aws

Guía del administrador

Amazon WorkSpaces Thin Client

Amazon WorkSpaces Thin Client: Guía del administrador

Table of Contents

¿Qué es la consola de administración de Amazon WorkSpaces Thin Client?

Con la consola de administración de Amazon WorkSpaces Thin Client, los administradores pueden gestionar los entornos y dispositivos de WorkSpaces Thin Client a través de un portal WorkSpaces Thin Client. Desde esta consola web, los administradores pueden crear entornos, administrar dispositivos y establecer parámetros para los usuarios de WorkSpaces Thin Client dentro de su red.

Los entornos de escritorios virtuales que utilice para WorkSpaces Thin Client deben crearse o modificarse en su propia consola.

> **Important**
>
> Para que la consola de administración de WorkSpaces Thin Client funcione correctamente, el sistema debe cumplir primero unos requisitos específicos. Estos requisitos se detallan en Requisitos previos y configuraciones.

Temas

¿Es la primera vez que usa ?

Si es la primera vez que utiliza la consola de administración de WorkSpaces Thin Client, le recomendamos que comience leyendo las siguientes secciones:

- Inicio de la consola de administración de WorkSpaces Thin Client
- Uso de la consola de administración de WorkSpaces Thin Client

Arquitectura

Cada WorkSpaces Thin Client está asociado a un proveedor de interfaz de escritorio virtual (VDI). WorkSpaces Thin Client admite tres proveedores de VDI:

- Amazon WorkSpaces
- AppStream 2.0
- Navegador Amazon WorkSpaces Secure

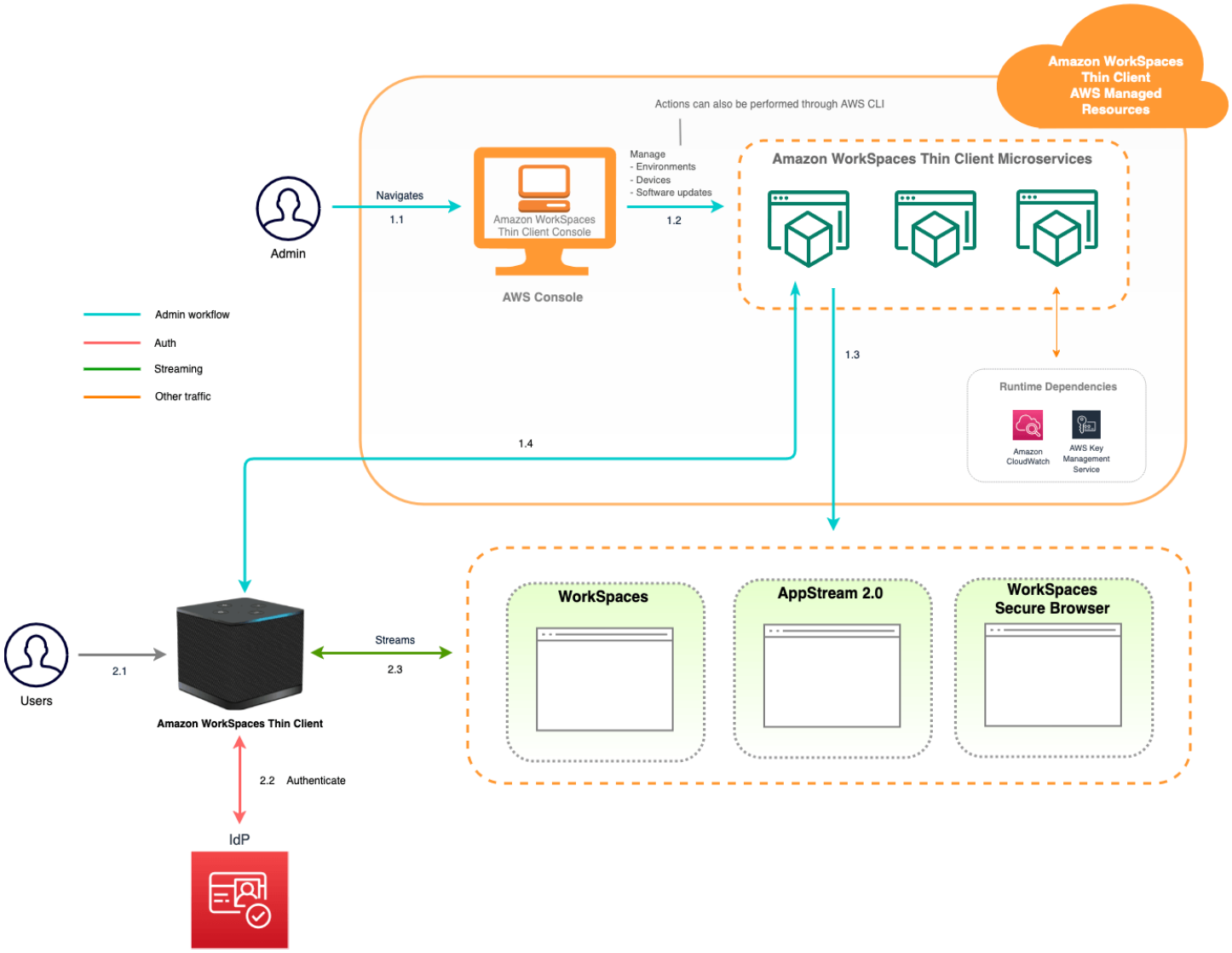
En función de la VDI utilizada, se accede a la información de su WorkSpaces Thin Client y se gestiona mediante directorios (para la versión 2.0) WorkSpaces, pilas (para la AppStream versión 2.0) y puntos de enlace del portal web (para WorkSpaces Secure Browser).

Para obtener más información sobre Amazon WorkSpaces, consulta Cómo empezar con la configuración WorkSpaces rápida. Los directorios se administran mediante el AWS Directory Service, que ofrece las siguientes opciones: Simple AD, AD Connector o, AWS Directory Service para Microsoft Active Directory, también conocido como Microsoft AD AWS administrado. Para obtener más información, consulte la Guía de administración de AWS Directory Service.

Para obtener más información sobre la AppStream versión 2.0, consulte Comenzar con Amazon AppStream 2.0: configuración con aplicaciones de muestra. AppStream La versión 2.0 administra AWS los recursos necesarios para alojar y ejecutar sus aplicaciones, se amplía automáticamente y proporciona acceso a los usuarios cuando lo soliciten. AppStream La versión 2.0 proporciona a los usuarios acceso a las aplicaciones que necesitan en el dispositivo que elijan, con una experiencia de usuario fluida y con capacidad de respuesta que es indistinguible de las aplicaciones instaladas de forma nativa.

Para obtener información sobre WorkSpaces Secure Browser, consulte Introducción a Amazon WorkSpaces Secure Browser. Amazon WorkSpaces Secure Browser es un servicio bajo demanda, totalmente gestionado y basado en Linux, diseñado para facilitar el acceso seguro del navegador a sitios web y aplicaciones (software-as-a-service SaaS) internas. Acceda al servicio desde los navegadores web existentes, sin la carga administrativa que supone la administración de la infraestructura, software cliente especializado o soluciones de redes privadas virtuales (VPN).

El siguiente diagrama muestra la arquitectura de Thin Client. WorkSpaces


Amazon WorkSpaces Thin Client AWS Managed Resources
Actions can also be performed through AWS CLI
Admin
Navigates
1.1
Amazon WorkSpaces Thin Client Console
AWS Console
Manage
- Environments
- Devices
- Software updates
1.2
Amazon WorkSpaces Thin Client Microservices
Admin workflow
Auth
Streaming
Other traffic
1.3
Runtime Dependencies
Amazon CloudWatch
AWS Key Management Service
1.4
WorkSpaces
AppStream 2.0
WorkSpaces Secure Browser
Users
2.1
Amazon WorkSpaces Thin Client
Streams
2.3
2.2 Authenticate
IdP

Configuración de la consola de administración de Amazon WorkSpaces Thin Client

Temas

Inscripción en AWS

Si no tiene una Cuenta de AWS, complete los siguientes pasos para crearla.

Para suscribirte a una Cuenta de AWS

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

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

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

Creación un usuario de IAM

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

Elegir una forma de administrar el administrador	Para	Haga esto	También puede
En IAM Identity Center (recomendado)	Usar credenciales a corto plazo para acceder a AWS. Esto se ajusta a 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 .	Configure el acceso programático configurando el AWS CLI que se utilizará AWS IAM Identity Center en la Guía del AWS Command Line Interface usuario.
En IAM (no recomendado)	Usar 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.	Configurar el acceso programático mediante Administración de las claves de acceso de los usuarios de IAM en la Guía del usuario de IAM.

Introducción a su VDI para Amazon WorkSpaces Thin Client

Amazon WorkSpaces Thin Client es un dispositivo de cliente ligero rentable diseñado para funcionar con los servicios de informática de usuario AWS final y proporcionarle un acceso seguro e instantáneo a las aplicaciones y escritorios virtuales.

Elija una infraestructura de escritorio virtual (VDI) y configúrela para que funcione con WorkSpaces Thin Client.

> **Important**
>
> Para que la consola de administración de WorkSpaces Thin Client funcione correctamente, el sistema debe cumplir primero unos requisitos específicos. Estos requisitos se enumeran en el procedimiento de configuración de cada proveedor de escritorios virtuales.

WorkSpaces Thin Client requiere configuraciones de software específicas, según el proveedor de escritorios virtuales.

Temas

Configuración WorkSpaces para Amazon WorkSpaces Thin Client

Para que WorkSpaces Thin Client se utilice con Amazon WorkSpaces, el servicio tendrá que estar configurado para acceder a los WorkSpaces directorios. Amazon WorkSpaces aparece en función de sus nombres de directorio en la página del entorno WorkSpaces Thin Client Create de AWS la consola.

> **Note**
>
> Las configuraciones se deben realizar antes de utilizar la consola por primera vez. No se recomienda modificar ninguna función previa después de empezar a utilizar la consola.

Antes de empezar

Asegúrese de tener una AWS cuenta para crear o administrar una WorkSpace. Sin embargo, los usuarios de dispositivos no necesitan una AWS cuenta para conectarse a ellos y usarlos WorkSpaces.

Revise y comprenda los siguientes conceptos antes de continuar con la configuración:

- Al lanzar un paquete WorkSpace, seleccione un WorkSpace paquete. Para obtener más información, consulta Amazon WorkSpaces Bundles.
- Al lanzar un paquete WorkSpace, selecciona el protocolo que quieres usar con el paquete. Para obtener más información, consulte Protocols for Amazon WorkSpaces.
- Al lanzar una WorkSpace, especifique la información del perfil de cada usuario, incluidos el nombre de usuario y la dirección de correo electrónico. Los usuarios completan sus perfiles creando una contraseña. La información sobre WorkSpaces los usuarios se almacena en un directorio. Para obtener más información, consulte Administrar directorios para WorkSpaces.
- Al lanzar un WorkSpace, habilite y configure el acceso a la WorkSpaces web. Para obtener más información, consulte Habilitar y configurar Amazon WorkSpaces Web Access

Paso 1: Compruebe que el sistema cumpla con las funciones WorkSpaces requeridas

Para que la consola de administración de WorkSpaces Thin Client funcione correctamente con Amazon WorkSpaces, el sistema debe cumplir los siguientes requisitos específicos. En esta tabla se enumeran todas estas funciones compatibles y sus requisitos.

Característica	Requisito
Acceso web	Habilitado
Sistemas operativos compatible	• Windows 10 • Windows 10 (Traiga su propia licencia) • Windows 11 • Windows 10 (Traiga su propia licencia)

Característica	Requisito
Paquetes compatibles	• Microsoft Power con Windows 10 (basado en servidores de 2016, 2019 y 2022) • Microsoft Power con Windows 10 (basado en Server 2016, 2019 y 2022) con Office • Microsoft PowerPro con Windows 10 (basado en Server 2016, 2019 y 2022) • Microsoft PowerPro con Windows 10 (basado en Server 2016, 2019 y 2022) w Office • Rendimiento de Microsoft con Windows 10 (basado en servidores de 2016, 2019 y 2022) • Rendimiento de Microsoft con Windows 10 (basado en Server 2016, 2019 y 2022) con Office
Protocolos admitidos	Solo WSP

Paso 2: Utilice la configuración avanzada para iniciar su WorkSpace

Para usar la configuración avanzada para iniciar su WorkSpace

1. Abra la WorkSpaces consola enhttps://console.aws.amazon.com/workspaces/.
2. Elija uno de los siguientes tipos de directorio y, a continuación, seleccione Siguiente:
   - AWS Managed Microsoft AD
   - AD sencillo
   - Conector de AD
3. Ingrese la información del directorio.
4. Elija dos subredes en una VPC de dos zonas de disponibilidad diferentes. Para obtener más información, consulte Configurar una VPC con subredes públicas.
5. Revise la información del directorio y seleccione Crear directorio.

Configuración de la AppStream versión 2.0 para Amazon WorkSpaces Thin Client

AppStream Las instancias 2.0 se enumerarán en función de los nombres de las pilas y requerirán que se configure una URL de inicio de sesión del IdP en la página de creación del entorno. Como la autenticación SAML para la AppStream versión 2.0 solo admite la autenticación iniciada, el administrador tendrá que introducir manualmente la URL de inicio de sesión correcta.

> **Note**
>
> Las configuraciones se deben realizar antes de utilizar la consola por primera vez. No se recomienda modificar ninguna función previa después de empezar a utilizar la consola.

Paso 1: Compruebe que el sistema cumpla con las funciones necesarias de la AppStream versión 2.0

Para que la consola de administración de WorkSpaces Thin Client funcione correctamente con la AppStream versión 2.0, el sistema debe cumplir los siguientes requisitos específicos. En esta tabla se enumeran todas estas funciones compatibles y sus requisitos.

Característica	Requisito
Proveedor de identidad	Para crear un proveedor de identidad, consulte Configuración de SAML en la Guía del administrador de la AppStream versión 2.0. Cuando se le pida que cree una consola env, introduzca la URL de inicio de sesión de su IDP.
Sistema operativo	Windows
Tipos de plataformas	Windows Server (2012 R2, 2016 o 2019)
Protocolo de transmisión	Transmisión TCP

Característica	Requisito
	Hay un mecanismo de retorno automático a TCP si UDP no está disponible.
Copiar y pegar de forma local	Deshabilitado Configurado a nivel de AppStream pila 2.0
Uso compartido de carpetas locales	Deshabilitado Configurado a nivel de pila AppStream 2.0
Impresión local	Deshabilitado Configurado a nivel de pila AppStream 2.0

También se admite el requisito de bloqueo de pantalla mediante la autenticación SAML en la AppStream versión 2.0. El grupo de usuarios y los mecanismos de autenticación programática no son compatibles con WorkSpaces Thin Client.

Paso 2: Configura tus pilas AppStream 2.0

Para transmitir sus aplicaciones, la AppStream versión 2.0 requiere un entorno que incluya una flota asociada a una pila y al menos una imagen de la aplicación. Siga estos pasos para configurar una flota y una pila y dar a los usuarios acceso a la pila. Si aún no lo ha hecho, le recomendamos que pruebe los procedimientos de Get Started with AppStream 2.0: Set Up With Sample Applications.

Si desea crear una imagen para utilizarla, consulte el tutorial: Creación de una imagen AppStream 2.0 personalizada mediante la consola AppStream 2.0.

Si tiene previsto unir una flota a un dominio de Active Directory, configure su dominio de Active Directory antes de realizar los pasos siguientes. Para obtener más información, consulte Uso de Active Directory con la AppStream versión 2.0.

Tareas

- Creación de una flota
- Creación de una pila
- Acceso para los usuarios

- Eliminación de recursos

Configuración de Amazon WorkSpaces Secure Browser para Amazon WorkSpaces Thin Client

Amazon WorkSpaces Secure Browser se basa en los puntos de enlace de su portal web en la página WorkSpaces Thin Client Create del entorno de la AWS consola.

> **Note**
>
> Las configuraciones se deben realizar antes de utilizar la consola por primera vez. No se recomienda modificar ninguna función previa después de empezar a utilizar la consola.

Paso 1: Comprueba que tu sistema cumple con las funciones requeridas por Amazon WorkSpaces Secure Browser

Para que WorkSpaces Thin Client Administrator Console funcione correctamente con Amazon WorkSpaces Secure Browser, el sistema debe cumplir los siguientes requisitos específicos. En esta tabla se enumeran todas estas funciones compatibles y sus requisitos.

Característica	Requisito
Copiar y pegar de forma local	Deshabilitado
Uso compartido de carpetas locales	Deshabilitado

> **Note**
>
> La extensión WorkSpaces Secure Browser para el inicio de sesión único no es compatible actualmente con WorkSpaces Thin Client.

Paso 2: Configurar los portales de WorkSpaces Secure Browser

WorkSpaces Thin Client funciona con la VPC de WorkSpaces Secure Browser en una configuración específica:

1. Cree una VPC con la plantilla de AWS CodeBuild Cloudformation.
2. Configure el proveedor de identidades.
3. Cree un portal de Amazon WorkSpaces Secure Browser.
4. Pruebe su nuevo portal Amazon WorkSpaces Secure Browser.

Inicio de la consola de administración de WorkSpaces Thin Client

WorkSpaces Thin Client es un dispositivo de cliente ligero rentable diseñado para funcionar con los servicios informáticos de usuario AWS final y proporcionarle un acceso seguro e instantáneo a las aplicaciones y escritorios virtuales.

Temas

Regiones cubiertas

WorkSpaces Thin Client está disponible en las siguientes regiones.

Solo la consola de administración de WorkSpaces Thin Client está disponible en estas regiones. WorkSpaces Los dispositivos Thin Client solo están disponibles actualmente en EE. UU., Alemania, Francia, Italia y España.

Nombre de la región	Región	Punto de conexión	Enlace a la consola
Este de EE. UU. (Norte de Virginia)	us-east-1	thinclient.us-east-1.amazonaws.com	https://us-east-1.console.aws.amazon.com/workspaces-thin-client/home
Oeste de EE. UU. (Oregón)	us-west-2	thinclient.us-west-2.amazonaws.com	https://us-west-2.console.aws.amazon.com/workspaces-thin-client/home
Asia Pacífico (Mumbai)	ap-south-1	thinclient.ap-south-1.amazonaws.com	https://ap-south-1.console.aws.amazon.com/workspaces-thin-client/home

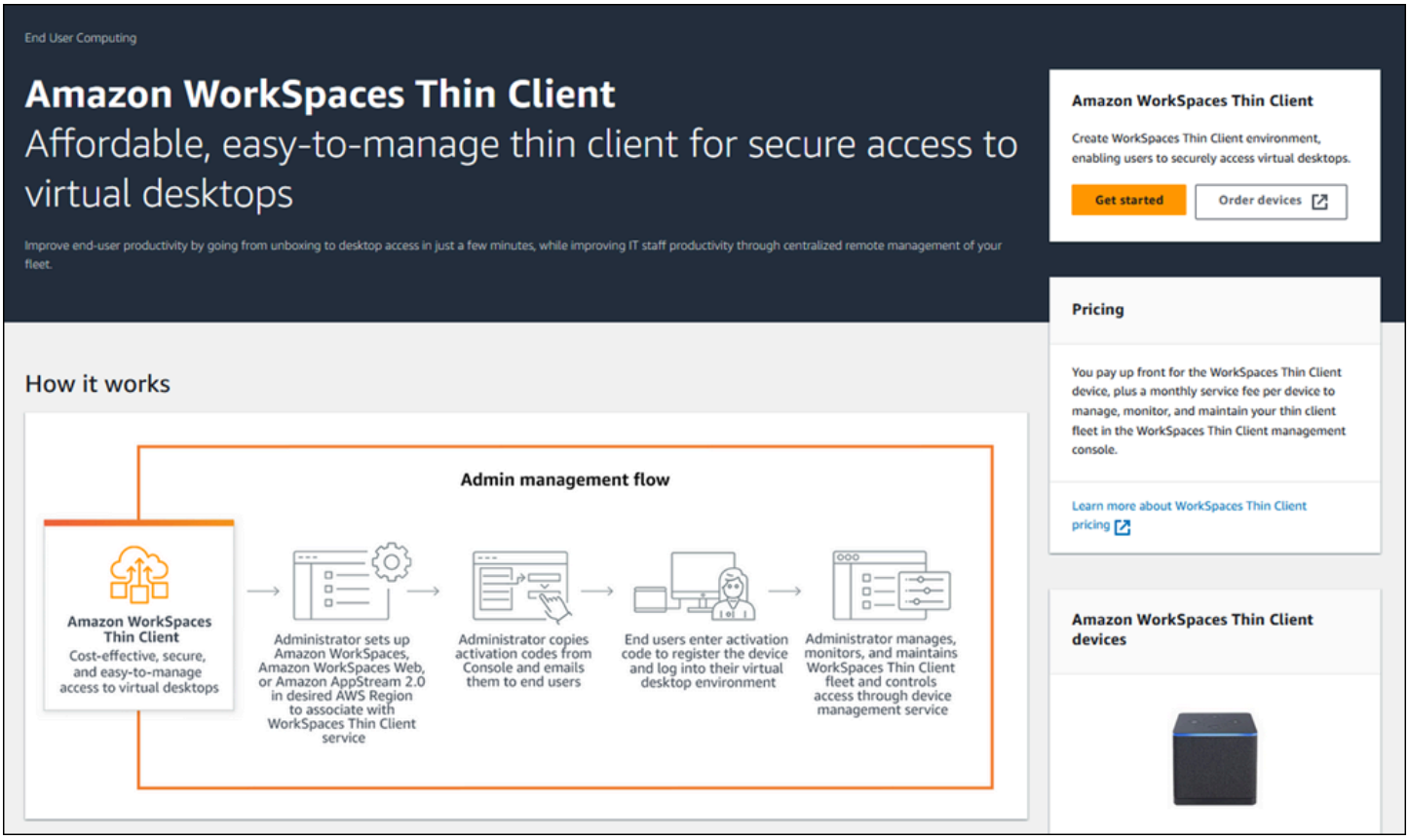
Nombre de la región	Región	Punto de conexión	Enlace a la consola
Europa (Irlanda)	eu-west-1	thinclient.eu-west-1.amazonaws.com	https://eu-west-1.console.aws.amazon.com/workspaces-thin-client/home
Canadá (Central)	ca-central-1	thinclient.ca-central-1.amazonaws.com	https://ca-central-1.console.aws.amazon.com/workspaces-thin-client/home
Europa (Frankfurt)	eu-central-1	thinclient.eu-central-1.amazonaws.com	https://eu-central-1.console.aws.amazon.com/workspaces-thin-client/home
Europa (Londres)	eu-west-2	thinclient.eu-west-2.amazonaws.com	https://eu-west-2.console.aws.amazon.com/workspaces-thin-client/home

Inicio de la consola de administración de WorkSpaces Thin Client

Si tiene una AWS cuenta, puede iniciar la consola de administración e ir a la consola WorkSpaces Thin Client. Para iniciar la consola, haga lo siguiente:

1. Inicie sesión en su AWS cuenta.
2. Acceda a la consola WorkSpaces Thin Client.
3. Seleccione Iniciar y se le redirigirá a Entornos.

Uso de la consola de administración de WorkSpaces Thin Client



¡Bienvenido a la consola de administración de WorkSpaces Thin Client!

Desde aquí, puede gestionar su flota de dispositivos y entornos WorkSpaces Thin Client para su equipo.

Para obtener información sobre el dispositivo WorkSpaces Thin Client, consulte la Guía del usuario de WorkSpaces Thin Client.

Comencemos.

Temas

Entornos

Cada dispositivo WorkSpaces Thin Client utiliza un entorno de escritorio virtual individual para acceder a sus recursos en línea. Los usuarios acceden a este entorno mediante uno de los siguientes proveedores de escritorios virtuales:

- Amazon WorkSpaces
- AppStream 2.0
- Navegador Amazon WorkSpaces Secure

Lista de entornos

Detalles de la lista de entornos

Nombre: el identificador único asociado a este entorno.

Servicio de escritorio virtual: el proveedor de escritorio virtual que utiliza este entorno.

ID del servicio de escritorio virtual: el identificador único que el proveedor de servicios de escritorio virtual asigna a este entorno.

Código de activación: el código que utilizan los usuarios finales para acceder al entorno de escritorio virtual.

Recuento de dispositivos: el número de dispositivos WorkSpaces Thin Client que acceden a este entorno.

Acciones de la lista de entornos

Buscar: busca en todos los entornos que administra.

Actualizar: actualiza la lista de entornos.

Ver detalles: muestra Detalles del entorno.

Acciones: abre una lista desplegable en la que puede editar o eliminar un entorno.

Crear entorno: inicia el proceso de creación de un entorno

Crear entorno: inicia el proceso de creación de un entorno.

Temas

Detalles del entorno

Al seleccionar un entorno, la consola WorkSpaces Thin Client muestra los detalles de ese entorno para que los revise. La consola también muestra los detalles sobre el proveedor de escritorios virtuales que utiliza este entorno.

Temas

Resumen

Nombre: el identificador único asociado a este entorno.

Servicio de escritorio virtual: el proveedor de escritorio virtual que utiliza este entorno.

ID de servicio de escritorio virtual: el identificador único que el proveedor de servicios de escritorio virtual asigna a este entorno.

Código de activación: este código es el que utilizan los usuarios finales para acceder al entorno de escritorio virtual.

Conservar siempre el software up-to-date: esta configuración permite las actualizaciones automáticas del software.

Hora de inicio del período de mantenimiento: hora de cada semana en la que comienzan las actualizaciones automáticas del software.

Hora de finalización del período de mantenimiento: hora de cada semana en la que finalizan las actualizaciones automáticas de software.

Periodo de mantenimiento (días de la semana): los días en los que se producen las actualizaciones automáticas de software.

Dispositivos asociados: la cantidad de dispositivos WorkSpaces Thin Client que acceden a este entorno.

Hora de creación: fecha y hora en que se creó este entorno.

Detalles del entorno de escritorio virtual

Detalles del WorkSpaces directorio de Amazon

ID de directorio: el WorkSpaces directorio de Amazon asociado a este entorno.

Nombre del directorio: el identificador único asociado a este WorkSpaces directorio de Amazon.

Nombre de la organización: el nombre de la organización que controla el WorkSpaces directorio de Amazon.

Tipo de directorio: el formato del WorkSpaces directorio de Amazon.

Registrado: si este WorkSpaces directorio de Amazon está registrado.

Estado: si este WorkSpaces directorio de Amazon está activo.

Detalles del portal Amazon WorkSpaces Secure Browser

Nombre: el identificador único asociado a este portal de Amazon WorkSpaces Secure Browser.

Hora de creación: fecha y hora en que se creó esta pila AppStream 2.0.

Punto de conexión del portal web: la URL que se utiliza para acceder a su entorno de escritorio virtual.

AppStream Detalles de la versión 2.0

Nombre de la pila: el identificador único asociado a esta pila AppStream 2.0.

URL de inicio de sesión del IdP: la URL del proveedor de identidad que se utiliza para iniciar y cerrar sesión en tu pila AppStream 2.0.

Hora de creación: fecha y hora en que se creó esta pila AppStream 2.0.

Creación de un entorno

Para empezar, cada dispositivo requiere un servicio informático para el usuario AWS final. WorkSpaces Thin Client utiliza los siguientes servicios:

- Amazon WorkSpaces a través de un directorio asignado
- AppStream 2.0 a través de una pila asignada
- Amazon WorkSpaces Secure Browser a través de una dirección de portal web

Debe asignar un servicio a un entorno existente o crear uno nuevo.

> **Note**
>
> WorkSpaces Thin Client solo muestra los escritorios virtuales de la misma región.

Temas

Paso 1: introducción de los detalles de su entorno

1. Ingrese un nombre para su entorno en el campo Detalles del entorno.
2. Para configurar los parches de software automáticos, marque la casilla Conservar siempre el software up-to-date.

> **Note**
>
> Si las actualizaciones automáticas de software no están habilitadas, los dispositivos registrados en este entorno no recibirán las actualizaciones de software hasta que la actualices manualmente o cuando el software caduque y el sistema fuerce una actualización.
> Además, el sistema determina la versión del conjunto de software del dispositivo. Es posible que esta versión no sea la más reciente.

3. Seleccione cuándo desea programar el período de mantenimiento de su entorno.

   - Aplique un período de mantenimiento a todo el sistema: actualiza automáticamente el software del entorno a una hora determinada cada semana.
   - Aplicar periodo de mantenimiento personalizado: establezca el día y la hora en que desea que el software del entorno se actualice cada semana.

4. Seleccione un servicio de escritorio virtual.

   - Amazon WorkSpaces
   - Navegador Amazon WorkSpaces Secure
   - AppStream 2.0

Paso 2: selección del proveedor de escritorio virtual

Debe disponer de un servicio para proporcionar a los usuarios acceso a su escritorio virtual y a los recursos compatibles.

> **Important**
>
> Para que la consola de administración de WorkSpaces Thin Client funcione correctamente, el sistema debe cumplir requisitos específicos. Estos requisitos se detallan en Requisitos previos y configuraciones.
> Asegúrese de que el sistema cumpla estos requisitos antes de configurar la consola.

Uso de Amazon WorkSpaces

Amazon WorkSpaces es un servicio de virtualización de escritorios totalmente gestionado para Windows que le permite acceder a los recursos desde cualquier dispositivo compatible.

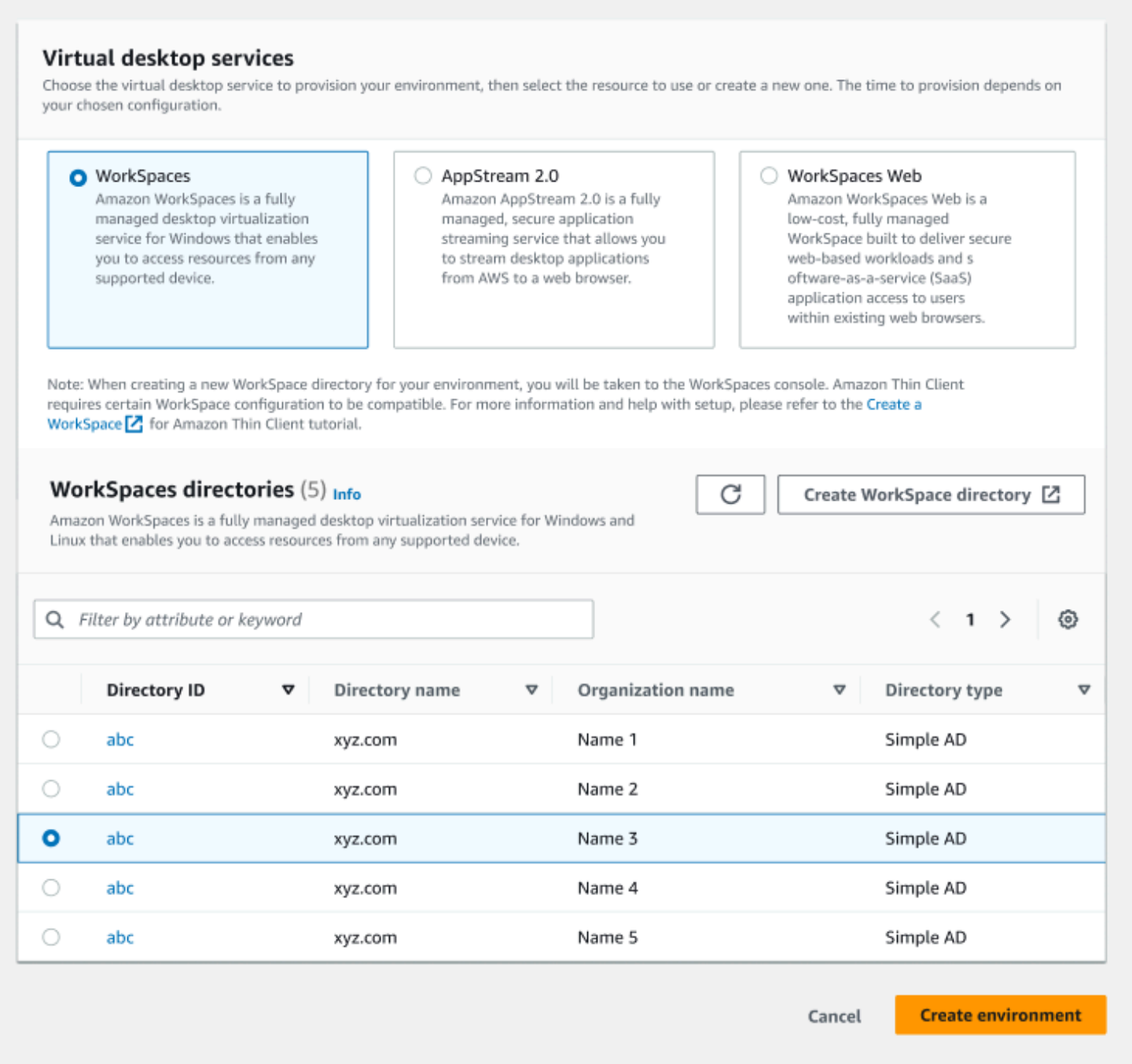
1. Para usar Amazon WorkSpaces, realiza una de las siguientes acciones:

   - Seleccione el directorio que desea utilizar para su entorno. Puedes navegar por la lista desplegable o buscar en los directorios mediante el campo de búsqueda.

> **Note**
>
> Si no ve los directorios existentes en la lista, compruebe en la consola de WorkSpaces administración que cumplen los requisitos de WorkSpaces Thin Client.

- Cree un directorio pulsando el botón Crear WorkSpaces directorio. Para obtener más información sobre la creación de WorkSpaces directorios, consulte Administrar directorios para WorkSpaces.

2. Seleccione el botón Crear entorno.



Cuando cree su entorno, podrá seguir editando los detalles más adelante. Para obtener más información, consulte Edición de un entorno.

Usando AppStream 2.0

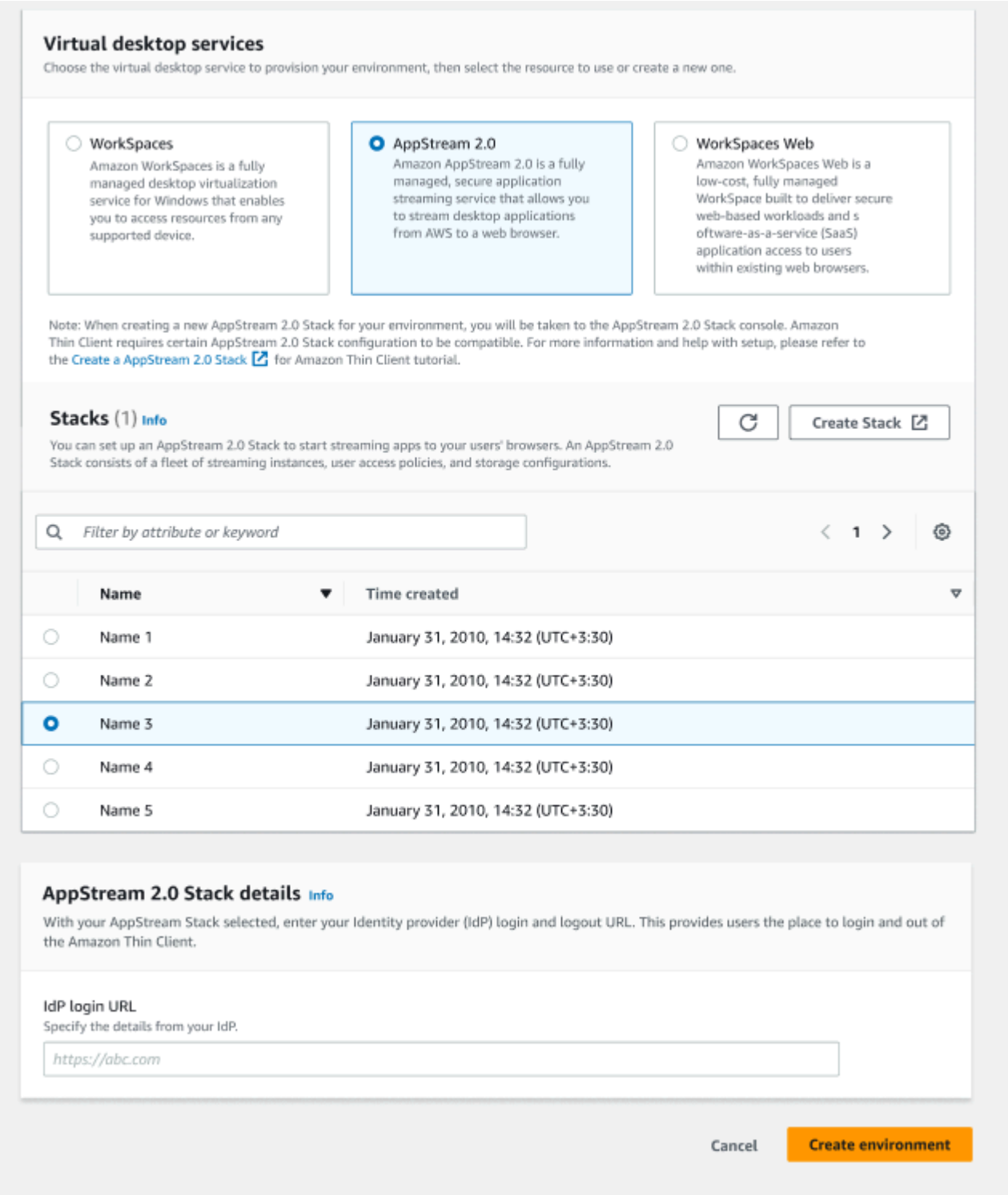
AppStream 2.0 es un servicio de streaming de aplicaciones seguro y totalmente gestionado que puede utilizar para transmitir aplicaciones de escritorio desde AWS un navegador web.

> **Warning**
>
> Para crear un entorno AppStream 2.0, debe haber `cli_follow_urlparam` configurado`false`. Para ello, haga lo siguiente:
>
> - Para un perfil predeterminado, ejecute `aws configure set cli_follow_urlparam false`.
> - Para un perfil con nombre `ProfileName`, ejecute `aws configure set cli_follow_urlparam false --profile ProfileName`.

1. Para configurar la AppStream versión 2.0, realice una de las siguientes acciones:
   - Seleccione la pila que quiere utilizar para su entorno. Puedes navegar por la lista desplegable o buscar las pilas mediante el campo de búsqueda.

     > **Note**
     >
     > Si las pilas existentes no aparecen en la lista, compruebe en la consola de administración AppStream 2.0 que cumplen los requisitos de WorkSpaces Thin Client.

   - Cree una pila seleccionando el botón Crear pila. Para obtener más información sobre la creación de pilas AppStream 2.0, consulta Crear una pila.
2. Ingrese la URL de inicio y cierre de sesión de su proveedor de identidad en el campo URL de inicio de sesión del IdP. Esto proporciona a los usuarios un lugar para iniciar y cerrar sesión en WorkSpaces Thin Client.
3. Seleccione el botón Crear entorno.



Después de crear el entorno, podrá seguir editando los detalles más adelante. Para obtener más información, consulte Edición de un entorno.

Uso de Amazon WorkSpaces Secure Browser

Amazon WorkSpaces Secure Browser es una WorkSpaces consola de bajo coste y totalmente gestionada que está diseñada para ofrecer a los usuarios cargas de trabajo seguras basadas en la web y acceso a aplicaciones de software como servicio (SaaS) desde los navegadores web existentes.

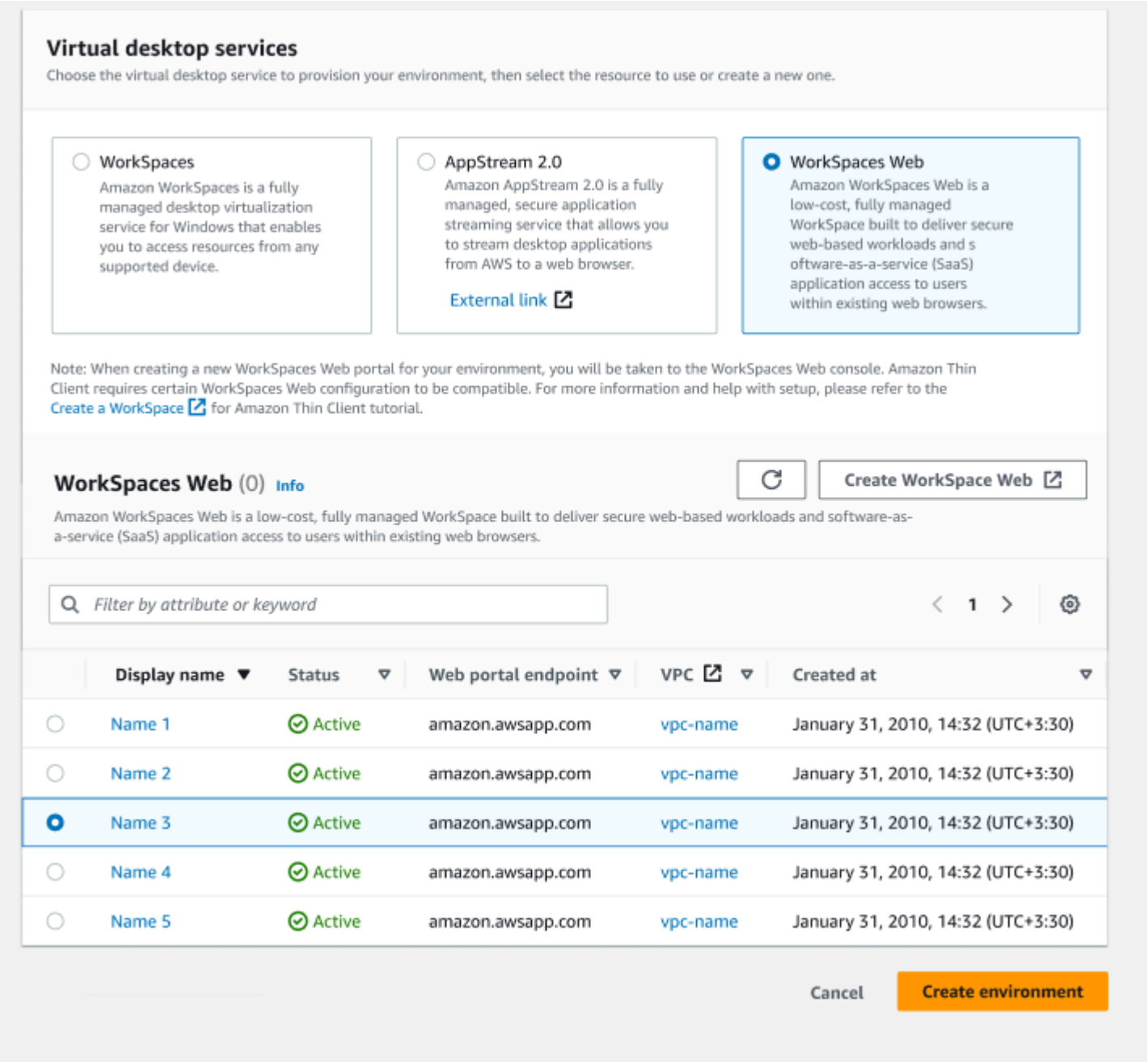
1. Para configurar Amazon WorkSpaces Secure Browser, realice una de las siguientes acciones:

   - Seleccione el portal web que desee utilizar para su entorno. Puede navegar por la lista desplegable o buscar en los portales web mediante el campo de búsqueda.

     > **Note**
     >
     > Si no ve sus portales web actuales en la lista, compruebe en la consola de administración de WorkSpaces Secure Browser que cumplen los requisitos de WorkSpaces Thin Client.

   - Cree un portal web seleccionando el botón Crear navegador WorkSpaces seguro. Para obtener más información sobre la creación de portales web de WorkSpaces Secure Browser, consulte Configuración de Amazon WorkSpaces Secure Browser.

2. Seleccione el botón Crear entorno.



Después de crear el entorno, podrá seguir editando los detalles más adelante. Para obtener más información, consulte Edición de un entorno.

Paso 3: envío del código de activación a los usuarios de su dispositivo

Después de configurar el entorno y el servicio de escritorio virtual, recibirá un código de activación único para la configuración en la consola AWS de administración.

Proporcione este código de activación a cualquier usuario de un dispositivo WorkSpaces Thin Client y podrá usarlo para acceder a su escritorio virtual.

Consulte la Guía del usuario de WorkSpaces Thin Client para obtener información adicional sobre cómo ayudar al usuario de su dispositivo a configurar su Amazon WorkSpaces Thin Client.

Edición de un entorno

La consola de administración de WorkSpaces Thin Client administra los entornos de escritorios virtuales para los usuarios individuales. Desde esta consola, puede editar o eliminar entornos de escritorios virtuales.

1. Seleccione el entorno que quiere editar.

   > **Note**
   >
   > Puede navegar por la lista desplegable o buscar en los entornos mediante el campo de búsqueda.

2. Selecciona el botón Acciones.
3. Selecciona Editar en la lista desplegable. Se le dirigirá a la ventana Editar entorno.
4. Edite cualquiera de los siguientes elementos:
   - Cambie el nombre de su entorno en el campo Nombre del entorno.
   - Cambie la casilla de verificación de los detalles de las actualizaciones de software para las actualizaciones de parches de software automáticas.
   - Cambie cuándo quiere programar el periodo de mantenimiento para su entorno.
5. Seleccione el botón Editar entorno.

Eliminación de un entorno

> **Note**
>
> No puede eliminar un entorno si tiene algún dispositivo registrado en él. En primer lugar, debe anular el registro y eliminar todos los dispositivos de un entorno.

1. Seleccione el entorno que quiere eliminar. Puede navegar por la lista desplegable o buscar en los entornos mediante el campo de búsqueda.
2. Selecciona el botón Acciones.
3. Selecciona Eliminar en la lista desplegable. Aparece la ventana de confirmación de eliminación del entorno.
4. Escriba “eliminar” en el campo de confirmación.
5. Seleccione el botón Eliminar.

Dispositivos

Cada usuario final de WorkSpaces Thin Client tiene un dispositivo dedicado que lo conecta a sus entornos de escritorios virtuales y recursos en línea. Estos dispositivos se administran a través de la consola de administración de WorkSpaces Thin Client del AWS sitio.

Desde esta consola, puede solicitar dispositivos para su equipo.

Lista de dispositivos

Detalles de la lista de dispositivos

ID de dispositivo: el número de identificación asignado a un dispositivo individual.

Nombre del dispositivo: (opcional) el nombre exclusivo que se le da a un dispositivo.

Estado de actividad: el estado actual de un dispositivo. Hay dos estados de estado:

- Activo: se conectó a una red al menos una vez en los últimos siete días.
- Inactivo: no se conectó a una red en los últimos siete días.

Estado de inscripción: confirmación de que un dispositivo se ha configurado, está asociado a esta AWS cuenta y forma parte de un entorno específico. Puede estar en uno de los siguientes estados:

- Registrado: este es el estado predeterminado.
- Anulación del registro: el dispositivo se encuentra en proceso de restablecimiento y anulación del registro.

> **Note**
>
> Puedes eliminar un dispositivo si se está cancelando el registro.

- Registro anulado: se ha anulado correctamente el registro del dispositivo.

> **Note**
>
> Solo puedes eliminar un dispositivo si está en estado Anulado o Anulado el registro.

- Archivado: el dispositivo está archivado.

ID del entorno: el identificador del entorno al que está conectado este dispositivo.

Cumplimiento de software: estado de conformidad del software del dispositivo. Hay dos estados de estado:

- Conforme
- No cumple con los requisitos

Acciones de la lista de dispositivos

Buscar: busca en todos los dispositivos que administra.

Actualizar: actualiza la lista de dispositivos.

Ver detalles: muestra Detalles del dispositivo.

Acciones: abre una lista desplegable en la que puede hacer lo siguiente:

- Editar nombre del dispositivo
- Anular registro
- Archivado
- Delete
- Exportar detalles del dispositivo

Pedir dispositivos: inicia el proceso de pedido de dispositivos.

Temas

Detalles del dispositivo

Resumen

Número de serie del dispositivo: el número de identificación asignado a un dispositivo individual.

ARN: el identificador único del dispositivo en formato Amazon Resource Name (ARN).

Nombre del dispositivo: el nombre que le das a un dispositivo. Si no ha creado un nombre, puede asignarle un nombre o tendrá un nombre predeterminado.

Tipo de dispositivo: el tipo de dispositivo del usuario final que está vinculado a la cuenta.

Estado de la actividad: el estado actual de este dispositivo. Los dos estados de estado son:

- Activo
- Inactivo

ID de entorno: el número de identificación del entorno que utiliza el dispositivo.

Estado de inscripción: confirmación de que un dispositivo se ha configurado, está asociado a esta AWS cuenta y forma parte de un entorno específico. Puede estar en uno de los cuatro estados siguientes:

- Registrado: este es el estado predeterminado.
- Anulación del registro: el dispositivo se encuentra en proceso de restablecimiento y anulación del registro.
- Registro anulado: se ha anulado correctamente el registro del dispositivo.

> **Note**
>
> Solo puedes eliminar el dispositivo si está archivado o dado de baja.

- Archivado: el administrador ha marcado este dispositivo como no en servicio actualmente.

Inscrito desde: la fecha en la que se activó el dispositivo.

Último inicio de sesión: la fecha y la hora del último inicio de sesión.

Última postura comprobada: fecha y hora de la última revisión del dispositivo.

Versión de software actual: la versión de software que utiliza actualmente este dispositivo.

Actualización de software programada: la versión de software programada del dispositivo.

Cumplimiento de software: confirmación de que el conjunto de software es válido. Hay dos estados de estado:

- Conforme
- No cumple con los requisitos

Registro de usuario

Último acceso al dispositivo: fecha y hora en que se utilizó este dispositivo por última vez.

Edición de un nombre de dispositivo

1. Seleccione el dispositivo que quiere editar. Puedes navegar por la lista desplegable o buscar el dispositivo mediante el campo de búsqueda.
2. Selecciona el botón Acciones.
3. Selecciona Editar el nombre del dispositivo en la lista desplegable. Aparece la ventana Editar el nombre del dispositivo.
4. Ingrese el nuevo nombre del dispositivo en el campo de confirmación Nombre del dispositivo.
5. Seleccione el botón Guardar.

Restablecimiento y anulación del registro de un dispositivo

1. Seleccione el dispositivo del que quiere anular el registro. Puede navegar por la lista desplegable o buscar el dispositivo mediante el campo de búsqueda.
2. Selecciona el botón Acciones.
3. Selecciona Anular registro en la lista desplegable. Aparece la ventana Anular el registro.
4. Escriba "anular registro" en el campo de confirmación.
5. Seleccione el botón Anular registro.

> **Note**
>
> Al anular el registro forzosamente, se cierra la sesión del usuario y es necesario reiniciar su dispositivo WorkSpaces Thin Client en mitad de la sesión.

Archivado de un dispositivo

1. Seleccione el dispositivo que quiere archivar. Puede navegar por la lista desplegable o buscar el dispositivo mediante el campo de búsqueda.
2. Selecciona el botón Acciones.
3. Selecciona Archivar en la lista desplegable. Aparece la ventana Archivar.
4. Escriba "restablecer y archivar" en el campo de confirmación.
5. Seleccione el botón Restablecer y archivar.

> **Note**
>
> Al archivar un dispositivo, se cierra la sesión del usuario por la fuerza y es necesario reiniciar el dispositivo WorkSpaces Thin Client en mitad de la sesión.

Eliminar un dispositivo

1. Seleccione el dispositivo que desea eliminar. Puede navegar por la lista desplegable o buscar el dispositivo mediante el campo de búsqueda.

2. Selecciona el botón Acciones.
3. Selecciona Eliminar en la lista desplegable. Aparece la ventana Eliminar.
4. Escriba "eliminar" en el campo de confirmación.
5. Seleccione el botón Eliminar.

> **Note**
>
> Cuando el dispositivo se haya eliminado correctamente, el usuario debe devolver el dispositivo WorkSpaces Thin Client a Amazon.

Exportación de los detalles del dispositivo

1. Seleccione el dispositivo del que quiere exportar los detalles. Puede navegar por la lista desplegable o buscar el dispositivo mediante el campo de búsqueda.
2. Selecciona el botón Acciones.
3. Selecciona Exportar detalles del dispositivo en la lista desplegable. Los detalles del dispositivo seleccionado se descargan en formato de hoja de cálculo.

Actualizaciones de software

WorkSpaces A veces, Thin Client requiere actualizaciones de software que introduzcan nuevas funcionalidades y apliquen parches de seguridad. Estas actualizaciones se representan mediante un conjunto de software versionado.

Un conjunto de software puede contener actualizaciones de las aplicaciones de software o del sistema operativo del dispositivo WorkSpaces Thin Client. Desde esta consola, puede optar por actualizar el software inmediatamente o programar una actualización automática durante el período de mantenimiento de los entornos.

Consulte los conjuntos de software para entornos WorkSpaces Thin Client para ver la lista de conjuntos de software publicados.

Temas

- Actualización del software del entorno

- Actualización del software del dispositivo
- WorkSpaces Versiones del software Thin Client

Actualización del software del entorno

WorkSpaces Thin Client es un servicio informático para el usuario AWS final que proporciona a los usuarios acceso a escritorios virtuales. Estos escritorios virtuales se actualizan periódicamente con nuevos conjuntos de software. Para actualizar el software del entorno, haga lo siguiente:

1. Seleccione el conjunto de software de la lista en Actualizaciones de software disponibles. Para obtener una lista de conjuntos de software, consulte los conjuntos de software de entorno WorkSpaces Thin Client.
2. Seleccione el botón Instalar.
3. Seleccione Entornos en la parte superior de la página.
4. Seleccione el entorno que desee actualizar de la lista de la sección Entornos.
5. Seleccione cuándo se actualizará el entorno en la sección Programar la actualización y elija una de las siguientes opciones:

   - Actualizar software ahora: inicia la actualización del software del entorno en todos los dispositivos registrados.

     > **Note**
     >
     > Si se actualiza el software ahora, es posible que se interrumpan las sesiones de usuario activas.

   - Actualizar el software durante el período de mantenimiento de cada entorno: actualiza el software del entorno durante el período de mantenimiento programado del entorno.
6. Marque la casilla para autorizar la actualización. Esta casilla debe estar marcada para que el software se actualice.
7. Seleccione el botón Instalar.

Actualización del software del dispositivo

WorkSpaces Thin Client es un servicio informático para usuarios AWS finales que proporciona un dispositivo de cliente ligero que conecta a los usuarios con escritorios virtuales dedicados. Estos

dispositivos se actualizan periódicamente con software nuevo. Para actualizar el software del dispositivo, haga lo siguiente:

1. Seleccione el conjunto de software de la lista en Actualizaciones de software disponibles.
2. Selecciona el botón Instalar.
3. Seleccione Dispositivo en la parte superior de la página.
4. Seleccione el dispositivo o los dispositivos que desee actualizar de la lista de la sección Dispositivos. Para obtener una lista de los conjuntos de software, consulte los conjuntos de software de entorno WorkSpaces Thin Client.
5. Seleccione cuándo se actualizará el entorno en las opciones de Programar la actualización y elija una de las siguientes opciones:
   - Actualizar software ahora: actualiza inmediatamente el software del dispositivo.

     > **Note**
     >
     > Si se actualiza el software ahora, es posible que se interrumpan las sesiones de usuario activas.

   - Actualizar el software durante el período de mantenimiento de cada dispositivo: actualiza el software del entorno durante el período de mantenimiento programado del dispositivo.
6. Marque la casilla para autorizar la actualización. Esta casilla debe estar marcada para que el software se actualice.
7. Seleccione el botón Instalar.

WorkSpaces Versiones del software Thin Client

WorkSpaces Thin Client es un servicio informático para el usuario AWS final que proporciona a los usuarios acceso a los escritorios virtuales de un dispositivo. Estos dispositivos se actualizan periódicamente con nuevos conjuntos de software. En la siguiente tabla se describen todos los conjuntos de software publicados. Los administradores pueden usar la consola AWS de administración para ver los conjuntos de software disponibles.

Conjunto de software	Fecha de publicación	Cambios
2.5.0	13-06-2024	• Se solucionó el problema por el que el dispositivo mostraba brevemente la pantalla de configuración del teclado y el ratón al despertarse del modo de suspensión antes de iniciar la sesión. • Se cambió el nombre del botón de inicio de la barra de herramientas del dispositivo a Iniciar sesión. • Mejoras en el rendimiento de las llamadas de audio y vídeo de la sesión.
2.4.3	29-05-2024	• Solución de día cero para el problema de seguridad crítico CVE-2024-5274 de Chromium.
2.4.2	17-05-2024	• Solución de día cero para un problema de seguridad crítico relacionado con el CVE-2024-4947 de Chromium.
2.4.1	15-05-2024	• Correcciones inmediatas para los problemas de seguridad críticos relacionados con los CVE-2024-4671 y CVE-2024-4761 de Chromium.

Conjunto de software	Fecha de publicación	Cambios
		• Se ha corregido el problema que permitía abrir el navegador en modo independiente al hacer clic con el botón derecho en los enlaces de AWS y de privacidad de la página de WorkSpaces inicio de sesión.
2.4.0	05-09-2024	• Se ha corregido un problema al bloquear «accounts.google.com» e impedir el uso de Google Workspace como IDP en la sesión 2.0. AppStream • La barra de herramientas de configuración del dispositivo se contrae automáticamente con un clic en cualquier área de la pantalla.

Conjunto de software	Fecha de publicación	Cambios
2.3.0	04-05-2024	• La configuración del dispositivo se muestra en una barra de herramientas comprimida, lo que permite un mejor uso de la pantalla visible. • Los usuarios finales ahora pueden configurar el tiempo de espera antes de que el dispositivo entre en reposo en caso de inactividad. • Se ha corregido el problema por el que la URL «about:blank» aparecía en la segunda pantalla. • Se ha corregido el problema que provocaba que la pantalla se viera blanca cuando se cerraba la pantalla extendida. • Los niveles de volumen establecidos por los usuarios finales ahora persisten cuando el dispositivo se reinicia.
2.2.1	16/02/2024	• Se ha corregido un problema que se producía durante el proceso de inicio de sesión y que impedía a los usuarios iniciar sesión en los sistemas WorkSpaces configurados con la autenticación SAML 2.0.

Conjunto de software	Fecha de publicación	Cambios
2.2.0	02-08-2024	• Se agregó soporte para teclados ISO con configuraciones regionales en inglés (Reino Unido), francés, alemán, italiano y español.
2.1.2	26-01-2024	• Solución de día cero para el problema de seguridad crítico CVE-2024-0519 de Chromium. • Mejora de la latencia del usuario final asociada a la funcionalidad de bloqueo. • Los puntos finales internos orientados al dispositivo se cambian al dominio «thinclient*».
2.1.1	21-12-2023	• Solución de día cero para el problema de seguridad crítico CVE-2023-7024 de Chromium.
2.1.0	20-12-2023	• Añade un botón de inicio a la configuración del dispositivo y permite la compatibilidad con las teclas Meta. Esto permite a los usuarios finales invocar la pantalla de bloqueo pulsando Meta+L.
2.0.1	12-06-2023	• Solución de día cero para el problema de seguridad crítico CVE-2024-6345 de Chromium.

Conjunto de software	Fecha de publicación	Cambios
2.0.0	15-11-2023	• Versión inicial

Uso de etiquetas en los recursos de WorkSpaces Thin Client

Puede organizar y administrar los recursos de su WorkSpaces Thin Client asignando sus propios metadatos a cada recurso en forma de etiquetas. Especificará una clave y un valor para cada etiqueta. Una clave puede ser una categoría general, como "proyecto", "propietario" o "entorno", con valores específicos asociados. Puede utilizar las etiquetas como una forma sencilla pero eficaz de gestionar los recursos de AWS y organizar los datos, incluidos los datos de facturación.

Cuando agrega etiquetas a un recurso existente, esas etiquetas no aparecen en el informe de asignación de costos hasta el primer día del mes siguiente. Por ejemplo, si añade etiquetas a un dispositivo WorkSpaces Thin Client existente el 15 de julio, las etiquetas no aparecerán en su informe de asignación de costes hasta el 1 de agosto. Para obtener más información, consulte Uso de etiquetas de asignación de costos en la Guía del usuario de facturación de AWS.

> **Note**
>
> Para ver las etiquetas de recursos de WorkSpaces Thin Client en el Cost Explorer, debe activar las etiquetas que ha aplicado a los recursos de WorkSpaces Thin Client siguiendo las instrucciones de Activación de etiquetas de asignación de costes definidas por el usuario de la Guía del AWS Billing usuario.
> Las etiquetas aparecen 24 horas después de la activación, pero los valores asociados a esas etiquetas pueden tardar entre 4 y 5 días en aparecer en el Cost Explorer. Además, para que aparezcan y proporcionen datos de costos en Cost Explorer, los recursos de WorkSpaces Thin Client que se hayan etiquetado deben incurrir en cargos durante ese tiempo. Cost Explorer solo muestra los datos de costos desde el momento en que se activaron las etiquetas. No hay datos históricos disponibles en este momento.

Recursos que puede etiquetar:

- Puede añadir etiquetas a los siguientes recursos al crearlos: entornos WorkSpaces Thin Client.
- Puede agregar etiquetas a los recursos existentes de los siguientes tipos: entornos, dispositivos y conjuntos de software de WorkSpaces Thin Client.

Restricciones de las etiquetas

- Número máximo de etiquetas por recurso: 50

- Longitud máxima de la clave: 128 caracteres Unicode
- Longitud máxima del valor: 256 caracteres Unicode
- Las claves y los valores de las etiquetas distinguen entre mayúsculas y minúsculas. Los caracteres permitidos son letras, espacios y números representables en UTF-8, además de los siguientes caracteres especiales: + - = . _ : / @. No utilice espacios iniciales ni finales.
- No utilice el `aws:` prefijo en los nombres o valores de las etiquetas porque está reservado para su uso. AWS Los nombres y valores de etiquetas que tienen este prefijo no se pueden editar ni eliminar.

Para actualizar las etiquetas de un entorno existente mediante la consola

1. Abra la consola WorkSpaces Thin Client.
2. Seleccione el entorno para abrir su página de detalles
3. Elija Editar.
4. En la sección Etiquetas, realice una o más de las siguientes acciones:.
   - Para agregar una etiqueta, seleccione Agregar nueva etiqueta y, a continuación, edite los valores de Clave y Valor.
   - Para actualizar una etiqueta, edite el valor de Value.
   - Para eliminar una etiqueta, selecciona Eliminar junto a la etiqueta.
5. Cuando hayas terminado de actualizar las etiquetas, selecciona Guardar.

Para actualizar las etiquetas de un dispositivo existente mediante la consola

1. Abra la consola WorkSpaces Thin Client.
2. Seleccione el dispositivo para abrir su página de detalles.
3. Seleccione Tags (Etiquetas).
4. Elija Administrar etiquetas.
5. Realice una o más de las siguientes acciones:
   - Para agregar una etiqueta, seleccione Agregar nueva etiqueta y, a continuación, edite los valores de Clave y Valor.
   - Para actualizar una etiqueta, edite el valor de Value.
   - Para eliminar una etiqueta, selecciona Eliminar junto a la etiqueta.

6. Cuando hayas terminado de actualizar las etiquetas, selecciona Guardar.

Para actualizar las etiquetas de una actualización de software mediante la consola

1. Abra la consola WorkSpaces Thin Client.
2. Seleccione la actualización de software para abrir su página de detalles.
3. En la sección Etiquetas, selecciona Administrar etiquetas.
4. Realice una o más de las siguientes acciones:
   - Para agregar una etiqueta, seleccione Agregar nueva etiqueta y, a continuación, edite los valores de Clave y Valor.
   - Para actualizar una etiqueta, edita el valor de Value.
   - Para eliminar una etiqueta, selecciona Eliminar junto a la etiqueta.
5. Cuando hayas terminado de actualizar las etiquetas, selecciona Guardar.

Seguridad en Amazon WorkSpaces Thin Client

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

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

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la Nube de AWS. AWS también le proporciona servicios que puede utilizar de forma segura. Los auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los AWS programas de de . Para obtener más información sobre los programas de conformidad que se aplican a Amazon WorkSpaces Thin Client, consulte AWS Services in Scope by Compliance Program AWS .
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio 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.

Esta documentación le ayuda a entender cómo aplicar el modelo de responsabilidad compartida al utilizar WorkSpaces Thin Client. En los temas siguientes se muestra cómo configurar WorkSpaces Thin Client para cumplir sus objetivos de seguridad y conformidad. También puede aprender a utilizar otros AWS servicios que le ayudan a supervisar y proteger los recursos de WorkSpaces Thin Client.

Temas

Protección de datos en Amazon WorkSpaces Thin Client

El modelo de se aplica a protección de datos en Amazon WorkSpaces Thin Client. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global en la que se ejecutan todos los Nube de AWS. Usted es responsable de mantener el control sobre el contenido

alojado en esta infraestructura. Usted también es responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulte las Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulte la publicación de blog sobre el Modelo de responsabilidad compartida de AWS y GDPR en el Blog de seguridad de AWS .

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

- Utilice la autenticación multifactor (MFA) en cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos. AWS Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios con. AWS CloudTrail
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utilice servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados por FIPS 140-2 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un punto final FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulte Estándar de procesamiento de la información federal (FIPS) 140-2.

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como, por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabaja con WorkSpaces Thin Client u otro tipo de cliente Servicios de AWS mediante la consola, la API o los SDK. AWS CLI AWS Cualquier dato que ingrese en etiquetas o campos de formato libre utilizados para nombres se puede emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya información de credenciales en la URL a fin de validar la solicitud para ese servidor.

Amazon WorkSpaces Thin Client recopila y proporciona información sobre el uso de los dispositivos WorkSpaces Thin Client por parte de los usuarios y su interacción con los servicios de escritorio

virtual. Por ejemplo, la memoria disponible, los diagnósticos de red, la información de la red, la conectividad del dispositivo, las credenciales de SAML, la información de identificación del dispositivo y los informes de fallos. Esta información se utiliza para proporcionarle el servicio y se puede utilizar para mejorar la experiencia del usuario con el servicio. Además, únicamente para proporcionarle el servicio, la información puede transferirse fuera de la AWS región en la que los usuarios utilizan el servicio. Procesamos esta información de acuerdo con el Aviso AWS de privacidad.

Temas

Cifrado de datos

WorkSpaces Thin Client recopila datos de personalización del entorno y del dispositivo, como la configuración del usuario, los identificadores del dispositivo, la información del proveedor de identidad y los identificadores de escritorio de streaming. WorkSpaces Thin Client también recopila las marcas de tiempo de las sesiones. Los datos recopilados se almacenan en Amazon DynamoDB y Amazon S3. WorkSpaces Thin Client utiliza AWS Key Management Service (KMS) para el cifrado.

Siga estas directrices para proteger su contenido:

- Implemente el acceso con privilegios mínimos y cree funciones específicas para utilizarlas en las acciones de WorkSpaces Thin Client.
- Proteja los datos proporcionando una clave administrada end-to-end por el cliente, de modo que WorkSpaces Thin Client pueda cifrar los datos en reposo con las claves que usted suministre.
- Tenga cuidado al compartir códigos de activación de entorno y credenciales de usuario:
  - Los administradores deben iniciar sesión en la consola de WorkSpaces Thin Client y los usuarios deben proporcionar códigos de activación para configurar WorkSpaces Thin Client y utilizar las credenciales para iniciar sesión en el escritorio de streaming.
  - Cualquier persona con acceso físico puede configurar un WorkSpaces Thin Client, pero no podrá iniciar una sesión a menos que tenga un código de activación válido y credenciales de usuario para iniciar sesión.

- Los usuarios pueden finalizar sus sesiones de forma explícita si eligen bloquear la pantalla, reiniciar o apagar el dispositivo mediante la barra de herramientas del dispositivo. Esto descarta la sesión del dispositivo y borra las credenciales de sesión.

WorkSpaces Thin Client protege el contenido y los metadatos de forma predeterminada al cifrar todos los datos confidenciales con AWS KMS. Si se produce un error al aplicar la configuración existente, un usuario no puede acceder a nuevas sesiones y los dispositivos no pueden aplicar actualizaciones de software.

Cifrado de datos en reposo para Amazon WorkSpaces Thin Client

Amazon WorkSpaces Thin Client proporciona cifrado de forma predeterminada para proteger los datos confidenciales de los clientes en reposo mediante claves de cifrado AWS propias.

- AWS claves propias: Amazon WorkSpaces Thin Client utiliza estas claves de forma predeterminada para cifrar automáticamente los datos de identificación personal. No puede ver, administrar ni usar claves AWS propias ni auditar su uso. Sin embargo, no tiene que realizar ninguna acción ni cambiar ningún programa para proteger las claves que cifran sus datos. Para obtener más información, consulte Claves propiedad de AWS en la Guía para desarrolladores de AWS Key Management Service.

El cifrado de los datos en reposo de forma predeterminada ayuda a reducir la sobrecarga operativa y la complejidad que implica la protección de los datos confidenciales. Al mismo tiempo, le permite crear aplicaciones seguras que cumplen con los estrictos requisitos normativos y de conformidad con el cifrado.

Si bien no puede deshabilitar esta capa de cifrado ni seleccionar un tipo de cifrado alternativo, puede agregar una segunda capa de cifrado sobre las claves de cifrado existentes propiedad de AWS si elige una clave administrada por el cliente al crear su entorno del cliente ligero:

- Claves administradas por el cliente: Amazon WorkSpaces Thin Client admite el uso de una clave simétrica administrada por el cliente que usted crea, posee y administra para añadir una segunda capa de cifrado al cifrado que ya AWS posee. Como tiene el control total de esta capa de cifrado, puede realizar tareas como las siguientes:
  - Establecer y mantener políticas de claves
  - Establecer y mantener concesiones y políticas de IAM
  - Habilitar y deshabilitar políticas de claves

- Rotar el material criptográfico
- Agregar etiquetas.
- Crear alias de clave
- Programar la eliminación de claves

Para obtener más información, consulte Clave administrada por el cliente en la Guía para desarrolladores de AWS Key Management Service.

En la siguiente tabla se resume cómo Amazon WorkSpaces Thin Client cifra los datos de identificación personal.

Tipo de datos	Cifrado de claves propiedad de AWS	Cifrado de claves administradas por el cliente (opcional)
Nombre del entorno WorkSpaces Nombre del entorno de Thin Client	Habilitado	Habilitado
Nombre de dispositivo WorkSpaces Nombre del dispositivo Thin Client	Habilitado	Habilitado

> **Note**
>
> Amazon WorkSpaces Thin Client habilita automáticamente el cifrado en reposo mediante el uso de claves AWS propias para proteger los datos de identificación personal sin coste alguno.
> Sin embargo, se aplican cargos de AWS KMS por el uso de una clave administrada por el cliente. Para obtener más información sobre precios, consulte los precios de AWS Key Management Service.

Cómo utiliza Amazon WorkSpaces Thin Client las subvenciones en AWS KMS

Amazon WorkSpaces Thin Client requiere una concesión para poder utilizar la clave gestionada por el cliente.

Al crear un entorno de clientes WorkSpaces ligeros cifrado con una clave gestionada por el cliente, Amazon WorkSpaces Thin Client crea una subvención en su nombre mediante el envío de una CreateGrant solicitud a AWS KMS. Las concesiones en AWS KMS se utilizan para dar acceso a Amazon WorkSpaces Thin Client a una clave de KMS de una cuenta de cliente.

Cuando un nuevo dispositivo Thin Client se registra en un entorno cifrado de WorkSpaces Thin Client con una clave gestionada por el cliente y se cambia el nombre de ese dispositivo, Amazon WorkSpaces Thin Client crea una concesión en su nombre mediante el envío de una CreateGrant solicitud a AWS KMS. Las concesiones en AWS KMS se utilizan para dar acceso a Amazon WorkSpaces Thin Client a una clave de KMS de una cuenta de cliente.

Amazon WorkSpaces Thin Client requiere la autorización para utilizar la clave gestionada por el cliente en las siguientes operaciones internas:

- Envíe las solicitudes de descifrado a AWS KMS para descifrar los datos cifrados

Puede revocar el acceso a la concesión o eliminar el acceso del servicio a la clave gestionada por el cliente en cualquier momento. Si lo hace, Amazon WorkSpaces Thin Client no podrá acceder a ninguno de los datos cifrados por la clave gestionada por el cliente, lo que afectará a las operaciones que dependen de esos datos. Por ejemplo, si intenta obtener detalles del entorno a los que Amazon WorkSpaces Thin Client no puede acceder, la operación devolverá un `AccessDeniedException` error. Además, el dispositivo WorkSpaces Thin Client no podrá utilizar un entorno WorkSpaces Thin Client.

Crear una clave administrada por el cliente

Puede crear una clave simétrica administrada por el cliente mediante la consola de administración de AWS o las operaciones de la API de AWS KMS.

Para crear una clave simétrica administrada por el cliente

Siga los pasos de Creación de claves de KMS de cifrado simétricas en la Guía para desarrolladores de AWS Key Management Service.

Política de claves

Las políticas de clave controlan el acceso a la clave administrada por el cliente. Cada clave administrada por el cliente debe tener exactamente una política de clave, que contiene instrucciones que determinan quién puede usar la clave y cómo puede utilizarla. Cuando crea la clave administrada por el cliente, puede especificar una política de clave. Para obtener más información, consulte Administración del acceso a las claves administradas por el cliente en la Guía para desarrolladores de AWS Key Management Service.

Para utilizar la clave gestionada por el cliente con los recursos de Amazon WorkSpaces Thin Client, la política de claves debe permitir las siguientes operaciones de API:

- `kms:DescribeKey`— Proporciona los detalles clave gestionados por el cliente para que Amazon WorkSpaces Thin Client pueda validar la clave.
- `kms:GenerateDataKey`: permite utilizar la clave administrada por el cliente para cifrar los datos.
- `kms:Decrypt`: permite utilizar la clave administrada por el cliente para descifrar los datos.
- `kms:CreateGrant`: agrega una concesión a una clave administrada por el cliente. Concede acceso de control a una clave de KMS específica, que permite el acceso a las operaciones de concesión que requiere Amazon WorkSpaces Thin Client. Para más información sobre el uso de concesiones, consulte la Guía para desarrolladores de AWS Key Management Service.

  Esto permite a Amazon WorkSpaces Thin Client hacer lo siguiente:

  - Llame a `Decrypt` para descifrar los datos cifrados.

Los siguientes son ejemplos de declaraciones de políticas que puede añadir a Amazon WorkSpaces Thin Client:

```
{
    "Statement": [
        {
            "Sid": "Allow access to principals authorized to use Amazon WorkSpaces Thin
 Client",
            "Effect": "Allow",
            "Principal": {"AWS": "*"},
            "Action": [
                "kms:DescribeKey",
                "kms:GenerateDataKey",
                "kms:Decrypt",
                "kms:CreateGrant"
```

```
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "thinclient.region.amazonaws.com",
                    "kms:CallerAccount": "111122223333"
                }
            }
        },
        {
            "Sid": "Allow access for key administrators",
            "Effect": "Allow",
            "Principal": {"AWS": "arn:aws:iam::111122223333:root"},
            "Action": ["kms:*"],
            "Resource": "arn:aws:kms:region:111122223333:key/key_ID"
        },
        {
            "Sid": "Allow read-only access to key metadata to the account",
            "Effect": "Allow",
            "Principal": {"AWS": "arn:aws:iam::111122223333:root"},
            "Action": [
                "kms:Describe*",
                "kms:Get*",
                "kms:List*",
                "kms:RevokeGrant"
            ],
            "Resource": "*"
        }
    ]
}
```

Para obtener más información sobre la especificación de permisos en una política, consulte la Guía para desarrolladores de AWS Key Management Service.

Para más información sobre la solución de problemas de acceso a claves, consulte la Guía para desarrolladores de AWS Key Management Service.

Especificación de una clave gestionada por el cliente para WorkSpaces Thin Client

Puede especificar una clave administrada por el cliente como cifrado de segunda capa para los siguientes recursos:

- WorkSpaces Entorno de Thin Client

Al crear un entorno, puede especificar la clave de datos proporcionando una`kmsKeyArn`, que Amazon WorkSpaces Thin Client utiliza para cifrar los datos personales identificables.

- `kmsKeyArn`— Un identificador clave para una clave de AWS KMS administrada por el cliente. Proporcione un ARN de clave.

Cuando se añade un nuevo dispositivo de cliente WorkSpaces ligero al entorno de cliente WorkSpaces ligero cifrado con una clave gestionada por el cliente, el dispositivo de cliente WorkSpaces ligero hereda la configuración de clave gestionada por el cliente del entorno de cliente WorkSpaces ligero.

Un contexto de cifrado es un conjunto opcional de pares clave-valor que contiene información contextual adicional sobre los datos.

AWS El KMS usa el contexto de cifrado como datos autenticados adicionales para admitir el cifrado autenticado. Al incluir un contexto de cifrado en una solicitud de cifrado de datos, AWS KMS vincula el contexto de cifrado a los datos cifrados. Para descifrar los datos, incluya el mismo contexto de cifrado en la solicitud.

Contexto de cifrado de Amazon WorkSpaces Thin Client

Amazon WorkSpaces Thin Client utiliza el mismo contexto de cifrado en todas las operaciones criptográficas de AWS KMS, donde la clave es `aws:thinclient:arn` y el valor es el nombre de recurso de Amazon (ARN).

El siguiente es el contexto de cifrado del entorno:

```
"encryptionContext": {
    "aws:thinclient:arn": "arn:aws:thinclient:region:111122223333:environment/
environment_ID"
}
```

El siguiente es el contexto de cifrado del dispositivo:

```
"encryptionContext": {
    "aws:thinclient:arn": "arn:aws:thinclient:region:111122223333:device/device_ID"
}
```

Uso del contexto de cifrado para la supervisión

Si utiliza una clave simétrica gestionada por el cliente para cifrar los datos del entorno y el dispositivo de WorkSpaces Thin Client, también puede utilizar el contexto de cifrado en los registros y registros de auditoría para identificar cómo se utiliza la clave gestionada por el cliente. El contexto de cifrado también aparece en los registros generados por AWS CloudTrail o Amazon CloudWatch Logs.

Utilizar el contexto de cifrado para controlar el acceso a la clave administrada por el cliente

Puede utilizar el contexto de cifrado en políticas de claves y políticas de IAM como condiciones para controlar el acceso a su clave simétrica administrada por el cliente. Puede usar también una restricción de contexto de cifrado en una concesión.

Amazon WorkSpaces Thin Client utiliza una restricción de contexto de cifrado en las concesiones para controlar el acceso a la clave gestionada por el cliente en su cuenta o región. La restricción de concesión requiere que las operaciones que permite la concesión utilicen el contexto de cifrado especificado.

Los siguientes son ejemplos de declaraciones de política clave para conceder acceso a una clave administrada por el cliente para un contexto de cifrado específico. La condición de esta declaración de política requiere que la llamada `kms:Decrypt` tenga una restricción de contexto de cifrado que especifique el contexto de cifrado.

```
{
    "Sid": "Enable Decrypt to access Thin Client Environment",
    "Effect": "Allow",
    "Principal": {"AWS": "arn:aws:iam::111122223333:role/ExampleReadOnlyRole"},
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
        "StringEquals": {"kms:EncryptionContext:aws:thinclient:arn":
 "arn:aws:thinclient:region:111122223333:environment/environment_ID"}
    }
}
```

Supervisión de las claves de cifrado para Amazon WorkSpaces Thin Client

Si utiliza una clave gestionada por el cliente de AWS KMS con sus recursos de Amazon WorkSpaces Thin Client, puede utilizar AWS CloudTrail Amazon CloudWatch Logs para realizar un seguimiento de las solicitudes que Amazon WorkSpaces Thin Client envía a AWS KMS.

Los siguientes ejemplos son AWS CloudTrail eventos para`DescribeKey`,, `CreateGrant` `GenerateDataKeyDecrypt`, `Decrypt` (que se utilizan`Grant`) para supervisar las operaciones de KMS solicitadas por Amazon WorkSpaces Thin Client para acceder a los datos cifrados por la clave gestionada por el cliente:

En los siguientes ejemplos, puede ver el entorno `encryptionContext` de WorkSpaces Thin Client. Se registran CloudTrail eventos similares en el dispositivo WorkSpaces Thin Client.

DescribeKey

Amazon WorkSpaces Thin Client utiliza la `DescribeKey` operación para verificar la clave administrada por el cliente de AWS KMS.

El siguiente evento de ejemplo registra la operación `DescribeKey`:


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
                "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-11-21T13:43:33Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "thinclient.amazonaws.com"
    },
    "eventTime": "2023-11-21T13:44:22Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "DescribeKey",
    "awsRegion": "eu-west-1",
```

```
    "sourceIPAddress": "thinclient.amazonaws.com",
    "userAgent": "thinclient.amazonaws.com",
    "requestParameters": {"keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"},
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

CreateGrant

Amazon WorkSpaces Thin Client utiliza la `CreateGrant` operación para crear una concesión de KMS, que le permite descifrar los datos cuando el dispositivo accede a ellos.

El siguiente evento de ejemplo registra la operación `CreateGrant`:

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
                "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
                "accountId": "111122223333",
                "userName": "Admin"
```

```
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-11-21T13:43:33Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "thinclient.amazonaws.com"
    },
    "eventTime": "2023-11-21T13:44:23Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "CreateGrant",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "thinclient.amazonaws.com",
    "userAgent": "thinclient.amazonaws.com",
    "requestParameters": {
        "granteePrincipal": "thinclient.eu-west-1.amazonaws.com",
        "operations": ["Decrypt"],
        "retiringPrincipal": "thinclient.eu-west-1.amazonaws.com",
        "constraints": {
            "encryptionContextSubset": {"aws:thinclient:arn":
 "arn:aws:thinclient:eu-west-1:111122223333:environment/abcSAMPLE"}
        },
        "keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
    },
    "responseElements": {
        "grantId":
 "0ab0ac0d0b000f00ea00cc0a0e00fc00bce000c000f0000000c0bc0a0000aaafSAMPLE",
        "keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
    },
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
```

```
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

GenerateDataKey

Amazon WorkSpaces Thin Client utiliza la `GenerateDataKey` operación para cifrar los datos.

El siguiente evento de ejemplo registra la operación `GenerateDataKey`:

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
                "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2024-03-12T12:21:03Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "thinclient.amazonaws.com"
    },
    "eventTime": "2024-03-12T13:03:56Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKey",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "thinclient.amazonaws.com",
    "userAgent": "thinclient.amazonaws.com",
    "requestParameters": {
        "keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE",
```

```
        "encryptionContext": {
            "aws-crypto-public-key": "ABC123def4567890abc12345678/90dE/F123abcDEF
+4567890abc123D+ef1==",
            "aws:thinclient:arn": "arn:aws:thinclient:eu-
west-1:111122223333:environment/abcSAMPLE"
        },
        "numberOfBytes": 32
    },
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Decrypt

Amazon WorkSpaces Thin Client utiliza la `Decrypt` operación para descifrar los datos.

El siguiente evento de ejemplo registra la operación `Decrypt`:

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
```

```
                "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-11-21T13:43:33Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "thinclient.amazonaws.com"
    },
    "eventTime": "2023-11-21T13:44:25Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "thinclient.amazonaws.com",
    "userAgent": "thinclient.amazonaws.com",
    "requestParameters": {
        "keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE",
        "encryptionContext": {
            "aws-crypto-public-key": "ABC123def4567890abc12345678/90dE/F123abcDEF
+4567890abc123D+ef1==",
            "aws:thinclient:arn": "arn:aws:thinclient:eu-
west-1:111122223333:environment/abcSAMPLE"
         },
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT"
    },
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
```

```
    "eventCategory": "Management"
}
```

Decrypt (using Grant)

Cuando un dispositivo WorkSpaces Thin Client accede a la información del entorno o del dispositivo, se utiliza la `Decrypt` operación, que se permite mediante una clave KMS. `Grant`

El siguiente ejemplo de evento registra la `Decrypt` operación, autorizada mediante: `Grant`

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "thinclient.amazonaws.com"
    },
    "eventTime": "2023-11-21T13:44:23Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "thinclient.amazonaws.com",
    "userAgent": "thinclient.amazonaws.com",
    "requestParameters": {
        "encryptionContext": {
            "aws-crypto-public-key": "ABC123def4567890abc12345678/90dE/F123abcDEF
+4567890abc123D+ef1==",
            "aws:thinclient:arn": "arn:aws:thinclient:eu-
west-1:111122223333:environment/abcSAMPLE"
        },
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT",
        "keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
    },
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
```

```
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "sharedEventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventCategory": "Management"
}
```

Más información

Los siguientes recursos proporcionan más información sobre cifrado de datos en reposo:

- Para obtener más información sobre los conceptos básicos de AWS Key Management Service, consulte la Guía para desarrolladores de AWS Key Management Service.
- Para obtener más información sobre las prácticas recomendadas de seguridad para AWS Key Management Service, consulte la Guía para desarrolladores de AWS Key Management Service.

Cifrado en tránsito

WorkSpaces Thin Client cifra los datos en tránsito a través de HTTPS y TLS 1.2. Puede enviar una solicitud a WorkSpaces Thin Client mediante la consola o mediante llamadas directas a la API. Los datos de la solicitud que se transfieren se cifran enviándolos a través de una conexión HTTPS o TLS. Los datos de la solicitud se pueden transferir desde la AWS consola, la interfaz de línea de AWS comandos o el AWS SDK a WorkSpaces Thin Client. Esto también incluye cualquier actualización de software del dispositivo.

El cifrado en tránsito y las conexiones seguras (HTTPS, TLS) están configurados de forma predeterminada.

Administración de claves

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

Privacidad del tráfico de trabajo en Internet

Los administradores pueden ver los eventos de las sesiones de WorkSpaces Thin Client, incluidas las horas de inicio y la información pendiente de actualización de software. Estos registros se cifran

y se envían de forma segura a los clientes en la consola de WorkSpaces Thin Client. Los servicios de escritorio graban la información del usuario y otros detalles sobre las sesiones individuales de streaming de escritorio. Para obtener más información, consulte Supervise su registro de acceso WorkSpaces, Monitoring and Reporting para AppStream 2.0 o User access log para WorkSpaces Web.

Administración de identidades y accesos para Amazon WorkSpaces Thin Client

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

Temas

- Público
- Autenticación con identidades
- Administración de acceso mediante políticas
- Cómo funciona Amazon WorkSpaces Thin Client con IAM
- Ejemplos de políticas basadas en identidad para Amazon Thin Client WorkSpaces
- Solución de problemas de identidad y acceso a Amazon WorkSpaces Thin Client

Público

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

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

Administrador de servicios: si está a cargo de los recursos de WorkSpaces Thin Client en su empresa, probablemente tenga acceso total a WorkSpaces Thin Client. Su trabajo consiste en determinar a qué funciones y recursos de WorkSpaces Thin Client deben acceder los usuarios del servicio. Luego, 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 la IAM con WorkSpaces Thin Client, consulteCómo funciona Amazon WorkSpaces Thin Client con IAM.

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

Autenticación con identidades

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

Puede iniciar sesión AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Identity Center Los usuarios (Centro de identidades de IAM), la autenticación de inicio de sesión único de su empresa y sus credenciales de Google o Facebook son ejemplos de identidades federadas. Al iniciar sesión como una identidad federada, su administrador habrá configurado previamente la federación de identidades mediante roles de IAM. Cuando accedes AWS mediante la federación, estás asumiendo un rol de forma indirecta.

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

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

Independientemente del método de autenticación que use, es posible que deba proporcionar información de seguridad adicional. Por ejemplo, le AWS recomienda que utilice la autenticación multifactor (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte

Autenticación multifactor en la Guía del usuario de AWS Single Sign-On y Uso de la autenticación multifactor (MFA) en AWS en la Guía del usuario de IAM.

Cuenta de AWS usuario root

Al crear una Cuenta de AWS, comienza con una identidad de inicio de sesión que tiene acceso completo a todos Servicios de AWS los recursos de la cuenta. Esta identidad se denomina usuario Cuenta de AWS raíz y se accede a ella iniciando sesión con la dirección de correo electrónico y la contraseña que utilizaste para crear la cuenta. Recomendamos encarecidamente que no utilice el usuario raíz para sus tareas diarias. Proteja las credenciales del usuario raíz y utilícelas solo para las tareas que solo el usuario raíz pueda realizar. Para ver la lista completa de las tareas que requieren que inicie sesión como usuario raíz, consulte Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Identidad federada

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

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

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

Usuarios y grupos de IAM

Un usuario de IAM es una identidad propia Cuenta de AWS que tiene 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 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 más información, consulte Cuándo crear un usuario de IAM (en lugar de un rol) en la Guía del usuario de IAM.

Roles de IAM

Un rol de IAM es una identidad dentro de usted Cuenta de AWS que tiene permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una determinada persona. Puede asumir temporalmente una función de IAM en el AWS Management Console cambiando de función. Puede asumir un rol llamando a una operación de AWS API AWS CLI o utilizando una URL personalizada. Para más información sobre 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 sus permisos. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos define el rol. Para obtener información 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 IAM Identity Center, debe configurar un conjunto de permisos. El IAM Identity Center 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 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. Sin embargo, en algunos casos Servicios de AWS, puedes adjuntar una política directamente a un recurso (en lugar de usar un rol como proxy). 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 funciones en 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 al servicio.
  - Sesiones de acceso directo (FAS): cuando utilizas un usuario o un rol de IAM para realizar acciones en ellas AWS, se te considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. El FAS utiliza los permisos del principal que llama Servicio de AWS y los solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.
  - 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.
  - Función vinculada al servicio: una función vinculada a un servicio es un tipo de función de servicio que está vinculada a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.
- Aplicaciones que se ejecutan en Amazon EC2: puede usar un rol de IAM para administrar las credenciales temporales de las aplicaciones que se ejecutan en una instancia EC2 y realizan AWS CLI solicitudes a la API. AWS Es preferible hacerlo de este modo a almacenar claves de acceso en la instancia EC2. Para asignar una AWS función a una instancia EC2 y ponerla a disposición de todas sus aplicaciones, debe crear un perfil de instancia adjunto a la instancia. Un perfil de instancia contiene el rol y permite a los programas que se ejecutan en la instancia EC2 obtener credenciales temporales. Para 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

El acceso se controla AWS creando políticas y adjuntándolas a AWS identidades o recursos. Una política es un objeto AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando un director (usuario, usuario raíz o sesión de rol) realiza una solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. La mayoría de las políticas se almacenan AWS como 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 usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

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

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 esa política puede obtener información sobre el rol de la API AWS Management Console AWS CLI, la o la AWS API.

Políticas basadas en identidades

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar 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 en 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 identidades pueden clasificarse además como políticas insertadas o políticas administradas. Las políticas insertadas se integran directamente en un único usuario, grupo

o rol. Las políticas administradas son políticas independientes que puede adjuntar a varios usuarios, grupos y roles de su Cuenta de AWS empresa. Las políticas administradas incluyen políticas AWS administradas y políticas administradas por el cliente. Para más información sobre 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 asocian 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 asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No puedes usar políticas AWS gestionadas de IAM 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 políticas JSON.

Amazon S3 y Amazon VPC son ejemplos de servicios que admiten las ACL. AWS WAF 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 tipos de políticas adicionales y menos comunes. Estos tipos de políticas pueden establecer el máximo de permisos que los tipos de políticas más frecuentes le conceden.

- Límites de permisos: un límite de permisos es una 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 entidad. Los permisos resultantes son la intersección de las políticas basadas en la identidad de la entidad y los límites de permisos. Las políticas basadas en recursos que especifique 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 servicios (SCP): las SCP son políticas de JSON que especifican los permisos máximos para una organización o unidad organizativa (OU). AWS Organizations AWS Organizations es un servicio para agrupar y gestionar de forma centralizada varios de los Cuentas de AWS que son propiedad de su empresa. Si habilita todas las características en una organización, entonces podrá aplicar políticas de control de servicio (SCP) a una o a todas sus cuentas. El SCP limita los permisos de las entidades en las cuentas de los miembros, incluidas las de cada una. Usuario raíz de la cuenta de AWS Para obtener más información 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 identidades del rol y las políticas de la sesión. Los permisos también pueden proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para 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 saber cómo AWS determinar si se debe permitir una solicitud cuando se trata de varios tipos de políticas, consulte la lógica de evaluación de políticas en la Guía del usuario de IAM.

Cómo funciona Amazon WorkSpaces Thin Client con IAM

Antes de usar IAM para administrar el acceso a WorkSpaces Thin Client, averigüe qué funciones de IAM están disponibles para su uso con WorkSpaces Thin Client.

Funciones de IAM que puede utilizar con Amazon WorkSpaces Thin Client

Característica de IAM	WorkSpaces Soporte para Thin Client
Políticas basadas en identidades	Sí

Característica de IAM	WorkSpaces Soporte para Thin Client
Políticas basadas en recursos	No
Acciones de políticas	Sí
Recursos de políticas	Sí
Claves de condición de políticas	Sí
ACL	No
ABAC (etiquetas en políticas)	Sí
Credenciales temporales	Sí
Permisos de entidades principales	Sí
Roles de servicio	No
Roles vinculados al servicio	No

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

Políticas basadas en la identidad para Thin Client WorkSpaces

Compatibilidad con las políticas basadas en identidades	Sí

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar 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 en 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 identidades de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. No es posible especificar la entidad principal en una política basada en identidad porque se aplica al usuario o rol al que está adjunto. Para más información sobre 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 la identidad para Thin Client WorkSpaces

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

Políticas basadas en recursos dentro de Thin Client WorkSpaces

Compatibilidad con las políticas basadas en recursos	No

Las políticas basadas en recursos son documentos de política JSON que se asocian 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 asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Para habilitar el acceso entre cuentas, puede especificar toda una cuenta o entidades de IAM de otra cuenta como la entidad principal de una política en función de recursos. Añadir a una política en función de recursos una entidad principal entre cuentas es solo una parte del establecimiento de una relación de confianza. Cuando el principal y el recurso son diferentes Cuentas de AWS, el 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, adjunte la entidad a una política basada en identidad. Sin embargo, si la política en función de recursos concede el acceso a una entidad principal de la misma cuenta, no es necesaria una política basada en identidad adicional. Para 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 Thin Client

Admite acciones de políticas	Sí

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

El elemento `Action` de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política. Las acciones políticas suelen tener el mismo nombre que la operación de AWS API 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 acciones de WorkSpaces Thin Client, consulte Acciones definidas por Amazon WorkSpaces Thin Client en la Referencia de autorización de servicios.

Las acciones políticas en WorkSpaces Thin Client utilizan el siguiente prefijo antes de la acción:

```
workspaces-thin-client
```

Para especificar varias acciones en una sola sentencia, sepárelas con comas, como se muestra en el siguiente ejemplo:

```
"Action": [
      "workspaces-thin-client:action1",
      "workspaces-thin-client:action2"
         ]
```

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

Recursos de políticas para Thin Client WorkSpaces

Admite recursos de políticas	Sí

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

El elemento `Resource` 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 los tipos de recursos de WorkSpaces Thin Client y sus ARN, consulte Recursos definidos por Amazon WorkSpaces Thin Client en la Referencia de autorización de servicios. Para saber con qué acciones puede especificar el ARN de cada recurso, consulte Acciones definidas por Amazon WorkSpaces Thin Client.

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

Claves de condición de la política para Thin Client WorkSpaces

Admite claves de condición de políticas específicas del servicio	Sí

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

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

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

También puede utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puede conceder un permiso de usuario de IAM para acceder a un recurso solo si está etiquetado con su nombre de usuario de IAM. Para 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 AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del usuario de IAM.

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

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

ACL en Thin Client WorkSpaces

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 políticas JSON.

ABAC con Thin Client WorkSpaces

Admite ABAC (etiquetas en las políticas)	Sí

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos en función de atributos. En AWS, estos atributos se denominan etiquetas. Puede adjuntar

etiquetas a las entidades de IAM (usuarios o roles) y a muchos AWS recursos. 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 Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial.

Para obtener más información 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 Thin Client

Compatible con el uso de credenciales temporales	Sí

Algunas Servicios de AWS no funcionan cuando se inicia sesión con credenciales temporales. Para obtener información adicional, incluida la información sobre cuáles Servicios de AWS funcionan con credenciales temporales, consulta Cómo Servicios de AWS funcionan con IAM en la Guía del usuario de IAM.

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

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

Permisos principales entre servicios para WorkSpaces Thin Client

Admite Forward access sessions (FAS)	Sí

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

Funciones de servicio para WorkSpaces Thin Client

Compatible con funciones de servicio	No

Un rol de 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 un rol 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 la funcionalidad de WorkSpaces Thin Client. Edite las funciones de servicio solo cuando WorkSpaces Thin Client le dé instrucciones para hacerlo.

Funciones vinculadas al servicio para WorkSpaces Thin Client

Compatible con roles vinculados al servicio	No

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

Para más información sobre cómo crear o administrar roles vinculados a servicios, consulte Servicios de AWS que funcionan con IAM. Busque un servicio en la tabla que incluya `Yes` en la columna Rol vinculado a un servicio. Seleccione el vínculo Sí para ver la documentación acerca del rol vinculado a servicios para ese servicio.

Ejemplos de políticas basadas en identidad para Amazon Thin Client WorkSpaces

De forma predeterminada, los usuarios y los roles no tienen permiso para crear o modificar los recursos de WorkSpaces Thin Client. Tampoco pueden realizar tareas mediante la AWS Management Console, AWS Command Line Interface (AWS CLI) o la AWS API. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puede agregar las políticas de IAM a roles, y los usuarios pueden asumirlos.

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 Thin Client, incluido el formato de los ARN de cada uno de los tipos de recursos, consulte Acciones, recursos y claves de condición de Amazon WorkSpaces Thin Client en la Referencia de autorización de servicios.

Temas

- Prácticas recomendadas sobre las políticas
- Uso de la consola Thin Client WorkSpaces
- Conceda acceso de solo lectura a Thin Client WorkSpaces

- Cómo permitir a los usuarios consultar sus propios permisos
- Conceda acceso completo a Thin Client WorkSpaces

Prácticas recomendadas sobre las políticas

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

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están disponibles en su. Cuenta de AWS Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. 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 del 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 del usuario de IAM.
- Utilice 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 políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo AWS CloudFormation. Para obtener más información, consulte Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.
- Utilice 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. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte Política de validación de Analizador de acceso de IAM en la Guía de usuario de IAM.

- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para mayor seguridad. Para solicitar la MFA cuando se invocan las operaciones de la API, agregue las condiciones de la MFA a sus políticas. Para más información, consulte Configuración del acceso a una API protegido 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 del usuario de IAM.

Uso de la consola Thin Client WorkSpaces

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

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

Conceda acceso de solo lectura a Thin Client WorkSpaces

En este ejemplo se muestra cómo se puede crear una política que permita a los usuarios de IAM ver la configuración de un WorkSpaces Thin Client, pero no realizar cambios. Esta política incluye permisos para completar esta acción en la consola o el programa mediante la AWS CLI o la API de AWS.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "thinclient:GetEnvironment",
                "thinclient:ListEnvironments",
                "thinclient:GetDevice",
                "thinclient:ListDevices",
                "thinclient:ListDeviceSessions",
                "thinclient:GetSoftwareSet",
```

```
                "thinclient:ListSoftwareSets",
                "thinclient:ListTagsForResource"
            ],
            "Resource": "arn:aws:thinclient:*:*:*"
        },
        {
            "Effect": "Allow",
            "Action": ["workspaces:DescribeWorkspaceDirectories"],
            "Resource": "arn:aws:workspaces:*:*:directory/*"
        },
        {
            "Effect": "Allow",
            "Action": ["workspaces-web:GetPortal"],
            "Resource": ["arn:aws:workspaces-web:*:*:portal/*"]
        },
        {
            "Effect": "Allow",
            "Action": ["workspaces-web:GetUserSettings"],
            "Resource": ["arn:aws:workspaces-web:*:*:userSettings/*"]
        },
        {
            "Effect": "Allow",
            "Action": ["appstream:DescribeStacks"],
            "Resource": ["arn:aws:appstream:*:*:stack/*"]
        }
    ]
}
```

Cómo 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 asocian a la identidad de sus usuarios. Esta política incluye permisos para completar esta acción en la consola o mediante programación mediante la API AWS CLI o 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": "*"
        }
    ]
}
```

Conceda acceso completo a Thin Client WorkSpaces

En este ejemplo, se muestra cómo se puede crear una política que conceda acceso total a los usuarios de WorkSpaces Thin Client IAM. Esta política incluye permisos para completar todas las acciones de WorkSpaces Thin Client en la consola o el programa mediante la AWS CLI o la API de AWS.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": ["thinclient:*"],
            "Resource": "arn:aws:thinclient:*:*:*"
        },
        {
            "Effect": "Allow",
            "Action": ["workspaces:DescribeWorkspaceDirectories"],
```

```
            "Resource": "arn:aws:workspaces:*:*:directory/*"
        },
        {
            "Effect": "Allow",
            "Action": ["workspaces-web:GetPortal"],
            "Resource": ["arn:aws:workspaces-web:*:*:portal/*"]
        },
        {
            "Effect": "Allow",
            "Action": ["workspaces-web:GetUserSettings"],
            "Resource": ["arn:aws:workspaces-web:*:*:userSettings/*"]
        },
        {
            "Effect": "Allow",
            "Action": ["appstream:DescribeStacks"],
            "Resource": ["arn:aws:appstream:*:*:stack/*"]
        }
    ]
}
```

Solución de problemas de identidad y acceso a Amazon WorkSpaces Thin Client

Utilice la siguiente información como ayuda para diagnosticar y solucionar los problemas habituales que pueden surgir al trabajar con WorkSpaces Thin Client e IAM.

Temas

- No estoy autorizado a realizar ninguna acción en WorkSpaces Thin Client
- Quiero ver mis claves de acceso
- Soy administrador y quiero permitir que otras personas accedan a WorkSpaces Thin Client
- Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis recursos de WorkSpaces Thin Client

No estoy autorizado a realizar ninguna acción en WorkSpaces Thin Client

Si AWS Management Console le indica que no está autorizado a realizar una acción, debe ponerse en contacto con su administrador para obtener 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-thin-client-device`*, pero no tiene los permisos ficticios `workspaces-thin-client:`*`ListDevices`*.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 workspaces-thin-client:ListDevices on resource: my-thin-client-device
```

En este caso, Mateo pide a su administrador que actualice sus políticas para permitirle acceder al *`my-thin-client-device`* recurso mediante la `workspaces-thin-client:`*`ListDevices`* acción.

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 lo ayuden a buscar el ID de usuario canónico. De este modo, podrías dar a alguien acceso permanente a tu Cuenta de AWS.

Cuando crea 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 una nueva. Para consultar las instrucciones, consulte Administración de claves de acceso en la Guía del usuario de IAM.

Soy administrador y quiero permitir que otras personas accedan a WorkSpaces Thin Client

Para permitir que otras personas accedan a WorkSpaces Thin Client, debe crear una entidad de IAM (usuario o rol) para la persona o aplicación a la 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 Thin Client.

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

Para obtener más información, consulte Conceda acceso completo a Thin Client WorkSpaces .

Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis recursos de WorkSpaces Thin Client

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 más información, consulte lo siguiente:

- Para saber si WorkSpaces Thin Client admite estas funciones, consulteCómo funciona Amazon WorkSpaces Thin Client con IAM.
- Para obtener información sobre cómo proporcionar acceso a los recursos de su Cuentas de AWS propiedad, consulte Proporcionar acceso a un usuario de IAM en otro usuario de su propiedad Cuenta de AWS en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta Cómo proporcionar acceso a recursos que Cuentas de AWS son propiedad de terceros en la Guía del usuario de IAM.

- Para obtener información sobre cómo proporcionar acceso mediante la federación de identidades, consulte Proporcionar acceso a usuarios autenticados externamente (federación de identidades) en la Guía del 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.

Resiliencia en Amazon WorkSpaces Thin Client

La infraestructura AWS global se basa en distintas zonas Regiones de AWS de disponibilidad. Regiones de AWS proporcionan varias zonas de disponibilidad aisladas y separadas físicamente, que están conectadas mediante redes de baja latencia, alto rendimiento y alta redundancia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre zonas de disponibilidad 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 zonas de disponibilidad Regiones de AWS y las zonas de disponibilidad, consulte Infraestructura global.AWS

Además de la infraestructura AWS global, WorkSpaces Thin Client ofrece varias funciones para ayudarlo a satisfacer sus necesidades de respaldo y resiliencia de datos.

Análisis y administración de vulnerabilidades en Amazon WorkSpaces Thin Client

La configuración y los controles de TI son una responsabilidad compartida entre usted AWS y usted. Para obtener más información, consulte el modelo de responsabilidad AWS compartida.

Amazon WorkSpaces Thin Client se integra de forma cruzada con Amazon WorkSpaces, Amazon AppStream 2.0 y WorkSpaces Web. Consulte los siguientes enlaces para obtener más información sobre la administración de actualizaciones para cada uno de estos servicios:

- Gestión de actualizaciones en Amazon AppStream 2.0
- Gestión de actualizaciones en Amazon WorkSpaces
- Análisis de configuración y vulnerabilidad en Amazon WorkSpaces Web

Supervisión de Amazon WorkSpaces Thin Client

La supervisión es una parte importante del mantenimiento de la fiabilidad, la disponibilidad y el rendimiento de Amazon WorkSpaces Thin Client y del resto de sus AWS soluciones. AWS proporciona las siguientes herramientas de supervisión para vigilar WorkSpaces Thin Client, informar cuando algo va mal y tomar medidas automáticas cuando sea necesario:

- AWS CloudTrailcaptura las llamadas a la API y los eventos relacionados realizados por su AWS cuenta o en su nombre y entrega los archivos de registro al bucket de Amazon S3 que especifique. Puede identificar los usuarios y las cuentas que llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron las llamadas. Para obtener más información, consulte la Guía del usuario de AWS CloudTrail.

Registro de llamadas a la API de Amazon WorkSpaces Thin Client mediante AWS CloudTrail

Amazon WorkSpaces Thin Client está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio en WorkSpaces Thin Client. CloudTrail captura todas las llamadas a la API de WorkSpaces Thin Client como eventos. Las llamadas capturadas incluyen llamadas desde la consola de WorkSpaces Thin Client y llamadas en código a las operaciones de la API de WorkSpaces Thin Client. Si crea una ruta, puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos para WorkSpaces Thin Client. Si no configura una ruta, podrá ver los eventos más recientes de la CloudTrail consola en el historial de eventos. Con la información recopilada por CloudTrail, puede determinar la solicitud que se realizó a WorkSpaces Thin Client, la dirección IP desde la que se realizó la solicitud, quién la realizó, cuándo se realizó y detalles adicionales.

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

WorkSpaces Información sobre Thin Client en CloudTrail

CloudTrail está habilitada en su cuenta Cuenta de AWS al crear la cuenta. Cuando se produce una actividad en WorkSpaces Thin Client, esa actividad se registra en un CloudTrail evento junto con otros eventos de AWS servicio en el historial de eventos. Puede ver, buscar y descargar eventos recientes en su Cuenta de AWS. Para obtener más información, consulte Visualización de eventos con el historial de CloudTrail eventos.

Para obtener un registro continuo de los eventos que se produzcan en su entorno Cuenta de AWS, incluidos los eventos de WorkSpaces Thin Client, cree un registro. Un rastro permite CloudTrail entregar 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. La ruta registra los eventos de todas las regiones de la AWS partición y envía los archivos de registro al bucket de Amazon S3 que especifique. Además, puede configurar otros AWS servicios para analizar más a fondo los datos de eventos recopilados en los CloudTrail registros y actuar en función de ellos. Para más información, consulte los siguientes temas:

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

Todas las acciones de WorkSpaces Thin Client se registran CloudTrail y se documentan en la referencia de la API de Amazon WorkSpaces Thin Client. Por ejemplo, las llamadas a las `CreateEnvironment` `GetSoftwareSet` acciones y las llamadas generan entradas en los archivos de CloudTrail registro. `ListDevices`

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

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

Descripción de las entradas del archivo de registro de WorkSpaces Thin Client

Un rastro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que usted especifique. CloudTrail Los archivos de registro contienen una o

más entradas de registro. Un evento representa una solicitud única de cualquier fuente e incluye información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. CloudTrail Los archivos de registro no son un registro ordenado de las llamadas a la API pública, por lo que no aparecen en ningún orden específico.

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

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "<principal-id>",
        "arn": "<arn>",
        "accountId": "<account-id>",
        "accessKeyId": "<access-key-id>",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "<principal-id>",
                "arn": "arn:aws:iam::<arn>",
                "accountId": "<accpimt-id>",
                "userName": "<user-name>"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-11-18T23:07:01Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-11-18T23:11:57Z",
    "eventSource": "thinclient.amazonaws.com",
    "eventName": "GetDevice",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "<source-ip-address>",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0)
 Gecko/20100101 Firefox/115.0",
    "requestParameters": {
        "id": "<ip>"
    },
    "responseElements": null,
    "requestID": "<request-id>",
```

```
    "eventID": "<event-id>",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "<recipient-account-id>",
    "eventCategory": "Management"
}
```

Creación de recursos de Amazon WorkSpaces Thin Client con AWS CloudFormation

Amazon WorkSpaces Thin Client está integrado con AWS CloudFormation un servicio que le ayuda a modelar y configurar sus AWS recursos. De este modo, puede dedicar menos tiempo a crear y administrar sus recursos e infraestructura. Usted crea una plantilla que describe todos los AWS recursos que desea (como los entornos) y AWS CloudFormation aprovisiona y configura esos recursos por usted.

Cuando la utilice AWS CloudFormation, podrá reutilizar la plantilla para configurar los recursos de WorkSpaces Thin Client de forma coherente y repetida. Describa sus recursos una vez y, a continuación, aprovisione los mismos recursos repetidamente en varias Cuentas de AWS regiones.

WorkSpaces Thin Client y AWS CloudFormation plantillas

Para aprovisionar y configurar los recursos para WorkSpaces Thin Client y los servicios relacionados, debe conocer AWS CloudFormation las plantillas. Las plantillas son archivos de texto formateados en formato JSON o YAML. Estas plantillas describen los recursos que deseas aprovisionar en tus AWS CloudFormation pilas. Si no estás familiarizado con los formatos JSON o YAML, puedes usar AWS CloudFormation Designer para ayudarte a empezar con AWS CloudFormation las plantillas. Para obtener más información, consulte ¿Qué es Designer de AWS CloudFormation ? en la Guía del usuario de AWS CloudFormation .

WorkSpaces Thin Client admite la creación de entornos en AWS CloudFormation. Para obtener más información, incluidos ejemplos de plantillas JSON y YAML para entornos, consulte la referencia sobre los tipos de recursos de Amazon WorkSpaces Thin Client en la Guía del AWS CloudFormation usuario.

Obtenga más información sobre AWS CloudFormation

Para obtener más información AWS CloudFormation, consulte los siguientes recursos:

- AWS CloudFormation
- AWS CloudFormation Guía del usuario
- Referencia de la API de AWS CloudFormation
- AWS CloudFormation Guía del usuario de la interfaz de línea de comandos

Acceda a Amazon WorkSpaces Thin Client mediante un punto final de interfaz (AWS PrivateLink)

Puede utilizarla AWS PrivateLink para crear una conexión privada entre su VPC y Amazon WorkSpaces Thin Client. Puede acceder a WorkSpaces Thin Client como una VPC, sin usar una puerta de enlace a Internet, un dispositivo NAT, una conexión VPN o AWS Direct Connect una conexión. Las instancias de su VPC no requieren direcciones IP públicas para acceder a WorkSpaces Thin Client.

Esta conexión privada se establece mediante la creación de un punto final de interfaz alimentado por AWS PrivateLink. Creamos una interfaz de red de punto de conexión en cada subred habilitada para el punto de conexión de interfaz. Se trata de interfaces de red administradas por el solicitante que sirven como punto de entrada para el tráfico destinado WorkSpaces a Thin Client.

Para obtener más información, consulte Acceso a Servicios de AWS a través de AWS PrivateLink en la Guía de AWS PrivateLink .

Consideraciones sobre Thin Client WorkSpaces

Antes de configurar un punto final de interfaz para WorkSpaces Thin Client, consulte las consideraciones de la AWS PrivateLink guía.

WorkSpaces Thin Client permite realizar llamadas a todas sus acciones de API a través del punto final de la interfaz.

Cree un punto final de interfaz para WorkSpaces Thin Client

Puede crear un punto final de interfaz para WorkSpaces Thin Client mediante la consola Amazon VPC o el AWS Command Line Interface ()AWS CLI. Para obtener más información, consulte Creación de un punto de conexión de interfaz en la Guía de AWS PrivateLink .

Cree un punto final de interfaz para WorkSpaces Thin Client con el siguiente nombre de servicio:

```
com.amazonaws.region.thinclient.api
```

Si habilita el DNS privado para el punto final de la interfaz, puede realizar solicitudes de API a WorkSpaces Thin Client utilizando su nombre de DNS regional predeterminado. Por ejemplo, `api.thinclient.us-east-1.amazonaws.com`.

Creación de una política de punto de conexión para el punto de conexión de interfaz

Una política de punto de conexión es un recurso de IAM que puede adjuntar al punto de conexión de su interfaz. La política de puntos finales predeterminada le proporciona acceso total a WorkSpaces Thin Client a través del punto final de la interfaz. Para controlar el acceso otorgado a WorkSpaces Thin Client desde su VPC, adjunte una política de punto final personalizada al punto final de la interfaz.

Una política de punto de conexión especifica la siguiente información:

- Las entidades principales que pueden llevar a cabo acciones (Cuentas de AWS, usuarios de IAM y roles de IAM).
- Las acciones que se pueden realizar.
- El recurso en el que se pueden realizar las acciones.

Para obtener más información, consulte Control del acceso a los servicios con políticas de punto de conexión en la Guía del usuario de AWS PrivateLink .

Ejemplo: política de puntos finales de VPC para acciones de WorkSpaces Thin Client

El siguiente es un ejemplo de una política de un punto de conexión personalizado. Al adjuntar esta política al punto final de la interfaz, concede acceso a las acciones de WorkSpaces Thin Client enumeradas a todos los principales de todos los recursos.

```
{
   "Statement": [
      {
         "Principal": "*",
         "Effect": "Allow",
         "Action": [
            "thinclient:ListEnvironments",
            "thinclient:ListDevices",
            "thinclient:ListSoftwareSets"
         ],
         "Resource":"*"
      }
   ]
}
```

Historial de documentos de la Guía del administrador de WorkSpaces Thin Client

En la siguiente tabla se describe el historial de documentación de las versiones de la Guía del administrador de WorkSpaces Thin Client.

Cambio	Descripción	Fecha
• Configuración WorkSpaces para Amazon WorkSpaces Thin Client • Configuración de la AppStream versión 2.0 para Amazon WorkSpaces Thin Client	• Se actualizó la lista de sistemas operativos. • Se actualizó el procedimiento del proveedor de identidad.	12 de febrero de 2024
Versión inicial	Versión inicial	26 de noviembre de 2023

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.