Amazon WorkSpaces Web

Guía de administración

Amazon WorkSpaces Web: Guía de administración

Table of Contents

¿Qué es Amazon? WorkSpaces ¿La web?

WorkSpaces La web es de bajo costo y totalmente administrada WorkSpace creado específicamente para facilitar cargas de trabajo seguras y basadas en web. WorkSpaces Web facilita a los clientes proporcionar a sus empleados acceso seguro a sitios web internos y aplicaciones web SaaS sin la carga administrativa de los dispositivos o el software de cliente especializado. WorkSpaces Web proporciona herramientas de políticas sencillas adaptadas a las interacciones de los usuarios, al tiempo que descarga tareas comunes como la administración de la capacidad, el escalado y el mantenimiento de las imágenes del navegador.

WorkSpaces Web ofrece una solución simple de administración y libre de compromisos para ayudar a los trabajadores que solo necesitan acceso a aplicaciones web internas y de SaaS. WorkSpaces El píxel web transmite contenido web desde AWS, por lo que los datos web confidenciales de la empresa nunca residen en dispositivos remotos, lo que reduce el riesgo de exfiltración de datos. La transmisión también proporciona una barrera entre los servidores internos y los dispositivos locales, lo que impide la transmisión de malware transmitido por el dispositivo a los servidores internos. WorkSpaces Web aplica políticas del navegador en su nombre o en el del cliente para aislar a los usuarios de la interfaz del navegador web. Como resultado, no pueden instalar aplicaciones desde Internet ni acceder a los menús del terminal o del sistema operativo durante una sesión.

WorkSpaces La web se administra automáticamente, con imágenes de capacidad, escalado y navegador actualizadas a la última versión de Chrome by AWS. Cada WorkSpaces La sesión web comienza con un navegador Chrome nuevo y completamente actualizado, con la política de navegador de tu empresa aplicada. Al final de la sesión, la instancia se termina, por lo que los datos de la empresa nunca residen en dispositivos remotos. WorkSpaces Web proporciona a los clientes herramientas sencillas para personalizar la experiencia del navegador, como configurar una StartURL o marcadores, y les permite aplicar políticas para el uso del portapapeles, la impresora y la transferencia de archivos. WorkSpaces Web también admite la política empresarial completa de Chrome en Linux, por lo que los clientes pueden utilizar más de 300 políticas de navegador de usuarios y dispositivos.

Introducción al WorkSpaces La web toma dos pasos. En primer lugar, los administradores crean un WorkSpaces Portal web del WorkSpaces Consola web. En segundo lugar, los administradores distribuyen la URL de punto final para que los usuarios puedan acceder a su navegador de streaming, ya sea agregando una puerta de enlace de aplicaciones SAML2.0 existente o enviando la URL por correo electrónico a los usuarios. A continuación, los usuarios acceden al punto final desde su navegador existente, inician sesión con sus credenciales de SAML e inician la sesión desde la URL de inicio establecida por el administrador. Los administradores tienen el control total del contenido al que pueden navegar los usuarios. Pueden establecer políticas de listas permitidas y denegadas de URL con la política de Chrome, o filtrar el tráfico del navegador a través de su VPC. WorkSpaces Web funciona con proveedores de identidad SAML2.0 (como Okta y Ping) y respeta las políticas de aplicación existentes. WorkSpaces Web solo cobra a los clientes mensualmente por los usuarios que inician sesión en el navegador web de streaming y no requiere costos iniciales, licencias ni acuerdos en curso.

Temas

Términos que debe conocer al usar WorkSpaces Web

Para ayudarle a comenzar a usar WorkSpaces web, familiarícese 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 existente para que funcione con WorkSpaces web.

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 los usuarios para que usen WorkSpaces Web en tu IdP.

Documento de metadatos del proveedor de identidades (IdP)

WorkSpaces La web requiere metadatos específicos de su proveedor de identidades (IdP) para establecer la confianza. Puede añadir estos metadatos a WorkSpaces Web mediante la carga de un archivo de intercambio de metadatos descargado de su IdP.

Proveedor de servicios (SP)

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

Documento de metadatos del proveedor de servicios (SP)

Deberá agregar los detalles de metadatos del proveedor de servicios a la interfaz de configuración de su proveedor de identidad (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)

Puedes usar una VPC nueva o existente, las subredes correspondientes y los grupos de seguridad para vincular tu contenido con WorkSpaces web.

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 as a Service (SaaS) para que los usuarios puedan acceder a estos recursos.

Las VPC, las subredes y los grupos de seguridad enumerados se toman de la misma región que WorkSpaces Consola web.

Trust store (Almacén de confianza)

Si un usuario accede a un sitio web a través de WorkSpaces Web recibe un error de privacidad, como NET: :ERR_CERT_INVALID, en el que el sitio podría estar usando un certificado firmado por una entidad de certificación privada (PCA). Es posible que tenga que añadir o cambiar los PCA en 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 permitir que el usuario acceda a ese sitio en WorkSpaces web.

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

Portal web

Un portal web proporciona a los 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 un aumento del límite para más de un portal, póngase en contacto con Support.

Servidor web

El punto de enlace del portal web es el punto de acceso desde el que los usuarios iniciarán el portal web después de iniciar sesión con el proveedor de identidad configurado para el portal.

El punto final está disponible públicamente en Internet y se puede integrar en su red.

Servicios relacionados de

WorkSpaces La web es una capacidad de Amazon WorkSpaces en la cartera de informática para usuarios finales de AWS. En comparación con WorkSpaces y AppStream 2.0, WorkSpaces Web se creó específicamente para facilitar las cargas de trabajo seguras y basadas en la web. WorkSpaces La web se administra automáticamente y AWS aprovisiona y actualiza la capacidad, el escalado y las imágenes a pedido. Por ejemplo, puedes elegir ofrecer un escritorio de Workspace persistente a tus desarrolladores de software que necesitan acceso a recursos de escritorio y Amazon WorkSpaces Web para los usuarios del centro de contacto que solo necesitan acceso a un puñado de sitios web internos y de SaaS (incluidos aquellos alojados fuera de la red) en computadoras de escritorio.

Acceso a Amazon WorkSpaces Web

Acceso de administradores a Amazon WorkSpaces Servidor web a través de AWS WorkSpaces Consola web, SDK, CLI o API. Sus usuarios acceden a él a través de Amazon WorkSpaces Punto de enlace web.

Configuración de Amazon WorkSpaces Web

Antes de poder configurar Amazon WorkSpaces Web Para acceder a sus sitios web internos y aplicaciones SaaS, debe cumplir los siguientes requisitos previos.

Temas

Obtenga una Cuenta de AWS y las credenciales de usuario raíz

A fin de acceder a AWS, debe registrarse para crear una Cuenta de AWS.

Para registrarse en Cuenta de AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga las instrucciones en línea.

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

   Cuando se inscribe en Cuenta de AWS, un Cuenta de AWS usuario raíz se crea. De forma predeterminada, solo el usuario raíz Servicios de AWS tiene acceso a todos los recursos de esa cuenta. Como práctica recomendada de seguridad,asignar acceso administrativo a un usuario administrativo y utilice únicamente el usuario raíz para realizar la ejecución tareas que requieren acceso de usuario raíz.

AWS le enviará un email de confirmación luego de completar 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 My Account (Mi cuenta).

Creación de un usuario de IAM

Si su cuenta ya incluye un usuario de IAM con todos los permisos administrativos de AWS, puede omitir esta sección.

Cuando se crea primero una Cuenta de AWS, se comienza con una identidad de inicio de sesión que tiene acceso completo a todos los recursos y Servicios de AWS de la cuenta. Esta identidad recibe el nombre de usuario raíz de la Cuenta de AWS y se accede a ella iniciando sesión con el email y la contraseña que utilizó para crear la cuenta.

> **Important**
>
> Recomendamos que no utilice el usuario raíz para las tareas cotidianas. Proteja las credenciales del usuario raíz y utilícelas solo para las tareas que este pueda realizar. Para ver la lista completa de las tareas que requieren que inicie sesión como usuario raíz, consulte Tareas que requieren credenciales de usuario raíz en la Referencia general de AWS.

Para crear un usuario administrador, elija una de las siguientes opciones.

Elegir una forma de administrar el administrad	Para	B	También puede
En Centro de identidades de IAM (Recomendado)	Use credenciales a corto plazo para acceder a AWS. Esto se alinea con las prácticas recomendadas de seguridad. Para obtener información sobre las prácticas recomendadas, consulte Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.	Siga las instrucciones en Introducción en la Guía del usuario de AWS IAM Identity Center (successor to AWS Single Sign-On).	Configure el acceso programático mediante Configuración de la AWS CLI para usar AWS IAM Identity Center (successor to AWS Single Sign-On) en la Guía del usuario de AWS Command Line Interface.
En IAM (No recomendado)	Use credenciales a largo plazo para acceder a AWS.	Siga las instrucciones en Creación del primer grupo de usuarios y usuario de administrador de IAM en la Guía del usuario de IAM.	Configure el acceso programático mediante Administración de las claves de acceso de los usuarios de IAM en la Guía del usuario de IAM.

Inicio de sesión como usuario de IAM

Inicie sesión en la consola de IAM; para ello, elija IAM user (Usuario de IAM) y escriba su ID de Cuenta de AWS o el alias de la cuenta. En la siguiente página, ingrese su nombre de usuario y su contraseña de IAM.

> **Note**
>
> Para su comodidad, en la página de inicio de sesión de AWS se utiliza una cookie del navegador para recordar su nombre de usuario de IAM y la información de su cuenta. Si ya ha iniciado sesión como otro usuario, elija el enlace de inicio de sesión debajo del botón para volver a la página principal de inicio de sesión. Desde allí, puede ingresar su ID de Cuenta de AWS o su alias de cuenta, de modo que se lo redirija a la página de inicio de sesión del usuario de IAM y tenga acceso a su cuenta.

Creación de claves de acceso para un usuario de IAM

Las claves de acceso constan de un ID de clave de acceso y una clave de acceso secreta, que se utilizan para firmar las solicitudes de programación que se realizan a AWS. Si no tiene claves de acceso, puede crearlas desde la AWS Management Console. Como práctica recomendada, no utilice la clave de acceso del usuario raíz de la Cuenta de AWS para realizar cualquier tarea en la que no sea necesario. Por el contrario, crear un nuevo usuario de IAM administrador con claves de acceso para usted.

El único momento que puede ver o descargar la clave de acceso secreta es cuando crea las claves. No puede recuperarla más adelante. Sin embargo, puede crear nuevas claves de acceso en cualquier momento. Debe tener permisos para realizar las acciones IAM requeridas. Para obtener más información, consulte Permisos necesarios para acceder a los recursos de IAM en la Guía del usuario de IAM.

Crear claves de acceso para un usuario de IAM

1. Inicie sesión en la AWS Management Console y abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. En el panel de navegación, seleccione Users (Usuarios).
3. Elija el nombre del usuario cuyas claves de acceso que desee crear y, a continuación, elija la pestaña de Security credentials (Credenciales de seguridad).
4. En la sección Access keys (Claves de acceso), haga clic en Create access key (Crear clave de acceso).
5. Para ver el nuevo par de claves de acceso, elija Show (Mostrar). No podrá obtener acceso de nuevo a la clave de acceso secreta cuando este cuadro de diálogo se cierre. Sus credenciales tendrán el aspecto siguiente:
   - ID de clave de acceso: AKIAIOSFODNN7EXAMPLE
   - Clave de acceso secreta: wJalrXUtnFEMI/K7MDENG/bPxRfiCLAVE DE EJEMPLO CY
6. Para descargar el par de claves, elija Download .csv file (Descargar archivo .csv). Almacene las claves en un lugar seguro. No podrá obtener acceso de nuevo a la clave de acceso secreta cuando este cuadro de diálogo se cierre.

   Mantenga las claves en secreto para proteger su Cuenta de AWS y no las envíe nunca por correo electrónico. No las comparta fuera de su organización, aunque reciba una petición que parezca provenir de AWS o Amazon.com. Nadie que represente legítimamente a Amazon pedirá nunca su clave secreta.
7. Cuando descargue el archivo `.csv`, elija Close (Cerrar). Cuando cree una clave de acceso, el par de claves se activa de forma predeterminada y puede utilizar el par de inmediato.

Temas relacionados

- Qué es IAM en la Guía del usuario de IAM
- Credenciales de seguridad de AWS en Referencia general de AWS

Redes y acceso

En los siguientes temas se explica cómo se configura WorkSpaces Instancias de transmisión web para que los usuarios puedan conectarse a ellas. También explica cómo habilitar su WorkSpaces Instancias de transmisión web para acceder a los recursos de VPC, así como a Internet.

Temas

Requisitos de la VPC

Durante WorkSpaces Al crear un portal web, seleccionará una VPC en su cuenta. También elegirá al menos dos subredes privadas en dos zonas de disponibilidad diferentes. Estas VPC y subredes deben cumplir los siguientes requisitos:

- La VPC debe tener un arrendamiento predeterminado. No se admiten las VPC con arrendamiento dedicado.
- Para tener en cuenta la disponibilidad, necesitamos al menos dos subredes creadas en dos zonas de disponibilidad diferentes. Sus subredes deben tener suficiente espacio IP para admitir lo esperado WorkSpaces Tráfico web Debe asignar una IP para el número máximo de sesiones simultáneas. Para obtener más información, consulte Crear y configurar una nueva VPC (p. 7).
- Todas las subredes deben tener una conexión estable con cualquier contenido interno, ya sea ubicado enNube de AWSo en las instalaciones, a las que los usuarios accederán con WorkSpaces Web Edition.

Para casos de uso comunes, recomendamos elegir subredes privadas en diferentes zonas de disponibilidad. Esto significa que, para cada sesión de navegador del usuario final, se asignará a esa sesión una dirección IP privada a la que no se puede acceder directamente desde Internet. También le recomendamos que elija tres subredes en diferentes zonas de disponibilidad para tener en cuenta la disponibilidad y la escalabilidad. Para obtener más información, consulte Crear y configurar una nueva VPC (p. 7).

Si quieres tu WorkSpaces Portal web para tener acceso tanto al contenido público de Internet como al contenido privado de VPC, complete los pasos descritos en(Recomendado) Configure el acceso a Internet en sus subredes privadas (p. 11).

Crear y configurar una nueva VPC

En esta sección se describe cómo usar 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 gateway de Internet y una gateway NAT. También crea una tabla de ruteo personalizada asociada a la subred pública. A continuación, actualiza la tabla de ruteo principal asociada a la subred privada. La gateway NAT se creará automáticamente en la subred pública de la VPC.

Después de usar el asistente para crear una configuración de VPC, agregará una segunda subred privada. Para obtener más información acerca de esta configuración, consulteVPC con subredes privadas y públicas (NAT).

Paso 1: Asignar una dirección IP elástica

Antes de crear su VPC, debe asignar una dirección IP elástica en su WorkSpaces Región web Una vez asignada, puede asociar la dirección IP elástica a su gateway NAT. Con una dirección IP elástica, puede enmascarar un error de su instancia de streaming volviendo a mapear rápidamente la dirección a otra instancia de streaming de su VPC. Para obtener más información, consulteDirecciones 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 tiene una dirección IP elástica, realice los pasos siguientes. Si desea utilizar una dirección IP elástica existente, debe comprobar primero que no esté actualmente asociada 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 Network & Security, seleccione Elastic IPs.
3. Elija Allocate New Address (Asignar nueva dirección) y, a continuación, elija Allocate (Asignar).
4. Anote la dirección IP elástica que se muestra en la consola.
5. En la esquina superior derecha deIPs elásticaspanel, haga clic en el×icono para cerrar el panel.

Paso 2: Crear una nueva VPC

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

Para crear una VPC nueva

1. Abra la consola de Amazon VPC enhttps://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija VPC Dashboard (Panel de VPC).
3. Elija Launch VPC Wizard (Lanzar el asistente de VPC).
4. EnPaso 1: Seleccione una configuración de VPC, eligeVPC con subredes públicas y privadasy, a continuación, elijaSelect.
5. EnPaso 2: VPC con subredes públicas y privadas, configure la VPC de la siguiente manera:
   - En IPv4 CIDR block (Bloque de CIDR IPv4), especifique un bloque de CIDR IPv4 para la VPC.
   - En IPv6 CIDR block (Bloque de CIDR IPv6), deje el valor predeterminado, No IPv6 CIDR Block (Sin bloque de CIDR IPv6).
   - ParaVPC name, escriba un nombre único para la VPC.
   - Configure la subred pública de la siguiente manera:
     - En Public subnet's IPv4 CIDR (CIDR IPv4 de la subred pública), especifique el bloque de CIDR para la subred.
     - En Availability Zone (Zona de disponibilidad), deje el valor predeterminado No preference (Sin preferencia).
     - ParaPublic subnet name, escriba un nombre para la subred. Por ejemplo, **`WorkSpaces Web Public Subnet`**.
   - Configure la primera subred privada de la siguiente manera:
     - En Private subnet's IPv4 CIDR (CIDR IPv4 de la subred privada), especifique el bloque de CIDR para la subred. Tome nota del valor que especifique.
     - En Availability Zone (Zona de disponibilidad), seleccione una zona específica y tome nota de la zona seleccionada.
     - ParaPrivate subnet name, escriba un nombre para la subred. Por ejemplo, **`WorkSpaces Web Private Subnet1`**.
   - En el resto de los campos, mantenga los valores predeterminados cuando proceda.
   - ParaID de asignación de IP elástica, introduzca el valor que corresponde a la dirección IP elástica que creó. Esta dirección se asigna a continuación al gateway NAT. Si no tiene una dirección IP elástica, cree una mediante la consola de Amazon VPC enhttps://console.aws.amazon.com/vpc/.
   - ParaService endpoints, si se requiere un punto de enlace de Amazon S3 para su entorno, especifique uno. Se requiere un punto de conexión S3 para proporcionar a los usuarios acceso a las carpetas de inicio. Este punto de conexión también es necesario para permitir la persistencia de la configuración de la aplicación para los usuarios en una red privada. Para obtener más información,

consulteHabilite y administre las carpetas de inicio para su AppStream 2.0 UsuariosyActive la persistencia de la configuración de la aplicación AppStream 2.0 Usuarios.

Para especificar un endpoint de Amazon S3, haga lo siguiente:

1. Elija Add endpoint (Agregar punto de enlace).
2. ParaServicio, seleccione lascom.amazonaws.***Región***s3de entrada, donde*Región*es elRegión de AWSestás creando tu VPC en.
3. En Subnet (Subred), elija subnet-2 (subred-2).
4. En Policy (Política), deje el valor predeterminado, Full Access (Acceso total).

- En Enable DNS hostnames (Habilitar nombres de host de DNS), deje el valor predeterminado, Yes (Sí).
- En Hardware tenancy (Tenencia de hardware), deje el valor predeterminado, Default (Predeterminado).
- Seleccione Create VPC (Crear VPC).
- La configuración de la VPC puede tardar varios minutos. Una vez creada la VPC, elija Aceptar.

Paso 3: Agregar 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 agregar una segunda subred privada a la VPC. Se recomienda agregar una segunda subred privada en una zona de disponibilidad diferente a la primera subred privada.

Para agregar una segunda subred privada

1. En el panel de navegación, elija Subnets (Subredes).
2. Seleccione la primera subred privada que creó en el paso anterior. En la pestaña Description (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 Create Subnet (Crear subred).
4. ParaName tag, escriba un nombre para la subred privada. Por ejemplo, **`WorkSpaces Web Private Subnet2`**.
5. En VPC, seleccione la VPC que creó en el paso anterior.
6. ParaZona de disponibilidad, selecciona una zona de disponibilidad que no sea la que usas para tu 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 IPv4 CIDR block (Bloque de CIDR IPv4), especifique un rango de bloques de CIDR único para la nueva subred. Por ejemplo, si su primera subred privada tiene un rango de bloques CIDR de IPv4 de**`10.0.1.0/24`**, puede especificar un rango de bloques CIDR de**`10.0.2.0/24`**para la segunda subred privada.
8. Seleccione Create (Crear).
9. Una vez creada la subred, elija Close (Cerrar).

Paso 4: Verifique y asigne un nombre a las tablas de rutas de

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

- La tabla de ruteo asociada a la subred en la que reside su gateway NAT debe incluir una ruta que apunte el tráfico de Internet a un puerto de enlace a Internet. Esto garantiza que la gateway NAT pueda acceder a Internet.
- Las tablas de ruteo asociadas a sus subredes privadas deben configurarse para que sus redes privadas apunten el tráfico de Internet a la gateway NAT. Esto permite a las instancias streaming de sus subredes privadas comunicarse con Internet.

Para verificar y asignar nombres a las tablas de rutas de subred

1. En el panel de navegación, elijaSubredesy, a continuación, seleccione la subred pública que creó. Por ejemplo,WorkSpaces Subred pública Web 2.0.
2. En la pestaña Route Table (tabla de ruteo), elija el ID de la tabla de ruteo. Por ejemplo,rtb-12345678.
3. Seleccione la tabla de ruteo. DebajoNombre, seleccione el icono de edición (lápiz) e introduzca un nombre para la tabla. Por ejemplo, escriba el nombre**`workspacesweb-public-routetable`**. Seleccione la marca de verificación para guardar el nombre.
4. Con la tabla de rutas públicas aún seleccionada, en elRutas, compruebe que hay dos rutas: una para el tráfico local y otra que envía el resto del tráfico a través de 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 de los recursos destinado a direcciones IPv4 dentro del bloque CIDR IPv4 de la subred pública. Este tráfico se enruta localmente dentro de la VPC.
Tráfico destinado al resto de direcciones IPv4 (por ejemplo, 0.0.0/0)	Saliente (IGW-ID)	El tráfico destinado a todas las demás direcciones IPv4 se enruta a la puerta de enlace de Internet (identificada por IGW-ID) que creó el asistente de VPC.

5. En el panel de navegación, elija Subnets (Subredes). A continuación, seleccione la primera subred privada que creó (por ejemplo,**`WorkSpaces Web Private Subnet1`**).
6. En elTabla de ruteopestaña, elija el ID de la tabla de rutas.
7. Seleccione la tabla de ruteo. DebajoNombre, seleccione el icono de edición (lápiz) e introduzca un nombre para la tabla. Por ejemplo, escriba el nombre**`workspacesweb-private-routetable`**. Seleccione la marca de verificación para guardar el nombre.
8. En la pestaña Routes (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 de subred pública se dirige localmente dentro de la VPC.
Tráfico destinado al resto de direcciones IPv4 (por ejemplo, 0.0.0/0)	Saliente (NAT-ID)	El tráfico destinado a todas las demás direcciones IPv4 se enruta a la puerta de enlace NAT (identificada por el NAT ID).
Tráfico destinado a los buckets de S3 (aplicable si especificó un punto final de S3) [PL-ID (com.amazonaws.region.s3)]	Almacenamiento (VPCE-ID)	El tráfico destinado a los buckets de S3 se enruta al punto final de S3 (identificado por VPC-ID).

9. En el panel de navegación, elija Subnets (Subredes). A continuación, seleccione la segunda subred privada que creó (por ejemplo,**`WorkSpaces Web Private Subnet2`**).
10. En elTabla de ruteotab, compruebe que la tabla de rutas seleccionada sea la tabla de rutas privadas (por ejemplo,**`workspacesweb-private-routetable`**). Si la tabla de rutas es diferente, elijaEditary selecciona tu tabla de rutas privadas en su lugar.

(Recomendado) Configure el acceso a Internet en sus subredes privadas

Para agregar una gateway NAT a un VPC existente

Si quieres tu WorkSpaces Portal web para tener acceso tanto al contenido público de Internet como al contenido privado de VPC, siga estos pasos:

> Note
>
> Si ya configuró una VPC, complete los siguientes pasos para agregar una puerta de enlace NAT a su VPC. Si necesita crear una VPC nueva, consulte Crear y configurar una nueva VPC (p. 7).

1. Para crear su puerta de enlace NAT, siga los pasos descritos enCreación de una gateway NAT. Asegúrese de que esta puerta de enlace de NAT tenga conectividad pública y se encuentre en una subred pública de su VPC.
2. Debe especificar 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 las fallas. Para obtener información sobre cómo crear una segunda subred privada, consulte the section called “Paso 3: Agregar una segunda subred privada” (p. 9).
3. Actualice la tabla de ruteo asociada a sus subredes privadas para que sus redes privadas apunten el tráfico vinculado a Internet a la gateway NAT. Esto permite a las instancias streaming de sus subredes privadas comunicarse con Internet. Para obtener información sobre cómo asociar una tabla de rutas a una subred privada, complete los pasos deConfigurar tablas de enrutamiento.

Interconexión de VPC

Cada WorkSpaces La instancia de transmisión web tiene una interfaz de red de cliente que proporciona conectividad a los recursos de la VPC, así como a Internet.

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

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

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

Conexión cliente/usuario

WorkSpaces La Web está configurada para rutear conexiones de streaming a través de Internet público. Se requiere conectividad a Internet para autenticar a los usuarios y entregar los activos web que WorkSpaces La web requiere funcionar. Para que este tráfico sea posible, debe permitir los dominios enumerados en Dominios permitidos (p. 12).

En los siguientes temas se proporciona información acerca de cómo habilitar las conexiones de usuario a WorkSpaces Web Edition.

Temas

Requisitos de dirección IP y puerto

Para acceder WorkSpaces Las instancias web y los dispositivos de usuario requieren acceso saliente en los siguientes puertos:

- Puerto 443 (TCP)
  - El puerto 443 se usa para la comunicación HTTPS entre los dispositivos de usuario y las instancias de transmisión cuando se utilizan los puntos finales 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. por lo que debe asegurarse de que el tráfico de retorno a este puerto está permitido.
  - Este puerto debe estar abierto a los dominios requeridos que figuran enDominios permitidos (p. 12).
  - AWSpublica sus rangos de direcciones IP actuales, incluidos los rangos que la gateway de sesión y CloudFront los dominios pueden resolverse en formato JSON. Para obtener información sobre cómo descargar el archivo .json y ver los rangos actuales, consulteAWSIntervalo de direcciones IP. O, si está utilizandoAWS Tools for Windows PowerShell, puede acceder a la misma información mediante elGet-AWSPublicIpAddressRange PowerShellcomando. Para obtener más información, consulte Querying the Public IP Address Ranges for AWS.
- (Opcional) Puerto 53 (UDP)
  - El puerto 53 se usa para la comunicación entre los dispositivos de usuario y los 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 el usuario pueda acceder a la WorkSpaces Servicio web desde su navegador local, debe agregar los siguientes dominios y direcciones IP a la lista de permitidos de la red desde la que el usuario intenta acceder al servicio.

La*{Región}*debe sustituirse el nombre de la operación por el siguienteRegión de AWS. Por ejemplo, s3.*{región}*.amazonaws.com debería ser s3.eu-west-1.amazonaws.com si es para Europa (Irlanda) (eu-west-1).

Categoría	Dominios o direcciones IP
WorkSpaces Recurso de transmisión web	s3.*{región}*.amazonaws.com s3.amazonaws.com appstream (2).*{región}*.aws.amazon.com *.amazonappstream.com *.shortbread.aws.dev

Categoría	Dominios o direcciones IP
WorkSpaces Web WebApp Activo	*.workspaces-web.com
WorkSpaces Autificación web	*.auth.*{región}*.amazoncognito.com identidad cognitiva.*{región}*.amazonaws.com cognito-idp.*{región}*.amazonaws.com *.cloudfront.net
WorkSpaces Estadísticas e informes web	*.ejecute-api.*{región}*.amazonaws.com unagi-na.amazon.com

En función del proveedor de identidad configurado, es posible que también tenga que permitir la lista de dominios adicionales. Revise la documentación de su IdP para identificar qué dominios debe permitir enumerar en orden. WorkSpaces Web para usar ese proveedor. Si utiliza el Centro de identidad de IAM, consulteRequisitos previos de IAM Identity Centerpara obtener más información.

Review policies

Para ofrecer una experiencia de navegación más segura a sus usuarios, WorkSpaces Web aplica varias políticas de navegador además de las que usted especifique. La siguiente es la lista de políticas que aplicamos, en formato JSON:

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

Las siguientes políticas anularán cualquier valor existente que haya establecido:

- DefaultDownloadDirectory
- DownloadDirectory
- DownloadRestrictions

Las siguientes políticas se combinarán con cualquier valor existente que haya establecido:

- Lista de URL permitidas
- Lista de URL bloqueadas

Configure su proveedor de identidad SAML 2.0

Siga estos pasos para aprender a integrar Amazon WorkSpaces Web con los siguientes proveedores de identidad SAML 2.0.

Temas

Configure IAM Identity Center como su IdP

En los pasos siguientes se describe cómo se configuraAWS IAM Identity Center (successor to AWS Single Sign-On)para usar con WorkSpaces Web Edition. Esta configuración no incluye ninguna función avanzada, como la compatibilidad con los servicios de directorio.

Si es la primera vez que visita el Centro de identidad de IAM, se le pedirá que habilite el servicio, lo que implica la configuraciónAWS Organizations. Para obtener más información, consulte¿Qué es AWS Organizations?.

Para configurar IAM Identity Center como IdP

1. En la consola de IAM Identity Center, elijaUsuarios,Añadir usuarioe introduzca los detalles del usuario.

   Note

   La dirección de correo electrónico ingresada se utilizará para enviar solicitudes de restablecimiento de contraseña.
2. (Opcional) ElijaSiguiente: Groups, cree un grupo nuevo al que asignar este usuario y elijaAñadir usuario.
3. ElegirAplicaciones,Agregar una nueva aplicación, yAgregar una aplicación SAML 2.0 personalizada.
4. En otra pestaña, desde el WorkSpaces Consola web, siga los pasos 1 a 3 dePaso 1: Creación de un portal web (p. 19)para descargar el archivo de metadatos del proveedor de servicios (SP). Mantén esta pestaña abierta.
5. Vuelva a la consola de IAM Identity Center y aMetadata de, cargue el archivo de metadatos SP descargado.

6. En lasMetadata IAM Identity Centersección, elijaDescargarpara el archivo de metadatos SAML de IAM Identity Center y, a continuación, seleccioneGuardar cambiospara terminar de crear la aplicación IAM Identity Center.
7. En la otra pestaña, desde la WorkSpaces Consola web, siga el paso 5 y los pasos restantes dePaso 1: Creación de un portal web (p. 19)para cargar el archivo de metadatos del IdP y terminar de crear el portal web.
8. Para configurar la aplicación IAM Identity Center para los usuarios, siga estos pasos en la consola de IAM Identity Center:

    1. ElegirMapeo de atributose ingrese los campos siguientes:
        - ParaAtributo de usuario en la aplicación, escribaAsunto.
        - ParaSe asigna a este valor de cadena o atributo de usuario en el Centro de identidades de IAM, escriba$ {usuario:email}.
        - ParaFormato, escribaEmailAddress.
    2. ElegirUsuarios asignadospara conceder acceso a un usuario individual o a todo un grupo.
9. Siga los pasos dePaso 2: Prueba del punto final (p. 22)para validar la configuración.

Configure Azure AD como su IdP

En los pasos siguientes se describe cómo se configura Azure AD para usarlo con WorkSpaces Web Edition. Esta configuración no incluye funciones avanzadas, como la conexión a un controlador de Active Directory local. Debe tener una cuenta de Azure para completar estos pasos.

Para configurar Azure AD como su IdP

1. Abra la consola de Microsoft Azure.
2. Para configurar usuarios y grupos, siga estos pasos:

    1. En la página de información general de su directorio, elijaUsuarios,Nuevo usuario,Crear usuarioy rellene los campos de usuario y la contraseña obligatorios.
    2. Si desea administrar el acceso de los usuarios a WorkSpaces Web con grupos, elige un grupo.
    3. Seleccione Create (Crear).
3. Para crear una aplicación empresarial personalizada, siga estos pasos:

    1. En la página de información general de su directorio, elijaAplicaciones empresariales,Nueva aplicación, y luegoCrear su propia aplicación.
    2. Escriba el nombre de la aplicación de prueba y elijaIntegre cualquier otra aplicación que no encuentre en la galería (que no sea de la galería).
4. Para asignar usuarios y grupos, sigue estos pasos:

    1. En la página de información general de su aplicación empresarial, elijaAsignar usuarios y grupos,Agregar usuario o grupo, yUsuarios y grupos.
    2. Elige tus usuarios y, a continuación, eligeSelectyAsignar.
5. Para configurar el inicio de sesión único, siga estos pasos:

    1. En la página de información general de su aplicación empresarial, en el punto 2 delIntroducciónsección (sección)Configurar inicio de sesión único), elijaIntroducción.
    2. Para el método de inicio de sesión único, elijaSAML.
    3. En otra pestaña, desde el WorkSpaces Consola web, siga los pasos 1 a 3 dePaso 1: Creación de un portal web (p. 19)para descargar el archivo de metadatos del proveedor de servicios. Mantén esta pestaña abierta.
    4. ElegirCargar archivo metadatos, elija el archivo que descargó en el paso anterior y elijaAñadir.

5. DebajoConfiguración básica de SAML, compruebe que elIdentity (IDyURL de Assertion Consumerlos campos están llenos y eligeGuardar.
6. DebajoCertificado de firma SAML, descargue lasMetadata de federación. Es posible que el archivo tarde un par de minutos en generarse y descargarse.
7. En la otra pestaña, desde la WorkSpaces Consola web, siga el paso 5 y los pasos restantes dePaso 1: Creación de un portal web (p. 19)para cargar el archivo de metadatos del IdP y terminar de crear el portal web.

6. Siga los pasos dePaso 2: Prueba del punto final (p. 22)para validar la configuración.

Configura Okta como tu IdP

En los pasos siguientes se describe cómo se configura Okta para usarlo con WorkSpaces Web Edition. Esta configuración no utiliza ninguna función avanzada, como la URL de metadatos del IdP dinámico ni el envío de una plantilla de aplicación para agregarla a la red de integración de Okta. Debes tener Okta configurado para poder continuar.

Para configurar Okta como su IdP

1. Para crear una integración de aplicaciones entre Okta y Workspaces Web, siga estos pasos:
   1. Desde la consola de Okta, seleccionaAplicaciones,Aplicaciones, yCrear la integración de aplicaciones.
   2. ElegirSAML 2.0,Próximo, introduzca unNombre de la aplicacióny, a continuación, elijaPróximo.
   3. En otra pestaña, desde el WorkSpaces Consola web, siga los pasos 1 a 3 dePaso 1: Creación de un portal web (p. 19)aMostrar valores de metadatos individualesdel archivo de metadatos del proveedor de servicios. Mantén esta pestaña abierta.
   4. Escriba los valores siguientes para OktaConfiguración SAML:
      - ParaURL de inicio de sesión único, introduzca elURL DE ACSdel paso anterior.
      - ParaURI de audiencia (ID de entidad SP), introduzca elID de entidad SPdel paso anterior.
      - CambioFormato de ID de nombreaEmailAddress.
      - DejarUsuario de la aplicaciónsegún lo especificado.
   5. ElegirPróximo, especifique si es cliente o socio cuando se le solicite y elijaAcabado.
2. Recupere y cargue el archivo XML de metadatos del IdP desde Okta.
   1. En la consola de Okta de la nueva aplicación, en elIniciar sesiónpestaña, botón derechoMetadata de identidad.
   2. ElegirGuardar enlace como...e introduzca un nombre para el archivo de metadatos del IdP que termina en **`.xml`**.
   3. En la otra pestaña, desde la WorkSpaces Consola web, siga el paso 5 y los pasos restantes dePaso 1: Creación de un portal web (p. 19)para cargar el archivo de metadatos del IdP desde Okta y terminar de crear el portal web.
3. (Opcional) Configure un usuario de prueba.
   1. Desde el panel de control de Okta, expande la barra lateral y seleccionaDirectorio,Gente, yAgregar persona.
   2. Rellene los campos del formulario y elijaGuardar.
4. Asigne un usuario de prueba a la aplicación.
   1. En la consola de Okta de tu nueva aplicación, seleccionaAsignaciones,Asignar, yAsignar a personas.
   2. Asigna a tu usuario de prueba, a ti mismo o a ambos con las credenciales configuradas durante el registro en Okta y eligeGuardar y volveryTerminado.

5. Siga los pasos dePaso 2: Prueba del punto final (p. 22)para validar la configuración.

Configurar PingIdentity como su proveedor de IdP

En los pasos siguientes se describe cómo se configura PingIdentity para usar con WorkSpaces Web Edition. Debe tener PingIdentity configurado para continuar.

Para configurar PingIdentity como su proveedor de IdP

1. Configure un entorno. (Omita este paso si desea utilizar el entorno de administrador para la integración SAML).
    1. Desde las PingIdentity consola, elijaAgregar entorno,Solución para el cliente,Próximo, y luegoPróximo.
    2. Para ver las opciones de implementación de su licencia, introduzca elEnvironment namey selecciona elGenere poblaciones de muestra y usuarios en este entornocasilla de verificación.
    3. Elija Finalizar.
2. En otra pestaña, desde el WorkSpaces Consola web, siga los pasos 1 a 3 dePaso 1: Creación de un portal web (p. 19)para descargar el archivo de metadatos del proveedor de servicios. Mantén esta pestaña abierta.
3. Configure SAML para su PingIdentity entorno del cliente.
    1. Desde las PingIdentity página de inicio, seleccione el entorno en el que desea configurar SAML.
    2. En el menú de navegación izquierdo, elijaConexiones.
    3. En la esquina superior derecha, elijaAñadir aplicación.
    4. DebajoSeleccione un tipo de aplicación, seleccione la primera opción para la aplicación web y elijaConfigurarpara elSAMLtipo de conexión.
    5. Escriba unaNombre de la aplicacióny eligePróximo.
    6. SobreConfigurar la conexión SAML, eligeElegir archivoy seleccione los metadatos SAML del SP que descargó en el paso 2.
    7. Vea los valores y, paraDURACIÓN DE LA VALIDEZ DE LA AFIRMACIÓN (EN SEGUNDOS), introduzca el tiempo que un usuario puede permanecer conectado, en segundos.
    8. ElegirGuardar y continuary, a continuación, elijaSave (Guardar).
4. Recupera los metadatos del IdP de la aplicación Ping y cárgal WorkSpaces Web Edition.
    1. Navegue hasta su entorno y elijaConexionesyAplicaciones.
    2. Amplíe la información de su aplicación yConfiguración.
    3. DebajoDetalles de conexión, elige elDescargar Metadatabotón para descargar los metadatos del IdP.
    4. En la otra pestaña, desde la WorkSpaces Consola web, siga el paso 5 y los pasos restantes dePaso 1: Creación de un portal web (p. 19)para cargar el archivo de metadatos del IdP desde Ping y terminar de crear su portal web.
5. Añada un usuario de prueba.
    1. Desde las PingIdentity consola, elijaIdentidades de,Añadir usuario, rellene los campos y elijaGuardar.
    2. El usuario se asignará a unPoblaciónque generaste automáticamente o una población preexistente. Si no tiene población, elijaPoblacióny cree una.
    3. ElegirRestablecer contraseña,Generar contraseñay selecciona el botón del ojo para ver la contraseña. Copie la contraseña para validarla más adelante y elijaGuardar.
6. Validar.

1. Si desea restringir los usuarios del WorkSpaces Aplicación web para un grupo determinado, seleccione los grupos a los que conceder acceso en la aplicación PingAccesoTabulador.
2. Para activar la aplicación Ping paraAcceso de usuarios, navegue hasta su entorno y elijaConexionesyAplicaciones.
3. Entre lasNombre de la aplicaciónyPromedio de inicios de sesión diarios, cambia la aplicación aEnabledpara el acceso de los usuarios.
4. Siga los pasos dePaso 2: Prueba del punto final (p. 22)para validar la configuración.

Introducción a Amazon WorkSpaces Web

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

> Note
>
> Para solicitar un aumento del límite para más de un portal, póngase en contacto con el servicio de asistencia con suAWSID de cuenta, número de portales a solicitar y región.

Este proceso suele tardar cinco minutos con el asistente de creación del portal web, además de hasta 15 minutos para que el portal se conviertaActivo.

No hay costos asociados con la creación de un portal web. WorkSpaces Ofertas web pay-as-you-goprecios, incluido un precio mensual bajo para los usuarios que utilizan el servicio de forma activa. No hay costos iniciales, licencias ni compromisos a largo plazo.

Temas

Requisitos previos

Antes de comenzar, asegúrese de que ha completado todos los requisitos previos necesarios. Para obtener más información, consulte Configuración de Amazon WorkSpaces Web (p. 4).

Paso 1: Creación de un portal web

Para crear un portal web, siga estos pasos.

Si ya has completado estos pasos enConfigure su proveedor de identidad SAML 2.0 (p. 14), puede omitir esta sección e ir aPaso 2: Prueba del punto final (p. 22).

1. Abra el WorkSpaces Consola web enhttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. ElegirWorkSpaces Web,Portal weby, a continuación, elijaCreación de un portal web.
3. En laPaso 1: Especificar conexión de red, complete los siguientes pasos para conectar la VPC al portal web y configurar la VPC y las subredes.

   > Note
   >
   > Puede optar por omitir este paso por ahora y completarlo después de crear un portal web, en el paso 13 a continuación.

   1. ParaDetalles de la red, elija una VPC.

2. Elija al menos dos subredes privadas que cumplan todos los requisitos. Para obtener más información, consulte Redes y acceso (p. 6).
3. Elija un grupo de seguridad.

4. En laPaso 2: Configuración del portal web, complete los siguientes pasos para personalizar la experiencia de navegación de los usuarios cuando inicien una sesión y, a continuación, seleccionePróximo:

   Note

   WorkSpaces Web aplica políticas de navegador adicionales para aislar a los usuarios de las sesiones de la interfaz del navegador, en nombre del cliente. Para obtener más información, consulte Review policies (p. 13).

   1. DebajoDetalles del portal web, paraNombre que mostrar, introduzca un nombre identificable para su portal web.
   2. DebajoConfiguración de política, ingrese los siguientes detalles:
      - ParaOpciones de la política, eligeVisual editor (Editor visual)oCargar archivo JSONpara elegir cómo proporcionar los detalles de configuración de políticas para su portal web. WorkSpaces Web incluye soporte para las políticas de Chrome Enterprise, y puedes añadir y administrar políticas mediante un editor visual o una carga manual de archivos de políticas. Puede cambiar de una de las dos opciones en cualquier momento.

        Cuando cargue un archivo de políticas, verá las políticas disponibles en el archivo. Sin embargo, no todas las políticas se pueden editar en el editor visual. Es posible que tenga que editar manualmente los datos JSON para realizar cambios en una política.
      - ParaURL de inicio (opcional), puede introducir un dominio para usarlo como página de inicio cuando los usuarios inicien su navegador. La VPC debe tener una conexión estable a esta URL.
      - ParaMarcadores del navegador: opcionales, puede especificar elNombre que mostrar,Dominio, yCarpetapara cualquier marcador que quiera que vean los usuarios en el navegador y elijaAgregar marcador.

        Note

        Dominioes un campo obligatorio para marcadores del navegador.

5. En laPaso 3: Seleccionar configuración de usuario, complete los siguientes pasos para elegir a qué funciones pueden acceder los usuarios desde la barra de navegación superior durante la sesión y, a continuación, seleccionePróximo:

   1. ParaPortapapeles, eligeDiscapacitadooEnabled.
   2. DebajoTransferencia de archivos, eligeDiscapacitadooEnabled.
   3. ParaImprimir en un dispositivo local, eligePermitidooNo permitido.
   4. ParaDetalles de sesión de usuario, especifique lo siguiente:
      - En Disconnect timeout in minutes (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 termina la sesión, no se aplica el tiempo de espera de desconexión. En cambio, se solicita al usuario que guarde los documentos abiertos y, a continuación, se desconecta inmediatamente de la instancia de streaming. La instancia que estaba utilizando el usuario termina.
      - En Idle disconnect timeout in minutes (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 Disconnect timeout in minutes (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 Disconnect timeout in minutes (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 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 Idle disconnect timeout in minutes (Tiempo de espera de desconexión de inactividad en minutos), se desconectan.

6. En laPaso 4: Configuración del proveedor de identidaddel asistente de creación, seleccioneDescargar archivo de metadatospara descargar el documento de metadatos del proveedor de servicios (SP) que cargará en su proveedor de identidad (IdP) en el siguiente paso. Debe cargar el archivo de metadatos del proveedor de servicios en su IdP. De lo contrario, los usuarios no podrán iniciar sesión.

   Note

   WorkSpaces Web admite los flujos de inicio de sesión iniciados por el proveedor de servicios (iniciados por el SP) con su IdP compatible con SAML 2.0. WorkSpaces Web aún no admite los flujos de inicio de sesión iniciados por el proveedor de identidad (iniciado por el proveedor de identidad)

7. Abre otra pestaña en tu navegador y completa los siguientes pasos para tu IdP:

   1. Cargue el documento de metadatos del SP que descargó en el paso anterior a su IdP. Debes subir el archivo a tu IdP o copiar y pegar los valores de los metadatos (para proveedores como Okta). Los detalles de este proceso de configuración varían de un proveedor a otro. Consulte la documentación de su proveedor para obtener ayuda detallada sobre cómo agregar los detalles proporcionados por WorkSpaces Web a su configuración.
   2. Otorga acceso a los usuarios de tu IdP para que usen WorkSpaces web ().
   3. Descargue un archivo de intercambio de metadatos de su IdP. Cargará estos metadatos en WorkSpaces En el siguiente paso.

8. Regrese a la WorkSpaces consola web y en laConfiguración del proveedor de identidadpágina del asistente de creación, enDocumento de metadatos IdP de identidades, eligeElegir archivopara cargar el archivo de metadatos con formato XML del proveedor de identidad que descargó en el paso anterior. WorkSpaces La Web requiere estos metadatos de su IdP para establecer la confianza. Cuando haya terminado, elija Next.

   Note

   WorkSpaces La web`subjectoNameID`para asignarlo y configurarlo en la aserción de SAML dentro de la configuración de tu IdP. El proveedor de IdP puede crear estas asignaciones automáticamente. Si estas asignaciones no están configuradas correctamente, es posible que un usuario que intente iniciar sesión en el portal web no pueda iniciar una sesión.

9. En laPaso 5: Revisión y lanzamiento, revise la configuración que ha seleccionado para el portal web. Puede elegirEditarpara realizar cualquier cambio, o puede cambiar esta configuración más adelante desde laPortal webde la consola.
10. Cuando haya terminado, elijaPortal web.
11. Para ver el estado de su portal web, elijaPortal web, elige tu portal y eligeConsultar detalles.

    Un portal web puede tener uno de los siguientes estados:

- Incompleto- La configuración del portal web carece de la configuración del proveedor de identidad requerida.
- Pendiente- El portal web está aplicando cambios a su configuración.
- Activo- El portal web está listo y disponible para su uso.

12. Espere hasta 15 minutos a que el portal se convierta enActivo.
13. Si se saltó el paso 3 anterior, siga estos pasos para configurar las subredes:

    1. ElegirPortal web, seleccione el portal y, a continuación, seleccioneEditar.
    2. EnDetalles de la red, elija una VPC con puntos de enlace de VPC.
    3. Elija al menos dos subredes privadas con los tres puntos de enlace de VPC que creó anteriormente. Asegúrese de que estén en zonas de disponibilidad diferentes.
    4. ElegirGuardary espere hasta 15 minutos a que los cambios surtan efecto.

Paso 2: Prueba del punto final

Una vez creado un portal web, podrá iniciar sesión en WorkSpaces Punto final web para navegar por sus sitios web conectados como lo haría un usuario final.

Si ya has completado estos pasos enConfigure su proveedor de identidad SAML 2.0 (p. 14), puede omitir esta sección e ir aPaso 4: Distribuir el punto final (p. 25).

1. Abra el WorkSpaces Consola web enhttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. ElegirWorkSpaces Web,Portal web, elija el portal web y, a continuación, seleccioneConsultar detalles
3. DebajoPunto web, vaya a la URL especificada para el portal. El punto de enlace del portal web es el punto de acceso desde el que los usuarios iniciarán el portal web después de iniciar sesión con el proveedor de identidad configurado para el portal. Está disponible públicamente en Internet y se puede integrar en su red.
4. En la WorkSpaces Página de inicio de sesión web, elijaIniciar sesión,SAMLe introduzca sus credenciales de SAML.
5. Cuando veas elSe está preparando su sesiónpágina, tu WorkSpaces Se está iniciando la sesión web. No cierre ni salga de esta página.
6. Se inicia el navegador web y se muestra la URL de inicio y cualquier otro comportamiento adicional configurado a través de la configuración de la directiva del navegador.
7. Ahora puede navegar a los sitios web conectados seleccionando enlaces o introduciendo las URL en la barra de direcciones.

Paso 3: Configuración de sesiones de usuario (opcional)

Después de configurar un portal web y haberlo probado, puede personalizarlo configurando las funciones a las que los usuarios acceden durante sus sesiones.

Este paso es opcional. Si no necesita personalizar las siguientes funciones, puede pasar al paso siguiente.

Temas

- Configuración del Editor de métodos de entrada (IME) (p. 23)
- Configurar la localización durante la sesión (p. 23)

Configuración del Editor de métodos de entrada (IME)

Un Editor de métodos de entrada (IME) es una utilidad que proporciona opciones al usuario final para introducir texto en idiomas que utilizan una distribución de teclado distinta del teclado QWERTY. Los IME ayudan a los usuarios a escribir texto en idiomas con conjuntos de idiomas más grandes y complejos, como el japonés, el chino y el coreano. WorkSpaces Las sesiones web incluyen soporte IME de forma predeterminada. Los usuarios pueden seleccionar idiomas alternativos en la barra de herramientas IME de la sesión o mediante métodos abreviados de teclado.

Los siguientes idiomas son compatibles actualmente con WorkSpaces IME de la web:

- Inglés
- Chino simplificado (pinyin)
- Chino tradicional (Bopomofo)
- Japonés
- Coreano

Para seleccionar un idioma de la barra de herramientas 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 mostraráen, para inglés.
2. En el menú desplegable, elija el idioma que desee.
3. En el submenú que aparece después de elegir un idioma, selecciona detalles adicionales del idioma.

Para seleccionar un idioma mediante métodos abreviados de teclado, utilice lo siguiente:

- Todas las IME
  - Para adelantar el IME (o pasar a la distribución de teclado derecha), pulseShift+Control+Left Alt.
- Japonés
  - Para elegir Hiragana, pulseF6.
  - Para elegir Katakana, pulsaF7.
  - Para elegir latín, pulsaF10.
  - Para elegir Wide Latin, pulseF9.
  - Para seleccionar Entrada directa, pulse ALT +, ALT+@, Zenkaku Hankaku.
- Coreano
  - Para elegir Hangul, pulsaShift+Space.
  - Para elegir Hanja, pulseF9.

Para quitar la barra de herramientas y el menú de IME del WorkSpaces SwebAWS Support.

Configurar la localización durante la sesión

Cuando un usuario inicia una sesión, WorkSpaces Web detecta la configuración de idioma y zona horaria del navegador local del usuario y los 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 en la ubicación del usuario.

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

- Alemán
  - de: alemán
  - de-AT — alemán (Austria)
  - de-DE: alemán (Alemania)
  - de-CH: alemán (Suiza)
  - De-li: alemán (Liechtenstein)
- Inglés
  - es — inglés
  - en-AU — Inglés (México)
  - en-CA — Inglés (Canadá)
  - en-IN — Inglés (India)
  - en-NZ — Inglés (Nueva Zelanda)
  - en-ZA — Inglés (África Austral)
  - es-ES — Inglés (Reino Unido)
  - en-US — Inglés (Estados Unidos)
- Español
  - en 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. LaForcedLanguagesen la configuración del navegador del portal web. Para obtener más información, consulteForcedLanguages.
2. La configuración de idioma del navegador local del usuario final.
3. El valor predeterminado,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 la zona horaria no es válida, se utiliza UTC.

Los siguientes componentes de WorkSpaces Localización de soporte web:

- WorkSpaces Página de inicio de sesión web
- WorkSpaces Mensajes de estado del portal web (incluidos los mensajes de carga y los errores)
- Browser Chrome
- System (Sistema)Contextomenú yGuardar comoWindow

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

- En Chrome, seleccionaConfiguración, eligelenguajesy, a continuación, ordena los idiomas según tus preferencias.
- En Firefox, eligeConfiguración,General,Idiomay seleccione el idioma en el menú desplegable.
- En Edge, eligeConfiguración, eligelenguajesy, a continuación, ordena los idiomas según tus preferencias.

Paso 4: Distribuir el punto final

Cuando esté listo para que los usuarios comiencen a usar WorkSpaces Web para acceder a su navegador de streaming, puede elegir entre las siguientes opciones para distribuirles el punto final:

- Envíe por correo electrónico la URL del punto final a sus usuarios
- Utilice una URL de su propiedad, seleccionando una de las siguientes opciones:
  - Utilice su IdP para registrar un enlace arbitrario (en este caso, el punto final del portal web) como algo que se mostrará como una aplicación para los usuarios que inicien sesión directamente en su IdP.
  - Agregue el punto final a un sitio web de su propiedad y utilice un redireccionamiento del navegador para dirigir a los usuarios al portal web.

Pasos siguientes

Después de crear su primer portal web, puede ver los detalles, editar detalles o eliminar el portal web en cualquier momento. Para obtener más información, consulte Administración de su portal web (p. 27).

Administración de su portal web

Después de configurar el portal web, puede ver o editar sus detalles, así como eliminar el portal si ya no lo necesita.

Temas

Consulte los detalles del portal web

Para ver los detalles del portal web

1. Abra el icono WorkSpaces Web Console enhttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. ElegirWorkSpaces Web,Portales web, seleccione su portal web y, a continuación, elijaView details (Ver detalles)..

Edición de un portal web

Para editar un portal web

1. Abra el icono WorkSpaces Web Console enhttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. ElegirWorkSpaces Web,Portales web, seleccione su portal web y, a continuación, elijaEditar.

   Note

   Si realiza cambios en la configuración de un usuario mientras el usuario está usando una sesión de forma activa, los cambios surtirán efecto la próxima vez que el usuario inicie una nueva sesión.

Eliminar un portal web

Para eliminar un portal web

1. Abra el icono WorkSpaces Web Console enhttps://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/.
2. ElegirWorkSpaces Web,Portales web, seleccione su portal web y, a continuación, elijaBorrar.

Solicitud de un aumento de cuota de servicio

Cuando cree suAWS, establecemos automáticamente las cuotas de servicio predeterminadas (también denominadas límites) para el uso de los recursos conAWSServicios WorkSpaces Web establece cuotas en dos tipos de recursos: portales web (por región) y sesiones simultáneas máximas (por portal web). WorkSpaces En la actualidad, Web tiene los siguientes límites de cuota de servicio:

Cuotas predeterminadas por región de AWS y cuenta	Valor
Portales web	1
Número de sesiones simultáneas	25

UNAportal webes el recurso fundamental para el WorkSpaces Servicio web Es una asociación entre su proveedor de identidad SAML 2.0 y su conexión de red a Internet y su contenido. Puede crear un portal web en cualquier región WorkSpaces La web de está disponible. Consulte la tabla de regiones para conocer la disponibilidad actual.

Lanúmero de sesiones simultáneases la mayor cantidad de usuarios que se conectarán al mismo tiempo a un portal web determinado. Si el límite de cuota de servicio para el máximo de sesiones simultáneas no se establece correctamente, es posible que los usuarios descubran que su sesión no está disponible cuando inician sesión WorkSpaces Web También debe asegurarse de que la VPC y las subredes tengan suficiente espacio IP para admitir el máximo de sesiones simultáneas, de lo contrario, es posible que los usuarios no puedan conectarse a una sesión.

Por ejemplo, un cliente tiene dos portales web en EE.UU. Este (Norte de Virginia) y 125 usuarios. El primer portal web (portal A) será utilizado por 25 usuarios y no requiere un aumento de la cuota de servicio. El segundo portal web (portal B) será utilizado por 100 usuarios. Estos usuarios se distribuyen en dos turnos y sus horas de trabajo no se superponen. Por lo tanto, el cliente tendría que solicitar un aumento de la cuota de servicio para el Portal B hasta un máximo de 50 sesiones simultáneas.

Puede solicitar un aumento de la cuota de servicio de. Para obtener más información, consulteSolicitud de aumento de cuota.

Para solicitar un aumento de la cuota de servicio

1. Abra el iconoPanel de AWS Support.
2. ElegirAumento de límites de servicio.

   Important

   WorkSpaces Las cuotas de servicio web afectan a una región a la vez. Debe solicitar aumentos de cuota de servicio en cada región de AWS en la que necesite más recursos. Para obtener más información, consulte Puntos de enlace de los servicios de AWS.
3. UnderDescripción del caso de uso, escriba 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 el aumento y el nuevo valor límite.
   - Si solicita un aumento para el 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, complete una solicitud de aumento de cuota en elSección Solicitudesy luego seleccioneAdd another solicitud.

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

Cuando un usuario visita un WorkSpaces Portal web, pueden iniciar sesión para iniciar una sesión de streaming. Todas las sesiones comienzan en la página de inicio, a menos que inicien sesión hace menos de 5 minutos. El portal busca tokens del proveedor de identidad (IdP) para determinar si se solicitan las credenciales al usuario cuando inicia 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 iniciar una sesión de streaming. Si un usuario ya ha generado un token de IdP de SAML al iniciar sesión en su IdP o en una aplicación protegida por el mismo IdP, no se le pedirá un nombre de usuario ni una contraseña.

Si un usuario tiene un token de IdP SAML válido, puede acceder WorkSpaces Web Puedes controlar el intervalo necesario 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. Establece la duración del tiempo de espera del IdP con tu proveedor de IdP SAML. Recomendamos configurar la duración del tiempo de espera de su IdP con el menor tiempo necesario para que un usuario complete sus tareas.

   - Para obtener más información acerca de Okta, consulte.Imponer una duración de sesión limitada para todas las políticas.
   - Para obtener más información acerca de Azure AD, consulte.Configuración de controles de sesión de autenticación.
   - Para obtener más información acerca de Ping, consulte.Sessions.
   - Para obtener más información acerca deAWS IAM Identity Center (successor to AWS Single Sign-On), consulteEstablezca la duración de.
2. Establezca su WorkSpaces Valores de inactividad y tiempo de espera de inactividad del portal web. Estos valores controlan la cantidad de tiempo entre la última interacción de un usuario y el momento en que un WorkSpaces La sesión web finaliza por inactividad. Cuando termina una sesión, el usuario pierde su estado de 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: Creación de un portal web” (p. 19).

   Note

   Si se agota el tiempo de espera de la sesión de un usuario, pero el usuario aún tiene un token de IdP SAML válido, no tiene que introducir su nombre de usuario y contraseña para iniciar un nuevo WorkSpaces Sesión web. Para controlar cómo se vuelven a autenticar los tokens, sigue las guías del paso anterior.

Seguridad en Amazon WorkSpaces Web

La seguridad en la nube de AWS es la mayor prioridad. Como cliente de AWS, se beneficia de una arquitectura de red y un centro de datos que se han diseñado para satisfacer los requisitos de seguridad de las organizaciones más exigentes.

La seguridad es una responsabilidad compartida entre 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 los servicios de AWS en la nube de AWS. AWS también proporciona servicios que puede utilizar de forma segura. Los auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los AWSProgramas de conformidad de . Para obtener más información acerca de los programas de conformidad que se aplican a Amazon WorkSpaces Web, consulteServicios de AWS en el ámbito del programa de conformidad.
- Seguridad en la nube: su responsabilidad viene determinada por el servicio de AWS que utilice. Usted también es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables que se apliquen a sus datos de.

Esta documentación lo ayuda a comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza Amazon WorkSpaces Web. Muestra cómo configurar Amazon WorkSpaces Web para cumplir sus objetivos de seguridad y conformidad. También aprenderás a utilizar otrosAWSservicios de que le ayudan a supervisar y proteger los recursos Web de Amazon WorkSpaces.

Contenido

Protección de datos en AmazonWorkSpacesWeb

LaAWS Modelo de responsabilidad compartidase aplica a la protección de datos en AmazonWorkSpacesWeb. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta toda la Nube de AWS. Usted es responsable de mantener el control sobre el contenido alojado en esta infraestructura. Este contenido incluye la configuración de seguridad y las tareas de administración de los servicios de Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulte las Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulte la publicación de blog AWSShared Responsability Model and GDPR en el Blog de seguridad de AWS.

Con fines de protección de datos, recomendamos proteger las credenciales de Cuenta de AWS y configurar cuentas de usuario individuales con AWS Identity and Access Management (IAM). De esta

manera, solo se otorgan a cada usuario los permisos necesarios para cumplir con sus obligaciones laborales. También recomendamos proteger sus datos de las siguientes formas:

- Utilice Multi-Factor Authentication (MFA) con cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos de AWS. Recomendamos TLS 1.2 o una versión posterior.
- Configure la API y el registro de actividad del usuario con AWS CloudTrail.
- Utilice las soluciones de cifrado de AWS, junto con todos los controles de seguridad predeterminados dentro de los servicios de AWS.
- Utilice avanzados servicios de seguridad administrados, como Amazon Macie, que lo ayuden a detectar y proteger los datos personales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados FIPS 140-2 al acceder a AWS a través de una interfaz de línea de comandos o una API, utilice un punto de enlace de FIPS. Para obtener más información sobre los puntos de enlace de FIPS disponibles, consulte Estándar de procesamiento de la información federal (FIPS) 140-2.

Recomendamos encarecidamente que nunca introduzca información de identificación confidencial, como, por ejemplo, direcciones de email de sus clientes, en etiquetas o en los campos de formato libre, como el campo Name (Nombre). Esto incluye cuando trabaje conWorkSpacesWeb u otroAWSservicios que utilizan la consola, API,AWS CLI, o bienAWSSDK de. Los datos que ingresa en etiquetas o campos de formato libre utilizados para los nombres se pueden utilizar para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya información de credenciales en la URL a fin de validar la solicitud para ese servidor.

Cifrado de datos

AmazonWorkSpacesWeb recopila datos de personalización del portal, como la configuración del navegador, la configuración de usuario, la configuración de red, la información del proveedor de identidad, los datos del almacén de confianza y los datos de certificados del almacén de confianza. WorkSpacesWeb también recopila datos de políticas del navegador, preferencias de usuario (para la configuración del navegador) y registros de sesión. Los datos recopilados se almacenan en Amazon DynamoDB y Amazon S3. WorkSpacesUsos webAWS Key Management Servicepara cifrado.

Para proteger el contenido, siga estas directrices:

- Implemente el acceso de menos privilegios y cree roles específicos para utilizarlosWorkSpacesAcciones web. Utilice plantillas de IAM para crear un rol de acceso completo o un rol de solo lectura. Para obtener más información, consulte AWSPolíticas administradas de para WorkSpaces Web (p. 45).
- Proteja los datos de extremo a extremo proporcionando una clave administrada por el cliente, por lo queWorkSpacesWeb puede cifrar los datos en reposo con las claves que proporcione.
- Tenga cuidado al compartir los dominios del portal y las credenciales de usuario:
  - Los administradores deben iniciar sesión en AmazonWorkSpacesconsola y los usuarios deben iniciar sesión en elWorkSpacesPortal web.
  - Cualquier persona en Internet puede acceder al portal web, pero no puede iniciar una sesión a menos que tenga credenciales de usuario válidas para el portal.
- Los usuarios pueden finalizar explícitamente sus sesiones eligiendoSesión final. Esto descarta la instancia que aloja la sesión del navegador y da como resultado el aislamiento del navegador.

WorkSpacesWeb protege el contenido y los metadatos de forma predeterminada cifrando todos los datos confidenciales conAWS KMS. Recopila la política del navegador y las preferencias del usuario para aplicar la política y la configuración duranteWorkSpacesSesiones web. Si se produce un error al aplicar la configuración existente, un usuario no puede acceder a nuevas sesiones y no puede acceder a los sitios internos y las aplicaciones SaaS de la empresa.

Cifrado en reposo

Cifrado en reposoestá configurado de forma predeterminada. Datos específicos del cliente utilizados enWorkSpacesLa web se encripta medianteAWS KMS. WorkSpacesWeb proporciona cifrado en reposo para los recursos que crea. El servicio acepta unAWS KMSClave administrada por el cliente en la creación de recursos y, si no se proporciona uno, unAWSLa clave de propiedad se utilizará para cifrar los recursos en reposo. El servicio cifra el documento de directiva del navegador que puede proporcionar para personalizar las sesiones del navegador, así como la configuración del proveedor de identidad y los nombres para mostrar de los portales. Esta información permanecerá cifrada mediante la clave administrada por el cliente o laAWSClave propia, mientras se almacena en nuestro backend.

Puede decidir qué clave se utilizará cuando cree unWorkSpacesRecurso web. Si los datos que forman parte de ese recurso están cifrados,WorkSpacesWeb acepta el`customerManagedKeyArn`como parte de la`create`API. La clave proporcionada debe ser simétricaAWS KMSy el administrador que crea el recurso utilizando esta clave debe tener`kms:Decrypt`,`kms:GenerateDataKey`, y`kms:CreateGrant`permisos. Después de crear un recurso con la clave, no se puede quitar ni cambiar la clave. Si ha utilizado una clave administrada por el cliente, el administrador que accede al recurso debe tener`kms:Decrypt`y`kms:GenerateDataKey`permisos. Si aparece un error sobre la denegación del acceso durante el uso de 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 claves comprobando el estado de laAWS KMSconcesiones. Para obtener más información, consulteAdministración de las concesiones. Durante la creación del portal,WorkSpacesWeb crea una concesión para permitir que el servicio acceda a la clave de forma asíncrona. Puede comprobar el estado de nuestro uso de claves comprobando la concesión, así como el contexto de cifrado proporcionado cuando se utiliza la subvención. El contexto de cifrado siempre contiene una entrada con la clave`aws:workspaces-web:portal:id`y un valor igual 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 del recurso correspondiente.

Cifrado en tránsito

WorkSpacesWeb cifra los datos en tránsito a través de HTTPS y TLS 1.2. Puede enviar una solicitud de aWorkSpacesmediante la consola o llamadas directas a la API. Los datos de solicitud que se transfieren se cifran enviando todo a través de una conexión HTTPS o TLS. Los datos de solicitud se pueden transferir desde elAWSConsola,AWS Command Line Interface, o bienAWSSDK de aWorkSpacesWeb.

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

Administración de claves

Puede suministrar su propio cliente gestionadoAWS KMSClave para cifrar la información de sus clientes. Si no se suministra una,WorkSpacesWeb utilizará unAWSClave de propiedad. Puede configurar la clave utilizando elAWSSDK.

Privacidad del tráfico entre redes

Para proteger conexiones entreWorkSpacesAplicaciones web y locales, utilizaWorkSpacesWeb para iniciar sesiones de navegador dentro de su propia VPC. La conexión a aplicaciones locales se configura en su propia VPC y no está controlada porWorkSpacesWeb.

Para proteger las conexiones entre cuentas,WorkSpacesWeb utiliza un rol vinculado a servicios para conectarse de forma segura a las cuentas de clientes y ejecutar operaciones en nombre del cliente. Para obtener más información, consulte Uso de roles vinculados a servicios de WorkSpaces Web (p. 51).

Identity and Access Management para Amazon Amazon Amazon WorkSpaces Web

AWS Identity and Access Management (IAM) es un Servicio de AWS que ayuda a los administradores a controlar de forma segura el acceso a los recursos de AWS. Los administradores de IAM controlan quién puede serautenticó ó ó(iniciado sesión) yautorizado(tienen permisos) para usar WorkSpaces Recursos web web web. IAM es un Servicio de AWS que se puede utilizar sin cargo adicional.

Temas

Público

Cómo utilizar el uso deAWS Identity and Access Management(IAM) difiere en función del trabajo que realice en WorkSpaces web web web.

Usuario del servicio— Si utiliza el WorkSpaces Servicio web para realizar su trabajo, luego su administrador le proporciona las credenciales y los permisos que necesita. A medida que usas más WorkSpaces Características web para realizar su trabajo, es posible que necesite permisos adicionales. Entender cómo se administra el acceso puede ayudarle a solicitar los permisos correctos a su administrador. Si no puede acceder a una característica en WorkSpaces Web, consulteSolución de problemas de WorkSpaces Web web web web web web web (p. 49).

Administrador de servicios web— Si estás a cargo de WorkSpaces Recursos web de su empresa a los que probablemente tenga acceso completo WorkSpaces web web web. Su trabajo consiste en determinar qué tipo de WorkSpaces Características y recursos web a los que deben acceder los usuarios del servicio. A continuación, debe enviar solicitudes a su administrador de IAM para cambiar los permisos de los usuarios de su servicio. Revise la información de esta página para conocer los conceptos básicos de IAM. Para obtener más información sobre cómo su empresa puede utilizar IAM con WorkSpaces Web, consulteCómo Amazon Amazon web WorkSpaces Web web web web web web web web (p. 38).

administrador de IAM— Si es un administrador de IAM, es posible que desee obtener información sobre cómo escribir políticas para administrar el acceso a WorkSpaces web web web. Para ver un ejemplo WorkSpaces Políticas basadas en identidades web que puede utilizar en IAM, consulteEjemplos de políticas basadas en identidades de Amazon para Amazon Amazon WorkSpaces Web (p. 43).

Autenticación con identidades

La autenticación es la manera de iniciar sesión en AWS mediante credenciales de identidad. Para obtener más información acerca de cómo iniciar sesión con la AWS Management Console, consulte Inicio de

sesión en la AWS Management Console como usuario de IAM o usuario raíz en la Guía del usuario de IAM.

Debe estar autenticado (haber iniciado sesión en AWS) como el usuario raíz de la Cuenta de AWS, como un usuario de IAM o asumiendo un rol de IAM. También puede utilizar la autenticación de inicio de sesión único de la empresa o incluso iniciar sesión con Google o Facebook. En estos casos, su administrador habrá configurado previamente la federación de identidad mediante roles de IAM. Cuando obtiene acceso a AWS mediante credenciales de otra empresa, asume un rol indirectamente.

Para iniciar sesión directamente en la AWS Management Console, utilice la contraseña con su dirección de email de usuario raíz o con su nombre de usuario de IAM. Puede acceder a AWS mediante programación utilizando sus claves de acceso de usuario raíz o usuario de IAM. AWS proporciona SDK y herramientas de línea de comandos para firmar criptográficamente su solicitud con sus credenciales. Si no utiliza las herramientas de AWS, debe firmar usted mismo la solicitud. Para ello, utilice Signature Version 4, un protocolo para autenticar solicitudes de API de entrada. Para obtener más información acerca de cómo autenticar solicitudes, consulte Proceso de firma de Signature Version 4 en la Referencia general de AWS.

Independientemente del método de autenticación que utilice, es posible que también deba proporcionar información de seguridad adicional. Por ejemplo, AWS le recomienda el uso de la autenticación multifactor (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte Uso de la autenticación multifactor (MFA) en AWS en la Guía del usuario de IAM.

Cuenta de AWS usuario raíz

Cuando se crea una Cuenta de AWS, se comienza con una identidad de inicio de sesión que tiene acceso completo a todos los recursos y Servicios de AWS de la cuenta. Esta identidad recibe el nombre de usuario raíz de la Cuenta de AWS y se accede a ella iniciando sesión con el email y la contraseña que utilizó para crear la cuenta. Recomendamos que no utilice el usuario raíz para las tareas cotidianas. Proteja las credenciales del usuario raíz y utilícelas solo para las tareas que este pueda realizar. Para ver la lista completa de las tareas que requieren que inicie sesión como usuario raíz, consulte Tareas que requieren credenciales de usuario raíz en la Referencia general de AWS.

Identidad federada

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

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

Para una administración de acceso centralizada, le recomendamos que utilice AWS IAM Identity Center (successor to AWS Single Sign-On). Puede crear usuarios y grupos en el Centro de identidades de IAM, o puede conectarse y sincronizar con un conjunto de usuarios y grupos de su propia fuente de identidad para usarlos en todas su sus aplicaciones y Cuentas de AWS. Para obtener más información, consulte ¿Qué es IAM Identity Center? en la Guía del usuario de AWS IAM Identity Center (successor to AWS Single Sign-On).

Usuarios y grupos de IAM

Un usuario de IAM es una identidad de la Cuenta de AWS que dispone de permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos emplear credenciales temporales, en lugar de crear usuarios de IAM que tengan credenciales de larga duración como contraseñas y claves de acceso. No obstante, si tiene casos de uso específicos que requieran credenciales de larga duración con usuarios de IAM, recomendamos rotar las claves de acceso. Para obtener más información, consulte Rotar

las claves de acceso periódicamente para casos de uso que requieran credenciales de larga duración en la Guía del usuario de IAM.

Un grupo de IAM es una identidad que especifica un conjunto de usuarios de IAM. 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 de grandes conjuntos de usuarios. Por ejemplo, podría tener un grupo cuyo nombre fuese IAMAdmins y conceder permisos a dicho grupo para administrar los recursos de IAM.

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 permanentes a largo plazo y los roles proporcionan credenciales temporales. Para obtener más información, consulte Cuándo crear un usuario de IAM (en lugar de un rol) en la Guía del usuario de IAM.

IAM roles

Un rol de IAM es una identidad de la Cuenta de AWS que dispone de permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una determinada persona. Puede asumir temporalmente un rol de IAM en la AWS Management Consolecambiando de roles. Puede asumir un rol llamando a una operación de la AWS CLI o de la API de AWS, o utilizando una URL personalizada. Para obtener más información acerca de los métodos para el uso de roles, consulte Uso de roles de IAM en la Guía del usuario de IAM.

Los roles de IAM 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 permisos para este. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos que están definidos en este. Para obtener información acerca de roles para federación, consulte Creación de un rol para un proveedor de identidades de terceros en la Guía del usuario de IAM. Si utiliza el Centro de identidades de IAM, debe configurar un conjunto de permisos. El Centro de identidades de IAM correlaciona el conjunto de permisos con un rol en IAM para controlar a qué pueden acceder las identidades después de autenticarse. Para obtener información acerca de los conjuntos de permisos, consulte Conjuntos de permisos en la Guía del usuario de AWS IAM Identity Center (successor to AWS Single Sign-On).
- Permisos de usuario de IAM temporales: un usuario de IAM puede asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.
- Acceso entre cuentas: puede utilizar un rol de IAM para permitir que alguien (una entidad principal de confianza) de otra cuenta acceda a los recursos de la cuenta. Los roles son la forma principal de conceder acceso entre cuentas. No obstante, con algunos Servicios de AWS se puede adjuntar una política directamente a un recurso (en lugar de utilizar un rol como representante). Para obtener información acerca de la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte Cómo los roles de IAM difieren de las políticas basadas en recursos en la Guía del usuario de IAM.
- Acceso entre servicios: algunos Servicios de AWS utilizan características de otros Servicios de AWS. Por ejemplo, cuando realiza una llamada en un servicio, es común 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 a servicios.
  - Permisos principales: cuando utiliza un usuario o un rol de IAM para llevar a cabo acciones en AWS, se lo considera una entidad principal. Las políticas conceden permisos a una entidad principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. En este caso, debe tener permisos para realizar ambas acciones. Para ver si una acción requiere acciones dependientes adicionales en una política, consulteAcciones, recursos y claves de condición de Amazon WorkSpaces Weben elReferencia de autorizaciones de servicio.
  - Rol de servicio: un rol de servicio es un rol de IAM que adopta un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

  - Rol vinculado a servicio: un rol vinculado a 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 a servicios aparecen en la cuenta de IAM y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.
- Aplicaciones que se ejecutan en Amazon EC2: puede utilizar un rol de IAM que le permita administrar credenciales temporales para las aplicaciones que se ejecutan en una instancia de EC2 y realizan solicitudes a la AWS CLI o a la API de AWS. Es preferible hacerlo de este modo a almacenar claves de acceso en la instancia de EC2. Para asignar un rol de AWS a una instancia de EC2 y ponerla a disposición de todas las aplicaciones, cree un perfil de instancia adjuntado a la instancia. Un perfil de instancia contiene el rol y permite a los programas que se ejecutan en la instancia de EC2 obtener credenciales temporales. Para obtener más información, consulte Uso de un rol de IAM para conceder permisos a aplicaciones que se ejecutan en instancias Amazon EC2 en la Guía del usuario de IAM.

Para obtener información sobre el uso de los roles de IAM, consulte Cuándo crear un rol de IAM (en lugar de un usuario) en la Guía del usuario de IAM.

Administración de acceso mediante políticas

Para controlar el acceso en AWS, se crean políticas y se asocian a identidades o recursos de AWS. Una política es un objeto de AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando una entidad principal (sesión de rol, usuario o usuario raíz) realiza una solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. Las mayoría de las políticas se almacenan en AWS como documentos JSON. Para obtener más información sobre la estructura y el contenido de los documentos de política JSON, consulte Información general de políticas JSON en la Guía del usuario de IAM.

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

Cada entidad de IAM (usuario o rol) comienza sin permisos. De forma predeterminada, los usuarios no pueden hacer nada, ni siquiera cambiar sus propias contraseñas. Para conceder permiso a un usuario para hacer algo, el administrador debe adjuntarle una política de permisos. O bien el administrador puede agregar al usuario a un grupo que tenga los permisos necesarios. Cuando el administrador concede permisos a un grupo, todos los usuarios de ese grupo obtienen los permisos.

Las políticas de IAM definen 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 dicha política puede obtener información del usuario de la AWS Management Console, la AWS CLI o la API de AWS.

Políticas basadas en identidad

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

Las políticas basadas en identidad 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 roles de su Cuenta de AWS. Las políticas administradas incluyen las políticas administradas por AWS y las políticas administradas por el cliente. Para obtener más información acerca de cómo elegir una política administrada o una política insertada, consulte Elegir entre políticas administradas y políticas insertadas en la Guía del usuario de IAM.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de política JSON que se adjuntan a un recurso. Ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM 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 adjunta 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 basada en recursos. Las entidades 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 se puede utilizar políticas de IAM administradas por AWS en una política basada en recursos.

Listas de control de acceso (ACL)

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de política JSON.

Amazon S3, AWS WAF y Amazon VPC son ejemplos de servicios que admiten las ACL. Para obtener más información sobre las ACL, consulte Información general de Lista de control de acceso (ACL) en la Guía para desarrolladores de Amazon Simple Storage Service.

Otros tipos de políticas

AWS admite otros tipos de políticas adicionales menos frecuentes. Estos tipos de políticas pueden establecer el máximo de permisos que los tipos de políticas más frecuentes le otorgan.

- Límites de permisos: un límite de permisos es una característica avanzada que le permite establecer los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM (usuario o rol de IAM). Puede establecer un límite de permisos para una identidad. Los permisos resultantes son la intersección de las políticas basadas en identidad de la entidad y los límites de sus 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 Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.
- Políticas de control de servicio (SCP): las SCP son políticas de JSON que especifican los permisos máximos de una organización o una unidad organizativa en AWS Organizations. AWS Organizations es un servicio que le permite agrupar y administrar de manera centralizada varias Cuentas de AWS que posea su empresa. Si habilita todas las características en una organización, entonces podrá aplicar políticas de control de servicio (SCP) a una o todas sus cuentas. Las SCP limitan los permisos de las entidades de las cuentas miembro, incluido cada usuario raíz de la Cuenta de AWS. Para obtener más información acerca de Organizations y las SCP, consulte Funcionamiento de las SCP en la Guía del usuario de AWS Organizations.
- 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 identidad del rol y las políticas de la sesión. Los permisos también pueden proceder de una política basada en recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información, consulte Políticas de sesión en la Guía del usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para obtener información acerca de cómo AWS decide si permitir o no una solicitud cuando

hay varios tipos de políticas implicados, consulte Lógica de evaluación de políticas en la Guía del usuario de IAM.

Cómo Amazon Amazon web WorkSpaces Web web web web web web web

Antes de utilizar IAM para administrar el acceso a WorkSpaces Web, conozca qué características de IAM están disponibles para utilizar con WorkSpaces web web web.

Características de IAM que puede utilizar con Amazon Amazon WorkSpaces Web

Características de IAM	WorkSpaces Web web web web
Políticas con base en identidad (p. 38)	Sí
Políticas basadas en recursos (p. 39)	No
Acciones de política (p. 39)	Sí
Recursos de políticas (p. 40)	Sí
Claves de condiciones de políticas (p. 40)	Sí
ACL (p. 41)	No
ABAC (etiquetas en políticas) (p. 41)	Parcial
Credenciales temporales (p. 42)	Sí
Permisos de entidades principales (p. 42)	Sí
Roles de servicio (p. 42)	No
Roles vinculados a servicios (p. 43)	Sí

Para obtener una visión de alto nivel de cómo WorkSpaces web web web y otrosAWSlos servicios funcionan con la mayoría de las funciones de IAM, consulteAWSServicios que funcionan con IAMen elIAM User Guide.

Políticas basadas en identidad de para WorkSpaces Web

Compatibilidad con las políticas basadas en identidad	Sí

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

Con las políticas basadas en identidad de IAM, puede especificar las acciones y 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 asociado. Para obtener más información acerca de los elementos que puede utilizar en una política de JSON, consulte Referencia de los elementos de las políticas de JSON de IAM en la Guía del usuario de IAM.

Ejemplos de políticas basadas en identidades de para WorkSpaces Web

Para ver ejemplos de WorkSpaces Políticas basadas en identidad web web web web web, consulteEjemplos de políticas basadas en identidades de Amazon para Amazon Amazon WorkSpaces Web (p. 43).

Políticas basadas en recursos de dentro de WorkSpaces Web

Compatibilidad con las políticas basadas en recursos	No

Las políticas basadas en recursos son documentos de política JSON que se adjuntan a un recurso. Ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM 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 adjunta 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 basada en recursos. Las entidades principales pueden incluir cuentas, usuarios, roles, usuarios federados o Servicios de AWS.

Para habilitar el acceso entre cuentas, puede especificar toda una cuenta o entidades de IAM de otra cuenta como la entidad principal de una política basada en recursos. Añadir a una política basada en recursos una entidad principal entre cuentas es solo una parte del establecimiento de una relación de confianza. Cuando la entidad principal y el recurso se encuentran en Cuentas de AWS diferentes, un administrador de IAM de la cuenta de confianza también debe conceder a la entidad principal (usuario o rol) permiso para acceder al recurso. Para conceder el permiso, asocie la entidad a una política basada en identidad. Sin embargo, si la política basada en 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 Cómo los roles de IAM difieren de las políticas basadas en recursos en la Guía del usuario de IAM.

Acciones políticas para WorkSpaces Web

Admite acciones de política	Sí

Los administradores pueden utilizar las políticas JSON de AWS para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede llevar a cabo acciones en qué recursos y bajo qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puede utilizar para permitir o denegar el acceso en una política. Las acciones de la política generalmente tienen el mismo nombre que la operación de API de AWS asociada. Hay algunas excepciones, como acciones de solo permiso que no tienen una operación de API coincidente. 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 WorkSpaces Acciones web, consulteAcciones definidas por Amazon Amazon Amazon web WorkSpaces Weben elReferencia de autorizaciones de servicio.

Acciones políticas políticas en WorkSpaces Web web web web web web web web de 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 WorkSpaces Políticas basadas en identidad web web web web web, consulteEjemplos de políticas basadas en identidades de Amazon para Amazon Amazon WorkSpaces Web (p. 43).

Recursos de políticas para WorkSpaces Web

Admite recursos de políticas	Sí

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

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso utilizando el 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 las WorkSpaces Tipos de recursos web web web web y sus ARN, consulteRecursos definidos por Amazon Amazon Amazon web WorkSpaces Weben elReferencia de autorizaciones de servicio. Para obtener información acerca de las acciones con las que puede especificar el ARN de cada recurso, consulteAcciones definidas por Amazon Amazon Amazon web WorkSpaces Web.

Para ver ejemplos de WorkSpaces Políticas basadas en identidad web web web web web, consulteEjemplos de políticas basadas en identidades de Amazon para Amazon Amazon WorkSpaces Web (p. 43).

Claves de condición de política para WorkSpaces Web

Admite claves de condición de política específicas del servicio	Sí

Los administradores pueden utilizar las políticas JSON de AWS para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y bajo 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 con una operación lógica `OR`. 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 un permiso de usuario de IAM para acceder a un recurso solo si está etiquetado con su nombre de usuario de IAM. Para obtener más información, consulte Elementos de la política de IAM: variables y etiquetas en la Guía del usuario de IAM.

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

Para ver una lista de las WorkSpaces Claves de estado web, consulteClaves de condición para Amazon Amazon WorkSpaces Weben elReferencia de autorizaciones de servicio. Para obtener información acerca de las acciones y los recursos con los que puede utilizar una clave de condición, consulteAcciones definidas por Amazon Amazon Amazon web WorkSpaces Web.

Para ver ejemplos de WorkSpaces Políticas basadas en identidad web web web web web, consulteEjemplos de políticas basadas en identidades de Amazon para Amazon Amazon WorkSpaces Web (p. 43).

Listas de control de acceso (ACL) en WorkSpaces Web

Admite las ACL	No

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de política JSON.

Control de acceso basado en atributos (ABAC) con WorkSpaces Web

Admite ABAC (etiquetas en las políticas)	Parcial

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos basados en atributos. En AWS, estos atributos se denominan etiquetas. Puede asociar etiquetas a entidades de IAM (usuarios o roles) y a muchos recursos de AWS. El etiquetado de entidades y recursos es el primer paso de ABAC. A continuación, designa las políticas de ABAC para permitir operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso al que se intenta acceder.

ABAC es útil en entornos que crecen con rapidez y ayuda en situaciones en las que la administración de las políticas resulta 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 Yes (Sí) para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Partial (Parcial).

Para obtener más información sobre ABAC, consulte ¿Qué es ABAC? en la Guía del usuario de IAM. Para ver un tutorial con los pasos para configurar ABAC, consulte Uso del control de acceso basado en atributos (ABAC) en la Guía del usuario de IAM.

Uso de credenciales temporales con WorkSpaces Web

Compatible con el uso de credenciales temporales.	Sí

Algunos servicios de Servicios de AWS no funcionan cuando inicia sesión con credenciales temporales. Para obtener información adicional, incluida la información sobre qué servicios de Servicios de AWS funcionan con credenciales temporales, consulte Servicios de Servicios de AWS que funcionan con IAM en la Guía del usuario de IAM.

Utiliza credenciales temporales si inicia sesión en la AWS Management Console con cualquier método excepto un nombre de usuario y una contraseña. Por ejemplo, cuando accede a AWS utilizando el enlace de inicio de sesión único (SSO) de la empresa, ese proceso crea automáticamente credenciales temporales. También crea automáticamente credenciales temporales cuando inicia sesión en la consola como usuario y luego cambia de rol. Para obtener más información acerca del cambio de roles, consulte Cambio a un rol (consola) en la Guía del usuario de IAM.

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

Permisos de entidades principales entre servicios de WorkSpaces Web

Admite permisos de entidades principales	Sí

Cuando utiliza un usuario o un rol de IAM para llevar a cabo acciones en AWS, se lo considera una entidad principal. Las políticas conceden permisos a una entidad principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. En este caso, debe tener permisos para realizar ambas acciones. Para ver si una acción requiere acciones dependientes adicionales en una política, consulteAcciones, recursos y claves de condición de Amazon para Amazon WorkSpaces Webenel Referencia de autorizaciones de servicio.

Roles de servicio para WorkSpaces Web

Compatible con funciones del servicio	No

Una función del servicio es un rol de IAM que asume un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de roles para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

Warning

Cambiar los permisos de un rol de servicio podría interrumpir WorkSpaces Funcionalidad de la web. Edite las funciones de servicio solo cuando WorkSpaces Web web web web web web web web web web web

Roles vinculados a servicios de WorkSpaces Web

Compatible con roles vinculados a servicios	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 a servicios aparecen en la cuenta de IAM y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

Para obtener más información acerca de cómo crear o administrar roles vinculados a servicios de, consulteAWSServicios que funcionan con IAM. Busque un servicio en la tabla que incluya unYesen elFunción vinculada al serviciocolumna web. Elija el vínculo Sí para ver la documentación acerca del rol vinculado al servicio en cuestión.

Ejemplos de políticas basadas en identidades de Amazon para Amazon Amazon WorkSpaces Web

De forma predeterminada, los usuarios y roles no tienen permiso para crear ni modificar. WorkSpaces Recursos web web web. Tampoco pueden realizar tareas mediante la AWS Management Console, la AWS Command Line Interface (AWS CLI) o la API de AWS. Un administrador de IAM debe crear políticas de IAM que concedan a los usuarios y a los roles permiso para realizar acciones en los recursos que necesitan. El administrador debe asociar esas políticas a los usuarios que las necesiten.

Para obtener información acerca de cómo crear una política basada en identidades de IAM mediante el uso de estos documentos de políticas JSON de ejemplo, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Para obtener más información sobre las acciones y los tipos de recursos definidos por WorkSpaces Web, incluido el formato de los ARN para cada uno de los tipos de recursos, consulteAcciones, recursos y claves de condición de Amazon para Amazon WorkSpaces Weben elReferencia de autorizaciones de servicio.

Temas

- Prácticas recomendadas relativas a políticas (p. 43)
- Uso de WorkSpaces Consola web (p. 44)
- Permitir a los usuarios consultar sus propios permisos (p. 44)

Prácticas recomendadas relativas a políticas

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

- Comience con las políticas administradas por AWS y continúe con los permisos de privilegio mínimo: a fin de comenzar a conceder permisos a los usuarios y las cargas de trabajo, utilice las políticas administradas por AWS, que conceden permisos para muchos casos de uso comunes. Están disponibles en la Cuenta de AWS. Se recomienda definir políticas administradas por el cliente de AWS específicas para sus casos de uso a fin de reducir aún más los permisos. Con el fin de obtener más información,

consulte las políticas administradas por AWS o las políticas administradas por AWS para funciones de trabajo en la Guía de usuario de IAM.

- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, 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. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulte Políticas y permisos en IAM en la Guía de usuario de IAM.
- Use condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar 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 utilizando SSL. También puede usar condiciones para conceder acceso a acciones de servicios si se emplean a través de un Servicio de AWS determinado, como por ejemplo AWS CloudFormation. Para obtener más información, consulteElementos de la política JSON de IAM Condiciónen elIAM User Guide.
- Use el Analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el Analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. IAM Access Analyzer proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para obtener más información, consulte la política de validación del Analizador de acceso de IAM en la Guía de usuario de IAM.
- Solicite la autenticación multifactor (MFA): si se encuentra en una situación en la que necesita usuarios raíz o de IAM en la cuenta, active la MFA para mayor seguridad. Para solicitar la MFA cuando se invocan las operaciones de la API, agregue las condiciones de MFA a sus políticas. Para obtener más información, consulte Configuración de acceso a una API protegida por MFA en la Guía de usuario de IAM.

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

Uso de WorkSpaces Consola web

Para acceder a la Amazonía WorkSpaces Consola web, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle registrar y consultar los detalles acerca de WorkSpaces Recursos web en tuCuenta de AWS. Si crea una política basada en identidad que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles de IAM) que tengan esa política.

No es necesario que conceda permisos mínimos para la consola a los usuarios que solo realizan llamadas a la AWS CLI o a la API de AWS. En su lugar, permite acceso únicamente a las acciones que coincidan con la operación de API que intenta realizar.

Para garantizar que los usuarios y los roles puedan seguir utilizando el WorkSpaces Consola web, adjunte también el WorkSpaces Web`ConsoleAccessoReadOnly` AWSpolítica gestionada para las entidades. Para obtener más información, consulte Adición de permisos a un usuario en la Guía del usuario de IAM:

Permitir a los usuarios consultar sus propios permisos

En este ejemplo, se muestra cómo podría crear una política que permita a los usuarios de IAM ver las políticas administradas e insertadas que se adjuntan a la identidad de sus usuarios. Esta política incluye permisos para llevar a cabo esta acción en la consola o mediante programación con la AWS CLI o la API de AWS.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
```

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

AWSPolíticas administradas de para WorkSpaces Web

Para agregar permisos a usuarios, grupos y roles, es más fácil utilizar las políticas administradas de AWS que escribirlas uno mismo. Se necesita tiempo y experiencia para crear políticas de IAM administradas por el cliente que proporcionen a su equipo solo los permisos necesarios. Para comenzar a hacerlo con rapidez, puede utilizar nuestras políticas administradas por AWS. Estas políticas cubren casos de uso comunes y están disponibles en su cuenta de AWS. Para obtener más información sobre las políticas administradas por AWS, consulte Políticas administradas por AWS en la Guía del usuario de IAM.

Los servicios de AWS mantienen y actualizan las políticas administradas por AWS. No puede cambiar los permisos en las políticas administradas por AWS. En ocasiones, los servicios pueden agregar permisos adicionales a unAWSpolítica administrada por para admitir características nuevas. 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 quitan los permisos de unAWSpolítica administrada, por lo que las actualizaciones de políticas no romperán los permisos existentes.

Además, AWS admite políticas administradas para funciones de trabajo que abarcan varios servicios. Por ejemplo, el`ReadOnlyAccess` AWSLa política administrada proporciona acceso de solo lectura a todosAWSservicios y recursos. Cuando un servicio lanza una nueva característica, AWS agrega permisos de solo lectura para las operaciones y los recursos nuevos. 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.

AWSPolítica administrada: AmazonWorkSpacesWebServiceRolePolicy

No puede adjuntar la política `AmazonWorkSpacesWebServiceRolePolicy` a sus entidades de IAM. Esta política está adjuntada a un rol vinculado a un servicio que permite WorkSpaces Web para realizar acciones en su nombre. Para obtener más información, consulte the section called “Uso de roles vinculados a servicios” (p. 51).

Esta política concede permisos administrativos que brindan acceso aAWSservicios y recursos utilizados o gestionados por Amazon WorkSpaces web.

Detalles sobre los permisos

Esta política incluye los siguientes permisos:

- `WorkSpaces Web`— Permite el acceso aAWSservicios y recursos utilizados o gestionados por Amazon WorkSpaces web.
- `ec2`permite a los principales describir VPC, subredes y zonas de disponibilidad; crear, etiquetar, describir y eliminar interfaces de red; asociar o desasociar una dirección; y describir tablas de enrutamiento, grupos de seguridad y puntos finales de VPC.
- `CloudWatch`— Permite a los directores poner datos de métricas.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "ec2:DescribeVpcs",
    "ec2:DescribeSubnets",
    "ec2:DescribeAvailabilityZones",
    "ec2:CreateNetworkInterface",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DeleteNetworkInterface",
    "ec2:AssociateAddress",
    "ec2:DisassociateAddress",
    "ec2:DescribeRouteTables",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeVpcEndpoints"
   ],
   "Resource": "*"
  },
  {
   "Effect": "Allow",
   "Action": [
    "ec2:CreateTags"
   ],
   "Resource": "arn:aws:ec2:*:*:network-interface/*",
   "Condition": {
    "StringEquals": {
     "ec2:CreateAction": "CreateNetworkInterface"
```

```
    },
    "ForAllValues:StringEquals": {
     "aws:TagKeys": [
      "WorkSpacesWebManaged"
     ]
    }
   }
  },
  {
   "Effect": "Allow",
   "Action": [
    "cloudwatch:PutMetricData"
   ],
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "cloudwatch:namespace": [
      "AWS/WorkSpacesWeb",
      "AWS/Usage"
     ]
    }
   }
  }
 ]
}
```

AWSPolítica administrada: AmazonWorkSpacesWebReadOnly

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

Esta política concede permisos de solo lectura que brindan acceso a WorkSpaces Web y sus dependencias a través delAWSConsola de administración, SDK y CLI.

Detalles sobre los permisos

Esta política incluye los siguientes permisos.

- `WorkSpaces Web`— Proporciona acceso de solo lectura a Amazon WorkSpaces Web y sus dependencias a través delAWSConsola de administración, SDK y CLI.
- `ec2`: permite a los principales describir VPC, redes y grupos de seguridad. Se utiliza en elAWSConsola de administración en WorkSpaces Web para mostrarle las VPC, las subredes y los grupos de seguridad que están disponibles para usar 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:ListBrowserSettings",
        "workspaces-web:ListIdentityProviders",
        "workspaces-web:ListNetworkSettings",
        "workspaces-web:ListPortals",
        "workspaces-web:ListTagsForResource",
        "workspaces-web:ListTrustStoreCertificates",
        "workspaces-web:ListTrustStores",
        "workspaces-web:ListUserSettings"
      ],
      "Resource": "arn:aws:workspaces-web:*:*:*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource": "*"
    }
  ]
}
```

WorkSpaces Actualizaciones web deAWSpolíticas administradas

Vea detalles sobre las actualizaciones deAWSPolíticas administradas de para WorkSpaces Web debido a que este servicio comenzó a realizar un seguimiento de estos cambios Para obtener alertas automáticas sobre cambios en esta página, suscríbase a la fuente RSS en la página de Historial de documentos (p. 61).

Cambio	Descripción	Fecha
AmazonWorkSpacesWebServiceRolePolicy (p. 49) Política actualizada	WorkSpaces Web actualizó la política para crear etiquetas durante la creación de ENI.	6 de septiembre de 2022
AmazonWorkSpacesWebServiceRolePolicy (p. 49) Política actualizada	WorkSpaces Web actualizó la política para agregar el espacio de nombres AWS/Usage al PutMetricData Permisos de la API	6 de abril de 2022
AmazonWorkSpacesWebReadOnly (p. 47) política nueva	WorkSpaces Web agregó una nueva política para proporcionar acceso de solo lectura a Amazon WorkSpaces Web y sus dependencias a través de la consola de administración de AWS, el SDK y la CLI.	30 de noviembre de 2021
AmazonWorkSpacesWebServiceRolePolicy (p. 49) política nueva	WorkSpaces Web agregó una nueva política para permitir el acceso a los servicios y recursos de AWS que Amazon utiliza o administra WorkSpaces web.	30 de noviembre de 2021

Cambio	Descripción	Fecha
WorkSpaces Web comenzó el seguimiento de los cambios	WorkSpaces Web comenzó hacer un seguimiento de los cambios paraAWSPolíticas administradas.	30 de noviembre de 2021

Solución de problemas de WorkSpaces Web web web web web web

Utilice la información siguiente para diagnosticar y solucionar los problemas comunes que puedan surgir cuando trabaje con WorkSpaces Web e IAM.

Temas

No tengo autorización para realizar una acción en WorkSpaces Web

Si la AWS Management Console le indica que no está autorizado para llevar a cabo una acción, debe ponerse en contacto con su administrador para recibir ayuda. Su administrador es la persona que le facilitó su nombre de usuario y contraseña.

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

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

En este caso, Mateo pide a su administrador que actualice sus políticas de forma que pueda obtener acceso al recurso *`my-example-widget`* mediante la acción `workspaces-web:`*`GetWidget`*.

No tengo autorización para realizar la siguiente operación:PassRole

Si recibe un error que indica que no está autorizado a realizar el`iam:PassRole`acción, sus políticas deben actualizarse para permitirle transferir un rol a WorkSpaces web web web.

Algunos servicios de Servicios de AWS le permiten transferir un rol existente a dicho servicio en lugar de crear un nuevo rol de servicio o uno vinculado al servicio. Para ello, debe tener permisos para transferir el rol al servicio.

En el siguiente ejemplo, el error se produce cuando un usuario de IAM denominado`marymajorse` utiliza la consola para realizar una acción en WorkSpaces web web web. Sin embargo, la acción requiere que el

servicio cuente con permisos que otorga 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 su administrador de AWS. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero ver mis claves de acceso

Después de crear sus claves de acceso de usuario de IAM, puede ver su ID de clave de acceso en cualquier momento. Sin embargo, no puede volver a ver su clave de acceso secreta. Si pierde la clave de acceso secreta, debe crear un nuevo par de claves de acceso.

Las claves de acceso se componen de dos partes: un ID de clave de acceso (por ejemplo, `AKIAIOSFODNN7EXAMPLE`) y una clave de acceso secreta (por ejemplo, `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`). El ID de clave de acceso y la clave de acceso secreta se utilizan juntos, como un nombre de usuario y contraseña, para autenticar sus solicitudes. Administre sus claves de acceso con el mismo nivel de seguridad que para el nombre de usuario y la contraseña.

> **Important**
>
> No proporcione las claves de acceso a terceros, ni siquiera para que le ayuden a buscar el ID de usuario canónico. Si lo hace, podría conceder a otra persona acceso permanente a su cuenta.

Cuando cree un par de claves de acceso, se le pide que guarde el ID de clave de acceso y la clave de acceso secreta en un lugar seguro. La clave de acceso secreta solo está disponible en el momento de su creación. Si pierde la clave de acceso secreta, debe agregar nuevas claves de acceso a su usuario de IAM. Puede tener un máximo de dos claves de acceso. Si ya cuenta con dos, debe eliminar un par de claves antes de crear uno nuevo. Para consultar las instrucciones, consulte Administración de claves de acceso en la Guía del usuario de IAM.

Soy administrador y deseo permitir que otros obtengan acceso a WorkSpaces Web

Para permitir que otros accedan WorkSpaces Web, debe crear una entidad de IAM (usuario o rol) para la persona o aplicación que necesita acceso. Esta persona utilizará las credenciales de la entidad para acceder a AWS. A continuación, debe adjuntar una política a la entidad que le conceda los permisos correctos en WorkSpaces web web web.

Para comenzar de inmediato, consulte Creación del primer grupo y usuario delegado de IAM en la Guía del usuario de IAM.

Quiero permitir que personas ajenas a miAWScuenta para acceder a mi WorkSpaces Recursos web web web

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 admitan las políticas basadas en recursos o las listas de control de acceso (ACL), puede utilizar dichas políticas para conceder a las personas acceso a sus recursos.

Para obtener más información, consulte lo siguiente:

- Para saber si WorkSpaces Web web web admite estas características, consulteCómo Amazon Amazon web WorkSpaces Web web web web web web web web (p. 38).

- Para obtener información acerca de cómo proporcionar acceso a los recursos de las Cuentas de AWS de su propiedad, consulte Proporcionar acceso a un usuario de IAM a otra Cuenta de AWS de la que es propietario en la Guía del usuario de IAM.
- Para obtener información acerca de cómo proporcionar acceso a los recursos a Cuentas de AWS de terceros, consulte Proporcionar acceso a Cuentas de AWS que son propiedad de terceros en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante una identidad federada, consulte Proporcionar acceso a usuarios autenticados externamente (identidad federada) en la Guía del usuario de IAM.
- Para obtener información sobre la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte Cómo los roles de IAM difieren de las políticas basadas en recursos en la Guía del usuario de IAM.

Uso de roles vinculados a servicios de WorkSpaces Web

WorkSpaces Usos webAWS Identity and Access Management(IAM)roles vinculados a servicios. Un rol vinculado a un servicio es un tipo único de rol de IAM que está vinculado directamente a WorkSpaces Web. Roles vinculados a servicios están predefinidos por WorkSpaces Web e incluya todos los permisos que requiere el servicio para llamar a otrosAWSservicios de en su nombre.

Un rol vinculado a un servicio simplifica la configuración WorkSpaces Web más fácil porque ya no tendrá que agregar manualmente los permisos necesarios. WorkSpaces Web define los permisos de sus roles vinculados a servicios y, a menos que esté definido de otra manera, solo WorkSpaces La web puede asumir sus funciones. Los permisos definidos incluyen las políticas de confianza y 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. De esta forma se protegen WorkSpaces Recursos web porque se evita que se puedan eliminar accidentalmente permisos de acceso a los recursos.

Para obtener información sobre otros servicios que son compatibles con los roles vinculados a servicios, consulte Servicios de AWS que funcionan con IAM y busque los servicios que muestran Yes (Sí) en la columna Service-Linked Role (Rol vinculado a servicios). Seleccione una opción Sí con un enlace para ver la documentación acerca del rol vinculado al servicio en cuestión.

Permisos de roles vinculados a servicios de WorkSpaces Web

WorkSpaces Web utiliza el rol vinculado a un servicio denominado`AWSServiceRoleForAmazonWorkSpacesWeb`– WorkSpaces Web utiliza este rol vinculado al servicio para obtener acceso a los recursos de Amazon EC2 de las cuentas de clientes de para instancias de streaming y CloudWatch Métricas de .

El rol vinculado a servicios `AWSServiceRoleForAmazonWorkSpacesWeb` confía en los siguientes servicios para asumir el rol:

- `workspaces-web.amazonaws.com`

La política de permisos del rol denominada`AmazonWorkSpacesWebServiceRolePolicy`permite WorkSpaces Web para completar las siguientes acciones en los recursos especificados:

- Acción: `ec2:DescribeVpcs` en `all AWS resources`
- Acción: `ec2:DescribeSubnets` en `all AWS resources`
- Acción: `ec2:DescribeAvailabilityZones` en `all AWS resources`

- Acción: `ec2:CreateNetworkInterface` en `all AWS resources`
- Acción: `ec2:DescribeNetworkInterfaces` en `all AWS resources`
- Acción: `ec2:DeleteNetworkInterface` en `all AWS resources`
- 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 `ec2:CreateNetworkInterface Operation with aws:TagKeys: ["WorkSpacesWebManaged"]`
- Acción: `cloudwatch:PutMetricData` en `all AWS resources`

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.

Creación de un rol vinculado a un servicio de WorkSpaces Web

No necesita crear manualmente un rol vinculado a servicios. Al crear el primer portal en elAWS Management Console, elAWS CLI, o elAWSAPI, WorkSpaces Web crea el rol vinculado a un servicio por usted.

> **Important**
>
> Este rol vinculado al servicio 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 al servicio y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Cuando creas tu primer portal, WorkSpaces Web vuelve a crear automáticamente la función vinculada al servicio.

También puede utilizar la consola de IAM para crear un rol vinculado al servicio con elWorkSpaces Webcaso de uso. En la AWS CLI o la API de AWS, cree un rol vinculado al servicio con el nombre de 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.

Modificación de un rol vinculado a un servicio de WorkSpaces Web

WorkSpaces Web no le permite editar el`AWSServiceRoleForAmazonWorkSpacesWeb`rol vinculado a un 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 utilizando IAM. Para obtener más información, consulte Editar un rol vinculado a servicios en la Guía del usuario de IAM..

Eliminación de un rol vinculado a un servicio de WorkSpaces Web

Si ya no necesita utilizar una característica o servicio que requiere un rol vinculado a un servicio, recomendamos que elimine dicho rol. De esta forma no tiene una entidad no utilizada que no se monitorice ni mantenga de forma activa. Sin embargo, debe limpiar los recursos del rol vinculado al servicio antes de eliminarlo manualmente.

Note

Si el archivo de WorkSpaces El servicio web está utilizando el rol cuando se intentan eliminar los recursos y es posible que se produzcan errores en la operación de eliminación. En tal caso, espere unos minutos e intente de nuevo la operación.

Para eliminar WorkSpaces Los recursos web utilizados por el AWSServiceRoleForAmazonWorkSpacesWeb

- Elija una de las siguientes opciones:
  - Si usas la consola, elimina todos los portales de 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 y los almacenes de confianza) de sus portales, elimine estos recursos y, a continuación, elimine los portales.

Para eliminar manualmente el rol vinculado a servicios mediante IAM

Puede usar la consola de IAM, la AWS CLI o la API de AWS para eliminar el rol vinculado a un servicio AWSServiceRoleForAmazonWorkSpacesWeb. Para obtener más información, consulte Eliminación de un rol vinculado a servicios en la Guía del usuario de IAM.

Regiones admitidas para WorkSpaces Roles vinculados a servicios web

WorkSpaces Web admite el uso de roles vinculados a servicios en todas las regiones en las que el servicio está disponible. Para obtener más información, consulte Regiones y puntos de enlace de AWS.

Respuesta frente a incidencias en Amazon WorkSpaces Web

Puede detectar incidentes monitoreando el`SessionFailure`Métrica de Amazon CloudWatch. Para recibir alertas de incidentes, utilice una alarma CloudWatch para el`SessionFailure`Métrica de. Para obtener más información, consulte Monitoreo de Amazon WorkSpaces Web con Amazon CloudWatch (p. 57).

Validación de conformidad para Amazon WorkSpaces Web

Auditores externos evalúan la seguridad y la conformidad de los Servicios de AWS como parte de varios programas de conformidad de AWS, como SOC, PCI, FedRAMP e HIPAA.

Para saber si Amazon WorkSpaces Web u otroServicios de AWSestán dentro del ámbito de los programas de cumplimiento específicos, véaseAWSServicios de en el ámbito del programa de conformidad. Para obtener información general, consulte Programas de conformidad de AWS.

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

Su responsabilidad de conformidad al utilizar Servicios de AWS se determina en función de la sensibilidad de los datos, los objetivos de cumplimiento de su empresa y la legislación y los reglamentos correspondientes. AWS proporciona los siguientes recursos para ayudar con la conformidad:

- Guías de inicio rápido de seguridad y conformidad: en estas guías de implementación, se analizan consideraciones de arquitectura y se proporcionan los pasos para implementar entornos de base de referencia en AWS que se centren en la seguridad y la conformidad.
- Architecting for HIPAA Security and Compliance on Amazon Web Services— En este documento técnico se describe cómo pueden utilizar las empresasAWSpara crear aplicaciones aptas para HIPAA.

  Note

  No todos los Servicios de AWS son aptos para HIPAA. Para obtener más información, consulte la Referencia de servicios aptos para HIPAA.
- Recursos de conformidad de AWS: este conjunto de manuales y guías podría aplicarse a su sector y ubicación.
- Evaluación de recursos con reglas en la Guía para desarrolladores de AWS Config: el servicio AWS Config evalúa en qué medida las configuraciones de sus recursos cumplen las prácticas internas, las directrices del sector y las normativas.
- AWS Security Hub: este Servicio de AWS proporciona una vista integral de su estado de seguridad en AWS que lo ayuda a verificar la conformidad con los estándares y las prácticas recomendadas del sector de seguridad.
- AWS Audit Manager: este Servicio de AWS le ayuda a auditar continuamente el uso de AWS con el fin de simplificar la forma en que administra el riesgo y la conformidad con las normativas y los estándares del sector.

Resiliencia en Amazon WorkSpaces Web

La infraestructura global de AWS se divide en Regiones de AWS y zonas de disponibilidad. Las Regiones de AWS proporcionan varias zonas de disponibilidad físicamente independientes y aisladas que se encuentran conectadas mediante redes con un alto nivel de rendimiento y redundancia, además de baja latencia. 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 centros de datos únicos o múltiples.

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

Actualmente no se admiten los siguientes elementos de WorkSpaces Web:

- Copia de seguridad de contenido en AZ o regiones
- Copias de seguridad cifradas
- Cifrado de contenido en tránsito entre AZ o regiones
- Respaldos automáticos o predeterminados

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

Seguridad de la infraestructura en Amazon WorkSpaces Web

Al tratarse de un servicio administrado, Amazon WorkSpaces Web está protegido por elAWSprocedimientos de seguridad de red globales de que se describen en elAmazon Web Services: Información general sobre procesos de seguridaddocumento técnico.

UsaAWSa la API publicadas de para obtener acceso a Amazon WorkSpaces Web a través de la red. Los clientes deben ser compatibles con Transport Layer Security (TLS) 1.0 o una versión posterior. Recomendamos TLS 1.2 o una versión posterior. Los clientes también deben ser compatibles con conjuntos de cifrado con confidencialidad directa total (PFS) tales como Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad principal de IAM. También puede utilizar laAWS Security Token Service(AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

WorkSpaces Web aísla el tráfico de servicios mediante la aplicación EstándarAWSAutenticación y autorización SigV4 para todos los servicios. El endpoint de recursos del cliente (o endpoint del portal web) está protegido por su proveedor de identidad. Puede aislar aún más el tráfico mediante la autorización multifactor y otro mecanismo de seguridad de su proveedor de identidad (IdP).

Todo el acceso a Internet se puede controlar configurando los ajustes de red, como la VPC, la subred o el grupo de seguridad. Los puntos de enlace de VPC de varios inquilinos y de VPC de (Privatelink) no son compatibles en la actualidad.

Configuración y análisis de vulnerabilidades en Amazon WorkSpaces Web

WorkSpaces Web actualiza y aplica parches a las aplicaciones y plataformas según sea necesario en su nombre, incluidos Chrome y Linux. No es necesario que parches ni reconstruyas. Sin embargo, es responsabilidad suya configurar WorkSpaces Web de acuerdo con las especificaciones y directrices y supervisar el uso de WorkSpaces Web por parte de los usuarios. Todas las configuraciones relacionadas con los servicios y el análisis de vulnerabilidades son responsabilidad de WorkSpaces Web.

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

Prácticas recomendadas de seguridad para Amazon WorkSpaces Web

Amazon WorkSpaces Web proporciona una serie de características de seguridad que puede utilizar a la perfección e implementación de sus propias políticas de seguridad. Las siguientes prácticas recomendadas son directrices generales y no suponen 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.

Las prácticas recomendadas para Amazon WorkSpaces Web incluyen las siguientes:

- Para detectar posibles eventos de seguridad asociados con el uso de WorkSpaces Web, utiliceAWS CloudTrailo Amazon CloudWatch para detectar y realizar un seguimiento del historial de acceso y los registros de procesos. Para obtener más información, consulte Monitoreo de Amazon WorkSpaces Web con Amazon CloudWatch (p. 57) y Registro de llamadas a la API de Amazon WorkSpaces medianteAWS CloudTrail (p. 58).
- Para implementar controles detectives e identificar anomalías, utilice los registros de CloudTrail y las métricas de CloudWatch. Para obtener más información, consulte Monitoreo de Amazon WorkSpaces Web con Amazon CloudWatch (p. 57) y Registro de llamadas a la API de Amazon WorkSpaces medianteAWS CloudTrail (p. 58).

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

- Implemente el acceso de menos privilegios y cree roles específicos para utilizarlos en las acciones WorkSpaces Web. Utilice plantillas de IAM para crear un rol de acceso completo o de solo lectura. Para obtener más información, consulte AWSPolíticas administradas de para WorkSpaces Web (p. 45).
- Tenga cuidado al compartir los dominios del portal y las credenciales de usuario. Cualquier persona en Internet puede acceder al portal web, pero no puede iniciar una sesión a menos que tenga una credencial de usuario válida para el portal. Tenga cuidado sobre cómo, cuándo y con quién comparte las credenciales del portal web.

Monitoreo de Amazon WorkSpaces Web

La monitorización es una parte importante del mantenimiento de la fiabilidad, la disponibilidad y el rendimiento de Amazon WorkSpaces Web y tus otrosAWSsoluciones.AWSofrece las siguientes herramientas de monitoreo para vigilar su WorkSpaces Los portales web y sus recursos, informa cuando algo no funciona y toma acciones automáticas cuando corresponda:

- Amazon CloudWatchmonitorea suAWSlos recursos de y las aplicaciones que se ejecutan enAWSen tiempo real. Puede recopilar métricas y realizar un seguimiento de ellas, 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 tener CloudWatch haga un seguimiento del uso de la CPU u otras métricas de las instancias de Amazon EC2 y lanzar nuevas instancias automáticamente cuando sea necesario. Para obtener más información, consulte la .Amazon CloudWatch Guía del usuario de.
- Amazon CloudWatch Registrosle permite monitorear, almacenar y tener acceso a los archivos de registro desde instancias de Amazon EC2, CloudTraily otras fuentes. CloudWatch Los registros pueden monitorear información en los archivos de registro y enviarle una notificación cuando se llega a determinados umbrales. También se pueden archivar los datos de los registros en un almacenamiento de larga duración. Para obtener más información, consulte la .Amazon CloudWatch Guía del usuario de registros.
- AWS CloudTrail captura llamadas a la API y eventos relacionados efectuados por su cuenta de AWS o en su nombre, y entrega los archivos de registro al bucket de Amazon S3 que se haya especificado. También pueden identificar qué usuarios y cuentas llamaron a AWS, la dirección IP de origen de las llamadas y el momento en que se hicieron. Para obtener más información, consulte la Guía del usuario de AWS CloudTrail.

Monitoreo de Amazon WorkSpaces Web con Amazon CloudWatch

Puede monitorear Amazon WorkSpaces Uso de Web CloudWatch, que recopila y procesa los datos sin procesar para convertirlos en métricas legibles casi 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, consulte la .Amazon CloudWatch Guía del usuario de.

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

CloudWatch métricas de Amazon WorkSpaces Web

Métrica	Descripción	Dimensiones	Estadísticas	Unidades
`SessionAttempt`	El número de Amazon WorkSpaces Intentos de sesión web.	`PortalId`	promedio, suma, máximo, mínimo	Recuento

Métrica	Descripción	Dimensiones	Estadísticas	Unidades
`SessionSuccess`	El número de Amazon exitosos WorkSpaces Se inicia la sesión web.	`PortalId`	promedio, suma, máximo, mínimo	Recuento
`SessionFailure`	El número de Amazon de servicio de WorkSpaces Se inicia la sesión web.	`PortalId`	promedio, suma, máximo, mínimo	Recuento

Registro de llamadas a la API de Amazon WorkSpaces medianteAWS CloudTrail

Amazon WorkSpaces Web se integra conAWS CloudTrail, un servicio que proporciona un registro de las medidas adoptadas por un usuario, un rol o unAWSservicio en Amazon WorkSpaces Web. CloudTrail captura todas las llamadas a la API de Amazon WorkSpaces Web como eventos. Incluyen las llamadas desde la consola Web de Amazon WorkSpaces y las llamadas desde el código a las operaciones de la API de Amazon WorkSpaces. Si crea un registro de seguimiento, puede habilitar la entrega continua de eventos de CloudTrail a un bucket de Amazon S3, incluidos los eventos de Amazon WorkSpaces Web. Si no configura un registro de seguimiento, puede ver los eventos más recientes de la consola de CloudTrail en el Event history (Historial de eventos). Mediante la información que recopila CloudTrail, se puede identificar la solicitud que se envió a Amazon WorkSpaces Web, la dirección IP desde la que se realizó la solicitud, quién realizó la solicitud, cuándo la realizó y detalles adicionales.

Para obtener más información acerca de CloudTrail, consulte la AWS CloudTrailGuía del usuario de .

Información de Amazon WorkSpaces en CloudTrail

CloudTrail se habilita en su cuenta de AWS cuando la crea. Cuando se produce una actividad en Amazon WorkSpaces Web, esta se registra en un evento de CloudTrail junto con los demásAWSeventos de servicio enHistorial de eventos. EnHistorial de eventos, puede ver, buscar y descargar los últimos eventos enAWSaccount. Para obtener más información, consulteVer eventos con el historial de eventos de CloudTrail.

Para mantener un registro continuo de los eventos de laAWScuenta, incluidos los eventos de Amazon WorkSpaces Web, puede crear un registro de seguimiento. Un registro de seguimiento permite a CloudTrail enviar archivos de registro a un bucket de Amazon S3. De forma predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las regiones de AWS. El registro de seguimiento registra los eventos de todas las regiones de la partición de AWS y envía los archivos de registro al bucket de Amazon S3 especificado. También es posible configurar otros servicios de AWS para analizar en profundidad y actuar en función de los datos de eventos recopilados en los registros de CloudTrail. Para obtener más información, consulte los siguientes temas:

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

CloudTrail registra todas las acciones de Amazon WorkSpaces y se documentan enReferencia de la API de Amazon WorkSpaces. Por ejemplo, las llamadas a las acciones `CreatePortal`, `DeleteUserSettings` y `ListBrowserSettings` generan entradas en los archivos de registros de CloudTrail.

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

- Si la solicitud se realizó con credenciales de usuario AWS Identity and Access Management (IAM) o credenciales de usuario raíz.
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro servicio de AWS.

Para obtener más información, consulte el elemento userIdentity de CloudTrail.

Descripción de las entradas de archivos de registro de Amazon WorkSpaces

Un registro de seguimiento es una configuración que permite la entrega de eventos como archivos de registros a un bucket de Amazon S3 que usted especifique. Los archivos log de CloudTrail pueden contener una o varias entradas de log. Un evento representa una única solicitud de cualquier origen e incluye información sobre la acción solicitada, la fecha y hora de la acción, los parámetros de la solicitud y otros detalles. Los archivos de registro de CloudTrail no rastrean el orden en la pila de las llamadas públicas a la API, por lo que estas no aparecen en ningún orden específico.

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


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

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

Historial de revisión de la Amazonía WorkSpaces Guía del usuario web

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

Cambio	Descripción	Fecha
Actualizaciones de redes	Diversas actualizaciones de la sección «Redes y acceso»	22 de septiembre de 2022
Actualización de la política administrada	Actualizado AmazonWorkSpacesWebServiceRolePolicy política administrada	6 de septiembre de 2022
Configuración de sesiones de usuarios	Configure el editor de métodos de entrada (IME) y la localización durante la sesión	28 de julio de 2022
Actualizaciones de redes	Diversas actualizaciones de la sección «Redes y acceso»	7 de julio de 2022
Valores de tiempo de espera	Especifique laTiempo de espera de desconexión en minutosyTiempo de espera de desconexión por inactividad en	16 de mayo de 2022
Política administrada actualizada	Actualizado el AmazonWorkSpacesWebServiceRolePolicy política gestionada para añadir el espacio de nombres AWS/Usage al PutMetricData Permisos de API	6 de abril de 2022
Función vinculada al servicio	Nuevo AWSServiceRoleForAmazonWorkSpacesWeb rol vinculado a servicios	30 de noviembre de 2021
Política administrada	Nuevo AmazonWorkSpacesWebReadOnly política administrada	30 de noviembre de 2021
Política administrada	Nuevo AmazonWorkSpacesWebServiceRolePolicy política administrada	30 de noviembre de 2021
Versión inicial	Versión inicial de WorkSpaces Guía de administración web	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.