aws

Guía de administración

Navegador Amazon WorkSpaces Secure

Navegador Amazon WorkSpaces Secure: Guía de administración

Table of Contents

¿Qué es Amazon WorkSpaces Secure Browser?

> **Note**
>
> Amazon WorkSpaces Secure Browser se conocía anteriormente como Amazon WorkSpaces Web.

Amazon WorkSpaces Secure Browser es un servicio de navegador hospedado, nativo de la nube y totalmente gestionado que se utiliza para acceder de forma segura a sitios web privados y aplicaciones web software-as-a-service (SaaS), interactuar con recursos en línea y navegar por Internet desde un contenedor desechable. WorkSpaces Secure Browser funciona con los navegadores web existentes del usuario, sin sobrecargar el departamento de TI con la administración de los dispositivos, la infraestructura, el software de cliente especializado o las conexiones de redes privadas virtuales (VPN). El contenido web se transmite al navegador web del usuario, mientras que el navegador y el contenido web reales están aislados. AWS Al utilizar las mismas tecnologías subyacentes que impulsan los servicios de informática para el usuario AWS final, como Amazon WorkSpaces y Amazon AppStream 2.0, WorkSpaces Secure Browser puede ser más rentable que los escritorios virtuales tradicionales y reducir la complejidad en comparación con el suministro de software de administración a los dispositivos propiedad de la empresa. WorkSpaces Secure Browser reduce el riesgo de exfiltración de datos mediante la transmisión de contenido web. No se transmite HTML, modelo de objetos de documento (DOM) ni datos confidenciales de la empresa a la máquina local. Al aislar el dispositivo, la red corporativa e Internet entre sí, prácticamente se elimina la superficie de ataque del navegador.

Puede aplicar la política de navegación empresarial (incluida la posibilidad o el bloqueo de URL) en todas las sesiones e incluye controles a nivel de sesión para el portapapeles, la transferencia de archivos y la impresora. También puede restringir el acceso a redes o dispositivos de confianza mediante los controles de acceso IP. WorkSpaces Secure Browser es fácil de configurar y operar. Cada sesión se inicia con una versión nueva y completamente parcheada del navegador Chrome, en la que se aplican las políticas y los ajustes de la empresa.

Historial de versiones

El 20 de mayo de 2024, Amazon WorkSpaces Web pasó a llamarse Amazon WorkSpaces Secure Browser. Para los clientes actuales, no hubo cambios en la forma en que administran los usuarios

o los recursos con el servicio. En la siguiente lista se describen las actualizaciones aplicables que también se produjeron como resultado de este cambio de nombre.

El espacio de nombres de la API workspaces-web permanece inalterado por motivos de compatibilidad con versiones anteriores. Como resultado, los siguientes recursos siguen siendo los mismos:

- Comandos CLI.
- CloudWatch Métricas de Amazon. Para obtener más información, consulte the section called "Monitorización con CloudWatch".
- Puntos finales de servicio. Para obtener más información, consulte los puntos de conexión y las cuotas de Amazon WorkSpaces Secure Browser.
- AWS CloudFormation recursos. Para obtener más información, consulte la referencia de tipos de recursos de Amazon WorkSpaces Secure Browser.
- Función vinculada a un servicio que contiene workspaces-web. Para obtener más información, consulte the section called "Usar roles vinculados a servicios".
- URL de consola que contienen workspaces-web.
- URL de documentación que contienen workspaces-web. Para obtener más información, consulte la documentación de Amazon WorkSpaces Secure Browser.
- Función ReadOnly gestionada existente. Para obtener más información, consulte the section called "AWS políticas gestionadas".
- Nombre de la concesión de KMS.
- Prefijo de transmisión de Kinesis UAL (registro de actividad del usuario).

Además, las URL de los portales existentes siguen siendo las mismas. <UUID>Las direcciones URL de los portales creados antes del 20 de mayo de 2024 utilizaban el formato .workspaces-web.com. WorkSpaces Los portales de Secure Browser siguen utilizando este formato y el dominio workspaces-web.com.

Términos que debe conocer al usar Secure Browser WorkSpaces

Para ayudarle a empezar a utilizar WorkSpaces Secure Browser, debe familiarizarse con los siguientes conceptos.

Identity provider (IdP) (Proveedor de identidad (IdP))

Un proveedor de identidad verifica las credenciales de los usuarios. A continuación, emite aserciones de autenticación para proporcionar acceso a un proveedor de servicios. Puede configurar su IdP actual para que funcione con WorkSpaces Secure Browser.

El proceso para configurar el proveedor de identidades (IdP) varía según el IdP.

Debe cargar el archivo de metadatos del proveedor de servicios en su IdP. De lo contrario, los usuarios no podrán iniciar sesión. También debe conceder acceso a sus usuarios para que utilicen WorkSpaces Secure Browser en su IdP.

Documento de metadatos del proveedor de identidades (IdP)

WorkSpaces Secure Browser requiere metadatos específicos de su proveedor de identidad (IdP) para establecer la confianza. Puede añadir estos metadatos a WorkSpaces Secure Browser cargando un archivo de intercambio de metadatos descargado de su IdP.

Proveedor de servicios (SP)

Un proveedor de servicios acepta las aserciones de autenticación y proporciona un servicio al usuario. WorkSpaces Secure Browser actúa como proveedor de servicios para los usuarios que han sido autenticados por su IdP.

Documento de metadatos del proveedor de servicios (SP)

Deberá añadir los detalles de los metadatos del proveedor de servicios a la interfaz de configuración de su proveedor de identidades (IdP). Los detalles de este proceso de configuración varían de un proveedor a otro.

SAML 2.0

Un estándar para intercambiar datos de autenticación y autorización de entre un proveedor de identidad y un proveedor de servicios.

Virtual Private Cloud (VPC) (Nube virtual privada)

Puede usar una VPC nueva o existente, las subredes correspondientes y los grupos de seguridad para vincular su contenido con WorkSpaces Secure Browser.

Las subredes deben tener una conexión estable a Internet, y la VPC y las subredes también deben tener una conexión estable a cualquier sitio web interno y de software como servicio (SaaS) para que los usuarios puedan acceder a estos recursos.

Las VPC, las subredes y los grupos de seguridad de la lista provienen de la misma región que la consola de Secure Browser. WorkSpaces

Almacén de confianza

Si un usuario que accede a un sitio web a través de WorkSpaces Secure Browser recibe un error de privacidad, como NET: :ERR_CERT_INVALID, es posible que ese sitio utilice un certificado firmado por una autoridad de certificación (PCA) privada. Es posible que tenga que añadir o cambiar los PCA de su almacén de confianza. Además, si el dispositivo de un usuario requiere que instales un certificado específico para cargar un sitio web, tendrás que añadir ese certificado a tu almacén de confianza para que el usuario pueda acceder a ese sitio en Secure Browser. WorkSpaces

Los sitios web de acceso público no suelen requerir ningún cambio en un almacén de confianza.

Portal web

Un portal web proporciona a sus usuarios acceso a sitios web internos y de SaaS desde sus navegadores. Puede crear un portal web en cualquier región admitida por cuenta. Para solicitar el aumento del límite para más de un portal, póngase en contacto con el servicio de soporte.

Punto de conexión del portal web

El punto de conexión del portal web es el punto de acceso desde el que los usuarios abrirán el portal web tras iniciar sesión con el proveedor de identidades configurado para el portal.

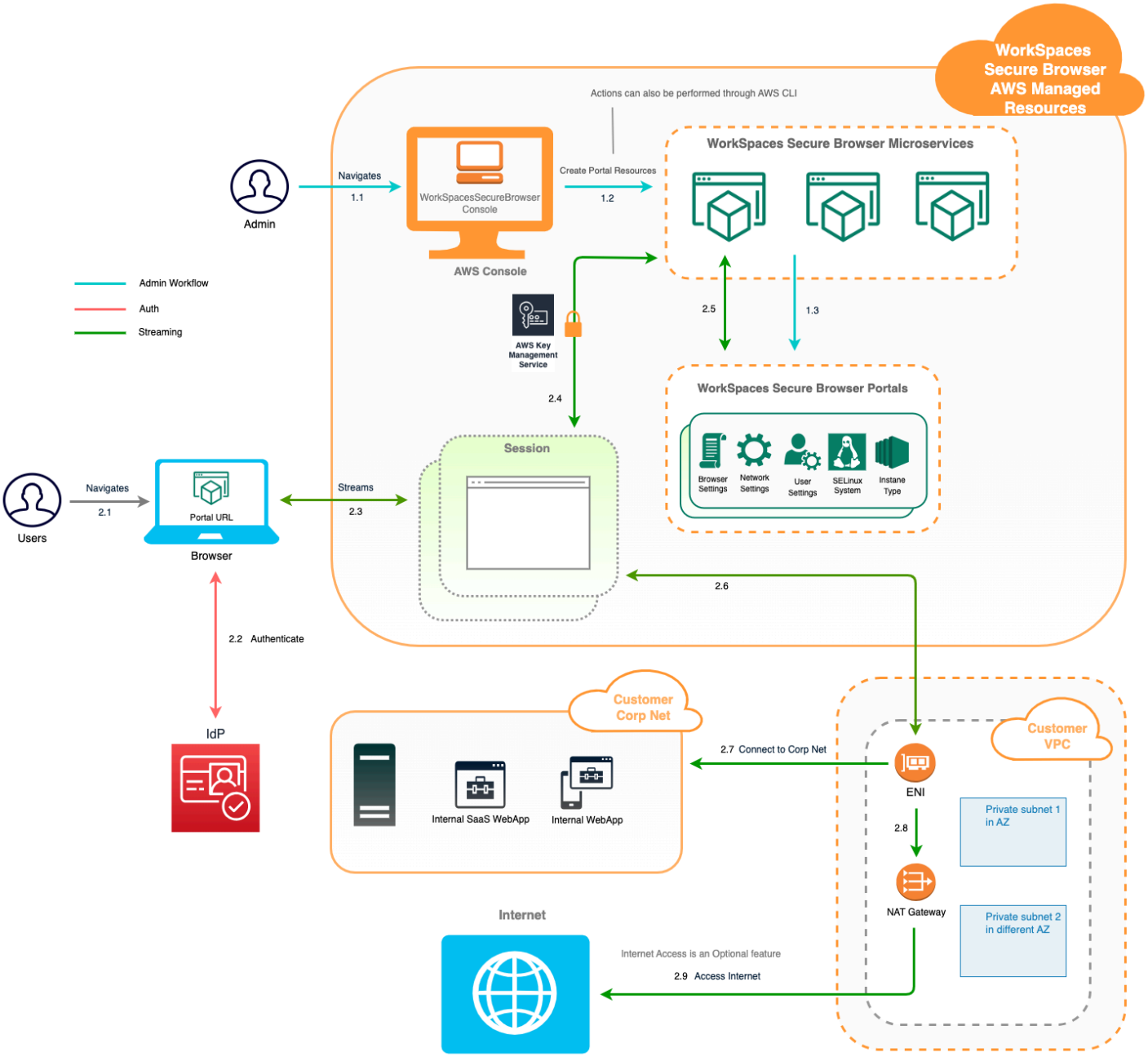
El punto de conexión está disponible públicamente en Internet y se puede integrar en la red.

Servicios relacionados

WorkSpaces Secure Browser es una capacidad de Amazon incluida WorkSpaces en la cartera de informática para usuarios finales de AWS. En comparación con WorkSpaces la AppStream versión 2.0, WorkSpaces Secure Browser está diseñada específicamente para facilitar cargas de trabajo seguras y basadas en la web. WorkSpaces Secure Browser se administra automáticamente y AWS aprovisiona y actualiza la capacidad, el escalado y las imágenes a pedido. Por ejemplo, puede optar por ofrecer un Workspace Desktop persistente a los desarrolladores de software que necesiten acceso a los recursos del escritorio, y WorkSpaces Secure Browser a los usuarios del centro de contacto que solo necesiten acceder a un puñado de sitios web internos y de SaaS (incluidos los alojados fuera de su red) en ordenadores de escritorio.

Arquitectura

El siguiente diagrama muestra la arquitectura de WorkSpaces Secure Browser.



Acceso a WorkSpaces Secure Browser

Los administradores acceden a WorkSpaces Secure Browser a través de la consola, el SDK, la CLI o la API de WorkSpaces Secure Browser. Sus usuarios acceden a él a través del punto final de WorkSpaces Secure Browser.

Configuración de WorkSpaces Secure Browser

Antes de poder configurar WorkSpaces Secure Browser para acceder a sus sitios web internos y aplicaciones SaaS, debe cumplir los siguientes requisitos previos.

Temas

Inicio de sesión y creación de un usuario

Inscríbase en una Cuenta de AWS

Si no tiene uno Cuenta de AWS, complete los siguientes pasos para crearlo.

Para suscribirte a una Cuenta de AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga las instrucciones que se le indiquen.

   Parte del procedimiento de registro consiste en recibir una llamada telefónica e indicar un código de verificación en el teclado del teléfono.

   Cuando te registras en un Cuenta de AWS, Usuario raíz de la cuenta de AWSse crea un. El usuario raíz tendrá acceso a todos los Servicios de AWS y recursos de esa cuenta. Como práctica recomendada de seguridad, asigne acceso administrativo a un usuario y utilice únicamente el usuario raíz para realizar tareas que requieren acceso de usuario raíz.

AWS te envía un correo electrónico de confirmación una vez finalizado el proceso de registro. Puede ver la actividad de la cuenta y administrar la cuenta en cualquier momento entrando en https://aws.amazon.com/ y seleccionando Mi cuenta.

Creación de un usuario con acceso administrativo

Después de registrarte en un usuario Cuenta de AWS, protege Usuario raíz de la cuenta de AWS AWS IAM Identity Center, habilita y crea un usuario administrativo para que no utilices el usuario root en las tareas diarias.

Proteja su Usuario raíz de la cuenta de AWS

1. Inicie sesión AWS Management Consolecomo propietario de la cuenta seleccionando el usuario root e introduciendo su dirección de Cuenta de AWS correo electrónico. En la siguiente página, escriba su contraseña.

   Para obtener ayuda para iniciar sesión con el usuario raíz, consulte Iniciar sesión como usuario raíz en la Guía del usuario de AWS Sign-In .
2. Active la autenticación multifactor (MFA) para el usuario raíz.

   Para obtener instrucciones, consulte Habilitar un dispositivo MFA virtual para el usuario Cuenta de AWS raíz (consola) en la Guía del usuario de IAM.

Creación de un usuario con acceso administrativo

1. Activar IAM Identity Center.

   Consulte las instrucciones en Activar AWS IAM Identity Center en la Guía del usuario de AWS IAM Identity Center .
2. En IAM Identity Center, conceda acceso administrativo a un usuario.

   Para ver un tutorial sobre su uso Directorio de IAM Identity Center como fuente de identidad, consulte Configurar el acceso de los usuarios con la configuración predeterminada Directorio de IAM Identity Center en la Guía del AWS IAM Identity Center usuario.

Iniciar sesión como usuario con acceso de administrador

- Para iniciar sesión con el usuario de IAM Identity Center, utilice la URL de inicio de sesión que se envió a la dirección de correo electrónico cuando creó el usuario de IAM Identity Center.

  Para obtener ayuda para iniciar sesión con un usuario del Centro de identidades de IAM, consulte Iniciar sesión en el portal de AWS acceso en la Guía del AWS Sign-In usuario.

Concesión de acceso a usuarios adicionales

1. En IAM Identity Center, cree un conjunto de permisos que siga la práctica recomendada de aplicar permisos de privilegios mínimos.

   Para conocer las instrucciones, consulte Create a permission set en la Guía del usuario de AWS IAM Identity Center .
2. Asigne usuarios a un grupo y, a continuación, asigne el acceso de inicio de sesión único al grupo.

   Para conocer las instrucciones, consulte Add groups en la Guía del usuario de AWS IAM Identity Center .

Concesión de acceso mediante programación

Los usuarios necesitan acceso programático si quieren interactuar con personas AWS ajenas a. AWS Management Console La forma de conceder el acceso programático depende del tipo de usuario que acceda. AWS

Para conceder acceso programático a los usuarios, elija una de las siguientes opciones.

¿Qué usuario necesita acceso programático?	Para	Mediante
Identidad del personal (Usuarios administrados en el IAM Identity Center)	Usa credenciales temporales para firmar las solicitudes programáticas a los AWS CLI AWS SDK o las API. AWS	Siga las instrucciones de la interfaz que desea utilizar: • Para ello AWS CLI, consulte Configuración del uso AWS IAM Identity Center en AWS CLI la Guía del AWS Command Line Interface usuario. • Para obtener AWS información sobre los SDK, las herramientas y AWS las API, consulte la autenticación del IAM Identity Center

¿Qué usuario necesita acceso programático?	Para	Mediante
		en la Guía de referenci a de AWS los SDK y las herramientas.
IAM	Utilice credenciales temporale s para firmar las solicitudes programáticas a los AWS SDK o las AWS CLI API. AWS	Siga las instrucciones de Uso de credenciales temporales con AWS recursos de la Guía del usuario de IAM.
IAM	(No recomendado) Utilice credenciales de larga duración para firmar las solicitudes programáticas a los AWS CLI AWS SDK o las API. AWS	Siga las instrucciones de la interfaz que desea utilizar: • Para ello AWS CLI, consulte Autenticación con credencia les de usuario de IAM en la Guía del usuario.AWS Command Line Interface • Para obtener informaci ón AWS sobre los SDK y las herramientas, consulte Autenticarse con credencia les de larga duración en la Guía de referencia de los AWS SDK y las herramien tas. • Para obtener informaci ón AWS sobre las API, consulte Administrar las claves de acceso para los usuarios de IAM en la Guía del usuario de IAM.

Redes y acceso

En los siguientes temas se explica cómo configurar las instancias de streaming de WorkSpaces Secure Browser para que los usuarios puedan conectarse a ellas. También explica cómo permitir que las instancias de streaming de WorkSpaces Secure Browser accedan a los recursos de la VPC, así como a Internet.

Temas

Requisitos de la VPC

Durante la creación del portal WorkSpaces Secure Browser, seleccionará una VPC en su cuenta. También debe elegir al menos dos subredes en dos zonas de disponibilidad diferentes. Estas VPC y subredes deben cumplir los siguientes requisitos:

- La VPC debe disponer de una tenencia predeterminada. No se admiten las VPC con una tenencia dedicada.
- Por motivos de disponibilidad, se requieren al menos dos subredes creadas en dos zonas de disponibilidad diferentes. Sus subredes deben tener direcciones IP suficientes para soportar el tráfico esperado de WorkSpaces Secure Browser. Configure cada una de las subredes con una máscara de subred que permita suficientes direcciones IP de cliente para tener capacidad para el número máximo de sesiones simultáneas. Para obtener más información, consulte Cree y configure una VPC nueva.
- Todas las subredes deben tener una conexión estable a cualquier contenido interno, ya sea local Nube de AWS o local, al que los usuarios puedan acceder con WorkSpaces Secure Browser.

Le recomendamos que elija tres subredes en distintas zonas de disponibilidad por motivos de disponibilidad y escalabilidad. Para obtener más información, consulte Cree y configure una VPC nueva.

WorkSpaces Secure Browser no asigna ninguna dirección IP pública a las instancias de streaming para permitir el acceso a Internet. Esto haría que sus instancias de streaming fueran accesibles desde Internet. Por lo tanto, ninguna instancia de streaming conectada a su subred pública tendrá acceso a Internet. Si desea que su portal WorkSpaces Secure Browser tenga acceso tanto al contenido público de Internet como al contenido privado de VPC, complete los pasos que se indican a continuación. Habilitación de la navegación por Internet sin restricciones (recomendado)

Cree y configure una VPC nueva

En esta sección, se describe cómo utilizar el asistente de VPC para crear una VPC con una subred pública y una subred privada. Como parte de este proceso, el asistente crea una puerta de enlace de Internet y una puerta de enlace NAT. También se crea una tabla de enrutamiento personalizada asociada a la subred pública. Luego, se actualiza la tabla de enrutamiento principal asociada a la subred privada. La puerta de enlace NAT se crea automáticamente en la subred pública de su VPC.

Después de utilizar el asistente para crear la configuración de la VPC, debe añadir una segunda subred privada. Para obtener más información acerca de esta configuración, consulte VPC con subredes privadas y públicas (NAT).

Paso 1: asigne una dirección IP elástica

Antes de crear su VPC, debe asignar una dirección IP elástica en su región de navegador WorkSpaces seguro. Una vez asignada, la dirección IP elástica se puede asociar a su puerta de enlace NAT. Con una dirección IP elástica, puede enmascarar un error de las instancias de streaming reasignando rápidamente la dirección a otra instancia de streaming de su VPC. Para obtener más información, consulte Direcciones IP elásticas.

> **Note**
>
> Es posible que se apliquen cargos a las direcciones IP elásticas que utilice. Para obtener más información, consulte la página de precios de direcciones IP elásticas.

Si aún no dispone de una dirección IP elástica, complete los siguientes pasos. Si desea utilizar una dirección IP elástica existente, primero debe verificar que no esté asociada ya a otra instancia o interfaz de red.

Para asignar una dirección IP elástica

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.

2. En el panel de navegación, en Red y seguridad, seleccione IP elásticas.
3. Elija Asignar nueva dirección y, a continuación, elija Asignar.
4. Anote la dirección IP elástica que se muestra en la consola.
5. En la esquina superior derecha del panel IP elásticas, haga clic en el icono × para cerrar el panel.

Paso 2: cree una VPC nueva

Realice los siguientes pasos para crear una VPC nueva con una subred pública y una subred privada.

Para crear una VPC nueva

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Panel de VPC.
3. Elija Lanzar el asistente de VPC.
4. En Paso 1: Seleccionar una configuración de VPC, elija VPC con subredes pública y privada y, a continuación, elija Seleccionar.
5. En Paso 2: VPC con subredes pública y privada, configure la VPC como sigue:
   - En Bloque de CIDR IPv4, especifique un bloque de CIDR IPv4 para la VPC.
   - En Bloque de CIDR IPv6, deje el valor predeterminado, Sin bloque de CIDR IPv6.
   - En Nombre de VPC, introduzca un nombre para la VPC.
   - Configure la subred pública de la siguiente manera:
     - En CIDR IPv4 de la subred pública, especifique el bloque de CIDR para la subred.
     - En Zona de disponibilidad, deje el valor predeterminado Sin preferencia.
     - En Nombre de la subred pública, escriba un nombre para la subred. Por ejemplo, **`WorkSpaces Secure Browser Public Subnet`**.
   - Configure la primera subred privada de la siguiente manera:
     - En CIDR IPv4 de la subred privada, especifique el bloque de CIDR para la subred. Tome nota del valor que especifique.
     - En Zona de disponibilidad, seleccione una zona específica y tome nota de la zona seleccionada.

  - En Nombre de la subred privada, escriba un nombre para la subred. Por ejemplo, **`WorkSpaces Secure Browser Private Subnet1`**.
- En los campos restantes, cuando corresponda, deje los valores predeterminados.
- En ID de asignación de IP elástica, introduzca el valor que corresponda a la dirección IP elástica creada. Esta dirección se asigna a la puerta de enlace NAT. Si no tiene una dirección IP elástica, cree una mediante la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
- En Puntos de enlace de servicio, si se requiere un punto de conexión de Amazon S3 para el entorno, especifique uno.

  Para especificar un punto de conexión de Amazon S3, haga lo siguiente:

  1. Elija Agregar punto de conexión.
  2. Para el servicio, seleccione com.amazonaws. Entrada ***`Región.s3`***, donde *`Región`* es la región en la Región de AWS que está creando su VPC.
  3. En Subred, elija subnet-2.
  4. En Política, deje el valor predeterminado, Acceso completo.
- En Habilitar nombres de host de DNS, deje el valor predeterminado, Sí.
- En Tenencia de hardware, deje el valor Predeterminado.
- Seleccione Crear VPC.
- Se necesitan varios minutos para configurar la VPC. Una vez creada la VPC, elija Aceptar.

Paso 3: añada una segunda subred privada

En el paso anterior, ha creado una VPC con una subred pública y una subred privada. Realice los siguientes pasos para añadir una segunda subred privada a su VPC. Se recomienda agregar una segunda subred privada en una zona de disponibilidad diferente a la primera subred privada.

Para añadir una segunda subred privada

1. En el panel de navegación, elija Subredes.
2. Seleccione la primera subred privada que creó en el paso anterior. En la pestaña Descripción debajo de la lista de subredes, tome nota de la zona de disponibilidad de esta subred.
3. En la parte superior izquierda del panel de subredes, elija Crear subred.
4. En Etiqueta de nombre, introduzca un nombre para la subred privada. Por ejemplo, **`WorkSpaces Secure Browser Private Subnet2`**.

5. En VPC, seleccione la VPC que creó en el paso anterior.
6. En Zona de disponibilidad, seleccione una zona de disponibilidad distinta de la que está utilizando para la primera subred privada. La selección de una zona de disponibilidad diferente aumenta la tolerancia a errores y ayuda a evitar problemas de falta de capacidad.
7. En Bloque de CIDR IPv4, especifique un rango de bloques de CIDR único para la nueva subred. Por ejemplo, si la primera subred privada tiene un rango de bloques de CIDR IPv4 de **`10.0.1.0/24`**, puede especificar un rango de bloques de CIDR de **`10.0.2.0/24`** para la segunda subred privada.
8. Seleccione Crear.
9. Una vez creada la subred, elija Cerrar.

Paso 4: verifique y asigne un nombre a las tablas de enrutamiento de la subred

Después de crear y configurar la VPC, siga los pasos siguientes para especificar un nombre para las tablas de enrutamiento. Deberá comprobar que los siguientes detalles son correctos para su tabla de enrutamiento:

- La tabla de enrutamiento asociada a la subred en la que reside su puerta de enlace NAT debe incluir una ruta que apunte el tráfico de Internet a una puerta de enlace de Internet. Esto garantiza que la puerta de enlace NAT pueda acceder a Internet.
- Las tablas de enrutamiento asociadas a las subredes privadas se deben configurar para dirigir el tráfico de Internet a la puerta de enlace NAT. Esto permite a las instancias streaming de sus subredes privadas comunicarse con Internet.

Para verificar y asignar un nombre a las tablas de enrutamiento de la subred

1. En el panel de navegación, elija Subredes y seleccione la subred pública que ha creado. Por ejemplo, WorkSpaces Secure Browser 2.0 Public Subnet.
2. En la pestaña Tabla de enrutamiento, elija el ID de la tabla de enrutamiento. Por ejemplo, rtb-12345678.
3. Seleccione la tabla de enrutamiento. En Nombre, elija el icono de edición (lápiz) e introduzca un nombre para la tabla. Por ejemplo, introduzca el nombre **`workspacesweb-public-routetable`**. Luego, seleccione la marca de verificación para guardar el nombre.

4. Con la tabla de enrutamiento pública aún seleccionada, en la pestaña Rutas, compruebe que haya dos rutas: una para el tráfico local y otra que envía el resto del tráfico hacia la puerta de enlace de Internet de la VPC. En la tabla siguiente se describen estas dos rutas:

Destino	Objetivo	Descripción
Bloque de CIDR IPv4 de subred pública (por ejemplo, 10.0.0/20)	Local	Todo el tráfico procedente de los recursos destinados a las direcciones IPv4 dentro del bloque de CIDR IPv4 de subred pública. Este tráfico se enruta localmente dentro de la VPC.
Tráfico destinado a todas las demás direcciones IPv4 (por ejemplo, 0.0.0.0/0)	Saliente (igw-ID)	El tráfico destinado a todas las demás direcciones IPv4 se dirige a la puerta de enlace de Internet (identifi cada por igw-ID) que ha creado el asistente de la VPC.

5. En el panel de navegación, elija Subnets (Subredes). A continuación, seleccione la primera subred privada que creó (por ejemplo, **`WorkSpaces Secure Browser Private Subnet1`**).
6. En la pestaña Tabla de enrutamiento, elija el ID de la tabla de enrutamiento.
7. Seleccione la tabla de enrutamiento. En Nombre, elija el icono de edición (lápiz) e introduzca un nombre para la tabla. Por ejemplo, introduzca el nombre **`workspacesweb-private-routetable`**. A continuación, seleccione la marca de verificación para guardar el nombre.
8. En la pestaña Rutas, compruebe que la tabla de enrutamiento incluye las siguientes rutas:

Destino	Objetivo	Descripción
Bloque de CIDR IPv4 de subred pública (por ejemplo, 10.0.0/20)	Local	Todo el tráfico procedente de los recursos destinados a las direcciones IPv4 dentro del bloque de CIDR IPv4

Destino	Objetivo	Descripción
		de subred pública se dirige localmente dentro de la VPC.
Tráfico destinado a todas las demás direcciones IPv4 (por ejemplo, 0.0.0.0/0)	Saliente (nat-ID)	El tráfico destinado a todas las demás direcciones IPv4 se dirige a la puerta de enlace NAT (identificada por nat-ID).
Tráfico destinado a buckets de S3 (aplicable si especificó un punto de conexión de S3) [pl-ID (com.amazonaws.region.s3)]	Almacenamiento (vpce-ID)	El tráfico destinado a los buckets de S3 se dirige al punto de conexión de S3 (identificado por vpce-ID).

9. En el panel de navegación, elija Subnets (Subredes). A continuación, seleccione la segunda subred privada que creó (por ejemplo, **`WorkSpaces Secure Browser Private Subnet2`**).
10. En la pestaña Tabla de enrutamiento, compruebe que la tabla de enrutamiento es la tabla de enrutamiento privada (por ejemplo, **`workspacesweb-private-routetable`**). Si la tabla de enrutamiento es diferente, elija Editar y seleccione su tabla de enrutamiento privada.

Habilitación de la navegación por Internet sin restricciones (recomendado)

Siga estos pasos para configurar una VPC con una puerta de enlace NAT para poder navegar por Internet sin restricciones. Esto otorga a WorkSpaces Secure Browser acceso a sitios de la Internet pública y a sitios privados alojados en su VPC o con una conexión a ella.

Para configurar una VPC con una puerta de enlace NAT para navegar por Internet sin restricciones

Si desea que su portal WorkSpaces Secure Browser tenga acceso tanto al contenido público de Internet como al contenido privado de VPC, siga estos pasos:

> **Note**
>
> Si ya ha configurado una VPC, siga los pasos siguientes para añadir una puerta de enlace NAT a la VPC. Si necesita crear una VPC nueva, consulte Cree y configure una VPC nueva.

1. Para crear la puerta de enlace NAT, complete los pasos de Crear una puerta de enlace NAT. Asegúrese de que esta puerta de enlace NAT tenga conectividad pública y se encuentre en una subred pública de la VPC.
2. Deberá especificar al menos dos subredes privadas de diferentes zonas de disponibilidad. La asignación de las subredes a diferentes zonas de disponibilidad ayuda a garantizar una mejor disponibilidad y tolerancia a los errores. Para obtener información sobre cómo crear una segunda subred privada, consulte the section called “Paso 3: añada una segunda subred privada”.

   > **Note**
   >
   > Para asegurarse de que todas las instancias de streaming tengan acceso a Internet, no conecte una subred pública a su portal de WorkSpaces Secure Browser.

3. Actualice la tabla de enrutamiento asociada a sus subredes privadas para que dirija el tráfico vinculado a Internet a la puerta de enlace NAT. Esto permite a las instancias streaming de sus subredes privadas comunicarse con Internet. Para obtener información sobre cómo asociar una tabla de enrutamiento a una subred privada, complete los pasos de Configurar tablas de enrutamiento.

Habilite la navegación restringida por Internet (mediante un proxy HTTP saliente)

La configuración de red recomendada de un portal de WorkSpaces Secure Browser es utilizar subredes privadas con una puerta de enlace NAT, de modo que el portal pueda navegar tanto por contenido público de Internet como privado. Para obtener más información, consulte the section called “Habilitación de la navegación por Internet sin restricciones (recomendado)”. Sin embargo, es posible que deba controlar la comunicación saliente desde un portal de WorkSpaces Secure Browser a Internet mediante un proxy web. Por ejemplo, si utiliza un proxy web como puerta de entrada a Internet, puede implementar controles de seguridad preventivos, como la inclusión de dominios permitidos y el filtrado de contenido. Esto también puede reducir el uso del ancho de banda y mejorar el rendimiento de la red al almacenar en caché los recursos a los que se accede con frecuencia, como páginas web o actualizaciones de software de forma local. En algunos casos de uso, es posible que tengas contenido privado al que solo se pueda acceder mediante un proxy web.

Es posible que ya esté familiarizado con la configuración del proxy en los dispositivos gestionados o en la imagen de sus entornos virtuales. Sin embargo, esto plantea problemas si no se tiene el control del dispositivo (por ejemplo, cuando los usuarios utilizan dispositivos que no son propiedad de la

empresa ni están gestionados por ella) o si se necesita gestionar la imagen de su entorno virtual. Con WorkSpaces Secure Browser, puedes configurar el proxy mediante las políticas de Chrome integradas en el navegador web. Para ello, configura un proxy HTTP de salida para WorkSpaces Secure Browser.

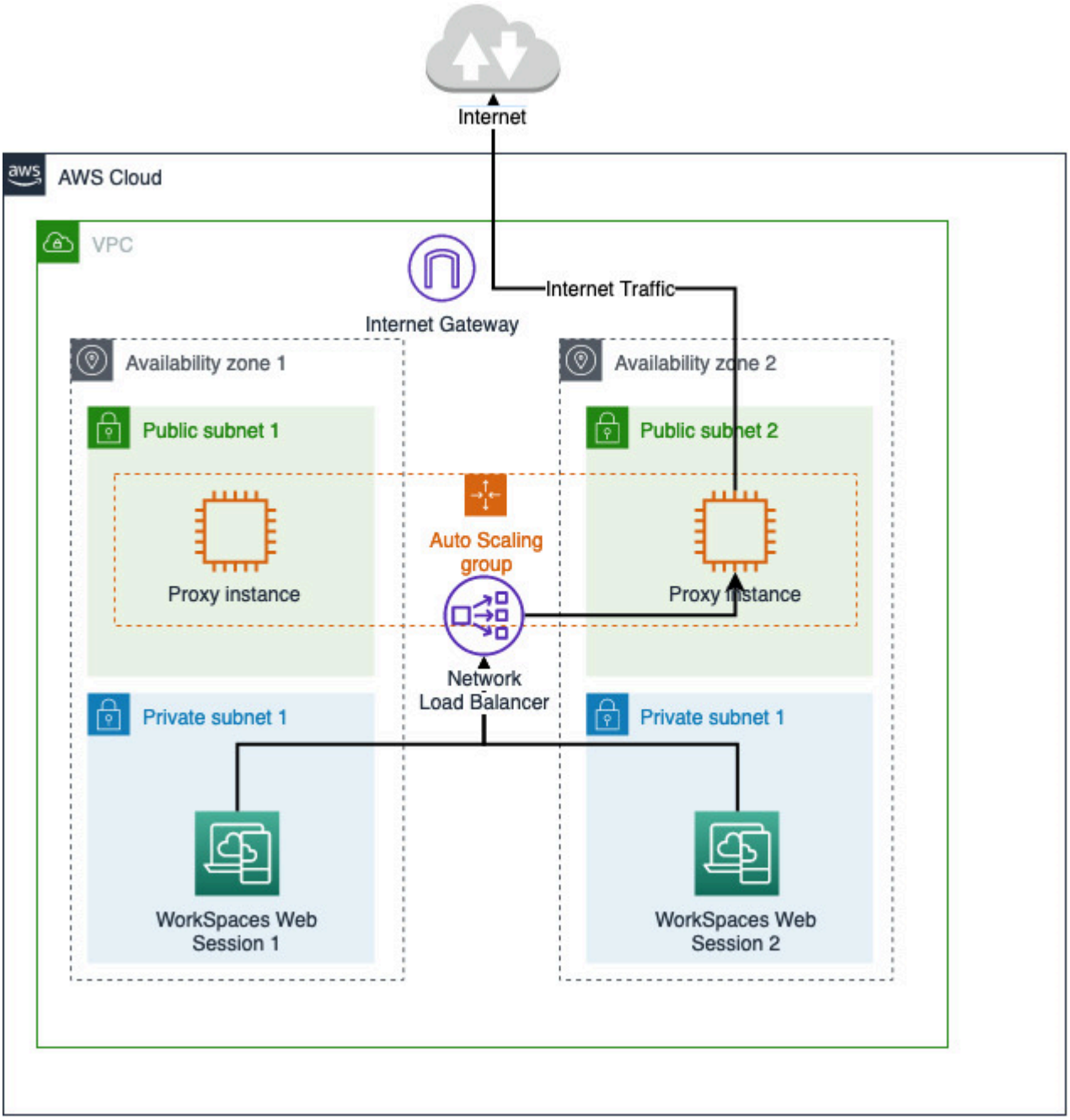
Esta solución se basa en una configuración de proxy de VPC saliente recomendada. La solución de proxy se basa en el proxy HTTP de código abierto Squid. A continuación, utiliza los ajustes del navegador WorkSpaces Secure Browser para configurar el portal WorkSpaces Secure Browser para que se conecte al punto final del proxy. Para obtener más información, consulta Cómo configurar un proxy de VPC saliente con listas blancas de dominios y filtrado de contenido.

Esta solución le ofrece las siguientes ventajas:

- Un proxy de salida que incluye un grupo de instancias de Amazon EC2 que se autoescalan y que están alojadas en un balanceador de carga de red. Las instancias proxy se encuentran en una subred pública y cada una de ellas está conectada con una IP elástica para que puedan tener acceso a Internet.
- Un portal de navegador WorkSpaces seguro implementado en subredes privadas. No necesita configurar la puerta de enlace NAT para habilitar el acceso a Internet. En su lugar, configura la política de su navegador para que todo el tráfico de Internet pase por el proxy saliente. Si desea utilizar su propio proxy, la configuración del portal WorkSpaces Secure Browser será similar.

Arquitectura

El siguiente es un ejemplo de una configuración de proxy típica en su VPC. La instancia proxy de Amazon EC2 se encuentra en subredes públicas y está asociada a Elastic IP, por lo que tiene acceso a Internet. Un balanceador de carga de red aloja un grupo de instancias proxy con escalado automático. Esto garantiza que las instancias proxy puedan ampliarse automáticamente y que el equilibrador de carga de red sea el único punto final del proxy, que pueden utilizar las sesiones de WorkSpaces Secure Browser.



Requisitos previos

Antes de empezar, asegúrese de cumplir los siguientes requisitos previos:

- Necesita una VPC ya implementada, con subredes públicas y privadas distribuidas en varias zonas de disponibilidad (AZ). Para obtener más información sobre cómo configurar su entorno de VPC, consulte VPC predeterminadas.

- Necesita un único punto de enlace proxy al que se pueda acceder desde las subredes privadas, donde se encuentran las sesiones de WorkSpaces Secure Browser (por ejemplo, el nombre DNS del balanceador de carga de red). Si quiere usar su proxy actual, asegúrese de que también tenga un único punto final al que se pueda acceder desde sus subredes privadas.

Configure un proxy HTTP de salida para WorkSpaces Secure Browser

Para configurar un proxy HTTP de salida para WorkSpaces Secure Browser, siga estos pasos.

1. Para implementar un ejemplo de proxy saliente en su VPC, siga los pasos de Cómo configurar un proxy de VPC saliente con listas blancas de dominios y filtrado de contenido.
   a. Siga los pasos de la sección «Instalación (configuración única)» para implementar la plantilla en su cuenta. CloudFormation Asegúrese de elegir la VPC y las subredes correctas como parámetros de la CloudFormation plantilla.
   b. Tras la implementación, busque los parámetros CloudFormation de salida OutboundProxyDominio y OutboundProxy puerto. Estos son el nombre y el puerto DNS de su proxy.
   c. Si ya tienes tu propio proxy, omite este paso y usa el nombre y el puerto DNS de tu proxy.
2. En la consola de WorkSpaces Secure Browser, seleccione su portal y, a continuación, elija Editar.
   a. En los detalles de la conexión de red, selecciona la VPC y las subredes privadas que tienen acceso al proxy.
   b. En la configuración de la política, agrega la siguiente ProxySettings política mediante un editor de JSON. El `ProxyServer` campo debe ser el nombre DNS y el puerto del proxy. Para obtener más información sobre ProxySettings la 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. En tu sesión de WorkSpaces Secure Browser, verás que el proxy está aplicado a Chrome y que Chrome utiliza la configuración de proxy de tu administrador.
4. Ve a chrome: //policy y a la pestaña de políticas de Chrome para confirmar que se aplica la política.
5. Compruebe que su sesión de WorkSpaces Secure Browser pueda navegar correctamente por el contenido de Internet sin la puerta de enlace NAT. En los CloudWatch registros, compruebe que los registros de acceso al proxy de Squid estén registrados.

Resolución de problemas

Una vez aplicada la política de Chrome, si tu sesión de WorkSpaces Secure Browser sigue sin poder acceder a Internet, sigue estos pasos para intentar resolver el problema:

- Comprueba que se pueda acceder al punto final del proxy desde las subredes privadas en las que se encuentra tu portal de WorkSpaces Secure Browser. Para ello, cree una instancia de EC2 en la subred privada y pruebe la conexión desde la instancia de EC2 privada a su punto de conexión proxy.
- Compruebe que el proxy tenga acceso a Internet.
- Comprueba que la política de Chrome sea correcta.
  - Confirme el siguiente formato para el `ProxyServer` campo de la política:`<Proxy DNS name>:<Proxy port>`. No debe haber ningún `http://` o `https://` en el prefijo.
  - En la sesión de WorkSpaces Secure Browser, usa Chrome para ir a chrome: //policy y asegúrate de que la ProxySettings política se ha aplicado correctamente.

Recomendaciones de configuración de la VPC

Las siguientes recomendaciones pueden ayudarle a configurar la VPC de forma más eficaz y segura.

Configuración general de la VPC

- Asegúrese de que la configuración de la VPC sea compatible con sus necesidades de escalado.
- Asegúrese de que sus cuotas de servicio de WorkSpaces Secure Browser (también denominadas límites) sean suficientes para satisfacer la demanda prevista. Para solicitar un aumento de cuota,

puede utilizar la consola de Service Quotas en https://console.aws.amazon.com/servicequotas/. Para obtener información sobre las cuotas predeterminadas de WorkSpaces Secure Browser, consultethe section called “Administre las cuotas de servicio de su portal”.

- Si planea proporcionar acceso a Internet a sus sesiones de streaming, le recomendamos que configure una VPC con una puerta de enlace NAT en una subred pública.

Interfaces de redes elásticas

- Cada sesión de WorkSpaces Secure Browser requiere su propia interface de red elástica durante la duración de la transmisión. WorkSpaces Secure Browser crea tantas interfaces de red elásticas (ENI) como la capacidad máxima deseada de su flota. De forma predeterminada, el límite de ENI por región es de 5000. Para obtener más información, consulte Interfaces de red.

  Cuando planifique la capacidad para implementaciones muy grandes, por ejemplo, miles de sesiones de streaming simultáneas, tenga en cuenta la cantidad de ENI que podrían necesitarse para el uso máximo. Le recomendamos que el límite de ENI sea igual o superior al límite máximo de uso simultáneo que configure para su portal web.

Subredes

- A medida que desarrolle su plan para aumentar el número de usuarios, tenga en cuenta que cada sesión de WorkSpaces Secure Browser requiere una dirección IP de cliente única en las subredes configuradas. Por lo tanto, el tamaño del espacio de direcciones IP del cliente configurado en las subredes determina la cantidad de usuarios que pueden transmitir de forma simultánea.
- Recomendamos que cada una de las subredes privadas esté configurada con una máscara de subred que permita suficientes direcciones IP de cliente para el número máximo de usuarios simultáneos previstos. Además, considere la posibilidad de añadir direcciones IP adicionales para tener en cuenta el crecimiento previsto. Para obtener más información, consulte Tamaño de subred Y VPC para direcciones IPv4.
- Le recomendamos que configure una subred en cada zona de disponibilidad única que admita WorkSpaces Secure Browser en la región que desee por motivos de disponibilidad y escalabilidad. Para obtener más información, consulte the section called “Cree y configure una VPC nueva”.
- Asegúrese de que los recursos de red necesarios para las aplicaciones son accesibles a través sus subredes.

Grupos de seguridad

- Utilice grupos de seguridad para proporcionar control de acceso adicional a la VPC.

  Los grupos de seguridad que pertenecen a su VPC le permiten controlar el tráfico de red entre las instancias de streaming de WorkSpaces Secure Browser y los recursos de red que requieren las aplicaciones web. Asegúrese de que los grupos de seguridad proporcionen acceso a los recursos de red que necesitan las aplicaciones web.

Zonas de disponibilidad admitidas

Al crear una nube privada virtual (VPC) para usarla con WorkSpaces Secure Browser, las subredes de la VPC deben residir en diferentes zonas de disponibilidad de la región en la que se está lanzando Secure Browser. WorkSpaces Las zonas de disponibilidad son ubicaciones diferentes diseñadas para quedar aisladas en caso de error en otras zonas de disponibilidad. Al lanzar instancias en distintas zonas de disponibilidad, puede proteger sus aplicaciones de los errores que se produzcan en una única ubicación. Cada subred debe residir enteramente en una zona de disponibilidad y no puede abarcar otras zonas. Le recomendamos configurar una subred para cada AZ compatible en la región que desee para conseguir la máxima resiliencia

Una zona de disponibilidad está representada por un código de región seguido de un identificador de letra; por ejemplo, `us-east-1a`. Para garantizar que los recursos se distribuyen por todas las zonas de disponibilidad de una región, asignamos zonas de disponibilidad de manera independiente a nombres de cada cuenta de AWS . Por ejemplo, es posible que la zona de disponibilidad `us-east-1a` de su cuenta de AWS no se encuentre en la misma ubicación de `us-east-1a` que otra cuenta de AWS .

Para coordinar las zonas de disponibilidad entre cuentas, debe usar el ID de AZ, que es un identificador único y constante de una zona de disponibilidad. Por ejemplo, `use1-az2` es un ID de zona de acceso para la `us-east-1` región y tiene la misma ubicación en todas las cuentas. AWS

La visualización de los ID de zona de disponibilidad le permite determinar la ubicación de los recursos de una cuenta en relación con los recursos de otra cuenta. Por ejemplo, si comparte una subred en la zona de disponibilidad con el ID de AZ `use1-az2` con otra cuenta, esta subred está disponible para dicha cuenta de la zona de disponibilidad cuyo ID de zona de disponibilidad es también `use1-az2`. El ID de zona de disponibilidad para cada VPC y subred aparece en la consola de Amazon VPC.

WorkSpaces Secure Browser está disponible en un subconjunto de las zonas de disponibilidad de cada región compatible. En la siguiente tabla, se enumeran los ID de AZ que puede usar para cada

región. Para ver la asignación de ID de AZ a las zonas de disponibilidad de su cuenta, consulte ID de AZ de sus recursos en la Guía del usuario de AWS RAM .

Nombre de la región	Código de región	ID de AZ admitidos
Este de EE. UU. (Norte de Virginia)	us-east-1	use1-az1, use1-az2, use1-az4, use1-az5, use1-az6
Oeste de EE. UU. (Oregón)	us-west-2	usw2-az1, usw2-az2, usw2-az3
Asia-Pacífico (Bombay)	ap-south-1	aps1-az1, aps1-az3
Asia-Pacífico (Seúl)	ap-northeast-2	apne2-az1 , apne2-az2 , apne2-az3
Asia-Pacífico (Singapur)	ap-southeast-1	apse1-az1 , apse1-az2 , apse1-az3
Asia-Pacífico (Sídney)	ap-southeast-2	apse2-az1 , apse2-az2 , apse2-az3
Asia-Pacífico (Tokio)	ap-northeast-1	apne1-az1 , apne1-az2 , apne1-az4
Canadá (centro)	ca-central-1	cac1-az1, cac1-az2, cac1-az4
Europa (Fráncfort)	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 obtener más información sobre las zonas de disponibilidad y los ID de zona de disponibilidad, consulte Regiones, zonas de disponibilidad y zonas locales en la Guía del usuario de Amazon EC2.

Conexión a VPC

Cada instancia de streaming de WorkSpaces Secure Browser tiene una interfaz de red de cliente que proporciona conectividad a los recursos de la VPC, así como a Internet si se configuran subredes privadas con una puerta de enlace NAT.

Para conectividad a Internet, los siguientes puertos deben estar abiertos a todos los destinos. Si utiliza un grupo de seguridad personalizado o modificado, tendrá que añadir las reglas manualmente. Para obtener más información, consulte Reglas del grupo de seguridad.

> **Note**
>
> Esto se aplica al tráfico de salida.

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

Conexión entre cliente y usuario

WorkSpaces Secure Browser está configurado para enrutar las conexiones de streaming a través de la Internet pública. La conectividad a Internet es necesaria para autenticar a los usuarios y ofrecer los activos web que WorkSpaces Secure Browser necesita para funcionar. Para que este tráfico sea posible, debe permitir los dominios enumerados en Dominios permitidos.

En los temas siguientes se proporciona información sobre cómo habilitar las conexiones de los usuarios a WorkSpaces Secure Browser.

Temas

Requisitos de puertos y direcciones IP

Para acceder a las instancias de WorkSpaces Secure Browser, los dispositivos de los usuarios requieren acceso saliente en los siguientes puertos:

- Puerto 443 (TCP)
  - El puerto 443 se utiliza para la comunicación HTTPS entre los dispositivos de los usuarios y las instancias de streaming cuando se utilizan los puntos de conexión de Internet. Normalmente, cuando los usuarios finales navegan por la web durante las sesiones de streaming, el navegador web selecciona de forma aleatoria un puerto de origen en el intervalo alto para tráfico de streaming. Debe asegurarse de que el tráfico de retorno a este puerto esté permitido.
  - Este puerto debe estar abierto a los dominios necesarios que se indican en Dominios permitidos.
  - AWS publica sus rangos de direcciones IP actuales, incluidos los rangos en los que la puerta de enlace de sesión y CloudFront los dominios pueden resolver, en formato JSON. Para obtener información acerca de cómo descargar el archivo .json y ver los rangos actuales, consulte Rangos de direcciones IP de AWS. O bien, si lo está utilizando AWS Tools for Windows PowerShell, puede acceder a la misma información mediante el Get-AWSPublicIpAddressRange PowerShell comando. Para obtener más información, consulte Consulta de los rangos de direcciones IP públicas para AWS.
- (Opcional) Puerto 53 (UDP)
  - El puerto 53 se utiliza para la comunicación entre los dispositivos de los usuarios y sus servidores DNS.
  - Si no se utilizan servidores DNS para resolver nombres de dominio, este puerto es opcional.
  - El puerto debe estar abierto a las direcciones IP para sus servidores DNS de modo que los nombres de dominio público se puedan resolver.

Dominios permitidos

Para que los usuarios puedan acceder a los portales web desde su navegador local, debe añadir los siguientes dominios a la lista de dominios permitidos en la red desde la que el usuario intenta acceder al servicio.

En la siguiente tabla, sustituya *{region}* por el código de la región del portal web operativo. Por ejemplo, s3. *{region}* .amazonaws.com debe ser s3.eu-west-1.amazonaws.com para un portal web de la región Europa (Irlanda). Para obtener una lista de los códigos de región, consulte los puntos de conexión y las cuotas de Amazon WorkSpaces Secure Browser.

Categoría	Dominio o dirección IP
WorkSpaces Activos de streaming de Secure Browser	s3.*{region}*.amazonaws.com

Categoría	Dominio o dirección IP
	s3.amazonaws.com appstream2.*{region}*.aws.amazon.com *.amazonappstream.com *.shortbread.aws.dev
WorkSpaces Activos estáticos de Secure Browser	*.workspaces-web.com di5ry4hb4263e.cloudfront.net
WorkSpaces Autenticación segura del navegador	*.auth.*{region}*.amazoncognito.com cognito-identity.*{region}*.amazonaws.com cognito-idp.*{region}*.amazonaws.com *.cloudfront.net
WorkSpaces Métricas e informes de Secure Browser	*.execute-api.*{region}*.amazonaws.com unagi-na.amazon.com

En función del proveedor de identidades configurado, es posible que también tenga que permitir dominios adicionales en la lista. Revise la documentación de su IdP para identificar qué dominios debe permitir en la lista para que WorkSpaces Secure Browser utilice ese proveedor. Si utiliza IAM Identity Center, consulte Requisitos previos de IAM Identity Center para obtener más información.

Cómo empezar a usar WorkSpaces Secure Browser

Siga estos pasos para crear un portal web de WorkSpaces Secure Browser y proporcionar a los usuarios acceso a sitios web internos y de SaaS desde sus navegadores actuales. Puede crear un portal web en cualquier región admitida por cuenta.

> **Note**
>
> Para solicitar un aumento del límite para más de un portal, ponte en contacto con el servicio de asistencia con tu Cuenta de AWS ID, el número de portales que deseas solicitar y Región de AWS.

Este proceso suele tardar cinco minutos con el asistente de creación del portal web y 15 minutos más como máximo para que el portal se Active.

La configuración de un portal web no conlleva ningún coste. WorkSpaces Secure Browser ofrece pay-as-you-go precios, que incluyen un precio mensual bajo para los usuarios que utilizan el servicio de forma activa. No hay costes iniciales, licencias ni compromisos a largo plazo.

> **Important**
>
> Antes de comenzar, debe cumplir los requisitos previos necesarios para un portal web. Para obtener más información acerca de los requisitos previos de un portal web, consulte Configuración de WorkSpaces Secure Browser.

Temas

Paso 1: cree un portal web

Para crear un portal web, siga estos pasos:

Temas

Configurar los ajustes de red

1. Abra la consola de WorkSpaces Secure Browser en https://console.aws.amazon.com/workspaces-web/home.
2. Elija WorkSpaces Secure Browser, después portales web y, a continuación, elija Crear portal web.
3. En la página Paso 1: especifique la conexión de red, complete los siguientes pasos para conectar la VPC al portal web y configurar la VPC y las subredes.

    1. Para obtener información sobre la red, elija una VPC con una conexión al contenido al que desee que accedan sus usuarios con WorkSpaces Secure Browser.
    2. Elija hasta tres subredes privadas que cumplan los siguientes requisitos. Para obtener más información, consulte Redes y acceso.
        - Debe elegir un mínimo de dos subredes privadas para crear un portal.
        - Para garantizar la alta disponibilidad de su portal web, le recomendamos que proporcione el número máximo de subredes privadas en zonas de disponibilidad únicas para su VPC.
    3. Elija un grupo de seguridad.

Configuración de los ajustes del portal

En la página Paso 2: configure los ajustes del portal web, complete los siguientes pasos para personalizar la experiencia de navegación de los usuarios al abrir una sesión.

1. En Detalles del portal web, en Nombre para mostrar, introduzca un nombre identificable para el portal web.
2. En Tipo de instancia, seleccione el tipo de instancia para su portal web en el menú desplegable. A continuación, introduzca su límite máximo de usuarios simultáneos para el portal web. Para

obtener más información, consulte the section called “Administre las cuotas de servicio de su portal”.

> **Note**
>
> Al seleccionar un nuevo tipo de instancia, se cambiará el costo de cada usuario activo mensual. Para obtener más información, consulta los precios de Amazon WorkSpaces Secure Browser.

3. En Registro de acceso de usuario, en el ID de flujo de Kinesis, seleccione el flujo de datos de Amazon Kinesis al que quiere enviar los datos. Para obtener más información, consulte the section called “Configuración del registro de acceso de usuario”.
4. En Configuración de la política, complete lo siguiente:

   - En Opciones de política, seleccione Editor visual o Cargar archivo JSON. Puede usar cualquiera de los dos métodos para proporcionar los detalles de configuración de la política para su portal web. Para obtener más información, consulte the section called “Configuración o edición de la política de su navegador”.
     - WorkSpaces Secure Browser incluye compatibilidad con las políticas empresariales de Chrome. Puede añadir y administrar políticas con un editor visual o cargando manualmente los archivos de políticas. Puede cambiar entre las opciones en cualquier momento.
     - Al cargar un archivo de política, puede ver las políticas disponibles en el archivo en la consola. Sin embargo, no es posible editar todas las políticas en el editor visual. La consola muestra las políticas de su archivo JSON, que no puede editar con el editor visual en Políticas JSON adicionales. Para realizar cambios en estas políticas, debe editarlas manualmente.
   - (Opcional) En URL de inicio: opcional, introduzca un dominio para usarlo como página de inicio cuando los usuarios abran su navegador. La VPC debe tener una conexión estable a esta URL.
   - Seleccione o desactive Navegación privada y Eliminación del historial para activar o desactivar estas características durante la sesión de un usuario

     > **Note**
     >
     > Las URL visitadas mientras navega de forma privada o antes de que un usuario elimine su historial de navegación no se pueden registrar en el registro de acceso de

usuarios. Para obtener más información, consulte the section called “Configuración del registro de acceso de usuario”.

- En el filtrado de URL, puedes configurar las URL que pueden visitar los usuarios durante una sesión. Para obtener más información, consulte the section called “Configure el filtrado de URL”.
- (Opcional) En Marcadores del navegador: opcional, introduzca el Nombre para mostrar, el Dominio y la Carpeta de los marcadores que desee que sus usuarios vean en su navegador. A continuación, seleccione Añadir marcador.

> **Note**
>
> Dominio es un campo obligatorio para los marcadores del navegador.
> En Chrome, los usuarios encontrarán los marcadores administrados en la carpeta Marcadores administrados de la barra de herramientas de marcadores.

- (Opcional) Añada Etiquetas a su portal. Puede usar etiquetas para buscar o filtrar sus AWS recursos. Las etiquetas constan de una clave y un valor opcional y están asociadas al recurso del portal.

5. En Control de acceso de IP (opcional), elija si desea restringir el acceso a redes de confianza. Para obtener más información, consulte the section called “Configure los controles de acceso de IP (opcional)”.
6. Elija Siguiente para continuar.

Configuración de los ajustes de usuario

En la página Paso 3: seleccione la configuración de usuario, complete los siguientes pasos para elegir las características a las que pueden acceder sus usuarios desde la barra de navegación superior durante la sesión y, a continuación, seleccione Siguiente:

1. En Permisos de usuario, elija si desea habilitar la extensión para el inicio de sesión único. Para obtener más información, consulte the section called “Habilite la extensión de inicio de sesión único (opcional)”.
2. En Permisos del portapapeles, seleccione Desactivado o Activado.
3. En Transferencia de archivos, seleccione Desactivado o Activado.

4. En Permitir a los usuarios imprimir en un dispositivo local desde su portal web, seleccione Permitido o No permitido.
5. En Permitir a los usuarios establecer enlaces profundos a su portal web, seleccione Permitido o No permitido. Para obtener más información sobre los enlaces profundos, consulte. the section called “Permitir enlaces profundos (opcional)”
6. En Detalles de la sesión de usuario, especifique lo siguiente:

   - En Tiempo de espera de desconexión en minutos, elija la cantidad de tiempo que una sesión de streaming permanece activa después de que los usuarios se hayan desconectado. Si los usuarios intentan volver a conectarse a la sesión de streaming después de una desconexión o interrupción de la red dentro de este intervalo de tiempo, se conectarán a la sesión anterior. De lo contrario, se conectan a una sesión nueva con una nueva instancia de streaming.

     Si un usuario finaliza la sesión, no se aplica el tiempo de espera de desconexión, sino que se pide al usuario que guarde cualquier documento que tenga abierto y, a continuación, se le desconecta inmediatamente de la instancia de streaming. La instancia que estaba utilizando el usuario termina.
   - En Tiempo de espera de desconexión de inactividad en minutos, elija la cantidad de tiempo que los usuarios pueden estar inactivos antes de desconectarlos de su sesión de streaming y de que comience el intervalo de tiempo Tiempo de espera de desconexión en minutos. Se notificará a los usuarios antes de que se desconecten por inactividad. Si intentan volver a conectarse a la sesión de streaming antes de que haya transcurrido el intervalo de tiempo especificado en Tiempo de espera de desconexión en minutos, se conectan a su sesión anterior. De lo contrario, se conectan a una sesión nueva con una nueva instancia de streaming. Si este valor se establece en 0, se deshabilita. Cuando este valor está deshabilitado, los usuarios no desconectan por inactividad.

     > **Note**
     >
     > Los usuarios se consideran inactivos cuando dejan de introducir datos a través del teclado o del ratón durante su sesión de streaming. Las cargas y descargas de archivos, la entrada y salida de audio y los cambios de píxeles no se consideran actividad del usuario. Si los usuarios siguen estando inactivos después de que haya transcurrido el intervalo de tiempo de Tiempo de espera de desconexión de inactividad en minutos, se desconectan.

Configuración del proveedor de identidades

Siga los siguientes pasos para configurar su proveedor de identidad (IdP).

Temas

Elija el tipo de proveedor de identidad

WorkSpaces Secure Browser ofrece dos tipos de autenticación: estándar y AWS IAM Identity Center. Puede elegir el tipo de autenticación que va a utilizar con su portal en la página Configurar el proveedor de identidad.

- En el caso de la versión estándar (opción predeterminada), federa tu proveedor de identidades SAML 2.0 externo (como Okta o Ping) directamente con tu portal. Para obtener más información, consulte the section called “Configure el tipo de autenticación estándar”. El tipo estándar admite flujos de autenticación iniciados por SP e iniciados por IdP.
- En el caso del Centro de identidades de IAM (opción avanzada), federe el Centro de identidades de IAM con su portal. Para usar este tipo de autenticación, el centro de identidad de IAM y el portal WorkSpaces Secure Browser deben residir en el mismo lugar. Región de AWS Para obtener más información, consulte the section called “Configure el tipo de autenticación del IAM Identity Center”.

Configure el tipo de autenticación estándar

En el caso de la versión estándar (predeterminada), federa tu proveedor de identidad SAML 2.0 externo (como Okta o Ping) directamente con tu portal.

El tipo de identidad estándar puede admitir flujos de inicio de sesión service-provider-initiated (iniciados por SP) e identity-provider-initiated (iniciados por IdP) con un IdP compatible con SAML 2.0.

Paso 1: Comience a configurar su proveedor de identidad en Secure Browser WorkSpaces

Complete los siguientes pasos para configurar su proveedor de identidad:

1. En la página Configurar proveedor de identidad del asistente de creación, elija Estándar.
2. Elija Continuar con el IdP estándar.
3. Descargue el archivo de metadatos del SP y mantenga la pestaña abierta para ver los valores de metadatos individuales.
   - Si el archivo de metadatos del SP está disponible, elija Descargar archivo de metadatos para descargar el documento de metadatos del proveedor de servicios (SP) y cargue el archivo de metadatos del proveedor de servicios en su iDP en el siguiente paso. Sin esto, los usuarios no podrán iniciar sesión.
   - Si su proveedor no carga los archivos de metadatos del SP, introduzca manualmente los valores de los metadatos.
4. En Elegir el tipo de inicio de sesión de SAML, elige entre aserciones de SAML iniciadas por SP e iniciadas por IDP, o solo aserciones de SAML iniciadas por SP.
   - Las aserciones SAML iniciadas por SP e iniciadas por IdP permiten que su portal admita ambos tipos de flujos de inicio de sesión. Los portales que admiten flujos iniciados por el IdP permiten presentar las aserciones de SAML en el punto final de la federación de identidades del servicio sin necesidad de que los usuarios inicien una sesión visitando la URL del portal.
     - Elija esta opción para permitir que el portal acepte aserciones de SAML iniciadas por el IdP no solicitadas.
     - Esta opción requiere que se configure un estado de retransmisión predeterminado en su proveedor de identidad de SAML 2.0. El parámetro de estado de retransmisión de su portal se encuentra en la consola, en el inicio de sesión SAML iniciado por el IdP, o puede copiarlo del archivo de metadatos del SP que se encuentra en. `<md:IdPInitRelayState>`
     - Nota
       - El siguiente es el formato del estado de retransmisión:. `redirect_uri=https%3A%2F%2Fportal-id.workspaces-web.com%2Fsso&response_type=code&client_id=1example23456789&identity_provider=ExIdentity-Provider`
       - Si copia y pega el valor del archivo de metadatos del SP, asegúrese de cambiarlo `&` a&. `&`es un carácter de escape XML.
   - Elija solo las aserciones SAML iniciadas por SP para que el portal solo admita los flujos de inicio de sesión iniciados por SP. Esta opción rechazará las afirmaciones de SAML no solicitadas de los flujos de inicio de sesión iniciados por el IdP.

> **Note**
>
> Algunos proveedores de terceros IdPs le permiten crear una aplicación SAML personalizada que puede ofrecer experiencias de autenticación iniciadas por el IdP aprovechando los flujos iniciados por el SP. Por ejemplo, consulte Add an Okta bookmark application.

5. Elija si desea habilitar la firma de solicitudes de SAML a este proveedor. La autenticación iniciada por el SP permite a su IdP validar que la solicitud de autenticación proviene del portal, lo que impide aceptar solicitudes de terceros.
   a. Descargue el certificado de firma y cárguelo en su IdP. Se puede usar el mismo certificado de firma para el cierre de sesión único.
   b. Habilita la solicitud firmada en tu IdP. El nombre puede ser diferente, según el IdP.

   > **Note**
   >
   > El RSA-SHA256 es el único algoritmo de firma de solicitudes y el predeterminado que se admite.

6. Elija si desea activar la opción Requerir aserciones SAML cifradas. Esto le permite cifrar la afirmación de SAML que proviene de su IdP. Puede evitar que los datos se intercepten en las afirmaciones de SAML entre el IdP y Secure Browser. WorkSpaces

   > **Note**
   >
   > El certificado de cifrado no está disponible en este paso. Se creará después de que se inicie el portal. Tras iniciar el portal, descargue el certificado de cifrado y cárguelo en su IdP. A continuación, habilite el cifrado de aserciones en su IdP (el nombre puede ser diferente, según el IdP).

7. Elija si desea habilitar el cierre de sesión único. El cierre de sesión único permite a los usuarios finales cerrar sesión tanto en su sesión de IdP WorkSpaces como en la de Secure Browser con una sola acción.
   a. Descargue el certificado de firma de WorkSpaces Secure Browser y cárguelo en su IdP. Es el mismo certificado de firma que se utilizó para solicitar la firma en el paso anterior.

b. Para usar el cierre de sesión único, debes configurar una URL de cierre de sesión único en tu proveedor de identidad de SAML 2.0. Puedes encontrar la URL de cierre de sesión único de tu portal en la consola, en la sección Detalles del proveedor de servicios (SP): Mostrar valores de metadatos individuales, o en el archivo de metadatos del SP, en la sección correspondiente. `<md:SingleLogoutService>`

c. Habilite el cierre de sesión único en su IdP. El nombre puede ser diferente, según el IdP.

Paso 2: Configura tu proveedor de identidad en tu propio IdP

Abra una nueva pestaña en el navegador. A continuación, realice los pasos siguientes con su IdP:

1. Agregue los metadatos del portal a su IDP de SAML.

   Cargue el documento de metadatos del SP que descargó en el paso anterior en su IdP o copie y pegue los valores de los metadatos en los campos correctos de su IdP. Algunos proveedores no permiten la carga de archivos.

   Los detalles de este proceso pueden variar de un proveedor a otro. Consulte la documentación de su proveedor the section called “Guía para información específica IdPs” para obtener ayuda sobre cómo agregar los detalles del portal a la configuración de su IdP.

2. Confirma el NameID de tu afirmación de SAML.

   Asegúrese de que su IdP de SAML complete NameID en la aserción de SAML con el campo de correo electrónico del usuario. NameID y el correo electrónico del usuario se utilizan para identificar de forma exclusiva a su usuario federado de SAML en el portal. Usa el formato de ID de nombre SAML persistente.

3. Opcional: configure el estado de retransmisión para la autenticación iniciada por el IdP.

   Si eligió Aceptar aserciones SAML iniciadas por el SP e iniciadas por el IDP en el paso anterior, siga los pasos del paso 2 the section called “Paso 1: Comience a configurar su proveedor de identidad en Secure Browser WorkSpaces ” para configurar el estado de retransmisión predeterminado para su aplicación de IdP.

4. Opcional: configura la firma de solicitudes. Si eligió Firmar las solicitudes de SAML a este proveedor en el paso anterior, siga los pasos del paso 3 the section called “Paso 1: Comience a configurar su proveedor de identidad en Secure Browser WorkSpaces ” para cargar el certificado de firma en su IdP y habilitar la firma de las solicitudes. Algunas IdPs , como Okta, pueden

requerir que tu NameID pertenezca al tipo «persistente» para usar la firma de solicitudes. Asegúrate de confirmar tu NameID para tu afirmación de SAML siguiendo los pasos anteriores.

5. Opcional: configura el cifrado de aserciones. Si seleccionó Requerir aserciones SAML cifradas de este proveedor, espere a que se complete la creación del portal y, a continuación, siga el paso 4 de «Cargar metadatos» que aparece a continuación para cargar el certificado de cifrado en su IDP y habilitar el cifrado de aserciones.
6. Opcional: configure el cierre de sesión único. Si eligió el cierre de sesión único, siga los pasos del paso 5 the section called “Paso 1: Comience a configurar su proveedor de identidad en Secure Browser WorkSpaces ” para cargar el certificado de firma en su IDP, complete la URL de cierre de sesión único y habilite el cierre de sesión único.
7. Conceda acceso a sus usuarios en su IdP para usar WorkSpaces Secure Browser.
8. Descargue un archivo de intercambio de metadatos desde su IdP. En el siguiente paso, cargará estos metadatos en WorkSpaces Secure Browser.

Paso 3: Termine de configurar su proveedor de identidad en WorkSpaces Secure Browser

Regrese a la consola de WorkSpaces Secure Browser. En la página Configurar el proveedor de identidad del asistente de creación, en Metadatos del IdP, cargue un archivo de metadatos o introduzca una URL de metadatos de su IdP. El portal utiliza estos metadatos de su IdP para establecer la confianza.

1. Para cargar un archivo de metadatos, en Documento de metadatos de IdP, elija Elegir archivo. Cargue el archivo de metadatos con formato XML del IDP que descargó en el paso anterior.
2. Para usar una URL de metadatos, vaya al IdP que configuró en el paso anterior y obtenga su URL de metadatos. Vuelva a la consola de WorkSpaces Secure Browser y, en URL de metadatos del IdP, introduzca la URL de metadatos que obtuvo de su IdP.
3. Cuando haya terminado, elija Next.
4. Para los portales en los que ha activado la opción Requerir aserciones SAML cifradas a este proveedor, debe descargar el certificado de cifrado de la sección de detalles del IdP del portal y cargarlo en su IdP. A continuación, puede activar la opción allí.

> **Note**
>
> WorkSpaces Secure Browser requiere que el asunto o NameID estén mapeados y configurados en la aserción SAML dentro de la configuración de su IdP. Su IdP puede

crear estas asignaciones automáticamente. Si estas asignaciones no están configuradas correctamente, los usuarios no podrán iniciar sesión en el portal web.
WorkSpaces Secure Browser requiere que las siguientes afirmaciones estén presentes en la respuesta de SAML. Puede buscar **<**Your SP Entity ID**>**y en los **<**Your SP ACS URL**>**detalles del proveedor de servicios o en el documento de metadatos de su portal, ya sea a través de la consola o la CLI.

- Una `AudienceRestriction` reclamación con un `Audience` valor que establece su ID de entidad de SP como objetivo de la respuesta. Ejemplo:

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

- Una reclamación `Response` con un valor `InResponseTo` del ID de solicitud SAML original. Ejemplo:

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

- Una `SubjectConfirmationData` reclamación con el `Recipient` valor de la URL de su SP ACS y un `InResponseTo` valor que coincide con el ID de solicitud de SAML original. Ejemplo:

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

WorkSpaces Secure Browser valida los parámetros de la solicitud y las afirmaciones de SAML. En el caso de las aserciones de SAML iniciadas por el IdP, los detalles de la solicitud deben formatearse como un `RelayState` parámetro en el cuerpo de una solicitud HTTP POST. El cuerpo de la solicitud también debe contener la aserción de SAML como parámetro. `SAMLResponse` Ambos deberían estar presentes si has seguido el paso anterior.
El siguiente es un ejemplo de `POST` cuerpo de un proveedor de SAML iniciado por un IdP.

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

Guía para información específica IdPs

Para asegurarse de configurar correctamente la federación de SAML para su portal, consulte los enlaces siguientes para ver la documentación más utilizada IdPs.

IdP	Configuración de la aplicación SAML	Administración de usuarios	Autenticación iniciada por IdP	Solicita la firma	Cifrado de aserciones	Cierre de sesión único
Okta	Cree integraciones de aplicaciones SAML	Administración de usuarios	Referencia de campo SAML del asistente de integración de aplicaciones	Referencia de campo SAML del Asistente de integración de aplicaciones	Referencia de campo SAML del Asistente de integración de aplicaciones	Referencia de campo SAML del Asistente de integración de aplicaciones
Entra	Crea tu propia aplicación	Inicio rápido: cree y asigne una cuenta de usuario	Habilite el inicio de sesión único para una aplicación empresarial	Verificación de firma de solicitud de SAML	Configurar el cifrado del token SAML Entra de Microsoft	Protocolo SAML de cierre de sesión único
Ping	Agregue una aplicación SAML	Usuarios	Habilitar el SSO iniciado por IdP	Configurar el inicio de sesión de la solicitud de autenticación para	¿ PingOne For Enterprise admite el cifrado?	Cierre de sesión único con SAML 2.0

IdP	Configuración de la aplicación SAML	Administración de usuarios	Autenticación iniciada por IdP	Solicita la firma	Cifrado de aserciones	Cierre de sesión único
				Enterprise PingOne		
Un inicio de sesión	Conector personalizado SAML (avanzado) (4266907)	Añadir usuarios manualmente OneLogin	Conector personalizado SAML (avanzado) (4266907)	Conector personalizado SAML (avanzado) (4266907)	Conector personalizado SAML (avanzado) (4266907)	Conector personalizado SAML (avanzado) (4266907)
IAM Identity Center	Configura tu propia aplicación SAML 2.0	Configura tu propia aplicación SAML 2.0	Configura tu propia aplicación SAML 2.0	N/A	N/A	N/A

Configure el tipo de autenticación del IAM Identity Center

Para el tipo de centro de identidad de IAM (avanzado), debe federar el centro de identidad de IAM con su portal. Seleccione esta opción únicamente si se aplica a usted lo siguiente:

- Su centro de identidad de IAM está configurado en el mismo portal web Cuenta de AWS y Región de AWS como él.
- Si lo está utilizando AWS Organizations, está utilizando una cuenta de administración.

Antes de crear un portal web con el tipo de autenticación del Centro de Identidad de IAM, debe configurar el Centro de Identidad de IAM como un proveedor independiente. Para obtener más información, consulte Comenzar con las tareas habituales en el Centro de identidades de IAM. O bien, puede conectar su IdP SAML 2.0 al IAM Identity Center. Para obtener más información, consulte Conectarse a un proveedor de identidad externo. De lo contrario, no tendrá ningún usuario o grupo que asignar a su portal web.

Si ya utiliza el Centro de identidad de IAM, puede elegir el Centro de identidad de IAM como tipo de proveedor y seguir los pasos que se indican a continuación para añadir, ver o eliminar usuarios o grupos de su portal web.

> **Note**
>
> Para poder utilizar este tipo de autenticación, su centro de identidad de IAM debe estar en el mismo portal de WorkSpaces Secure Browser Cuenta de AWS y al mismo Región de AWS nivel que él. Si su centro de identidad de IAM se encuentra en un sitio separado Cuenta de AWS o Región de AWS, siga las instrucciones para el tipo de autenticación estándar. Para obtener más información, consulte the section called “Configure el tipo de autenticación estándar”.
>
> Si lo utiliza AWS Organizations, solo puede crear portales de WorkSpaces Secure Browser integrados con el Centro de Identidad de IAM mediante una cuenta de administración.

Para crear un portal web con IAM Identity Center

1. Durante la creación del portal, en el paso 4: configurar el proveedor de identidad, elija AWS IAM Identity Center.
2. Elija Continuar con IAM Identity Center.
3. En la página Asignar usuarios y grupos, seleccione la pestaña Usuarios y/o grupos.
4. Marque la casilla situada junto a los usuarios o grupos que desee añadir al portal.
5. Tras crear el portal, los usuarios a los que ha asociado pueden iniciar sesión en WorkSpaces Secure Browser con su nombre de usuario y contraseña del IAM Identity Center.

Para crear un portal web con IAM Identity Center

1. Tras crear el portal, aparecerá en la consola del IAM Identity Center como una aplicación configurada.
2. Para acceder a la configuración de esta aplicación, seleccione Aplicaciones en la barra lateral y busque una aplicación configurada con un nombre que coincida con el nombre mostrado de su portal web.

> **Note**
>
> Si no ha introducido un nombre para mostrar, en su lugar se muestra el GUID del portal. El GUID es el ID que lleva un prefijo con la URL del punto de conexión de su portal web.

Para añadir usuarios y grupos adicionales a un portal web existente

1. Abra la consola de WorkSpaces Secure Browser enhttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Elija WorkSpaces Secure Browser, portales web, elija su portal web y, a continuación, elija Editar.
3. Elija Configuración del proveedor de identidad y Asigne usuarios y grupos adicionales. Desde aquí, puede añadir usuarios y grupos a su portal web.

> **Note**
>
> No puede añadir usuarios ni grupos desde la consola de IAM Identity Center. Debe hacerlo desde la página de edición de su portal de WorkSpaces Secure Browser.

Para ver o eliminar usuarios y grupos de su portal web

- Puede ver o eliminar el acceso de los usuarios a esta aplicación mediante las acciones disponibles en la tabla Usuarios asignados. Para obtener más información, consulte Administrar el acceso a las aplicaciones.

> **Note**
>
> No puede ver ni eliminar usuarios y grupos de la página de edición del portal WorkSpaces Secure Browserportal. Debe hacerlo desde la página de edición de la consola de IAM Identity Center.

Cambie el tipo de proveedor de identidad

Siga estos pasos para cambiar el tipo de autenticación de su portal en cualquier momento:

- Para cambiar de IAM Identity Center a Standard, siga los pasos que se indican enthe section called “Configure el tipo de autenticación estándar”.
- Para cambiar del centro de identidad estándar al de IAM, siga los pasos que se indican en. the section called “Configure el tipo de autenticación del IAM Identity Center”

Los cambios en el tipo de proveedor de identidad pueden tardar hasta 15 minutos en implementarse y no finalizarán automáticamente las sesiones en curso.

Puede ver los cambios de tipo de proveedor de identidad en su portal AWS CloudTrail inspeccionando los eventos`UpdatePortal`. El tipo está visible en las cargas útiles de solicitud y respuesta del evento.

Revisar y lanzar

1. En la página Paso 5: revisar y lanzar, revise la configuración que seleccionó para su portal web. Puede elegir Editar para cambiar la configuración dentro de una sección determinada. También puede cambiar esta configuración más adelante desde la pestaña Portales web de la consola.
2. Cuando haya acabado, elija Lanzar portal web.
3. Para ver el estado de su portal web, elija Portales web, seleccione su portal y, a continuación, elija Ver detalles.

   Los portales web tienen uno de los siguientes estados:

   - Incompleto: a la configuración del portal web le faltan los ajustes de proveedor de identidad necesarios.
   - Pendiente: el portal web está aplicando cambios en su configuración.
   - Activo: el portal web está listo y disponible para su uso.
4. Espere un máximo de 15 minutos a que el portal esté Activo.

Paso 2: pruebe el portal

Tras crear un portal web, puede iniciar sesión en el terminal de WorkSpaces Secure Browser para navegar por los sitios web conectados como lo haría un usuario final.

Si ya he realizado estos pasos en the section called “Configuración del proveedor de identidades”, puede omitir esta sección y pasar a Paso 3: distribuya su portal web.

1. Abra la consola de WorkSpaces Secure Browser en https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Elija WorkSpaces Secure Browser, portales web, elija su portal web y, a continuación, elija Ver detalles
3. En Punto de conexión del portal web, vaya a la URL especificada para su portal. El punto de conexión del portal web es el punto de acceso desde el que los usuarios abrirán el portal web tras iniciar sesión con el proveedor de identidades configurado para el portal. Está disponible públicamente en Internet y se puede integrar en la red.
4. En la página de inicio de sesión de WorkSpaces Secure Browser, selecciona Iniciar sesión, SAML e introduce tus credenciales de SAML.
5. Cuando aparezca la página Su sesión se está preparando, se iniciará la sesión de WorkSpaces Secure Browser. No cierre esta página ni salga de ella.
6. Se abrirá el navegador web con la URL de inicio y cualquier otro comportamiento adicional configurado en los ajustes de la política del navegador.
7. Ahora puede navegar a los sitios web conectados. Para ello, seleccione los enlaces o introduzca las URL en la barra de direcciones.

Paso 3: distribuya su portal web

Cuando esté listo para que sus usuarios comiencen a usar WorkSpaces Secure Browser, elija una de las siguientes opciones para distribuir el portal:

- Agregue su portal a la puerta de enlace de aplicaciones SAML para que los usuarios puedan iniciar una sesión directamente desde su IdP. Puede hacerlo mediante el flujo de inicio de sesión iniciado por el IdP con su IdP compatible con SAML 2.0. Para obtener más información, consulte Afirmaciones de SAML iniciadas por SP e iniciadas por IDP en. the section called “Configure el tipo de autenticación estándar” Como alternativa, puede crear una aplicación SAML personalizada que pueda ofrecer experiencias de autenticación iniciadas por el IdP mediante flujos iniciados por el SP. Para obtener más información, consulte Crear una integración de aplicaciones con marcadores.
- Añadir la URL del portal a un sitio web de su propiedad y utilizar un redireccionamiento del navegador para dirigir a los usuarios al portal web.
- Enviar por correo electrónico la URL del portal a sus usuarios o colocarla en un dispositivo que administre en la página de inicio o en un marcador del navegador.

Siguientes pasos

Después de crear su primer portal web, puede ver los detalles, editarlos o eliminar el portal web en cualquier momento. Para obtener más información, consulte Administración de su portal web.

Cuenta de AWS Puede crear un portal web en cada uno de los sitios en los Región de AWS que WorkSpaces Secure Browser esté disponible. Cada portal web puede admitir hasta 25 conexiones de usuario en un momento dado. Para aumentar el número de portales que puede crear en una región o para admitir más sesiones simultáneas en un portal, consulte the section called “Administre las cuotas de servicio de su portal”.

Administración de su portal web

Tras configurar el portal web, puede ver o editar sus datos, así como eliminar el portal si ya no lo necesita.

Temas

Visualización de los datos del portal web

Para ver los datos del portal web

1. Abra la consola de WorkSpaces Secure Browser enhttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Elija WorkSpaces Secure Browser, portales web, elija su portal web y, a continuación, elija Ver detalles.

Edición de un portal web

Para editar un portal web

1. Abra la consola de WorkSpaces Secure Browser enhttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Elija WorkSpaces Secure Browser, portales web, elija su portal web y, a continuación, elija Editar.

> **Note**
>
> Los cambios en la configuración de red o en la configuración del tiempo de espera finalizan inmediatamente cualquier sesión activa del portal. Los usuarios se desconectan y deben volver a conectarse para iniciar una nueva sesión. Los cambios en los Permisos del portapapeles, los Permisos de transferencia de archivos o Imprimir en dispositivo local se aplican a partir de la primera sesión nueva. Las sesiones activas en ese momento no se desconectan. Los cambios no afectan a los usuarios conectados a las sesiones activas hasta que se desconecten y se conecten a una nueva sesión.

Eliminación de un portal web

Para eliminar un portal web

1. Abra la consola de WorkSpaces Secure Browser enhttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Elija WorkSpaces Secure Browser, portales web, elija su portal web y, a continuación, elija Eliminar.

Administre las cuotas de servicio de su portal

Al crear las suyas Cuenta de AWS, establecemos automáticamente las cuotas de servicio predeterminadas (también denominadas límites) para el uso de los recursos con Servicios de AWS. Los administradores deben conocer dos cuotas que podrían necesitar aumentarse para respaldar su caso de uso. Estas dos cuotas son el número de portales web que puede crear en cada región y el número máximo de sesiones simultáneas que puede admitir con cada tipo de instancia disponible en cada región. Puede solicitar un aumento de estas cuotas en la página Service Quotas de la AWS consola.

La siguiente tabla muestra los límites de las cuotas de servicio predeterminados.

Cuotas predeterminadas dentro y Región de AWS por cuenta	Valor
Portales web	3
Número máximo de sesiones simultáneas: estándar.regular	25
Número máximo de sesiones simultáneas: estándar.large	10
Número máximo de sesiones simultáneas: standard.xlarge	5

> **Important**
>
> Las cuotas de servicio se aplican de una en una Región de AWS . Debe solicitar aumentos de la cuota de servicio en cada uno de los Región de AWS casos en los que necesite más recursos. Para obtener más información, puntos de conexión y cuotas de Amazon WorkSpaces Secure Browser.

Para solicitar un aumento de la cuota de servicio

1. Abra el panel de AWS Support.
2. Seleccione Aumento del límite de servicio.

   > **Important**
   >
   > WorkSpaces Las cuotas del servicio de Secure Browser afectan a una región a la vez. Debe solicitar el aumento de la cuota de servicio para cada región de AWS en la que necesite más recursos. Para obtener más información, consulte Puntos de enlace de los servicios de AWS.

3. En Descripción del caso de uso, introduzca la siguiente información:

- Si solicita un aumento del número de portales web, especifique este tipo de recurso e incluya su ID de cuenta de AWS, la región en la que desea que se aumente y el nuevo valor límite.
- Si solicita un aumento del número máximo de sesiones simultáneas, especifique este tipo de recurso e incluya su ID de cuenta de AWS, la región en la que desea el aumento, el ARN del portal web y el nuevo valor límite.

4. (Opcional) Para solicitar varios aumentos de cuota de servicio al mismo tiempo, realice una solicitud de aumento de cuota en la sección Solicitudes y, a continuación, seleccione Añadir otra solicitud.

Solicite un aumento del portal

Un portal es el recurso fundamental del servicio. Cada portal es una asociación entre su proveedor de identidad SAML 2.0 y su conexión de red a Internet y cualquier contenido web privado. Cada portal puede tener una política de navegador y una configuración de usuario independientes, por lo que los administradores suelen crear varios portales en la misma región para abordar distintos casos de uso. Por ejemplo, puede proporcionar al Grupo A acceso a un sitio web específico con políticas restrictivas (por ejemplo, deshabilitar el portapapeles y la transferencia de archivos) y, al Grupo B, acceso a Internet en general sin filtrar las URL. Puede crear un portal en cualquier sitio compatible Región de AWS. Para ver la disponibilidad actual de los servicios, consulte Servicios de AWS por región.

Para solicitar un aumento de la cuota de servicio

1. Abre la página Service Quotas en la región que desees.
2. Elija el número de portales web.
3. Elija Solicitar un aumento a nivel de cuenta.
4. En Aumentar el valor de la cuota, introduce el importe total que deseas que alcance la cuota.

Solicita un aumento máximo de sesiones simultáneas

La cuota máxima de sesiones simultáneas es la cantidad máxima de usuarios que se pueden conectar al mismo tiempo a un portal. Si el límite de cuota de servicio para el número máximo de sesiones simultáneas no está establecido de forma adecuada, es posible que los usuarios descubran que una sesión no está disponible al iniciar sesión. Además de aumentar esta cuota de servicio, los

clientes también deben asegurarse de que su VPC y sus subredes tengan suficiente espacio IP para admitir el máximo de sesiones simultáneas.

Para solicitar un aumento máximo de sesiones simultáneas

1. Abre la página Service Quotas en la región que desees.
2. Elija el número máximo de sesiones simultáneas por portal para el tipo de instancia que desee aumentar.
3. Elija Solicitar un aumento a nivel de cuenta.
4. En Aumentar el valor de la cuota, introduce el importe total que deseas que alcance la cuota.

> **Note**
>
> Para aumentos importantes o urgentes, vaya a la página de historial de Service Quotas, seleccione el enlace en la columna de estado de su solicitud, enlace a su caso de soporte y añada una respuesta con detalles sobre su caso de uso y/o la urgencia. Esta información ayuda al equipo de servicio a priorizar las solicitudes y a garantizar que se asigne suficiente capacidad a tu cuenta.

Ejemplo de límite

Por ejemplo, supongamos que un administrador está configurando dos portales web en EE. UU. Este (Virginia del Norte) para un total de 125 usuarios. Antes de crear el portal web, el administrador identifica el primer portal web (Portal A) que admitirá 100 usuarios. Al probar el flujo de trabajo para estos usuarios, el administrador determina que necesitarán el tipo de instancia XL para admitir la transmisión de audio y vídeo durante la sesión. El segundo portal web (Portal B) debe estar disponible para un máximo de 25 usuarios para permitir el acceso a una única página web estática alojada en la VPC del cliente. Al probar este caso de uso, el administrador determina que el tipo de instancia estándar puede admitir este caso de uso.

En el caso del portal A, el administrador debe enviar una solicitud de aumento de la cuota de servicio para aumentar el límite de las instancias XL de las instancias predeterminadas en la región (es decir, 5) a 100. Una vez completada, el administrador puede asignar la capacidad editando el portal web. En el caso del portal B, el administrador puede avanzar sin solicitar un aumento de cuota (es decir, dado que la región tiene una cuota predeterminada de 25 para el tipo de instancia estándar).

Administre las cuotas de servicio

Para ver las cuotas de servicio asignadas a su cuenta para cada región en cualquier momento, consulte la página Service Quotas.

Otras cuotas de servicio

Puede ver y solicitar aumentos para otras cuotas que figuran en la página Service Quotas. En la práctica, a la mayoría de los clientes les resultará innecesario solicitar aumentos para estos límites. A grandes rasgos, estas cuotas se agrupan en dos tipos: numéricas y tarifarias.

En el caso de las cuotas numéricas, al enviar un aumento de la cuota de servicio para Número de portales web, recibirá automáticamente un aumento en la cantidad de recursos secundarios necesarios para crear un portal único. Esto se reflejará en la página Service Quotas. Por ejemplo, si solicita que se aumente el número de portales de 3 a 5, recibirá automáticamente un aumento de la cuota de servicio de 3 a 5 en la configuración del navegador y del usuario. Tiene la opción de reutilizar o crear nuevos subrecursos según lo desee.

En raras ocasiones, los clientes pueden encontrar un caso práctico para aumentar el número o la tasa de otras cuotas de recursos. Por ejemplo, es posible que los administradores deseen aumentar el número de ajustes del navegador para probar configuraciones de portal adicionales. Estas solicitudes de cuotas de servicio se revisarán y tramitarán de case-by-case forma periódica.

En el caso de las cuotas de tarifas, no debería ser necesario ajustar los límites de tarifas expuestos en Service Quotas, independientemente del límite del portal de la cuenta.

Controle el intervalo para volver a autenticar un token de IdP de SAML

Cuando un usuario visita un portal de WorkSpaces Secure Browser, puede iniciar sesión para iniciar una sesión de streaming. Todas las sesiones empiezan en la página de inicio, a menos que hayan iniciado sesión hace menos de 5 minutos. El portal comprueba los tokens del proveedor de identidades (IdP) para determinar si se deben solicitar las credenciales al usuario al comenzar una sesión. Un usuario sin un token de IdP válido debe introducir un nombre de usuario, una contraseña y (opcionalmente) una autenticación multifactor (MFA) para comenzar una sesión de streaming. Si un usuario ya generó un token de IdP de SAML al iniciar sesión en su IdP o en una aplicación protegida por el mismo IdP, no se le pedirán las credenciales de inicio de sesión.

Si un usuario tiene un token de IDP de SAML válido, puede WorkSpaces acceder a Secure Browser. Puede controlar el intervalo para volver a autenticar un token de IdP de SAML

Para controlar el intervalo para volver a autenticar un token de IdP de SAML

1. Establezca la duración del tiempo de espera del IdP con su proveedor de IdP de SAML. Recomendamos configurar la duración del tiempo de espera del IdP en el menor tiempo necesario para que el usuario realice sus tareas.

   - Para obtener más información sobre Okta, consulte Enforce a limited session lifetime for all policies.
   - Para obtener más información sobre Azure AD, consulte Configuración de los controles de sesión de autenticación.
   - Para obtener más información acerca de Ping, consulte Sessions.
   - Para obtener más información AWS IAM Identity Center, consulte Establecer la duración de la sesión.
2. Establezca los valores de inactividad y tiempo de espera de inactividad del portal WorkSpaces Secure Browser. Estos valores controlan el tiempo transcurrido entre la última interacción de un usuario y el momento en que finaliza una sesión de WorkSpaces Secure Browser debido a la inactividad. Cuando finaliza una sesión, el usuario pierde el estado de la sesión (incluidas las pestañas abiertas, el contenido web no guardado y el historial) y vuelve a un estado nuevo al comienzo de la siguiente sesión. Para obtener más información, consulte el paso 5 de the section called “Paso 1: cree un portal web”.

   > **Note**
   >
   > Si se agota el tiempo de espera de la sesión de un usuario, pero el usuario aún tiene un token de IDP de SAML válido, no tendrá que introducir su nombre de usuario y contraseña para iniciar una WorkSpaces nueva sesión de Secure Browser. Para controlar cómo se vuelven a autenticar los tokens, utilice las guías del paso anterior.

Configuración del registro de acceso de usuario

Puede configurar el registro de acceso de usuario para registrar los siguientes eventos de los usuarios:

- Inicio de sesión: marca el inicio de una sesión de WorkSpaces Secure Browser.
- Fin de sesión: marca el final de una sesión de WorkSpaces Secure Browser.
- Navegación por URL: registra la URL que carga un usuario.

> **Note**
>
> Los registros de navegación por URL se registran desde el historial del navegador. Las URL no registradas en el historial del navegador (ya sea que se visiten en el modo Incógnito o se eliminen del historial del navegador) no se registran en los registros. Los clientes deben decidir si desean desactivar el modo Incógnito o eliminar el historial con la política de su navegador.

Además, se incluye la siguiente información para cada evento:

- Hora del evento
- Nombre de usuario
- ARN de portal web

Los clientes son responsables de comprender los posibles problemas legales que surjan con el uso de WorkSpaces Secure Browser y de asegurarse de que su uso de WorkSpaces Secure Browser cumpla con todas las leyes y reglamentos aplicables. Estas incluyen las leyes que regulan la capacidad del empleador para supervisar el uso de WorkSpaces Secure Browser por parte de un empleado, incluidas las actividades que se realizan dentro de la aplicación.

La activación de los registros de acceso de los usuarios en su portal WorkSpaces Secure Browser podría generar cargos por parte de Amazon Kinesis Data Streams. Para obtener más información sobre los precios, consulte Precios de Amazon Kinesis Data Streams.

Para activar el registro de acceso de usuarios en la consola de WorkSpaces Secure Browser, en Registro de acceso de usuarios, seleccione el Kinesis Stream ID que desee usar para recibir datos. Los datos registrados se enviarán directamente a ese flujo.

Para obtener más información acerca de cómo crear un flujo de datos de Amazon Kinesis, consulte ¿Qué es Amazon Kinesis Data Streams?.

> **Note**
>
> Para recibir registros de WorkSpaces Secure Browser, debe tener un Amazon Kinesis Data Stream que comience por "amazon-workspaces-web-*». La transmisión de datos de Amazon Kinesis debe tener desactivado el cifrado del lado del servidor o debe usarse Claves administradas por AWS para el cifrado del lado del servidor.
> Para obtener más información sobre cómo configurar el cifrado del servidor en Amazon Kinesis, consulte How Do I Get Started with Server-Side Encryption?

Registros de ejemplo

A continuación, se muestra un ejemplo de cada evento disponible, que incluye la validación,, y. StartSessionVisitPageEndSession

Los siguientes campos se incluyen siempre para cada evento:

- timestamp se incluye como tiempo en milisegundos.
- eventType se incluye como cadena.
- details se incluye como otro objeto json.
- portalArn y userName se incluyen en todos los eventos excepto en 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"
}
```

Configuración o edición de la política de su navegador

Con WorkSpaces Secure Browser, puedes configurar una política de navegación personalizada utilizando las políticas de Chrome disponibles en la última versión estable. Hay más de 300 políticas que puede aplicar a un portal web. Para obtener más información, consulte the section called "Definición de una política de navegador personalizada (ejemplo)" y Lista de políticas de Chrome Enterprise.

Si utiliza la vista de consola para crear un portal web, puede aplicar las siguientes políticas:

- `StartURL`
- Marcadores y carpetas de marcadores
- Activación y desactivación de la navegación privada
- Eliminación del historial
- Filtrado de URL con `AllowURL` y `BlockURL`

Para obtener más información acerca del uso de las políticas de visualización de la consola, consulte Cómo empezar a usar WorkSpaces Secure Browser.

WorkSpaces Secure Browser aplica una configuración básica de políticas de navegación a todos los portales, junto con las políticas que especifique. Puede editar algunas de estas políticas con su archivo JSON personalizado. Para obtener más información, consulte the section called “Edición de la política básica del navegador”.

Temas

- Definición de una política de navegador personalizada (ejemplo)
- Edición de la política básica del navegador

Definición de una política de navegador personalizada (ejemplo)

Para configurar una política de Chrome compatible para Linux, cargue un archivo JSON. Para obtener más información sobre las políticas de Chrome, consulte Lista de políticas de Chrome Enterprise y seleccione la plataforma Linux. A continuación, busque y revise las políticas de la versión estable más reciente.

En el ejemplo siguiente, cree un portal web con los siguientes controles de políticas:

- Configure marcadores
- Configure las páginas de inicio predeterminadas
- Impida que el usuario instale otras extensiones
- Impida que el usuario borre el historial
- Impida que el usuario acceda al modo Incógnito
- Preinstale la extensión del complemento Okta para todas las sesiones.

Temas

- Paso 1: creación de un portal web
- Paso 2: recopilación de políticas
- Paso 3: cree un archivo de política JSON personalizado
- Paso 4: añada las políticas a la plantilla
- Paso 5: cargue el archivo JSON de su política en su portal web

Paso 1: creación de un portal web

Para cargar el archivo JSON de la política de Chrome, debes crear un portal de WorkSpaces Secure Browser. Para obtener más información, consulte the section called “Paso 1: cree un portal web”.

Paso 2: recopilación de políticas

Busque y localice las políticas que desee en la Política de Chrome. A continuación, utilice las políticas para crear un archivo JSON en el siguiente paso.

1. Vaya a la Lista de políticas de Chrome Enterprise.
2. Elija la plataforma Linux y, a continuación, elija la versión más reciente de Chrome.
3. Busque las políticas que quiera establecer. Para este ejemplo, busque extensiones para encontrar políticas para administrarlas. Cada política incluye una descripción, un nombre de preferencia de Linux y un valor de ejemplo.
4. Según los resultados de la búsqueda, hay tres políticas que cumplen los requisitos empresariales si se utilizan juntas:
   - ExtensionSettings— Instala una extensión al iniciar el navegador.
   - ExtensionInstallBlocklist— Impide la instalación de extensiones específicas.
   - ExtensionInstallAllowlist— Permite instalar determinadas extensiones.
5. Las políticas adicionales satisfacen los requisitos restantes.
   - ManagedBookmarks— Añade marcadores a las páginas web.
   - RestoreOnStartupURL: configura qué páginas web se abren cada vez que se abre una nueva ventana del navegador.
   - AllowDeletingBrowserHistory— Configura si los usuarios pueden eliminar su historial de navegación.
   - IncognitoModeAvailability— Configura si los usuarios pueden acceder al modo incógnito.

Paso 3: cree un archivo de política JSON personalizado

Cree un archivo JSON con un editor de texto, una plantilla y las políticas que encontró en el paso anterior.

1. Abra un editor de texto.
2. Copie y pegue la siguiente plantilla en un 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
        }
    }
}
```

Paso 4: añada las políticas a la plantilla

Añada sus políticas personalizadas a la plantilla para cada requisito empresarial.

1. Configure las URL de los marcadores.
   a. En la clave `value`, añada pares de claves `url` y `name` para cada marcador que quiera añadir.
   b. Establezca `bookmark-url-1` en `https://www.amazon.com`.
   c. Establezca `bookmark-url-2` en `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 las direcciones URL de inicio. Esta política permite a los administradores configurar las páginas web que se muestran cuando un usuario abre una nueva ventana del navegador.

   a. Configure el `RestoreOnStartup` en 4. Esto configura la acción `RestoreOnStartup` para abrir una lista de direcciones URL. También puede utilizar otras acciones en las URL de inicio. Para obtener más información, consulte Lista de políticas de Chrome Enterprise.

   b. Establezca `RestoreOnStartupURLs` en https://www.aboutamazon.com/news.

```
    "RestoreOnStartup":
        {
            "value": 4
        },
    "RestoreOnStartupURLs":
        {
            "value":
            [
                "https://www.aboutamazon.com/news"
            ]
        },
```

3. Para evitar que el usuario borre su historial de navegación, establezca `AllowDeletingBrowserHistory` en `false`.

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

4. Para desactivar el acceso al modo Incógnito para sus usuarios, establezca `IncognitoModeAvailability` en 1.

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

5. Configure y aplique el complemento Okta con las siguientes políticas:

   - `ExtensionSettings`: instala una extensión al iniciar el navegador. El valor de la extensión está disponible en la página de ayuda del complemento Okta.
   - `ExtensionInstallBlocklist`: impide la instalación de extensiones específicas. Utilice un valor * para impedir todas las extensiones de forma predeterminada. Los administradores pueden controlar qué extensiones se permiten en `ExtensionInstallAllowlist`.
   - `ExtensionInstallAllowlist` le permite instalar determinadas extensiones. Como `ExtensionInstallBlocklist` está configurado en *, añada aquí el valor del complemento Okta para permitirlo.

   A continuación, se muestra un ejemplo de política para activar el complemento 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"
    }
}
```

Paso 5: cargue el archivo JSON de su política en su portal web

1. Abra la consola de WorkSpaces Secure Browser en. https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/
2. Elija WorkSpaces Secure Browser y, a continuación, elija portales web.
3. Elija su portal web y, a continuación, elija Editar.
4. Seleccione Configuración de políticas y, a continuación, Carga de archivos JSON.
5. Seleccione Elegir archivo. Navegue hasta el archivo JSON, selecciónelo y cárguelo.
6. Seleccione Guardar.

Edición de la política básica del navegador

Para ofrecer el servicio, WorkSpaces Secure Browser aplica una política de navegación básica a todos los portales. Esta política básica se aplica adicionalmente a las que especifique en la vista de la consola o en el archivo JSON que cargue. Esta es la lista de políticas que aplica el servicio en 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",
            ]
        }
    }
}
```

Los clientes no pueden realizar cambios en las siguientes políticas:

- `DefaultDownloadDirectory`: esta política no se puede editar. El servicio sobrescribe cualquier cambio en esta política.
- `DownloadDirectory`: esta política no se puede editar. El servicio sobrescribe cualquier cambio en esta política.

Los clientes pueden actualizar las siguientes políticas para su portal web:

- `DownloadRestrictions`: la configuración predeterminada es `1` para impedir que la navegación segura de Chrome identifique las descargas como maliciosas. Para obtener más información, consulte Prevent users from downloading harmful files. Puede cambiar el valor de `0` a `4`.
- Las políticas `URLAllowlist` y `URLBlocklist` se pueden ampliar mediante la característica de filtrado de URL de la vista de consola o mediante la carga de archivos JSON. Sin embargo, las URL de referencia no se pueden sobrescribir. Estas políticas no son visibles en un archivo JSON descargado de su portal web. Sin embargo, si visita “chrome://policy” durante una sesión, el navegador remoto mostrará las políticas aplicadas.

Configure el editor de métodos de entrada (IME)

Un editor de métodos de entrada (IME) es una utilidad que ofrece opciones al usuario final para introducir texto en idiomas que utilizan un diseño de teclado distinto del teclado QWERTY. Los IME ayudan a los usuarios a escribir texto en idiomas con conjuntos de caracteres más grandes y complejos, como el japonés, el chino y el coreano. WorkSpaces Las sesiones de Secure Browser incluyen la compatibilidad con IME de forma predeterminada. Los usuarios pueden seleccionar idiomas alternativos en la barra de herramientas del IME en la sesión o mediante atajos de teclado.

El IME de WorkSpaces Secure Browser admite actualmente los siguientes idiomas:

- Inglés
- Chino simplificado (Pinyin)

- Chino tradicional (Bopomofo)
- Japonés
- Coreano

Para seleccionar un idioma en la barra de herramientas del IME, haga lo siguiente:

1. Seleccione el menú desplegable del selector de idioma ubicado en el lado derecho de la barra negra del panel superior. De forma predeterminada, el selector mostrará en, que representa el inglés.
2. En el menú desplegable, elija el idioma deseado.
3. En el submenú que aparece después de elegir un idioma, seleccione los detalles adicionales del idioma.

Para seleccionar un idioma mediante atajos del teclado, utilice lo siguiente:

- Todos los IME
  - Para avanzar en el IME (o moverlo a la distribución de teclado correcta), pulse Shift+Control+Left Alt.
- Japonés
  - Para elegir Hiragana, pulse F6.
  - Para elegir Katakana, pulse F7.
  - Para elegir Latín, pulse F10.
  - Para elegir Latín amplio, pulse F9.
  - Para seleccionar Entrada directa, pulse ALT +, ALT+@, Zenkaku Hankaku.
- Coreano
  - Para seleccionar Hangul, pulse Shift+Space.
  - Para seleccionar Hanja, pulse F9.

Para eliminar la barra de herramientas y el menú del IME, o para desactivar el teclado en pantalla de sus sesiones de WorkSpaces Secure Browser, póngase en contacto con AWS Support.

Configure la localización durante la sesión

Cuando un usuario inicia una sesión, WorkSpaces Secure Browser detecta la configuración de idioma y zona horaria del navegador local del usuario y la aplica a la sesión. Esto afecta al idioma de visualización durante la sesión y ayuda a garantizar que la hora mostrada coincida con la hora actual de la ubicación del usuario.

La siguiente lista muestra los códigos de idioma que actualmente admite WorkSpaces Secure Browser. Si el navegador local del usuario está configurado para usar un código de idioma que no es compatible, el idioma predeterminado de la sesión es el inglés (en-US).

- Alemán
  - de: alemán
  - de-AT: alemán (Austria)
  - de-DE: alemán (Alemania)
  - de-CH: alemán (Suiza)
  - de-LI: alemán (Liechtenstein)
- Inglés
  - en: inglés
  - en-AU: inglés (Australia)
  - en-CA — inglés (Canadá)
  - en-IN: inglés (India)
  - en-NZ: inglés (Nueva Zelanda)
  - en-ZA: inglés (África austral)
  - en-GB: inglés (Reino Unido)
  - en-US: inglés (Estados Unidos)
- Español
  - es: español
  - es-AR: español (Argentina)
  - es-CL: español (Chile)
  - es-CO: español (Colombia)
  - es-CR: español (Costa Rica)
  - es-HN: español (Honduras)

- es-419: español (Latinoamérica)
- es-MX: español (México)
- es-PE: español (Perú)
- es-ES: español (España)
- es-US: español (Estados Unidos)
- es-UY: español (Uruguay)
- es-VE: español (Venezuela)

- Francés
  - fr: francés
  - fr-CA: francés (Canadá)
  - fr-FR: francés (Francia)
  - fr-CH: francés (Suiza)
- Indonesio
  - id: indonesio
  - id-ID: indonesio (Indonesia)
- Italiano
  - it: italiano
  - it-IT: italiano (Italia)
  - it-CH: italiano (Suiza)
- Japonés
  - ja: japonés
  - ja-JP: japonés (Japón)
- Coreano
  - ko: coreano
  - ko-KR: coreano (Corea)
- Portugués
  - pt: portugués
  - pt-BR: portugués (Brasil)
  - pt-PT: portugués (Portugal)
- Chino

- zh: chino
- zh-CN: chino (China)
- zh-HK: chino (Hong Kong)
- zh-TW: chino (Taiwán)

El idioma de la sesión se determina en el siguiente orden de prioridad:

1. La ForcedLanguagespolítica de la configuración del navegador del portal web. Para obtener más información, consulte ForcedLanguages.
2. La configuración de idioma del navegador local del usuario final.
3. El valor predeterminado es Inglés (en-US).

La zona horaria viene determinada por la configuración de zona horaria local especificada en el navegador del usuario final. Si la configuración de zona horaria no es válida, se usa UTC.

Los siguientes componentes de WorkSpaces Secure Browser admiten la localización:

- WorkSpaces Página de inicio de sesión de Secure Browser
- WorkSpaces Mensajes de estado del portal de Secure Browser (incluidos los mensajes de carga y los errores)
- Navegador Chrome
- Menú Contextual del sistema y ventana Guardar como

Para establecer la configuración del navegador local de un usuario, realice una de las siguientes operaciones:

- En Chrome, seleccione Ajustes, Idiomas y, a continuación, ordene los idiomas según sus preferencias.
- En Firefox, seleccione Ajustes, General e Idioma, y seleccione el idioma en el menú desplegable.
- En Edge, seleccione Ajustes, Idiomas y, a continuación, ordene los idiomas según sus preferencias.

Configure los controles de acceso de IP (opcional)

WorkSpaces Secure Browser le permite controlar las direcciones IP desde las que se puede acceder a su portal web. Al usar la configuración de acceso de IP, puede definir y administrar grupos de direcciones IP de confianza y solo permitir que los usuarios accedan a su portal cuando están conectados a una red de confianza.

De forma predeterminada, WorkSpaces Secure Browser permite a los usuarios acceder a su portal web desde cualquier lugar. Un grupo de control de acceso IP actúa como un firewall virtual que filtra la dirección IP que un usuario puede usar para conectarse al portal web. Cuando está asociado a su portal web, la configuración de acceso IP detectará la IP del usuario antes de la autenticación para determinar si es apto para conectarse. Una vez conectado, WorkSpaces Secure Browser monitorea continuamente la dirección IP del usuario para garantizar que permanezca conectado desde una red confiable. Si la IP de un usuario cambia, WorkSpaces Secure Browser detectará y finalizará la sesión.

Para especificar los rangos de direcciones del CIDR, añada reglas a su grupo de control de acceso de IP y, a continuación, asocie el grupo a su portal web. Puede asociar cada configuración de acceso de IP a uno o más portales web. Para especificar las direcciones IP públicas y los intervalos de direcciones IP para sus redes de confianza, añada reglas a sus grupos de control de acceso a direcciones IP. Si los usuarios tienen acceso a su portal web a través de una puerta de enlace NAT o VPN, debe crear reglas que permitan el tráfico desde las direcciones IP públicas para la puerta de enlace NAT o VPN.

> **Note**
>
> Los clientes son responsables de comprender los posibles problemas legales que surjan con el uso de WorkSpaces Secure Browser y deben asegurarse de que su uso de WorkSpaces Secure Browser cumpla con todas las leyes y reglamentos aplicables. Esto incluye las leyes que regulan la capacidad del empleador para supervisar el uso de WorkSpaces Secure Browser por parte de un empleado, incluidas las actividades que se realizan dentro de la aplicación.

Cree un grupo de control de acceso IP

Para crear un grupo de control de acceso IP, siga estos pasos.

1. Abra la consola de WorkSpaces Secure Browser enhttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. En el panel de navegación, seleccione Controles de acceso de IP.
3. Elija Crear grupo de control de acceso de IP.
4. En el cuadro de diálogo Crear grupo de control de acceso de IP, introduzca un nombre (obligatorio) y una descripción (opcional) para el grupo.
5. Introduzca la dirección IP o el rango de IP del CIDR que se asociará a la Fuente y una Descripción (opcional).
6. En Etiquetas, elija si desea etiquetar un par clave-valor para cada grupo de control de acceso IP.
7. Cuando haya acabado de añadir las reglas y etiquetas, elija Guardar.

Asocie una configuración de acceso IP a un portal web

Para asociar un grupo de control de acceso de IP a un portal web existente, siga estos pasos.

1. Abra la consola de WorkSpaces Secure Browser enhttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. En el panel de navegación, elija Portales web.
3. Seleccione el portal web y elija Editar.
4. En Grupo de control de acceso de IP, seleccione los grupos de control de acceso de IP para el portal web.
5. Seleccione Guardar.

Para asociar un grupo de control de acceso de IP al crear un nuevo portal web, siga estos pasos.

1. Complete los pasos 1 a 4 en the section called “Configuración de los ajustes del portal” para acceder a Control de acceso de IP (opcional).
2. Elija Crear controles de acceso de IP.
3. En el cuadro de diálogo Crear grupo de IP, introduzca un nombre (obligatorio) y una descripción (opcional) para el grupo.
4. Introduzca la dirección IP o el rango de IP del CIDR que se asociará a la Fuente y una Descripción (opcional).
5. En Etiquetas, elija si desea etiquetar un par clave-valor para cada grupo de control de acceso IP.

6. Cuando haya terminado de añadir reglas y etiquetas, elija Crear control de acceso de IP.
7. Su grupo de control de acceso de IP se asociará a este portal web cuando se inicie.

Edite un grupo de control de acceso de IP

Puede eliminar una regla de una configuración de acceso de IP en cualquier momento. Si elimina una regla que se utilizó para permitir la conexión a un portal web, todos los usuarios que tengan una sesión actual se desconectarán del portal web.

Para editar un grupo de control de acceso de IP, siga estos pasos.

1. Abra la consola de WorkSpaces Secure Browser enhttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. En el panel de navegación, seleccione Controles de acceso de IP.
3. Seleccione el grupo y elija Edit (Editar).
4. Edite la Fuente y la Descripción de las reglas existentes (opcional) o añada reglas adicionales.
5. En Etiquetas, elija si desea etiquetar un par clave-valor para cada grupo de control de acceso IP.
6. Cuando haya acabado de añadir las reglas y etiquetas, elija Guardar.
7. Si actualizó una configuración de acceso de IP existente, espere hasta 15 minutos para que la regla nueva o editada se aplique.

Elimine un grupo de control de acceso de IP

Puede eliminar una regla de un grupo de control de acceso a direcciones IP en cualquier momento. Si elimina una regla que se utilizó para permitir la conexión a un portal web, todos los usuarios que tengan una sesión actual se desconectarán del portal web.

Para eliminar un grupo de control de acceso de IP, siga estos pasos.

1. Abra la consola de WorkSpaces Secure Browser enhttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. En el panel de navegación, seleccione Grupo de control de acceso de IP.
3. Seleccione el grupo de ubicación y elija Eliminar.

Habilite la extensión de inicio de sesión único (opcional)

Puede habilitar una extensión para que sus usuarios finales tengan una mejor experiencia de inicio de sesión en el portal. Por ejemplo, si usa Okta como proveedor de identidades (IdP) SAML 2.0 de su portal y también lo usa como IdP para los sitios web que desea que los usuarios visiten durante una sesión, puede pasar la cookie de inicio de sesión de Okta a la sesión con la extensión. Posteriormente, cuando los usuarios visiten un sitio web que requiera la cookie del dominio de Okta, podrán acceder al sitio web sin tener que iniciar sesión durante la sesión.

La extensión es compatible con los navegadores Chrome y Firefox. La extensión permite la sincronización de cookies en los dominios permitidos desde el inicio de sesión del usuario. La extensión no requiere que el usuario inicie sesión y funciona en segundo plano para permitir la sincronización de las cookies sin que el usuario tenga que realizar ninguna acción después de la instalación. La extensión no almacena ningún dato.

Se solicita a los usuarios que instalen la extensión cuando inician sesión en un portal.

De forma predeterminada, las extensiones no están habilitadas en Chrome en las ventanas de incógnito o en las ventanas de navegación privada de Firefox. Los usuarios pueden activarlas manualmente. Para obtener más información sobre Chrome, consulta Extensiones en modo incógnito. Para obtener más información sobre Firefox, consulta Extensiones en la navegación privada.

Puede actualizar la configuración de usuario existente de un portal o al crear un portal web por primera vez. En primer lugar, determine qué dominios necesita para su IdP y sitios web de SAML. Puede añadir hasta 10 dominios.

Eres responsable de probar e identificar el dominio apropiado para que se sincronicen las cookies. Es posible que se requieran cambios en el nivel de autenticación del IdP o del sitio web para garantizar que el inicio de sesión único funcione según lo esperado.

Para ver qué dominios usar con el IdP más común, consulta la siguiente tabla:

IdP y dominios

IdP	Dominio
Okta	okta.com
Introduzca un ID	microsoftonline.com

IdP	Dominio
AWS Identity Center	awsapps.com
Un inicio de sesión	onelogin.com
Duo	duosecurity.com

A continuación, visite su portal web en la consola. A continuación, permita la extensión y añada las cookies de los dominios que deben sincronizarse. Siga los pasos que se indican a continuación para crear un nuevo portal con la extensión permitida o para actualizar un portal existente.

Para permitir la extensión al crear un nuevo portal web, siga estos pasos:

1. Siga los pasos que se indican en the section called “Paso 1: cree un portal web” hasta llegar a the section called “Configuración de los ajustes de usuario”.
2. En el paso 1 de the section called “Configuración de los ajustes de usuario”, en Permisos de usuario, seleccione Permitido para habilitar la extensión para tu portal web.
3. Introduzca el dominio para la sincronización de las cookies y seleccione Añadir nuevo dominio.
4. Complete los pasos de the section called “Configuración de los ajustes de usuario” y las secciones restantes de the section called “Paso 1: cree un portal web” para crear su portal web.

Para añadir la extensión a un portal web existente, siga estos pasos:

1. Abra la consola de WorkSpaces Secure Browser en https://console.aws.amazon.com/workspaces-web/home.
2. Seleccione el portal web que desea editar.
3. Elija Configuración de usuario, Permisos de usuario y Permitido para habilitar la extensión para su portal web.
4. Introduzca el dominio para la sincronización de las cookies y seleccione Añadir nuevo dominio.
5. Guarde los cambios del portal. Los portales solicitarán a los usuarios que instalen la extensión en 15 minutos.

Para editar dominios o eliminar la extensión, siga estos pasos:

1. Abra la consola de WorkSpaces Secure Browser en https://console.aws.amazon.com/workspaces-web/home.
2. Seleccione el portal web que desea editar.
3. Seleccione Configuración de usuario, Permisos de usuario y No permitido para eliminar la extensión de su portal web.
4. Elimine o edite dominios individuales.
5. Una vez eliminadas, las sesiones ya no sincronizarán las cookies, incluso si el usuario tiene la extensión WorkSpaces Secure Browser instalada en su navegador.

Para obtener más información sobre la experiencia del usuario con la extensión, consulte the section called “Extensión de inicio de sesión único”.

Configure el filtrado de URL

Puedes usar la Política de Chrome para filtrar las URL a las que pueden acceder los usuarios desde su navegador remoto. La política de Chrome proporciona dos mecanismos para filtrar las URL: URLAllowList y URLBlockList. Puedes usar la interfaz de consola de WorkSpaces Secure Browser para configurar el filtrado de URL como una configuración del portal, o puedes añadirlo como parte de tu declaración JSON personalizada (ya sea en el editor integrado o al subir un archivo JSON).

Para configurar el filtrado de URL mediante la consola

1. Abra la consola de WorkSpaces Secure Browser enhttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. Elija WorkSpaces Secure Browser, portales web, elija su portal web y, a continuación, elija Ver detalles.
3. Para el filtrado de URL, elija una de las siguientes opciones:

   - Permitir el acceso a todas las URL: de forma predeterminada, un portal web permite el acceso a todas las URL. Puede añadir sitios web específicos a la lista BlockUrl para evitar que los usuarios visiten esos sitios durante una sesión. Por ejemplo, añadir www.anycorp.com a la lista BlockUrl impedirá que el usuario navegue a www.anycorp.com durante la sesión.
   - Bloquear el acceso a todas las URL: de forma predeterminada, el portal web bloquea el acceso a todas las URL. Puede añadir sitios web específicos a la lista de direcciones URL permitidas para crear una lista de sitios web que los usuarios pueden visitar y bloquear el

tráfico a cualquier otro sitio web. Considere la posibilidad de añadir cada URL como marcador para que los usuarios puedan acceder a ellas con un solo clic durante la sesión.

- Configuración avanzada: elija esta opción para crear listas AllowURL y BlockURL en paralelo. La lista de URL permitidas tiene prioridad sobre la lista de URL bloqueadas. Esta opción permite filtrar las URL por ruta. Por ejemplo, puede añadir www.anycorp.com a la lista de bloqueados y, a continuación, añadir www.anycorp.com/hr a la lista de permitidos. Esto permite a los usuarios visitar www.anycorp.com/hr, pero no podrán acceder a otras rutas URL, como www.anycorp.com/finance.

Para obtener más información sobre cómo bloquear y permitir direcciones URL, consulta Permitir o bloquear el acceso a sitios web. Añade las URL a estas listas siguiendo el formato de filtro de listas bloqueadas de Chrome para obtener los mejores resultados. Para obtener más información, consulta el formato de filtro de listas de URL bloqueadas.

Para configurar el filtrado de URL mediante el editor JSON o la carga de archivos

1. En el módulo de configuración de políticas, selecciona el editor JSON y omite el módulo de interfaz de usuario de la consola para ver el editor o la vista de carga de archivos.

   - El editor permite a los clientes crear declaraciones de políticas personalizadas en línea en la consola. El editor resalta los errores en la declaración JSON durante la creación de la política.
   - La carga de archivos permite a los clientes añadir un archivo JSON creado fuera de la consola (por ejemplo, exportado desde un navegador Chrome existente).
2. Consulta los detalles de la política de Chrome de URLAllowList y URLBlockList para formatear correctamente una lista de URL permitidas o denegadas para tu portal web. Para obtener más información, consulta URLAllowList y URLBlocklist.

Permitir enlaces profundos (opcional)

Cuando un usuario inicia sesión en WorkSpaces Secure Browser, inicia la sesión en una página de inicio establecida por el administrador. También puede permitir que los portales reciban enlaces profundos que conecten a los usuarios con un sitio web específico durante una sesión. Cuando se selecciona un enlace profundo, el portal muestra la URL especificada en el enlace profundo. El enlace se muestra junto a las páginas de inicio configuradas para el inicio de la sesión o solo si la sesión ya está en curso. Esta función permite a los administradores crear experiencias de usuario más dinámicas con WorkSpaces Secure Browser. Para permitir el uso de enlaces profundos,

seleccione Permitido al crear la configuración de usuario. Para obtener más información, consulte the section called “Configuración de los ajustes de usuario”.

Los enlaces profundos abren páginas en una sesión de WorkSpaces Secure Browser. Si una sesión ya está en ejecución, se abrirá el enlace profundo en una pestaña nueva. Si una sesión aún no está en marcha, se abrirá la URL del enlace directo en una pestaña nueva y la página de inicio predeterminada del portal en una pestaña independiente. Si un enlace profundo contiene más de una URL, mostrará la URL del enlace profundo que aparezca en primer lugar y cada URL posterior (incluida la página de inicio predeterminada) se abrirá en pestañas distintas.

Los enlaces profundos deben cumplir los siguientes requisitos:

- El portal debe tener los permisos de enlace profundo establecidos en Permitidos. Para obtener más información, consulte the section called “Configuración de los ajustes de usuario”.
- El sitio al que deseas establecer un enlace profundo debe estar codificado en una URL. Por ejemplo, para vincular a un usuario a «https://www.example.com/?query=true», actualiza el enlace a https://%3A%2F%2Fwww.example.com%2F%3Fquery%3DTrue.
- Añada la URL a una URL de portal incluida en la lista de permitidos con el siguiente formato, donde UUID es el identificador del portal:

  <uuid>https://.workspaces-web.com/? deeplinks=https%3A%2F%2Fwww.example.com%2F%3Fquery%3DTrue
- Un enlace profundo puede contener hasta 10 direcciones URL, delimitadas por comas. Por ejemplo:

  <uuid>https://.workspaces-web.com/? deeplinks=https%3A%2F%2Fwww.example.com%2F%3Fquery%3DTrue, https://3A%2F%2Fwww.example.com%2F%3Fquery%3Dtrue2, https://3A%2F%2Fwww.example.com%2F%3Fquery%3Dtrue3, https://. %3A%2F%2Fwww.example.com%2F%3Fquery%3Dtrue4

Cualquier usuario con el que compartas este enlace del portal puede manipular el valor del enlace profundo para visitar un sitio web, si se puede acceder a ese dominio desde el portal y no está en la lista de URL bloqueadas. Para crear una lista de permitidos o bloqueados restrictiva que impida que los usuarios visiten dominios no deseados a través de su portal, utilice el filtrado de URL. La lista de permitidos y la lista de bloqueados de un portal se pueden editar con el filtrado de URL en la configuración del navegador del portal. Para obtener más información, consulte the section called “Configure el filtrado de URL” Permitir o bloquear el acceso a sitios web.

Seguridad en Amazon WorkSpaces Secure Browser

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de una arquitectura de centro de datos y red diseñada para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre usted AWS y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la AWS nube. AWS también le proporciona servicios que puede utilizar de forma segura. Los auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los AWS programas de de . Para obtener más información sobre los programas de conformidad que se aplican a Amazon WorkSpaces Secure Browser, consulte AWS Services in .
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. También es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables relacionados con sus datos.

Esta documentación le ayuda a entender cómo aplicar el modelo de responsabilidad compartida al utilizar Amazon WorkSpaces Secure Browser. Le muestra cómo configurar Amazon WorkSpaces Secure Browser para cumplir sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros AWS servicios que le ayudan a supervisar y proteger los recursos de Amazon WorkSpaces Secure Browser.

Contenido

Protección de datos en Amazon WorkSpaces Secure Browser

El modelo de se aplica a protección de datos en Amazon WorkSpaces Secure Browser. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global en la que se ejecutan todos los Nube de AWS. Usted es responsable de mantener el control sobre el contenido alojado en esta infraestructura. Usted también es responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulte la sección Privacidad de datos FAQ. Para obtener información sobre la protección de datos en Europa, consulte el modelo de responsabilidad AWS compartida y la entrada del GDPR blog sobre AWS seguridad.

Con fines de protección de datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure los usuarios individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utilice la autenticación multifactorial (MFA) con cada cuenta.
- UseSSL/TLSpara comunicarse con AWS los recursos. Necesitamos TLS 1.2 y recomendamos TLS 1.3.
- Configure API y registre la actividad del usuario con AWS CloudTrail.
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utilice servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita entre FIPS 140 y 3 módulos criptográficos validados para acceder a AWS través de una interfaz de línea de comandos o unaAPI, utilice un FIPS terminal. Para obtener más información sobre los FIPS puntos finales disponibles, consulte la Norma federal de procesamiento de información () FIPS 140-3.

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como, por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabaja con WorkSpaces Secure Browser u otro dispositivo Servicios de AWS mediante la consola, API AWS CLI, o. AWS SDKs Cualquier dato que ingrese en etiquetas o campos de formato libre utilizados para nombres se puede emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, le

recomendamos encarecidamente que no incluya información sobre las credenciales URL para validar su solicitud a ese servidor.

Cifrado de datos

Amazon WorkSpaces Secure Browser recopila datos de personalización del portal, como la configuración del navegador, la configuración del usuario, la configuración de la red, la información del proveedor de identidad, los datos del almacén de confianza y los datos de los certificados del almacén de confianza. WorkSpaces Secure Browser también recopila datos sobre las políticas del navegador, las preferencias del usuario (para la configuración del navegador) y los registros de sesión. Los datos recopilados se almacenan en Amazon DynamoDB y Amazon S3. WorkSpaces Secure Browser se utiliza AWS Key Management Service para el cifrado.

Siga estas directrices para proteger su contenido:

- Implemente el acceso con privilegios mínimos y cree funciones específicas para utilizarlas en las acciones de WorkSpaces Secure Browser. Utilice IAM plantillas para crear un rol de acceso total o un rol de solo lectura. Para obtener más información, consulte AWS políticas administradas para WorkSpaces Secure Browser.
- Proteja los datos de principio a fin proporcionando una clave gestionada por el cliente, de modo que WorkSpaces Secure Browser pueda cifrar los datos en reposo con las claves que usted suministre.
- Tenga cuidado al compartir los dominios del portal y las credenciales de usuario.
  - Los administradores deben iniciar sesión en la WorkSpaces consola de Amazon y los usuarios deben iniciar sesión en el portal WorkSpaces Secure Browser.
  - Cualquier usuario de Internet puede acceder al portal web, pero no puede iniciar sesión a menos que tenga credenciales de usuario válidas del portal.
- Los usuarios pueden finalizar sus sesiones de forma explícita seleccionando Finalizar sesión. De este modo, se descarta la instancia que aloja la sesión del navegador y se aísla el navegador.

WorkSpaces Secure Browser protege el contenido y los metadatos de forma predeterminada al cifrar todos los datos confidenciales con. AWS KMS Recopila la política del navegador y las preferencias de los usuarios para aplicar la política y la configuración durante las sesiones de WorkSpaces Secure Browser. Si se produce un error al aplicar la configuración existente, el usuario no puede acceder a las nuevas sesiones y tampoco a los sitios internos ni a las aplicaciones SaaS de la empresa.

Cifrado en reposo

El cifrado en reposo está configurado de forma predeterminada. Los datos específicos del cliente utilizados en WorkSpaces Secure Browser se cifran mediante. AWS KMS WorkSpaces Secure Browser proporciona un cifrado en reposo para los recursos que cree. El servicio acepta una clave gestionada por el AWS KMS cliente al crear el recurso y, si no se proporciona, se utilizará una AWS clave propia para cifrar los recursos en reposo. El servicio cifra el documento de política del navegador que puede proporcionar para personalizar las sesiones del navegador, así como la configuración del proveedor de identidades, y los nombres para mostrar en sus portales. Esta información permanecerá cifrada mediante la clave gestionada por el cliente o la AWS clave propia mientras esté almacenada en nuestro servidor.

Puede decidir qué clave se utilizará al crear un recurso de WorkSpaces Secure Browser. Si los datos que forman parte de ese recurso están cifrados, WorkSpaces Secure Browser acepta el `customerManagedKeyArn` campo como parte del `create`API. La clave proporcionada debe ser una clave AWS KMS simétrica y el administrador que crea el recurso con esta clave debe tener permisos `kms:Decrypt`, `kms:GenerateDataKey` y `kms:CreateGrant`. Una vez creado un recurso con la clave, esta no se puede quitar ni cambiar. Si ha utilizado una clave administrada por el cliente, el administrador que accede al recurso debe disponer de permisos `kms:Decrypt` y `kms:GenerateDataKey`. Si aparece un error que indica que se ha denegado el acceso al utilizar la consola, asegúrese de que el usuario que utiliza la consola tenga estos permisos con la clave utilizada.

Puede solucionar problemas y auditar el uso de las claves comprobando el estado de las AWS KMS concesiones. Para obtener más información, consulte Administración de las concesiones. Durante la creación del portal, WorkSpaces Secure Browser crea una concesión para permitir que el servicio acceda a la clave de forma asíncrona. Para comprobar el estado del uso de las claves, compruebe la concesión, así como el contexto de cifrado que se proporciona cuando se utiliza la concesión. El contexto de cifrado siempre contiene una entrada con la clave `aws:workspaces-web:portal:id` y un valor equivalente al ID del portal. Para otros recursos, el contexto de cifrado siempre contendrá una entrada en el formato `aws:workspaces-web:`*`RESOURCE_TYPE`*`:id` y el ID de recurso correspondiente.

Cifrado en tránsito

WorkSpaces Secure Browser cifra los datos en tránsito a través de la versión 1.2. HTTPS TLS Puede enviar una solicitud a WorkSpaces mediante la consola o mediante API llamadas directas. Los datos de la solicitud que se transfieren se cifran enviándolos todos a través de una TLS conexión HTTPS

o. Los datos de la solicitud se pueden transferir desde la AWS consola o AWS SDK a WorkSpaces Secure Browser. AWS Command Line Interface

El cifrado en tránsito se configura de forma predeterminada y las conexiones seguras (HTTPS,TLS) se configuran de forma predeterminada.

Administración de claves

Puede proporcionar su propia AWS KMS clave gestionada por el cliente para cifrar la información de sus clientes. Si no proporciona una, WorkSpaces Secure Browser utilizará una clave AWS propia. Puede configurar su clave mediante AWS SDK.

Privacidad del tráfico entre redes

Para proteger las conexiones entre WorkSpaces Secure Browser y las aplicaciones locales, usa WorkSpaces Secure Browser para iniciar sesiones de navegador dentro de las suyas propiasVPC. La conexión a las aplicaciones locales se configura por su cuenta VPC y WorkSpaces Secure Browser no la controla.

Para proteger las conexiones entre cuentas, WorkSpaces Secure Browser utiliza una función vinculada al servicio para conectarse de forma segura a las cuentas de los clientes y ejecutar las operaciones en nombre del cliente. Para obtener más información, consulte Uso de funciones vinculadas a servicios para WorkSpaces Secure Browser.

Registro de acceso de usuario

Los administradores pueden registrar los eventos de la sesión de WorkSpaces Secure Browser, incluidos el inicio, la finalización y URL las visitas. Estos registros se cifran y se envían de forma segura a los clientes a través de un Amazon Kinesis Data Stream. La información de navegación del registro de acceso de los usuarios no se almacena en las sesiones sin configurar el registro ni está disponible en ellas. AWS URLlas visitas en modo incógnito o las eliminadas URLs del historial del navegador no se registran en el registro de acceso de los usuarios.

Identity and Access Management para Amazon WorkSpaces Secure Browser

AWS Identity and Access Management (IAM) es una Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a AWS los recursos. IAMlos administradores controlan quién puede autenticarse (iniciar sesión) y quién puede autorizarse (tener permisos) para usar los recursos de WorkSpaces Secure Browser. IAMes una Servicio de AWS que puede utilizar sin coste adicional.

Temas

Público

La forma de usar AWS Identity and Access Management (IAM) varía según el trabajo que realice en WorkSpaces Secure Browser.

Usuario del servicio: si utiliza el servicio WorkSpaces Secure Browser para realizar su trabajo, el administrador le proporcionará las credenciales y los permisos que necesita. A medida que vaya utilizando más funciones de WorkSpaces Secure Browser para realizar su trabajo, es posible que necesite permisos adicionales. Entender cómo se administra el acceso puede ayudarlo a solicitar los permisos correctos al administrador. Si no puede acceder a una función de WorkSpaces Secure Browser, consulteSolución de problemas de identidad y acceso a Amazon WorkSpaces Secure Browser.

Administrador de servicios: si está a cargo de los recursos de WorkSpaces Secure Browser en su empresa, probablemente tenga acceso total a WorkSpaces Secure Browser. Es su trabajo determinar a qué funciones y recursos de WorkSpaces Secure Browser deben acceder los usuarios del servicio. A continuación, debe enviar solicitudes a su IAM administrador para cambiar los permisos de los usuarios del servicio. Revise la información de esta página para comprender los conceptos básicos delAM. Para obtener más información sobre cómo su empresa puede utilizar IAM WorkSpaces Secure Browser, consulteCómo funciona Amazon WorkSpaces Secure Browser con IAM.

IAMadministrador: si es IAM administrador, puede que desee obtener más información sobre cómo puede redactar políticas para administrar el acceso a WorkSpaces Secure Browser. Para ver ejemplos de políticas basadas en la identidad de WorkSpaces Secure Browser que puede utilizarIAM, consulte. Ejemplos de políticas basadas en identidad para Amazon Secure Browser WorkSpaces

Autenticación con identidades

La autenticación es la forma de iniciar sesión AWS con sus credenciales de identidad. Debe estar autenticado (con quien haya iniciado sesión AWS) como IAM usuario o asumiendo un IAM rol. Usuario raíz de la cuenta de AWS

Puede iniciar sesión AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Identity Center Los usuarios (IAMIdentity Center), la autenticación de inicio de sesión único de su empresa y sus credenciales de Google o Facebook son ejemplos de identidades federadas. Al iniciar sesión como una identidad federada, el administrador configuró previamente la federación de identidades mediante roles. IAM Cuando accede AWS mediante la federación, asume indirectamente un rol.

Según el tipo de usuario que sea, puede iniciar sesión en el portal AWS Management Console o en el de AWS acceso. Para obtener más información sobre cómo iniciar sesión AWS, consulte Cómo iniciar sesión Cuenta de AWS en su Guía del AWS Sign-In usuario.

Si accede AWS mediante programación, AWS incluye un kit de desarrollo de software (SDK) y una interfaz de línea de comandos (CLI) para firmar criptográficamente sus solicitudes con sus credenciales. Si no utilizas AWS herramientas, debes firmar las solicitudes tú mismo. Para obtener más información sobre cómo usar el método recomendado para firmar las solicitudes usted mismo, consulte Firmar AWS API las solicitudes en la Guía del IAM usuario.

Independientemente del método de autenticación que use, es posible que deba proporcionar información de seguridad adicional. Por ejemplo, le AWS recomienda que utilice la autenticación multifactorial (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte Autenticación multifactorial en la Guía del AWS IAM Identity Center usuario y Uso de la autenticación multifactorial (MFA) AWS en la Guía del IAM usuario.

Cuenta de AWS usuario root

Al crear una Cuenta de AWS, comienza con una identidad de inicio de sesión que tiene acceso completo a todos Servicios de AWS los recursos de la cuenta. Esta identidad se denomina usuario Cuenta de AWS raíz y se accede a ella iniciando sesión con la dirección de correo electrónico y la

contraseña que utilizaste para crear la cuenta. Recomendamos encarecidamente que no utilice el usuario raíz para sus tareas diarias. Proteja las credenciales del usuario raíz y utilícelas solo para las tareas que solo el usuario raíz pueda realizar. Para ver la lista completa de tareas que requieren que inicie sesión como usuario root, consulte Tareas que requieren credenciales de usuario root en la Guía del IAM usuario.

Identidad federada

Como práctica recomendada, exija a los usuarios humanos, incluidos los que requieren acceso de administrador, que utilicen la federación con un proveedor de identidades para acceder Servicios de AWS mediante credenciales temporales.

Una identidad federada es un usuario del directorio de usuarios de su empresa, un proveedor de identidades web AWS Directory Service, el directorio del Centro de Identidad o cualquier usuario al que acceda Servicios de AWS mediante las credenciales proporcionadas a través de una fuente de identidad. Cuando las identidades federadas acceden Cuentas de AWS, asumen funciones y las funciones proporcionan credenciales temporales.

Para una administración de acceso centralizada, le recomendamos que utilice AWS IAM Identity Center. Puede crear usuarios y grupos en IAM Identity Center, o puede conectarse y sincronizarse con un conjunto de usuarios y grupos de su propia fuente de identidad para usarlos en todas sus aplicaciones Cuentas de AWS . Para obtener información sobre IAM Identity Center, consulte ¿Qué es IAM Identity Center? en la Guía AWS IAM Identity Center del usuario.

Usuarios y grupos de IAM

Un IAMusuario es una identidad propia Cuenta de AWS que tiene permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos utilizar credenciales temporales en lugar de crear IAM usuarios con credenciales de larga duración, como contraseñas y claves de acceso. Sin embargo, si tiene casos de uso específicos que requieren credenciales a largo plazo con IAM los usuarios, le recomendamos que rote las claves de acceso. Para obtener más información, consulte Rotar las claves de acceso con regularidad para los casos de uso que requieran credenciales de larga duración en la Guía del IAM usuario.

Un IAMgrupo es una identidad que especifica un conjunto de IAM usuarios. No puede iniciar sesión como grupo. Puede usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos para grandes conjuntos de usuarios. Por ejemplo, puede asignar un nombre a un grupo IAMAdminsy concederle permisos para administrar IAM los recursos.

Los usuarios son diferentes de los roles. Un usuario se asocia exclusivamente a una persona o aplicación, pero la intención es que cualquier usuario pueda asumir un rol que necesite. Los usuarios tienen credenciales de larga duración permanentes; no obstante, los roles proporcionan credenciales temporales. Para obtener más información, consulte Cuándo crear un IAM usuario (en lugar de un rol) en la Guía del IAM usuario.

IAMroles

Un IAMrol es una identidad dentro de ti Cuenta de AWS que tiene permisos específicos. Es similar a un IAM usuario, pero no está asociado a una persona específica. Puede asumir temporalmente un IAM rol en el AWS Management Console cambiando de rol. Puede asumir un rol llamando a una AWS API operación AWS CLI o o utilizando una operación personalizadaURL. Para obtener más información sobre los métodos de uso de roles, consulte Uso de IAM roles en la Guía del IAM usuario.

IAMlos roles con credenciales temporales son útiles en las siguientes situaciones:

- Acceso de usuario federado: para asignar permisos a una identidad federada, puede crear un rol y definir sus permisos. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos define el rol. Para obtener información sobre los roles para la federación, consulte Creación de un rol para un proveedor de identidad externo en la Guía del IAM usuario. Si usa IAM Identity Center, configura un conjunto de permisos. Para controlar a qué pueden acceder sus identidades después de autenticarse, IAM Identity Center correlaciona el conjunto de permisos con un rol en. IAM Para obtener información acerca de los conjuntos de permisos, consulte Conjuntos de permisos en la Guía del usuario de AWS IAM Identity Center .
- Permisos IAM de usuario temporales: un IAM usuario o rol puede asumir un IAM rol para asumir temporalmente diferentes permisos para una tarea específica.
- Acceso multicuenta: puedes usar un IAM rol para permitir que alguien (un responsable de confianza) de una cuenta diferente acceda a los recursos de tu cuenta. Los roles son la forma principal de conceder acceso entre cuentas. Sin embargo, con algunos Servicios de AWS, puedes adjuntar una política directamente a un recurso (en lugar de usar un rol como proxy). Para conocer la diferencia entre las funciones y las políticas basadas en recursos para el acceso multicuenta, consulta el tema sobre el acceso a los recursos entre cuentas IAM en la Guía del IAM usuario.
- Acceso entre servicios: algunos Servicios de AWS utilizan funciones en otros. Servicios de AWS Por ejemplo, cuando realizas una llamada en un servicio, es habitual que ese servicio ejecute aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio

haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado al servicio.

- Sesiones de acceso directo (FAS): cuando utilizas un IAM usuario o un rol para realizar acciones en AWS ellas, se te considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FASutiliza los permisos del principal que llama a an Servicio de AWS, junto con los que solicitan, Servicio de AWS para realizar solicitudes a los servicios descendentes. FASlas solicitudes solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información detallada sobre la política a la hora de realizar FAS solicitudes, consulte Reenviar las sesiones de acceso.
- Función de servicio: una función de servicio es una IAMfunción que un servicio asume para realizar acciones en su nombre. Un IAM administrador puede crear, modificar y eliminar un rol de servicio desde dentroIAM. Para obtener más información, consulte Crear un rol para delegar permisos Servicio de AWS en un rol en el IAMManual del usuario.
- Función vinculada a un servicio: una función vinculada a un servicio es un tipo de función de servicio que está vinculada a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un IAM administrador puede ver los permisos de los roles vinculados al servicio, pero no editarlos.

- Aplicaciones que se ejecutan en Amazon EC2: puedes usar un IAM rol para administrar las credenciales temporales de las aplicaciones que se ejecutan en una EC2 instancia y que realizan AWS CLI o AWS API solicitan. Esto es preferible a almacenar las claves de acceso en la EC2 instancia. Para asignar un AWS rol a una EC2 instancia y ponerlo a disposición de todas sus aplicaciones, debe crear un perfil de instancia adjunto a la instancia. Un perfil de instancia contiene el rol y permite que los programas que se ejecutan en la EC2 instancia obtengan credenciales temporales. Para obtener más información, consulte Uso de un IAM rol para conceder permisos a aplicaciones que se ejecutan en EC2 instancias de Amazon en la Guía del IAM usuario.

Para saber si se deben usar IAM roles o IAM usuarios, consulte Cuándo crear un IAM rol (en lugar de un usuario) en la Guía del IAM usuario.

Administración de acceso mediante políticas

El acceso se controla AWS creando políticas y adjuntándolas a AWS identidades o recursos. Una política es un objeto AWS que, cuando se asocia a una identidad o un recurso, define sus permisos.

AWS evalúa estas políticas cuando un director (usuario, usuario raíz o sesión de rol) realiza una solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. La mayoría de las políticas se almacenan AWS como JSON documentos. Para obtener más información sobre la estructura y el contenido de los documentos de JSON políticas, consulte Descripción general de JSON las políticas en la Guía del IAM usuario.

Los administradores pueden usar AWS JSON las políticas para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Para conceder a los usuarios permiso para realizar acciones en los recursos que necesitan, un IAM administrador puede crear IAM políticas. A continuación, el administrador puede añadir las IAM políticas a las funciones y los usuarios pueden asumir las funciones.

IAMlas políticas definen los permisos para una acción independientemente del método que se utilice para realizar la operación. Por ejemplo, suponga que dispone de una política que permite la acción `iam:GetRole`. Un usuario con esa política puede obtener información sobre el rol de AWS Management Console AWS CLI, el o el AWS API.

Políticas basadas en identidad

Las políticas basadas en la identidad son documentos de política de JSON permisos que se pueden adjuntar a una identidad, como un IAM usuario, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener información sobre cómo crear una política basada en la identidad, consulte Creación de IAM políticas en la Guía del usuario. IAM

Las políticas basadas en identidades pueden clasificarse además como políticas insertadas o políticas administradas. Las políticas insertadas se integran directamente en un único usuario, grupo o rol. Las políticas administradas son políticas independientes que puede adjuntar a varios usuarios, grupos y funciones de su empresa. Cuenta de AWS Las políticas administradas incluyen políticas AWS administradas y políticas administradas por el cliente. Para saber cómo elegir entre una política gestionada o una política integrada, consulte Elegir entre políticas gestionadas y políticas integradas en la Guía del IAM usuario.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de JSON política que se adjuntan a un recurso. Algunos ejemplos de políticas basadas en recursos son las políticas de confianza de IAM roles y

las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No puede usar políticas AWS administradas desde una política IAM basada en recursos.

Listas de control de acceso () ACLs

Las listas de control de acceso (ACLs) controlan qué responsables (miembros de la cuenta, usuarios o roles) tienen permisos para acceder a un recurso. ACLsson similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de JSON políticas.

Amazon S3 AWS WAF y Amazon VPC son ejemplos de servicios compatiblesACLs. Para obtener más informaciónACLs, consulte la descripción general de la lista de control de acceso (ACL) en la Guía para desarrolladores de Amazon Simple Storage Service.

Otros tipos de políticas

AWS admite tipos de políticas adicionales y menos comunes. Estos tipos de políticas pueden establecer el máximo de permisos que los tipos de políticas más frecuentes le conceden.

- Límites de permisos: un límite de permisos es una función avanzada en la que se establecen los permisos máximos que una política basada en la identidad puede conceder a una IAM entidad (IAMusuario o rol). Puede establecer un límite de permisos para una entidad. Los permisos resultantes son la intersección de las políticas basadas en la identidad de la entidad y los límites de permisos. Las políticas basadas en recursos que especifiquen el usuario o rol en el campo `Principal` no estarán restringidas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información sobre los límites de los permisos, consulte los límites de los permisos para IAM las entidades en la Guía del IAMusuario.
- Políticas de control de servicios (SCPs): SCPs son JSON políticas que especifican los permisos máximos para una organización o unidad organizativa (OU) AWS Organizations. AWS Organizations es un servicio para agrupar y administrar de forma centralizada varios de los Cuentas de AWS que son propiedad de su empresa. Si habilitas todas las funciones de una organización, puedes aplicar políticas de control de servicios (SCPs) a una o a todas tus cuentas.

SCPLimita los permisos de las entidades en las cuentas de los miembros, incluidas las de cada una Usuario raíz de la cuenta de AWS. Para obtener más información sobre OrganizationsSCPs, consulte las políticas de control de servicios en la Guía del AWS Organizations usuario.

- Políticas de sesión: las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de la sesión resultantes son la intersección de las políticas basadas en identidades del rol y las políticas de la sesión. Los permisos también pueden proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información, consulte las políticas de sesión en la Guía del IAM usuario.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para saber cómo se AWS determina si se debe permitir una solicitud cuando se trata de varios tipos de políticas, consulte la lógica de evaluación de políticas en la Guía del IAM usuario.

Cómo funciona Amazon WorkSpaces Secure Browser con IAM

Antes de administrar el acceso IAM a WorkSpaces Secure Browser, infórmese sobre IAM las funciones disponibles para su uso con WorkSpaces Secure Browser.

IAMfunciones que puede utilizar con Amazon WorkSpaces Secure Browser

IAMcaracterística	WorkSpaces Compatibilidad con Secure Browser
Políticas basadas en identidades	Sí
Políticas basadas en recursos	No
Acciones de políticas	Sí
Recursos de políticas	Sí
Claves de condición de política	Sí
ACLs	No

IAMcaracterística	WorkSpaces Compatibilidad con Secure Browser
ABAC(etiquetas en las políticas)	Parcial
Credenciales temporales	Sí
Permisos de entidades principales	Sí
Roles de servicio	No
Roles vinculados al servicio	Sí

Para obtener una visión general de cómo funcionan WorkSpaces Secure Browser y otros AWS servicios con la mayoría de IAM las funciones, consulte AWS los servicios con los que funcionan IAM en la Guía del IAM usuario.

Políticas basadas en la identidad de Secure Browser WorkSpaces

Compatibilidad con las políticas basadas en identidad: sí

Las políticas basadas en la identidad son documentos de política de JSON permisos que se pueden adjuntar a una identidad, como un IAM usuario, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener información sobre cómo crear una política basada en la identidad, consulte Creación de IAM políticas en la Guía del usuario. IAM

Con las políticas IAM basadas en la identidad, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. No es posible especificar la entidad principal en una política basada en identidad porque se aplica al usuario o rol al que está adjunto. Para obtener más información sobre todos los elementos que puede utilizar en una JSON política, consulte la referencia sobre los elementos de la IAM JSON política en la Guía del IAMusuario.

Ejemplos de políticas basadas en la identidad para WorkSpaces Secure Browser

Para ver ejemplos de políticas basadas en la identidad de WorkSpaces Secure Browser, consulte. Ejemplos de políticas basadas en identidad para Amazon Secure Browser WorkSpaces

Políticas basadas en recursos de Secure Browser WorkSpaces

Admite políticas basadas en recursos: no

Las políticas basadas en recursos son JSON documentos de políticas que se adjuntan a un recurso. Algunos ejemplos de políticas basadas en recursos son las políticas de confianza de IAM roles y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Para habilitar el acceso entre cuentas, puede especificar una cuenta completa o IAM entidades de otra cuenta como principales en una política basada en recursos. Añadir a una política en función de recursos una entidad principal entre cuentas es solo una parte del establecimiento de una relación de confianza. Cuando el principal y el recurso son diferentes Cuentas de AWS, el IAM administrador de la cuenta de confianza también debe conceder permiso a la entidad principal (usuario o rol) para acceder al recurso. Para conceder el permiso, adjunte la entidad a una política basada en identidad. Sin embargo, si la política en función de recursos concede el acceso a una entidad principal de la misma cuenta, no es necesaria una política basada en identidad adicional. Para obtener más información, consulte Acceso a recursos entre cuentas IAM en la Guía del IAM usuario.

Acciones políticas para WorkSpaces Secure Browser

Compatibilidad con las acciones de política: sí

Los administradores pueden usar AWS JSON políticas para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El `Action` elemento de una JSON política describe las acciones que puede utilizar para permitir o denegar el acceso en una política. Las acciones de política suelen tener el mismo nombre que la AWS API operación asociada. Hay algunas excepciones, como las acciones que solo permiten permisos y que no tienen una operación coincidente. API También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Para ver una lista de las acciones de WorkSpaces Secure Browser, consulte Acciones definidas por Amazon WorkSpaces Secure Browser en la Referencia de autorización del servicio.

Las acciones políticas de WorkSpaces Secure Browser utilizan el siguiente prefijo antes de la acción:

```
workspaces-web
```

Para especificar varias acciones en una única instrucción, sepárelas con comas.

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

Para ver ejemplos de políticas basadas en la identidad de WorkSpaces Secure Browser, consulte. Ejemplos de políticas basadas en identidad para Amazon Secure Browser WorkSpaces

Recursos de políticas para Secure Browser WorkSpaces

Compatibilidad con los recursos de políticas: sí

Los administradores pueden usar AWS JSON políticas para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` JSON de política especifica el objeto o los objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso mediante su nombre de recurso de Amazon (ARN). Puede hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, utilice un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

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

Para ver una lista de los tipos de recursos de WorkSpaces Secure Browser y sus ARNs correspondientes, consulte Recursos definidos por Amazon WorkSpaces Secure Browser en la

Referencia de autorización de servicio. Para saber con qué acciones puede especificar cada recurso, consulte Acciones definidas por Amazon WorkSpaces Secure Browser. ARN

Para ver ejemplos de políticas basadas en la identidad de WorkSpaces Secure Browser, consulte. Ejemplos de políticas basadas en identidad para Amazon Secure Browser WorkSpaces

Claves de condición de la política para Secure Browser WorkSpaces

Compatibilidad con claves de condición de políticas específicas del servicio: sí

Los administradores pueden usar AWS JSON políticas para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` (o bloque de `Condition`) permite especificar condiciones en las que entra en vigor una instrucción. El elemento `Condition` es opcional. Puede crear expresiones condicionales que utilicen operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud.

Si especifica varios elementos de `Condition` en una instrucción o varias claves en un único elemento de `Condition`, AWS las evalúa mediante una operación `AND` lógica. Si especifica varios valores para una única clave de condición, AWS evalúa la condición mediante una `OR` operación lógica. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puede utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puede conceder a un IAM usuario permiso para acceder a un recurso solo si está etiquetado con su nombre de IAM usuario. Para obtener más información, consulte los elementos IAM de la política: variables y etiquetas en la Guía del IAM usuario.

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas las claves de condición AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del IAMusuario.

Para ver una lista de claves de condición de WorkSpaces Secure Browser, consulte Claves de condición de Amazon WorkSpaces Secure Browser en la Referencia de autorización de servicio. Para saber con qué acciones y recursos puede utilizar una clave de condición, consulte Acciones definidas por Amazon WorkSpaces Secure Browser.

Para ver ejemplos de políticas basadas en la identidad de WorkSpaces Secure Browser, consulte. Ejemplos de políticas basadas en identidad para Amazon Secure Browser WorkSpaces

Listas de control de acceso (ACLs) en Secure Browser WorkSpaces

SoportaACLs: No

Las listas de control de acceso (ACLs) controlan qué directores (miembros de la cuenta, usuarios o roles) tienen permisos para acceder a un recurso. ACLsson similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de JSON políticas.

Control de acceso basado en atributos () ABAC con Secure Browser WorkSpaces

Soportes ABAC (etiquetas en las políticas): parciales

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define los permisos en función de los atributos. En AWS, estos atributos se denominan etiquetas. Puede adjuntar etiquetas a IAM entidades (usuarios o roles) y a muchos AWS recursos. Etiquetar entidades y recursos es el primer paso deABAC. Luego, diseñe ABAC políticas para permitir las operaciones cuando la etiqueta del principal coincida con la etiqueta del recurso al que está intentando acceder.

ABACes útil en entornos de rápido crecimiento y ayuda en situaciones en las que la administración de políticas se vuelve engorrosa.

Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política utilizando las claves de condición `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Si un servicio admite las tres claves de condición para cada tipo de recurso, el valor es Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial.

Para obtener más información al respectoABAC, consulte ¿Qué es? ABAC en la Guía IAM del usuario. Para ver un tutorial con los pasos de configuraciónABAC, consulte Usar el control de acceso basado en atributos (ABAC) en la Guía del IAMusuario.

Uso de credenciales temporales con Secure Browser WorkSpaces

Compatibilidad con credenciales temporales: sí

Algunas Servicios de AWS no funcionan cuando se inicia sesión con credenciales temporales. Para obtener información adicional, incluida la información sobre cuáles Servicios de AWS funcionan con credenciales temporales, consulta Servicios de AWS la guía del IAM usuario sobre cómo trabajar con IAM ellas.

Está utilizando credenciales temporales si inicia sesión AWS Management Console con cualquier método excepto un nombre de usuario y una contraseña. Por ejemplo, cuando accedes AWS mediante el enlace de inicio de sesión único (SSO) de tu empresa, ese proceso crea automáticamente credenciales temporales. También crea credenciales temporales de forma automática cuando inicia sesión en la consola como usuario y luego cambia de rol. Para obtener más información sobre el cambio de rol, consulte Cambiar a un rol (consola) en la Guía del IAMusuario.

Puede crear credenciales temporales manualmente con la tecla AWS CLI o AWS API. A continuación, puede utilizar esas credenciales temporales para acceder AWS. AWS recomienda generar credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para obtener más información, consulte Credenciales de seguridad temporales en IAM.

Permisos principales entre servicios para WorkSpaces Secure Browser

Admite sesiones de acceso directo (FAS): Sí

Cuando utilizas un IAM usuario o un rol para realizar acciones en AWSél, se te considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FASutiliza los permisos del principal que llama a una Servicio de AWS, junto con los que solicita, Servicio de AWS para realizar solicitudes a los servicios descendentes. FASlas solicitudes solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información detallada sobre la política a la hora de realizar FAS solicitudes, consulte Reenviar las sesiones de acceso.

Funciones de servicio para WorkSpaces Secure Browser

Compatible con roles de servicio: No

Una función de servicio es una IAMfunción que asume un servicio para realizar acciones en su nombre. Un IAM administrador puede crear, modificar y eliminar un rol de servicio desde dentroIAM. Para obtener más información, consulte Crear un rol para delegar permisos Servicio de AWS en un rol en el IAMManual del usuario.

> **Warning**
>
> Cambiar los permisos de un rol de servicio podría interrumpir la funcionalidad de WorkSpaces Secure Browser. Edite las funciones de servicio solo cuando WorkSpaces Secure Browser proporcione instrucciones para hacerlo.

Funciones vinculadas a servicios para WorkSpaces Secure Browser

Admite roles vinculados al servicio: sí

Un rol vinculado a un servicio es un tipo de rol de servicio que está vinculado a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un IAM administrador puede ver los permisos de los roles vinculados al servicio, pero no editarlos.

Para obtener más información sobre la creación o la administración de funciones vinculadas a un servicio, consulte los AWS servicios que funcionan con. IAM Busque un servicio en la tabla que incluya `Yes` en la columna Rol vinculado a un servicio. Seleccione el vínculo Sí para ver la documentación acerca del rol vinculado a servicios para ese servicio.

Ejemplos de políticas basadas en identidad para Amazon Secure Browser WorkSpaces

De forma predeterminada, los usuarios y los roles no tienen permiso para crear o modificar los recursos de WorkSpaces Secure Browser. Tampoco pueden realizar tareas con AWS Management Console, AWS Command Line Interface (AWS CLI) o AWS API. Para conceder a los usuarios permiso para realizar acciones en los recursos que necesitan, un IAM administrador puede crear IAM políticas. A continuación, el administrador puede añadir las IAM políticas a las funciones y los usuarios pueden asumir las funciones.

Para obtener información sobre cómo crear una política IAM basada en la identidad mediante estos documentos de JSON política de ejemplo, consulte Creación de IAM políticas en la Guía del IAMusuario.

Para obtener más información sobre las acciones y los tipos de recursos definidos por WorkSpaces Secure Browser, incluido el ARNs formato de cada uno de los tipos de recursos, consulte Acciones, recursos y claves de condición de Amazon WorkSpaces Secure Browser en la Referencia de autorización de servicios.

Temas

- Prácticas recomendadas sobre las políticas
- Uso de la consola de WorkSpaces Secure Browser
- Cómo permitir a los usuarios consultar sus propios permisos

Prácticas recomendadas sobre las políticas

Las políticas basadas en la identidad determinan si alguien puede crear, acceder o eliminar los recursos de WorkSpaces Secure Browser de su cuenta. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están disponibles en su. Cuenta de AWS Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Para obtener más información, consulte las políticas AWS gestionadas o las políticas AWS gestionadas para las funciones laborales en la Guía del IAM usuario.
- Aplique permisos con privilegios mínimos: cuando establezca permisos con IAM políticas, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Para obtener más información sobre cómo IAM aplicar permisos, consulte Políticas y permisos IAM en la IAM Guía del usuario.
- Utilice las condiciones en IAM las políticas para restringir aún más el acceso: puede añadir una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de política para especificar que todas las solicitudes deben enviarse medianteSSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo AWS CloudFormation. Para obtener más información, consulte los elementos IAM JSON de la política: Condición en la Guía del IAM usuario.
- Utilice IAM Access Analyzer para validar sus IAM políticas y garantizar permisos seguros y funcionales: IAM Access Analyzer valida las políticas nuevas y existentes para que se ajusten al lenguaje de las políticas (JSON) y IAM a las IAM mejores prácticas. IAMAccess Analyzer proporciona más de 100 comprobaciones de políticas y recomendaciones prácticas para ayudarle a crear políticas seguras y funcionales. Para obtener más información, consulte la validación de políticas de IAM Access Analyzer en la Guía del IAM usuario.
- Requerir autenticación multifactorial (MFA): si se encuentra en una situación en la que se requieren IAM usuarios o un usuario raíz Cuenta de AWS, actívela MFA para aumentar la seguridad. Para solicitarlo MFA cuando se convoque a API las operaciones, añada MFA

condiciones a sus políticas. Para obtener más información, consulte Configuración del API acceso MFA protegido en la Guía del IAM usuario.

Para obtener más información sobre las prácticas recomendadasIAM, consulte las prácticas recomendadas de seguridad IAM en la Guía del IAM usuario.

Uso de la consola de WorkSpaces Secure Browser

Para acceder a la consola de Amazon WorkSpaces Secure Browser, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle enumerar y ver detalles sobre los recursos de WorkSpaces Secure Browser de su propiedad Cuenta de AWS. Si crea una política basada en identidades que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles) que tengan esa política.

No es necesario conceder permisos mínimos de consola a los usuarios que realicen llamadas únicamente al AWS CLI o al AWS API. En su lugar, permita el acceso únicamente a las acciones que coincidan con la API operación que están intentando realizar.

Para garantizar que los usuarios y los roles puedan seguir utilizando la consola de WorkSpaces Secure Browser, adjunte también el navegador WorkSpaces seguro `ConsoleAccess` o la política `ReadOnly` AWS administrada a las entidades. Para obtener más información, consulte Añadir permisos a un usuario en la Guía del IAM usuario.

Cómo permitir a los usuarios consultar sus propios permisos

En este ejemplo se muestra cómo se puede crear una política que permita a IAM los usuarios ver las políticas integradas y administradas asociadas a su identidad de usuario. Esta política incluye permisos para completar esta acción en la consola o mediante programación mediante la tecla o. AWS CLI AWS API

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
```

```
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS políticas administradas para WorkSpaces Secure Browser

Para añadir permisos a usuarios, grupos y roles, es más fácil usar políticas AWS administradas que escribirlas usted mismo. Se necesita tiempo y experiencia para crear políticas administradas por el cliente de IAM que proporcionen a su equipo solo los permisos necesarios. Para empezar rápidamente, puedes usar nuestras políticas AWS gestionadas. Estas políticas cubren casos de uso comunes y están disponibles en tu AWS cuenta. Para obtener más información sobre las políticas AWS administradas, consulte las políticas AWS administradas en la Guía del usuario de IAM.

AWS los servicios mantienen y AWS actualizan las políticas gestionadas. No puede cambiar los permisos en las políticas AWS gestionadas. En ocasiones, los servicios pueden añadir permisos adicionales a una política AWS gestionada para admitir nuevas funciones. Este tipo de actualización afecta a todas las identidades (usuarios, grupos y roles) donde se asocia la política. Es más probable que los servicios actualicen una política administrada por AWS cuando se lanza una nueva

característica o cuando se ponen a disposición nuevas operaciones. Los servicios no eliminan los permisos de una política AWS administrada, por lo que las actualizaciones de la política no afectarán a los permisos existentes.

Además, AWS admite políticas administradas para funciones laborales que abarcan varios servicios. Por ejemplo, la política `ReadOnlyAccess` AWS gestionada proporciona acceso de solo lectura a todos los AWS servicios y recursos. Cuando un servicio lanza una nueva función, AWS agrega permisos de solo lectura para nuevas operaciones y recursos. Para obtener una lista y descripciones de las políticas de funciones de trabajo, consulte Políticas administradas de AWS para funciones de trabajo en la Guía del usuario de IAM.

AWS política gestionada: AmazonWorkSpacesWebServiceRolePolicy

No puede adjuntar la política `AmazonWorkSpacesWebServiceRolePolicy` a sus entidades de IAM. Esta política está asociada a un rol vinculado a un servicio que permite a WorkSpaces Secure Browser realizar acciones en su nombre. Para obtener más información, consulte the section called "Usar roles vinculados a servicios".

Esta política otorga permisos administrativos que permiten el acceso a los AWS servicios y recursos utilizados o administrados por WorkSpaces Secure Browser.

Detalles de los permisos

Esta política incluye los permisos siguientes:

- `workspaces-web`— Permite el acceso a AWS los servicios y recursos utilizados o administrados por WorkSpaces Secure Browser.
- `ec2`: permite a las entidades principales describir las VPC, las subredes y las zonas de disponibilidad; crear, etiquetar, describir y eliminar interfaces de red; asociar o desasociar una dirección; y describir las tablas de enrutamiento, los grupos de seguridad y los puntos de conexión de VPC.

- `CloudWatch`: permite a las entidades principales colocar datos métricos.
- `Kinesis`: permite a las entidades principales describir un resumen de los flujos de datos de Kinesis y colocar registros en flujos de datos de Kinesis para registrar el acceso de los usuarios. Para obtener más información, consulte the section called “Configuración del registro de acceso de usuario”.

```
{
    "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 gestionada: AmazonWorkSpacesSecureBrowserReadOnly

Puede adjuntar la política `AmazonWorkSpacesSecureBrowserReadOnly` a las identidades de IAM.

Esta política otorga permisos de solo lectura que permiten el acceso a WorkSpaces Secure Browser y sus dependencias a través de la consola de AWS administración, el SDK y la CLI. Esta política no incluye los permisos necesarios para interactuar con los portales utilizando `IAM_Identity_Center` como tipo de autenticación. Para obtener estos permisos, combine esta política con `AWSSSOReadOnly`.

Detalles de los permisos

Esta política incluye los siguientes permisos.

- `workspaces-web`— Proporciona acceso de solo lectura a WorkSpaces Secure Browser y sus dependencias a través de la consola de AWS administración, el SDK y la CLI.
- `ec2`: permite a las entidades principales describir las VPC y los grupos de seguridad. Se utiliza en la consola de AWS administración de WorkSpaces Secure Browser para mostrarle las VPC, las subredes y los grupos de seguridad que están disponibles para su uso con el servicio.

- `Kinesis`: permite a las entidades principales obtener una lista de los flujos de datos de Kinesis. Se usa en la consola de AWS administración de WorkSpaces Secure Browser para mostrarle las transmisiones de datos de Kinesis que están disponibles para su uso con el servicio.

```
{
    "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 gestionada: AmazonWorkSpacesWebReadOnly

Puede adjuntar la política `AmazonWorkSpacesWebReadOnly` a las identidades de IAM.

Esta política otorga permisos de solo lectura que permiten el acceso a WorkSpaces Secure Browser y sus dependencias a través de la consola de AWS administración, el SDK y la CLI. Esta política no incluye los permisos necesarios para interactuar con los portales utilizando `IAM_Identity_Center` como tipo de autenticación. Para obtener estos permisos, combine esta política con `AWSSSOReadOnly`.

> **Note**
>
> Si actualmente usa esta política, cámbiese a la nueva política. `AmazonWorkSpacesSecureBrowserReadOnly`

Detalles de los permisos

Esta política incluye los siguientes permisos.

- `workspaces-web`— Proporciona acceso de solo lectura a WorkSpaces Secure Browser y sus dependencias a través de la consola de AWS administración, el SDK y la CLI.
- `ec2`: permite a las entidades principales describir las VPC y los grupos de seguridad. Se utiliza en la consola de AWS administración de WorkSpaces Secure Browser para mostrarle las VPC, las subredes y los grupos de seguridad que están disponibles para su uso con el servicio.
- `Kinesis`: permite a las entidades principales obtener una lista de los flujos de datos de Kinesis. Se usa en la consola de AWS administración de WorkSpaces Secure Browser para mostrarle las transmisiones de datos de Kinesis que están disponibles para su uso con el servicio.

```
{
    "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 Secure Browser actualiza las políticas AWS administradas

Consulte los detalles sobre las actualizaciones de las políticas AWS administradas de WorkSpaces Secure Browser desde que este servicio comenzó a rastrear estos cambios. Para obtener alertas

automáticas sobre cambios en esta página, suscríbase a la fuente RSS en la página de Historial de documentos.

Cambio	Descripción	Fecha
AmazonWorkSpacesSecureBrowserReadOnly: política nueva	WorkSpaces Secure Browser agregó una nueva política para proporcionar acceso de solo lectura a WorkSpaces Secure Browser y sus dependencias a través de la consola de administración de AWS, el SDK y la CLI.	24 de junio de 2024
AmazonWorkSpacesWebServiceRolePolicy: política actualizada	WorkSpaces Secure Browser actualizó la política CreateNetworkInterface para restringir las etiquetas con aws:RequestTag/WorkSpacesWebManaged: true y actuar en los recursos de subredes y grupos de seguridad, así como restringir DeleteNetworkInterface el uso de los ENI etiquetados con aws:/: true. ResourceTag WorkSpacesWebManaged	15 de diciembre de 2022
AmazonWorkSpacesWebReadOnly: política actualizada	WorkSpaces Secure Browser actualizó la política para incluir permisos de lectura para el acceso de los usuarios, el registro y la lista de las transmisiones de datos de Kinesis. Para obtener más información, consulte the section called “Configuración	2 de noviembre de 2022

Cambio	Descripción	Fecha
	del registro de acceso de usuario”.	
AmazonWorkSpacesWebServiceRolePolicy: política actualizada	WorkSpaces Secure Browser actualizó la política para describir un resumen de las transmisiones de datos de Kinesis e incluir registros en las transmisiones de datos de Kinesis para registrar el acceso de los usuarios. Para obtener más información, consulte the section called “Configuración del registro de acceso de usuario”.	17 de octubre de 2022
AmazonWorkSpacesWebServiceRolePolicy: política actualizada	WorkSpaces Secure Browser actualizó la política para crear etiquetas durante la creación de ENI.	6 de septiembre de 2022
AmazonWorkSpacesWebServiceRolePolicy: política actualizada	WorkSpaces Secure Browser actualizó la política para añadir el espacio de nombres AWS/Usage a los permisos de la API. PutMetricData	6 de abril de 2022
AmazonWorkSpacesWebReadOnly: política nueva	WorkSpaces Secure Browser agregó una nueva política para proporcionar acceso de solo lectura a WorkSpaces Secure Browser y sus dependencias a través de la consola de administración de AWS, el SDK y la CLI.	30 de noviembre de 2021

Cambio	Descripción	Fecha
AmazonWorkSpacesWebServiceRolePolicy: política nueva	WorkSpaces Secure Browser agregó una nueva política para permitir el acceso a los servicios y recursos de AWS utilizados o administrados por WorkSpaces Secure Browser.	30 de noviembre de 2021
WorkSpaces Secure Browser comenzó a rastrear los cambios	WorkSpaces Secure Browser comenzó a rastrear los cambios en sus políticas AWS administradas.	30 de noviembre de 2021

Solución de problemas de identidad y acceso a Amazon WorkSpaces Secure Browser

Utilice la siguiente información para ayudarlo a diagnosticar y solucionar los problemas comunes que pueden surgir al trabajar con WorkSpaces Secure Browser yIAM.

Temas

- No estoy autorizado a realizar ninguna acción en WorkSpaces Secure Browser
- No estoy autorizado a realizar tareas como: PassRole
- Quiero permitir que personas ajenas a mi AWS cuenta accedan a mis recursos de WorkSpaces Secure Browser

No estoy autorizado a realizar ninguna acción en WorkSpaces Secure Browser

Si recibe un error que indica que no tiene autorización para realizar una acción, las políticas se deben actualizar para permitirle realizar la acción.

El siguiente ejemplo de error se produce cuando el `mateojackson` IAM usuario intenta usar la consola para ver detalles sobre un *`my-example-widget`* recurso ficticio pero no tiene los `workspaces-web:`*`GetWidget`* permisos ficticios.

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

En este caso, la política del usuario `mateojackson` debe actualizarse para permitir el acceso al recurso *`my-example-widget`* mediante la acción `workspaces-web:`*`GetWidget`*.

Si necesita ayuda, póngase en contacto con AWS el administrador. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

No estoy autorizado a realizar tareas como: PassRole

Si recibe un error que indica que no está autorizado a realizar la `iam:PassRole` acción, sus políticas deben actualizarse para que pueda transferir una función a WorkSpaces Secure Browser.

Algunas Servicios de AWS permiten transferir una función existente a ese servicio en lugar de crear una nueva función de servicio o una función vinculada a un servicio. Para ello, debe tener permisos para transferir el rol al servicio.

El siguiente ejemplo de error se produce cuando un IAM usuario denominado `marymajor` intenta utilizar la consola para realizar una acción en WorkSpaces Secure Browser. Sin embargo, la acción requiere que el servicio cuente con permisos que otorguen un rol de servicio. Mary no tiene permisos para transferir el rol al servicio.

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

En este caso, las políticas de Mary se deben actualizar para permitirle realizar la acción `iam:PassRole`.

Si necesita ayuda, póngase en contacto con AWS el administrador. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero permitir que personas ajenas a mi AWS cuenta accedan a mis recursos de WorkSpaces Secure Browser

Puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Puede especificar una persona de confianza para que asuma el rol. En el caso de los servicios que admiten políticas basadas en recursos o listas de

control de acceso (ACLs), puede usar esas políticas para permitir que las personas accedan a sus recursos.

Para más información, consulte lo siguiente:

- Para saber si WorkSpaces Secure Browser admite estas funciones, consulte. Cómo funciona Amazon WorkSpaces Secure Browser con IAM
- Para obtener información sobre cómo proporcionar acceso a los recursos de su propiedad, consulte Proporcionar acceso a un IAM usuario en otro Cuenta de AWS de su propiedad en la Guía del IAM usuario. Cuentas de AWS
- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta Cómo permitir el acceso a recursos que Cuentas de AWS son propiedad de terceros en la Guía del IAM usuario.
- Para obtener información sobre cómo proporcionar acceso mediante la federación de identidades, consulte Proporcionar acceso a usuarios autenticados externamente (federación de identidades) en la Guía del IAM usuario.
- Para saber la diferencia entre el uso de roles y políticas basadas en recursos para el acceso entre cuentas, consulte el acceso a recursos entre cuentas IAM en la Guía del usuario. IAM

Uso de funciones vinculadas a servicios para WorkSpaces Secure Browser

Amazon WorkSpaces Secure Browser utiliza AWS Identity and Access Management funciones vinculadas a servicios (IAM). Un rol vinculado a un servicio es un tipo único de rol de IAM que está vinculado directamente a Secure Browser. WorkSpaces Los roles vinculados al servicio están predefinidos por WorkSpaces Secure Browser e incluyen todos los permisos que el servicio requiere para llamar a otros AWS servicios en su nombre.

Un rol vinculado a un servicio facilita la configuración de WorkSpaces Secure Browser, ya que no es necesario añadir manualmente los permisos necesarios. WorkSpaces Secure Browser define los permisos de sus funciones vinculadas al servicio y, a menos que se defina lo contrario, solo WorkSpaces Secure Browser puede asumir sus funciones. Los permisos definidos incluyen políticas de confianza y políticas de permisos. La política de permisos no se puede adjuntar a ninguna otra entidad de IAM.

Solo puede eliminar un rol vinculado a servicios después de eliminar sus recursos relacionados. Esto protege los recursos de WorkSpaces Secure Browser porque no puede eliminar inadvertidamente el permiso de acceso a los recursos.

Para obtener información acerca de otros servicios que admiten roles vinculados a servicios, consulte Servicios de AWS que funcionan con IAM y busque los servicios que muestran Sí en la columna Rol vinculado a un servicio. Elija una opción Sí con un enlace para ver la documentación acerca del rol vinculado a servicios en cuestión.

Permisos de rol vinculados al servicio para Secure Browser WorkSpaces

WorkSpaces Secure Browser usa el rol vinculado al servicio denominado`AWSServiceRoleForAmazonWorkSpacesWeb`: WorkSpaces Secure Browser usa este rol vinculado al servicio para acceder a los recursos de Amazon EC2 de las cuentas de los clientes para transmitir instancias y métricas. CloudWatch

El rol vinculado al servicio `AWSServiceRoleForAmazonWorkSpacesWeb` depende de los siguientes servicios para asumir el rol:

- `workspaces-web.amazonaws.com`

La política de permisos de roles denominada `AmazonWorkSpacesWebServiceRolePolicy` permite a WorkSpaces Secure Browser realizar las siguientes acciones en los recursos especificados. Para obtener más información, consulte the section called "AmazonWorkSpacesWebServiceRolePolicy".

- Acción: `ec2:DescribeVpcs` en `all AWS resources`
- Acción: `ec2:DescribeSubnets` en `all AWS resources`
- Acción: `ec2:DescribeAvailabilityZones` en `all AWS resources`
- Acción: `ec2:CreateNetworkInterface` con `aws:RequestTag/WorkSpacesWebManaged: true` en recursos de subred y grupo de seguridad
- Acción: `ec2:DescribeNetworkInterfaces` en `all AWS resources`
- Acción: `ec2:DeleteNetworkInterface` en las interfaces de red con `aws:ResourceTag/ WorkSpacesWebManaged: true`
- Acción: `ec2:DescribeSubnets` en `all AWS resources`
- Acción: `ec2:AssociateAddress` en `all AWS resources`
- Acción: `ec2:DisassociateAddress` en `all AWS resources`
- Acción: `ec2:DescribeRouteTables` en `all AWS resources`
- Acción: `ec2:DescribeSecurityGroups` en `all AWS resources`

- Acción: `ec2:DescribeVpcEndpoints` en `all AWS resources`
- Acción: `ec2:CreateTags` en la operación `ec2:CreateNetworkInterface` con `aws:TagKeys: ["WorkSpacesWebManaged"]`
- Acción: `cloudwatch:PutMetricData` en `all AWS resources`
- Acción: `kinesis:PutRecord` en flujos de datos de Kinesis con nombres que comiencen por `amazon-workspaces-web-`
- Acción: `kinesis:PutRecords` en flujos de datos de Kinesis con nombres que comiencen por `amazon-workspaces-web-`
- Acción: `kinesis:DescribeStreamSummary` en flujos de datos de Kinesis con nombres que comiencen por `amazon-workspaces-web-`

Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o rol) crear, editar o eliminar un rol vinculado a servicios. Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de IAM.

Crear un rol vinculado a un servicio para WorkSpaces Secure Browser

No necesita crear manualmente un rol vinculado a servicios. Al crear su primer portal en la AWS Management Console, la o la AWS API AWS CLI, WorkSpaces Secure Browser crea automáticamente la función vinculada al servicio.

> **Important**
>
> Este rol vinculado a servicios puede aparecer en su cuenta si se ha completado una acción en otro servicio que utilice las características compatibles con este rol.

Si elimina este rol vinculado a un servicio y luego necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Cuando crea su primer portal, WorkSpaces Secure Browser vuelve a crear el rol vinculado al servicio para usted.

También puede usar la consola de IAM para crear un rol vinculado a un servicio con el caso de uso de Secure Browser. WorkSpaces En la API AWS CLI o en la AWS API, cree una función vinculada a un servicio con el nombre del servicio. `workspaces-web.amazonaws.com` Para obtener más información, consulte Crear un rol vinculado a un servicio en la Guía del usuario de IAM. Si elimina este rol vinculado al servicio, puede utilizar este mismo proceso para volver a crear el rol.

Edición de un rol vinculado a un servicio para Secure Browser WorkSpaces

WorkSpaces Secure Browser no le permite editar el rol vinculado al `AWSServiceRoleForAmazonWorkSpacesWeb` servicio. Después de crear un rol vinculado a un servicio, no puede cambiarle el nombre, ya que varias entidades pueden hacer referencia a él. Sin embargo, puede editar la descripción del rol mediante IAM. Para obtener más información, consulte Editar un rol vinculado a servicios en la Guía del usuario de IAM.

Eliminar un rol vinculado a un servicio para Secure Browser WorkSpaces

Si ya no necesita usar una característica o servicio que requieran un rol vinculado a un servicio, le recomendamos que elimine dicho rol. Así no tendrá una entidad no utilizada que no se monitorice ni mantenga de forma activa. Sin embargo, debe limpiar los recursos de su rol vinculado al servicio antes de eliminarlo manualmente.

> **Note**
>
> Si el servicio WorkSpaces Secure Browser utiliza el rol al intentar eliminar los recursos, es posible que la eliminación no se realice correctamente. En tal caso, espere unos minutos e intente de nuevo la operación.

Para eliminar los recursos de WorkSpaces Secure Browser utilizados por el AWSServiceRoleForAmazonWorkSpacesWeb

- Elija una de las siguientes opciones.
  - Si usa la consola, elimine todos los portales en la consola.
  - Si usa la CLI o la API, desasocie todos sus recursos (incluida la configuración del navegador, la configuración de red, la configuración de usuario, los almacenes de confianza y la configuración de registro de acceso de los usuarios) de sus portales, elimine estos recursos y, a continuación, elimine los portales.

Eliminación manual del rol vinculado a servicios mediante IAM

Utilice la consola de IAM AWS CLI, la o la AWS API para eliminar la función vinculada al AWSServiceRoleForAmazonWorkSpacesWeb servicio. Para más información, consulte Eliminación de un rol vinculado a servicios en la Guía del usuario de IAM.

Regiones compatibles con las funciones vinculadas al servicio de WorkSpaces Secure Browser

WorkSpaces Secure Browser admite el uso de funciones vinculadas al servicio en todas las regiones en las que el servicio está disponible. Para obtener más información, consulte Regiones y puntos de conexión de AWS.

Respuesta a incidentes en Amazon WorkSpaces Secure Browser

Puedes detectar incidentes supervisando la CloudWatch métrica de `SessionFailure` Amazon. Para recibir alertas de incidentes, usa una CloudWatch alarma para la `SessionFailure` métrica. Para obtener más información, consulte Supervisión de Amazon WorkSpaces Secure Browser con Amazon CloudWatch.

Validación de conformidad para Amazon WorkSpaces Secure Browser

Para saber si uno Servicio de AWS está dentro del ámbito de aplicación de programas de cumplimiento específicos, consulte Servicios de AWS Alcance por programa de cumplimiento Servicios de AWS de cumplimiento y elija el programa de cumplimiento que le interese. Para obtener información general, consulte Programas de AWS cumplimiento > Programas AWS .

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact .

Su responsabilidad de cumplimiento al Servicios de AWS utilizarlos viene determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y reglamentos aplicables. AWS proporciona los siguientes recursos para ayudar con el cumplimiento:

- Guías de inicio rápido sobre seguridad y cumplimiento: estas guías de implementación analizan las consideraciones arquitectónicas y proporcionan los pasos para implementar entornos básicos centrados en AWS la seguridad y el cumplimiento.
- Diseñando una arquitectura basada en la HIPAA seguridad y el cumplimiento en Amazon Web Services: en este documento técnico se describe cómo pueden utilizar las empresas AWS para crear HIPAA aplicaciones aptas.

> **Note**
>
> No todos son aptos. Servicios de AWS HIPAA Para obtener más información, consulta la Referencia de servicios HIPAA aptos.

- AWS Recursos de de cumplimiento: esta colección de libros de trabajo y guías puede aplicarse a su industria y ubicación.
- AWS Guías de cumplimiento para clientes: comprenda el modelo de responsabilidad compartida desde la perspectiva del cumplimiento. En las guías se resumen las mejores prácticas para garantizar la seguridad Servicios de AWS y se orientan a los controles de seguridad en varios marcos (incluidos el Instituto Nacional de Estándares y Tecnología (NIST), el Consejo de Normas de Seguridad de la Industria de Tarjetas de Pago (PCI) y la Organización Internacional de Normalización (ISO)).
- Evaluación de los recursos con reglas en la guía para AWS Config desarrolladores: el AWS Config servicio evalúa en qué medida las configuraciones de los recursos cumplen con las prácticas internas, las directrices del sector y las normas.
- AWS Security Hub— Esto Servicio de AWS proporciona una visión completa del estado de su seguridad interior AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos de AWS y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulte la Referencia de controles de Security Hub.
- Amazon GuardDuty: Servicio de AWS detecta posibles amenazas para sus cargas de trabajo Cuentas de AWS, contenedores y datos mediante la supervisión de su entorno para detectar actividades sospechosas y maliciosas. GuardDuty puede ayudarlo a cumplir con varios requisitos de conformidad, por ejemplo PCIDSS, cumpliendo con los requisitos de detección de intrusiones exigidos por ciertos marcos de cumplimiento.
- AWS Audit Manager— Esto le Servicio de AWS ayuda a auditar continuamente su AWS consumo para simplificar la gestión del riesgo y el cumplimiento de las normativas y los estándares del sector.

Resiliencia en Amazon WorkSpaces Secure Browser

La infraestructura AWS global se basa en distintas zonas Regiones de AWS de disponibilidad. Regiones de AWS proporcionan varias zonas de disponibilidad aisladas y separadas físicamente,

que están conectadas mediante redes de baja latencia, alto rendimiento y alta redundancia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre las zonas sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de uno o varios centros de datos.

Para obtener más información sobre las zonas de disponibilidad Regiones de AWS y las zonas de disponibilidad, consulte Infraestructura global.AWS

Actualmente, WorkSpaces Secure Browser no admite lo siguiente:

- Realizar copias de seguridad del contenido en zonas de disponibilidad o regiones
- Copias de seguridad cifradas
- Cifrar el contenido en tránsito entre zonas de disponibilidad o regiones
- Copias de seguridad automáticas o predeterminadas

Para configurar la alta disponibilidad de Internet, puede ajustar la configuración de la VPC. Para conseguir una alta disponibilidad de la API, puede solicitar la cantidad correcta de TPS.

Seguridad de la infraestructura en Amazon WorkSpaces Secure Browser

Como servicio gestionado, Amazon WorkSpaces Secure Browser está protegido por la seguridad de la red AWS global. Para obtener información sobre los servicios AWS de seguridad y cómo se AWS protege la infraestructura, consulte Seguridad AWS en la nube. Para diseñar su AWS entorno utilizando las mejores prácticas de seguridad de la infraestructura, consulte Protección de infraestructuras en un marco de buena AWS arquitectura basado en el pilar de la seguridad.

Utiliza las API llamadas AWS publicadas para acceder a Amazon WorkSpaces Secure Browser a través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Necesitamos TLS 1.2 y recomendamos TLS 1.3.
- Cifre suites con perfecto secreto (PFS), como (Ephemeral Diffie-Hellman) o DHE ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben firmarse con un identificador de clave de acceso y una clave de acceso secreta que esté asociada a un director. IAM También puede utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

WorkSpaces Secure Browser aísla el tráfico del servicio al aplicar la autenticación y autorización AWS SigV4 estándar a todos los servicios. El punto de conexión del recurso del cliente (o punto de conexión del portal web) está protegido por su proveedor de identidades. Puede aislar aún más el tráfico mediante la autorización multifactor y otros mecanismos de seguridad de su proveedor de identidades (IdP).

Todo el acceso a Internet se puede controlar configurando los ajustes de la red, como la VPC subred o el grupo de seguridad. En la actualidad, no se admiten la multitenencia VPC ni los puntos finales (PrivateLink).

Análisis de configuración y vulnerabilidad en Amazon WorkSpaces Secure Browser

WorkSpaces Secure Browser actualiza y corrige las aplicaciones y plataformas según sea necesario en su nombre, incluidos Chrome y Linux. No es necesario aplicar parches ni recopilaciones. Sin embargo, es su responsabilidad configurar WorkSpaces Secure Browser de acuerdo con las especificaciones y directrices, y supervisar el uso de WorkSpaces Secure Browser por parte de sus usuarios. Todas las configuraciones relacionadas con el servicio y los análisis de vulnerabilidades son responsabilidad de WorkSpaces Secure Browser.

Puede solicitar un aumento del límite de los recursos de WorkSpaces Secure Browser, como el número de portales web y el número de usuarios. WorkSpaces Secure Browser garantiza la disponibilidad del servicio y del SLA.

Mejores prácticas de seguridad para Amazon WorkSpaces Secure Browser

Amazon WorkSpaces Secure Browser ofrece una serie de funciones de seguridad que puede utilizar a medida que desarrolla e implementa sus propias políticas de seguridad. Las siguientes prácticas recomendadas son directrices generales y no constituyen una solución de seguridad completa. Puesto que es posible que estas prácticas recomendadas no sean adecuadas o suficientes para el entorno, considérelas como consideraciones útiles en lugar de como normas.

Entre las prácticas recomendadas para Amazon WorkSpaces Secure Browser se incluyen las siguientes:

- Para detectar posibles eventos de seguridad asociados con su uso de WorkSpaces Secure Browser, utilice AWS CloudTrail Amazon CloudWatch para detectar y rastrear el historial de acceso y los registros de procesos. Para obtener más información, consulte Supervisión de Amazon WorkSpaces Secure Browser con Amazon CloudWatch y Registro de llamadas a la API de WorkSpaces Secure Browser mediante AWS CloudTrail.
- Para implementar controles de detección e identificar anomalías, utilice CloudTrail registros y CloudWatch métricas. Para obtener más información, consulte Supervisión de Amazon WorkSpaces Secure Browser con Amazon CloudWatch y Registro de llamadas a la API de WorkSpaces Secure Browser mediante AWS CloudTrail.
- Puede configurar el registro de acceso de usuarios para registrar los eventos de los usuarios. Para obtener más información, consulte the section called “Configuración del registro de acceso de usuario”.

Para evitar posibles eventos de seguridad asociados con el uso de WorkSpaces Secure Browser, siga estas prácticas recomendadas:

- Implemente el acceso con privilegios mínimos y cree funciones específicas para utilizarlas en las acciones de WorkSpaces Secure Browser. Utilice plantillas de IAM para crear un rol de acceso completo o de solo lectura. Para obtener más información, consulte AWS políticas administradas para WorkSpaces Secure Browser.
- Tenga cuidado al compartir los dominios del portal y las credenciales de usuario. Cualquier usuario de Internet puede acceder al portal web, pero no puede comenzar una sesión a menos que tenga credenciales de usuario válidas del portal. Tenga cuidado con la forma, el momento y la persona con quién comparte las credenciales del portal web.

Supervisión de Amazon WorkSpaces Secure Browser

La supervisión es una parte importante del mantenimiento de la fiabilidad, la disponibilidad y el rendimiento de Amazon WorkSpaces Secure Browser y sus demás AWS soluciones. AWS proporciona las siguientes herramientas de monitoreo para vigilar los portales de WorkSpaces Secure Browser y sus recursos, informar cuando algo anda mal y tomar medidas automáticas cuando sea apropiado:

- Amazon CloudWatch monitorea tus AWS recursos y las aplicaciones en las que AWS ejecutas en tiempo real. Puede recopilar métricas y realizar un seguimiento de las métricas, crear paneles personalizados y definir alarmas que le advierten o que toman medidas cuando una métrica determinada alcanza el umbral que se especifique. Por ejemplo, puede CloudWatch hacer un seguimiento del uso de la CPU u otras métricas de sus instancias de Amazon EC2 y lanzar automáticamente nuevas instancias cuando sea necesario. Para obtener más información, consulta la Guía del CloudWatch usuario de Amazon.
- Amazon CloudWatch Logs le permite supervisar, almacenar y acceder a sus archivos de registro desde instancias de Amazon EC2 y otras fuentes. CloudTrail CloudWatch Los registros pueden monitorear la información de los archivos de registro y notificarle cuando se alcanzan ciertos umbrales. También se pueden archivar los datos del registro en un almacenamiento de larga duración. Para obtener más información, consulta la Guía del usuario CloudWatch de Amazon Logs.
- AWS CloudTrailcaptura las llamadas a la API y los eventos relacionados realizados por su AWS cuenta o en su nombre y entrega los archivos de registro a un bucket de Amazon S3 que especifique. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron las llamadas. Para obtener más información, consulte la Guía del usuario de AWS CloudTrail.

Temas

Supervisión de Amazon WorkSpaces Secure Browser con Amazon CloudWatch

Puedes monitorizar Amazon WorkSpaces Secure Browser CloudWatch, que recopila datos sin procesar y los procesa para convertirlos en métricas legibles prácticamente en tiempo real. Estas estadísticas se mantienen durante 15 meses, de forma que pueda obtener acceso a información histórica y disponer de una mejor perspectiva sobre el desempeño de su aplicación web o servicio. También puede establecer alarmas que vigilen determinados umbrales y enviar notificaciones o realizar acciones cuando se cumplan dichos umbrales. Para obtener más información, consulta la Guía del CloudWatch usuario de Amazon.

El espacio de nombres de `AWS/WorkSpacesWeb` incluye las siguientes métricas.

CloudWatch métricas de Amazon WorkSpaces Secure Browser

Métrica	Descripción	Dimensiones	Statistics	Unidades
`SessionAttempt`	El número de intentos de sesión de Amazon WorkSpaces Secure Browser.	`PortalId`	Promedio, suma, máximo, mínimo	Recuento
`SessionSuccess`	El número de inicios de sesión satisfactorios de Amazon WorkSpaces Secure Browser.	`PortalId`	Promedio, suma, máximo, mínimo	Recuento
`SessionFailure`	El número de inicios de sesión fallidos de Amazon WorkSpaces Secure Browser.	`PortalId`	Promedio, suma, máximo, mínimo	Recuento

Métrica	Descripción	Dimensiones	Statistics	Unidades
`GlobalCpuPercent`	El uso de CPU de la instancia de sesión de Amazon WorkSpaces Secure Browser.	`PortalId`	Promedio, suma, máximo, mínimo	Porcentaje
`GlobalMemoryPercent`	El uso de memoria (RAM) de la instancia de sesión de Amazon WorkSpaces Secure Browser.	`PortalId`	Promedio, suma, máximo, mínimo	Porcentaje

> **Note**
>
> Puede ver la estadística métrica «SampleCount» `GlobalMemoryPercent` para `GlobalCpuPercent` determinar el número de sesiones simultáneas activas en su portal. Cada sesión emite los puntos de datos una vez por minuto.

Registro de llamadas a la API de WorkSpaces Secure Browser mediante AWS CloudTrail

WorkSpaces Secure Browser está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio en Amazon WorkSpaces Secure Browser. CloudTrail captura todas las llamadas a la API de Amazon WorkSpaces Secure Browser como eventos. Estas incluyen las llamadas desde la consola de Amazon WorkSpaces Secure Browser y las llamadas en código a las operaciones de la API de Amazon WorkSpaces Secure Browser. Si crea una ruta, puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos de Amazon WorkSpaces Secure Browser. Si no configura una ruta, podrá ver los eventos más recientes en la CloudTrail consola, en el historial de eventos. Con la información recopilada por CloudTrail, puede identificar la solicitud que se realizó a

Amazon WorkSpaces Secure Browser, la dirección IP desde la que se realizó la solicitud, quién la realizó, cuándo se realizó, así como detalles adicionales.

Para obtener más información CloudTrail, consulte la Guía AWS CloudTrail del usuario.

WorkSpaces Información sobre Secure Browser en CloudTrail

CloudTrail está habilitada en su AWS cuenta al crear la cuenta. Cuando se produce una actividad en Amazon WorkSpaces Secure Browser, esa actividad se registra en un CloudTrail evento junto con otros eventos de AWS servicio en el historial de eventos. En el historial de eventos, puede ver, buscar y descargar los eventos recientes de su AWS cuenta. Para obtener más información, consulta Cómo ver eventos con el historial de CloudTrail eventos.

Para obtener un registro continuo de los eventos de su AWS cuenta, incluidos los eventos de Amazon WorkSpaces Secure Browser, puede crear un registro. Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. De manera predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las regiones de AWS. La ruta registra los eventos de todas las regiones de la AWS partición y envía los archivos de registro al bucket de Amazon S3 que especifique. Además, puede configurar otros AWS servicios para analizar más a fondo los datos de eventos recopilados en los CloudTrail registros y actuar en función de ellos. Para más información, consulte los siguientes temas:

- Introducción a la creación de registros de seguimiento
- CloudTrail servicios e integraciones compatibles
- Configuración de las notificaciones de Amazon SNS para CloudTrail
- Recibir archivos de CloudTrail registro de varias regiones y recibir archivos de CloudTrail registro de varias cuentas

Todas las acciones de Amazon WorkSpaces Secure Browser se registran CloudTrail y se documentan en la referencia de la WorkSpaces API de Amazon. Por ejemplo, las llamadas a `DeleteUserSettings` y `ListBrowserSettings` las acciones generan entradas en los archivos de CloudTrail registro. `CreatePortal`

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario lo ayuda a determinar lo siguiente:

- Si la solicitud se realizó con las credenciales raíz o del usuario de IAM.

- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro AWS servicio.

Para obtener más información, consulte el elemento CloudTrail UserIdentity.

Descripción de las entradas del archivo de registro de WorkSpaces Secure Browser

Un rastro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro. Un evento representa una solicitud única de cualquier fuente e incluye información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud y otros detalles. CloudTrail Los archivos de registro no son un registro ordenado de las llamadas a la API pública, por lo que no aparecen en ningún orden específico.

En el siguiente ejemplo, se muestra una entrada de CloudTrail registro que demuestra la `ListBrowserSettings` acción.


```
{
   "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 acceso de usuario

Amazon WorkSpaces Secure Browser permite a los clientes registrar los eventos de la sesión, incluidos el inicio, la finalización y las visitas a la URL. Estos registros se envían a un Amazon Kinesis Data Stream que especifique para su portal web. Para obtener más información, consulte the section called “Configuración del registro de acceso de usuario”.

Guía para usuarios de WorkSpaces Secure Browser

Los administradores utilizan WorkSpaces Secure Browser para crear portales web que se conectan a los sitios web de la empresa, como sitios web internos, aplicaciones web software-as-a-service (SAAS) o Internet. Los usuarios finales utilizan sus navegadores web actuales para acceder a estos portales web con el fin de iniciar una sesión y acceder al contenido.

El siguiente contenido ayuda a guiar a los usuarios finales que desean obtener más información sobre el acceso a WorkSpaces Secure Browser, el inicio y la configuración de una sesión y el uso de la barra de herramientas y el navegador web.

Temas

Compatibilidad de navegadores y dispositivos

Amazon WorkSpaces Secure Browser funciona con el cliente de navegador web NICE DCV, que se ejecuta dentro de un navegador web, por lo que no es necesaria ninguna instalación. El cliente de navegador web es compatible con los navegadores web más comunes, como Chrome y Firefox, y con los principales sistemas operativos de escritorio, como Windows, macOS y Linux.

Para up-to-date obtener más información sobre la compatibilidad con clientes de navegadores web, consulte Cliente de navegador web.

> **Note**
>
> Actualmente, la compatibilidad con webcam solo está disponible en los navegadores basados en Chromium, como Google Chrome y Microsoft Edge. Actualmente, Apple Safari y Mozilla FireFox no admiten cámaras web.

Acceso al portal web

El administrador puede proporcionarle acceso a su portal web con las siguientes opciones:

- Puede seleccionar un enlace desde un correo electrónico o un sitio web y, a continuación, iniciar sesión con sus credenciales de identidad de SAML.
- Puede iniciar sesión en su proveedor de identidades de SAML (como Okta, Ping o Azure) y abrir una sesión con un solo clic desde la página de inicio de la aplicación de su proveedor de SAML (como el panel de usuario final de Okta o el portal Azure Myapps).

Guía de sesiones

Tras iniciar sesión en el portal web, puede abrir una sesión y realizar diversas acciones durante la sesión.

Temas

Inicio de una sesión

Después de iniciar sesión para abrir una sesión, verá el mensaje Abriendo sesión y la barra de progreso. Esto indica que Amazon WorkSpaces Secure Browser está creando una sesión para usted. Entre bastidores, Amazon WorkSpaces Secure Browser crea la instancia, lanza el navegador web gestionado y aplica la configuración del administrador y las políticas del navegador.

Si es la primera vez que inicia sesión en su portal web, verá los iconos con el signo + en azul en la barra de herramientas. Este icono indica que hay disponible un tutorial que le mostrará las características disponibles en la barra de herramientas. Puede usar estos iconos para aprender a:

- Conceder permisos de navegador al micrófono, la webcam y el portapapeles. Para ello, seleccione el icono del candado situado junto al navegador local y cambie el botón a Activado junto al portapapeles, el micrófono y la cámara.

> **Note**
>
> Si habilita los permisos de la webcam al principio de la primera sesión, la cámara se activará brevemente y parpadeará una luz del ordenador. Esto da acceso al navegador local a la webcam.

- Habilite Amazon WorkSpaces Secure Browser para abrir ventanas de monitor adicionales, seleccionando el icono de candado en su navegador y configurando Permitir siempre ventanas emergentes.

Si alguna vez quiere volver a iniciar un tutorial, puede elegir Perfil en la barra de herramientas, Ayuda e Iniciar el tutorial.

Uso de la barra de herramientas

Para mover la barra de herramientas, seleccione la barra más clara en la sección superior de la barra de herramientas, arrástrela hasta la ubicación que desee y, a continuación, suéltela.

Para contraer la barra de herramientas, coloca el cursor sobre ella y selecciona el botón de flecha hacia arriba o haz doble clic en la barra más clara de la sección superior. La vista contraída le proporciona más espacio en la pantalla y acceso con un clic a los iconos más utilizados.

Para aumentar el tamaño de la pantalla, seleccione la ventana del navegador y amplíela. Para aumentar el tamaño de visualización de los iconos y el texto de la barra de herramientas, seleccione la barra de herramientas y amplíela.

Para acercar o alejar la imagen en un dispositivo Windows, sigue estos pasos:

1. Selecciona la barra de herramientas o el contenido web.
2. Pulse Ctrl + + para ampliar o pulse Ctrl + - para alejar el zoom.

Para acercar o alejar la imagen en un dispositivo Mac, sigue estos pasos:

1. Selecciona la barra de herramientas o el contenido web.
2. Pulse Cmd + + para acercar la imagen o pulse Cmd + - para alejarla.

Para fijar la barra de herramientas a la parte superior de la pantalla, seleccione Preferencias, General y Acoplada en el modo Barra de herramientas.

En la siguiente tabla, se incluye una descripción de todos los iconos disponibles en la barra de herramientas:

Icon	Title	Description
	**Windows**	Move between windows or launch additional browser windows.
	**Launch additional monitor window**	Launch an additional monitor window with a separate browser window. Then drag to your secondary monitor.
	**Full screen**	Launch a full screen experience view.
	**Microphone**	Activate mic input for the session.
	**Preferences**	Access the **General** and **Keyboard** menus. From the **General** menu, toggle between light and dark mode, activate the keyboard input selector (for changing the keyboard language), and switch between streaming mode or display resolution. From the **Keyboard** menu, change the option and command key settings (on Mac devices), or activate **Functions** (see below).
	**Profile**	End your session, view performance metrics, access **Feedback** and **Help**, and learn about Amazon WorkSpaces Web. **End Session** ends the Amazon WorkSpaces Web session. **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**
>
> Los iconos del portapapeles y de los archivos están ocultos de forma predeterminada, a menos que el administrador conceda estos permisos. Solo los administradores pueden activar o desactivar el portapapeles y los archivos de un portal web. Si estos iconos están ocultos y necesita acceder a ellos, póngase en contacto con su administrador.

Uso del navegador

Al iniciar la sesión, el navegador muestra la URL de inicio, que es una URL elegida por el administrador. Si el administrador no ha elegido una URL de inicio, verá la nueva pestaña predeterminada de Google Chrome.

Desde el navegador, puede abrir pestañas, abrir ventanas adicionales del navegador (desde el icono de la barra de herramientas de Windows o el menú de tres puntos del navegador), introducir una URL o realizar búsquedas en la barra de direcciones, o ir a sitios web desde los marcadores administrados. Para acceder a los marcadores del portal web, abra la carpeta Marcadores administrados en la barra de marcadores (debajo de la barra de URL) o abra el administrador de marcadores desde el menú de tres puntos situado a la derecha de la barra de direcciones.

Para cambiar el tamaño de la ventana del navegador o moverla, arrastre hacia abajo la barra de pestañas de Chrome. Esto permite disponer de más espacio en la pantalla para varias ventanas del navegador durante la sesión.

> **Note**
>
> Es posible que las características del navegador, como el modo Incógnito, no estén disponibles durante la sesión si el administrador las ha desactivado.

Finalización de una sesión

Para finalizar una sesión, seleccione Perfil y Finalizar sesión. Una vez finalizada la sesión, Amazon WorkSpaces Secure Browser elimina todos los datos de la sesión. Una vez finalizada la sesión, los datos del navegador, como los sitios web abiertos o el historial, o los archivos o datos del Explorador de archivos, dejan de estar disponibles.

Si cierra una pestaña durante una sesión activa, la sesión finaliza después de un periodo de tiempo establecido por el administrador. Si cierra la pestaña y vuelve a visitar el portal web antes de que se agote el tiempo de espera, podrá unirse a la sesión actual y ver todos los datos de la sesión anterior, como los sitios web y los archivos abiertos.

Resolución de problemas

Mi portal Amazon WorkSpaces Secure Browser no me permite iniciar sesión. He recibido un mensaje de error que dice “Your web portal isn't set up yet. Para obtener ayuda, póngase en contacto con su administrador”.

El administrador debe crear el portal con un proveedor de identidades SAML 2.0 para que pueda iniciar sesión. Para obtener ayuda, póngase en contacto con su administrador.

Mi portal no inicia una sesión. He recibido un mensaje de error que dice “Failed to reserve session. There was an internal error. Please retry."

Se ha producido un problema al iniciar la sesión del portal web. Intente iniciar la sesión de nuevo. Si esto continúa, póngase en contacto con el administrador para obtener ayuda.

No puedo usar el portapapeles, el micrófono o la webcam.

Para permitir los permisos del navegador, seleccione el icono de candado situado junto a la URL y active el conmutador azul situado junto a Portapapeles, Micrófono, Cámara y Ventanas emergentes y redireccionamientos para activar estas características.

> **Note**
>
> Si su navegador web no admite la entrada de vídeo o audio, estas opciones no aparecerán en la barra de herramientas.

El audio/vídeo (AV) en tiempo real de Amazon WorkSpaces Secure Browser redirige el vídeo de la cámara web local y la entrada de audio del micrófono a la sesión de streaming del navegador. De esta forma, puede usar sus dispositivos locales para realizar videoconferencias y audioconferencias dentro de su sesión de streaming con navegadores web basados en Chromium, como Google Chrome o Microsoft Edge. Actualmente, las webcam no son compatibles con navegadores que no sean Chromium.

Para obtener información sobre cómo configurar Google Chrome, consulte Usar la cámara y el micrófono.

Mi portal web no abre una ventana de monitor adicional.

Si intenta abrir dos monitores y ve el icono de Ventanas emergentes bloqueadas al final de la barra de direcciones de la parte superior del navegador, seleccione el icono y el botón de opción situado junto a Permitir siempre ventanas emergentes y redireccionamientos. Si se permiten las ventanas emergentes, seleccione el icono del Monitor doble en la barra de herramientas para abrir una nueva ventana, cambie la posición de la ventana en el monitor y arrastre una pestaña del navegador hasta la ventana.

Cuando intento descargar archivos desde el panel Archivos, no ocurre nada.

Si intenta descargar archivos desde el panel Archivos y ve el icono de Ventanas emergentes bloqueadas al final de la barra de direcciones de la parte superior del navegador, seleccione el icono y el botón de opción situado junto a Permitir siempre ventanas emergentes y redireccionamientos. Con las ventanas emergentes permitidas, intente descargar los archivos de nuevo.

Extensión de inicio de sesión único

Amazon WorkSpaces Secure Browser ofrece una extensión para el inicio de sesión único con los navegadores Chrome y Firefox en ordenadores de sobremesa. Si su administrador ha habilitado la extensión, el portal web le pedirá que la instale cuando inicie sesión.

Amazon WorkSpaces Secure Browser creó la extensión para permitir el inicio de sesión único en los sitios web durante la sesión. Por ejemplo, si inicia sesión en su portal web con un proveedor de identidades SAML 2.0 (como Okta o Ping) y visita un sitio web durante la sesión que utiliza el mismo proveedor de identidades, la extensión puede facilitar el acceso al sitio web al eliminar las solicitudes de inicio de sesión adicionales.

No es necesario que instale la extensión para acceder a su portal web, pero esto puede mejorar su experiencia al reducir el número de veces que se le pide que introduzca el nombre de usuario y contraseña.

Al iniciar sesión, la extensión localiza las cookies que el administrador ha incluido para la sesión. Todos los datos que localiza la extensión se cifran en reposo y durante el tránsito. Ninguno de estos datos se almacena en el navegador local. Al finalizar la sesión, se eliminan todos los datos de la sesión (como las pestañas abiertas, los archivos descargados y las cookies enviadas o creadas durante la sesión).

Compatibilidad

La extensión funciona con los siguientes dispositivos:

- Ordenadores portátiles
- Equipos de escritorio

La extensión funciona con los siguientes dispositivos:

- Chrome
- Firefox

Instalación

Cuando inicies sesión en el portal, sigue las instrucciones para instalar la extensión en tu navegador Chrome o Firefox. Solo tiene que hacerlo una vez por cada navegador web.

Si cambia de dispositivo, cambia a un navegador diferente en el mismo dispositivo o elimina la extensión de su navegador local, verá un mensaje para instalar la extensión cuando abra su próxima sesión.

Para garantizar que la extensión funcione como se espera, utilízala en una ventana de navegación normal, en lugar de utilizar la navegación de incógnito (Chrome) o privada (Firefox).

Resolución de problemas

Si tiene la extensión instalada, pero le sigue pidiendo que inicie sesión durante la sesión, siga estos pasos:

1. Asegúrese de tener la extensión Amazon WorkSpaces Secure Browser instalada en su navegador. Si ha eliminado los datos del navegador, es posible que haya eliminado la extensión por accidente.
2. Asegúrese de que no está navegando de incógnito (Chrome) ni de navegación privada (Firefox). Estos modos pueden provocar problemas con las extensiones.
3. Si el problema persiste, póngase en contacto con el administrador del portal para obtener ayuda adicional.

Historial de documentos de la Guía de administración de Amazon WorkSpaces Secure Browser

En la siguiente tabla se describen las versiones de documentación de Amazon WorkSpaces Secure Browser.

Cambio	Descripción	Fecha
Permitir enlaces profundos	Permita que los portales reciban enlaces profundos que conecten a los usuarios con un sitio web específico durante una sesión.	25 de junio de 2024
Actualización de la política administrada	Se agregó una política AmazonWorkSpacesSecureBrowserReadOnly administrada	24 de junio de 2024
Utilice la barra de herramientas para hacer zoom	Puede aumentar el tamaño de la pantalla, los iconos y el texto con la barra de herramientas.	1 de mayo de 2024
Nueva configuración del portal web	Ahora puede especificar el tipo de instancia y el límite máximo de usuarios simultáneos para su portal web.	22 de abril de 2024
CloudWatch métricas	GlobalMemoryPercent Métricas GlobalCpuPercent y métricas añadidas.	26 de febrero de 2024
Configura el filtrado de URL	Puedes usar la Política de Chrome para filtrar las URL a las que pueden acceder los	21 de febrero de 2024

	usuarios desde su navegador remoto.	
Tipos de autenticación de IdP	Puede elegir el tipo de autenticación estándar o el de IAM Identity Center.	5 de febrero de 2024
Habilite la extensión de inicio de sesión único	Puede habilitar una extensión para que sus usuarios finales tengan una mejor experiencia de inicio de sesión en el portal.	28 de agosto de 2023
Guía de usuario para Amazon WorkSpaces Secure Browser	Se agregó contenido para ayudar a guiar a los usuarios finales que desean obtener más información sobre cómo acceder a Amazon WorkSpaces Secure Browser, iniciar y configurar una sesión y usar la barra de herramien tas y el navegador web.	17 de julio de 2023
Control de acceso de IP	WorkSpaces Secure Browser le permite controlar las direcciones IP desde las que se puede acceder a su portal web.	31 de mayo de 2023
Actualización de la política administrada	Política AmazonWor kSpacesWebReadOnly gestionada actualizada	15 de mayo de 2023
Configure la actualización del proveedor de identidades	WorkSpaces Secure Browser ofrece dos tipos de autentica ción: estándar y AWS IAM Identity Center	15 de marzo de 2023

Actualización de la política del navegador	Sección de políticas del navegador actualizada y reestructurada	31 de enero de 2023
Actualización de la política administrada	Política AmazonWorkSpacesWebServiceRolePolicy gestionada actualizada	15 de diciembre de 2022
Lista de permitidos y lista de bloqueados	Especifique la lista de permitidos y la lista de bloqueados para especificar una lista de dominios a los que sus usuarios pueden o no pueden acceder.	14 de noviembre de 2022
Actualización de la política administrada	Política AmazonWorkSpacesWebReadOnly gestionada actualizada	2 de noviembre de 2022
Actualización de la política administrada	Política AmazonWorkSpacesWebServiceRolePolicy gestionada actualizada	24 de octubre de 2022
Registro de acceso de usuario	Configure el registro de acceso de los usuarios para registrar los eventos de los usuarios	17 de octubre de 2022
Actualizaciones de red	Varias actualizaciones de la sección “Redes y acceso”	22 de septiembre de 2022
Actualización de la política administrada	Política AmazonWorkSpacesWebServiceRolePolicy gestionada actualizada	6 de septiembre de 2022

Configure las sesiones de usuario	Configure el editor de métodos de entrada (IME) y la localización durante la sesión	28 de julio de 2022
Actualizaciones de red	Varias actualizaciones de la sección “Redes y acceso”	7 de julio de 2022
Valores de tiempo de espera	Especifique el Tiempo de espera de desconexión en minutos y el Tiempo de espera de desconexión por inactividad en minutos.	16 de mayo de 2022
Políticas administrada actualizada	Se actualizó la política AmazonWorkSpacesWebServiceRolePolicy administrada para añadir el espacio de nombres AWS/Usage a los permisos de la API PutMetricData	6 de abril de 2022
Rol vinculado a servicio	Nueva función vinculada al servicio AWSServiceRoleForAmazonWorkSpacesWeb	30 de noviembre de 2021
Política administrada	Nueva política gestionada AmazonWorkSpacesWebReadOnly	30 de noviembre de 2021
Política administrada	Nueva política AmazonWorkSpacesWebServiceRolePolicy gestionada	30 de noviembre de 2021
Versión inicial	Versión inicial de la Guía de administración de WorkSpaces Secure Browser	30 de noviembre de 2021

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.