 2021 |
| WorkSpaces O Secure Browser começou a rastrear as alterações | WorkSpaces O Secure Browser começou a rastrear as alterações em suas políticas AWS gerenciadas. | 30 de novembro de 2021 |

# Solução de problemas de identidade e acesso ao Amazon WorkSpaces Secure Browser

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

Tópicos

- Não estou autorizado a realizar uma ação no WorkSpaces Secure Browser
- Não estou autorizado a realizar iam: PassRole
- Quero permitir que pessoas fora da minha AWS conta acessem os recursos do meu Navegador WorkSpaces Seguro

## Não estou autorizado a realizar uma ação no WorkSpaces Secure Browser

Se você receber uma mensagem de erro informando que não tem autorização para executar uma ação, é preciso atualizar suas políticas para permitir que você realize a ação.

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

```
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 recurso *`my-example-widget`* usando a ação `workspaces-web:GetWidget`.

Se precisar de ajuda, entre em contato com seu AWS administrador. 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 o Navegador WorkSpaces Seguro.

Alguns Serviços da AWS permitem que você passe uma função existente para esse serviço em vez de criar uma nova função de serviço ou uma função vinculada ao serviço. Para fazer isso, é preciso ter permissões para passar o perfil para o serviço.

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

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

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

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

### Quero permitir que pessoas fora da minha AWS conta acessem os recursos do meu Navegador WorkSpaces Seguro

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

Para saber mais, consulte:

- Para saber se o WorkSpaces Secure Browser oferece suporte a esses recursos, consulteComo o Amazon WorkSpaces Secure Browser funciona com IAM.
- Para saber como fornecer acesso aos seus recursos em todos os Contas da AWS que você possui, consulte Fornecer acesso a um IAM usuário em outro Conta da AWS de sua propriedade no Guia do IAM usuário.
- Para saber como fornecer acesso aos seus recursos a terceiros Contas da AWS, consulte Fornecer Contas da AWS acesso a terceiros no Guia do IAM usuário.
- Para saber como fornecer acesso por meio da federação de identidades, consulte Fornecendo acesso a usuários autenticados externamente (federação de identidades) no Guia do IAMusuário.
- Para saber a diferença entre usar funções e políticas baseadas em recursos para acesso entre contas, consulte Acesso a recursos entre contas IAM no Guia do IAM usuário.

## Usando funções vinculadas ao serviço para WorkSpaces o Secure Browser

O Amazon WorkSpaces Secure Browser usa AWS Identity and Access Management funções vinculadas ao serviço (IAM). Uma função vinculada ao serviço é um tipo exclusivo de função do IAM vinculada diretamente ao WorkSpaces Secure Browser. As funções vinculadas ao serviço são predefinidas pelo WorkSpaces Secure Browser e incluem todas as permissões que o serviço exige para chamar outros AWS serviços em seu nome.

Uma função vinculada ao serviço facilita a configuração do Navegador WorkSpaces Seguro porque você não precisa adicionar manualmente as permissões necessárias. WorkSpaces O Navegador Seguro define as permissões de suas funções vinculadas ao serviço e, a menos que seja definido de outra forma, somente o Navegador WorkSpaces Seguro pode assumir suas funções. 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 só pode excluir um perfil vinculado a serviço depois de excluir os recursos relacionados. Isso protege seus recursos do Navegador WorkSpaces Seguro porque você não pode remover inadvertidamente a permissão 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 apresentam Sim na coluna Função vinculada a serviço. Escolha um Sim com um link para visualizar a documentação do perfil vinculado a esse serviço.

## Permissões de função vinculadas ao serviço para WorkSpaces o Secure Browser

WorkSpaces O Secure Browser usa a função vinculada ao serviço chamada `AWSServiceRoleForAmazonWorkSpacesWeb` — O WorkSpaces Secure Browser usa essa função vinculada ao serviço para acessar recursos do Amazon EC2 de contas de clientes para instâncias e métricas de streaming. CloudWatch

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

- `workspaces-web.amazonaws.com`

A política de permissões de função denominada `AmazonWorkSpacesWebServiceRolePolicy` permite que o WorkSpaces Secure Browser conclua as seguintes ações nos recursos especificados. Para ter 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 a serviço. Para mais informações, consulte Permissões de perfil vinculado ao serviço no Guia do usuário do IAM.

## Criação de uma função vinculada ao serviço para WorkSpaces o Secure Browser

Não é necessário criar manualmente uma função vinculada a serviço. Quando você cria seu primeiro portal na AWS Management Console, na ou na AWS API AWS CLI, o WorkSpaces Secure Browser cria a função vinculada ao serviço para você.

> **Important**
>
> Esse perfil vinculado ao serviço pode aparecer em sua conta se você concluiu uma ação em outro serviço que usa os atributos compatíveis com esse perfil.

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 Secure Browser cria a função vinculada ao serviço para você novamente.

Você também pode usar o console do IAM para criar uma função vinculada ao serviço com o caso de uso do WorkSpaces Secure Browser. Na AWS CLI ou na AWS API, crie uma função vinculada ao serviço com o nome do `workspaces-web.amazonaws.com` serviço. 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.

## Editando uma função vinculada ao serviço para WorkSpaces o Secure Browser

WorkSpaces O Secure Browser não permite que você edite a função `AWSServiceRoleForAmazonWorkSpacesWeb` vinculada ao serviço. Depois que você criar um perfil vinculado ao serviço, não poderá alterar o nome do perfil, pois várias entidades podem fazer

referência ao perfil. No entanto, você poderá editar a descrição do perfil usando o IAM. Para obter mais informações, consulte Editar uma função vinculada a serviço no Guia do usuário do IAM.

## Excluindo uma função vinculada ao serviço para o Secure Browser WorkSpaces

Se você não precisar mais usar um recurso ou serviço que requer um perfil vinculado ao serviço, é recomendável excluí-lo. 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 Navegador WorkSpaces Seguro estiver usando a função quando você tentar excluir os recursos, a exclusão poderá falhar. Se isso acontecer, espere alguns minutos e tente a operação novamente.

Para excluir os recursos do Navegador WorkSpaces Seguro usados pelo 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 a serviço usando o IAM

Use o console do IAM AWS CLI, o ou a AWS API para excluir a função AWSServiceRoleForAmazonWorkSpacesWeb vinculada ao serviço. Para mais informações, consulte Excluir um perfil vinculado ao serviço no Guia do usuário do IAM.

## Regiões suportadas para funções vinculadas ao serviço WorkSpaces Secure Browser

WorkSpaces O Secure Browser oferece suporte ao uso de funções vinculadas ao serviço em todas as regiões em que o serviço está disponível. Para obter mais informações, consulte Regiões e endpoints da AWS.

# Resposta a incidentes no Amazon WorkSpaces Secure Browser

Você pode detectar incidentes monitorando a CloudWatch métrica da `SessionFailure` Amazon. Para receber alertas de incidentes, use um CloudWatch alarme para a `SessionFailure` métrica. Para ter mais informações, consulte Monitorando o Amazon WorkSpaces Secure Browser com a Amazon CloudWatch.

# Validação de conformidade para o Amazon WorkSpaces Secure Browser

Para saber se um AWS service (Serviço da AWS) está dentro do escopo de programas de conformidade específicos, consulte Serviços da AWS Escopo por Programa de Conformidade Serviços da AWS e escolha o programa de conformidade em que você está interessado. Para obter informações gerais, consulte Programas de AWS conformidade Programas AWS de .

Você pode baixar relatórios de auditoria de terceiros usando AWS Artifact. Para obter mais informações, consulte Baixar relatórios em AWS Artifact .

Sua responsabilidade de conformidade ao usar Serviços da AWS é determinada pela confidencialidade de seus dados, pelos objetivos de conformidade de sua empresa e pelas leis e regulamentações aplicáveis. AWS fornece os seguintes recursos para ajudar na conformidade:

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

> **Note**
>
> Nem todos Serviços da AWS são HIPAA elegíveis. Para obter mais informações, consulte a Referência de serviços HIPAA elegíveis.

- AWS Recursos de https://aws.amazon.com/compliance/resources/ de conformidade — Essa coleção de pastas de trabalho e guias pode ser aplicada ao seu setor e local.
- AWS Guias de conformidade do cliente — Entenda o modelo de responsabilidade compartilhada sob a ótica da conformidade. Os guias resumem as melhores práticas de proteção Serviços da

AWS e mapeiam as diretrizes para controles de segurança em várias estruturas (incluindo o Instituto Nacional de Padrões e Tecnologia (NIST), o Conselho de Padrões de Segurança do Setor de Cartões de Pagamento (PCI) e a Organização Internacional de Padronização ()). ISO

- Avaliação de recursos com regras no Guia do AWS Config desenvolvedor — O AWS Config serviço avalia o quão bem suas configurações de recursos estão em conformidade com as práticas internas, as diretrizes e os regulamentos do setor.
- AWS Security Hub— Isso AWS service (Serviço da AWS) fornece uma visão abrangente do seu estado de segurança interno AWS. O Security Hub usa controles de segurança para avaliar os recursos da AWS e verificar a conformidade com os padrões e as práticas recomendadas do setor de segurança. Para obter uma lista dos serviços e controles aceitos, consulte a Referência de controles do Security Hub.
- Amazon GuardDuty — Isso AWS service (Serviço da AWS) detecta possíveis ameaças às suas cargas de trabalho Contas da AWS, contêineres e dados monitorando seu ambiente em busca de atividades suspeitas e maliciosas. GuardDuty pode ajudá-lo a atender a vários requisitos de conformidade, por exemplo PCIDSS, atendendo aos requisitos de detecção de intrusões exigidos por determinadas estruturas de conformidade.
- AWS Audit Manager— Isso AWS service (Serviço da AWS) ajuda você a auditar continuamente seu AWS uso para simplificar a forma como você gerencia o risco e a conformidade com as regulamentações e os padrões do setor.

# Resiliência no Amazon WorkSpaces Secure Browser

A infraestrutura AWS global é construída em torno Regiões da AWS de zonas de disponibilidade. Regiões da AWS fornecem várias zonas de disponibilidade fisicamente separadas e isoladas, conectadas a redes de baixa latência, alta taxa de transferência e alta redundância. Com as zonas de disponibilidade, é possível projetar e operar aplicações e bancos de dados que automaticamente executam o failover entre as zonas sem interrupção. As zonas de disponibilidade são mais altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de datacenter tradicionais.

Para obter mais informações sobre zonas de disponibilidade Regiões da AWS e zonas de disponibilidade, consulte Infraestrutura AWS global.

No momento, o WorkSpaces Secure Browser não oferece suporte aos itens a seguir:

- 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 Secure Browser

Como um serviço gerenciado, o Amazon WorkSpaces Secure Browser é protegido pela segurança de rede AWS global. Para obter informações sobre serviços AWS de segurança e como AWS proteger a infraestrutura, consulte AWS Cloud Security. Para projetar seu AWS ambiente usando as melhores práticas de segurança de infraestrutura, consulte Proteção de infraestrutura no Security Pillar AWS Well-Architected Framework.

Você usa API chamadas AWS publicadas para acessar o Amazon WorkSpaces Secure Browser pela rede. Os clientes devem oferecer suporte para:

- Segurança da camada de transporte (TLS). Exigimos TLS 1,2 e recomendamos TLS 1,3.
- Suítes de criptografia com sigilo direto perfeito (), como (Ephemeral PFS Diffie-Hellman) ou DHE (Elliptic Curve Ephemeral Diffie-Hellman). ECDHE A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

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

WorkSpaces O Secure Browser isola o tráfego do serviço aplicando a autenticação e autorização AWS SigV4 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 sub-rede ou grupo de segurança. VPC Atualmente, não há suporte para multilocação e VPC endpoints (PrivateLink).

# Análise de configuração e vulnerabilidade no Amazon WorkSpaces Secure Browser

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

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

# Melhores práticas de segurança para o Amazon WorkSpaces Secure Browser

O Amazon WorkSpaces Secure Browser fornece vários recursos de segurança que você pode usar ao desenvolver e implementar suas próprias políticas de segurança. As melhores práticas a seguir são diretrizes gerais e não representam uma solução completa de segurança. Como essas melhores práticas podem não ser adequadas ou suficientes para o seu ambiente, trate-as como considerações úteis em vez de prescrições.

As melhores práticas para o Amazon WorkSpaces Secure Browser incluem o seguinte:

- Para detectar possíveis eventos de segurança associados ao uso do WorkSpaces Secure Browser, use AWS CloudTrail CloudWatch a Amazon para detectar e rastrear o histórico de acesso e os registros de processos. Para obter mais informações, consulte Monitorando o Amazon WorkSpaces Secure Browser com a Amazon CloudWatch e Registrando chamadas da API do WorkSpaces Secure Browser usando AWS CloudTrail.
- Para implementar controles de detetive e identificar anomalias, use CloudTrail registros e métricas. CloudWatch Para obter mais informações, consulte Monitorando o Amazon WorkSpaces Secure Browser com a Amazon CloudWatch e Registrando chamadas da API do WorkSpaces Secure Browser usando AWS CloudTrail.

- É possível configurar o registro em log de acesso do usuário para registrar os eventos do usuário. Para ter mais informações, consulte the section called “Configurar o registro de acesso do usuário”.

Para evitar possíveis eventos de segurança associados ao uso do WorkSpaces Secure Browser, siga estas melhores práticas:

- Implemente o acesso com privilégios mínimos e crie funções específicas para serem usadas nas ações do Navegador WorkSpaces Seguro. Use modelos do IAM para criar um perfil de acesso total ou somente leitura. Para ter mais informações, consulte AWS políticas gerenciadas para o WorkSpaces Secure Browser.
- 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.

# Monitorando o Amazon WorkSpaces Secure Browser

O monitoramento é uma parte importante da manutenção da confiabilidade, disponibilidade e desempenho do Amazon WorkSpaces Secure Browser e de suas outras AWS soluções. AWS fornece as seguintes ferramentas de monitoramento para monitorar seus portais do WorkSpaces Secure Browser 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 CloudTrailcaptura 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 mais informações, consulte o Guia do usuário do AWS CloudTrail.

Tópicos

# Monitorando o Amazon WorkSpaces Secure Browser com a Amazon CloudWatch

Você pode monitorar o Amazon WorkSpaces Secure Browser 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 o Amazon WorkSpaces Secure Browser

| Métrica | Descrição | Dimensões | Statistics | Unidades |
|---|---|---|---|---|
| `SessionAttempt` | O número de tentativas de sessão do Amazon WorkSpaces Secure Browser. | `PortalId` | Média, Soma, Máximo, Mínimo | Contagem |
| `SessionSuccess` | O número de sessões bem-sucedidas do Amazon WorkSpaces Secure Browser começa. | `PortalId` | Média, Soma, Máximo, Mínimo | Contagem |
| `SessionFailure` | O número de sessões com falha do Amazon WorkSpaces Secure Browser começa. | `PortalId` | Média, Soma, Máximo, Mínimo | Contagem |

| Métrica | Descrição | Dimensões | Statistics | Unidades |
| --- | --- | --- | --- | --- |
| `GlobalCpuPercent` | O uso da CPU da instância de sessão do Amazon WorkSpaces Secure Browser. | `PortalId` | Média, Soma, Máximo, Mínimo | Percentual |
| `GlobalMemoryPercent` | O uso da memória (RAM) da instância de sessão do Amazon WorkSpaces Secure Browser. | `PortalId` | Média, Soma, Máximo, Mínimo | Percentual |

> **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.

# Registrando chamadas da API do WorkSpaces Secure Browser usando AWS CloudTrail

WorkSpaces O Secure Browser é integrado com AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, função ou AWS serviço no Amazon WorkSpaces Secure Browser. CloudTrail captura todas as chamadas de API para o Amazon WorkSpaces Secure Browser como eventos. Isso inclui chamadas do console do Amazon WorkSpaces Secure Browser e chamadas de código para operações da API do Amazon WorkSpaces Secure Browser. Se você criar uma trilha, poderá habilitar a entrega contínua de CloudTrail eventos para um bucket do Amazon S3, incluindo eventos para o Amazon WorkSpaces Secure Browser. Se você não configurar uma trilha, ainda poderá ver os eventos mais recentes no CloudTrail console no Histórico de eventos. Usando as informações coletadas por CloudTrail, você pode identificar a solicitação que foi feita ao

Amazon WorkSpaces Secure Browser, o endereço IP a partir do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita, bem como detalhes adicionais.

Para saber mais sobre isso CloudTrail, consulte o Guia AWS CloudTrail do usuário.

## WorkSpaces Informações do Navegador Seguro em CloudTrail

CloudTrail é ativado em sua AWS conta quando você cria a conta. Quando a atividade ocorre no Amazon WorkSpaces Secure Browser, essa atividade é registrada em um CloudTrail evento junto com outros eventos AWS de serviço no histórico de eventos. No Histórico de eventos, você pode visualizar, pesquisar e baixar eventos recentes em sua AWS conta. Para obter mais informações, consulte Visualização de eventos com histórico de CloudTrail eventos.

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

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

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

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

- Se a solicitação foi feita com credenciais de usuário raiz ou do usuário do IAM.
- Se a solicitação foi feita com credenciais de segurança temporárias de um perfil ou de um usuário federado.

- Se a solicitação foi feita por outro AWS serviço.

Para obter mais informações, consulte o elemento CloudTrail userIdentity.

## Entendendo as entradas do arquivo de log do WorkSpaces Secure Bro

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

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


```
{
   "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

O Amazon WorkSpaces Secure Browser permite que os clientes registrem eventos da sessão, incluindo início, parada e visitas de 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 do WorkSpaces Secure Browser

Os administradores usam o WorkSpaces Secure Browser para criar portais da Web que se conectam aos sites da empresa, como sites internos, aplicativos da 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 o WorkSpaces Secure Browser, iniciar e configurar uma sessão e usar a barra de ferramentas e o navegador da web.

Tópicos



## Compatibilidade de navegadores e dispositivos

O Amazon WorkSpaces Secure Browser 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

Depois de entrar para iniciar uma sessão, você verá a mensagem de Inicialização da sessão e a barra de progresso. Isso indica que o Amazon WorkSpaces Secure Browser está criando uma sessão para você. Nos bastidores, o Amazon WorkSpaces Secure Browser 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.

- Ative o Amazon WorkSpaces Secure Browser para abrir 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 aumentar o tamanho da tela, selecione a janela do navegador e aumente o zoom. Para aumentar o tamanho de exibição dos ícones e do texto da barra de ferramentas, selecione a barra de ferramentas e aumente o zoom.

Para aumentar ou diminuir o zoom em um dispositivo Windows, siga estas etapas:

1. Selecione a barra de ferramentas ou o conteúdo da web.
2. Pressione Ctrl + para ampliar ou pressione Ctrl + - para diminuir o zoom.

Para aumentar ou diminuir o zoom em um dispositivo Mac, siga estas etapas:

1. Selecione a barra de ferramentas ou o conteúdo da web.
2. Pressione Cmd + + para ampliar ou pressione Cmd + - para diminuir o zoom.

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 |
|---|---|---|
|  | **Windows** | Move between windows or launch additional browser windows. |
|  | **Launch additional monitor window** | Launch an additional monitor window with a separate browser window. Then drag to your secondary monitor. |
|  | **Full screen** | Launch a full screen experience view. |
|  | **Microphone** | Activate mic input for the session. |
|  | **Preferences** | Access the **General** and **Keyboard** menus. From the **General** 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 **Keyboard** menu, change the option and command key settings (on Mac devices), or activate **Functions** (see below). |
|  | **Profile** | End your session, view performance metrics, access **Feedback** and **Help**, and learn about Amazon WorkSpaces Web. **End Session** ends the Amazon WorkSpaces Web session.<br><br>**Performance metrics** displays the frame rate, network latency, and bandwidth usage graph. This information is useful for administrators when investigating issues with the service.<br><br>**Feedback** provides you with an email address to share feedback to the Amazon WorkSpaces Web team.<br><br>**Help** 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.<br><br>**About** provides more information about Amazon WorkSpaces Web. |
|  | **Notifications** | Get one-click access to session notifications. |
|  | **Clipboard** | 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 administator. |
|  | **Files** | 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 **Files** are deleted at the end of the session. This icon only displays if **Files** permission is granted by your administator. |

> **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, o Amazon WorkSpaces Secure Browser 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 do Amazon WorkSpaces Secure Browser 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 do Amazon WorkSpaces Secure Browser 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

O Amazon WorkSpaces Secure Browser 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.

O Amazon WorkSpaces Secure Browser 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 entrar no portal, siga as instruções para instalar a extensão no seu navegador Chrome ou Firefox. 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 janela 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 Secure Browser instalada em seu navegador. Se você excluiu os dados do navegador, talvez tenha removido a extensão acidentalmente.
2. Certifique-se de que você não esteja usando a Navegação 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 Guia de administração do Amazon WorkSpaces Secure Browser

A tabela a seguir descreve os lançamentos da documentação do Amazon WorkSpaces Secure Browser.

| Alteração | Descrição | Data |
| --- | --- | --- |
| Permitir links diretos | Permita que os portais recebam links diretos que conectam usuários a um site específico durante uma sessão. | 25 de junho de 2024 |
| Atualização da política gerenciada | Política AmazonWorkSpacesSecureBrowserReadOnly gerenciada adicionada | 24 de junho de 2024 |
| Use a barra de ferramentas para ampliar | Você pode aumentar o tamanho da tela, dos ícones e do texto com a barra de ferramentas. | 1º de maio de 2024 |
| Novas configurações do portal da web | Agora você pode especificar o tipo de instância e o limite máximo de usuários simultâneos para seu portal da web. | 22 de abril de 2024 |
| CloudWatch métricas | Adicionado GlobalCpuPercent e GlobalMemoryPercent métricas. | 26 de fevereiro de 2024 |
| Configurar a filtragem de URL | Você pode usar a Política do Chrome para filtrar quais URLs os usuários podem | 21 de fevereiro de 2024 |

| | | |
|---|---|---|
| | acessar a partir do navegador remoto. | |
| Tipos de autenticação IdP | Você pode escolher o tipo de autenticação padrão ou o do IAM Identity Center. | 5 de fevereiro de 2024 |
| Habilitar extensão de autenticação única | É possível habilitar uma extensão para que os usuários finais tenham uma melhor experiência de login no portal. | 28 de agosto de 2023 |
| Orientação do usuário para o Amazon WorkSpaces Secure Browser | Conteúdo adicionado para ajudar a orientar os usuários finais que desejam saber mais sobre como acessar o Amazon WorkSpaces Secure Browser, iniciar e configurar uma sessão e usar a barra de ferramentas e o navegador da web. | 17 de julho de 2023 |
| Controles de acesso de IP | WorkSpaces O Navegador Seguro permite que você controle de quais endereços IP seu portal da web pode ser acessado. | 31 de maio de 2023 |
| Atualização da política gerenciada | Política AmazonWorkSpacesWebReadOnly gerenciada atualizada | 15 de maio de 2023 |
| Configurar a atualização do provedor de identidades | WorkSpaces O Secure Browser oferece dois tipos de autenticação: Padrão e AWS IAM Identity Center | 15 de março de 2023 |

| | | |
|---|---|---|
| Atualização da política do navegador | Seção de política do navegador atualizada e reestruturada | 31 de janeiro de 2023 |
| Atualização da política gerenciada | Política AmazonWorkSpacesWebServiceRolePolicy gerenciada atualizada | 15 de dezembro de 2022 |
| Lista de permissões e lista de bloqueio | 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 |
| Atualização da política gerenciada | Política AmazonWorkSpacesWebReadOnly gerenciada atualizada | 2 de novembro de 2022 |
| Atualização da política gerenciada | Política AmazonWorkSpacesWebServiceRolePolicy gerenciada atualizada | 24 de outubro de 2022 |
| Registro em log do acesso do usuário | Configurar o registro em log de acesso do usuário para registrar eventos do usuário | 17 de outubro de 2022 |
| Atualizações de rede | Várias atualizações na seção “Redes e acesso” | 22 de setembro de 2022 |
| Atualização da política gerenciada | Política AmazonWorkSpacesWebServiceRolePolicy gerenciada atualizada | 6 de setembro de 2022 |

| | | |
|---|---|---|
| Configurar sessões do usuário | Configurar o Input Method Editor (IME) e a localização na sessão | 28 de julho de 2022 |
| Atualizações de rede | Várias atualizações na seção “Redes e acesso” | 7 de julho de 2022 |
| Valores de tempo limite | Especifique o Tempo limite de desconexão em minutos e o Tempo limite de desconexão de inatividade em minutos | 16 de maio de 2022 |
| Política gerenciada atualizada | Atualizou a política AmazonWorkSpacesWebServiceRolePolicy gerenciada para adicionar o namespace AWS/Usage às permissões da API PutMetricData | 6 de abril de 2022 |
| Perfil vinculado ao serviço | Nova função AWSServiceRoleForAmazonWorkSpacesWeb vinculada ao serviço | 30 de novembro de 2021 |
| Política gerenciada | Nova política AmazonWorkSpacesWebReadOnly gerenciada | 30 de novembro de 2021 |
| Política gerenciada | Nova política AmazonWorkSpacesWebServiceRolePolicy gerenciada | 30 de novembro de 2021 |
| Lançamento inicial | Versão inicial do Guia de Administração do Navegador WorkSpaces Seguro | 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.