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? 1
¿Es la primera vez que usa ? 1
Arquitectura 1
Configuración de la consola de administración de Amazon WorkSpaces Thin Client 4
Inscripción en AWS 4
Creación un usuario de IAM 4
Introducción a la consola de administrador de VDI para Amazon WorkSpaces Thin Client 6
Configuración de WorkSpaces Personal para WorkSpaces Thin Client 6
Antes de empezar 7
Paso 1: Compruebe que el sistema cumpla con las funciones WorkSpaces personales requeridas 7
Paso 2: Usa la configuración avanzada para iniciar tu WorkSpace 8
Continuidad empresarial 9
Configuración de WorkSpaces grupos para WorkSpaces Thin Client 10
Antes de empezar 10
Cree un WorkSpaces grupo 11
Configuración del acceso a WorkSpaces Thin Client 14
Configuración de la AppStream versión 2.0 para Amazon WorkSpaces Thin Client 14
Paso 1: Compruebe que el sistema cumpla con las funciones necesarias de la AppStream versión 2.0 14
Paso 2: Configura tus pilas AppStream 2.0 15
Configuración de Amazon WorkSpaces Secure Browser para Amazon WorkSpaces Thin Client 16
Paso 1: Comprueba que tu sistema cumple con las funciones requeridas por Amazon WorkSpaces Secure Browser 16
Paso 2: Configurar los portales de WorkSpaces Secure Browser 17
Inicio de la consola de administración de WorkSpaces Thin Client 18
Regiones cubiertas 18
Inicio de la consola de administración de WorkSpaces Thin Client 19
Uso de la consola de administración de WorkSpaces Thin Client 20
Entornos 21
Lista de entornos 21
Detalles del entorno 23
Creación de un entorno 26

Edición de un entorno ... 30
Eliminación de un entorno ... 31
Dispositivos ... 31
Lista de dispositivos ... 31
Detalles del dispositivo ... 34
Edición de un nombre de dispositivo ... 41
Restablecimiento y anulación del registro de un dispositivo ... 41
Archivado de un dispositivo ... 42
Eliminar un dispositivo ... 42
Exportación de los detalles del dispositivo ... 43
Actualizaciones de software ... 43
Actualización del software del entorno ... 43
Actualización del software del dispositivo ... 44
WorkSpaces Versiones del software Thin Client ... 45
Uso de etiquetas en los recursos de WorkSpaces Thin Client ... 59
Seguridad ... 63
Protección de los datos ... 63
Cifrado de datos ... 65
Cifrado en reposo ... 66
Cifrado en tránsito ... 80
Administración de claves ... 80
Privacidad del tráfico de trabajo en Internet ... 81
Identity and Access Management ... 81
Público ... 81
Autenticación con identidades ... 82
Administración de acceso mediante políticas ... 86
Cómo funciona Amazon WorkSpaces Thin Client con IAM ... 89
Ejemplos de políticas basadas en identidades ... 96
AWS políticas gestionadas ... 101
Solución de problemas ... 106
Resiliencia ... 109
Análisis y administración de vulnerabilidades ... 109
Monitorización ... 111
CloudTrail registra ... 111
CloudTrail eventos de datos ... 113
CloudTrail eventos de gestión ... 114

CloudTrail ejemplos de eventos 114
AWS CloudFormation recursos 119
WorkSpaces Thin Client y AWS CloudFormation plantillas 119
Obtenga más información sobre AWS CloudFormation 119
AWS PrivateLink 120
Consideraciones 120
Creación de un punto de conexión de interfaz 120
Creación de una política de punto de conexión 121
Historial de documentos 122
..... cxxv

¿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 ?
- Arquitectura

¿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

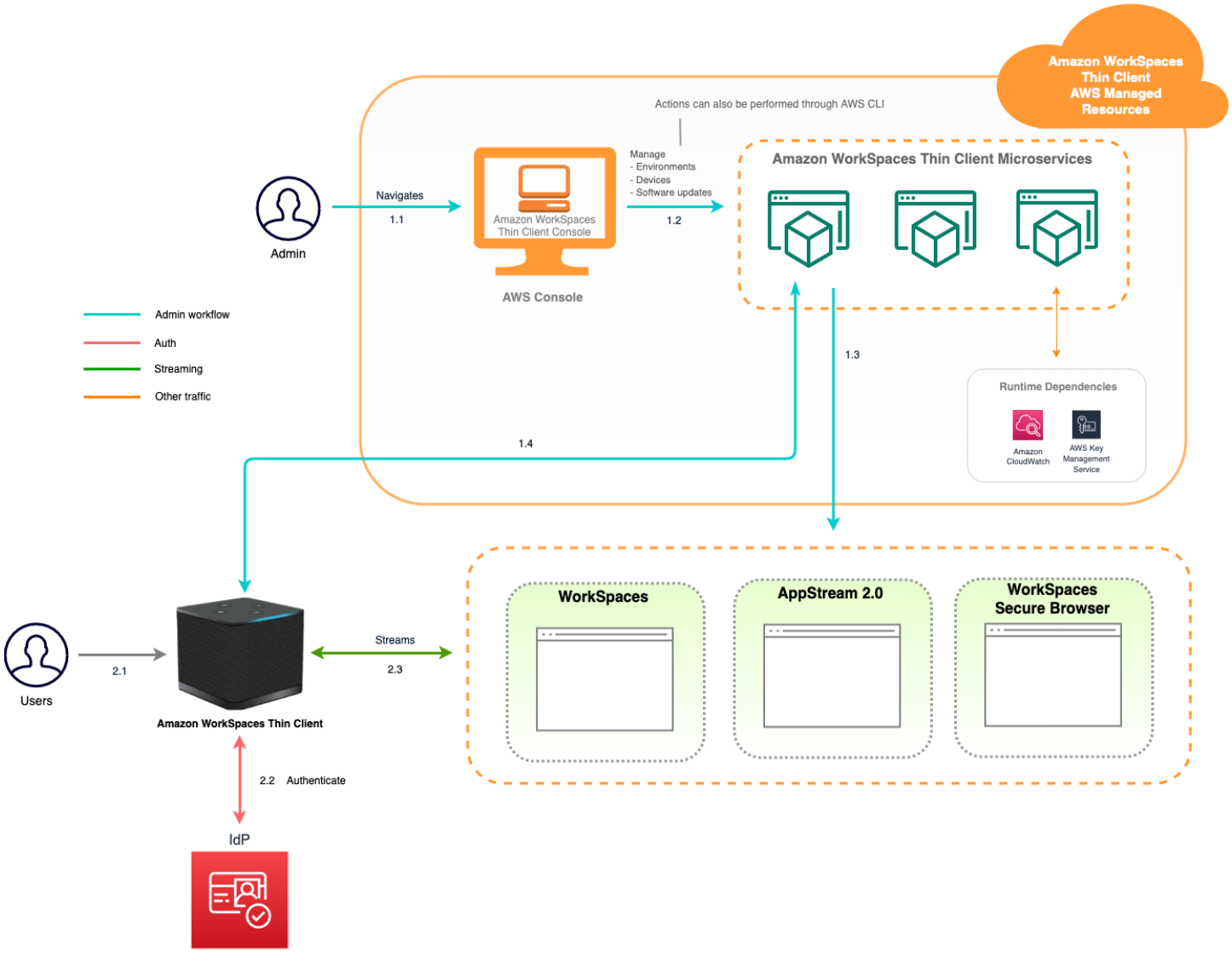
En función de la VDI utilizada, se accede a la información de su WorkSpaces Thin Client y se gestiona mediante directorios (para la versión 2.0) WorkSpaces, pilas (para la AppStream versión 2.0) y puntos de enlace del portal web (para WorkSpaces Secure Browser).

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-serviceSaaS) 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
- Creación un usuario de IAM

Inscripción en AWS

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

Para suscribirte a una Cuenta de AWS

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

   Parte del procedimiento de registro consiste en recibir una llamada telefónica o mensaje de texto 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, consulta 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.	Siguiendo las instrucciones de Crear un usuario de IAM para acceso de emergencia de la Guía del usuario de IAM.	Configure el acceso programático mediante Administrar 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 de WorkSpaces Personal para WorkSpaces Thin Client
- Configuración de WorkSpaces grupos para WorkSpaces Thin Client
- Configuración de la AppStream versión 2.0 para Amazon WorkSpaces Thin Client
- Configuración de Amazon WorkSpaces Secure Browser para Amazon WorkSpaces Thin Client

Configuración de WorkSpaces Personal para WorkSpaces Thin Client

Para utilizar WorkSpaces Thin Client con Amazon WorkSpaces Personal, es necesario configurar el servicio para acceder a los WorkSpaces directorios. Los directorios WorkSpaces personales de Amazon aparecen 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 Protocolos para Amazon WorkSpaces Personal.
- 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 de WorkSpaces Personal.
- Al iniciar un WorkSpace, habilite y configure el acceso web de WorkSpaces Thin Client. Para obtener más información, consulte Configurar WorkSpaces Thin Client

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

Para que la consola de administración de WorkSpaces Thin Client funcione correctamente con Amazon WorkSpaces Personal, 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

Característica	Requisito
	• Windows 10 (Traiga su propia licencia) • Windows 11 • Windows 10 (Traiga su propia licencia)
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 servidores de 2016, 2019 y 2022) con Office
Protocolos admitidos	Solo DCV

Paso 2: Usa la configuración avanzada para iniciar tu WorkSpace

Para usar la configuración avanzada para iniciar su WorkSpace

1. Abra la WorkSpaces consola enhttps://console.aws.amazon.com/workspaces/v2/home/.
2. Elija uno de los siguientes tipos de directorio y, a continuación, seleccione Siguiente:
   - AWS Microsoft AD gestionado
   - 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 elija Crear directorio.

Continuidad empresarial

WorkSpaces Thin Client brinda soporte para la continuidad del negocio como parte de un plan de continuidad del negocio (BCP). WorkSpaces La continuidad empresarial de Thin Client solo está disponible para su uso con WorkSpaces Personal. Para obtener más información sobre la continuidad empresarial, consulta Continuidad empresarial para WorkSpaces personal en la guía de WorkSpaces administración de Amazon.

Requisitos previos

Para que la continuidad empresarial funcione en WorkSpaces Thin Client, se deben cumplir los siguientes requisitos previos:

- Para el WorkSpaces redireccionamiento entre regiones: se han configurado el servicio DNS y las políticas de enrutamiento. Para configurarlas, consulte Configurar el servicio DNS y configurar las políticas de enrutamiento DNS.
- Para la resiliencia WorkSpaces multirregional: se WorkSpaces ha creado un modo de espera. Para crearlo, consulte Crear un dispositivo en espera WorkSpace.
- Un alias de conexión en la región mediante WorkSpaces Thin Client. Para verificar su región, consulte Regiones cubiertas.

Configuración de la continuidad empresarial para WorkSpaces Thin Client

Para habilitar WorkSpaces Personal DR en Amazon WorkSpaces Thin Client, necesitará configurar los alias de conexión para asignarlos al entorno mediante el SDK.

Ejemplo de explicación documental para configurar la recuperación ante desastres:

Example

Un ejemplo de comando que utiliza la AWS CLI para crear un nuevo entorno mediante un alias de WorkSpaces conexión para el escritorio de streaming:

```
aws workspaces-thin-client create-environment --region region --desktop-arn/
arn:aws:workspaces:region:account:connectionalias/wsca-id
```

*wsca-id*Sustitúyalo por tu alias de conexión WorkSpaces personal. El ID del alias de WorkSpaces conexión se encuentra en la consola WorkSpaces de administración o en el SDK.

Experiencia de usuario final

Una vez configurada la continuidad empresarial, los dispositivos deben estar registrados y activos en los últimos 15 días. Después, si los servicios de administración de WorkSpaces Thin Client dejan de estar disponibles, los usuarios pueden permanecer conectados a sus sesiones durante un máximo de 24 horas. En este estado, el dispositivo no recibirá actualizaciones de software, no intercambiará información de postura y no podrá activarse. La entrada del dispositivo correspondiente en la consola de WorkSpaces Thin Client no mostrará la información más reciente.

Si los servicios de administración de dispositivos WorkSpaces Thin Client no están disponibles más allá de 24 horas, aparecerá el siguiente mensaje de error:

«Se ha producido un error. Inténtelo de nuevo. Si el problema persiste, póngase en contacto con su administrador de TI. (Código de error: 3006)».

Configuración de WorkSpaces grupos para WorkSpaces Thin Client

Para que WorkSpaces Thin Client se utilice con Amazon WorkSpaces Pools, tendrá que configurar su proveedor de identidades (IdP) de SAML 2.0 para acceder WorkSpaces al directorio de pools. Los directorios de Amazon WorkSpaces Pools son un grupo no persistente WorkSpaces asignado a un grupo de usuarios.

> **Note**
>
> Las configuraciones se deben realizar antes de usar la consola por primera vez.

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 conceptos que se enumeran en Antes de empezar a utilizar Active Directory con WorkSpaces grupos de la Guía de WorkSpaces administración de Amazon antes de continuar con la configuración.

Cree un WorkSpaces grupo

Configure y cree un grupo desde el que se inicien y transmitan las aplicaciones de los usuarios.

> **Note**
>
> Debe crear un directorio antes de crear un WorkSpaces grupo. Para obtener más información, consulte Configurar SAML 2.0 y crear un directorio de WorkSpaces grupos.

Cómo configurar y crear un grupo

1. Abra la WorkSpaces consola en. https://console.aws.amazon.com/workspaces/v2/home/
2. En el panel de navegación WorkSpaces, elija Pools.
3. Elija Crear WorkSpaces grupos.
4. En Incorporación (opcional), puedes elegir Recomendarme opciones en función de mi caso de uso para obtener recomendaciones sobre el tipo de opciones WorkSpaces que quieres usar. Puedes saltarte este paso si sabes que quieres usar WorkSpaces Pools.
5. En Configurar WorkSpaces, introduzca los siguientes detalles:
   - En Nombre, introduzca un nombre identificador único para el grupo. No se admiten caracteres especiales.
   - En Descripción, escriba una descripción para el grupo (como máximo 256 caracteres).
   - En Bundle, elige entre las siguientes opciones el tipo de paquete que quieres usar para tu WorkSpaces.
     - Usa un WorkSpaces paquete base: elige uno de los paquetes del menú desplegable. Para obtener más información sobre el tipo de paquete que ha seleccionado, elija Detalles del paquete. Para comparar los paquetes que se ofrecen para los grupos, elija Comparar todos los paquetes.
     - Usa tu propio paquete personalizado: elige un paquete que hayas creado anteriormente. Para crear un paquete personalizado, consulte Crear una WorkSpaces imagen y un paquete personalizados para WorkSpaces Personal.

> **Note**
>
> BYOL no está disponible actualmente para WorkSpaces piscinas.

- En Duración máxima de la sesión en minutos, seleccione el tiempo máximo que puede permanecer activa una sesión de streaming. Si hay usuarios que siguen estando conectados a una instancia de streaming cinco minutos antes de que se alcance este límite, se les pedirá que guarden cualquier documento que tengan abierto antes de desconectarlos. Una vez transcurrido este tiempo, la instancia se termina y se sustituye por una nueva instancia. La duración máxima de la sesión que puede configurar en la consola de WorkSpaces Pools es de 5760 minutos (96 horas). La duración máxima de sesión que puede establecer mediante la API y la CLI de WorkSpaces Pools es de 432 000 segundos (120 horas).
- En Tiempo de espera de desconexión en minutos, elija la cantidad de tiempo que una sesión de streaming permanece activa después de que los usuarios se hayan desconectado. Si los usuarios intentan volver a conectarse a la sesión de streaming después de una desconexión o interrupción de la red dentro de este intervalo de tiempo, se conectarán a la sesión anterior. De lo contrario, se conectan a una sesión nueva con una nueva instancia de streaming.
- Si un usuario finaliza la sesión eligiendo Finalizar sesión o Cerrar sesión en la barra de herramientas de WorkSpaces Pools, no se aplica el tiempo de espera de desconexión. sino que se pide al usuario que guarde cualquier documento que tenga abierto y, a continuación, se le desconecta inmediatamente de la instancia de streaming. La instancia que estaba utilizando el usuario termina.
- En Tiempo de espera de desconexión de inactividad en minutos, elija la cantidad de tiempo que los usuarios pueden estar inactivos antes de desconectarlos de su sesión de streaming y de que comience el intervalo de tiempo Tiempo de espera de desconexión en minutos. Se notificará a los usuarios antes de que se desconecten por inactividad. Si intentan volver a conectarse a la sesión de streaming antes de que haya transcurrido el intervalo de tiempo especificado en Tiempo de espera de desconexión en minutos, se conectan a su sesión anterior. De lo contrario, se conectan a una sesión nueva con una nueva instancia de streaming. Si este valor se establece en 0, se deshabilita. Cuando este valor está deshabilitado, los usuarios no desconectan por inactividad.

> **Note**
>
> Los usuarios se consideran inactivos cuando dejan de introducir datos a través del teclado o del ratón durante su sesión de streaming. En el caso de los grupos

vinculados a un dominio, la cuenta regresiva para el tiempo de espera de desconexión por inactividad no comienza hasta que los usuarios inicien sesión con su contraseña de dominio de Active Directory o con una tarjeta inteligente. Las cargas y descargas de archivos, la entrada y salida de audio y los cambios de píxeles no se consideran actividad del usuario. Si los usuarios siguen estando inactivos después de que haya transcurrido el intervalo de tiempo de Tiempo de espera de desconexión de inactividad en minutos, se desconectan.

- En Políticas de capacidad programada (opcional), elija Añadir nueva capacidad de programación. Indique la fecha y hora de inicio y finalización del aprovisionamiento del número mínimo y máximo de instancias para el grupo en función del número mínimo previsto de usuarios simultáneos.
- En Políticas de escalado manual (opcional), especifique las políticas de escalado de los grupos que se usarán para aumentar y reducir la capacidad del grupo. Amplíe las políticas de escalado manual para añadir nuevas políticas de escalado.

> **Note**
>
> El tamaño del grupo está limitado en función de la capacidad mínima y máxima que haya especificado.

  - Seleccione Añadir nuevas políticas de escalado horizontal e introduzca los valores para añadir instancias específicas si la utilización de la capacidad especificada es inferior o superior al valor del umbral indicado.
  - Seleccione Añadir nuevas políticas de reducción horizontal e introduzca los valores para eliminar instancias específicas si la utilización de la capacidad especificada es inferior o superior al valor del umbral indicado.
- En Etiquetas, especifique el valor del par de claves que desee usar. Una clave puede ser una categoría general, como "proyecto", "propietario" o "entorno", con valores específicos asociados.

6. En la página Seleccionar directorio, elija el directorio que ha creado. Para crear un directorio, elija Crear directorio. Para obtener más información, consulte Administrar directorios para WorkSpaces grupos.
7. Elija Crear WorkSpace grupo.

Configuración del acceso a WorkSpaces Thin Client

Para configurar el acceso web para que WorkSpaces Pools utilice WorkSpaces Thin Client, necesitará utilizar la interfaz terrestre de AWS comandos.

1. Instalar o actualizar la AWS Command Line Interface
2. Configure sus AWS CLI ajustes.
3. Abre el AWS CLI.
4. Ejecute lo siguiente reemplazando `WORKSPACES_DIRECTORY_ID` y `REGION` con la información adecuada:

```
aws workspaces modify-workspace-access-properties --resource-
id WORKSPACES_DIRECTORY_ID  --workspace-access-properties
 '{"DeviceTypeWorkSpacesThinClient":"ALLOW"}' --region REGION
```

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 identidades	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)
Portapapeles	Deshabilitado Configurado a nivel de AppStream pila 2.0
File transfer	Deshabilitado Configurado a nivel de pila AppStream 2.0
Imprima en un dispositivo 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
Portapapeles	Deshabilitado
File transfer	Deshabilitado

Característica	Requisito
Imprima en un dispositivo local	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
- Inicio de la consola de administración de WorkSpaces Thin Client

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
EE. UU. Oeste (Oregon)	us-west-2	thinclient.us-west-2.amazonaws.com	https://us-west-2.console.aws.amazon.com/workspaces-thin-client/home
Asia Pacífico (Bombay)	ap-south-1	thinclient.ap-south-1.amazonaws.com	https://ap-south-1.console.aws.amazon.com/workspaces-thin-client/home

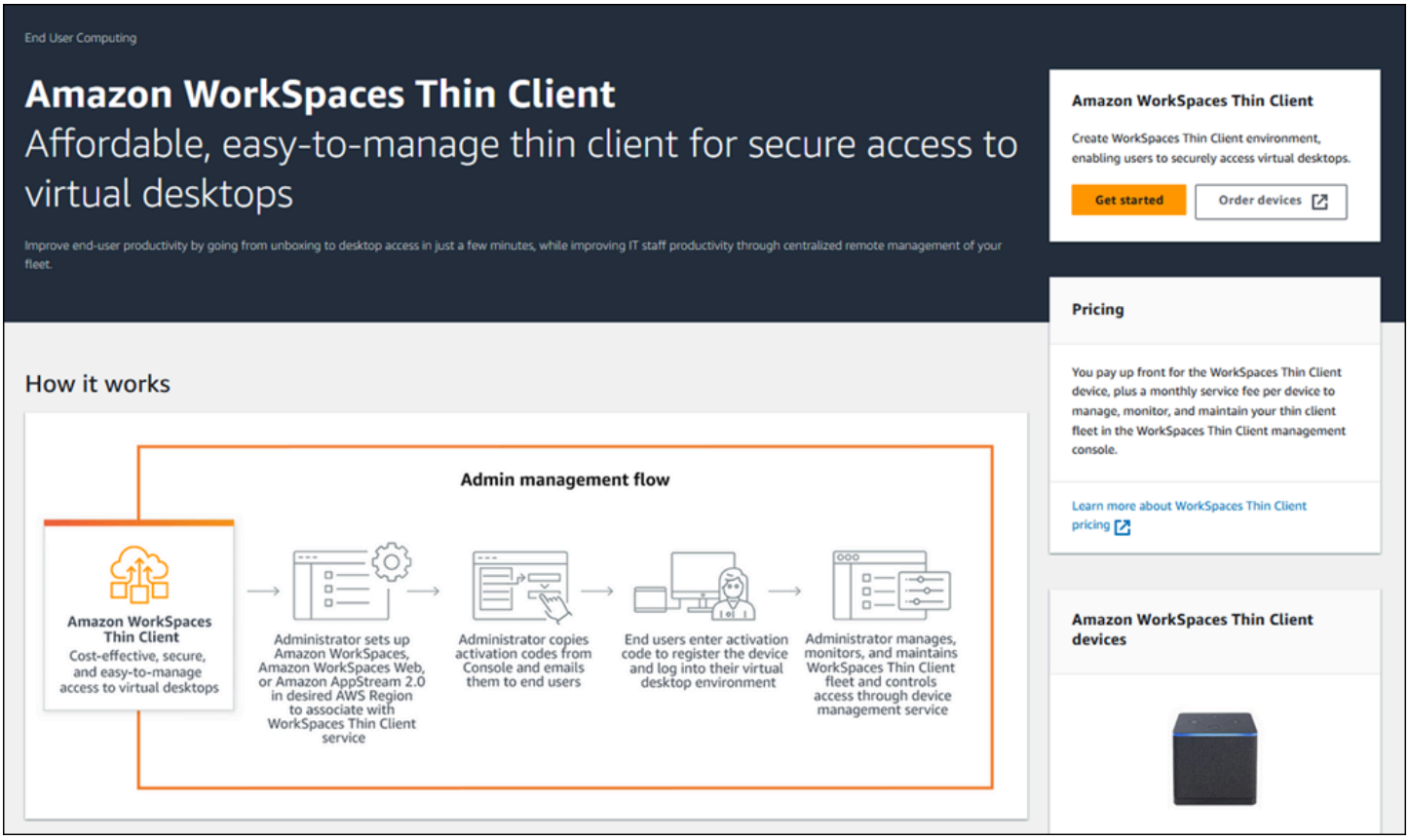
Nombre de la región	Región	Punto de conexión	Enlace a la consola
Europa (Irlanda)	eu-west-1	thinclient.eu-west-1.amazonaws.com	https://eu-west-1.console.aws.amazon.com/workspaces-thin-client/home
Canadá (Central)	ca-central-1	thinclient.ca-central-1.amazonaws.com	https://ca-central-1.console.aws.amazon.com/workspaces-thin-client/home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

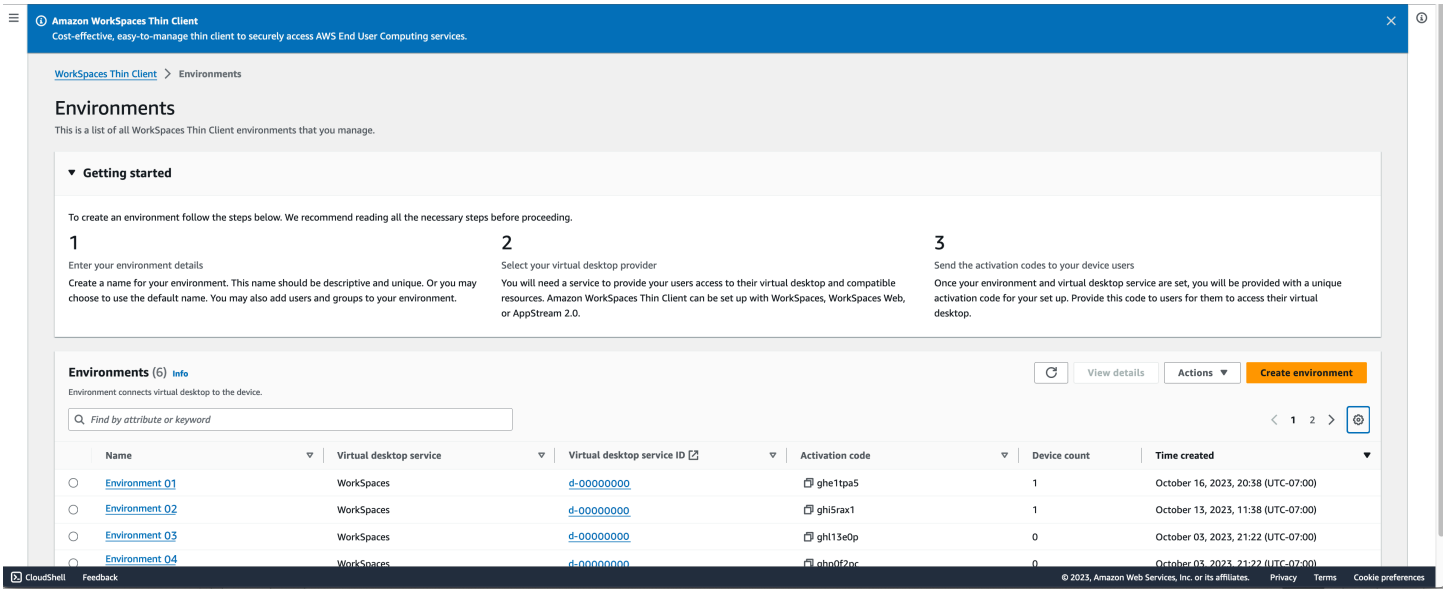
Entornos

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

Hay una serie de parámetros de su entorno que debe revisar, así como algunas acciones que puede realizar.



Detalles de la lista de entornos

Los parámetros de su entorno se muestran en una lista para que los revise. En la siguiente tabla se muestra cada elemento del resumen y su funcionamiento.

Elemento	Descripción
Nombre	El identificador único asociado a este entorno.

Elemento	Descripción
Servicio de escritorio virtual	El proveedor de escritorios virtuales 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	El código que utilizan los usuarios finales para acceder al entorno de escritorio virtual.
Recuento de dispositivos	La cantidad de dispositivos WorkSpaces Thin Client que acceden a este entorno.
Hora de creación	La fecha y la hora en que se creó el entorno.

Acciones de la lista de entornos

Hay una serie de acciones que puede realizar desde aquí. Seleccione cualquiera de estas opciones para realizar la acción correspondiente.

Elemento	Descripción
Búsqueda	Busca en todos los entornos que gestione.
Actualizar	Actualiza la lista de entornos.
View details (Ver detalles).	Muestra los detalles del entorno.
Acciones	Abre una lista desplegable en la que puede editar o eliminar un entorno.
Creación de un entorno	Inicia el proceso de creación de un entorno.

Temas

- Detalles del entorno
- Creación de un entorno

- Edición de un entorno
- Eliminación de un entorno

Detalles del entorno

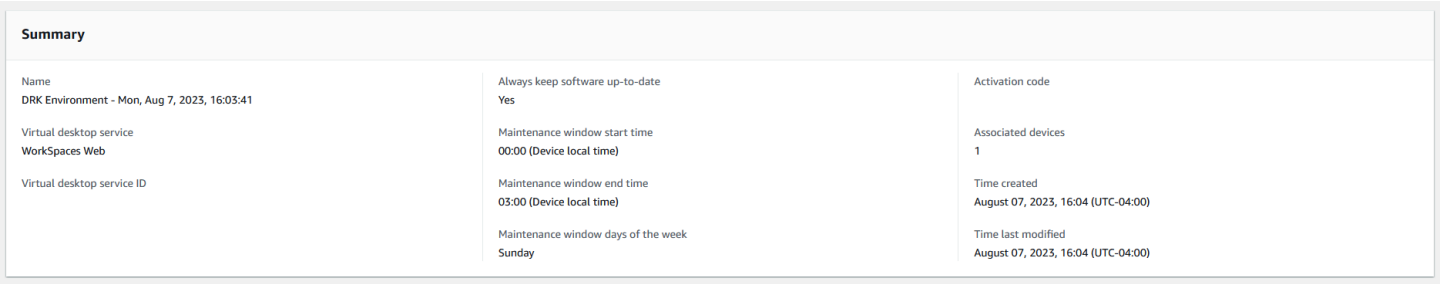
Al seleccionar un entorno, la consola WorkSpaces Thin Client muestra los detalles de ese entorno para que los revise. La consola también muestra los detalles sobre el proveedor de escritorios virtuales que utiliza este entorno.

Temas

- Resumen
- Detalles del entorno de escritorio virtual

Resumen

La sección de resumen proporciona una descripción general de alto nivel de las características clave del entorno WorkSpaces Thin Client. La siguiente tabla muestra cada elemento del resumen y su funcionamiento.



Elemento	Descripción
Nombre	El identificador único asociado a este entorno.
Servicio de escritorio virtual	El proveedor de escritorios virtuales que utiliza este entorno.
Nombre del servicio de escritorio virtual	El identificador único que el proveedor de servicios de escritorio virtual asigna a este entorno.

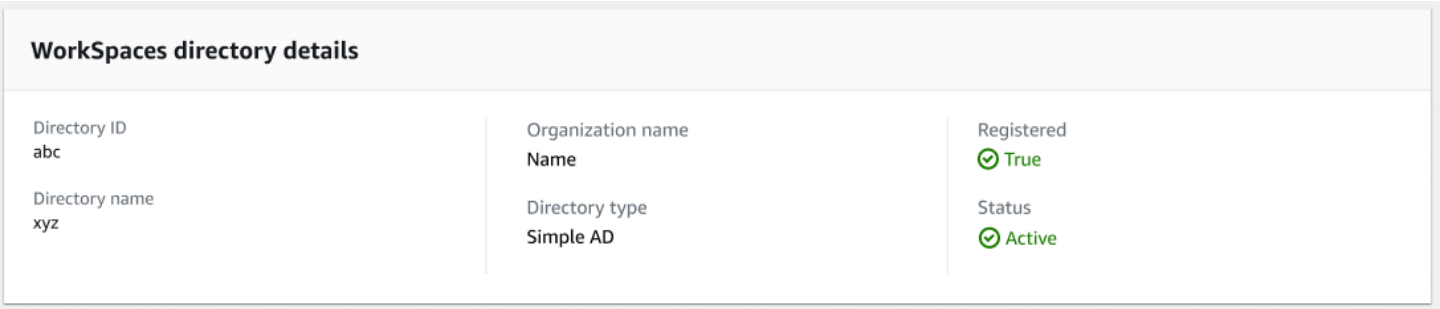
Elemento	Descripción
Código de activación	Los usuarios finales utilizan este código para acceder al entorno de escritorio virtual.
Conserve siempre el software up-to-date	Esta configuración permite las actualizaciones automáticas del software.
Hora de inicio de la ventana de mantenimiento	La hora de la semana en que comienzan las actualizaciones automáticas del software.
Hora de finalización del período de mantenimiento	La hora de la semana en la que finalizan las actualizaciones automáticas del software.
Periodo de mantenimiento: días de la semana	Los días en que se realizan las actualizaciones automáticas del software.
Dispositivos asociados	La cantidad de dispositivos WorkSpaces Thin Client que acceden a este entorno.
Hora de creación	La fecha y la hora en que se creó este entorno.

Detalles del entorno de escritorio virtual

WorkSpaces Los entornos Thin Client se ejecutan en una interfaz de escritorio virtual. Cada interfaz tiene un conjunto diferente de parámetros que controlan el entorno dedicado.

Detalles del WorkSpaces directorio de Amazon

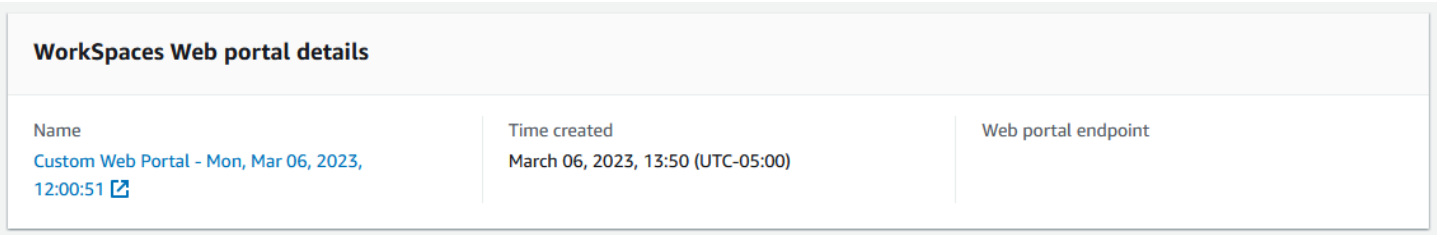
WorkSpaces Los entornos Thin Client que se ejecutan en Amazon WorkSpaces utilizan directorios para crear y ejecutar sus escritorios virtuales. La siguiente tabla muestra los detalles de cada elemento y su funcionamiento.



Elemento	Descripción
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.
Registered	Si este WorkSpaces directorio de Amazon está registrado.
Estado	Si este WorkSpaces directorio de Amazon está activo.

Detalles del portal Amazon WorkSpaces Secure Browser

WorkSpaces Los entornos Thin Client que se ejecutan en Amazon WorkSpaces Secure Browser utilizan portales web para crear y ejecutar sus escritorios virtuales. La siguiente tabla muestra los detalles de cada elemento y su funcionamiento.

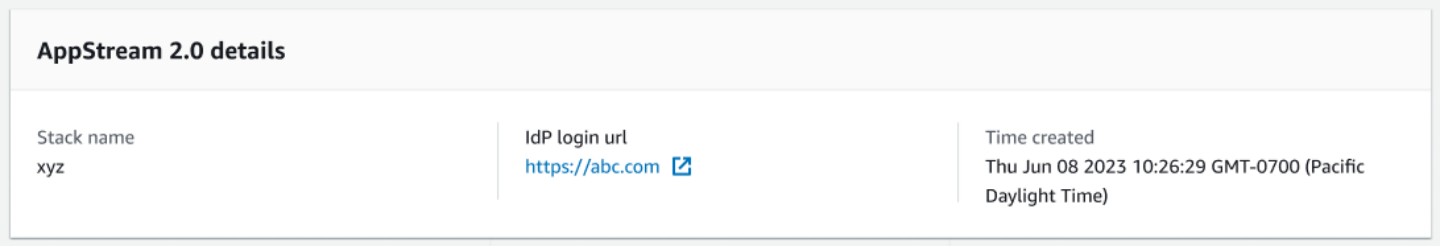


Elemento	Descripción
Nombre	El identificador único asociado a este portal de WorkSpaces Secure Browser.

Elemento	Descripción
Hora de creación	La fecha y la hora en que se creó este portal de WorkSpaces Secure Browser.
Punto de conexión del portal web	La dirección URL utilizada para acceder a su entorno de escritorio virtual.

AppStream Detalles de la versión 2.0

WorkSpaces Los entornos Thin Client se ejecutan en pilas de información AppStream 2.0 para crear y ejecutar sus escritorios virtuales. La siguiente tabla muestra los detalles de cada elemento y su funcionamiento.



Elemento	Descripción
Nombre de pila	El identificador único asociado a esta pila AppStream 2.0.
URL de inicio de sesión de IdP	La URL del proveedor de identidad que se utiliza para iniciar y cerrar sesión en tu stack AppStream 2.0.
Hora de creación	La fecha y la 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
- Paso 2: selección del proveedor de escritorio virtual
- Paso 3: envío del código de activación a los usuarios de su dispositivo

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 que proporcione a sus 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 enumeran 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.
- Cree un directorio seleccionando 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.

> **Important**
>
> 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.
   - Para crear una pila, selecciona 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.
- 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.

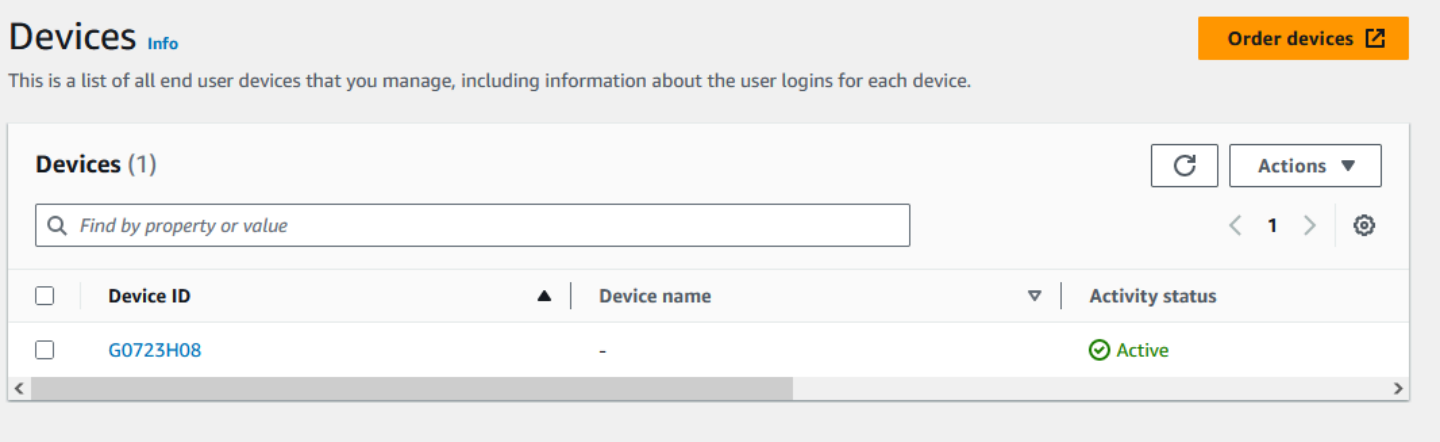
Dispositivos

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

Hay una serie de parámetros para cada dispositivo de la red que puede revisar, así como algunas acciones que puede realizar.



Detalles de la lista de dispositivos

Los parámetros de su dispositivo aparecen en una lista para que los revise. En la siguiente tabla se muestra cada elemento del resumen y su funcionamiento.

Elemento	Descripción
Device ID (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 la actividad	El estado actual de un dispositivo. Hay dos estados de estado: • Activo: se ha conectado a una red al menos una vez en los últimos siete días. • Inactivo: no se ha conectado a una red en los últimos siete días.
Estado de inscripción	Confirmación de que un dispositivo se ha configurado, está asociado a esta cuenta de AWS y forma parte de un entorno específico. Puede estar en uno de los siguientes estados: • Registrado: este es el estado predeterm inado.

Elemento	Descripción
	• 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. • Anulado del registro: el dispositivo se ha dado de baja correctamente. **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.
Conformidad con el software	El estado de conformidad del software del dispositivo. Hay dos estados de estado: • Conforme • No cumple con las normas

Acciones de la lista de dispositivos

Hay una serie de acciones que puede realizar desde aquí. Seleccione cualquiera de estas opciones para realizar la acción correspondiente.

Elemento	Descripción
Búsqueda	Busca en todos los dispositivos que gestionas.
Actualizar	Actualiza la lista de dispositivos.
View details (Ver detalles).	Muestra los detalles del dispositivo.
Acciones	Abre una lista desplegable en la que puede hacer lo siguiente: • Editar el nombre del dispositivo • Anular el registro • Archive (Archivado) • Delete • Exporte los detalles del dispositivo
Solicite dispositivos	Inicia el proceso de pedido de los dispositivos.

Temas

- Detalles del dispositivo
- Edición de un nombre de dispositivo
- Restablecimiento y anulación del registro de un dispositivo
- Archivado de un dispositivo
- Eliminar un dispositivo
- Exportación de los detalles del dispositivo

Detalles del dispositivo

Al seleccionar un dispositivo, la consola WorkSpaces Thin Client muestra los detalles de ese dispositivo para que los revise. La consola también muestra los detalles sobre el tipo de red del dispositivo y los periféricos conectados.

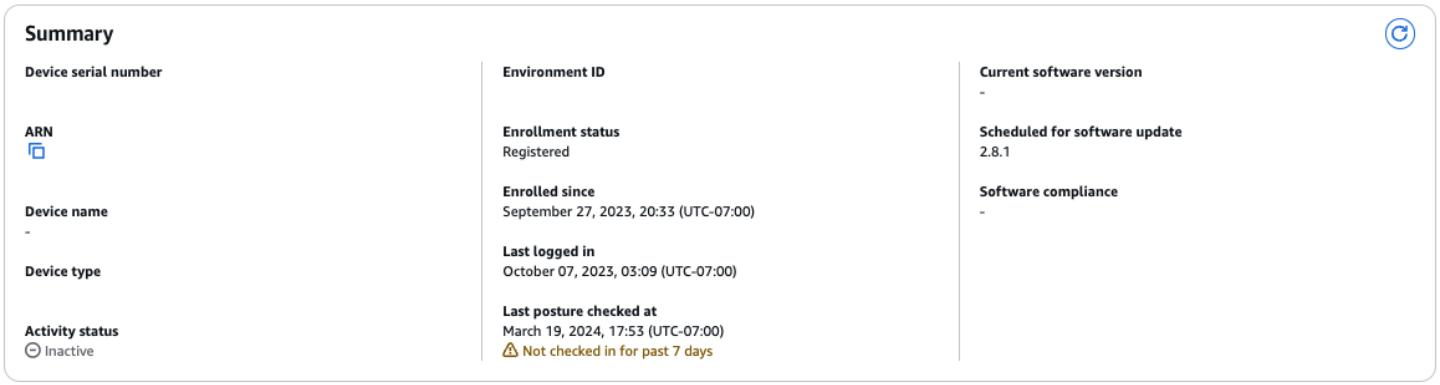
Temas

- Resumen

- Configuración del dispositivo
- Actividad del usuario

Resumen

La sección Resumen proporciona una descripción general de alto nivel de las funciones clave del dispositivo WorkSpaces Thin Client. La siguiente tabla muestra cada elemento del resumen y su funcionamiento.

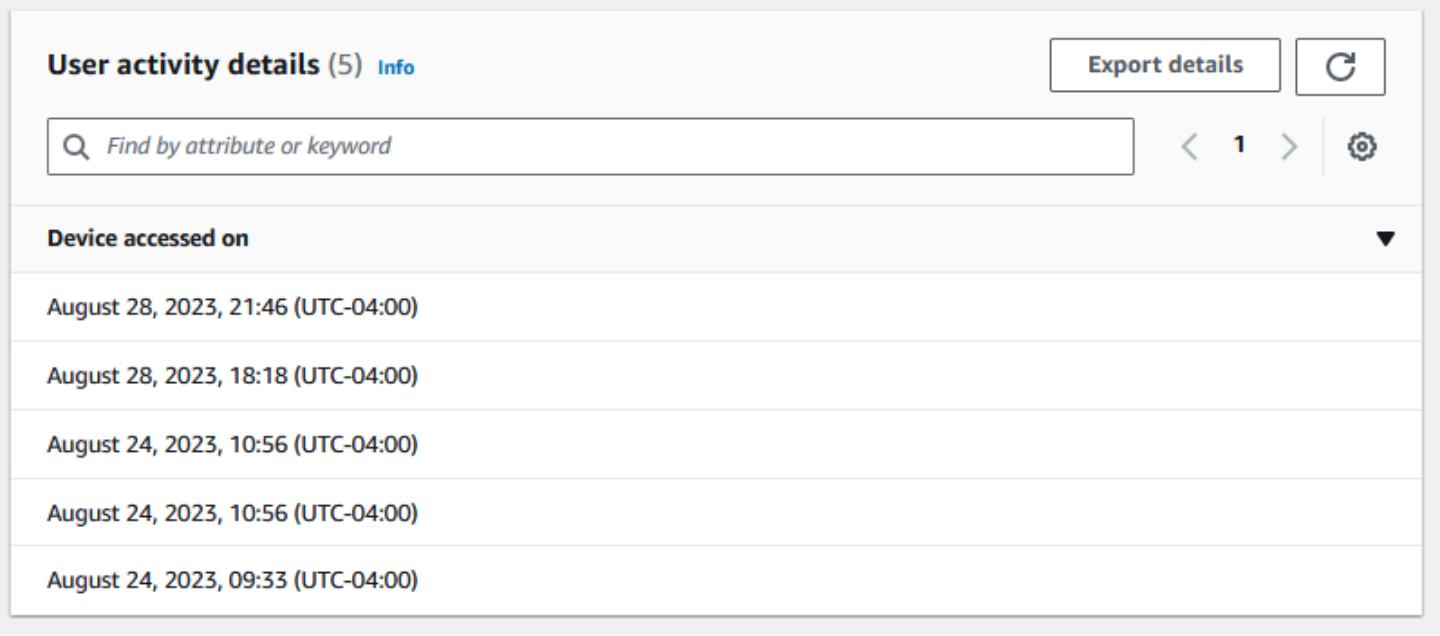


Elemento	Descripción
Número de serie del dispositivo	El número de identificación asignado a un dispositivo individual.
ARN	El identificador único del dispositivo en formato Amazon Resource Name (ARN).
Nombre del dispositivo	El nombre que le das a un dispositivo. Si no ha creado un nombre, puede asignarle un nombre o obtendrá 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 • Inactive

Elemento	Descripción
ID del 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 cuenta de AWS 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. • Anulado del registro: el dispositivo se ha dado de baja correctamente. **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 que se activó el dispositivo.
Se conectó por última vez	La fecha y la hora del inicio de sesión más reciente.
Última postura comprobada a las	La fecha y la hora de la última revisión del dispositivo.
Versión de software actual	La versión de software que utiliza este dispositivo actualmente.

Elemento	Descripción
Actualización de software programada	La versión de software programada del dispositivo.
Cumplimiento del software	Confirmación de que el conjunto de software es válido. Hay dos estados de estado: • Conforme • No cumple con los requisitos

Registro de usuario



Elemento	Descripción
Último acceso al dispositivo	La fecha y la hora en que se utilizó este dispositivo por última vez.

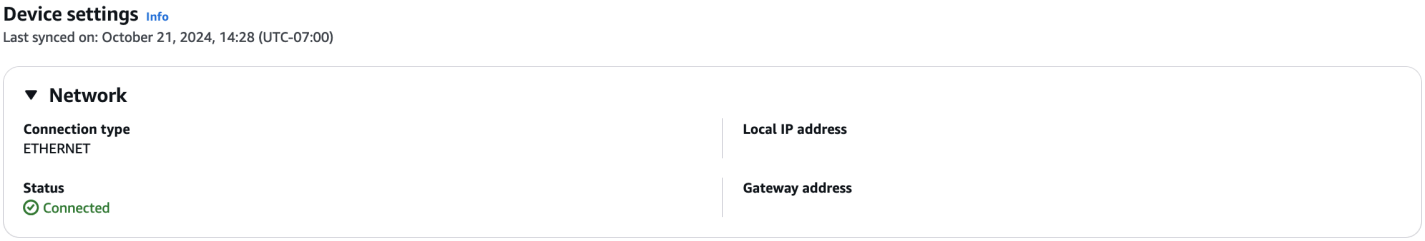
Configuración del dispositivo

Los parámetros de su dispositivo aparecen en una lista para que los revise. En la siguiente tabla se muestra cada elemento y su funcionamiento.

> **Note**
>
> La información de configuración del dispositivo se actualiza solo cuando el dispositivo está en línea. Si el dispositivo está desconectado, es posible que parte de la información esté desactualizada.

Dirección y red

WorkSpaces Los detalles del dispositivo Thin Client proporcionan una descripción general de las conexiones de red del dispositivo. En la siguiente tabla se muestra cada elemento y su funcionamiento.

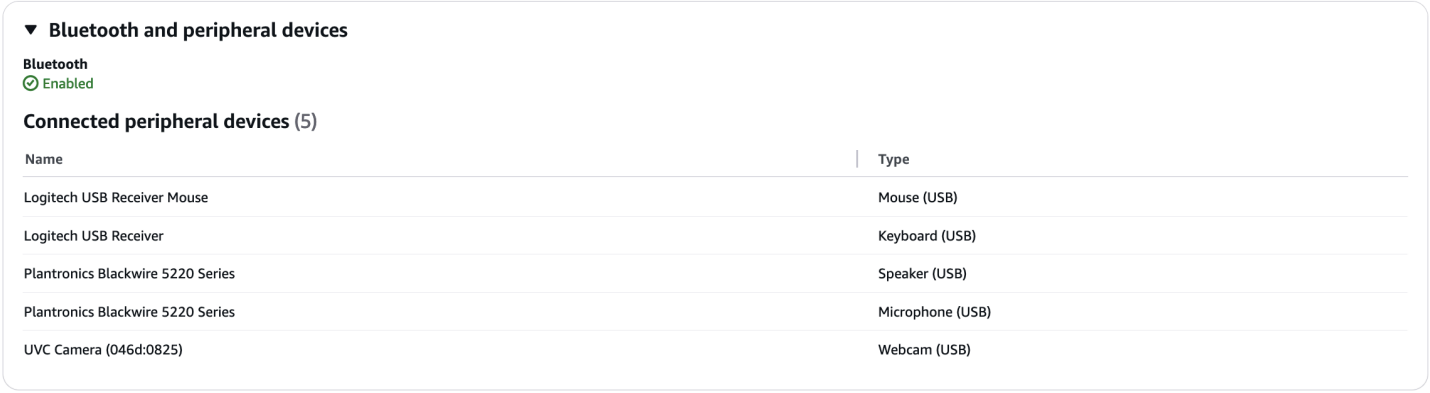


Elemento	Descripción
Se sincronizó por última vez el	La fecha y la hora de la configuración más reciente del dispositivo se sincronizan con la consola.
Tipo de conexión	El tipo de conexión de red que utiliza el dispositivo. El tipo de conexión puede ser Ethernet o Wifi.
Estado	El estado de la red. Si el dispositivo está conectado actualmente o se ha conectado en los últimos 20 minutos, el estado aparecerá como «conectado». Si la red ha estado desconectada durante más de 20 minutos, el estado cambiará para mostrar el tiempo transcurrido desde la última vez que el dispositi

Elemento	Descripción
	vo se conectó a Internet, por ejemplo, «se conectó por última vez hace 20 minutos».
Dirección IP local	La dirección IP local de la red conectada.
Dirección de puerta de enlace	La dirección de la puerta de enlace de la red conectada.

Bluetooth y dispositivos periféricos

WorkSpaces Los detalles del dispositivo Thin Client proporcionan una lista de todos los periféricos conectados a un dispositivo. La siguiente tabla muestra cada elemento y su funcionamiento.



Elemento	Descripción
Bluetooth	El estado de Bluetooth del dispositivo. Los dos estados de estado son: • Habilitado • Deshabilitado
Dispositivos periféricos conectados	La lista de nombres de los periféricos conectados, como el ratón Logitech, y el tipo de periféricos conectados, como el ratón (USB).

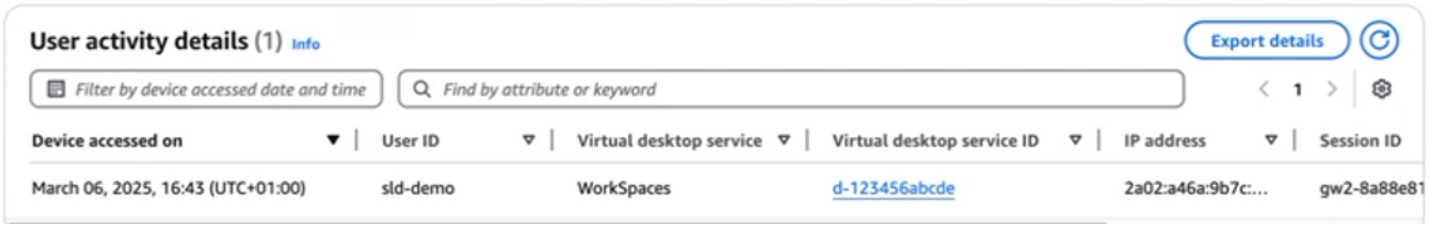
Alimentación y modo de suspensión

Cada dispositivo WorkSpaces Thin Client tiene un modo de ahorro de energía. La siguiente tabla muestra el estado de este modo.

Elemento	Descripción
Apague la pantalla después	El período de tiempo de inactividad tras el cual el dispositivo apaga la pantalla.

Actividad del usuario

Esta pestaña muestra el registro de la información de configuración y uso de un dispositivo específico. La siguiente tabla muestra cada elemento de este registro.



Elemento	Descripción
Se accedió al dispositivo el	La fecha y la hora en que se activó el dispositivo.
ID de usuario	El número de identificación del usuario que accede al dispositivo.
Servicio de escritorio virtual	El servicio de escritorio virtual que utiliza el dispositivo.
ID del servicio de escritorio virtual	El número de ID del servicio de escritorio virtual asociado al usuario.

Elemento	Descripción
Dirección IP	El número de identificación de la IP que accede al dispositivo.
Tipo de evento	Detalles sobre cómo se utiliza el dispositivo.

> **Note**
>
> Con la excepción de WorkSpaces Personal, muestra VDIs solo un evento iniciado por el inicio de sesión.

Puede utilizar la barra de búsqueda situada encima de la tabla para buscar información específica en la tabla. También puede filtrar los resultados de la tabla por fecha y hora.

Puede exportar la tabla a un archivo csv seleccionando el botón Exportar detalles.

Edición de un nombre de dispositivo

1. Seleccione el dispositivo que quiere editar. Puede 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.

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
2.16.1	7-3-2025	• Se corrigieron los problemas de seguridad críticos relacionados con el CVE-2025-6554 de Chromium.
2.16.0	27-6-2025	• Se agregaron notificaciones para la latencia de la red. • Se ha añadido la capacidad de recuperación cuando el segundo monitor se apaga durante una sesión.

Conjunto de software	Fecha de publicación	Cambios
		• Se solucionó el problema por el que los monitores mostraban una pantalla blanca o no se extendían automáticamente después de que el dispositivo volviera del modo de suspensión.
2.15.0	19-6-2025	• Se agregó soporte para teclados en español de América Latina e inglés internacional. • Los usuarios finales ven notificaciones cuando el dispositivo no detecta la actividad del teclado o el ratón durante un período prolongado.
2.14.1	6-09-2025	• Se corrigieron los problemas de seguridad críticos de Chromium relacionados con el CVE-2025-5419.

Conjunto de software	Fecha de publicación	Cambios
2.13.0	31-3-2025	• Los usuarios finales verán la encuesta de satisfacción con el producto como una notificación. • Añade una función prelimina r que admite el flujo de FIDO2 autenticación. Consulte los detalles FIDO2 previos a la sesión. • El dispositivo no entrará en modo de suspensión si audio/video está jugando durante la sesión. • Los usuarios finales ven notificaciones cuando el monitor está conectado y desconectado. • El dispositivo recopila información de diagnóstico del sistema operativo para mejorar el servicio. • Soluciona un problema por el que se mostraba una fecha incorrecta en la configuración de la fecha de instalación del software.
2.14.0	29-4-2025	• Mejoras de usabilidad y correcciones de errores.

Conjunto de software	Fecha de publicación	Cambios
2.13.0	31-3-2025	• Los usuarios finales verán la encuesta de satisfacción con el producto como una notificación. • Añade una función prelimina r que admite el flujo de FIDO2 autenticación. Consulte los detalles FIDO2 previos a la sesión. • El dispositivo no entrará en modo de suspensión si audio/video está jugando durante la sesión. • Los usuarios finales ven notificaciones cuando el monitor está conectado y desconectado. • El dispositivo recopila información de diagnóstico del sistema operativo para mejorar el servicio. • Soluciona un problema por el que se mostraba una fecha incorrecta en la configuración de la fecha de instalación del software.
2.12.0	30-1-2025	• Soluciona un problema por el que el usuario final cerraba la sesión al pulsar el botón de retroceso del ratón.

Conjunto de software	Fecha de publicación	Cambios
2.11.2	1-24-2025	• Soluciona un problema que provocaba que el audio crepitara durante las llamadas al moverse el ratón por los monitores.
2.11.1	27-12-2024	• Soluciona el problema de extensión automática de dos monitores. • Mejoras menores en la VoiceView etiqueta.
2.11.0	19-12-2024	• WorkSpaces Thin Client ahora admite VoiceView una lupa.
2.10.0	22-11-2024	• Los usuarios finales pueden utilizar un método abreviado de teclado para contraer la barra de herramientas del dispositivo.

Conjunto de software	Fecha de publicación	Cambios
2.9.0	28-10-2024	• Los administradores ahora pueden ver la configuración de los dispositivos de sus usuarios finales en la AWS consola, en la página de detalles del dispositivo de un dispositivo específico. • WorkSpaces Thin Client ahora es compatible con un monitor con una resolució n de 2K para una sola pantalla. • Los usuarios finales pueden ver las notificac iones relacionadas con los diagnósticos de red en sus dispositivos WorkSpaces Thin Client. • El usuario final ahora puede elegir colocar la barra de herramientas del dispositivo a la izquierda o a la derecha según sus preferencias. • Se ha corregido un problema que provocaba que el dispositivo no instalara las actualizaciones de software durante el tiempo de reposo o inactivid ad.

Conjunto de software	Fecha de publicación	Cambios
2.8.1	26-09-2024	• Se ha corregido un error grave que provocaba que el segundo monitor no se pudiera encender después de que el dispositivo se despertara del modo de suspensión.
2.8.0	09-06-2024	• Thin Client es compatible con monitores con resolución 4K. • Los usuarios pueden conectarse a la sesión de VDI incluso si los servicios de administración de dispositivos WorkSpaces Thin Client no están disponibles temporalmente. • Se solucionó el problema por el que la sección de detalles de la actividad del usuario de AWS la consola mostraba entradas duplicadas. • Los usuarios finales pueden usar PrintScreen la opción mientras transmiten WorkSpaces en WorkSpaces Thin Client.

Conjunto de software	Fecha de publicación	Cambios
2.7.1	27-08-2024	• Correcciones inmediatas para los problemas de seguridad críticos relacionados con los CVE-2024-7971 y CVE-2024-7965 de Chromium.
2.7.0	29-07-2024	• Mejoras en el rendimiento del segundo monitor. • Se ha corregido un problema por el que el idioma de la barra de herramientas no se veía afectado al cambiar el idioma del dispositivo. • El dispositivo ahora recopila información de diagnóstico para mejorar el servicio.

Conjunto de software	Fecha de publicación	Cambios
2.6.0	07-09-2024	• Los usuarios pueden aplazar las actualizaciones de software entrantes para poder terminar su trabajo sin interrupciones. • La configuración del dispositivo permite a los usuarios olvidar WiFi las redes guardadas. • Mejoras en el rendimiento de audio/video las llamadas de la sesión. • Algunos ajustes de usuario para las sesiones de VDI persisten tras el reinicio del dispositivo.
2.5.0	13-06-2024	• Se ha corregido un error que provocaba que el dispositivo mostrara 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 audio/video las llamadas de la sesión.

Conjunto de software	Fecha de publicación	Cambios
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 el problema de seguridad crítico 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. • 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.

Conjunto de software	Fecha de publicación	Cambios
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.
- Puede configurar las etiquetas de un dispositivo en un entorno para que se apliquen automáticamente al registrar un dispositivo.

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 administrar 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 gestionar 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 gestionar las etiquetas de un dispositivo nuevo 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 de creación de dispositivos, realice una o varias 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.

Cuando se crea un dispositivo, se registra en el entorno y se aplican las etiquetas de creación del dispositivo. Esto solo ocurre durante el registro de un nuevo dispositivo. Además, la etiqueta `aws:thinclient:environment-id` del sistema se aplica con el identificador de entorno utilizado como valor.

Para administrar 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. También eres responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y la normativa aplicables.

Esta documentación le ayuda a entender cómo aplicar el modelo de responsabilidad compartida al utilizar WorkSpaces Thin Client. Los siguientes temas muestran 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
- Administración de identidades y accesos para Amazon WorkSpaces Thin Client
- Resiliencia en Amazon WorkSpaces Thin Client
- Análisis y administración de vulnerabilidades en Amazon WorkSpaces Thin Client

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. Eres responsable de mantener el control sobre el contenido

alojado en esta infraestructura. También eres 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, consulta las Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulta 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:

- Utiliza 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 Para obtener información sobre el uso de CloudTrail senderos para capturar AWS actividades, consulte Cómo trabajar con CloudTrail senderos en la Guía del AWS CloudTrail usuario.
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utiliza 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 140-3 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, consulta Estándar de procesamiento de la información federal (FIPS) 140-3.

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabaja con WorkSpaces Thin Client u otro tipo de cliente Servicios de AWS mediante la consola, la API o. AWS CLI AWS SDKs Cualquier dato que ingrese en etiquetas o campos de texto 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
- Cifrado de datos en reposo para Amazon WorkSpaces Thin Client
- Cifrado en tránsito
- Administración de claves
- Privacidad del tráfico de trabajo en Internet

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 del dispositivo WorkSpaces Nombre del dispositivo Thin Client	Habilitado	Habilitado
Configuración del dispositivo WorkSpaces Configuración del dispositivo Thin Client	Habilitado	Habilitado
Etiquetas de creación de dispositivos	Habilitado	Habilitado

Tipo de datos:	Cifrado de claves propiedad de AWS	Cifrado de claves administradas por el cliente (opcional)
WorkSpaces Etiquetas de creación de dispositivos en Thin Client Environment		

> **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 AWS KMS

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

Amazon WorkSpaces Thin Client requiere que la política de claves utilice la clave gestionada por el cliente para las siguientes operaciones internas:

- Envíe `GenerateDataKey`solicitudes a AWS KMS para cifrar los datos.
- Envíe `Decrypt`solicitudes a AWS KMS para descifrar los datos cifrados.

Puede 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 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.

Creación de 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.

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"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "thinclient.region.amazonaws.com",
                    "kms:CallerAccount": "111122223333"
                }
            }
        },
        {
            "Sid": "Allow Amazon WorkSpaces Thin Client service to encrypt and decrypt
data",
            "Effect": "Allow",
            "Principal": {"Service": "thinclient.amazonaws.com"},
            "Action": [
                "kms:GenerateDataKey",
                "kms:Decrypt"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "aws:SourceArn":
                         "arn:aws:thinclient:region:111122223333:*",
                    "kms:EncryptionContext:aws:thinclient:arn":
                         "arn:aws:thinclient:region: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*"
```

```
            ],
            "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.

Los siguientes son ejemplos de declaraciones de política de claves 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`, `GenerateDataKeyDecrypt`, monitorear las operaciones de KMS solicitadas por Amazon WorkSpaces Thin Client para acceder a los datos cifrados por la clave administrada 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": "1.09",
    "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"
            },
            "attributes": {
```

```
                "creationDate": "2024-04-08T13:43:33Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "thinclient.amazonaws.com"
    },
    "eventTime": "2024-04-08T13:44:22Z",
    "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"
}
```

GenerateDataKey

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

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

```
{
    "eventVersion": "1.09",
    "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"
            },
            "attributes": {
                "creationDate": "2024-04-08T12:21:03Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "thinclient.amazonaws.com"
    },
    "eventTime": "2024-04-08T13:03:56Z",
    "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",
    "sharedEventID": "1234abcd-12ab-34cd-56ef-123456SAMPLE",
    "vpcEndpointId": "vpce-1234abcd567SAMPLE",
    "vpcEndpointAccountId": "thinclient.amazonaws.com",
    "eventCategory": "Management"
}
```

GenerateDataKey (by service)

Cuando Amazon WorkSpaces Thin Client utiliza la información `GenerateDataKey` guardada del dispositivo, la `GenerateDataKey` operación se utiliza para cifrar los datos.

La `GenerateDataKey` operación está permitida en la declaración de política clave de KMS con el texto «Permitir que el servicio Amazon WorkSpaces Thin Client cifre y descifre datos».

El siguiente evento de ejemplo registra la GenerateDataKey operación:

```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "thinclient.amazonaws.com"
    },
    "eventTime": "2024-04-08T13:03:56Z",
    "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",
    "sharedEventID": "1234abcd-12ab-34cd-56ef-123456SAMPLE",
    "vpcEndpointId": "vpce-1234abcd567SAMPLE",
    "vpcEndpointAccountId": "thinclient.amazonaws.com",
    "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": "1.09",
    "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"
            },
            "attributes": {
```

```
                "creationDate": "2024-04-08T13:43:33Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "thinclient.amazonaws.com"
    },
    "eventTime": "2024-04-08T13:44:25Z",
    "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",
    "sharedEventID": "1234abcd-12ab-34cd-56ef-123456SAMPLE",
    "vpcEndpointId": "vpce-1234abcd567SAMPLE",
    "vpcEndpointAccountId": "thinclient.amazonaws.com",
    "eventCategory": "Management"
}
```

Decrypt (by service)

Cuando un dispositivo WorkSpaces Thin Client accede a la información del entorno o del dispositivo, la `Decrypt` operación se utiliza para descifrar los datos. La `Decrypt` operación está permitida en la declaración de política clave de KMS con el texto «Permitir que el servicio Amazon WorkSpaces Thin Client cifre y descifre datos».

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


```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "thinclient.amazonaws.com"
    },
    "eventTime": "2024-04-08T13:44:25Z",
    "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",
    "sharedEventID": "1234abcd-12ab-34cd-56ef-123456SAMPLE",
    "vpcEndpointId": "vpce-1234abcd567SAMPLE",
    "vpcEndpointAccountId": "thinclient.amazonaws.com",
    "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
- AWS políticas gestionadas para Amazon WorkSpaces Thin Client
- 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 ayudarle 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 gestionador 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 (IAM Identity Center), la autenticación de inicio de sesión único de su empresa y sus credenciales de Google o Facebook son ejemplos de identidades federadas. Al iniciar sesión como una identidad federada, su gestionador 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 la firma de solicitudes, consulte AWS Signature Versión 4 para solicitudes 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 IAM Identity Center y Autenticación multifactor AWS en IAM 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 utiliza 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, consulta 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 empresarial, 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 utiliza AWS IAM Identity Center. 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, consulta ¿Qué es el Centro de identidades de IAM? en la Guía del usuario de AWS IAM Identity Center .

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 puedes iniciar sesión como grupo. Puedes usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos para grandes conjuntos de usuarios. Por ejemplo, puede asignar un nombre a un grupo IAMAdminsy concederle permisos para administrar 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 de larga duración permanentes; no obstante, los roles proporcionan credenciales temporales. Para obtener más información, consulte Casos de uso para usuarios de IAM 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 persona determinada. Para asumir temporalmente un rol de IAM en el AWS Management Console, puede cambiar de un rol de usuario a uno de IAM (consola). Puedes asumir un rol llamando a una operación de AWS API AWS CLI o usando una URL personalizada. Para más información sobre los métodos para el uso de roles, consulta Métodos para asumir un rol 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 de federación, consulte Crear un rol para un proveedor de identidad de terceros (federación) en la Guía de usuario de IAM. Si utiliza el IAM Identity Center, debe configurar un conjunto de permisos. 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, consulta Conjuntos de permisos en la Guía del usuario de AWS IAM Identity Center .

- 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, con algunas 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, consulta Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.
- Acceso entre servicios: algunos Servicios de AWS utilizan funciones en otros Servicios de AWS. Por ejemplo, cuando realizas una llamada en un servicio, es habitual que ese servicio ejecute aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado al servicio.
  - Sesiones de acceso directo (FAS): cuando utilizas un usuario o un rol de IAM para realizar acciones en AWS ellas, se te considera principal. 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: puedes usar un rol de IAM para administrar las credenciales temporales de las aplicaciones que se ejecutan en una EC2 instancia y realizan AWS CLI solicitudes a la AWS API. Esto es preferible a almacenar las claves de acceso en la EC2 instancia. Para asignar un AWS rol a una EC2 instancia y ponerlo a disposición de todas sus aplicaciones, debe crear un perfil de instancia adjunto a la instancia. Un perfil de instancia contiene el rol y permite que los programas que se ejecutan en la EC2 instancia obtengan credenciales temporales. Para obtener más información, consulte Usar un rol de IAM para conceder permisos a las aplicaciones que se ejecutan en EC2 instancias de Amazon 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. 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 añadir las políticas de IAM a roles y los usuarios pueden asumirlos.

Las políticas de IAM definen permisos para una acción independientemente del método que se utiliza 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 obtener 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. Los 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 () ACLs

Las listas de control de acceso (ACLs) controlan qué responsables (miembros de la cuenta, usuarios o roles) tienen permisos para acceder a un recurso. ACLs 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 compatibles. AWS WAF ACLs Para obtener más información ACLs, consulte la descripción general de la lista de control de acceso (ACL) en la Guía para desarrolladores de Amazon Simple Storage Service.

Otros tipos de políticas

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

- Límites de permisos: un límite de permisos es una 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). Puedes establecer un límite de permisos para una entidad. Los permisos resultantes son la intersección de las políticas basadas en la identidad de la entidad y los límites de permisos. Las políticas basadas en recursos que especifiquen el usuario o rol en el campo `Principal` no estarán restringidas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información sobre los límites de los permisos, consulte Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.
- Políticas de control de servicios (SCPs): SCPs 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 administrar de forma centralizada varios de los Cuentas de AWS que son propiedad de su empresa. Si habilitas todas las funciones de una organización, puedes aplicar políticas de control de servicios (SCPs) a una o a todas tus cuentas. 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 sobre Organizations SCPs, consulte las políticas de control de servicios en la Guía del AWS Organizations usuario.
- Políticas de control de recursos (RCPs): RCPs son políticas de JSON que puedes usar para establecer los permisos máximos disponibles para los recursos de tus cuentas sin actualizar las políticas de IAM asociadas a cada recurso que poseas. El RCP limita los permisos de los recursos en las cuentas de los miembros y puede afectar a los permisos efectivos de las identidades, incluidos los permisos Usuario raíz de la cuenta de AWS, independientemente de si pertenecen a su organización. Para obtener más información sobre Organizations e RCPs incluir una lista de Servicios de AWS ese apoyo RCPs, consulte Políticas de control de recursos (RCPs) en la Guía del AWS Organizations usuario.
- Políticas de sesión: las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de la sesión resultantes son la intersección de las políticas basadas en identidades del rol y las políticas de la sesión. Los permisos también pueden proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para 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 se AWS determina si se debe permitir una solicitud

cuando se trata de varios tipos de políticas, consulte la lógica de evaluación de políticas en la Guía del 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
Políticas basadas en recursos	No
Acciones de políticas	Sí
Recursos de políticas	Sí
Claves de condición de política	Sí
ACLs	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 identidad: 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 asociada. Para obtener 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

Admite políticas basadas en recursos: no

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Los 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 basada en recursos concede acceso a una entidad principal de la misma cuenta, no es necesaria una política basada en identidad adicional.

Para obtener más información, consulte Cross account resource access in IAM en la Guía del usuario de IAM.

Acciones políticas para WorkSpaces Thin Client

Compatibilidad con las 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:

```
thinclient
```

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

```
"Action": [
      "thinclient:action1",
      "thinclient: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

Compatibilidad con los 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 puedes 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). Puedes 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, utiliza 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 ARNs correspondientes, 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

Compatibilidad con 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 puedes 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. Puedes crear expresiones condicionales que utilizan operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud.

Si especifica varios elementos de `Condition` en una instrucción o varias claves en un único elemento de `Condition`, AWS las evalúa mediante una operación `AND` lógica. Si especifica varios

valores para una única clave de condición, AWS evalúa la condición mediante una `OR` operación lógica. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puedes utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puedes 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, consulta 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

ACLs en Thin Client WorkSpaces

Soporta ACLs: No

Las listas de control de acceso (ACLs) controlan qué directores (miembros de la cuenta, usuarios o roles) tienen permisos para acceder a un recurso. ACLs 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 Definición de permisos con la autorización de 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

Compatibilidad con credenciales temporales: sí

Algunas Servicios de AWS no funcionan cuando se inicia sesión con credenciales temporales. Para obtener información adicional, incluida la información sobre cuáles Servicios de AWS funcionan con credenciales temporales, consulta 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 obtener más información sobre el cambio de roles, consulte Cambio de un usuario a un rol de IAM (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 obtener más información, consulte Credenciales de seguridad temporales en IAM.

Permisos principales entre servicios para WorkSpaces Thin Client

Admite sesiones de acceso directo (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 roles 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 únicamente cuando WorkSpaces Thin Client le dé instrucciones para hacerlo.

Funciones vinculadas al servicio para WorkSpaces Thin Client

Compatibilidad 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 puedes ver, pero no editar, los permisos de los roles vinculados a servicios.

Para más información sobre cómo crear o administrar roles vinculados a servicios, consulta 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 puedes añadir las políticas de IAM a roles y los usuarios puedes 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 (consola) 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 ARNs formato 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 servicio.

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 costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están

disponibles en su. Cuenta de AWS Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Con el fin de obtener más información, consulta las políticas administradas por AWS o las políticas administradas por AWS para funciones de tarea en la Guía de usuario de IAM.

- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulta 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, consulta Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.
- Utiliza 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 Validación de políticas con el Analizador de acceso de IAM en la Guía del 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 exigir la MFA cuando se invoquen las operaciones de la API, añada condiciones de MFA a sus políticas. Para más información, consulte Acceso seguro a la API con MFA en la Guía del usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte 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 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 el 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.

JSON

```
{
    "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 gestionadas 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.

JSON

```
{
    "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/*"]
        }
    ]
}
```

AWS políticas gestionadas para Amazon WorkSpaces Thin Client

Una política AWS gestionada es una política independiente creada y administrada por AWS. AWS Las políticas administradas están diseñadas para proporcionar permisos para muchos casos de uso comunes, de modo que pueda empezar a asignar permisos a usuarios, grupos y funciones.

Ten en cuenta que es posible que las políticas AWS administradas no otorguen permisos con privilegios mínimos para tus casos de uso específicos, ya que están disponibles para que los usen todos los AWS clientes. Se recomienda definir políticas administradas por el cliente específicas para sus casos de uso a fin de reducir aún más los permisos.

No puedes cambiar los permisos definidos en AWS las políticas administradas. Si AWS actualiza los permisos definidos en una política AWS administrada, la actualización afecta a todas las identidades principales (usuarios, grupos y roles) a las que está asociada la política. AWS es más probable que actualice una política AWS administrada cuando Servicio de AWS se lance una nueva o cuando estén disponibles nuevas operaciones de API para los servicios existentes.

Para obtener más información, consulte Políticas administradas de AWS en la Guía del usuario de IAM.

AWS política gestionada: AmazonWorkSpacesThinClientReadOnlyAccess

Puede adjuntar la política `AmazonWorkSpacesThinClientReadOnlyAccess` a las identidades de IAM. Esta política otorga permisos de acceso total al servicio WorkSpaces Thin Client y sus dependencias. Para obtener más información sobre esta política administrada, consulte la guía AmazonWorkSpacesThinClientReadOnlyAccessde referencia de políticas AWS administradas.

Detalles de los permisos

Esta política incluye los siguientes permisos.

- `thinclient`(WorkSpaces Thin Client): permite el acceso de solo lectura a todas las acciones de WorkSpaces Thin Client.
- `workspaces`(WorkSpaces): permite permisos para describir los WorkSpaces directorios y los alias de conexión. Se utiliza para comprobar que sus WorkSpaces recursos son compatibles con WorkSpaces Thin Client. También se usa para mostrar estos recursos en la AWS consola de WorkSpaces Thin Client.
- `workspaces-web`(WorkSpaces Secure Browser): permite permisos para describir los WorkSpaces Secure Browser portales y la configuración del usuario. Se utiliza para comprobar que sus WorkSpaces Secure Browser recursos son compatibles con WorkSpaces Thin Client. También se usa para mostrar estos recursos en la AWS consola de WorkSpaces Thin Client.
- `appstream`(AppStream 2.0): permite permisos para describir las pilas AppStream 2.0. Se utiliza para comprobar que los recursos de la AppStream versión 2.0 son compatibles con WorkSpaces Thin Client. También se usa para mostrar estos recursos en la AWS consola de WorkSpaces Thin Client.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowThinClientReadAccess",
      "Effect": "Allow",
      "Action": [
        "thinclient:GetDevice",
        "thinclient:GetDeviceDetails",
        "thinclient:GetEnvironment",
        "thinclient:GetSoftwareSet",
        "thinclient:ListDevices",
        "thinclient:ListDeviceSessions",
        "thinclient:ListEnvironments",
        "thinclient:ListSoftwareSets",
        "thinclient:ListTagsForResource"
      ],
      "Resource": "*"
    },
    {
```

```
      "Sid": "AllowWorkSpacesAccess",
      "Effect": "Allow",
      "Action": [
        "workspaces:DescribeConnectionAliases",
        "workspaces:DescribeWorkspaceDirectories"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowWorkSpacesSecureBrowserAccess",
      "Effect": "Allow",
      "Action": [
        "workspaces-web:GetPortal",
        "workspaces-web:GetUserSettings",
        "workspaces-web:ListPortals"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowAppStreamAccess",
      "Effect": "Allow",
      "Action": [
        "appstream:DescribeStacks"
      ],
      "Resource": "*"
    }
  ]
}
}
```

AWS política gestionada: AmazonWorkSpacesThinClientFullAccess

Puede adjuntar la política `AmazonWorkSpacesThinClientFullAccess` a las identidades de IAM. Esta política otorga permisos de acceso total al servicio WorkSpaces Thin Client y sus dependencias. Para obtener más información sobre esta política administrada, consulte la Guía AmazonWorkSpacesThinClientFullAccessde referencia de políticas AWS administradas.

Detalles de los permisos

Esta política incluye los permisos siguientes:

- `thinclient`(WorkSpaces Thin Client): permite el acceso total a todas las acciones de WorkSpaces Thin Client.

- `workspaces`(WorkSpaces): permite permisos para describir los WorkSpaces directorios y los alias de conexión. Se utiliza para comprobar que sus WorkSpaces recursos son compatibles con WorkSpaces Thin Client. También se usa para mostrar estos recursos en la AWS consola de WorkSpaces Thin Client.
- `workspaces-web`(WorkSpaces Secure Browser): permite permisos para describir los WorkSpaces Secure Browser portales y la configuración del usuario. Se utiliza para comprobar que sus WorkSpaces Secure Browser recursos son compatibles con WorkSpaces Thin Client. También se usa para mostrar estos recursos en la AWS consola de WorkSpaces Thin Client.
- `appstream`(AppStream 2.0): permite permisos para describir las pilas AppStream 2.0. Se utiliza para comprobar que los recursos de la AppStream versión 2.0 son compatibles con WorkSpaces Thin Client. También se usa para mostrar estos recursos en la AWS consola de WorkSpaces Thin Client.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowThinClientFullAccess",
      "Effect": "Allow",
      "Action": [
        "thinclient:*"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowWorkSpacesAccess",
      "Effect": "Allow",
      "Action": [
        "workspaces:DescribeConnectionAliases",
        "workspaces:DescribeWorkspaceDirectories"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowWorkSpacesSecureBrowserAccess",
      "Effect": "Allow",
      "Action": [
        "workspaces-web:GetPortal",
        "workspaces-web:GetUserSettings",
        "workspaces-web:ListPortals"
```

```
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowAppStreamAccess",
      "Effect": "Allow",
      "Action": [
        "appstream:DescribeStacks"
      ],
      "Resource": "*"
    }
  ]
}
}
```

WorkSpaces Thin Client actualiza las políticas AWS gestionadas

Cambio	Descripción	Fecha
AmazonWorkSpacesThinClientReadOnlyAccess: política actualizada	WorkSpaces Thin Client actualizó la política para incluir permisos de lectura limitados para los detalles de los dispositivos y los alias de WorkSpaces conexión.	9 de enero de 2025
AmazonWorkSpacesThinClientFullAccess: política actualizada	WorkSpaces Thin Client actualizó la política para incluir permisos de lectura limitados para los alias de WorkSpaces conexión.	9 de enero de 2025
AmazonWorkSpacesThinClientReadOnlyAccess: política actualizada	WorkSpaces Thin Client actualizó la política para incluir permisos de lectura limitados para las AppStream versiones 2.0, WorkSpaces Web y WorkSpaces.	9 de agosto de 2024

Cambio	Descripción	Fecha
AmazonWorkSpacesThinClientFullAccess: política nueva	Proporciona acceso completo a Amazon WorkSpaces Thin Client, así como acceso limitado a los servicios relacionados necesarios.	9 de agosto de 2024
AmazonWorkSpacesThinClientReadOnlyAccess: política nueva	Proporciona acceso de solo lectura a Amazon WorkSpaces Thin Client y sus dependencias.	19 de julio de 2024
WorkSpaces Thin Client comenzó a rastrear los cambios	WorkSpaces Thin Client comenzó a realizar un seguimiento de los cambios en sus políticas AWS gestionadas.	19 de julio de 2024

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 `thinclient:`*`ListDevices`*.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 thinclient: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 `thinclient:`*`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 conceder permiso a las personas o aplicaciones que necesiten acceso. Si usa AWS IAM Identity Center para administrar las personas y las aplicaciones, debe asignar conjuntos de permisos a los usuarios o grupos para definir su nivel de acceso. Los conjuntos de permisos crean políticas de IAM y las asignan a los roles de IAM asociados a la persona o aplicación de forma automática. Para obtener más información, consulte la sección Conjuntos de permisos en la Guía del usuario de AWS IAM Identity Center .

Si no utiliza IAM Identity Center, debe crear entidades de IAM (usuarios o roles) para las personas o aplicaciones que necesitan acceso. A continuación, debe adjuntar una política a la entidad que les conceda los permisos correctos en WorkSpaces Thin Client. Una vez concedidos los permisos, proporcione las credenciales al usuario o al desarrollador de la aplicación. Utilizarán esas credenciales para acceder a AWS. Para obtener más información sobre la creación de usuarios, grupos, políticas y permisos de IAM, consulte Identidades de IAM y Políticas y permisos en 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 admiten políticas basadas en recursos o listas de control de acceso (ACLs), puede utilizar esas políticas para permitir que las personas accedan a sus recursos.

Para obtener más información, consulte lo siguiente:

- Para saber si WorkSpaces Thin Client admite estas funciones, consulte. Cómo 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 una federación de identidades, consulta Proporcionar acceso a usuarios autenticados externamente (identidad federada) en la Guía del usuario de IAM.
- Para conocer sobre la diferencia entre las políticas basadas en roles y en recursos para el acceso entre cuentas, consulte Acceso a recursos entre cuentas en IAM 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, puedes 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 AWS CloudTrail Guía del usuario de .

Temas

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

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

Amazon WorkSpaces Thin Client está integrado con AWS CloudTrailun servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un Servicio de AWS. 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. Con la información recopilada por Thin Client CloudTrail, puede determinar la solicitud que se realizó a WorkSpaces Thin Client, la dirección IP desde la que se realizó la solicitud, cuándo se realizó y detalles adicionales.

Todas las acciones de Amazon 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 `DeleteDevice` y `GetSoftwareSet` las acciones generan entradas en los archivos de CloudTrail registro. `CreateEnvironment`

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 las credenciales del usuario raíz o del usuario.

- Si la solicitud se realizó en nombre de un usuario de IAM Identity Center.
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro Servicio de AWS.

CloudTrail está activo en tu cuenta Cuenta de AWS al crear la cuenta y automáticamente tienes acceso al historial de CloudTrail eventos. El historial de CloudTrail eventos proporciona un registro visible, consultable, descargable e inmutable de los últimos 90 días de eventos de gestión registrados en un. Región de AWSPara obtener más información, consulte Uso del historial de CloudTrail eventos en la Guía del usuario.AWS CloudTrail La visualización del historial de eventos no conlleva ningún CloudTrail cargo.

Para tener un registro continuo de los eventos de Cuenta de AWS los últimos 90 días, crea un almacén de datos de eventos de senderos o CloudTraillagos.

CloudTrail senderos

Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. Todos los senderos creados con él AWS Management Console son multirregionales. Puede crear un registro de seguimiento de una sola región o de varias regiones mediante la AWS CLI. Se recomienda crear un sendero multirregional, ya que puedes capturar toda la actividad de tu Regiones de AWS cuenta. Si crea un registro de seguimiento de una sola región, solo podrá ver los eventos registrados en la Región de AWS del registro de seguimiento. Para obtener más información acerca de los registros de seguimiento, consulte Creación de un registro de seguimiento para su Cuenta de AWS y Creación de un registro de seguimiento para una organización en la Guía del usuario de AWS CloudTrail .

Puede enviar una copia de sus eventos de administración en curso a su bucket de Amazon S3 sin coste alguno CloudTrail mediante la creación de una ruta; sin embargo, hay cargos por almacenamiento en Amazon S3. Para obtener más información sobre CloudTrail los precios, consulte AWS CloudTrail Precios. Para obtener información acerca de los precios de Amazon S3, consulte Precios de Amazon S3.

CloudTrail Almacenes de datos de eventos en Lake

CloudTrail Lake le permite ejecutar consultas basadas en SQL en sus eventos. CloudTrail Lake convierte los eventos existentes en formato JSON basado en filas al formato Apache ORC. ORC es un formato de almacenamiento en columnas optimizado para una recuperación rápida

de datos. Los eventos se agregan en almacenes de datos de eventos, que son recopilaciones inmutables de eventos en función de criterios que se seleccionan aplicando selectores de eventos avanzados. Los selectores que se aplican a un almacén de datos de eventos controlan los eventos que perduran y están disponibles para la consulta. Para obtener más información sobre CloudTrail Lake, consulte Cómo trabajar con AWS CloudTrail Lake en la Guía del AWS CloudTrail usuario.

CloudTrail Los almacenes de datos y las consultas sobre eventos de Lake conllevan costes. Cuando crea un almacén de datos de eventos, debe elegir la opción de precios que desee utilizar para él. La opción de precios determina el costo de la incorporación y el almacenamiento de los eventos, así como el período de retención predeterminado y máximo del almacén de datos de eventos. Para obtener más información sobre CloudTrail los precios, consulte AWS CloudTrail Precios.

WorkSpaces Eventos de datos de Thin Client en CloudTrail

Los eventos de datos proporcionan información sobre las operaciones de recursos realizadas en o dentro de un recurso (por ejemplo, el registro de un dispositivo por parte de un usuario final). Se denominan también operaciones del plano de datos. Los eventos de datos suelen ser actividades de gran volumen. De forma predeterminada, CloudTrail no registra los eventos de datos. El historial de CloudTrail eventos no registra los eventos de datos.

Se aplican cargos adicionales a los eventos de datos. Para obtener más información sobre CloudTrail los precios, consulta AWS CloudTrail Precios.

Puede registrar eventos de datos para los tipos de recursos de WorkSpaces Thin Client mediante la CloudTrail consola o las operaciones de la CloudTrail API. AWS CLI Para obtener más información sobre cómo registrar los eventos de datos, consulte Registro de eventos de datos con la AWS Management Console y Registro de eventos de datos con la AWS Command Line Interface en la Guía del usuario de AWS CloudTrail .

En la siguiente tabla se enumeran los tipos de recursos de WorkSpaces Thin Client para los que puede registrar eventos de datos. La columna Tipo de evento de datos (consola) muestra el valor que se puede elegir en la lista de tipos de eventos de datos de la CloudTrail consola. La columna de valores resources.type muestra el `resources.type` valor que se debe especificar al configurar los selectores de eventos avanzados mediante o. AWS CLI CloudTrail APIs La CloudTrail columna Datos APIs registrados muestra las llamadas a la API registradas CloudTrail para el tipo de recurso.

Tipo de evento de datos (consola)	resources.type value	Datos APIs registrados en CloudTrail
ThinClientDevice	`AWS::WorkSpacesThinClient::Device`	• RegisterDevice • UpdateDeviceDetails

Puede configurar selectores de eventos avanzados para filtrar según los campos `eventName`, `readOnly` y `resources.ARN` y así registrar solo los eventos que son importantes para usted. Para obtener más información sobre estos campos, consulte AdvancedFieldSelector en la Referencia de la API de AWS CloudTrail .

WorkSpaces Eventos de administración de Thin Client en CloudTrail

Los eventos de administración proporcionan información sobre las operaciones de administración que se llevan a cabo en los recursos de su empresa Cuenta de AWS. Se denominan también operaciones del plano de control. De forma predeterminada, CloudTrail registra los eventos de administración.

Amazon WorkSpaces Thin Client registra todas las operaciones del plano de control de WorkSpaces Thin Client como eventos de administración. Para obtener una lista de las operaciones del plano de control de Amazon WorkSpaces Thin Client en las que WorkSpaces Thin Client inicia sesión CloudTrail, consulte la referencia de la API de Amazon WorkSpaces Thin Client.

WorkSpaces Ejemplos de eventos de Thin Client

Un evento representa una solicitud única de cualquier fuente e incluye información sobre la operación de API solicitada, la fecha y la hora de la operación, 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 los eventos no aparecen en ningún orden específico.

El siguiente ejemplo muestra un CloudTrail evento que demuestra la `RegisterDevice` operación.


```
{
      "eventVersion": "1.10",
      "userIdentity": {
        "type": "Unknown",
        "accountId": "111111111111",
        "userName": "DSN: G1X11X11111111XX"
```

```
    },
    "eventTime": "2024-06-19T17:13:44Z",
    "eventSource": "thinclient.amazonaws.com",
    "eventName": "RegisterDevice",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": {
      "dsn": "G1X11X11111111XX",
      "activationCode": "xxx1xxx1",
      "model": "AFTGAZL"
    },
    "responseElements": null,
    "requestID": "f626fb2b-a841-4b87-9a9b-685a62024058",
    "eventID": "214385d7-9249-4f60-af56-b4c951e0491d",
    "readOnly": false,
    "resources": [
      {
        "type": "AWS::ThinClient::Device",
        "ARN": "arn:aws:thinclient:us-west-2:111111111111:device/DEVICE_ID"
      }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": false,
    "recipientAccountId": "111111111111",
    "eventCategory": "Data"
  }
```

El siguiente ejemplo muestra un CloudTrail evento que demuestra la `UpdateDeviceDetails` operación.

```
{
    "eventVersion": "1.10",
    "userIdentity": {
      "type": "Unknown",
      "accountId": "111111111111",
      "userName": "DSN: G1X11X11111111XX"
    },
    "eventTime": "2024-10-21T17:46:27Z",
    "eventSource": "thinclient.amazonaws.com",
    "eventName": "UpdateDeviceDetails",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "AWS Internal",
```

```
    "userAgent": "AWS Internal",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "7d562fcf-a9ce-40da-9e5c-9ef390b8b83c",
    "eventID": "f294b614-b00c-45ef-b293-cd389121033a",
    "readOnly": false,
    "resources": [
      {
        "type": "AWS::ThinClient::Device",
        "ARN": "arn:aws:thinclient:us-west-2:111111111111:device/DEVICE_ID"
      }
    ],
    "eventType": "AwsServiceEvent",
    "managementEvent": false,
    "recipientAccountId": "111111111111",
    "serviceEventDetails": {
      "settings": {
        "network": {
          "ethernet": {
            "addresses": [
              {
                "gateway": "gateway",
                "localIp": "localIp",
                "type": "IPV4"
              }
            ],
            "connectionStatus": "NOT_CONNECTED"
          },
          "networkInterfaceInUse": "ETHERNET",
          "wifi": {
            "addresses": [
              {
                "gateway": "gateway",
                "localIp": "localIp",
                "type": "IPV4"
              }
            ],
            "connectionStatus": "NOT_CONNECTED"
          }
        },
        "peripherals": {
          "bluetooth": {
            "enabledStatus": "ENABLED"
          },
```

```
            "keyboards": [
              {
                "name": "name",
                "type": "USB"
              }
            ],
            "mice": [
              {
                "name": "name",
                "type": "BLUETOOTH"
              }
            ],
            "sound": {
              "microphones": [
                {
                  "name": "name",
                  "selectionStatus": "SELECTED",
                  "type": "BUILT_IN"
                }
              ],
              "speakers": [
                {
                  "name": "name",
                  "selectionStatus": "SELECTED",
                  "type": "BUILT_IN"
                }
              ]
            },
            "webcams": [
              {
                "name": "name",
                "selectionStatus": "SELECTED",
                "type": "USB"
              }
            ]
          },
          "powerAndSleep": {
            "sleepAfter": "FIFTEEN_MINUTES"
          }
        },
        "updatedAt": "2024-10-21T17:46:27.624Z"
      },
      "eventCategory": "Data"
```

```
    }
```

Para obtener información sobre el contenido de los CloudTrail registros, consulte el contenido de los CloudTrail registros en la Guía del AWS CloudTrail usuario.

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 los 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 puntos 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
AWS política gestionada: AmazonWorkSpacesThinClientFullAccess	Amazon WorkSpaces Thin Client ha añadido la versión 2 de la política AmazonWorkSpacesThinClientFullAccess gestionada.	9 de enero de 2025
AWS política gestionada: AmazonWorkSpacesThinClientReadOnlyAccess	Amazon WorkSpaces Thin Client agregó la versión 3 de políticas AmazonWorkSpacesThinClientReadOnlyAccess administradas.	9 de enero de 2025
Registro de llamadas a la API de Amazon WorkSpaces Thin Client mediante AWS CloudTrail Configuración del dispositivo Cifrado de datos en reposo para Amazon WorkSpaces Thin Client	Se agregó una nueva sección para eventos de datos. Se agregó una nueva sección para la configuración del dispositivo. Se actualizó la información del KMS en la sección sobre el cifrado de datos en reposo.	28 de octubre de 2024
Continuidad empresarial	Se agregó una nueva sección para la continuidad empresarial y la recuperación ante desastres.	6 de septiembre de 2024

Cambio	Descripción	Fecha
AWS política gestionada: AmazonWorkSpacesThinClientFullAccess	Amazon WorkSpaces Thin Client ha añadido una política AmazonWorkSpacesThinClientFullAccess gestionada.	9 de agosto de 2024
AWS política gestionada: AmazonWorkSpacesThinClientReadOnlyAccess	Amazon WorkSpaces Thin Client agregó la versión 2 de las políticas AmazonWorkSpacesThinClientReadOnlyAccess administradas.	9 de agosto de 2024
Configuración de WorkSpaces Personal para WorkSpaces Thin Client	Actualizado el para el nuevo WorkSpaces Personal.	7 de agosto de 2024
Configuración de WorkSpaces grupos para WorkSpaces Thin Client	Se agregó una nueva sección para nuevos WorkSpaces grupos.	7 de agosto de 2024
AWS política gestionada: AmazonWorkSpacesThinClientReadOnlyAccess	Amazon WorkSpaces Thin Client ha añadido una política AmazonWorkSpacesThinClientReadOnlyAccess gestionada.	19 de julio de 2024
AWS políticas gestionadas para Amazon WorkSpaces Thin Client	Amazon WorkSpaces Thin Client ha empezado a realizar un seguimiento de los cambios.	19 de julio de 2024
Configuración WorkSpaces para Amazon WorkSpaces Thin Client	Se actualizó la lista de sistemas operativos.	12 de febrero de 2024

Cambio	Descripción	Fecha
Configuración de la AppStream versión 2.0 para Amazon WorkSpaces Thin Client	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.