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-serviceSaaS), 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 WorkSpaces Applications, 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 lançamento do Amazon WorkSpaces Secure Browser

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 obter mais informações, consulte the section called “Monitoramento com CloudWatch”.
- Service endpoints. 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.
- Perfil vinculado ao serviço contendo workspaces-web. Para obter mais informações, consulte the section called “Uso de perfis vinculados ao serviço”.
- Console URLs contendo espaços de trabalho-web.
- Documentação URLs contendo workspaces-web. Para obter mais informações, consulte a documentação do Amazon WorkSpaces Secure Browser.
- Função ReadOnly gerenciada existente. Para obter 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, o portal existente URLs permanece o mesmo. URLs <UUID>para portais criados antes de 20 de maio de 2024, usei 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 Amazon 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 os 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 o PCAs em sua loja 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 repositório 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.

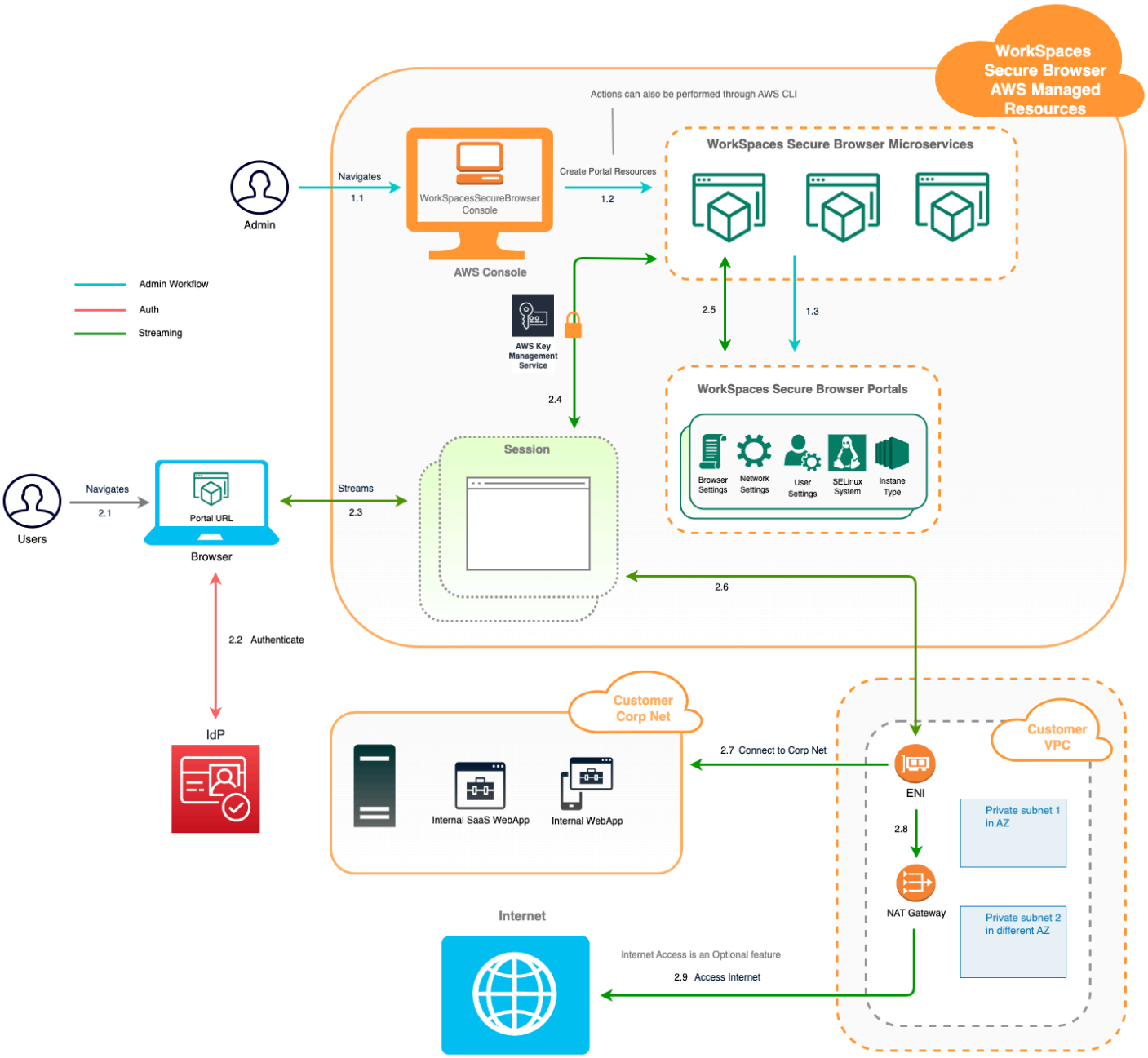
AWS serviços relacionados ao Amazon WorkSpaces Secure Browser

Existem vários AWS serviços relacionados ao WorkSpaces Secure Browser.

WorkSpaces O Secure Browser é um recurso da Amazon WorkSpaces no portfólio de computação para usuários AWS finais. 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 do Amazon WorkSpaces Secure Browser

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



Acessando o Amazon WorkSpaces Secure Browser

Você pode acessar o WorkSpaces Secure Browser de várias maneiras.

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 Amazon WorkSpaces Secure Browser

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 a https://portal.aws.amazon.com/billing/inscrição.
2. Siga as instruções online.

   Parte do procedimento de inscrição envolve receber uma chamada telefônica ou uma mensagem de texto e inserir um código de verificação pelo 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 recursos 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, você pode visualizar a atividade atual da sua conta e gerenciar sua conta acessando https://aws.amazon.com/e escolhendo 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 Centro de Identidade do AWS IAM, 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 Console de gerenciamento da AWScomo proprietário da conta escolhendo Usuário raiz e inserindo seu endereço de Conta da AWS e-mail. Na próxima página, insira a 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. Habilita o Centro de Identidade do IAM.

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

Iniciar sessão como o usuário com acesso administrativo

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

  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 Criar um conjunto de permissões no Guia do usuário do Centro de Identidade do AWS IAM .
2. Atribua usuários a um grupo e, em seguida, atribua o acesso de logon único ao grupo.

   Para obter instruções, consulte Adicionar grupos no Guia do usuário do Centro de Identidade do AWS IAM .

Conceder acesso programático

Os usuários precisam de acesso programático se quiserem interagir com pessoas AWS fora do Console de gerenciamento da AWS. 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
IAM	(Recomendado) Use as credenciais do console como credenciais temporárias para assinar solicitações programáticas para o AWS CLI, AWS SDKs ou. AWS APIs	Siga as instruções da interface que deseja utilizar. • Para o AWS CLI, consulte Login para desenvolvimento AWS local no Guia AWS Command Line Interface do usuário. • Para AWS SDKs isso, consulte Login para desenvolvimento AWS local no Guia de referência de ferramentas AWS SDKs e ferramentas.

Qual usuário precisa de acesso programático?	Para	Por
Identidade da força de trabalho (Usuários gerenciados no Centro de Identidade do IAM)	Use credenciais temporárias para assinar solicitações programáticas para o AWS CLI AWS SDKs, ou. AWS APIs	Siga as instruções da interface que deseja utilizar. • Para o AWS CLI, consulte Configurando o AWS CLI para uso Centro de Identidade do AWS IAM no Guia do AWS Command Line Interface usuário. • Para AWS SDKs, ferramentas e AWS APIs, consulte a autenticação do IAM Identity Center no Guia de referência de ferramentas AWS SDKs e ferramentas.
IAM	Use credenciais temporárias para assinar solicitações programáticas para o AWS CLI AWS SDKs, ou. AWS APIs	Siga as instruções em Como usar credenciais temporárias com AWS recursos no Guia do usuário do IAM.

Qual usuário precisa de acesso programático?	Para	Por
IAM	(Não recomendado) Use credenciais de longo prazo para assinar solicitaç ões programáticas para o AWS CLI, AWS SDKs, ou. AWS APIs	Siga as instruções da interface que deseja utilizar. • Para isso AWS CLI, consulte Autenticação usando credenciais de usuário do IAM no Guia do AWS Command Line Interface usuário. • Para ferramentas AWS SDKs e ferramentas, consulte Autenticar usando credenciais de longo prazo no Guia de referência de ferramentas AWS SDKs e ferramentas. • Para isso AWS APIs, consulte Gerenciamento de chaves de acesso para usuários do IAM no Guia do usuário do IAM.

Rede para o Amazon WorkSpaces Secure Browser

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

- Configurando uma VPC para o Amazon WorkSpaces Secure Browser
- Habilitando conexões de usuários para o Amazon WorkSpaces Secure Browser

Configurando uma VPC para o Amazon WorkSpaces Secure Browser

Para instalar e configurar uma VPC para o WorkSpaces Secure Browser, conclua as etapas a seguir.

Tópicos

Requisitos de VPC para o Amazon Secure WorkSpaces Browser

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 aos seguintes requisitos:

- A VPC deve ter locação padrão. VPCs com locação dedicada não são suportadas.
- 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 obter mais informações, consulte Criação de uma nova VPC para o Amazon WorkSpaces Secure Browser.
- 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 obter mais informações, consulte Criação de uma nova VPC para o Amazon WorkSpaces Secure Browser.

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. Habilitar a navegação irrestrita na Internet para o Amazon WorkSpaces Secure Browser (recomendado)

Criação de uma nova VPC para o Amazon WorkSpaces Secure Browser

Esta seção descreve como usar o assistente de VPC para criar rapidamente uma VPC com sub-redes públicas e privadas. O assistente cria automaticamente um gateway de internet, um gateway NAT, e configura tabelas de rotas para suas sub-redes.

Para obter mais informações sobre essa configuração, consulte Exemplo: VPC com servidores em sub-redes privadas e NAT.

Tópicos

Configuração rápida de VPC (1 minuto)

Conclua as etapas a seguir para criar rapidamente uma VPC dedicada para o WorkSpaces Secure Browser com sub-redes públicas e privadas para acesso à Internet. Se você quiser usar uma VPC existente, verifique Requisitos de VPC para o Amazon Secure WorkSpaces Browser se ela atende aos requisitos.

> **Note**
>
> Verifique se você está no local desejado Região da AWS. Você pode alterar a região no console, se necessário.

Para configurar rapidamente uma VPC

1. Abra o assistente de criação de VPC: crie uma VPC com recursos. Mantenha todas as configurações como padrão, a menos que especificado abaixo:

   - Em Resource to create, selecione VPC e muito mais.
   - Em Tag de nome, selecione gerar automaticamente e insira um nome descritivo para sua VPC (por exemplo,). **`WSB-VPC`**
   - Para o bloco IPv4 CIDR, por padrão, a **`10.0.0.0/16`** VPC usa. Você pode especificar um bloco IPv4 CIDR diferente, se necessário.

- Em Locação, selecione Padrão (VPCs não há suporte para locação dedicada).
- Em Número de zonas de disponibilidade (AZs), selecione 2.
  - Expanda Personalizar AZs e selecione duas zonas de disponibilidade diferentes que são suportadas pelo WorkSpaces Secure Browser. Para obter a lista dos compatíveis AZs, consulteZonas de disponibilidade suportadas para o Amazon WorkSpaces Secure Browser.
- Em Número de sub-redes públicas, selecione 2.
- Em Número de sub-redes privadas, selecione 2.
- Para blocos CIDR de sub-rede, se você precisar personalizar os blocos CIDR em suas sub-redes, expanda Personalizar blocos CIDR de sub-redes. Certifique-se de que cada sub-rede tenha endereços IP suficientes para o tráfego esperado.
- Para gateways NAT, selecione Regional para permitir o acesso à Internet para sub-redes privadas em todas as zonas de disponibilidade.
- Para VPC endpoints, selecione Nenhum. Se você precisar de acesso direto ao S3 sem passar pelo gateway NAT, selecione S3 Gateway.
- Para opções de DNS, mantenha as opções de DNS ativadas (padrão) para garantir a resolução adequada de nomes em sua VPC.

2. Examine o painel de visualização e escolha Criar VPC.

> **Note**
>
> Cobranças adicionais se aplicam a gateways NAT e endpoints VPC. Para obter mais informações, consulte a página de preços da VPC.

Verificando suas tabelas de rotas de sub-rede (opcional)

O assistente de VPC configura automaticamente as tabelas de rotas para você. Se você criou sua VPC manualmente ou deseja confirmar a configuração, pode verificar se os detalhes a seguir estão corretos para 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 uma sub-rede pública. Por exemplo, WSB-VPC-Subnet-Public1-US-East-1a.
2. Na Tabela de rotas, escolha o ID da tabela de rotas. Por exemplo, rtb-12345678.
3. Selecione a tabela de rotas. 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)	Alvo	Description
Bloco IPv4 CIDR de sub-rede pública (por exemplo, 10.0.0/20)	Local	Todo o tráfego dos recursos destinados aos IPv4 endereços dentro do bloco IPv4 CIDR da sub-rede pública. Esse tráfego é roteado localmente dentro da VPC.
Tráfego destinado a todos os outros IPv4 endereços (por exemplo, 0.0.0.0/0)	Saída (igw-ID)	O tráfego destinado a todos os outros IPv4 endereços é roteado para o gateway da Internet (identificado pelo iGW-ID) que foi criado pelo assistente de VPC.

5. No painel de navegação, escolha Sub-redes. Em seguida, selecione uma sub-rede privada (por exemplo,**`WSB-VPC-subnet-private1-us-east-1a`**).
6. Na guia Tabela de rotas, escolha o ID da tabela de rotas.

7. Selecione a tabela de rotas. Em Nome, escolha o ícone de edição (lápis) e insira um nome para a tabela. Por exemplo, insira o nome **`WSB-VPC-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)	Alvo	Description
Bloco IPv4 CIDR de sub-rede pública (por exemplo, 10.0.0/20)	Local	Todo o tráfego dos recursos destinados aos IPv4 endereços dentro do bloco IPv4 CIDR da sub-rede pública é roteado localmente na VPC.
Tráfego destinado a todos os outros IPv4 endereços (por exemplo, 0.0.0.0/0)	Saída (nat-ID)	O tráfego destinado a todos os outros IPv4 endereços é roteado para o gateway NAT (identificado pelo 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.

Habilitando a navegação na Internet para o Amazon WorkSpaces Secure Browser

Você pode optar por ativar a navegação irrestrita na Internet (a opção recomendada) ou a navegação restrita na Internet.

Tópicos

- Habilitar a navegação irrestrita na Internet para o Amazon WorkSpaces Secure Browser (recomendado)
- Habilitando a navegação restrita na Internet para o Amazon WorkSpaces Secure Browser
- Portas de conectividade com a Internet para o Amazon WorkSpaces Secure Browser

Habilitar a navegação irrestrita na Internet para o Amazon WorkSpaces Secure Browser (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 Criação de uma nova VPC para o Amazon WorkSpaces Secure Browser.

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 VPC com sub-redes privadas, consulte. the section called “Configuração rápida de VPC”

   > **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.

Habilitando a navegação restrita na Internet para o Amazon WorkSpaces Secure Browser

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 obter mais informações, consulte the section called “Navegação irrestrita na Internet”. 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 gateway 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 representará 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 precisar 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 de permissões de domínio e filtragem de conteúdo.

Essa solução oferece a você os seguintes benefícios:

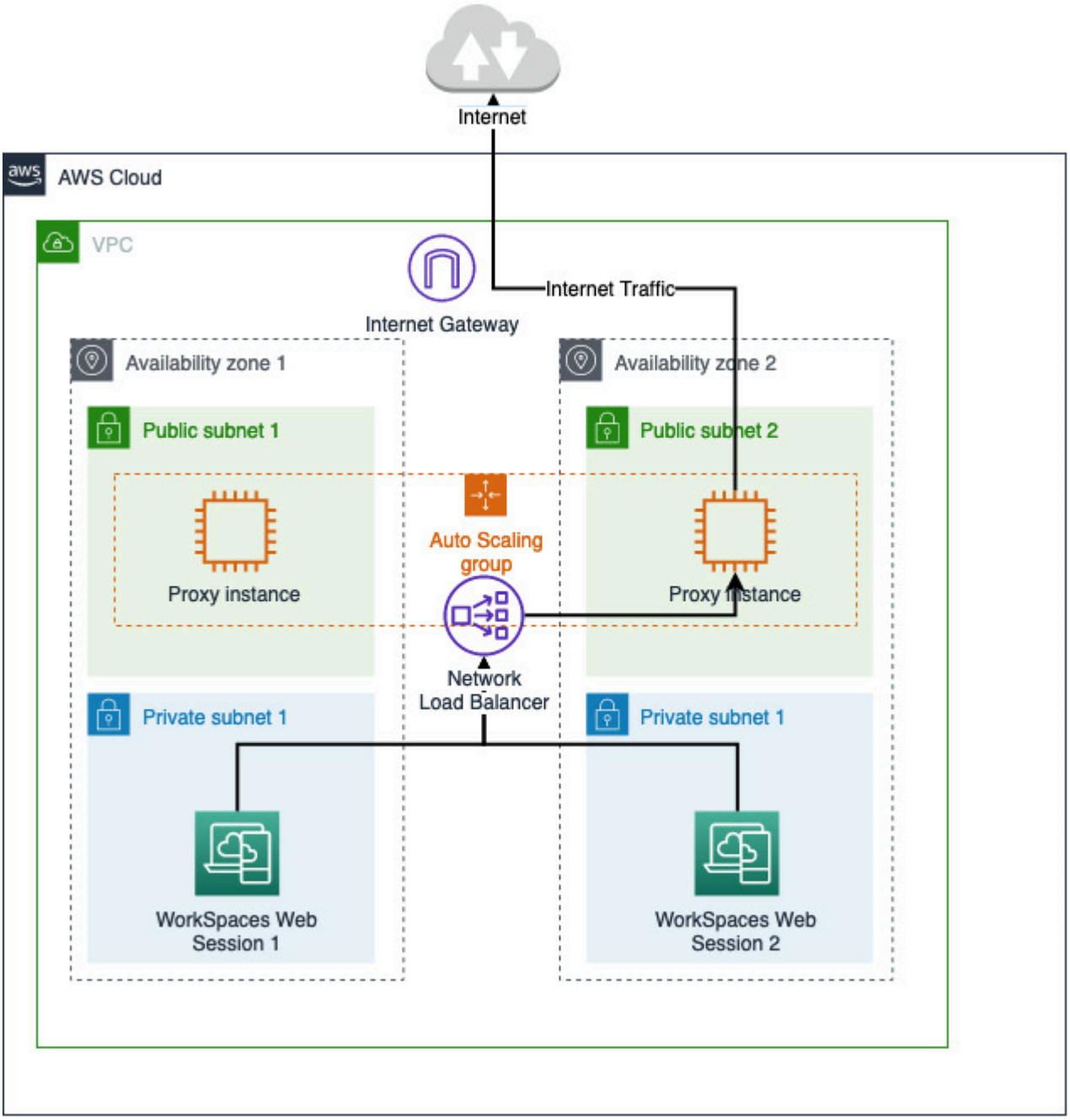
- Um proxy de saída que inclui um grupo de instâncias do Amazon EC2 com ajuste de escala automático, hospedadas por um balanceador de carga de rede. As instâncias de proxy residem em uma sub-rede pública e cada uma delas é conectada com um IP elástico, para permitir o acesso à Internet.

- 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.

Tópicos

Arquitetura de navegação restrita na Internet para o Amazon WorkSpaces Secure Browser

Veja a seguir um exemplo de uma configuração de proxy típica na sua VPC. A instância de proxy do Amazon EC2 está em sub-redes públicas e associada ao IP elástico, portanto, elas têm acesso à Internet. Um balanceador de carga de rede hospeda um grupo de instâncias de proxy com ajuste de escala automático. 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 de navegação restrita na Internet para o Amazon Secure Browser WorkSpaces

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

- 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 VPC, consulte Padrão. VPCs

- 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 um proxy existente, certifique-se de que ele também tenha um único endpoint acessível a partir de suas sub-redes privadas.

Proxy de saída HTTP para o Amazon 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 de permissões de domínio e filtragem de conteúdo.
   a. Siga as etapas em “Instalação (configuração única)” para implantar o CloudFormation modelo em sua conta. Certifique-se de escolher a VPC e as sub-redes corretas como parâmetros do modelo. CloudFormation
   b. Após a implantação, encontre o parâmetro CloudFormation de saída OutboundProxyDomainOutboundProxyPorte. Esse é o nome e a porta DNS do seu proxy.
   c. Se você já tem seu próprio proxy, pule esta etapa e use o nome e a porta DNS do seu proxy.
2. 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 campo `ProxyServer` 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 que 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 de navegação restrita na Internet para o Amazon WorkSpaces Secure Browser

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 formatação a seguir para o campo `ProxyServer` 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.

Portas de conectividade com a Internet para o Amazon WorkSpaces Secure Browser

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

Melhores práticas de VPC para o Secure Browser WorkSpaces

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 de cota, você pode usar o console Service Quotas em. https://console.aws.amazon.com/servicequotas/ Para obter informações sobre as cotas padrão do WorkSpaces Secure Browser, consultethe section called “Gerenciar cotas de serviço”.
- Se você planeja conceder acesso à internet para suas sessões de streaming, é recomendável configurar 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 ENIs por região é 5000. 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 ENIs que pode ser necessário 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.

Sub-redes

- 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 de VPC e 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 obter mais informações, consulte the section called “Criar 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 suportadas para o Amazon WorkSpaces Secure Browser

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 do AZ IDs permite determinar a localização dos 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 as AZ IDs que você pode usar para cada região. Para ver o mapeamento de AZ IDs para zonas de disponibilidade em sua conta, consulte AZ IDs para seus recursos no Guia do AWS RAM usuário.

Nome da região	Código da região	AZ suportado IDs
Leste dos EUA (N. 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`
Ásia-Pacífico (Mumbai)	`ap-south-1`	`aps1-az1`, `aps1-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`

Nome da região	Código da região	AZ suportado IDs
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 AZ IDs, consulte Regiões, Zonas de disponibilidade e Zonas Locais no Guia do usuário do Amazon EC2.

Habilitando conexões de usuários para o Amazon WorkSpaces Secure Browser

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 para o Amazon WorkSpaces Secure Browser.

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 o Amazon WorkSpaces Secure Browser
- Domínios permitidos para o Amazon WorkSpaces Secure Browser

Requisitos de endereço IP e porta para o Amazon WorkSpaces Secure Browser

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 para o Amazon WorkSpaces Secure Browser.
- 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 o Amazon WorkSpaces Secure Browser

Para que os usuários possam acessar portais da Web pelo navegador local, você deve adicionar os domínios a seguir à lista de permissões na rede da qual o usuário está tentando acessar o serviço.

Na tabela a seguir, *{region}* substitua 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. *{region}*.amazonaws.com s3.amazonaws.com appstream2. *{region}*.aws.amazon.com

Categoria	Domínio ou endereço IP
	*.amazonappstream.com *.shortbread.aws.dev
WorkSpaces Recursos estáticos do Secure Browser	*.workspaces-web.com di5ry4hb4263e.cloudfront.net
WorkSpaces Autenticação de navegador seguro	*.auth. *{region}*.amazoncognito.com identidade cognitiva. *{region}*.amazonaws.com cognito-idp. *{region}*.amazonaws.com *.cloudfront.net
WorkSpaces Métricas e relatórios do Secure Browser	*.execute-api. *{region}*.amazonaws.com 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 Amazon 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 Amazon WorkSpaces Secure Browser.

Tópicos

Criação de um portal web para o Amazon WorkSpaces Secure Browser

Siga estas etapas para criar um portal da web.

Tópicos

Definindo as configurações de rede para o Amazon WorkSpaces Secure Browser

Para definir as configurações de rede para o WorkSpaces Secure Browser, siga estas etapas.

1. Abra o console do WorkSpaces Secure Browser em https://console.aws.amazon.com/workspaces-web/casa.
2. Escolha Navegador WorkSpaces seguro, depois Portais da Web e escolha Criar portal da Web.
3. Na página Etapa 1: especificar conexão de rede, conclua as etapas a seguir para conectar a VPC ao portal da web e configurar a VPC e sub-redes.

    1. Para obter detalhes da rede, escolha uma VPC com uma conexão com o conteúdo que você deseja que seus usuários acessem com o WorkSpaces Secure Browser.
    2. Escolha até três sub-redes privadas que atendam aos requisitos a seguir. Para obter mais informações, consulte Rede para o Amazon WorkSpaces Secure Browser.
        - 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.

Definindo as configurações do portal para o Amazon WorkSpaces Secure Browser

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 no portal da web no menu suspenso. Em seguida, insira seu limite máximo de usuários simultâneos para o portal da web. Para obter mais informações, consulte the section called “Gerenciar cotas de serviço”.

   > **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 Domínio Personalizado, você pode configurar um domínio personalizado para seu portal para habilitar o acesso através do seu próprio nome de domínio em vez do endpoint padrão do portal. Para obter mais informações, consulte the section called “Domínio personalizado”. Isso é opcional.
4. Em Registrador de sessão, você pode especificar um bucket do S3 para armazenar arquivos de log de sessão. Para obter mais informações, consulte the section called “Configurando o Registrador de Sessões”. Isso é opcional.
5. Em Registro de acesso do usuário, para Kinesis stream ID, selecione o stream de dados do Amazon Kinesis para o qual você deseja enviar os arquivos de log. Para obter mais informações, consulte the section called “Configurando o registro de atividades do usuário”. Isso é opcional.
6. Em Controle de acesso IP, escolha se deseja restringir o acesso a redes confiáveis. Para obter mais informações, consulte the section called “Gerenciar controles de acesso de IP”. Isso é opcional.
7. Em Configurações de proteção de dados, você pode criar políticas para o WorkSpaces Secure Browser para redigir informações confidenciais. Para obter mais informações, consulte the section called “Configurações de proteção de dados”. Isso é opcional.
8. Em Filtragem de URL, você pode especificar quais usuários URLs finais têm permissão para acessar ou bloquear categorias específicas URLs ou de domínio para restringir o acesso. Para obter mais informações, consulte the section called “Filtragem de conteúdo da Web”. Isso é opcional.

1. Para restringir a navegação por sessão a alguns domínios selecionados, ative a opção Bloquear tudo URLs e clique em adicionar URL para fornecer a lista de URLs seus usuários finais que podem acessar.
2. Para criar uma lista de bloqueios URLs para usuários finais, clique em Adicionar URL para listar o único URLs a ser bloqueado ou clique em Adicionar categorias para selecionar categorias de domínios que estão bloqueados (por exemplo, redes sociais).

9. Em Configurações de política, você pode definir qualquer política do navegador usando as políticas do Chrome disponíveis para a versão estável mais recente do portal da web. Para obter mais informações, consulte the section called “Gerenciar a política do navegador”. Isso é opcional.

   1. Você pode selecionar rapidamente algumas das políticas mais comuns no editor visual
      - Para 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**
        >
        > URLs visitado enquanto navega de forma privada, ou antes de um usuário excluir o histórico do navegador, não pode ser registrado no registro de acesso do usuário. Para obter mais informações, consulte the section called “Configurando o registro de atividades do usuário”.

      - Para Favoritos do navegador - opcional, insira o nome de exibição, o domínio e a pasta dos favoritos que você deseja que seus 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.

2. Você também pode adicionar ou editar políticas diretamente usando o editor JSON em vez do editor visual. Para saber o formato específico de uma política, consulte a lista de políticas do Chrome Enterprise.
3. Você também pode importar as políticas do Chrome usadas em sua organização fazendo o upload de um arquivo JSON no portal da web. Para obter detalhes, consulte the section called "Tutorial: Como configurar uma política de navegador personalizada"

   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.

10. 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. Isso é opcional.
11. Escolha Próximo para continuar.

Definindo as configurações do usuário para o Amazon WorkSpaces Secure Browser

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 Personalização da marca, você pode personalizar as telas de login e carregamento que aparecem para seus usuários finais modificando elementos visuais, conteúdo de texto e termos de serviço. Para obter mais informações, consulte the section called "Personalização da marca". Isso é opcional.
2. Em Permissões, escolha se deseja ativar a extensão para login único. Para obter mais informações, consulte the section called "Gerenciar a extensão de login único".
3. Em Permitir que os usuários imprimam em um dispositivo local a partir do portal da web, escolha Permitir ou Não permitir.
4. Em Permitir que os usuários façam um deep link para o portal da web, escolha Permitir ou Não permitir. Para obter mais informações sobre deep links, consulte the section called "Deep links".

5. Em Permitir que os usuários utilizem a autenticação local em sua sessão do portal, escolha Permitido ou Não Permitido. Para obter mais informações sobre autenticação na web, consultethe section called “Redirecionamento de autenticação da Web”.
6. Em Controles da barra de ferramentas, escolha as configurações desejadas em Recursos.
7. Em Configurações, gerencie a exibição da apresentação da barra de ferramentas no início da sessão, incluindo o estado da barra de ferramentas (encaixada ou desconectada), o tema (modo escuro ou claro), a visibilidade do ícone e a resolução máxima de exibição da sessão. Deixe essas configurações desdefinidas para conceder aos usuários finais controle total sobre essas opções. Para obter mais informações, consulte the section called “Controles da barra de ferramentas”.
8. Para Tempos limite de sessão, 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 ociosos quando param de fornecer entradas de teclado ou mouse 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.

Configurando seu provedor de identidade para o Amazon WorkSpaces Secure Browser

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

Tópicos

Escolha do tipo de provedor de identidade para o Amazon WorkSpaces Secure Browser

WorkSpaces O Secure Browser oferece dois tipos de autenticação: Padrão Centro de Identidade do AWS IAMe. Na página Configurar o provedor de identidade, escolha qual tipo de autenticação deve ser utilizada com o portal.

- Para o tipo Padrão (opção padrão), faça a federação de seu provedor de identidade SAML 2.0 de terceiros (como Okta ou Ping) diretamente com seu portal. Para obter mais informações, consulte the section called “Tipo de autenticação padrão”. O tipo padrão é compatível com fluxos de autenticação iniciados pelo SP ou pelo IdP.
- Para o IAM Identity Center (opção avançada), faça a federação do 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 obter mais informações, consulte the section called “Tipo de autenticação do Centro de Identidade do IAM”.

Tópicos

Configurando o tipo de autenticação padrão para o Amazon WorkSpaces Secure Browser

O tipo de autenticação padrão é o tipo de autenticação inicial fornecido. Ele dá suporte a fluxos de login iniciados pelo provedor de serviços (iniciados pelo SP) e pelo provedor de identidades (iniciados pelo IdP) com IdP compatível com SAML 2.0. Para configurar o tipo de autenticação padrão, siga as etapas abaixo para federar o IdP SAML 2.0 de terceiros (como Okta ou Ping) diretamente com seu portal.

Tópicos

Configurando seu provedor de identidade no Amazon WorkSpaces Secure Browser

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

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 os 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 carregar o arquivo de metadados do provedor de serviços no 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 declarações de SAML iniciadas pelo SP e iniciadas pelo IdP ou somente declarações de SAML iniciadas pelo SP.

- As declarações de SAML iniciadas pelo SP e pelo IdP permitem que seu portal ofereça suporte aos dois tipos de fluxos de login. Os portais que oferecem suporte a fluxos iniciados pelo IdP permitem que você apresente declarações 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 declarações de 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 de SAML iniciado por IdP, ou você pode copiá-lo do arquivo de metadados SP em `<md:IdPInitRelayState>`.
  - Observação
    - O formato a seguir representa o estado de retransmissão: `redirect_uri=https%3A%2F%2Fportal-id.workspaces-web.com%2Fsso&response_type=code&client_id=1example23456789&identity_provider=Ex` `Identity-Provider`.
    - Se você copiar e colar o valor do arquivo de metadados do SP, certifique-se de alterar `&` para &. `&` é um caractere de escape de XML.
- Escolha somente declarações de SAML iniciadas pelo SP para que o portal ofereça suporte somente aos fluxos de login iniciados pelo SP. Essa opção rejeitará declarações de 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 habilitar Assinar solicitações de SAML para esse provedor. A autenticação iniciada pelo SP permite que o 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. Habilitar a solicitação assinada em seu IdP. O nome pode ser diferente, dependendo do IdP.

> **Note**
>
> RSA- SHA256 é o único algoritmo de solicitação e assinatura de solicitação padrão suportado.

6. Escolha se você deseja habilitar Exigir declarações de SAML criptografadas. Isso permite que você criptografe a declaração de SAML que vem do seu IdP. Isso pode impedir que os dados sejam interceptados em declarações SAML entre o IdP e o Secure Browser. WorkSpaces

> **Note**
>
> O certificado de criptografia não está disponível nessa etapa. Ele será criado após o portal ser iniciado. Depois de iniciar o portal, baixe o certificado de criptografia e faça o upload para o IdP. Em seguida, habilite a criptografia de declaração 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 Solicitar assinatura na etapa anterior.
   b. Usar o Logout único exige que você configure um URL de logout único no seu provedor de identidade SAML 2.0. Você pode encontrar o 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. Habilitar logout único em seu IdP. O nome pode ser diferente, dependendo do IdP.

Configurar seu IdP em seu próprio IdP

Para configurar seu IdP em seu próprio IdP, siga estas etapas.

1. Abra uma nova guia no navegador.
2. Adicione os metadados do portal ao SAML IdP.

   Faça o upload do documento de metadados do SP que você baixou na etapa anterior no IdP ou copie e cole os valores dos metadados nos campos corretos do IdP. Alguns provedores não permitem o upload de arquivos.

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

3. Confirme o NameID para sua declaração de SAML.

   Certifique-se de que seu SAML IdP preencha o NameID na declaração de SAML com o campo de e-mail do usuário. O NameID e e-mail do usuário são usados para identificar exclusivamente o usuário federado de SAML com o portal. Use o formato de ID de Nome do SAML persistente.
4. Opcional: configure o estado de retransmissão para a autenticação iniciada pelo IdP.

   Se você escolheu Aceitar declarações de SAML iniciadas pelo SP e iniciadas pelo IdP na etapa anterior, siga as etapas na etapa 2 de the section called “Configuração do IdP no WorkSpaces Secure Browser” para definir o estado de retransmissão padrão para seu aplicativo de IdP.
5. Opcional: configure Solicitar assinatura. Se você escolheu Assinar solicitações de SAML para esse provedor na etapa anterior, siga as etapas na etapa 3 de the section called “Configuração do IdP no WorkSpaces Secure Browser” para fazer upload do 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.
6. Opcional: configure a criptografia de declaração. Se você escolher Exigir declarações de SAML criptografadas desse provedor, aguarde até que a criação do portal seja concluída e siga a etapa 4 em “Fazer upload de metadados” abaixo para carregar o certificado de criptografia em seu IdP e habilitar a criptografia de declaração.
7. Opcional: configure o logout único. Se você escolheu Logout único, siga as etapas na etapa 5 de the section called “Configuração do IdP no WorkSpaces Secure Browser” para carregar o certificado de assinatura em seu IdP, preencher o URL de logout único e habilite o Logout único.
8. Conceda acesso aos seus usuários em seu IdP para usar o Navegador WorkSpaces Seguro.
9. Baixe um arquivo de troca de metadados do seu IdP. Você fará o upload desses metadados para o WorkSpaces Secure Browser na próxima etapa.

Concluindo a configuração do IdP no Amazon Secure WorkSpaces Browser

Para concluir a configuração do IdP no WorkSpaces Secure Browser, siga estas etapas.

1. 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 um URL de metadados do IdP. O portal usa esses metadados do IdP para estabelecer confiança.

2. Para carregar um arquivo de metadados, em Documento de metadados do IdP, selecione Escolher arquivo. Carregue o arquivo de metadados no formato XML do IdP que você baixou na etapa anterior.
3. Para usar um URL de metadados, acesse o IdP que você configurou na etapa anterior e obtenha o 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.
4. Quando concluir, escolha Next.
5. Para portais nos quais você habilitou a opção Exigir declarações 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. Seu 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 reivindicação `AudienceRestriction` com um valor de `Audience` que define o ID da 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 reivindicação `SubjectConfirmationData` com um valor de `Recipient` do URL ACS SP e um valor de `InResponseTo` que corresponde 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 de SAML iniciadas pelo IdP, os detalhes da solicitação devem ser formatados como um parâmetro `RelayState` no corpo de uma solicitação HTTP POST. O corpo da solicitação também deve conter sua declaração de SAML como um parâmetro `SAMLResponse`. Ambos devem estar presentes se você tiver seguido a etapa anterior.

Veja a seguir um exemplo de corpo de `POST` para um provedor de SAML iniciado pelo IdP.

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

Orientação para uso específico IdPs com o Amazon WorkSpaces Secure Browser

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 da declaração	Logout único
Okta	Criar integrações de aplicativos SAML	Gerenciamento de usuários	Referência do campo SAML do Assistente de integração	Referência do campo SAML do Assistente de integração	Referência do campo SAML do Assistente de integração	Referência do campo SAML do Assistente de integração

IdP	Configuração do aplicativo SAML	Gerenciamento de usuários	Autenticação iniciada pelo IDP	Solicitar assinatura	Criptografia da declaração	Logout único
			de aplicativo	de aplicativo	de aplicativo	de aplicativo
Entra	Criar seu próprio aplicativo	Início rápido: criar e atribuir uma conta de usuário	Habilitar 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 logout único
Ping	Adicionar um aplicativo SAML	Usuários	Habilitar o SSO iniciado pelo IdP	Configurando o login da solicitação de autenticação PingOne para Enterprise	O PingOne for Enterprise oferece suporte à criptografia?	Logout único do SAML 2.0
One 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)
Centro de Identidade do IAM	Configurar sua própria aplicação SAML 2.0	Configurar sua própria aplicação SAML 2.0	Configurar sua própria aplicação SAML 2.0	N/D	N/D	N/D

Configurando o tipo de autenticação do IAM Identity Center para o Amazon WorkSpaces Secure Browser

Para o Centro de Identidade do IAM (avançado), faça a federação do Centro de Identidade do IAM 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 Centro de Identidade do IAM, você deve configurá-lo como um provedor independente. Para obter mais informações, consulte Get started with common tasks in IAM Identity Center. Ou você pode conectar seu IdP SAML 2.0 ao Centro de Identidade do IAM. Para obter mais informações, consulte Conectar-se a um provedor de identidade externo. Caso contrário, você não terá nenhum usuário ou grupo para atribuir ao portal da web.

Se você já usa o Centro de Identidade do IAM, pode escolhê-lo como um tipo de provedor e seguir as etapas abaixo para adicionar, visualizar ou remover usuários ou grupos do 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 obter mais informações, consulte the section called “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.

Tópicos

Criar um portal da web com o Centro de Identidade do IAM

Para criar um portal da web com o Centro de Identidade do IAM, siga estas etapas.

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 Centro de Identidade do AWS IAM.
2. Escolha Continuar com o IAM Identity Center.
3. Na página Atribuir usuários e grupos, escolha a guia and/or Grupos de usuários.
4. Marque a caixa próxima aos usuários ou grupos que deseja adicionar ao 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.

Gerenciar o portal da web com o Centro de Identidade do IAM

Para gerenciar um portal da web com o Centro de Identidade do IAM, siga estas etapas.

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

1. Depois que o portal for criado, ele será listado no console do Centro de Identidade do IAM como uma aplicação configurada.
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.

Adicionar mais usuários e grupos a um portal da web

Para adicionar mais usuários e grupos a um portal da web existente, siga estas etapas.

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 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.

Visualizar e remover usuários e grupos do portal da web

Para visualizar ou remover usuários e grupos do seu portal da web, use as ações disponíveis na tabela Usuários atribuídos. Para obter mais informações, consulte Manage access to applications

> **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.

Alteração do tipo de provedor de identidade para o Amazon WorkSpaces Secure Browser

É possível alterar o tipo de autenticação do portal a qualquer momento. Para isso, siga estas etapas.

- Para mudar de Centro de Identidade do IAM para Padrão, siga as etapas em the section called “Tipo de autenticação padrão”.
- Para mudar de Padrão para Centro de Identidade do IAM, siga as etapas em the section called “Tipo de autenticação do Centro de Identidade do IAM”.

As alterações no tipo de provedor de identidade podem levar até 15 minutos para serem implantadas e não se 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 fica visível nas cargas úteis de solicitação e resposta do evento.

Lançamento de um portal web com o Amazon WorkSpaces Secure Browser

Quando terminar de configurar seu portal da web, você poderá seguir estas etapas para iniciá-lo.

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.

Testando seu portal web no Amazon WorkSpaces Secure Browser

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 “Configuração do provedor de identidade”, ignore esta seção e vá para Distribuindo seu portal web no Amazon WorkSpaces Secure Browser.

1. Abra o console do WorkSpaces Secure Browser em https://console.aws.amazon.com/workspaces-web/casa? região = us-east-1#/.
2. Escolha Navegador WorkSpaces seguro, portais da Web, escolha seu portal da Web e 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 você pode navegar até sites conectados escolhendo links ou URLs entrando na barra de endereço.

Distribuindo seu portal web no Amazon WorkSpaces Secure Browser

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 o portal ao gateway do aplicativo SAML para que os usuários iniciem uma sessão diretamente do 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 Declarações de SAML iniciadas pelo SP e iniciadas pelo IdP em the section called “Tipo de autenticação padrão”. Como alternativa, você pode criar um aplicativo SAML personalizado que possa fornecer experiências de autenticação iniciadas pelo IdP usando fluxos iniciados pelo SP. Para ver mais informações, consulte Create a Bookmark App integration.
- Adicione o URL do portal a um site de sua propriedade e use um redirecionamento de navegador para direcionar os usuários ao portal da web.
- Envie por e-mail o URL do portal para seus usuários ou envie para um dispositivo que você gerencia como página inicial ou marcador do navegador.
- Use um domínio personalizado se você tiver configurado um para o seu portal em vez da URL do portal para uma experiência de identidade visual mais integrada aos seus usuários. Para obter mais informações, consulte the section called “Domínio personalizado”.

Gerenciando seu portal web no Amazon WorkSpaces Secure Browser

Depois de configurar o portal da web, você pode executar as ações a seguir para gerenciá-lo.

Tópicos

Visualizando detalhes do portal web no Amazon WorkSpaces Secure Browser

Para visualizar detalhes do portal da web, siga estas etapas.

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 escolha Exibir detalhes.

Editando um portal da web no Amazon WorkSpaces Secure Browser

Para editar um portal da web, siga estas etapas.

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 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.

Excluindo um portal da web no Amazon WorkSpaces Secure Browser

Para excluir um portal da web, siga estas etapas.

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 escolha Excluir.

Gerenciando cotas de serviço para seu portal no Amazon WorkSpaces Secure Browser

Quando você cria seu Conta da AWS, definimos automaticamente 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 dar suporte ao 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 manter 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

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

> **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.

Tópicos

Solicitando um aumento da cota de serviço no Amazon WorkSpaces Secure Browser

Para solicitar um aumento da cota de serviço, siga estas etapas.

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.

Solicitando um aumento do portal no Amazon WorkSpaces Secure Browser

Um portal é o recurso fundamental do serviço. Cada portal é uma associação entre seu provedor de identidades 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 do 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 desabilitadas) e ao Grupo B acesso à Internet geral sem filtragem de URL. Você pode criar um portal em qualquer Região da AWS compatível. 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. Para Aumentar valor da cota, insira o valor total que você deseja que a cota tenha.

Solicitando um aumento máximo de sessões simultâneas no Amazon WorkSpaces Secure Browser

A cota máxima de sessões simultâneas é a maior quantidade de usuários que podem ser conectados ao mesmo tempo a determinado portal. Se o limite de cota de serviço para o máximo de sessões simultâneas não for definido adequadamente, os usuários poderão encontrar uma sessão indisponível ao fazer login. Além de aumentar essa cota de serviço, os clientes também devem garantir que a VPC e as sub-redes tenham espaço de IP suficiente para dar suporte ao máximo de sessões simultâneas.

Para solicitar um aumento máximo de sessões simultâneas

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. Para Aumentar valor da cota, insira o valor total que você deseja que a cota tenha.

> **Note**
>
> Para aumentos grandes ou urgentes, acesse sua página de histórico de Cotas de Serviço, selecione o link na coluna de status da sua solicitação, vincule seu caso de suporte e adicione uma resposta com detalhes sobre a urgência and/or do seu caso de uso. 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 para o Amazon WorkSpaces Secure Browser

Por exemplo, suponha que um administrador esteja configurando dois portais da web na região 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) dará suporte a 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 dar 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 da região padrão (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).

Outras cotas de serviço no Amazon WorkSpaces Secure Browser

Você pode visualizar e solicitar aumentos de 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 de Número, 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 Service Quotas. 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 Taxa, os limites de taxa expostos em Service Quotas não precisam ser ajustados, independentemente do limite do portal da conta.

Controle do intervalo para reautenticar um token SAML IdP no Amazon Secure Browser WorkSpaces

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 Centro de Identidade do AWS IAM, 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 “Criação de 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.

Configurando o registro de atividades do usuário no Amazon WorkSpaces Secure Browser

WorkSpaces O Secure Browser oferece duas opções para registrar a atividade do usuário e os eventos relacionados à segurança:

- O Session Logger captura uma ampla variedade de eventos de sessão. Esses registros são entregues em um bucket do Amazon S3 em sua conta, permitindo fácil integração com sua plataforma SIEM preferida.
- O registro de acesso do usuário captura os eventos mais críticos da sessão. Esses registros são transmitidos para um stream do Amazon Kinesis para processamento e análise em tempo real.

Ambas as opções de registro são configuradas no nível do portal. Você deve configurar cada opção individualmente para cada portal em que você deseja que o registro esteja ativo. Você pode ativar uma opção ou ambas, dependendo dos seus requisitos para cada portal.

Você é responsável por cumprir todos os requisitos aplicáveis ao registro ou monitoramento da atividade do usuário ao usar esse recurso, incluindo o registro ou o monitoramento da atividade dos funcionários.

Tópicos

Configurando o Session Logger para o Amazon WorkSpaces Secure Browser

> **Warning**
>
> A ativação do Registrador de Sessões desativa os seguintes recursos do Chrome:
>
> - Modo de navegação anônima
> - Developer Tools
> - Mudança de perfil do Chrome

Para ativar o registrador de sessão para um portal do WorkSpaces Secure Browser, você deve primeiro identificar o bucket do Amazon S3 onde os eventos da sessão serão coletados. Você pode usar um bucket existente que já armazena registros semelhantes ou criar um novo especificamente para essa finalidade.

O bucket do Amazon S3 deve ter uma política de bucket que conceda permissão do WorkSpaces Secure Browser para gravar registros nele. Recomendamos colocar o bucket do Amazon S3 na mesma região do portal Conta da AWS do WorkSpaces Secure Browser.

Não há exigência de nomenclatura para o bucket do Amazon S3. Para criar um novo bucket, siga as etapas abaixo ou consulte Criar um bucket de uso geral no Guia do usuário do Amazon Simple Storage Service. Para obter orientação sobre a configuração de permissões, consulte as políticas de bucket para o Amazon S3 no Guia do usuário do Amazon Simple Storage Service.

Abaixo está um exemplo de uma política para seu bucket do Amazon S3. Certifique-se de atualizar a política com o nome do seu bucket do Amazon S3. Observe que o diretor é “workspaces-web.amazonaws.com”.

```
{
  "Version": "2012-10-17",
  "Statement": [
      {
          "Sid": "AllowSessionLogger",
          "Effect": "Allow",
          "Principal": {
              "Service": "workspaces-web.amazonaws.com"
          },
          "Action": [
              "s3:PutObject"
          ],
          "Resource": [
              "arn:aws:s3:::bucket-name/*"
          ]
      }
  ]
}
```

A ativação do Session Logger no portal do WorkSpaces Secure Browser pode resultar em cobranças do Amazon S3. Para ter informações, consulte Definição de preço do Amazon S3.

Para obter mais informações sobre os eventos relacionados à sessão que o Session Logger captura, consulte. the section called “Eventos de sessão no Session Logger”

Buckets S3 com criptografia KMS (opcional)

WorkSpaces O Secure Browser Session Logger é totalmente compatível com buckets AWS KMS Amazon S3 com criptografia ativada. Para garantir a funcionalidade de registro adequada com seu bucket criptografado do Amazon S3, você deve conceder ao Session Logger as permissões necessárias para usar sua chave. AWS KMS

Adicione a seguinte política à sua configuração de AWS KMS chave:

```
{
  "Sid": "Session Logger",
  "Effect": "Allow",
  "Principal": {
```

```
    "Service": "workspaces-web.amazonaws.com"
  },
  "Action": [
    "kms:Encrypt",
    "kms:GenerateDataKey*"
  ],
  "Resource": "*"
},
```

No AWS console, selecione o portal do WorkSpaces Secure Browser do qual você coletará eventos e escolha a guia Registrador de sessão e Editar.

Insira as seguintes informações para configurar o Registrador de Sessão para o portal:

- Localização do S3 (obrigatório): o nome do seu bucket do Amazon S3 onde os eventos serão entregues.
- Prefixo da chave (opcional): a pasta na qual os eventos são entregues. Se a pasta não existir, ela será criada. Se o campo for deixado em branco, o Session Logger gravará eventos na raiz do bucket do Amazon S3.

Em Avançado, você pode configurar os seguintes campos:

- Filtro de eventos: esta é a lista de eventos monitorados pelo Registrador de Sessões.
  - Todos: Selecionar essa opção significa que todos os eventos atuais e futuros serão monitorados
  - Incluir: Isso permite que você selecione manualmente eventos específicos para monitorar. Somente os eventos selecionados explicitamente serão registrados. Novos eventos introduzidos em futuras atualizações não serão monitorados, a menos que sejam adicionados manualmente à seleção.
- Formato do arquivo
  - JSON (padrão): esse é um formato de arquivo em que cada arquivo de log é apresentado como uma matriz de eventos. Recomendamos esse formato para a maioria dos casos de uso.
  - JSONLines: Esse é um formato de arquivo otimizado para o Amazon Athena.
- Estrutura de pastas: determina como os arquivos de log são armazenados.
  - Plano (padrão): todos os arquivos de log estão em uma única pasta.
  - Aninhado por data: os arquivos de log são organizados em pastas por data e hora. Particionado para o Amazon Athena e otimizado para consultas do Amazon Athena.

Você pode testar a configuração do Registrador de Sessões e garantir que o Registrador de Sessões esteja funcionando corretamente. Quando a configuração estiver concluída, o sistema tentará gravar um arquivo de teste com o nome `_workspaces_secure_browser.tmp` do bucket e da pasta do Amazon S3 especificados. Isso serve como uma validação da funcionalidade de registro e da configuração de permissões.

Você também pode executar uma sessão de teste iniciando uma sessão do Navegador Seguro no portal e usando o navegador como faria normalmente. O Session Logger grava arquivos de log em seu bucket Amazon S3 configurado a cada 15 minutos durante uma sessão ativa ou quando a sessão termina.

Depois de encerrar a sessão ou aguardar o próximo intervalo de registro, verifique o bucket do Amazon S3 para confirmar se os arquivos de log da sua sessão foram gerados e armazenados conforme o esperado.

Configurando o registro de acesso do usuário para o Amazon WorkSpaces Secure Browser

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?.

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?.

Gerenciando a política do navegador no Amazon WorkSpaces Secure Browser

Você pode definir qualquer política de navegador personalizada usando as políticas do Chrome disponíveis para a versão estável mais recente do WorkSpaces Secure Browser. Quando você

define uma política no portal do WorkSpaces Secure Browser, a política será aplicada a todas as sessões gerenciadas por esse portal da web.

Há mais de 300 políticas que você pode aplicar a um portal da web. Para obter mais informações, incluindo a lista completa das políticas do Chrome, consulte a lista de políticas do Chrome Enterprise.

Você tem três maneiras de definir uma política do Chrome:

1. Usando o editor visual no portal da web

   Ao usar a visualização do console para criar um portal da web, você pode aplicar algumas das políticas mais comuns no editor visual:

   - `StartURL`
   - Ativar e desativar a navegação privada
   - Exclusão do histórico
   - Favoritos e pastas de favoritos
2. Usando o editor JSON no portal da web

   Você também pode adicionar ou editar políticas diretamente usando o editor JSON em vez do editor visual.

   Para saber o formato específico de uma política, consulte a lista de políticas do Chrome Enterprise.
3. Carregando um arquivo JSON no portal da web

   Você também pode importar as políticas do Chrome usadas em sua organização fazendo o upload de um arquivo JSON no portal da web.

   Para obter detalhes, consulte the section called “Tutorial: Como configurar uma política de navegador personalizada”

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 obter mais informações, consulte the section called “Editar a política básica do navegador”.

Tópicos

- Tutorial: Definindo uma política de navegador personalizada no Amazon WorkSpaces Secure Browser
- Editando a política básica do navegador no Amazon WorkSpaces Secure Browser

Tutorial: Definindo uma política de navegador personalizada no Amazon WorkSpaces Secure Browser

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 tutorial a seguir, você cria um portal da web com os seguintes controles de política:

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

Tópicos

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

Etapa 1: criar um portal da web

Para fazer o upload do arquivo JSON da política do Chrome, você deve criar um portal do Navegador WorkSpaces Seguro. Para obter mais informações, consulte the section called “Criação de 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. Configurar marcador URLs.
   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 a inicialização URLs. 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 `RestoreOnStartup` ação para abrir uma lista de URLs . Você também pode usar outras ações na sua startup URLs. Para obter mais informações, consulte Lista de políticas do Chrome Enterprise.

   b. Defina como `RestoreOnStartupURLs` 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.

Editando a política básica do navegador no Amazon WorkSpaces Secure Browser

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.

A linha de base `URLAllowlist` e `URLBlocklist` as políticas não podem ser substituídas. Observe que o arquivo de política do navegador JSON associado ao seu portal da web não conterá essas políticas básicas. Para ver uma lista completa de todas as políticas aplicadas e seus valores, navegue até “chrome: //policy” em uma sessão de navegação remota.

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`.

Configurando o editor de método de entrada para o Amazon WorkSpaces Secure Browser

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. 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 idiomas
  - Para avançar o IME (ou mover para o layout direito do teclado), pressione Shift+Control+Left Alt.
  - Para acessar as configurações de idioma e entrada, use o seletor de idiomas na barra superior do painel. Se não estiver visível, ative-o na Barra de ferramentas → Preferências → Geral → Método de entrada do teclado.
- Japonesa
  - Para usuários do macOS: se você estiver usando uma fonte de entrada dos EUA, poderá ter problemas de entrada. Para resolver esse problema:
    1. Selecione uma fonte de entrada japonesa (por exemplo, japonês - Kana ou japonês - Romaji) em vez da fonte de entrada dos EUA em seu macOS.
    2. Na sessão do Navegador WorkSpaces Seguro, vá para Barra de Ferramentas → Preferências → Teclado → Configuração da tecla Opção e selecione Usar Opção () como tecla Alt remota (Mac) para garantir que os atalhos do teclado funcionem corretamente.
  - Convertendo caracteres de entrada
    - Para converter caracteres em Hiragana, pressione. F6
    - Para converter caracteres em Katakana, pressione. F7
    - Para converter caracteres em Hankaku Katakana (Katakana de meia largura), pressione F8
    - Para converter caracteres em latim, pressioneF10.

    - Para converter caracteres em Wide Latin, pressioneF9.
  - Alternando os modos de entrada
    - Para mudar de Hiragana para Katakana, pressione. Alt/Option+K
    - Para mudar de Katakana para Hankaku Katakana, pressione. Alt/Option+K
    - Para mudar do Hankaku Katakana (Katakana de meia largura) para o Hiragana, pressione. Alt/Option+K
    - Para alternar de qualquer modo japonês ou latim largo para latim, pressioneAlt/Option+L.
    - Para mudar do latim para o latim amplo, pressioneAlt/Option+L.
    - Para alternar de qualquer modo para Entrada direta, pressioneHenkaku/Zenkaku key.
    - Para mudar da Entrada Direta de volta para o Hiragana, pressione. Henkaku/Zenkaku key
- Coreana
  - Para escolher hangul, pressione Shift+Space.
  - Para escolher hanja, pressione F9.

Para desativar o teclado na tela das sessões do Navegador WorkSpaces Seguro, entre em contato com Suporte.

Configurando a localização em sessão para o Amazon Secure Browser WorkSpaces

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.

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

Tópicos

Códigos de idioma compatíveis com o Amazon WorkSpaces Secure Browser

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).

- Alemã
  - 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)
- Espanhola
  - 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)
- Francesa
  - fr: francês
  - fr-CA: francês (Canadá)
  - fr-FR: francês (França)
  - fr-CH: francês (Suíça)
- Indonésia
  - id: indonésio
  - id-ID: indonésio (Indonésia)
- Italiana
  - it: italiano
  - it-IT: italiano (Itália)
  - it-CH: italiano (Suíça)
- Japonesa

  - ja: japonês
  - Ja-JP: japonês (Japão)
- Coreana
  - ko: coreano
  - ko-KR: coreano (Coreia)
- Portuguesa
  - pt: português
  - pt-BR: português (Brasil)
  - pt-PT: português (Portugal)
- Chinesa
  - zh: chinês
  - zh-CN: chinês (China)
  - zh-HK: chinês (Hong Kong)
  - zh-TW: chinês (Taiwan)

Selecionar idiomas nas configurações de navegador do usuário

Para definir as configurações do navegador local do usuário, siga as etapas apropriadas.

- 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.

Gerenciando controles de acesso IP no Amazon WorkSpaces Secure Browser

> **Important**
>
> Só há suporte para controles de acesso IP IPv4. Os usuários que se conectam IPv6 somente a partir de redes serão bloqueados.

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.

Tópicos

Criação de um grupo de controle de acesso IP no Amazon WorkSpaces Secure Browser

> **Important**
>
> Só há suporte para controles de acesso IP IPv4. Os usuários que se conectam IPv6 somente a partir de redes serão bloqueados.

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.

Associando uma configuração de acesso IP a um portal da web no Amazon WorkSpaces Secure Browser

> **Important**
>
> Só há suporte para controles de acesso IP IPv4. Os usuários que se conectam IPv6 somente a partir de redes serão bloqueados.

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 “Configurações de 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.

Editando um grupo de controle de acesso IP no Amazon WorkSpaces Secure Browser

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.
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.

Excluindo um grupo de controle de acesso IP no Amazon WorkSpaces Secure Browser

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.

Gerenciando a extensão de login único no Amazon WorkSpaces Secure Browser

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.

Por padrão, as extensões não estão habilitadas no Chrome nas janelas anônimas ou nas janelas de navegação privada do Firefox. Os usuários podem habilitá-las 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 privativa.

Os usuários são solicitados a instalar a extensão quando fazem login em um portal. Para obter detalhes sobre a experiência do usuário com a extensão, consulte the section called “Extensão de autenticação única”.

Tópicos

- Identificação de domínios para a extensão de login único no Amazon Secure Browser WorkSpaces
- Adicionar a extensão de login único a um novo portal da web no Amazon WorkSpaces Secure Browser
- Adicionar a extensão de login único a um portal web existente no Amazon WorkSpaces Secure Browser
- Editando ou removendo a extensão de login único no Amazon WorkSpaces Secure Browser

Identificação de domínios para a extensão de login único no Amazon Secure Browser WorkSpaces

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 comuns, consulte a tabela a seguir:

IdP e domínios

IdP	Domínio
Okta	okta.com

IdP	Domínio
ID Entra	microsoftonline.com
Centro de Identidade da AWS	awsapps.com
One Login	onelogin.com
Duo	duosecurity.com

Adicionar a extensão de login único a um novo portal da web no Amazon WorkSpaces Secure Browser

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

1. Siga as etapas em the section called “Criação de um portal da web” até chegar a the section called “Configurações de usuário”.
2. Para a etapa 1 de the section called “Configurações de 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 “Configurações de usuário” e as seções restantes em the section called “Criação de um portal da web” para criar seu portal da web.

Adicionar a extensão de login único a um portal web existente no Amazon WorkSpaces Secure Browser

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/casa.
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.

Editando ou removendo a extensão de login único no Amazon WorkSpaces Secure Browser

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/casa.
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.

Filtragem de conteúdo da Web no Amazon WorkSpaces Secure Browser

A filtragem de conteúdo da Web é um recurso de segurança e conformidade que permite que sua organização defina políticas e regule o acesso ao conteúdo no WorkSpaces Secure Browser. Com a Filtragem de Conteúdo da Web, você pode especificar quais usuários URLs finais têm permissão para acessar ou bloquear categorias específicas URLs ou de domínio para restringir o acesso, atendendo aos requisitos críticos de segurança e conformidade regulatória.

> **Note**
>
> Embora você possa configurar políticas de filtragem de URL por meio das políticas do Chrome para bloquear ou permitir domínios específicos, não recomendamos essa abordagem porque as ações das políticas do Chrome não serão capturadas como parte dos recursos de registro de serviços. Para obter relatórios abrangentes de monitoramento e conformidade, use as políticas de filtragem de conteúdo da Web descritas nesta página.

Tópicos

Restringindo a navegação a informações específicas URLs

Você pode implementar uma política de “negação padrão” em que somente sites explicitamente URLs aprovados e acessíveis. É ideal para ambientes de alta segurança em que o acesso à Internet deve ser rigorosamente controlado e todos os sites permitidos foram examinados quanto às necessidades comerciais e à conformidade de segurança.

No AWS console, em Filtragem de URL:

- Navegue até Lista de bloqueios e selecione a opção Bloquear tudo URLs
- Em Lista de permissões, clique em Adicionar URL para adicionar uma URL que será listada como permitida para seu usuário final. Adicione uma entrada por URL.
- Clique em Salvar

Bloqueio específico URLs

Você pode equilibrar segurança e produtividade mantendo o acesso aberto à Internet e bloqueando sites problemáticos conhecidos. É adequado para organizações que confiam em seus usuários, mas desejam impedir o acesso a ameaças específicas ou conteúdo impróprio sem restringir excessivamente as atividades comerciais legítimas.

No seu AWS console, em Filtragem de URL:

- Navegue até Bloqueado URLs
- Selecione Adicionar URL e insira o URL a ser bloqueado. Adicione uma entrada por URL que você deseja bloquear
- Clique em Salvar

Categorias de bloqueio

Além de bloquear grupos específicos URLs, você também pode bloquear automaticamente grupos de URLs com base em categorias de conteúdo. Isso é útil para organizações que precisam de uma cobertura abrangente contra vários tipos de conteúdo impróprio ou arriscado sem precisar identificar e bloquear manualmente sites individuais.

No seu AWS console, em Filtragem de URL:

- Navegue até Categorias bloqueadas e clique em Adicionar categorias
- Selecione qualquer categoria que você deseja bloquear
- Você pode criar exceções a essas categorias adicionando URLs à Lista de Permissões. Para isso, clique em Adicionar URL e insira o entry/ies URLs que você deseja permitir. Mesmo que estejam incluídos nas categorias, os usuários finais poderão visitar URLs o.
- Clique em Salvar

As seguintes categorias podem ser selecionadas. Você pode selecionar uma, várias ou todas as categorias.

Categorias de filtragem disponíveis

Tema	Categoria	Description
Conteúdo adulto e impróprio	Nudez	Sites que contêm imagens ou obras de arte não sexuais de nudez.
Conteúdo adulto e impróprio	Pornografia	Sites com conteúdo sexual explícito ou material provocativo com nudez.
Conteúdo adulto e impróprio	Educação sexual	Recursos de saúde e sexualidade adequados à idade e revisados por médicos.
Conteúdo adulto e impróprio	Insípido	Conteúdo impróprio para crianças não abrangido por outras categorias.
Comunicação e Social	Chat	Plataformas de mensagens privadas e em grupo em tempo real.

Tema	Categoria	Description
Comunicação e Social	Mensagens instantâneas	Serviços de mensagens privadas.
Comunicação e Social	Rede profissional	Plataformas de construção de relacionamento com foco nos negócios.
Comunicação e Social	Redes sociais	Plataformas de interação com o usuário para compartilhar conteúdo e experiências pessoais.
Comunicação e Social	E-mail baseado na Web	Serviços de mensagens acessíveis pelo navegador, incluindo cartões eletrônicos e sistemas de saudação.
Entretenimento	Jogos	Recursos de jogos recreativos, incluindo videogames, quebra-cabeças e atividades que não sejam jogos de azar.
Entretenimento	Compartilhamento de imagens	Plataformas de conteúdo visual que oferecem recursos de hospedagem, pesquisa e compartilhamento.
Entretenimento	Ponto a ponto	Fornecedores de aplicativos de compartilhamento de arquivos e ferramentas de software relacionadas.
Conteúdo prejudicial e ilegal	Atividade criminosa	Instruções ou materiais que promovam atos ilegais.
Conteúdo prejudicial e ilegal	Hackeando	Ferramentas de acesso não autorizado ao sistema e recursos de exploração da rede.
Conteúdo prejudicial e ilegal	Droga ilegal	Conteúdo que promova o uso recreativo de drogas ou abuso de substâncias.

Tema	Categoria	Description
Conteúdo prejudicial e ilegal	Software ilegal	Material não autorizado protegido por direitos autorais e distribuição de software malicioso.
Conteúdo prejudicial e ilegal	Violência	Conteúdo que promova danos físicos ou exiba material gráfico.
Conteúdo prejudicial e ilegal	Armas	Recursos legítimos de uso de armas de fogo esportivas e recreativas.
Comportamentos de alto risco	Cultos	Conteúdo espiritual e metafísico não convencional.
Comportamentos de alto risco	Jogos de aposta	Atividades e informações relacionadas a apostas.
Comportamentos de alto risco	Ódio e intolerância	Conteúdo que promove preconceito contra características protegidas.
Comportamentos de alto risco	Traição escolar	Assistência acadêmica não autorizada e serviços de conclusão de trabalhos de casa.
Comportamentos de alto risco	Automutilação	Conteúdo promovendo ou discutindo comportamentos autodestrutivos.
Tecnologia e IA	Sites de download	Plataformas de hospedagem de software, aplicativos e ativos digitais.
Tecnologia e IA	IA generativa	Recursos de tecnologia de IA e aprendizado de máquina.
Tecnologia e IA	Domínios estacionados	Domínios de conteúdo mínimos usados para publicidade ou vendas de domínios.

Tema	Categoria	Description
Tecnologia e IA	Streaming de mídia e downloads	Plataformas de conteúdo de áudio/vídeo, incluindo músicas, vídeos e rádio na Internet.

Exemplo de URLs

Os seguintes tipos de URLs podem ser fornecidos no AllowedUrls ou BlockedUrls

Tipo	Exemplo
Domínio	exemplo.com
Subdomínio	login.example.com
Path	exemplo.com/myvideos
Parâmetro de consulta	exemplo.com/? parameter=123

Transferindo políticas do Chrome

Caso você já tenha políticas do Chrome configuradas para permitir ou bloquear domínios específicos, recomendamos que você as transfira para o recurso de filtragem de conteúdo da Web.

O recurso de filtragem de conteúdo da Web detectará URLAllow qualquer URLBlock política aplicável a uma sessão do WorkSpaces Secure Browser e a sinalizará no AWS console.

Para transferir as políticas do Chrome para URLAllowlist e/ ou URLBlocklist:

- Em seu AWS console, em Filtragem de URL, clique em Revisar políticas do Chrome (se você não ver o botão Revisar políticas do Chrome, isso significa que as políticas do Chrome não se aplicam atualmente ao URL Permitido ou URLBlock)
- Sob a sobreposição, revise as políticas do Chrome
- Clique em Transferir

As políticas do Chrome serão removidas do Editor JSON em Configurações de política e novas URLs serão adicionadas automaticamente ao recurso de filtragem de conteúdo da Web.

Links diretos no Amazon WorkSpaces Secure Browser

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 deep links que conectam usuários a um site específico durante uma sessão. Quando um deep link é selecionado, o portal exibe o URL especificado no deep link. O link é exibido ao lado das páginas iniciais configuradas 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.

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

Tópicos

Configurando links diretos no Amazon WorkSpaces Secure Browser

Para dar a permissão a deep links, escolha Permitido ao criar as configurações do usuário. O site para o qual você deseja criar um deep link deve estar codificado em URL. Por exemplo, para vincular um usuário a “https://www.example.com/? query=true”, atualize o link para %2F%3Fquery%3Dtrue. https%3A%2F%2Fwww.example.com

Um link direto pode conter até 10 URLs, delineado por vírgula. Por exemplo:

<uuid>https://.workspaces-web.com/? DeepLinks= %2F%3Fquery%3Dtrue, %2F%3Fquery %3Dtrue2, %2F%3Fquery%3Dtrue3, %2F%3Fquery%3Dtrue4https%3A%2F%2Fwww.example.com. https%3A%2F%2Fwww.example.com https%3A%2F%2Fwww.example.com https%3A%2F %2Fwww.example.com

Para obter mais informações sobre a permissão de deep links, consulte the section called “Configurações de usuário”.

Usando a filtragem de URL para links diretos no Amazon WorkSpaces Secure Browser

Qualquer usuário com quem você compartilhar esse link do portal pode manipular o valor do deep link 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 inadequados com seu portal, utilize a filtragem de URL.

A lista de permissões e de bloqueio de um portal podem ser editadas com a filtragem de URL nas configurações do navegador do seu portal. <uuid>Para fazer isso, anexe a URL a uma URL de portal listada como permitida no seguinte formato, em que UUID é a ID do portal: https://.workspaces-web.com/? DeepLinks= %2F%3Fquery%3Dtrue https%3A%2F%2Fwww.example.com

Para obter mais informações, consulte the section called “Filtragem de conteúdo da Web” e Permitir ou bloquear o acesso a sites.

Usando o painel de gerenciamento de sessões no Amazon WorkSpaces Secure Browser

Use o painel de gerenciamento de sessões no console do WorkSpaces Secure Browser para monitorar e gerenciar sessões ativas e completas.

Acesso ao painel

Para acessar o painel, siga estas etapas.

Para acessar o painel

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 e escolha seu portal da web.
3. Escolha a guia Sessão ou escolha Visualizar sessões para abrir o painel em um painel dividido abaixo.

Filtros do painel

No painel de sessões, você pode filtrar as sessões pelas seguintes propriedades ou valores:

- Status
  - Ativo: indica que uma sessão está sendo executada no momento. Para encerrar a sessão, consulte abaixo.
  - Encerrado: indica que uma sessão não está mais ativa.
- ID da sessão
- Nome de usuário
- Hora de início da sessão

Encerrar sessões

Para encerrar uma sessão, siga estas etapas.

Para encerrar uma sessão

1. No painel de sessões, selecione a sessão que deseja interromper.
2. Escolha Encerrar.
3. Usuários desconectados perdem todo o estado da sessão. Todas as guias abertas, o histórico do navegador e os arquivos baixados para o navegador seguro são reciclados.

Histórico da sessão

O painel contém sessões dos últimos 35 dias. Você pode usar a CLI para listar sessões, com ou sem filtro. O histórico da sessão é entregue como JSON, que os administradores podem processar, gerenciar e armazenar em um repositório separado.

Veja a seguir exemplos de comandos da CLI para gerenciar sessões na região US-West-2 (Oregon).

Para listar todas as sessões de um portal da web, execute o seguinte comando:

aws workspaces-web list-sessions --portal-arn arn:aws:workspaces-web:us-west-2:<accountId>:portal/<portalId>

Para listar todas as sessões de um usuário específico de um portal da web, execute o seguinte comando:

aws workspaces-web list-sessions --portal-arn arn:aws:workspaces-web:us-west-2:<accountId>:portal/<portalId> --username <username>

Protegendo dados em trânsito com endpoints FIPS e Amazon WorkSpaces Secure Browser

Por padrão, quando você se comunica com o serviço WorkSpaces Secure Browser como administrador usando o console, a AWS CLI (AWS Command Line Interface) ou um AWS SDK, ou durante a sessão de um usuário, todos os dados em trânsito são criptografados usando o TLS 1.2.

Se você precisar de módulos criptográficos validados pelo FIPS 140-3 ao acessar a AWS por meio de uma interface de linha de comandos ou de uma API, use um endpoint do FIPS. Quando você usa um endpoint do FIPS, todos os dados em trânsito são criptografados usando padrões criptográficos que estão em conformidade com o Federal Information Processing Standard (FIPS) 140-3. Para obter informações sobre endpoints FIPS, incluindo uma lista de endpoints do WorkSpaces Secure Browser, consulte. https://aws.amazon.com/compliance/fips

Depois que um portal é criado com endpoints do FIPS, todas as sessões de usuário e alterações administrativas são feitas automaticamente usando endpoints 140-3 do FIPS. Você pode usar a variável do ambiente `AWS_USE_FIPS_ENDPOINT=true` para localizar endpoints do FIPS e enviar solicitações com o SDK. Veja um exemplo do a seguir:

```
$ export AWS_USE_FIPS_ENDPOINT=true
$ aws workspaces-web list-portal
```

Você também pode usar a opção `–endpoint-url` de enviar solicitações diretamente para endpoints do FIPS. O exemplo a seguir é um exemplo de portais de lista de chamadas na região US-West-2 (Oregon):

```
$ aws workspaces-web list-portal --endpoint-url https://workspaces-web-fips.us-west-2.amazonaws.com
```

Gerenciando configurações de proteção de dados no Amazon WorkSpaces Secure Browser

As configurações de proteção de dados são usadas para ajudar a impedir que os dados sejam compartilhados durante uma sessão. As configurações podem ser criadas e aplicadas a vários portais.

Tópicos

Redação de dados em linha no Amazon WorkSpaces Secure Browser

Ao adicionar a redação de dados em linha a um portal, você pode prever e redigir automaticamente determinados dados de uma sequência de texto exibida em páginas da web. Você pode criar políticas de redação escolhendo entre padrões incorporados (como números de previdência social ou números de cartão de crédito) ou criar seus próprios tipos de dados personalizados usando expressões regulares e palavras-chave. As políticas incluem níveis configuráveis de fiscalização e controles sobre URLs onde a redação deve ser aplicada.

Os componentes a seguir determinam quando os dados são editados:

- Configurações de proteção de dados - Configurações de proteção de dados é o nome do recurso que inclui seus tipos de dados e critérios de imposição. Para utilizar esse recurso, primeiro crie suas configurações e, em seguida, associe-as a um portal. Quando os usuários iniciam uma sessão, suas configurações são aplicadas durante a sessão.
- Extensão do navegador na sessão - Quando você associa as configurações de redação ao seu portal, o navegador da sessão será iniciado com uma extensão de navegador imposta pelo sistema que impõe suas configurações. As configurações de proteção de dados impõem a

redação por meio de correspondência de padrões (expressões regulares) e pesquisa por palavra-chave de acordo com seu nível de confiança e configuração de imposição de URL. O conteúdo é previsto a partir de sequências de texto e editado antes de ser exibido na tela. A extensão também define políticas de navegador relacionadas que controlam a capacidade dos usuários de contornar a redação (como navegação privada desativada, acesso às ferramentas do desenvolvedor e inspeção de rede).

As seguintes alterações na política do navegador Chrome são aplicadas pela extensão do navegador em sessão. Para obter mais informações, consulte Lista de políticas do Chrome Enterprise.

- Aplique a política do navegador para impedir que os usuários visualizem a sessão sem redação:
  - IncognitoModeAvailability = 1
  - DeveloperToolsAvailability = 2
  - BrowserAddPersonEnabled= falso
  - BrowserGuestModeEnabled= falso
- A extensão também impede que os usuários baixem arquivos HTML URLs que estejam aplicando as configurações de proteção de dados cancelando o evento de download.

Em geral, você deve usar a redação com sites privados e estruturados (como suas ferramentas de gerenciamento de clientes, sistemas de emissão de bilhetes ou wikis), e não para navegação pública não estruturada (como Facebook ou Google). Você pode escolher entre os tipos de dados incorporados (veja abaixo a lista completa) ou definir tipos de dados personalizados usando seus próprios valores de expressão regular e palavras-chave. Os administradores são responsáveis por testar e validar se cada tipo de dados, nível de confiança e aplicação de URL estão funcionando conforme o esperado. AWS não podemos garantir a compatibilidade com sites ou aplicativos personalizados fornecidos por terceiros.

WorkSpaces Atualmente, o Secure Browser não oferece suporte à redação de tipos de dados compatíveis ou personalizados em formatos não textuais, incluindo texto nos seguintes formatos:

- Imagens, como JPEG, PNG ou GIF
- Páginas da Web que permitem que os usuários usem processamento ou edição dinâmica de texto, como Google Docs ou Sheets
- Fluxos de áudio ou vídeo acessados no navegador, como YouTube vídeos
- PDFs visualizado pelo navegador Chrome

Não use redação para conteúdo em um formato incompatível. Os administradores são responsáveis por validar a compatibilidade do site e do conteúdo antes de conceder aos usuários acesso ao conteúdo que eles pretendem editar.

Configuração de redação padrão no Amazon WorkSpaces Secure Browser

A configuração de redação padrão aplicará automaticamente um nível de confiança e uma imposição de URL para todos os tipos de dados incorporados nas configurações de proteção de dados. Você tem a opção de substituir a configuração padrão ao adicionar um tipo de dados incorporado.

Os níveis de confiança permitem que você ajuste a lógica de redação para tipos de dados incorporados usando uma combinação de formato, palavras-chave e texto não formatado. Escolha o nível de rigor de como a redação é aplicada, incluindo Alto, Médio ou Baixo. O valor padrão será aplicado a todos os tipos de dados, a menos que uma substituição seja aplicada no nível do tipo de dados. Em geral, comece com uma configuração padrão do Medium e refine validando se a redação é aplicada conforme o esperado em seus sites.

Nível de confiança	Description	Exemplo
Alto	Requer uma correspondência de padrão de texto formatado para que o conteúdo seja editado.	O SSN de 123-45-6798 seria redigido, enquanto 123456789 não.
Médio	A redação considera texto formatado e não formatado e adiciona a palavra-chave associada à lógica.	O SSN de 123-45-6798 seria editado. 123456789 seria editado se detectado próximo a uma palavra-chave (como “número do seguro social”).
Baixo	Redação aplicada tanto para padrão formatado quanto para padrão não formatado sem palavra-chave.	Os SSN em qualquer formato - 123-45-6798 e 123456789 - são editados sem a necessida de de palavra-chave.

Você deve definir a configuração de redação padrão para todos os tipos de dados. Você pode escolher entre as seguintes opções:

- Tudo URLs
- Específico URLs
- Configurações avançadas

O valor padrão será aplicado a todos os tipos de dados, a menos que uma substituição seja aplicada no nível do tipo de dados. A fiscalização de URL usa uma lógica semelhante à política do Chrome para gerenciar listas de permissões e bloqueios. Para obter orientação sobre como bloquear e permitir URLs, consulte Permitir ou bloquear o acesso a sites. Para obter os melhores resultados, adicione URLs a essas listas seguindo o formato de filtro da lista de bloqueio do Chrome. Para obter mais informações, consulte Formato do filtro da lista de bloqueio de URLs.

Baseie a redação em linha no Amazon Secure WorkSpaces Browser

A redação de dados em linha tem suporte para padrões integrados (como números de previdência social e números de cartão de crédito), que você pode encontrar listados em Base de redação embutida. Escolha o (s) tipo (s) de dados no menu suspenso e especifique o valor de substituição para cada tipo de dados. Todos os tipos de dados seguem o padrão de imposição de configuração padrão acima, mas você pode optar por substituir o nível de confiança e ajustar o padrão de imposição de domínio para cada tipo de dados.

Para inserir um valor alternativo da configuração padrão, escolha Substituição do nível de confiança. Por exemplo, com a configuração padrão definida como Média, você pode notar durante o teste que um dos seus tipos de dados não está sendo editado de forma confiável. Você pode definir a substituição como Baixa para aumentar a chance de redação, sem ajustar a lógica usada para seus outros tipos de dados.

Para ajustar a forma como a redação é aplicada URLs sem alterar a configuração padrão, aplique substituições de imposição de URL. Por exemplo, você pode definir o uso de substituições de URL para impor a redação de endereços de e-mail em seu sistema de gerenciamento de relacionamento com o cliente, sem interromper o acesso do usuário aos endereços de e-mail no site do diretório da empresa ou no e-mail baseado na web.

Veja a seguir uma lista dos tipos de dados e seus padrões incorporados correspondentes IDs:

builtInPatternIdentificação	Tipo de dados
awsAccessKey:	Chave de acesso da AWS

builtInPatternIdentificação	Tipo de dados
awsSecretKey:	Chave secreta da AWS
Números do cartão:	Números de cartão de crédito
cripto:	Endereços de criptomoeda
CusipNum:	Número CUSIP
data:	Data
Anum:	Números DEA dos EUA
cão:	Data de nascimento
Carteira de motorista:	Carteiras de motorista dos EUA
Endereço de e-mail:	Endereço de e-mail
uma:	Número de identificação do empregador dos EUA
Data de expiração:	Data de vencimento do cartão de crédito
healthInsuranceNum:	Número de reclamação do seguro de saúde do Medicare
Código HIPAA:	Código HIPAA ICD-10
indivTaxId:	ID fiscal individual dos EUA
Endereço IP:	Endereço IP
está em:	Números de identificação de valores mobiliári os internacionais
jato:	JSON Web Token
Coordenada de localização:	Coordenadas de localização
Endereço MAC:	MAC Address

builtInPatternIdentificação	Tipo de dados
medicareBeneficiaryId:	Número do beneficiário do Medicare
npi:	Número de identificação do provedor nacional
ndc:	Códigos Nacionais de Medicamentos (NDC)
Número do passaporte:	Número do passaporte dos EUA
Número de telefone:	Número de telefone
Número de roteamento:	Número de roteamento ABA
ssn:	Número do Seguro Social dos EUA
Código Swift:	Código SWIFT
hora:	Hora
vinho:	Número de identificação do veículo nos EUA

Redação embutida personalizada no Amazon WorkSpaces Secure Browser

Os clientes podem definir seus próprios padrões usando expressões regulares, como aplicativos internos personalizados IDs. Para criar seu padrão de redação em linha personalizado, siga estas etapas:

1. Acesse sua configuração de proteção de dados.
2. Escolha Redação embutida personalizada e adicione.
3. Insira um nome para o tipo de dados personalizado.
4. Insira o valor da expressão regular.
   - Os valores da expressão regular devem corresponder à sintaxe literal da expressão JavaScript regular. Para obter mais informações, consulte Expressões regulares. Um exemplo de expressão regular `é/ex[am]+ple/i`.
   - Certifique-se de testar seus padrões personalizados nos sites que você planeja oferecer suporte. Se os padrões personalizados forem escritos com erros, eles podem introduzir problemas de desempenho não intencionais.

5. Especifique o valor de substituição.
6. Escolha Mais opções para obter mais personalizações opcionais, incluindo as seguintes:
   - Adicione palavras-chave para ajustar a lógica de redação. As palavras-chave podem aumentar a precisão da fiscalização. Adicione palavras-chave na sintaxe literal da expressão regular do Javascript. Para obter mais informações, consulte Expressões regulares.

     Por exemplo, se você estiver criando um padrão de redação personalizado para o cliente IDs usado em um sistema interno, poderá adicionar `/client name/i` ao campo de palavra-chave para informar a lógica de digitalização e detecção.
   - Aplique substituições de imposição de URL para ajustar a forma como a redação é aplicada URLs, sem alterar a configuração padrão.

     Por exemplo, você pode definir o uso de substituições de URL para impor a redação de endereços de e-mail em seu sistema de gerenciamento de relacionamento com o cliente, sem interromper o acesso do usuário aos endereços de e-mail no site do diretório da empresa ou no e-mail baseado na web.
   - Insira uma descrição (opcional) para o tipo de dados.

Crie configurações de proteção de dados no Amazon WorkSpaces Secure Browser

Você pode criar configurações de proteção de dados no WorkSpaces Secure Browser.

Para criar configurações de proteção de dados

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 à esquerda, escolha Configurações de proteção de dados.
3. Escolha Criar configurações de proteção de dados.
4. Insira um nome de exibição (obrigatório) e uma descrição (opcional) para a configuração.
5. Selecione as configurações padrão para redação em linha. Você pode definir o seguinte:
   - O nível de rigor de todos os tipos de dados
   - Os domínios nos quais a redação deve ser aplicada

6. Escolha seus tipos básicos de dados de redação em linha dentre os tipos compatíveis ou crie um tipo de dados personalizado. Você pode definir substituições para cada tipo de dados, incluindo o nível de rigor e as exceções de domínio.
7. Adicione quaisquer tags (opcional) para gerar relatórios.
8. Quando concluir, selecione Save.

Associe as configurações de proteção de dados no Amazon WorkSpaces Secure Browser

Você pode associar as configurações de proteção de dados no WorkSpaces Secure Browser.

Para associar uma configuração de proteção de dados a um portal existente

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 à esquerda, escolha Portais da Web.
3. Selecione o portal da web e escolha Editar.
4. Em Configurações de proteção de dados, selecione a configuração do seu portal.
5. Escolha Salvar.

Para associar uma configuração de proteção de dados ao criar um novo portal, siga estas etapas.

Para associar uma configuração de proteção de dados ao criar um novo portal

1. Siga as instruções em the section called “Criação de um portal da web” para criar um portal, até chegar à configuração de proteção de dados.
2. Escolha sua configuração de proteção de dados no menu suspenso.
3. Conclua as etapas the section called “Criação de um portal da web” para concluir a criação do seu portal.

Para criar uma configuração de proteção de dados ao criar um novo portal, siga estas etapas.

Para criar uma configuração de proteção de dados ao criar um novo portal

1. Siga as instruções em the section called “Criação de um portal da web” para criar um portal, até chegar à configuração de proteção de dados.

2. Escolha as configurações de proteção de dados no menu suspenso.
3. Insira um nome de exibição (obrigatório) e uma descrição (opcional) para a configuração.
4. Selecione as configurações padrão para redação em linha. Você pode definir o seguinte:
   - O nível de rigor de todos os tipos de dados
   - Os domínios nos quais a redação deve ser aplicada
5. Escolha seus tipos básicos de dados de redação em linha dentre os tipos compatíveis ou crie um tipo de dados personalizado. Você pode definir substituições para cada tipo de dados, incluindo o nível de rigor e as exceções de domínio.
6. Adicione quaisquer tags (opcional) para gerar relatórios.
7. Quando concluir, selecione Save.
8. Selecione o botão de atualização nas configurações de proteção de dados e, em seguida, escolha sua configuração de proteção de dados no menu suspenso.
9. Continue seguindo as instruções de criação do portal para concluir a criação do seu portal.

Edite as configurações de proteção de dados no Amazon WorkSpaces Secure Browser

Você pode editar as configurações de proteção de dados no WorkSpaces Secure Browser.

Para editar as configurações de proteção de dados

1. Abra o console do WorkSpaces Secure Browser emhttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Escolha as configurações de proteção de dados e a configuração de proteção de dados que você deseja editar na exibição em lista.
3. Você pode atualizar o nome, a descrição, as configurações padrão, os tipos de dados (compatíveis ou personalizados) e aplicar substituições de nível de confiança ou domínio.
4. Escolha Salvar.

Exclua as configurações de proteção de dados no Amazon WorkSpaces Secure Browser

Você pode excluir as configurações de proteção de dados no WorkSpaces Secure Browser.

Para excluir as configurações de proteção de dados

1. Se você tiver um portal associado a uma configuração de proteção de dados, primeiro remova a associação antes de excluir a configuração de proteção de dados.
2. Abra o console do WorkSpaces Secure Browser emhttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
3. Escolha as configurações de proteção de dados e a configuração de proteção de dados que você deseja excluir da exibição em lista.
4. Escolha Excluir.

Personalização da marca no Amazon WorkSpaces Secure Browser

Você pode personalizar as telas de login e carregamento que aparecem para seus usuários finais modificando elementos visuais, conteúdo de texto e termos de serviço. A personalização da marca ajuda a criar uma experiência consistente que se alinha à identidade da sua organização.

Visão geral

A personalização da marca permite que você personalize os seguintes aspectos da experiência do usuário:

- Elementos visuais - Faça upload de logotipo, favicon e papel de parede e selecione temas de cores que combinem com a identidade da sua marca.
- Conteúdo de texto - personalize as mensagens de boas-vindas, o título da guia do navegador e outros campos de texto opcionais para manter a voz da sua marca durante todo o fluxo de login. Se você não especificar texto personalizado para determinados campos, o texto padrão será usado. Para obter detalhes, consulte the section called “Diretrizes de personalização”.
- Termos de serviço (opcional) - adicione os termos de serviço da sua organização que os usuários devem reconhecer antes de iniciar uma sessão.

> **Note**
>
> Você também pode personalizar o nome de domínio do seu portal. Para obter detalhes, consulte the section called “Domínio personalizado”.

Tópicos

Configurando a personalização da marca para seu portal

Como funciona

Quando você configura a personalização da marca:

- Elementos visuais e de texto são aplicados tanto na tela de login quanto na tela de carregamento.
- A guia do navegador exibe seu favicon e título personalizados.
- Os usuários finais verão suas alterações de personalização ao iniciar uma nova sessão. Em alguns casos, pode levar alguns minutos até que suas alterações sejam visíveis.
- Se os termos de serviço estiverem configurados, os usuários finais deverão aceitar seus termos de serviço antes de iniciar a sessão de streaming. Observe que eles serão solicitados no início de cada sessão.

Pré-requisitos

Antes de começar

- Certifique-se de ter as permissões necessárias para modificar as configurações do portal, consultethe section called “AWS políticas gerenciadas”.
- Prepare seus ativos de marca (logotipo, favicon, papel de parede) de acordo com as especificações em. the section called “Diretrizes de personalização”

Introdução

Para configurar a personalização da marca, siga estas etapas.

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 e escolha seu portal da web.
3. Selecione seu portal e escolha a guia Configurações do usuário.
4. Na seção Personalização da marca, escolha Editar.
5. Configure as seguintes seções conforme necessário:

- No editor de conteúdo - Faça o upload de todos os elementos visuais (o logotipo da sua empresa, seu favicon e um papel de parede opcional) e selecione o tema de cores. Você pode carregar os arquivos do seu computador local ou de um bucket do S3. Para obter informações sobre como configurar permissões de bucket do S3, consultethe section called “Configurando permissões de bucket do S3”.
- No Editor de texto - Personalize o texto que aparece na tela de login.
- No editor de Termos de Serviço - Opcionalmente, adicione termos que os usuários devem reconhecer.

6. Escolha Salvar alterações.

Para obter instruções detalhadas sobre cada opção de personalização, consultethe section called “Diretrizes de personalização”.

Configurando permissões de bucket do S3

Você pode fazer upload de arquivos de identidade visual diretamente do seu computador ou selecionar objetos existentes nos buckets do S3. Se você optar por carregar os arquivos dos elementos visuais (logotipo da sua empresa, seu favicon e um papel de parede) de um bucket do S3, certifique-se de configurar as permissões adequadas para o bucket do S3.

Seleção de objetos do S3 na mesma conta

Se seu usuário ou função do IAM já tiver `s3:GetObject` permissão para o bucket que contém seus ativos de marca, nenhuma configuração adicional será necessária.

Seleção de objetos do S3 em outra conta

Para selecionar um bucket do S3 em uma AWS conta diferente, você precisa configurar a política do bucket na conta de origem e a política do IAM na sua conta de administrador.

Exemplo de política de bucket (na conta de origem):

Aplique essa política ao bucket do S3 na conta de origem. *123456789012*Substitua pelo ID da sua conta de administrador e *source-account-bucket-name* pelo nome real do bucket.

```
{
  "Version": "2012-10-17",
```

```
  "Statement": [
    {
      "Sid": "AllowCrossAccountAccess",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:root"
      },
      "Action": [
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::source-account-bucket-name",
        "arn:aws:s3:::source-account-bucket-name/*"
      ]
    }
  ]
}
```

Exemplo de política do IAM (na sua conta de administrador):

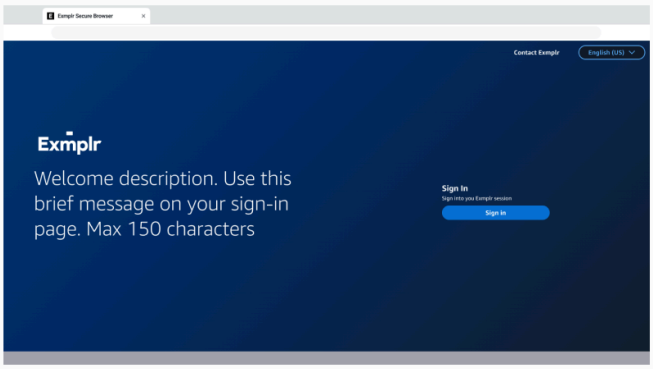
Anexe essa política ao usuário ou função do IAM em sua conta de administrador. *source-account-bucket-name*Substitua pelo nome real do bucket da conta de origem.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowCrossAccountS3Access",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::source-account-bucket-name",
        "arn:aws:s3:::source-account-bucket-name/*"
      ]
    }
  ]
}
```

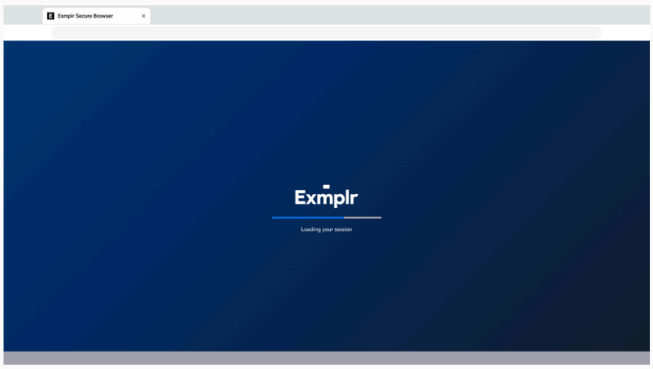
Para obter informações detalhadas sobre o acesso entre contas, consulte O S3 Access concede acesso entre contas.

Diretrizes de personalização

Personalize a experiência de login e carregamento para seus usuários finais atualizando os elementos de identidade visual e o texto nas páginas de login e carregamento. Você pode modificar elementos visuais, como logotipos e papéis de parede, editar elementos de texto, como mensagens de boas-vindas e cabeçalhos, e, opcionalmente, configurar um contrato de Termos de Serviço que os usuários devem aceitar antes de iniciar a sessão.



Sign in Page

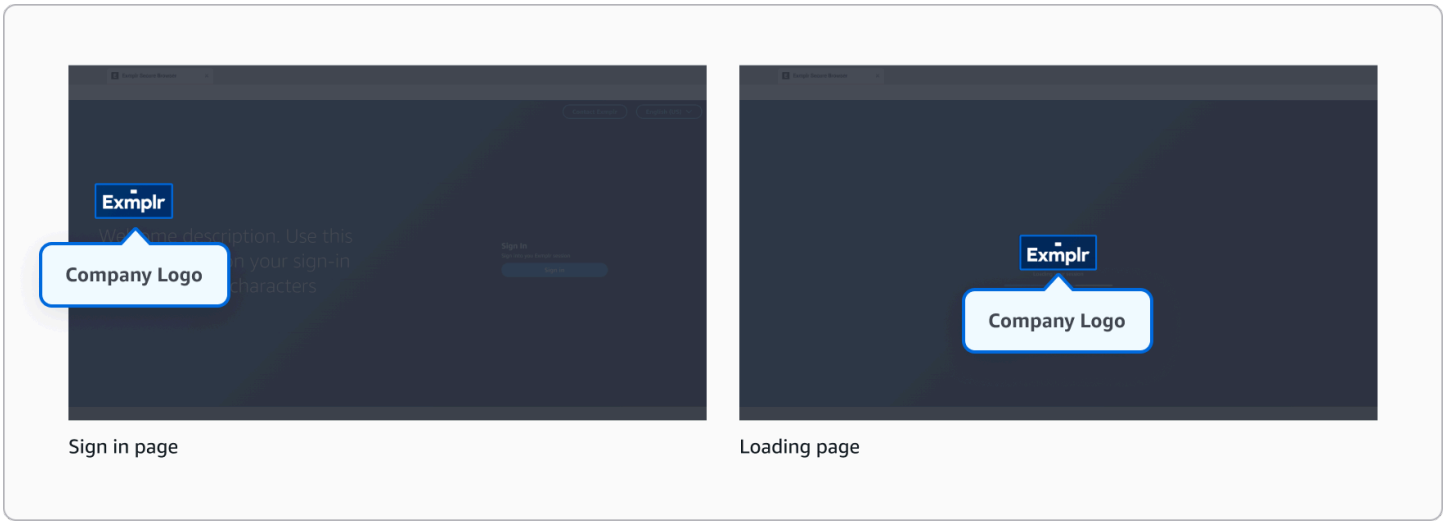


Loading Page

Editor de conteúdo

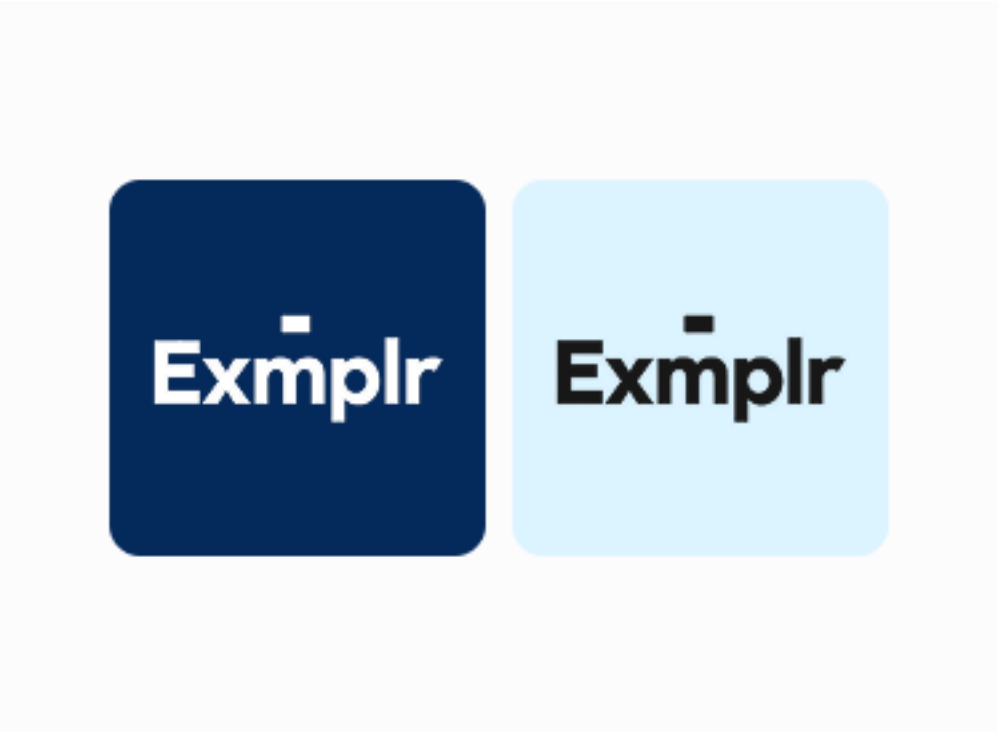
Logotipo da empresa

O logotipo aparece na tela de login e na tela de carregamento, fornecendo uma marca consistente em toda a experiência do usuário.



- Formatos aceitos: JPG, ICO ou PNG
- Tamanho máximo do arquivo: 100 KB

Faça



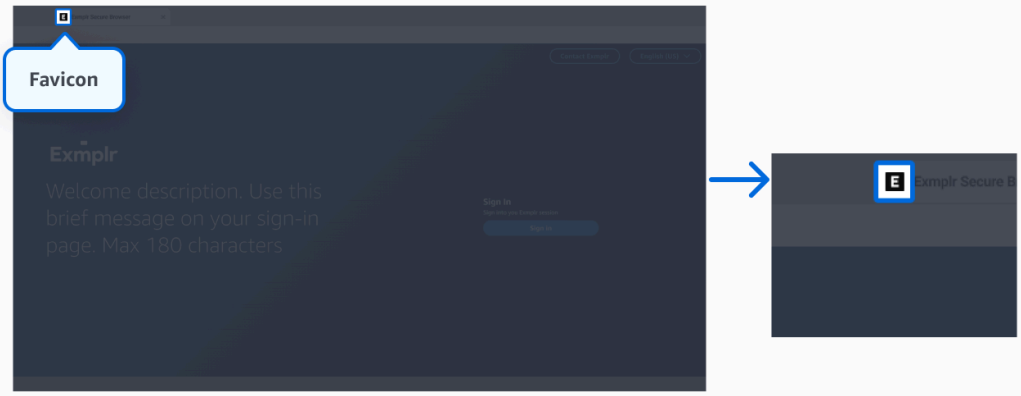
- Se você tiver variações de logotipo diferentes (como cores ou estilos diferentes), escolha aquela que ofereça o melhor contraste com o fundo do papel de parede selecionado.

Não

- Não ignore a proporção ao redimensionar seu logotipo.
- Não use logotipos que não tenham o tamanho correto de antemão, pois eles podem parecer distorcidos.

Favicon

Um favicon é um pequeno ícone que aparece nas guias do navegador, ajudando os usuários a identificar seu aplicativo entre várias guias abertas.



- Formatos aceitos: JPG, ICO ou PNG
- Tamanho máximo do arquivo: 100 KB
- Proporção recomendada: 1:1

Papel de parede - opcional

O papel de parede serve como imagem de fundo em todas as telas, criando uma experiência visual coesa. Se você não fizer upload de um papel de parede personalizado, o papel de parede padrão mostrado abaixo será usado. Escolha uma imagem que complemente sua marca sem interferir na legibilidade do conteúdo.

Wallpaper will be the same across all pages

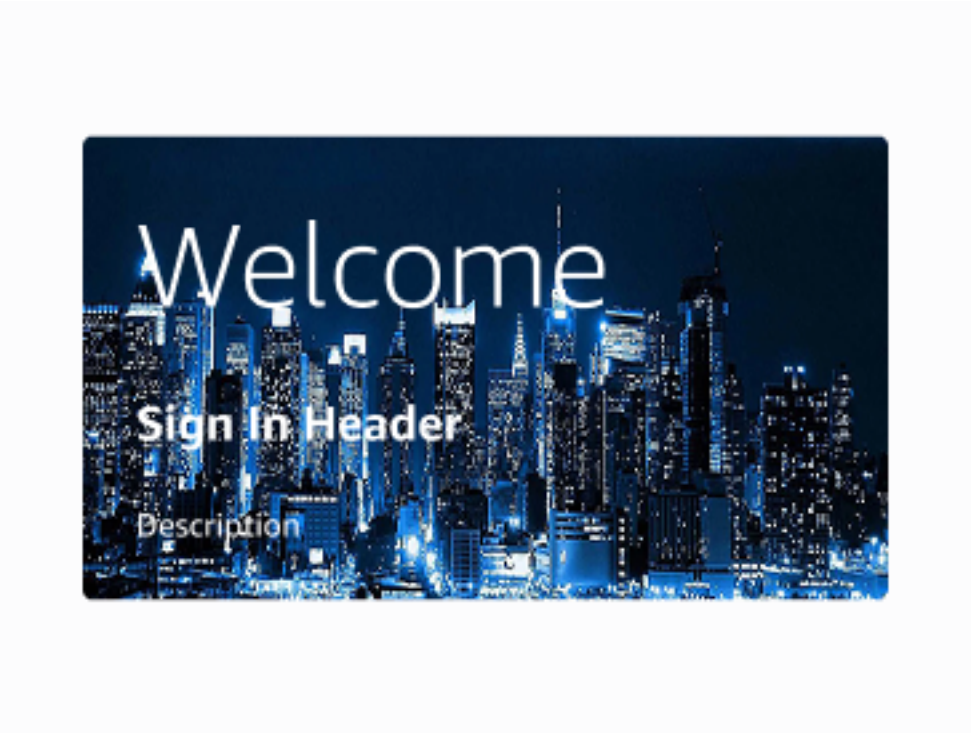
- Formatos aceitos: JPG ou PNG
- Tamanho máximo do arquivo: 5 MB

- Proporção recomendada: 16:9
- Resolução mínima recomendada: 1920 x 1080

Faça

- Use papéis de parede sutis e de baixo contraste ou imagens desfocadas que não interfiram no conteúdo em primeiro plano.
- Considere o posicionamento predefinido do texto para evitar áreas ocupadas atrás do texto.
- Utilize as cores da marca e use sobreposições para criar melhor contraste e legibilidade.

Não



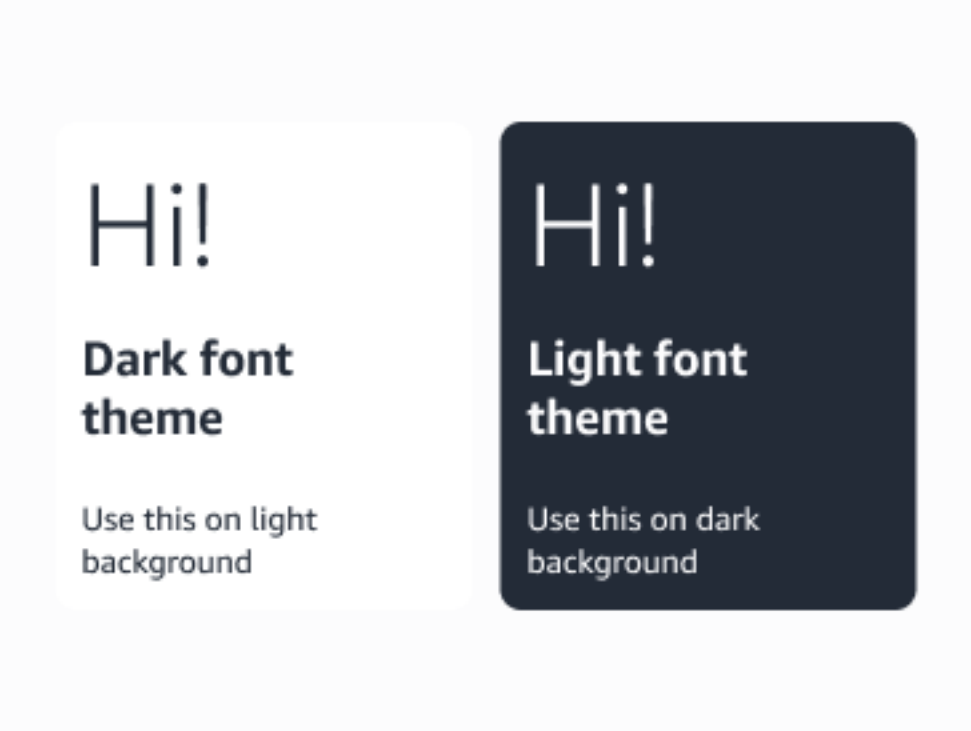
- Não use imagens ocupadas, saturadas ou com muitos detalhes diretamente atrás de textos importantes.
- Não use imagens visualmente complexas ou imagens com transições nítidas que causem limitações de legibilidade com localizações de texto predefinidas.
- Não confie apenas na cor para separar o texto do plano de fundo sem contraste suficiente.

Tema de cores

Selecione entre temas claros ou escuros que se refletem em fontes, botões e modais.

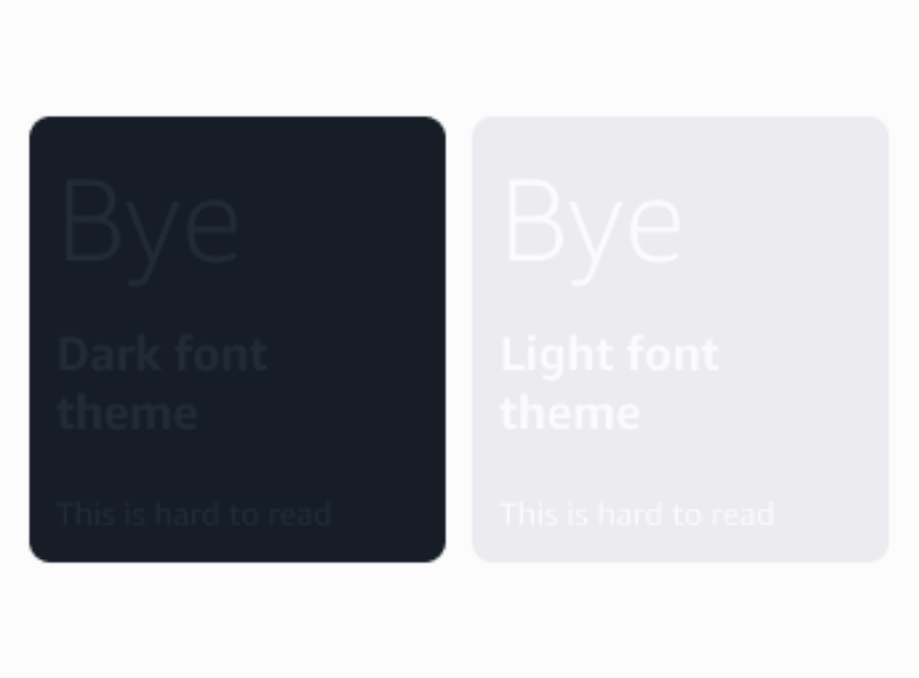
- Tema claro: ideal para fundos mais escuros, oferecendo contraste nítido e reduzindo o cansaço visual quando se trabalha em ambientes com pouca luz.
- Tema escuro: ideal para fundos claros, oferecendo visualização confortável e brilho reduzido em ambientes claros.

Faça



- Garanta um forte contraste com elementos de fundo/papel de parede.
- Use o tema de cores escuras em fundos claros.
- Use o tema de cores claras em fundos escuros.

Não



- Não coloque fontes claras ou escuras sobre imagens ou papéis de parede complexos.

Editor de texto

O editor de texto permite que você personalize o texto que aparece na tela de login dos usuários finais. Para habilitar a personalização da marca, você deve adicionar ao menos um idioma.

Para novo usuário: detectamos a preferência de idioma do seu navegador e exibimos a página do portal nesse idioma caso você o tenha configurado nos idiomas de sua marca. Se o idioma do seu navegador não estiver nos idiomas configurados, o padrão será inglês (en-US), se disponível. Se você não configurou o inglês, usamos o primeiro idioma em ordem alfabética dos idiomas configurados.

Para usuários recorrentes: armazenamos sua preferência de idioma da sessão anterior em um cookie do navegador. Se esse idioma estiver entre os configurados da sua marca, nós o usaremos. Caso contrário, seguiremos a mesma lógica alternativa: inglês (en-US), se disponível, ou o primeiro idioma configurado em ordem alfabética.

As seguintes localidades (códigos de idioma) são aceitas:

- Alemão (de-DE)
- Inglês (en-US)
- Espanhol (es-ES)

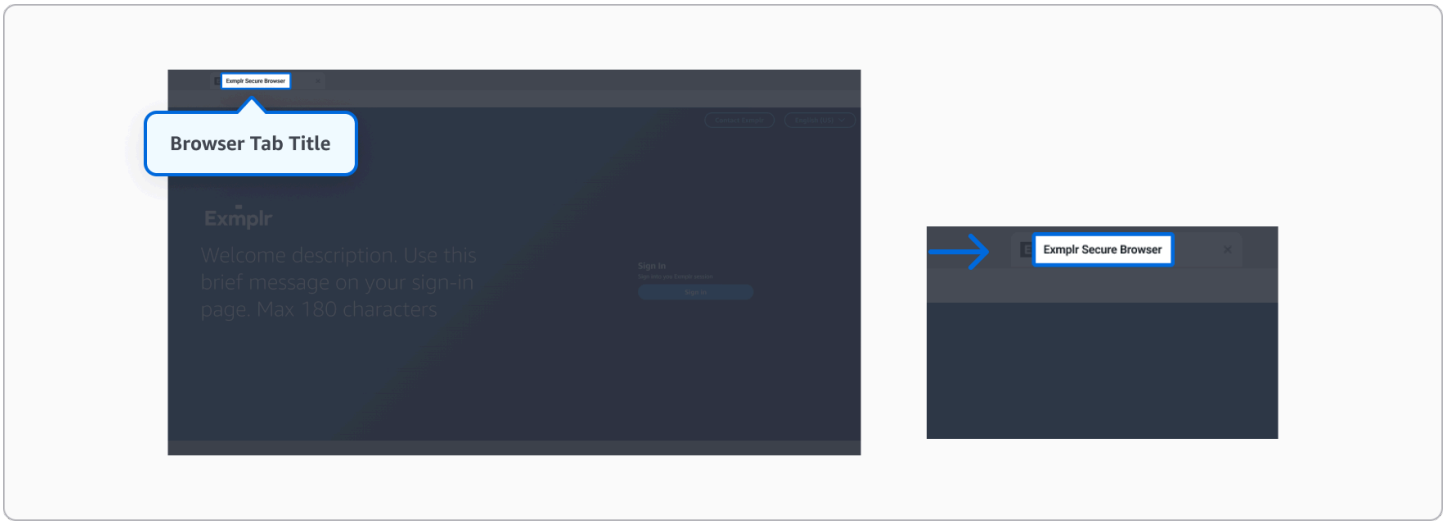
- Francês (fr-FR)
- Indonésio (id-ID)
- Italiano (it-IT)
- Japonês (ja-JP)
- Coreano (ko-KR)
- Português (pt-BR)
- Chinês: simplificado (zh-CN)
- Chinês: tradicional (zh-TW)

Por motivos de segurança, os seguintes caracteres estão bloqueados em todos os campos de texto:

- < (menor que)
- > (maior que)
- & (e comercial)
- ' (apóstrofo reto)
- ` (acento grave)
- ~ (til)
- \ (barra invertida).

Título da guia do navegador

O texto mostrado na guia do navegador. Máximo de 25 caracteres.

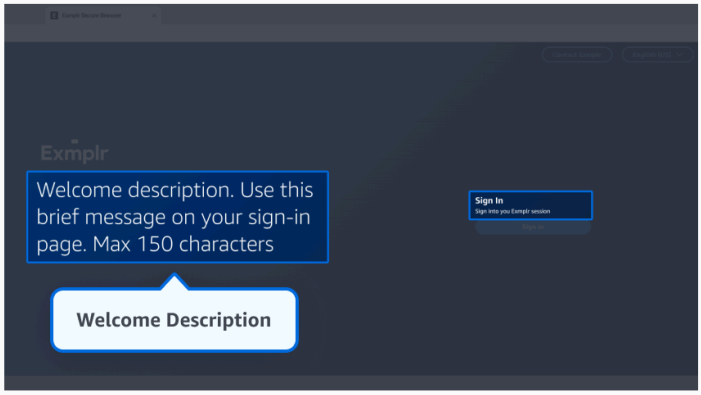


Recomendação

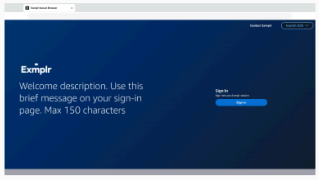
Considere usar títulos curtos e claros para que permaneçam legíveis mesmo quando várias guias estiverem abertas.

Descrição de boas-vindas

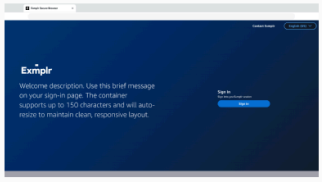
Uma breve descrição ao lado do logotipo da sua empresa na tela de login. Máximo de 150 caracteres.



Welcome description



Starting font sizing



Adapted sizing to Max characters

Recomendação

Mantenha o texto conciso para melhor legibilidade. Observe que textos mais longos serão automaticamente redimensionados para um tamanho de fonte menor, enquanto mensagens mais curtas serão exibidas com mais destaque.

Seção de contato

Botão de contato: opcional

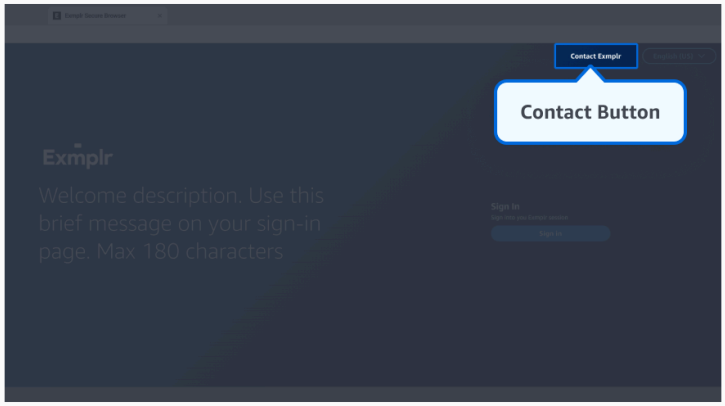
Texto do botão de contato na tela de login. Se for deixado em branco, “Entre em contato conosco” será exibido. Máximo de 30 caracteres.

Link de contato: opcional

Texto do botão de contato na tela de login. Você pode usar:

- Um URL HTTPS para direcionar os usuários para uma página da web.
- Um mailto: link para abrir o cliente de e-mail do usuário.

Se esse campo ficar em branco, o botão de contato ficará oculto na tela.



Recomendação

Mantenha o texto curto, idealmente de 2 a 3 palavras.

Seção de login

Cabeçalho de login: opcional

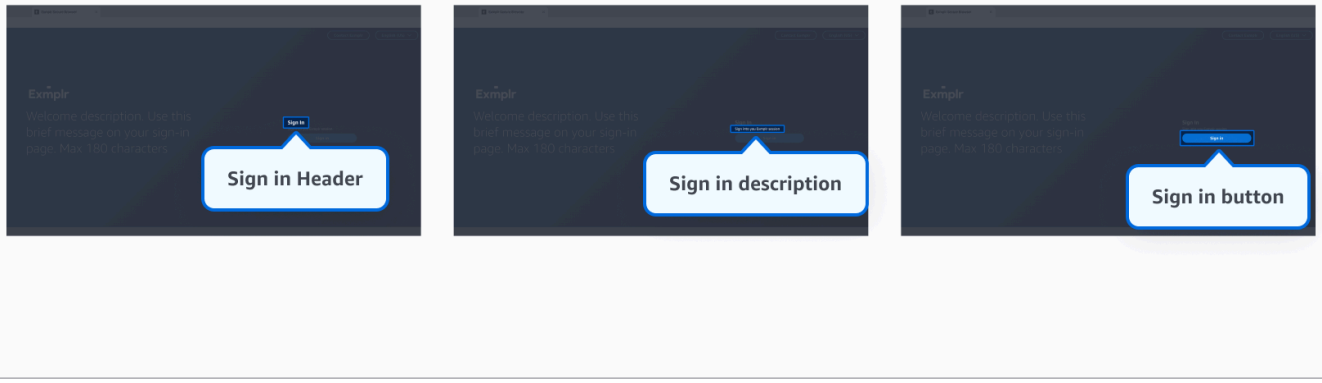
Cabeçalho da seção de login da página de login. Se for deixado em branco, “Entrar” será exibido. Máximo de 100 caracteres.

Descrição do login: opcional

Texto descritivo da seção de login. Se for deixado em branco, “Entrar na sessão do navegador WorkSpaces seguro” será exibido. Máximo de 250 caracteres.

Botão de login: opcional

Texto exibido no botão de login. Se for deixado em branco, “Entrar” será exibido. Máximo de 30 caracteres.

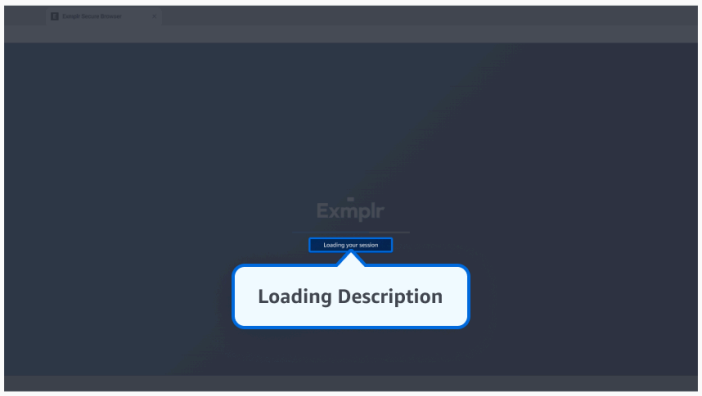


Recomendações

- Mantenha o texto curto.
- Considere que o botão de entrada direcione os usuários para o provedor de identidade configurado para seu portal. Você pode personalizar o texto do botão para refletir seu provedor de identidade específico.

Carregando descrição

Texto mostrado durante a conexão na tela de carregamento. Se for deixado em branco, “Conectando…” será exibido. Máximo de 300 caracteres.



Loading screen

Recomendação

Essa mensagem só é exibida enquanto a sessão está sendo carregada, portanto, os usuários finais podem não ter tempo de lê-la. Tente evitar demorar muito.

Termos de serviço: opcional

É possível personalizar os termos de serviço que os usuários finais devem analisar e aceitar antes de iniciarem uma sessão de streaming. Esse conteúdo pode ser adicionado fazendo upload de um arquivo Markdown ou usando o editor Markdown integrado.

Os usuários receberão os termos de serviço após o login bem-sucedido. Eles devem percorrer todo o documento e clicar no botão “Aceitar” para prosseguir com a sessão do Secure Browser. Se o usuário clicar em “Recusar”, ele será redirecionado de volta para a página de login.

Observe que essa é uma configuração opcional. Se você não adicionar um termo de serviço, os usuários seguirão diretamente para suas sessões após o login.

Formatação suportada:

- Estilos de texto básicos (negrito, itálico)
- Títulos
- Listas ordenadas e não ordenadas
- Cotações em bloco
- Regras horizontais
- Parágrafos e quebras de linha simples

Por motivos de segurança, os seguintes elementos estão bloqueados:

- Scripts e execução de código
- Elementos interativos como formulários e iframes
- Protocolos e caminhos de arquivo inseguros
- Atributos e estilo HTML
- Links e tabelas externos

Lembre-se de que seu arquivo de termos de serviço não deve exceder 150 KB.

Habilitando WebAuthn o suporte de redirecionamento no Amazon WorkSpaces Secure Browser

> **Warning**
>
> WebAuthn o redirecionamento só funciona em sessões do navegador com acesso à Internet ativado. Garanta que as configurações de rede do seu portal permitam o acesso à Internet para que a WebAuthn funcionalidade funcione corretamente.

WorkSpaces O Secure Browser suporta WebAuthn (Autenticação da Web) para sites acessados na sessão remota do navegador. Isso permite que os usuários se autentiquem em sites usando suas chaves de FIDO2 segurança locais, autenticadores biométricos e autenticadores de plataforma enquanto navegam na sessão do Navegador Seguro. WorkSpaces

> **Note**
>
> WebAuthn o redirecionamento está disponível para usuários finais que usam o Google Chrome 136 (ou posterior) ou o Microsoft Edge 137 (ou posterior). Esse recurso não está disponível para navegadores que não sejam Chromium, como Safari ou Firefox.
> Para habilitar a funcionalidade de WebAuthn redirecionamento, os administradores devem configurar as duas coisas:
>
> 1. Configurações do usuário do portal - Habilite o WebAuthn redirecionamento nas configurações do portal
> 2. Políticas de navegador local do usuário final - Configure a política do WebAuthenticationRemoteDesktopAllowedOrigins navegador nos dispositivos do usuário para permitir o redirecionamento WebAuthn

Tópicos

Habilitando WebAuthn o redirecionamento nas configurações do portal

Para habilitar o WebAuthn redirecionamento para sites acessados na sessão remota do navegador, siga estas etapas.

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 escolha Editar.
3. Navegue até a seção Configurações do usuário.
4. Em Permissões do usuário, defina Permitir que os usuários utilizem a autenticação local em sua sessão do portal como Permitido.
5. Escolha Salvar para aplicar a configuração.

Configurando a política do navegador local para WebAuthn

Além de habilitar o WebAuthn redirecionamento nas configurações do seu portal, a política do navegador local deve ser configurada para permitir o WebAuthn redirecionamento entre o dispositivo local do usuário e a sessão do navegador remoto e vice-versa. Essa configuração geralmente é gerenciada por administradores de TI para ambientes corporativos ou por usuários individuais para cenários de BYOD.

A política do navegador deve incluir o domínio de conteúdo do WorkSpaces Secure Browser da sua região. Adicione a seguinte origem à `WebAuthenticationRemoteDesktopAllowedOrigins` política com base na sua região:

`https://<region>.content.workspaces-web.com`

Por exemplo, em us-west-2: `https://us-west-2.content.workspaces-web.com`

O método de configuração específico depende se você está gerenciando navegadores em um ambiente corporativo ou configurando dispositivos individuais para usuários de BYOD. Para obter mais informações sobre a política do navegador, consulte a documentação da política do Chrome Enterprise e a documentação da política do Microsoft Edge.

> **Note**
>
> A reinicialização do navegador pode ser necessária para que a política entre em vigor.

Usando o WebAuthn redirecionamento em sessões remotas do navegador

Depois que o WebAuthn redirecionamento estiver habilitado nas configurações do portal e a política do navegador local estiver configurada, os usuários poderão usar a WebAuthn autenticação em sites em suas sessões de navegador remoto do WorkSpaces Secure Browser.

Os usuários podem se autenticar em sites usando:

- FIDO2 chaves de segurança conectadas ao dispositivo local
- Chaves de acesso
- Autenticadores de plataforma como Windows Hello ou Touch ID

O processo de WebAuthn autenticação é encaminhado sem problemas da sessão remota do navegador para o dispositivo local do usuário, fornecendo autenticação segura sem senha e mantendo os benefícios de segurança do ambiente de navegação remota.

Solução de problemas WebAuthn de redirecionamento

Se os usuários tiverem problemas com o WebAuthn redirecionamento nas sessões remotas do navegador, use as etapas de solução de problemas a seguir para identificar e resolver problemas comuns.

Tópicos

WebAuthn o redirecionamento não está funcionando

Se os prompts de WebAuthn autenticação não aparecerem ou não funcionarem:

1. Verifique se WebAuthn está habilitado nas configurações do portal em Permissões do usuário.
2. Verifique se a política do navegador local está configurada corretamente navegando até `chrome://policy` ou `edge://policy` confirmando se `WebAuthenticationRemoteDesktopAllowedOrigins` inclui o URL de conteúdo da sua região.
3. Verifique se a versão do navegador atende aos requisitos: Chrome 136+ ou Edge 137+.

4. Teste com um autenticador diferente (chave de segurança versus autenticador de plataforma).

Mensagens de erro comuns

A seguir estão as mensagens de erro comuns e suas resoluções:

WebAuthn mensagens de erro e resoluções

Mensagem de erro	Resolução
O WebAuthn redirecionamento do Amazon DCV falhou ao concluir a solicitação de registro: o redirecionamento Webauthn não é suportado pelo cliente	Verifique se você está usando um navegador e uma versão compatíveis (Chrome 136+ ou Edge 137+).
O prompt aparece, mas não é possível interagir com os autenticadores locais	Verifique se a extensão de WebAuthn redirecio namento Amazon DCV está instalada e habilitada em seu navegador remoto.
O WebAuthn redirecionamento do Amazon DCV falhou ao concluir a solicitação de registro: o ID da parte confiável não é um sufixo de domínio registrável nem igual ao domínio atual. Posteriormente, uma tentativa de buscar o recurso .well-known/webauthn do ID RP reivindicado falhou.	Isso significa que a política do navegador WebAuthenticationRemoteDesktopAllowe dOrigins local não é aplicada. Verifique a política e atualize para permitir o domínio do conteúdo. Verifique se o navegador foi reiniciad o. Talvez seja necessário iniciar uma nova sessão para que as alterações sejam aplicadas .
A operação atingiu o tempo limite ou não foi permitida. Consulte: https://www.w3. org/TR/we bauthn-2/#sctn-privacy-considerations-client.	Esse erro pode ocorrer se: (1) A extensão de WebAuthn redirecionamento DCV não estiver instalada ou habilitada, (2) O usuário cancelar a solicitação de autenticação, (3) o usuário inserir um PIN incorreto para sua chave de segurança ou (4) O usuário não interagir com a solicitação e a solicitação expirar.

Gerenciamento de controles da barra de ferramentas no Amazon WorkSpaces Secure Browser

Com os controles da barra de ferramentas, você pode configurar a apresentação da barra de ferramentas para as sessões do usuário final, incluindo as seguintes opções:

- Recursos
  - Área de transferência: quando ativada, permite copy/paste com controles granulares (somente copiar, somente colar ou ambos). Quando desativado, oculta o ícone e impede o uso da barra de ferramentas.
  - Transferência de arquivos: quando ativada, permite operações de arquivo com controles granulares (somente upload, somente download ou ambos). Quando desativado, oculta o ícone e impede transferências.
  - Microfone: quando ativado, permite o uso do microfone. Quando desativado, oculta o ícone.
  - Webcam: quando ativada, permite o uso da câmera. Quando desativado, oculta o ícone.
  - Monitor duplo: quando ativado, permite o uso de dois monitores. Quando desativado, oculta o ícone.
  - Tela cheia: quando ativada, ativa o modo de tela cheia. Quando desativado, oculta o ícone.
  - Windows: Quando ativado, permite mover-se entre janelas. Quando desativado, oculta o ícone.
- Configurações
  - Tema da barra de ferramentas: controla a exibição do modo claro ou escuro. A configuração remove o controle do tema do usuário final.
  - Estado da barra de ferramentas: define o estado encaixado ou desconectado da barra de ferramentas. A configuração remove o controle do usuário final sobre o estado da barra de ferramentas.
  - Resolução máxima: define a maior resolução de exibição permitida. Os usuários só podem selecionar resoluções até esse limite definido.

Configurando domínio personalizado para seu portal

Você pode configurar um domínio personalizado para um portal do Navegador WorkSpaces Seguro para permitir o acesso por meio de seu próprio nome de domínio em vez da URL padrão do portal. Esse recurso permite que você forneça aos usuários uma experiência mais integrada usando um domínio que se alinha à marca da sua organização.

Visão geral

O domínio personalizado permite que você personalize os seguintes aspectos da experiência do usuário:

- Acesso ao portal com marca — Os usuários acessam seu portal por meio do domínio da sua organização em vez do endpoint padrão da AWS.
- Experiência consistente do usuário - Mantenha a consistência da marca usando nomes de domínio familiares que se alinham à sua organização.

> **Note**
>
> Para personalizar a aparência visual e os elementos de identidade visual do seu portal, consultethe section called “Personalização da marca”.

Tópicos

Configurando domínio personalizado para seu portal

Como funciona

Quando você configura um domínio personalizado:

- Você cria e configura um proxy reverso com seu domínio personalizado para rotear o tráfego para o endpoint do portal.
- Os usuários acessam seu portal através do seu domínio personalizado em vez do endpoint padrão do portal.
- Os certificados SSL garantem conexões seguras durante todo o processo.

Pré-requisitos

Antes de configurar domínios personalizados, verifique se você tem:

- Um nome de domínio que você gerencia por meio de um provedor de serviços de DNS, como o Amazon Route53.
- Um portal de Navegador WorkSpaces Seguro. Para obter mais informações sobre a criação de um portal, consultethe section called “Criação de um portal da web”.
- Certifique-se de ter as permissões necessárias para gerenciar o AWS Certificate Manager e CloudFront as configurações de DNS.

Important

Os usuários devem habilitar cookies de terceiros para o domínio personalizado em seus navegadores para garantir a funcionalidade adequada do portal.
Certifique-se de que você possua e gerencie adequadamente o domínio personalizado e seus registros DNS para manter a segurança e a funcionalidade do seu portal.

Note

Para habilitar a extensão de login único para domínios personalizados, os usuários devem instalar a extensão no navegador com uma versão posterior à 1.0.2505.6608.
Os usuários são solicitados a instalar a extensão quando fazem login em um portal. Para obter detalhes sobre a experiência do usuário com a extensão, consulte the section called “Extensão de autenticação única”.

Introdução

Você pode configurar seu domínio personalizado como um atributo de configurações do portal ao criar um novo portal ou ao editar um portal existente. Isso pode ser feito usando os comandos AWS Console, SDK CloudFormation ou AWS CLI.

Recomendamos configurar uma CloudFront distribuição da Amazon como um proxy reverso que roteia o tráfego do seu domínio personalizado para o endpoint do portal WorkSpaces Secure Browser.

> **Note**
>
> Embora a Amazon CloudFront seja recomendada como solução de proxy reverso, você pode usar configurações alternativas de proxy reverso. Certifique-se de atender às configurações de origem e cache exigidas, conforme detalhado nas etapas de CloudFront configuração da Amazon.

Configurando CloudFront como proxy reverso

Para concluir a configuração de um proxy reverso, você precisa:

- Um certificado SSL por meio de AWS Certificate Manager (ACM)
- Uma CloudFront distribuição da Amazon
- Registros de DNS
- Portal configurado com seu domínio personalizado

SSL Certificate (Certificado SSL)

Se você ainda não tiver um, siga estas etapas para solicitar um por meio do ACM:

1. Navegue até o console do ACM emhttps://console.aws.amazon.com/acm.

   > **Important**
   >
   > Use a região Leste dos EUA (Norte da Virgínia), pois CloudFront exige que os certificados sejam armazenados lá.

2. Solicite um certificado:

   - Para novos usuários do ACM: escolha Começar em Provisionar certificados
   - Para usuários existentes do ACM: escolha Solicitar um certificado

3. Escolha Solicitar um certificado público e, em seguida, escolha Solicitar um certificado.

> **Note**
>
> Você também pode importar um certificado existente. Para obter mais informações, consulte Importação de certificados para o ACM no Guia do usuário do ACM.

4. Insira seu nome de domínio principal (por exemplo,**`myportal.example.com`**).
5. Escolha um método de validação:
   - Validação de DNS (recomendada para usuários do Route 53) — Permite a criação automática de conjuntos de registros em sua zona hospedada. Para obter mais informações, consulte Validação de DNS no Guia do usuário do ACM.
   - Validação de e-mail — Para obter mais informações, consulte Validação de e-mail no Guia do usuário do ACM.
6. Revise suas configurações e escolha Confirmar e solicitar.

CloudFront distribuição

Crie uma CloudFront distribuição para solicitações de proxy do seu domínio personalizado para o endpoint do portal.

1. Navegue até o CloudFront console emhttps://console.aws.amazon.com/cloudfront.
2. Escolha Criar distribuição.
   - Nome da distribuição: insira um nome para a distribuição
   - Tipo de distribuição: Site ou aplicativo único

> **Note**
>
> Se seu domínio personalizado for gerenciado no Route 53 na mesma conta da AWS, CloudFront poderá gerenciar automaticamente seu DNS para você. Insira seu domínio personalizado e clique em “Verificar domínio”. Se você tiver um domínio de um provedor de DNS diferente, pule esta etapa e configure seu domínio posteriormente.

3. Defina as configurações de origem:
   - Tipo de origem: Outro

- Origem personalizada: insira o endpoint do portal .workspaces-web.com *<portalId>*
- Caminho de origem: deixe em branco (padrão)

4. Personalize as configurações de origem:

   - Adicionar cabeçalho personalizado

     > **Important**
     >
     > O acesso ao portal por meio de domínio personalizado só funcionará se esse cabeçalho estiver presente em solicitações com proxy. Certifique-se de que o nome e o valor do cabeçalho estejam especificados exatamente como mencionado.

     - Nome do cabeçalho: workspacessecurebrowser-custom-domain
     - Valor: Seu domínio personalizado (por exemplo,**myportal.example.com**)
   - Protocolo: somente HTTPS
   - Porta HTTPS: 443 (mantenha o padrão)
   - Protocolo SSL original mínimo: TLSv1 .2 (padrão)
   - Tipo de endereço IP de origem: IPv4 somente (o Amazon WorkSpaces Secure Browser não oferece suporte IPv6 no momento da redação deste guia de administração).

5. Personalize as configurações de cache:

   - Política de protocolo do visualizador: redirecionar HTTP para HTTPS
   - Métodos HTTP permitidos: GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE
   - Política de cache: CachingDisabled
   - Política de solicitação de origem: AllViewerExceptHostHeader

     > **Important**
     >
     > O acesso ao portal por meio de domínio personalizado só funcionará se a política de solicitação de origem estiver definida como AllViewerExceptHostHeader. Como o nome sugere, essa política filtra somente o cabeçalho do host dos cabeçalhos da solicitação e passa todos os cabeçalhos restantes para a origem.

6. Você pode configurar o WAF se quiser, mas isso não é necessário para o propósito desta configuração.

7. Em Obter certificado TLS, selecione o certificado TLS criado na Etapa 1.
8. Revise as configurações e escolha Criar distribuição.

Registros DNS

O Cloudfront pode atualizar seus registros DNS no Route 53 para rotear o tráfego dos domínios especificados para a distribuição criada na Etapa 2, se sua zona hospedada estiver na mesma conta da AWS.

1. Navegue até CloudFront as configurações
2. Clique em “Encaminhar domínios para CloudFront”
3. Clique em “Configurar roteamento automaticamente”

Se você configurou o DNS para o domínio personalizado em outro provedor de serviços ou outra conta da AWS, configure seu provedor de DNS para rotear o tráfego do seu domínio para a distribuição. As etapas a seguir descrevem como fazer isso usando o Route 53.

1. Abra o console do Amazon Route 53 emhttps://console.aws.amazon.com/route53.
2. Acesse o gerenciamento de DNS:
   - Se você está começando a usar o Route 53 com essa AWS conta, a página de visão geral do Amazon Route 53 é aberta. Em Gerenciamento de DNS, escolha Começar agora.
   - Se você já usou o Route 53 com essa AWS conta, vá para a próxima etapa.
3. No painel de navegação, escolha Zonas hospedadas.
4. Crie uma zona hospedada se você ainda não tiver uma:
   - Para direcionar o tráfego da Internet para seus recursos, consulte Criação de uma zona hospedada pública no Guia do desenvolvedor do Amazon Route 53.
   - Para rotear o tráfego em sua VPC, consulte Criação de uma zona hospedada privada no Guia do desenvolvedor do Amazon Route 53.
5. Na página Zonas hospedadas, escolha o nome da zona hospedada que você deseja administrar.
6. Escolha Create Record Set (Criar conjunto de registros).
7. Crie uma entrada para seu domínio (por exemplo,**`myportal.example.com`**):
   - Tipo: A — IPv4 endereço

- Alias: Yes
- Alvo do alias: URL CloudFront de distribuição

Mantenha os valores padrão para todas as demais configurações.

> **Note**
>
> Se você não estiver usando o Route 53 para gerenciar o DNS do seu domínio, use seu provedor de serviços de DNS e adicione entradas de DNS que apontem para seu domínio na URL da sua distribuição. CloudFront

Como alternativa, você pode usar o CloudFormation modelo a seguir para criar sua CloudFront distribuição:

Esse CloudFormation modelo cria automaticamente a CloudFront distribuição, configura as configurações de proxy reverso e, opcionalmente, cria registros DNS do Route53:

Example workspaces-web-custom-domain-template.yaml

```
AWSTemplateFormatVersion: '2010-09-09'
Description: 'CloudFront Distribution for custom domain configuration with existing AWS
 WorkSpaces Secure Browser Portal'

Parameters:
  PortalEndpoint:
    Type: String
    Description: 'The endpoint of your existing WorkSpaces Web Portal (e.g.,
 abc123.workspaces-web.com)'
    AllowedPattern: '^[a-zA-Z0-9-]+(\.[a-zA-Z0-9-]+)?\.workspaces-web\.com$'
    ConstraintDescription: 'Must be a valid WorkSpaces Web portal endpoint'

  CustomDomainName:
    Type: String
    Description: 'Custom domain name for the portal (e.g., myportal.example.com)'
    AllowedPattern: '^([a-zA-Z0-9]?((?!-)([A-Za-z0-9-]*[A-Za-z0-9])\.)+[a-zA-Z0-9]+)$'
    ConstraintDescription: 'Must be a valid domain name'

  CertificateArn:
```

```
    Type: String
    Description: 'ARN of the validated SSL certificate in ACM (must be in us-east-1
 region for CloudFront)'
    AllowedPattern: 'arn:aws:acm:us-east-1:[0-9]{12}:certificate/[a-f0-9]{8}-[a-f0-9]
{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}'
    ConstraintDescription: 'Must be a valid ACM certificate ARN in us-east-1 region'

  CreateRoute53Record:
    Type: String
    Description: 'Create Route53 record for custom domain (requires existing hosted
 zone)'
    Default: 'No'
    AllowedValues:
      - 'Yes'
      - 'No'

  HostedZoneId:
    Type: String
    Description: 'Route53 Hosted Zone ID for the custom domain (required if creating
 Route53 record)'
    Default: ''

Conditions:
  ShouldCreateRoute53Record: !And
    - !Equals [!Ref CreateRoute53Record, 'Yes']
    - !Not [!Equals [!Ref HostedZoneId, '']]

Resources:
  # CloudFront Distribution
  CloudFrontDistribution:
    Type: AWS::CloudFront::Distribution
    Properties:
      DistributionConfig:
        Aliases:
          - !Ref CustomDomainName
        Comment: !Sub 'CloudFront distribution for WorkSpaces Web Portal -
 ${CustomDomainName}'
        Enabled: true
        HttpVersion: http2
        IPV6Enabled: false  # WorkSpaces Secure Browser does not support IPv6
        PriceClass: PriceClass_All

        # Origin Configuration
        Origins:
```

```
          - Id: WorkSpacesWebOrigin
            DomainName: !Ref PortalEndpoint
            CustomOriginConfig:
              HTTPSPort: 443
              OriginProtocolPolicy: https-only
              OriginSSLProtocols:
                - TLSv1.2
            OriginCustomHeaders:
              - HeaderName: workspacessecurebrowser-custom-domain
                HeaderValue: !Ref CustomDomainName

        # Default Cache Behavior
        DefaultCacheBehavior:
          TargetOriginId: WorkSpacesWebOrigin
          ViewerProtocolPolicy: https-only
          AllowedMethods:
            - GET
            - HEAD
            - OPTIONS
            - PUT
            - POST
            - PATCH
            - DELETE
          Compress: false
          # Cache Policy: CachingDisabled (using predefined managed policy)
          CachePolicyId: 4135ea2d-6df8-44a3-9df3-4b5a84be39ad
          # Origin Request Policy: AllViewerExceptHostHeader (using predefined managed
policy)
          OriginRequestPolicyId: b689b0a8-53d0-40ab-baf2-68738e2966ac

        # SSL Configuration
        ViewerCertificate:
          AcmCertificateArn: !Ref CertificateArn
          SslSupportMethod: sni-only
          MinimumProtocolVersion: TLSv1.2_2021

      Tags:
        - Key: Name
          Value: !Sub '${AWS::StackName}-cloudfront'

  # Route 53 Record (optional - requires hosted zone to exist)
  Route53Record:
    Type: AWS::Route53::RecordSet
    Condition: ShouldCreateRoute53Record
```

```
    Properties:
      HostedZoneId: !Ref HostedZoneId
      Name: !Ref CustomDomainName
      Type: A
      AliasTarget:
        DNSName: !GetAtt CloudFrontDistribution.DomainName
        HostedZoneId: Z2FDTNDATAQYW2  # CloudFront Hosted Zone ID
        EvaluateTargetHealth: false

Outputs:
  PortalEndpoint:
    Description: 'WorkSpaces Web Portal endpoint used as origin'
    Value: !Ref PortalEndpoint
    Export:
      Name: !Sub '${AWS::StackName}-PortalEndpoint'

  CustomDomainEndpoint:
    Description: 'Custom domain endpoint for the portal'
    Value: !Sub 'https://${CustomDomainName}'
    Export:
      Name: !Sub '${AWS::StackName}-CustomDomainEndpoint'

  CloudFrontDistributionId:
    Description: 'CloudFront Distribution ID'
    Value: !Ref CloudFrontDistribution
    Export:
      Name: !Sub '${AWS::StackName}-CloudFrontDistributionId'

  CloudFrontDomainName:
    Description: 'CloudFront Distribution Domain Name'
    Value: !GetAtt CloudFrontDistribution.DomainName
    Export:
      Name: !Sub '${AWS::StackName}-CloudFrontDomainName'

  CertificateArn:
    Description: 'SSL Certificate ARN used by CloudFront'
    Value: !Ref CertificateArn
    Export:
      Name: !Sub '${AWS::StackName}-CertificateArn'

Metadata:
  AWS::CloudFormation::Interface:
    ParameterGroups:
      - Label:
```

```
          default: "Existing Portal Configuration"
        Parameters:
          - PortalEndpoint
      - Label:
          default: "Custom Domain Configuration"
        Parameters:
          - CustomDomainName
          - CertificateArn
          - CreateRoute53Record
          - HostedZoneId
    ParameterLabels:
      PortalEndpoint:
        default: "Portal Endpoint"
      CustomDomainName:
        default: "Custom Domain Name"
      CertificateArn:
        default: "SSL Certificate ARN"
      CreateRoute53Record:
        default: "Create Route53 Record"
      HostedZoneId:
        default: "Hosted Zone ID"
```

Para usar esse modelo:

1. Salve o modelo acima como `workspaces-web-custom-domain-template.yaml`
2. Implante usando o AWS console, a AWS CLI ou o AWS SDK com seus valores de parâmetros específicos
3. Após a implantação, configure seu portal com o domínio personalizado conforme descrito na Etapa 4 abaixo

Configuração do portal

Registre seu domínio personalizado como um atributo de configurações do portal usando o AWS console, a UpdatePortal API ou o comando da CLI AWS update-portal.

1. Abra o console do WorkSpaces Secure Browser emhttps://console.aws.amazon.com/workspaces-web/home.
2. No painel de navegação, selecione Portais da Web.
3. Selecione o portal da web que você deseja configurar e escolha Editar.

4. Nas configurações do portal, adicione seu domínio personalizado.
5. Salve a configuração do portal.

Teste sua configuração

Para testar sua configuração, siga estas etapas:

1. Abra um navegador da Web e navegue até o URL do seu domínio personalizado (por exemplo,**`https://myportal.example.com`**).
2. Se tudo estiver configurado corretamente, você deverá ver a página de entrada do seu portal.
3. Em seguida, insira a URL do portal em seu navegador, você deve ser redirecionado para o domínio personalizado após fazer login no seu IdP.
4. Finalmente, entre no seu IdP e clique no mosaico do aplicativo do seu portal. Você deve ser redirecionado para um domínio personalizado.

Solução de problemas de domínio personalizado

Se os usuários tiverem problemas com o acesso ao portal por meio de domínio personalizado em suas sessões de navegador remoto, use as seguintes etapas de solução de problemas para identificar e resolver problemas comuns.

Tópicos

Mensagens de erro comuns

Veja a seguir mensagens de erro comuns e suas resoluções ao configurar domínios personalizados:

Erro de token CSRF inválido

Esse erro ocorre quando o Secure Browser não recebe sua solicitação corretamente por meio da CloudFront configuração.

Para resolver esse problema:

- Verifique as configurações de origem personalizadas em sua CloudFront distribuição.

- Verifique se o nome do cabeçalho personalizado corresponde exatamente `workspacessecurebrowser-custom-domain` e se o valor corresponde exatamente ao seu domínio personalizado (sem https://ou qualquer parâmetro de consulta).
- Limpe o cache do seu navegador local.
- Invalide o cache ativado. CloudFront

502 Erro de gateway incorreto

Esse erro normalmente indica problemas de configuração do cache.

Para resolver esse problema:

- Verifique as configurações de cache na sua CloudFront distribuição.
- Verifique se a política de cache está definida como`CachingDisabled`.
- Verifique se a política de solicitação do Origin está definida como`AllViewerExceptHostHeader`.
- Limpe o cache do seu navegador local.
- Invalide o cache ativado. CloudFront

Erro de acesso negado

Esse erro pode ocorrer se seu domínio personalizado estiver configurado incorretamente.

Para resolver esse problema:

- Verifique as configurações de origem em sua CloudFront distribuição.
- Verifique se a origem está definida como a URL correta do portal.
- Verifique se o portal está configurado com o domínio personalizado correto.
- Limpe o cache do seu navegador local.
- Invalide o cache ativado. CloudFront

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 o conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para saber mais sobre a privacidade de dados, consulte as Data Privacy FAQ. Para saber mais sobre a proteção de dados na Europa, consulte a postagem do blog AWS Shared Responsibility Model and RGPD no Blog de segurança da AWS .

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

- Use uma autenticação multifator (MFA) com cada conta.
- Use SSL/TLS para se comunicar com AWS os recursos. Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure a API e o registro de atividades do usuário com AWS CloudTrail. Para obter informações sobre o uso de CloudTrail trilhas para capturar AWS atividades, consulte Como trabalhar com CloudTrail trilhas no Guia AWS CloudTrail do usuário.
- 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 sensíveis armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-3 ao acessar AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint FIPS. Para saber mais sobre os endpoints FIPS disponíveis, consulte Federal Information Processing Standard (FIPS) 140-3.

É altamente recomendável que nunca sejam colocadas informações confidenciais ou sensíveis, como endereços de e-mail de clientes, em tags 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 console AWS CLI, a API ou AWS SDKs. Quaisquer dados inseridos em tags ou em 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 fortemente recomendável que não sejam incluídas informações de credenciais no URL para validar a solicitação nesse servidor.

Tópicos

Criptografia de dados no Amazon WorkSpaces Secure Browser

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 modelos do IAM para criar um perfil de acesso total ou 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 para o Amazon WorkSpaces Secure Browser

A criptografia em repouso é configurada por padrão e todos os dados do cliente (por exemplo, declarações de política do navegador, nomes de usuário, registros ou endereços IP) usados no Navegador WorkSpaces Seguro são criptografados usando AWS KMS. Por padrão, o WorkSpaces Secure Browser habilita a criptografia com uma AWS chave própria. Você também pode usar uma chave gerenciada pelo cliente (CMK), especificando sua CMK na criação de recursos. Este é o único valor aceito no momento via CLI.

Se você optar por passar uma CMK, a chave fornecida deverá ser uma AWS KMS chave de criptografia simétrica e você, como administrador, deverá ter as seguintes permissões:

```
kms:DescribeKey

kms:GenerateDataKey

kms:GenerateDataKeyWithoutPlaintext

kms:Decrypt

kms:ReEncryptTo
kms:ReEncryptFrom
```

Se você usar uma CMK, precisará permitir que o responsável pelo serviço externo do WorkSpaces Secure Browser acesse a chave.
Para obter mais informações, consulte Exemplo de política de chaves CMK com escopo definido com aws: SourceAccount

Sempre que possível, o WorkSpaces Secure Browser usará as credenciais do Forward Access Sessions (FAS) para acessar sua chave. Para obter mais informações sobre o FAS, consulte Sessões de acesso direto.

Há casos em que o WorkSpaces Secure Browser pode precisar acessar sua chave de forma assíncrona. Ao listar o principal serviço externo do WorkSpaces Secure Browser em sua política de chaves, o WorkSpaces Secure Browser poderá realizar o conjunto permitido de operações criptográficas com sua chave.

Depois que um recurso é criado com a chave, ela não pode ser removida nem alterada. Se você usou uma CMK, você, como administrador que acessa o recurso, deve ter as seguintes permissões:

```
kms:GenerateDataKey
kms:GenerateDataKeyWithoutPlaintext
kms:Decrypt

kms:ReEncryptTo
kms:ReEncryptFrom
```

Se você ver um erro de Acesso negado ao usar o console, é provável que o usuário que está acessando o console não tenha as permissões necessárias para usar a CMK na chave atual.

Principais exemplos de políticas e escopo para o WorkSpaces Secure Browser

CMKs exigem a seguinte política fundamental:

```
{
  "Version": "2012-10-17",
  "Statement": [
  ...,
    {
      "Sid": "Allow WorkSpaces Secure Browser to encrypt/decrypt",
      "Effect": "Allow",
      "Principal": {
        "Service": "workspaces-web.amazonaws.com"
      },
      "Action": [
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
       ],
      "Resource": "*",
      }
```

```
    ]
}
```

As seguintes permissões são exigidas pelo WorkSpaces Secure Browser:

- `kms:DescribeKey`— Valida se a AWS KMS chave fornecida está configurada corretamente.
- `kms:GenerateDataKeyWithoutPlaintext`e `kms:GenerateDataKey` — Solicitação da AWS KMS chave para criar chaves de dados usadas para criptografar objetos.
- `kms:Decrypt`— Solicita a AWS KMS chave para descriptografar as chaves de dados criptografadas. Essas chaves de dados são usadas para criptografar seus dados.
- `kms:ReEncryptToe` `kms:ReEncryptFrom` — Solicitação da AWS KMS chave para permitir a recriptografia de ou para uma chave KMS.

Definindo o escopo das permissões do WorkSpaces Secure Browser em sua chave AWS KMS

Quando o diretor em uma declaração de política chave é um diretor de AWS serviço, é altamente recomendável que você use as chaves de condição SourceAccount globais aws: SourceArn ou aws:, além do contexto de criptografia.

O contexto de criptografia utilizado para um recurso sempre conterá uma entrada no formato `aws:workspaces-web:RESOURCE_TYPE:id` e o ID do recurso correspondente.

O ARN de origem e os valores da conta de origem são incluídos no contexto de autorização somente quando uma solicitação AWS KMS vem de outro AWS serviço. Essa combinação de condições implementa permissões de privilégio mínimo e evita um possível cenário de auxiliar confuso. Para obter mais informações, consulte Permissões para serviços da AWS nas políticas de chave.

```
  "Condition": {
       "StringEquals": {
         "aws:SourceAccount": "AccountId",
         "kms:EncryptionContext:aws:workspaces-web:resourceType:id": "resourceId"
       },
       "ArnEquals": {
         "aws:SourceArn": [
           "arn:aws:workspaces-web:Region:AccountId:resourceType/resourceId"
         ]
       },
     }
```

> **Note**
>
> Antes da criação do recurso, a política de chave deve usar apenas a Condição `aws:SourceAccount`, pois o ARN completo do recurso ainda não terá sido criado. Após a criação do recurso, a política de chave pode ser atualizada para incluir as Condições `aws:SourceArn` e `kms:EncryptionContext`.

Exemplo da política de chaves CMK com escopo definido com **`aws:SourceAccount`**

```
{
  "Version": "2012-10-17",
  "Statement": [
  ...,
    {
      "Sid": "Allow WorkSpaces Secure Browser to encrypt/decrypt",
      "Effect": "Allow",
      "Principal": {
        "Service": "workspaces-web.amazonaws.com"
      },
      "Action": [
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
       ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "<AccountId>"
        }
      }
    }
  ]
}
```

Exemplo da política de chave CMK com escopo definido e caractere curinga de recursos **aws:SourceArn**

```
{
  "Version": "2012-10-17",
  "Statement": [
  ...,
    {
      "Sid": "Allow WorkSpaces Secure Browser to encrypt/decrypt",
      "Effect": "Allow",
      "Principal": {
        "Service": "workspaces-web.amazonaws.com"
      },
      "Action": [
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
       ],
      "Resource": "*",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:workspaces-web:<Region>:<AccountId>:*/*"
        }
      }
    }
  ]
}
```

Exemplo da política de chaves CMK com escopo definido com **aws:SourceArn**

```
{
  "Version": "2012-10-17",
  "Statement": [
  ...,
    {
      "Sid": "Allow WorkSpaces Secure Browser to encrypt/decrypt",
      "Effect": "Allow",
      "Principal": {
        "Service": "workspaces-web.amazonaws.com"
      },
```

```
      "Action": [
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
       ],
      "Resource": "*",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": [
            "arn:aws:workspaces-web:<Region>:<AccountId>:portal/*",
            "arn:aws:workspaces-web:<Region>:<AccountId>:browserSettings/*",
            "arn:aws:workspaces-web:<Region>:<AccountId>:userSettings/*",
            "arn:aws:workspaces-web:<Region>:<AccountId>:ipAccessSettings/*"
          ]
        }
    }
  ]
}
```

> **Note**
>
> Depois de criar o recurso, você pode atualizar o caractere curinga em `SourceArn` para ele. Se você usa o WorkSpaces Secure Browser para criar um novo recurso que exija acesso à CMK, certifique-se de atualizar sua política de chaves adequadamente.

Exemplo da política de chave CMK com **`aws:SourceArn`** e **`EncryptionContext`** específico do recurso

```
{
  "Version": "2012-10-17",
  "Statement": [
  ...,
    {
      "Sid": "Allow WorkSpaces Secure Browser to encrypt/decrypt portal",
      "Effect": "Allow",
      "Principal": {
        "Service": "workspaces-web.amazonaws.com"
      },
```

```
      "Action": [
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
       ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "<AccountId>",
            "kms:EncryptionContext:aws:workspaces-web:portal:id": "<portalId>>"
        }
      }
    },
    {
      "Sid": "Allow WorkSpaces Secure Browser to encrypt/decrypt userSettings",
      "Effect": "Allow",
      "Principal": {
        "Service": "workspaces-web.amazonaws.com"
      },
      "Action": [
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
       ],
      "Resource": "*",
      "Condition": {
         "StringEquals": {
            "aws:SourceAccount": "<AccountId>",
            "kms:EncryptionContext:aws:workspaces-web:userSetttings:id":
"<userSetttingsId>"
        }
      }
    },
    {
      "Sid": "Allow WorkSpaces Secure Browser to encrypt/decrypt browserSettings",
      "Effect": "Allow",
      "Principal": {
        "Service": "workspaces-web.amazonaws.com"
```

```
      },
      "Action": [
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
       ],
      "Resource": "*",
      "Condition": {
         "StringEquals": {
            "aws:SourceAccount": "<AccountId>",
            "kms:EncryptionContext:aws:workspaces-web:browserSettings:id":
 "<browserSettingsId>"
        }
      }
    },
    {
      "Sid": "Allow WorkSpaces Secure Browser to encrypt/decrypt ipAccessSettings",
      "Effect": "Allow",
      "Principal": {
        "Service": "workspaces-web.amazonaws.com"
      },
      "Action": [
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
       ],
      "Resource": "*",
      "Condition": {
         "StringEquals": {
            "aws:SourceAccount": "<AccountId>",
            "kms:EncryptionContext:aws:workspaces-web:ipAccessSettings:id":
 "<ipAccessSettingsId>"
        }
      }
    },
  ]
}
```

> **Note**
>
> Certifique-se de criar declarações separadas ao incluir um `EncryptionContext` específico do recurso na mesma política de chave. Para obter mais informações, consulte a seção Usando vários pares de contexto de criptografia em kms:EncryptionContext: chave de contexto.

Criptografia em trânsito para o Amazon WorkSpaces Secure Browser

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

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

Gerenciamento de chaves para o Amazon WorkSpaces Secure Browser

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. É possível definir sua chave usando o SDK da AWS .

Privacidade do tráfego entre redes no Amazon WorkSpaces Secure Browser

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 da sua própria VPC. A conexão com aplicativos locais é configurada em sua própria VPC e não é controlada pelo Secure Browser. WorkSpaces

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 a serviços para o Amazon Secure WorkSpaces Browser.

Login de acesso do usuário no Amazon WorkSpaces Secure Browser

Os administradores podem registrar os eventos da sessão do WorkSpaces Secure Browser, incluindo visitas de início, término e URL. Esses logs são criptografados e entregues com segurança aos clientes por meio de um Amazon Kinesis Data Stream. As informações de navegação do registro de acesso do usuário não são AWS armazenadas nem estão disponíveis nas sessões sem o registro configurado. As visitas ao URL 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. Os administradores do IAM controlam quem pode ser autenticado (conectado) e autorizado (tem permissões) para usar os recursos do WorkSpaces Secure Browser. O IAM é 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 com base na sua função:

- Usuário do serviço: solicite permissões ao seu administrador se você não conseguir acessar os atributos (consulte Solução de problemas de identidade e acesso ao Amazon WorkSpaces Secure Browser).
- Administrador do serviço: determine o acesso do usuário e envie solicitações de permissão (consulte Como o Amazon WorkSpaces Secure Browser funciona com o IAM)
- Administrador do IAM: escreva políticas para gerenciar o acesso (consulte Exemplos de políticas baseadas em identidade para o Amazon Secure WorkSpaces Browser)

Autenticação com identidades

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

Você pode fazer login como uma identidade federada usando credenciais de uma fonte de identidade como Centro de Identidade do AWS IAM (IAM Identity Center), autenticação de login único ou credenciais. Google/Facebook Para ter mais informações sobre como fazer login, consulte Como fazer login em sua Conta da AWS no Guia do usuário do Início de Sessão da AWS .

Para acesso programático, AWS fornece um SDK e uma CLI para assinar solicitações criptograficamente. Para ter mais informações, consulte AWS Signature Version 4 para solicitações de API no Guia do usuário do IAM.

Conta da AWS usuário root

Ao criar um Conta da AWS, você começa com uma identidade de login chamada usuário Conta da AWS raiz que tem acesso completo a todos Serviços da AWS os recursos. É altamente recomendável não usar o usuário-raiz em tarefas diárias. Consulte as tarefas que exigem credenciais de usuário-raiz em Tarefas que exigem credenciais de usuário-raiz no Guia do usuário do IAM.

Identidade federada

Como prática recomendada, exija que os usuários humanos 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 corporativo, provedor de identidade da web ou Directory Service que acessa Serviços da AWS usando credenciais de uma fonte de identidade. As identidades federadas assumem funções que oferecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, recomendamos Centro de Identidade do AWS IAM. Para saber mais, consulte O que é o IAM Identity Center? no Guia do usuário do Centro de Identidade do AWS IAM .

Usuários e grupos do IAM

Um usuário do IAM é uma identidade com permissões específicas para uma única pessoa ou aplicação. É recomendável usar credenciais temporárias, em vez de usuários do IAM com credenciais de longo prazo. Para obter mais informações, consulte Exigir que usuários humanos usem a federação com um provedor de identidade para acessar AWS usando credenciais temporárias no Guia do usuário do IAM.

Um grupo do IAM especifica um conjunto de usuários do IAM e facilita o gerenciamento de permissões para grandes conjuntos de usuários. Para ter mais informações, consulte Casos de uso de usuários do IAM no Guia do usuário do IAM.

Perfis do IAM

Uma perfil do IAM é uma identidade com permissões específicas que oferece credenciais temporárias. Você pode assumir uma função mudando de um usuário para uma função do IAM (console) ou chamando uma operação de AWS API AWS CLI ou. Para saber mais, consulte Métodos para assumir um perfil no Manual do usuário do IAM.

Os perfis do IAM são úteis para acesso de usuário federado, permissões de usuário do IAM temporárias, acesso entre contas, acesso entre serviços e aplicações em execução no Amazon EC2. Consulte mais informações em Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

Gerenciar o acesso usando políticas

Você controla o acesso AWS criando políticas e anexando-as a AWS identidades ou recursos. Uma política define permissões quando associada a uma identidade ou recurso. AWS avalia essas políticas quando um diretor faz uma solicitação. A maioria das políticas é armazenada AWS como documentos JSON. Para ter mais informações sobre documentos de política JSON, consulte Visão geral das políticas JSON no Guia do usuário do IAM.

Por meio de políticas, os administradores especificam quem tem acesso a que, definindo qual entidade principal pode realizar ações em quais recursos e sob quais condições.

Por padrão, usuários e perfis não têm permissões. Um administrador do IAM cria políticas do IAM e as adiciona aos perfis, os quais os usuários podem então assumir. As políticas do IAM definem permissões, independentemente do método usado para realizar a operação.

Políticas baseadas em identidade

As políticas baseadas em identidade são documentos de políticas de permissão JSON que você anexa a uma identidade (usuário, grupo ou perfil). Essas políticas controlam quais ações as identidades podem realizar, em quais recursos e sob quais condições. Para saber como criar uma política baseada em identidade, consulte Definir permissões personalizadas do IAM com as políticas gerenciadas pelo cliente no Guia do Usuário do IAM.

As políticas baseadas em identidade podem ser políticas em linha (incorporadas diretamente em uma única identidade) ou políticas gerenciadas (políticas autônomas anexadas a várias identidades). Para saber como escolher entre uma política gerenciada e políticas em linha, consulte Escolher entre políticas gerenciadas e políticas em linha no Guia do usuário do IAM.

Políticas baseadas em recursos

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. Entre os exemplos estão políticas de confiança de perfil do IAM e políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. É necessário especificar uma entidade principal em uma política baseada em recursos.

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

Outros tipos de política

AWS oferece suporte a tipos de políticas adicionais que podem definir o máximo de permissões concedidas por tipos de políticas mais comuns:

- Limites de permissões: definem o número máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM. Para saber mais sobre limites de permissões, consulte Limites de permissões para identidades do IAM no Guia do usuário do IAM.
- Políticas de controle de serviço (SCPs) — Especifique as permissões máximas para uma organização ou unidade organizacional em AWS Organizations. Para saber mais, consulte Políticas de controle de serviço no Guia do usuário do AWS Organizations .

- Políticas de controle de recursos (RCPs) — Defina o máximo de permissões disponíveis para recursos em suas contas. Para obter mais informações, consulte Políticas de controle de recursos (RCPs) no Guia AWS Organizations do usuário.
- Políticas de sessão: políticas avançadas transmitidas como um parâmetro durante a criação de uma sessão temporária para um perfil ou um usuário federado. Para saber mais, consulte Políticas de sessão no Guia do usuário do IAM.

Vários tipos de política

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

Como o Amazon WorkSpaces Secure Browser funciona com o IAM

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

Recursos do IAM que você pode usar com o Amazon WorkSpaces Secure Browser

Recurso do IAM	WorkSpaces Suporte ao Secure Browser
Políticas baseadas em identidade	Sim
Políticas baseadas em recurso	Não
Ações de políticas	Sim
Recursos de políticas	Sim
Chaves de condição de políticas	Sim
ACLs	Não
ABAC (tags em políticas)	Parcial
Credenciais temporárias	Sim

Recurso do IAM	WorkSpaces Suporte ao Secure Browser
Permissões de entidade principal	Sim
Perfis de serviço	Não
Perfis vinculados ao serviço	Sim

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

Tópicos

- Políticas baseadas em identidade para WorkSpaces o Secure Browser
- Políticas baseadas em recursos no Secure WorkSpaces Browser
- Ações de política para o WorkSpaces Secure Browser
- Recursos de política para o WorkSpaces Secure Browser
- Chaves de condição de política para o WorkSpaces Secure Browser
- Listas de controle de acesso (ACLs) no WorkSpaces Secure Browser
- Controle de acesso baseado em atributos (ABAC) com Secure Browser WorkSpaces
- Usando credenciais temporárias com o WorkSpaces Secure Browser
- Permissões principais entre serviços para o WorkSpaces Secure Browser
- Funções de serviço para o WorkSpaces Secure Browser
- Funções vinculadas ao serviço para WorkSpaces o Secure Browser

Políticas baseadas em identidade para WorkSpaces o Secure Browser

Compatível com políticas baseadas em identidade: sim

As políticas baseadas em identidade são documentos de políticas de permissões JSON que podem ser anexados a uma identidade, como usuário do IAM, grupo de usuários ou perfil. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Definir permissões personalizadas do IAM com as políticas gerenciadas pelo cliente no Guia do Usuário do IAM.

Com as políticas baseadas em identidade do IAM, é possível especificar ações e recursos permitidos ou negados, assim como as condições sob as quais as ações são permitidas ou negadas. Para saber mais sobre todos os elementos que podem ser usados em uma política JSON, consulte Referência de elemento de política JSON do IAM no Guia do usuário do IAM.

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

Compatibilidade com políticas baseadas em recursos: não

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

Para permitir o acesso entre contas, é possível especificar uma conta inteira ou as entidades do IAM em outra conta como a entidade principal em uma política baseada em recursos. Consulte mais informações em Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

Ações de política para o WorkSpaces Secure Browser

Compatível com ações de políticas: sim

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

O elemento `Action` de uma política JSON descreve as ações que podem ser usadas para permitir ou negar acesso em uma política. 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 declaração, 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 políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento de política JSON `Resource` especifica o objeto ou os objetos aos quais a ação se aplica. Como prática recomendada, especifique um recurso usando seu nome do recurso da Amazon (ARN). Para ações que não oferecem compatibilidade com permissões em nível de recurso, 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 seus ARNs, consulte Recursos definidos pelo Amazon WorkSpaces Secure Browser na Referência de Autorização de Serviço. Para saber com quais ações você pode especificar o ARN de cada recurso, consulte Ações definidas pelo Amazon WorkSpaces 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

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

O elemento `Condition` especifica quando as instruções são executadas com base em critérios definidos. 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. Para ver todas as chaves de condição AWS globais, consulte as chaves de contexto de condição AWS global no Guia do usuário do IAM.

Para ver uma lista das chaves de condição do WorkSpaces 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

Suportes ACLs: Não

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

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

Compatível com ABAC (tags em políticas): parcial

O controle de acesso por atributo (ABAC) é uma estratégia de autorização que define permissões com base em atributos chamados de tags. Você pode anexar tags a entidades e AWS recursos do IAM e, em seguida, criar políticas ABAC para permitir operações quando a tag do diretor corresponder à tag no recurso.

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 for compatível com as três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço for compatível com as três chaves de condição somente para alguns tipos de recursos, o valor será Parcial

Para saber mais sobre o ABAC, consulte Definir permissões com autorização do ABAC no Guia do usuário do IAM. Para visualizar um tutorial com etapas para configurar o ABAC, consulte Usar controle de acesso por atributo (ABAC) no Guia do usuário do IAM.

Usando credenciais temporárias com o WorkSpaces Secure Browser

Compatível com credenciais temporárias: sim

As credenciais temporárias fornecem acesso de curto prazo aos AWS recursos e são criadas automaticamente quando você usa a federação ou troca de funções. AWS recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para ter mais informações, consulte Credenciais de segurança temporárias no IAM e Serviços da Serviços da AWS que funcionam com o IAM no Guia do usuário do IAM.

Permissões principais entre serviços para o WorkSpaces Secure Browser

Compatibilidade com o recurso de encaminhamento de sessões de acesso (FAS): sim

As sessões de acesso direto (FAS) usam as permissões do principal chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) de fazer solicitações aos serviços posteriores. Para obter detalhes da política ao fazer solicitações de FAS, consulte Sessões de acesso direto.

Funções de serviço para o WorkSpaces Secure Browser

Compatível com perfis de serviço: não

O perfil de serviço é um perfil do IAM que um serviço assume para executar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para saber mais, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do Usuário do IAM.

> **Warning**
>
> Alterar as permissões de uma função de serviço pode 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

Compatibilidade com 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 assumir o perfil 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 administrador do IAM pode visualizar, mas não editar as permissões para perfis vinculados ao serviço.

Para obter detalhes sobre como criar ou gerenciar perfis vinculados a serviços, consulte Serviços da AWS que funcionam com o IAM. Encontre um serviço na tabela que inclua um `Yes` na coluna Perfil vinculado ao serviço. Escolha o link Sim para visualizar a documentação do perfil vinculado a 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. Para conceder permissão aos usuários para executar ações nos recursos que eles precisam, um administrador do IAM pode criar políticas do IAM.

Para aprender a criar uma política baseada em identidade do IAM ao usar esses documentos de política em JSON de exemplo, consulte Criar políticas do IAM (console) no Guia do usuário do IAM.

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 baseada em identidade para o Amazon WorkSpaces Secure Browser
- Usando o console do Amazon WorkSpaces Secure Browser
- Permitindo que os usuários visualizem suas próprias permissões para o Amazon WorkSpaces Secure Browser

Melhores práticas de política baseada em identidade para o Amazon WorkSpaces Secure Browser

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 sua 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 saber mais, consulte Políticas gerenciadas pela AWS ou Políticas gerenciadas pela AWS para funções de trabalho no Guia do usuário do IAM.
- Aplique permissões de privilégio mínimo: ao definir permissões com as políticas do IAM, conceda apenas as permissões necessárias para executar uma tarefa. Você faz isso definindo as ações que podem ser executadas em recursos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para saber mais sobre como usar o IAM para aplicar permissões, consulte Políticas e permissões no IAM no Guia do usuário do IAM.
- Use condições nas políticas do IAM para restringir ainda mais o acesso: é possível adicionar uma condição às políticas para limitar o acesso a ações e recursos. Por exemplo, é possível escrever uma condição de política para especificar que todas as solicitações devem ser enviadas usando SSL. Você também pode usar condições para conceder acesso às ações de serviço se elas forem usadas por meio de uma ação específica AWS service (Serviço da AWS), como CloudFormation. Para saber mais, consulte Elementos da política JSON do IAM: condição no Guia do usuário do IAM.
- Use o IAM Access Analyzer para validar suas políticas do IAM a fim de garantir permissões seguras e funcionais: o IAM Access Analyzer valida as políticas novas e existentes para que elas sigam a linguagem de política do IAM (JSON) e as práticas recomendadas do IAM. O IAM Access Analyzer oferece mais de cem verificações de política e recomendações práticas para ajudar a criar políticas seguras e funcionais. Para saber mais, consulte Validação de políticas do IAM Access Analyzer no Guia do Usuário do IAM.
- Exigir autenticação multifator (MFA) — Se você tiver um cenário que exija usuários do IAM ou um usuário root, ative Conta da AWS a MFA para obter segurança adicional. Para exigir MFA quando

as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para saber mais, consulte Configuração de acesso à API protegido por MFA no Guia do Usuário do IAM.

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

Usando o console do Amazon 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. Caso crie uma política baseada em identidade mais restritiva que as permissões mínimas necessárias, o console não funcionará como pretendido para entidades (usuários ou perfis) com essa política.

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

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 saber mais, consulte Adicionar permissões a um usuário no Guia do usuário do IAM.

Permitindo que os usuários visualizem suas próprias permissões para o Amazon WorkSpaces Secure Browser

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

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam: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 perfis de trabalho, consulte Políticas gerenciadas pela AWS para perfis de trabalho no Guia do usuário do IAM.

Tópicos

- AWS política gerenciada: AmazonWorkSpacesWebServiceRolePolicy
- AWS política gerenciada: AmazonWorkSpacesSecureBrowserReadOnly
- AWS política gerenciada: AmazonWorkSpacesWebReadOnly
- WorkSpaces Atualizações do Secure Browser para políticas AWS gerenciadas

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 obter mais informações, consulte the section called “Uso de perfis vinculados ao serviço”.

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

Detalhes de permissões

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 os diretores 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 de VPC.
- `CloudWatch`: permite que as entidades principais coloquem dados de métricas.
- `Kinesis`: permite que as entidades principais descrevam um resumo dos fluxos de dados do Kinesis e coloquem registros nos fluxos de dados do Kinesis para registro em log de acesso do usuário. Para obter mais informações, consulte the section called “Configurando o registro de atividades 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` às 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 os diretores 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` às 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 política de `AmazonWorkSpacesSecureBrowserReadOnly`.

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 os diretores 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 acesso somente de leitura ao WorkSpaces Secure Browser e suas dependências por meio do AWS Management Console, SDK e CLI.	24 de junho de 2024
AmazonWorkSpacesWebServiceRolePolicy: política atualizada	WorkSpaces O Secure Browser atualizou a política CreateNetworkInterface para restringir a marcação com awsRequestTag/WorkSpacesWebManaged: true and act on subnet and security group resources, as well as restrict DeleteNetworkInterface to ENIs tagged with aws:ResourceTag/WorkSpacesWebManaged:: true.	15 de dezembro de 2022
AmazonWorkSpacesWebReadOnly: política atualizada	WorkSpaces O Secure Browser atualizou a política para incluir permissões de	2 de novembro de 2022

Alteração	Descrição	Data
	leitura para o registro de acesso do usuário e para listar streams de dados do Kinesis. Para obter mais informações, consulte the section called “Configurando o registro de atividades do usuário”.	
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 obter mais informações, consulte the section called “Configurando o registro de atividades 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 AWS/Usage namespace às permissões da PutMetricData API.	6 de abril de 2022

Alteração	Descrição	Data
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
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 o 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, suas políticas deverão ser atualizadas para permitir que você realize a ação.

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

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

Nesse caso, a política do usuário `mateojackson` deve ser atualizada para permitir o acesso ao 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 usuário do IAM chamado `marymajor` tenta usar o console para realizar uma ação no WorkSpaces Secure Browser. 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

É possível criar um perfil que os usuários de outras contas ou pessoas fora da organização podem usar para acessar seus recursos. É possível 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 o IAM.
- Para saber como fornecer acesso aos seus recursos em todos os Contas da AWS que você possui, consulte Como fornecer acesso a um usuário do IAM em outro Conta da AWS que você possui no Guia do usuário do IAM.
- Para saber como fornecer acesso aos seus recursos a terceiros Contas da AWS, consulte Como fornecer acesso Contas da AWS a terceiros no Guia do usuário do IAM.
- Para saber como conceder acesso por meio da federação de identidades, consulte Conceder acesso a usuários autenticados externamente (federação de identidades) no Guia do usuário do IAM.
- Para conhecer a diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

Usando funções vinculadas a serviços para o Amazon Secure WorkSpaces 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 perfis vinculados a serviços, consulte Serviços da AWS compatíveis com o IAM e procure os serviços que contenham Sim na coluna Service-Linked Role. Escolha um Sim com um link para visualizar a documentação do perfil vinculado para esse serviço.

Tópicos

- Permissões de função vinculadas ao serviço para WorkSpaces o Secure Browser
- Criação de uma função vinculada ao serviço para WorkSpaces o Secure Browser
- Editando uma função vinculada ao serviço para WorkSpaces o Secure Browser
- Excluindo uma função vinculada ao serviço para o Secure Browser WorkSpaces
- Regiões suportadas para funções vinculadas ao serviço WorkSpaces Secure Browser

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

O perfil vinculado ao serviço `AWSServiceRoleForAmazonWorkSpacesWeb` confia nos seguintes serviços para aceitar o perfil:

- `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 obter mais informações, consulte the section called “AmazonWorkSpacesWebServiceRolePolicy”.

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

Você deve configurar permissões para que uma entidade do IAM (por exemplo, um usuário, grupo ou função) crie, edite ou exclua um perfil vinculado a serviço. Para saber mais, consulte Permissões de Função Vinculadas 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 um perfil vinculado ao serviço. Quando você cria seu primeiro portal na Console de gerenciamento da AWS, 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 saber mais, 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 atributo ou serviço que requer uma função vinculada a serviço, é recomendável excluí-la. Dessa forma, você não tem uma entidade não utilizada que não seja monitorada ativamente ou mantida. No entanto, você deve limpar os recursos de seu perfil vinculado ao serviço antes de excluí-lo 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 AWSService RoleForAmazonWorkSpacesWeb

- 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 o perfil vinculado ao serviço usando o IAM

Use o console do IAM AWS CLI, o ou a AWS API para excluir a função AWSService RoleForAmazonWorkSpacesWeb vinculada ao serviço. Para saber mais, 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 obter 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. Para obter mais informações sobre sua responsabilidade de conformidade ao usar Serviços da AWS, consulte a documentação AWS de segurança.

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 altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de data center 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:

- Fazendo backup de conteúdo em AZs nossas regiões
- Backups criptografados
- Criptografando 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 chamadas de API AWS publicadas para acessar o Amazon WorkSpaces Secure Browser pela rede. Os clientes devem oferecer compatibilidade com:

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

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 VPC, sub-rede ou grupo de segurança. Atualmente, não há suporte para endpoints de multilocação e VPC (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.

Acesse APIs usando uma interface VPC endpoint ()AWS PrivateLink

Você pode ligar diretamente para o endpoint da API do Amazon WorkSpaces Secure Browser de dentro de uma nuvem privada (VPC), em vez de se conectar pela Internet. Você pode fazer isso sem o uso de um gateway de internet, dispositivo NAT, conexão VPN ou Direct Connect conexão.

Você estabelece essa conexão privada criando uma interface VPC endpoint que é alimentada por. AWS PrivateLink Para cada sub-rede que você especifica em sua VPC, criamos uma interface de rede de endpoint na sub-rede. Uma interface de rede de endpoint é uma interface de rede gerenciada pelo solicitante que serve como ponto de entrada para o tráfego da API do Amazon WorkSpaces Secure Browser.

Para obter mais informações, consulte Acessar AWS serviços por meio de AWS PrivateLink.

Tópicos

Considerações sobre o Amazon WorkSpaces Secure Browser

Antes de configurar uma interface VPC endpoint para o Amazon WorkSpaces Secure Browser APIs, certifique-se de revisar os “Pré-requisitos” nos serviços de acesso por meio de. AWSAWS PrivateLink O Amazon WorkSpaces Secure Browser oferece suporte para fazer chamadas para todas as suas ações de API por meio da interface VPC endpoint.

Por padrão, o acesso total ao Amazon WorkSpaces Secure Browser é permitido por meio do endpoint. Para mais informações, consulte Controlar o acesso a serviços com VPC endpoints no Guia do usuário da Amazon VPC.

Criação de uma interface VPC endpoint para o Amazon Secure Browser WorkSpaces

Você pode criar uma interface VPC endpoint para o serviço Amazon WorkSpaces Secure Browser usando o console Amazon VPC ou o (). AWS Command Line Interface AWS CLI Para obter mais informações, consulte Criar um endpoint de interface no Guia do usuário da Amazon VPC.

Crie uma interface VPC endpoint para o Amazon WorkSpaces Secure Browser usando o seguinte nome de serviço:

- com.amazonaws. *region*.espaços de trabalho na web

Para regiões compatíveis com FIPS, crie uma interface VPC endpoint para o WorkSpaces Amazon Secure Browser usando o seguinte nome de serviço:

- com.amazonaws. *region*. workspaces-web-fips

Criação de uma política de endpoint para sua interface VPC endpoint

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

Uma política de endpoint especifica as seguintes informações:

- As entidades principais que podem realizar ações (Contas da AWS, usuários do IAM e perfis do IAM).
- As ações que podem ser realizadas.
- Os recursos aos quais as ações podem ser aplicadas.

Para mais informações, consulte Controlar o acesso a serviços com VPC endpoints no Guia do usuário da Amazon VPC.

Exemplo: política de VPC endpoint para ações do Amazon WorkSpaces Secure Browser

Veja a seguir um exemplo de uma política de endpoint personalizado. Quando você anexa essa política à sua interface VPC endpoint, ela concede acesso às ações listadas do Amazon WorkSpaces Secure Browser para todos os diretores em todos os recursos.

```
{
     "Statement": [
         {
             "Action": "workspaces-web:*",
             "Effect": "Allow",
             "Resource": "*",
             "Principal": "*"
         }
     ]
}
```

Solução de problemas

Se suas chamadas para o Amazon WorkSpaces Secure Browser APIs estiverem suspensas, é provável que haja uma configuração incorreta no grupo de segurança do VPC Endpoint Service ou na configuração da função do IAM. Para resolver isso, tente o seguinte:

- Ao criar sua interface VPC endpoint, ela pode ter sido automaticamente anexada ao seu grupo Conta da AWS de segurança padrão. Tente usar um grupo de segurança diferente e certifique-se de que as permissões de entrada e saída permitam que você transfira seus dados adequadamente.
- Verifique se você está usando uma função do IAM que permite chamar o Amazon WorkSpaces Secure Browser APIs.

Para obter mais informações, consulte O que é AWS PrivateLink? no Guia do usuário da Amazon VPC.

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 práticas recomendadas a seguir são diretrizes gerais e não representam uma solução completa de segurança. Como essas

práticas recomendadas podem não ser adequadas ou suficientes 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 ter 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 ter 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 obter mais informações, consulte the section called “Configurando o registro de atividades 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 obter 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 EC2 instâncias da Amazon 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 de EC2 instâncias da Amazon 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 obter 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
`SessionIdleDisconnect`	O número de conexões que foram fechadas devido à inatividade do usuário.	`[PortalId]`	Média	Contagem
`ActiveSession`	O número de sessões ativas em um portal.	`[PortalId]`	Média	Contagem
`GlobalCpuPercent`	O uso da CPU da instância de sessão do Amazon WorkSpaces Secure Browser.	`[PortalId]` `[PortalId, UserName]`	Média, Soma, Máximo, Mínimo	Percentual
`GlobalMemoryPercent`	O uso da memória (RAM) da instância de sessão do Amazon WorkSpaces Secure Browser.	`[PortalId]` `[PortalId, UserName]`	Média, Soma, Máximo, Mínimo	Percentual
`DisplayLatency`	O tempo médio em milissegundos entre a captura do quadro e a apresentação.	`[PortalId]` `[PortalId, UserName]`	Média, Máxima, Mínima	Milissegundos

Métrica	Descrição	Dimensões	Statistics	Unidades
`InputLatency`	A latência de entrada entre cliente e servidor. Por exemplo, a latência entre o clique do mouse do cliente e o clique do mouse do servidor.	`[PortalId]` `[PortalId, UserName]`	Média, Máxima, Mínima	Milissegundos
`SessionLoggerEventDelivered`	O número de eventos que cada arquivo do Session Logger entregue tem.	`[PortalId]`	Média, Soma, Máximo, Mínimo	Contagem
`SessionLoggerTargetNotFoundError`	O número de entregas de arquivos de log que resultaram na não localização do bucket.	`[PortalId]`	Média, Soma, Máximo, Mínimo	Contagem
`SessionLoggerAccessDeniedError`	O número de entregas de arquivos de log que resultaram em permissões negadas.	`[PortalId]`	Média, Soma, Máximo, Mínimo	Contagem

> **Note**
>
> Os pontos de dados métricos são coletados por cada sessão uma vez por minuto e publicados CloudWatch uma vez a cada 5 minutos. As métricas do Session Logger são emitidas imediatamente, para cada entrega do arquivo de log.

Dimensões das métricas do Amazon WorkSpaces Secure Browser

Dimensão	Descrição
PortalId	Filtra os dados métricos do Amazon WorkSpaces Secure Browser para um portal específico.
UserName	Filtra os dados métricos do Amazon WorkSpaces Secure Browser para um portal e usuário específicos.

Você pode utilizar a SessionLoggerEventDeliveredmétrica para monitorar o número agregado de eventos do seu portal ou ver o número de arquivos de log que foram entregues contando o número de pontos de dados em vez de somar valores. Recomendamos configurar alarmes nas SessionLoggerAccessDeniedErrormétricas SessionLoggerTargetNotFoundErrore para detectar a exclusão acidental de recursos ou permissões.

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.

Tópicos

- WorkSpaces Informações do Navegador Seguro em CloudTrail
- Entendendo as entradas do arquivo de log do WorkSpaces Secure Bro

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 uma trilha é criada no console, a mesma é aplicada a todas as regiões da AWS. A trilha registra eventos de todas as regiões na AWS partição e entrega os arquivos de log ao bucket do Amazon S3 que você especificar. Além disso, você pode configurar outros AWS serviços para analisar e agir com base nos dados de eventos coletados nos CloudTrail registros. Para obter mais informações, consulte:

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

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

Para obter mais informações, consulte Elemento userIdentity do CloudTrail .

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 de atividades do usuário no Amazon WorkSpaces Secure Browser

O Amazon WorkSpaces Secure Browser permite que os clientes registrem eventos de sessão relacionados às atividades do usuário nas sessões do navegador seguro.

WorkSpaces O Secure Browser oferece duas opções para registrar a atividade do usuário e os eventos relacionados à segurança:

- O Session Logger captura uma ampla variedade de eventos de sessão. Esses registros são entregues em um bucket do Amazon S3 em sua conta, permitindo fácil integração com sua plataforma SIEM preferida.
- O registro de acesso do usuário captura os eventos mais críticos da sessão. Esses registros são transmitidos para um stream do Amazon Kinesis para processamento e análise em tempo real.

Para obter mais informações sobre como configurar essas opções, consulte the section called “Configurando o Registrador de Sessões” the section called “Configurando o registro de acesso do usuário” e.

Tópicos

- Eventos de sessão no Session Logger para Amazon WorkSpaces Secure Browser
- Eventos de sessão no registro de acesso do usuário para o Amazon WorkSpaces Secure Browser

Eventos de sessão no Session Logger para Amazon WorkSpaces Secure Browser

O Session Logger captura vários eventos relacionados à sessão para fins de monitoramento e auditoria.

Você pode configurar o Session Logger para coletar todos os eventos da sessão ou um subconjunto selecionado, dependendo das necessidades do portal do WorkSpaces Secure Browser. Para obter mais informações sobre configuração, consultethe section called “Configurando o Registrador de Sessões”.

Para manter a privacidade do usuário, o Session Logger não grava conteúdo confidencial, como dados da área de transferência ou o conteúdo de arquivos carregados ou baixados.

Os seguintes campos estão incluídos em todos os eventos:

- Tempo
- Nome de usuário
- ID do portal
- IP do portal
- IP do cliente
- ID da sessão

Nome	Descrição	Campos adicionais incluídos no evento
SessionStart	Uma sessão segura do navegador foi iniciada, mas o usuário ainda não se conectou.	
SessionConnect	O usuário está conectado à sessão segura do navegador.	
TabOpen	Na sessão segura do navegador, o usuário abriu uma nova guia ou abriu um link em uma nova guia.	Nome do host, caminho, URL (se o usuário abrir um link em uma nova guia), nenhum (se o usuário abrir uma nova guia)
UrlVisit	Na sessão do navegador, o usuário navegou até uma URL.	Nome do host, caminho, URL
WebsiteInteract	O usuário alterou um elemento HTML padrão em um site (por exemplo, clica em uma caixa de seleção, botão de rádio ou botão, ou	Nome do host, caminho, URL

Nome	Descrição	Campos adicionais incluídos no evento
	seleciona um item no menu suspenso).	
TabClose	Na sessão do navegador, o usuário fechou uma guia.	Nome do host, caminho, URL (se o usuário fechar uma guia para a qual navegou), nenhum (se o usuário fechar uma nova guia)
ContentTransferFromLocalToRemoteClipboard	O usuário atualizou a área de transferência dentro do navegador seguro usando o conteúdo do navegador local (fora do ambiente seguro). Essa atualização pode ocorrer copiando conteúdo por meio da barra de ferramentas da sessão ou transferindo dados por meio de atalhos de teclado (Ctrl+C/Ctrl+V).	
ContentCopyFromWebsite	O usuário atualizou a área de transferência dentro do navegador seguro usando o conteúdo do navegador seguro (dentro do ambiente seguro).	Nome do host, caminho, URL

Nome	Descrição	Campos adicionais incluídos no evento
ContentPasteToWebsite	O conteúdo da área de transferência foi colado em uma página da web dentro do navegador. (Esse evento não captura instâncias em que o conteúdo da área de transferência é colado na barra de URL do navegador.)	Nome do host, caminho, URL
PrintJobSubmit	O usuário enviou uma solicitação de trabalho para a impressora virtual do navegador (“Impressora DCV”). O conteúdo é salvo como PDF na máquina local do usuário.	Nome do arquivo, tamanho, extensão
FileDownloadFromSecureBrowserToRemoteDisk	Um arquivo foi salvo da sessão no disco local da instância remota.	Nome do host, caminho URLfilename, tamanho, extensão
FileTransferFromRemoteToLocalDisk	Um arquivo foi baixado do disco da instância remota para o dispositivo local do usuário.	Nome do arquivo, tamanho, extensão
FileUploadFromRemoteDiskToSecureBrowser	Um arquivo armazenado no disco local da instância remota foi enviado para uma plataforma SaaS de compartilhamento de arquivos (por exemplo, Google Drive, Box ou File.io) por meio da sessão do navegador.	

Nome	Descrição	Campos adicionais incluídos no evento
FileTransferFromLocalToRemoteDisk	Um arquivo foi carregado do dispositivo do usuário para a sessão segura do navegador.	Nome, tamanho e extensão do arquivo
SessionDisconnection	O usuário é desconectado da sessão segura do navegador.	
SessionEnd	A sessão do navegador seguro foi encerrada. O encerramento pode ocorrer de três maneiras: o administrador encerra a sessão por meio do Gerenciador de Sessões do Usuário no console, o usuário encerra manualmente a sessão usando Encerrar Sessão na barra de ferramentas ou a sessão expira após exceder a duração definida pelo administrador.	

Cada evento segue o padrão OCSF e inclui uma lista de atributos que são comuns a todos os eventos:

```
{
    activity_name : String | A human readable name of the event | eg. UrlLoad
    activity_id : Integer | OCSF standard value 99 for 'others'
    category_name : "WorkSpacesSecureBrowser" | The category name where the event
 belongs to.
    category_id : 2 | Numerical identifier for category,
    metadata : link | Required {
        product : link {
            vendor_name : "wsb",
            name : "WorkSpacesSecureBrowser"
```

```
        }
        version : String | Version of the schema | eg. 1.0.0
    },
    severity_id : 1 | The severity of the event. All events will have a severity of 1,
 meaning 'Informational',
    type_id : class_uid * 100 + activity_id
    time : The time the event happened (RFC3339 format),
    observables : link [
        {
            name : "session_detail.portal_id",
            type_id : 10 //Resource UID
            value : //Generated value
        },
        {
            name : "session_detail.session_id",
            type_id : 10 //Resource UID
            value : //Generated value
        },
        {
            name : "session_detail.client_ip",
            type_id : 2 //IP Address
            value : //Generated value
        },
        {
            name : "session_detail.portal_ip",
            type_id : 2 //IP Address
            value : //Generated value
        },
        {
            name : "session_detail.username",
            type_id : 10 //Resource UID
            value : //Generated value
        }
    ],

    // New Events
    session_detail : {
        portal_id : String | UUID of the Portal | eg.
 1ebe42de-86bb-4073-88a4-34284bc5bcbb,
        session_id : String | SessionId of the user session | eg. 17be80fa-7bc2-4675-
b17a-791243938cdf
        client_ip : String | IP Address from which user LoggedIn From | eg. 31.65.180.9
        portal_ip : String | IP Address of the AWS AppStream Instance that is running
 the Portal | eg.240.62.100.169
```

```
        username : String | The logged-in username | eg. bobross
    }
}
```

Abaixo está um exemplo do URLVisit evento:

```
{
    activity_id : 99,
    activity_name : "URLVisit",
    ...
    observables : [
        ...
        {
            name : "url",
            type_id : 23 //Unified Resource Locator
        }
    ]
    ...
    url : {
        url_string : String | Full URL path,
        hostname : String | The hostname in the URL
        path : String | Path in the domain
    }
}
```

Abaixo está um exemplo do PrintJobSubmit evento:

```
{
    activity_id : 99,
    activity_name : "PrintJobSubmitted",
    observable : [
        ...
        {
            name : "file.name",
            type_id : 24 // File
        }
    ]
    ...
    file : {
```

```
        name : String | The file name,
        type_id : 1 //Regular file
        size : Long | Size in bytes
        ext : String | File extension
    }
}
```

Métricas do Session Logger para o Amazon WorkSpaces Secure Browser

O Session Logger emite as seguintes Amazon CloudWatch métricas.

Você pode utilizar a SessionLoggerEventDeliveredmétrica para monitorar o número agregado de eventos do seu portal ou ver o número de arquivos de log que foram entregues contando o número de pontos de dados em vez de somar valores. Recomendamos configurar alarmes nas SessionLoggerAccessDeniedErrormétricas SessionLoggerTargetNotFoundErrore para detectar a exclusão acidental de recursos ou permissões.

> **Note**
>
> Os pontos de dados métricos são coletados por cada sessão uma vez por minuto e publicados Amazon CloudWatch uma vez a cada 5 minutos. As métricas do Session Logger são emitidas imediatamente, para cada entrega do arquivo de log.

Métricas do Session Logger

Métrica	Descrição	Dimensão	Statistics	Unidade
SessionLoggerEventDelivered	O número de eventos que cada arquivo do Session Logger entregue tem.	[PortalId]	Média, Soma, Máximo, Mínimo	Contagem
SessionLoggerTargetNotFoundError	O número de entregas de arquivos de log que resultaram	[PortalId]	Média, Soma, Máximo, Mínimo	Contagem

Métrica	Descrição	Dimensão	Statistics	Unidade
	na não localizaç ão do bucket.			
SessionLo ggerAcces sDeniedError	O número de entregas de arquivos de log que resultaram em permissões negadas.	[PortalId]	Média, Soma, Máximo, Mínimo	Contagem

Eventos de sessão no registro de acesso do usuário para o Amazon WorkSpaces Secure Browser

Os seguintes eventos de sessão estão disponíveis para registro de acesso do usuário:

- Validação: o evento é colocado com sucesso no stream de dados do Kinesis.
- StartSession: o usuário iniciou uma sessão e está conectado à sessão segura do navegador.
- VisitPage: O usuário está visitando uma página na sessão.
- EndSession: O usuário encerrou a sessão.

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

Abaixo está um exemplo de cada evento disponível. 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"
}
```

Orientação para usuários do Amazon 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 com o Amazon WorkSpaces Secure Browser

O Amazon WorkSpaces Secure Browser é desenvolvido pelo cliente de navegador Amazon 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 web para o Amazon WorkSpaces Secure Browser

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 de sessão para o Amazon WorkSpaces Secure Browser

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

Tópicos

Iniciando uma sessão no Amazon WorkSpaces Secure Browser

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.

Usando a barra de ferramentas no Amazon WorkSpaces Secure Browser

Para aprender a usar a barra de ferramentas, siga estas etapas:

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 ampliar ou reduzir 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 ampliar ou reduzir 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. Use the down arrow to select from a list of available microphones.
	**Webcam**	Activate webcam for the session. Use the down arrow to select from a list of available webcams.
	**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. **Performance metrics** displays the frame rate, network latency, and bandwidth usage graph. This information is useful for administrators when investigating issues with the service. **Feedback** provides you with an email address to share feedback to the Amazon WorkSpaces Web team. **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. **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.

Usando o navegador no Amazon WorkSpaces Secure Browser

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.

Encerramento de uma sessão no Amazon WorkSpaces Secure Browser

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 de usuários no Amazon WorkSpaces Secure Browser

Se você encontrar algum dos problemas a seguir ao usar o WorkSpaces Secure Browser, tente as seguintes resoluções.

Meu portal 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.

Como posso saber qual and/or webcam de microfone está sendo usada e como posso alterá-la?

Clique no ícone de seta para baixo ao lado do microfone ou da câmera. O menu exibe os dispositivos disponíveis, com uma marca de seleção indicando seu dispositivo atual. Selecione um dispositivo diferente para alterar o dispositivo que você deseja usar na sua sessão.

Meu portal da web não será iniciado quando acessado diretamente do domínio personalizado da empresa

Se você estiver tentando iniciar uma sessão usando um nome de domínio que não seja workspaces-web.comacme`.secureportal.mycompany.com`, certifique-se de que seu navegador tenha cookies de terceiros habilitados para o domínio da empresa que você está acessando.

Extensão de login único para o Amazon WorkSpaces Secure Browser

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.

Tópicos

Compatibilidade da extensão de login único para o Amazon WorkSpaces Secure Browser

A extensão de login único funciona com os seguintes dispositivos e navegadores:

- Dispositivos
  - Notebooks
  - Computadores desktop
- Navegadores
  - Google Chrome
  - Mozilla Firefox

Instalação da extensão de login único para o Amazon WorkSpaces Secure Browser

Para instalar a extensão de login único, siga estas etapas.

Ao fazer login no portal, siga as instruções para instalar a extensão para 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 uma de navegação anônima (Chrome) ou navegação privada (Firefox).

Solução de problemas da extensão de login único para o Amazon WorkSpaces Secure Browser

Ao usar a extensão de login único, você pode encontrar o problema a seguir.

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. Verifique se você não está navegando de forma anônima (Chrome) ou privada (Firefox). Esses modos podem causar problemas com extensões.
3. Se o problema persistir, entre em contato com o administrador do portal para obter ajuda adicional.

Histórico de documentos do 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
Registrador de sessão	Configure o Session Logger para capturar uma ampla variedade de eventos de sessão.	1.º de agosto de 2025
CloudWatch métricas	CloudWatch Métricas atualizadas.	21 de julho de 2025
Controles da barra de ferramentas	Com os controles da barra de ferramentas, você pode configurar a apresentação da barra de ferramentas para as sessões do usuário final.	21 de fevereiro de 2025
Acesse APIs usando uma interface VPC endpoint ()AWS PrivateLink	Ligue diretamente para o endpoint da API do Amazon WorkSpaces Secure Browser de dentro de uma nuvem privada (VPC), em vez de se conectar pela Internet.	10 de janeiro de 2025
Configurações de proteção de dados	Adicione configurações de proteção de dados para ajudar a impedir que os dados sejam compartilhados durante uma sessão.	20 de novembro de 2024
Endpoints do FIPS	Proteger dados em trânsito com endpoints do FIPS.	7 de outubro de 2024

Painel de gerenciamento de sessões	Use o painel de gerenciamento de sessões para monitorar e gerenciar sessões ativas e completas.	19 de setembro de 2024
Permitir deep links	Permita que os portais recebam deep links 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 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 filtragem de URL	Você pode usar a Política do Chrome para filtrar quais URLs usuários podem acessar a partir do navegador remoto.	21 de fevereiro de 2024
Tipos de autenticação IdP	Você pode escolher o tipo de autenticação padrão ou a 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 Centro de Identidade do AWS IAM	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 AWS/Usage namespace 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.