AWS Documento técnico

Mejores prácticas para la implementación WorkSpaces

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Mejores prácticas para la implementación WorkSpaces: AWS Documento técnico

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Las marcas comerciales y la imagen comercial de Amazon no se pueden utilizar en relación con ningún producto o servicio que no sea de Amazon, de ninguna manera que pueda causar confusión entre los clientes y que menosprecie o desacredite a Amazon. Todas las demás marcas comerciales que no son propiedad de Amazon son propiedad de sus respectivos propietarios, que pueden o no estar afiliados, relacionados o patrocinados por Amazon.

Table of Contents

Mejores prácticas para la implementación de Amazon WorkSpaces

Fecha de publicación: 1 de junio de 2022 () Revisiones del documento

Resumen

Este documento técnico describe un conjunto de mejores prácticas para la implementación de. WorkSpaces El documento técnico cubre las consideraciones sobre la red, los servicios de directorio y la autenticación de usuarios, la seguridad y la supervisión y el registro.

Este documento técnico también permite un acceso rápido a la información relevante y está dirigido a ingenieros de redes, ingenieros de directorios o ingenieros de seguridad.

Introducción

Amazon WorkSpaces es un servicio de computación de escritorio gestionado en la nube. Amazon WorkSpaces elimina la carga de adquirir o implementar hardware o instalar software complejo, y ofrece una experiencia de escritorio con unos pocos clics en la AWS Management Consoleinterfaz de línea de comandos (CLIAWS) de Amazon Web Services () o mediante la interfaz de programación de aplicaciones (API). Con Amazon WorkSpaces, puede lanzar un escritorio Microsoft Windows o Amazon Linux en cuestión de minutos, lo que le permite conectarse y acceder a su software de escritorio de forma segura, fiable y rápida desde las instalaciones o desde una red externa. Puede hacer lo siguiente:

- Aproveche su Microsoft Active Directory (AD) local existente mediante Directory Service: AWS Active Directory Connector (AD Connector).
- Amplíe su directorio a la AWS nube.
- Cree un directorio administrado con AWS Directory Service Microsoft AD o Simple AD para administrar sus usuarios y WorkSpaces.
- Aproveche su servidor RADIUS local o alojado en la nube con AD Connector para proporcionarle autenticación multifactor (MFA). WorkSpaces

Puede automatizar el aprovisionamiento de Amazon WorkSpaces mediante la CLI o la API, lo que le permite WorkSpaces integrar Amazon en sus flujos de trabajo de aprovisionamiento existentes.

Por motivos de seguridad, además del cifrado de red integrado que proporciona el WorkSpaces servicio de Amazon, también puedes habilitar el cifrado en reposo para tu WorkSpaces. Consulte la WorkSpaces sección Cifrado de este documento.

Puede implementar aplicaciones en su empresa WorkSpaces mediante las herramientas locales existentes, como Microsoft System Center Configuration Manager (SCCM), Puppet Enterprise o Ansible.

En las siguientes secciones se proporcionan detalles sobre Amazon WorkSpaces, se explica cómo funciona el servicio, se describe lo que se necesita para lanzar el servicio y se indican las opciones y funciones disponibles para su uso.

WorkSpaces requisitos

El WorkSpaces servicio de Amazon requiere tres componentes para implementarse correctamente:

- WorkSpaces aplicación cliente: dispositivo cliente WorkSpaces compatible con Amazon. Consulte Cómo empezar con su. WorkSpace

  También puede utilizar un ordenador personal a través del protocolo de Internet (PCoIP) Zero Clients para conectarse. WorkSpaces Para obtener una lista de los dispositivos disponibles, consulte PCoIP Zero Clients for Amazon. WorkSpaces
- Un servicio de directorio para autenticar a los usuarios y proporcionarles acceso WorkSpace: Amazon trabaja WorkSpaces actualmente con AWS Directory Service y Microsoft AD. Puedes usar tu servidor AD local con AWS Directory Service para respaldar tus credenciales de usuario empresarial actuales en Amazon WorkSpaces.
- Amazon Virtual Private Cloud (Amazon VPC) en la que ejecutar tu Amazon WorkSpaces: necesitarás un mínimo de dos subredes para una implementación de Amazon, ya que cada construcción de AWS Directory Service requiere dos subredes en una WorkSpaces implementación Multi-AZ.

Consideraciones sobre la red

Cada una WorkSpace está asociada a la construcción específica de Amazon VPC y AWS Directory Service que utilizó para crearla. Todas las estructuras de AWS Directory Service (Simple AD, AD Connector y Microsoft AD) requieren dos subredes para funcionar, cada una en distintas zonas de disponibilidad (AZ). Las subredes están afiliadas permanentemente a una construcción de Directory Service y no se pueden modificar una vez creada. Por ello, es imprescindible que determine los tamaños de subred correctos antes de crear la estructura de servicios de directorio. Tenga en cuenta lo siguiente antes de crear las subredes:

- ¿Cuántas WorkSpaces necesitará con el tiempo?
- ¿Cuál es el crecimiento esperado?
- ¿Qué tipos de usuarios necesitará acomodar?
- ¿Cuántos dominios de AD conectarás?
- ¿Dónde se encuentran sus cuentas empresariales?

Amazon recomienda definir los grupos de usuarios, o personas, en función del tipo de acceso y la autenticación de usuario que necesite como parte del proceso de planificación. Las respuestas a estas preguntas son útiles cuando necesitas limitar el acceso a determinadas aplicaciones o recursos. Las personas de usuario definidas pueden ayudarle a segmentar y restringir el acceso mediante AWS Directory Service, listas de control de acceso a la red, tablas de enrutamiento y grupos de seguridad de VPC. Cada construcción de AWS Directory Service usa dos subredes y aplica la misma configuración a todos los WorkSpaces lanzamientos desde esa construcción. Por ejemplo, puede usar un grupo de seguridad que se aplique a todos los WorkSpaces conectados a un AD Connector para especificar si se requiere MFA o si un usuario final puede tener acceso de administrador local en su dispositivo. WorkSpace

> **Note**
>
> Cada AD Connector se conecta a su Microsoft AD empresarial existente. Para aprovechar esta capacidad y especificar una unidad organizativa (OU), debe crear su Directory Service para tener en cuenta las personas de sus usuarios.

Diseño de VPC

En esta sección, se describen las prácticas recomendadas para dimensionar la VPC y las subredes, el flujo de tráfico y las implicaciones para el diseño de los servicios de directorio.

Estos son algunos aspectos que debe tener en cuenta al diseñar la VPC, las subredes, los grupos de seguridad, las políticas de enrutamiento y las listas de control de acceso a la red (ACL) para su Amazon, de WorkSpaces modo que pueda crear su WorkSpaces entorno con escalabilidad, seguridad y facilidad de administración:

- VPC: se recomienda utilizar una VPC independiente específica para la implementación. WorkSpaces Con una VPC independiente, puede especificar las barreras de control y seguridad necesarias para su empresa WorkSpaces mediante la creación de una separación de tráfico.
- Servicios de directorio: cada AWS Directory Service construcción requiere un par de subredes que proporcionen un servicio de directorio de alta disponibilidad dividido entre las AZ.
- Tamaño de subred: WorkSpaces las implementaciones están vinculadas a una construcción de directorio y residen en la misma VPC que haya elegido AWS Directory Service, pero pueden estar en diferentes subredes de VPC. Algunas consideraciones:
  - Los tamaños de las subredes son permanentes y no pueden cambiar. Debe dejar un amplio espacio para el crecimiento futuro.
  - Puede especificar un grupo de seguridad predeterminado para el que elija AWS Directory Service. El grupo de seguridad se aplica a todos los WorkSpaces que están asociados a la AWS Directory Service construcción específica.
  - Puede hacer que varias instancias AWS Directory Service usen la misma subred.

Tenga en cuenta sus planes para el futuro cuando diseñe su VPC. Por ejemplo, es posible que desee agregar componentes de administración, como un servidor antivirus, un servidor de administración de parches o un servidor de MFA AD o RADIUS. Vale la pena planificar direcciones IP adicionales disponibles en el diseño de su VPC para adaptarse a dichos requisitos.

Para obtener orientación y consideraciones detalladas sobre el diseño de las VPC y el tamaño de las subredes, consulte la presentación de re:Invent How Amazon.com is Moving to Amazon. WorkSpaces

Interfaces de red

Cada una WorkSpaces tiene dos interfaces de red elásticas (ENI), una interfaz de red de administración () y una interfaz de red `eth0` principal (). `eth1` AWS utiliza la interfaz de red de administración para administrar la WorkSpace : es la interfaz en la que termina la conexión del cliente. AWS utiliza un rango de direcciones IP privadas para esta interfaz. Para que el enrutamiento de red funcione correctamente, no puede usar este espacio de direcciones privado en ninguna red que pueda comunicarse con su WorkSpaces VPC.

Para obtener una lista de los rangos de IP privadas que se utilizan por región, consulta Amazon WorkSpaces Details.

> **Note**
>
> Amazon WorkSpaces y sus interfaces de red de administración asociadas no residen en su VPC y no puede ver la interfaz de red de administración ni el ID de instancia de Amazon Elastic Compute Cloud (Amazon EC2) en AWS Management Console su VPC (consulteFigure 5, y). Figure 6 Figure 7 Sin embargo, puede ver y modificar la configuración del grupo de seguridad de su interfaz de red principal (`eth1`) en la consola. La interfaz de red principal de cada una de WorkSpace ellas cuenta para sus cuotas de recursos de ENI en Amazon EC2. Para despliegues grandes de Amazon WorkSpaces, necesitas abrir un ticket de soporte a través del AWS Management Console para aumentar tus cuotas de ENI.

Flujo de tráfico

Puedes dividir el WorkSpaces tráfico de Amazon en dos componentes principales:

- El tráfico entre el dispositivo cliente y el WorkSpaces servicio de Amazon.
- El tráfico entre el WorkSpaces servicio de Amazon y el tráfico de la red del cliente.

En la siguiente sección se analizan estos dos componentes.

Dispositivo cliente para WorkSpace

Independientemente de su ubicación (local o remota), el dispositivo que ejecuta el WorkSpaces cliente de Amazon utiliza los mismos dos puertos para la conectividad con el WorkSpaces servicio

de Amazon. El cliente utiliza el puerto 443 (puerto HTTPS) para toda la información relacionada con la autenticación y la sesión, y el puerto 4172 (puerto PCoIP), con el protocolo de control de transmisión (TCP) y el protocolo de datagramas de usuario (UDP), para la transmisión de píxeles a una determinada red y para comprobar el estado de la red. WorkSpace El tráfico de ambos puertos está cifrado. El tráfico del puerto 443 se usa para la autenticación y la información de sesión y usa TLS para cifrar el tráfico. El tráfico de streaming de píxeles utiliza el cifrado AES de 256 bits para la comunicación entre el cliente y el cliente, a través de la WorkSpace pasarela `eth0` de streaming. Puede encontrar más información en la Seguridad sección de este documento.

Publicamos los rangos de IP por región de nuestras pasarelas de transmisión PCoIP y los puntos finales de comprobación del estado de la red. Puedes limitar el tráfico saliente en el puerto 4172 desde tu red corporativa a la pasarela de AWS streaming y a los puntos finales de comprobación del estado de la red permitiendo únicamente el tráfico saliente del puerto 4172 a AWS las regiones específicas en las que utilizas Amazon. WorkSpaces Para conocer los rangos de IP y los puntos finales de comprobación del estado de la red, consulte los rangos de IP de Amazon WorkSpaces PCoIP Gateway.

El WorkSpaces cliente de Amazon tiene una verificación de estado de la red integrada. Esta utilidad muestra a los usuarios si su red admite una conexión mediante un indicador de estado en la parte inferior derecha de la aplicación. La siguiente figura muestra una vista más detallada del estado de la red. Para acceder a ella, seleccione Red en la parte superior derecha del cliente.

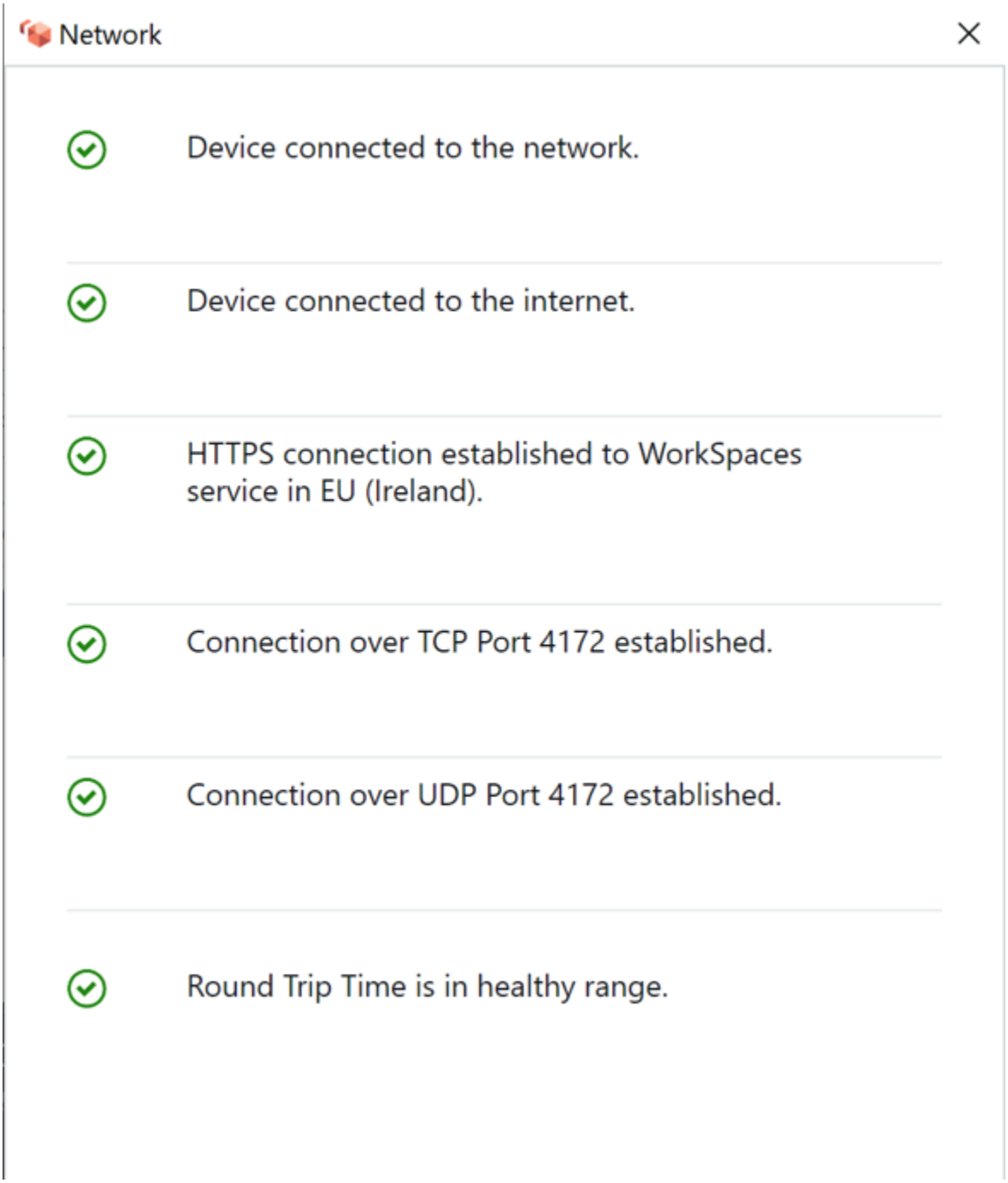

Figura 1: WorkSpaces Cliente: comprobación de red

Un usuario inicia una conexión desde su cliente al WorkSpaces servicio de Amazon proporcionando su información de inicio de sesión para el directorio utilizado por la construcción de Directory Service, normalmente su directorio corporativo. La información de inicio de sesión se envía mediante HTTPS a las pasarelas de autenticación del WorkSpaces servicio de Amazon en la región en la que WorkSpace se encuentra. A continuación, la pasarela de autenticación del WorkSpaces servicio de

Amazon reenvía el tráfico a la construcción específica de AWS Directory Service asociada a la suya WorkSpace.

Por ejemplo, cuando se utiliza el AD Connector, el AD Connector reenvía la solicitud de autenticación directamente a tu servicio de AD, que puede estar en las instalaciones o en una AWS VPC. Para obtener más información, consulte la sección Escenarios de implementación de AD DS de este documento. El AD Connector no almacena ninguna información de autenticación y actúa como un proxy sin estado. Como resultado, es imprescindible que el AD Connector tenga conectividad con un servidor AD. El AD Connector determina a qué servidor AD conectarse mediante los servidores DNS que defina al crear el AD Connector.

Si utilizas un AD Connector y tienes el MFA activado en el directorio, el token de MFA se comprueba antes de la autenticación del servicio de directorio. Si se produce un error en la validación de la MFA, la información de inicio de sesión del usuario no se reenvía a AWS Directory Service.

Una vez que el usuario se autentica, el tráfico de transmisión comienza utilizando el puerto 4172 (puerto PCoIP) a través de la puerta de enlace de transmisión hasta el AWS . WorkSpace La información relacionada con la sesión se sigue intercambiando a través de HTTPS durante toda la sesión. El tráfico de streaming utiliza el primer ENI de la WorkSpace (`eth0`de la WorkSpace) que no está conectada a la VPC. La conexión de red desde la pasarela de streaming al ENI la gestiona AWS. En caso de que se produzca un fallo de conexión entre las pasarelas de transmisión y la ENI de WorkSpaces transmisión, se CloudWatch generará un evento. Para obtener más información, consulta la CloudWatch sección Supervisión o registro con Amazon de este documento.

La cantidad de datos que se envían entre el WorkSpaces servicio de Amazon y el cliente depende del nivel de actividad de los píxeles. Para garantizar una experiencia óptima para los usuarios, recomendamos que el tiempo de ida y vuelta (RTT) entre el WorkSpaces cliente y la AWS región en la que WorkSpaces se encuentra usted sea inferior a 100 milisegundos (ms). Por lo general, esto significa que su WorkSpaces cliente se encuentra a menos de dos mil millas de la región en la que WorkSpace se aloja. La página web Connection Health Check puede ayudarte a determinar la AWS región más óptima para conectarte al WorkSpaces servicio de Amazon.

Amazon WorkSpaces Service a VPC

Una vez que se autentica una conexión de un cliente a un cliente WorkSpace y se inicia el tráfico de streaming, el WorkSpaces cliente mostrará un escritorio Windows o Linux (su Amazon WorkSpace) que está conectado a su nube privada virtual (VPC), y su red debería mostrar que ha establecido esa conexión. La interfaz WorkSpace de red elástica (ENI) principal, identificada como`eth1`, tendrá

una dirección IP asignada desde el servicio de Protocolo de configuración dinámica de host (DHCP) que proporciona la VPC, normalmente desde las mismas subredes que su Directory AWS Service. La dirección IP permanece en ella WorkSpace durante toda la vida útil de la. WorkSpace El ENI de su VPC tiene acceso a cualquier recurso de la VPC y a cualquier red que haya conectado a su VPC (mediante un emparejamiento de VPC, una conexión o una conexión VPN). AWS Direct Connect

El acceso del ENI a los recursos de la red viene determinado por la tabla de rutas de la subred y el grupo de seguridad predeterminado que el AWS Directory Service configura para cada uno WorkSpace, así como por cualquier grupo de seguridad adicional que usted asigne al ENI. Puede añadir grupos de seguridad al ENI situado frente a su VPC en cualquier momento mediante la AWS Management Console tecla o. AWS CLI (Para obtener más información sobre los grupos de seguridad, consulte Security Groups for Your WorkSpaces.) Además de los grupos de seguridad, puede usar el firewall basado en host que prefiera en un momento dado WorkSpace para limitar el acceso de la red a los recursos de la VPC.

Se recomienda crear el conjunto de opciones de DHCP con las IP del servidor DNS y los nombres de dominio totalmente cualificados que sean autoritativos para su Active Directory específico de su entorno y, a continuación, asignar esas opciones de DHCP creadas de forma personalizada y configuradas a la Amazon VPC que utiliza Amazon. WorkSpaces De forma predeterminada, Amazon Virtual Private Cloud (Amazon VPC) usa el AWS DNS en lugar del DNS del servicio de directorio. El uso de un conjunto de opciones de DHCP garantizará una resolución adecuada de los nombres de DNS y una configuración coherente de sus servidores de nombres de DNS internos WorkSpaces, no solo para su carga de trabajo o instancia, sino también para cualquier carga de trabajo o instancia de soporte que haya planificado para su implementación.

Cuando se aplican las opciones de DHCP, hay dos diferencias importantes en la forma en que se aplican WorkSpaces en comparación con la forma en que se aplican en las instancias EC2 tradicionales:

- La primera diferencia es la forma en que se aplicarán los sufijos DNS de las opciones de DHCP. Cada uno WorkSpace tiene una configuración de DNS configurada para su adaptador de red con las opciones Añadir sufijos DNS principales y específicos de la conexión y Añadir sufijos principales de los sufijos DNS principales activadas. La configuración se actualizará con el sufijo DNS configurado en el AWS Directory Service que registró y asociado al mismo de forma WorkSpace predeterminada. Además, si el sufijo DNS configurado en el conjunto de opciones de DHCP utilizado es diferente, se agregará y se aplicará a todos los sufijos asociados. WorkSpaces

- La segunda diferencia es que las IP DNS de la opción DHCP configuradas no se aplicarán a ellas WorkSpace debido a que el WorkSpaces servicio Amazon prioriza las direcciones IP de los controladores de dominio del directorio configurado.

Como alternativa, puede configurar una zona alojada privada de Route 53 para admitir un entorno de DNS híbrido o dividido y obtener la resolución de DNS adecuada para su WorkSpaces entorno de Amazon. Para obtener más información, consulte Opciones de DNS de nube híbrida para VPC y DNS AWS híbrido con Active Directory.

> **Note**
>
> Cada uno WorkSpace debe actualizar la tabla de IP al aplicar un conjunto de opciones de DHCP nuevo o diferente a la VPC. Para actualizar, puede ejecutar ipconfig /renew o reiniciar cualquiera WorkSpace de las unidades de la VPC configuradas con las opciones de DHCP actualizadas configuradas. Si utilizas AD Connector y actualizas las direcciones IP de las direcciones IP/controladores de dominio conectados, debes actualizar la clave de `DomainJoinDNS` registro de Skylight en tu. WorkSpaces Se recomienda hacerlo mediante un GPO. La ruta a esta clave de registro es`HKLM:\SOFTWARE\Amazon\Skylight`. Este valor no `REG_SZ` se actualiza si se modifica la configuración de DNS del conector AD y los conjuntos de opciones de DHCP de la VPC tampoco actualizarán esta clave.

La figura de la sección Escenarios de implementación de AD DS de este documento técnico muestra el flujo de tráfico descrito.

Como se ha explicado anteriormente, el WorkSpaces servicio Amazon prioriza las direcciones IP del controlador de dominio del directorio configurado para la resolución de DNS e ignora los servidores DNS configurados en el conjunto de opciones de DHCP. Si necesitas tener un control más detallado de la configuración del servidor DNS de tu Amazon WorkSpaces, puedes usar las instrucciones para actualizar los servidores DNS de Amazon WorkSpaces en la guía Actualizar servidores DNS para Amazon de la WorkSpaces Guía de WorkSpaces administración de Amazon.

Si WorkSpaces necesita resolver otros servicios en AWS la VPC y utiliza las opciones de DHCP predeterminadas establecidas con su VPC, el servicio DNS del controlador de dominio de esta VPC debe estar configurado para utilizar el reenvío de DNS, apuntando al servidor DNS de Amazon con la dirección IP en la base del CIDR de la VPC más dos; es decir, si el CIDR de la VPC es 10.0.0.0/24, debe configurar el reenvío de DNS utilizando el solucionador de DNS de Route 53 estándar en 10.0.0.2.

En caso de WorkSpaces que necesite la resolución de DNS de los recursos de su red local, puede usar un punto final de salida de Route 53 Resolver, crear una regla de reenvío de Route 53 y asociar esta regla a las VPC que requieren esta resolución de DNS. Si ha configurado el reenvío del servicio DNS de su controlador de dominio al solucionador de DNS de Route 53 predeterminado de su VPC, como se explica en el párrafo anterior, el proceso de resolución de DNS se encuentra en la guía Resolución de consultas de DNS entre VPC y su red de la Guía para desarrolladores de Amazon Route 53.

Si utiliza el conjunto de opciones de DHCP predeterminado y necesita otros hosts de sus VPC que no forman parte de su dominio de Active Directory para poder resolver los nombres de host en su espacio de nombres de Active Directory, puede usar este punto final saliente de Route 53 Resolver y agregar otra regla de reenvío de Route 53 que reenvíe las consultas de DNS de su dominio de Active Directory a sus servidores DNS de Active Directory. Esta regla de reenvío de Route 53 tendrá que estar asociada al punto final saliente de Route 53 Resolver que puede acceder al servicio DNS de Active Directory y a todas las VPC que desee habilitar para resolver los registros de DNS en su dominio de WorkSpaces Active Directory.

Del mismo modo, se puede utilizar un terminal entrante de Route 53 Resolver para permitir la resolución por DNS de los registros DNS de su dominio de WorkSpaces Active Directory procedentes de la red local.

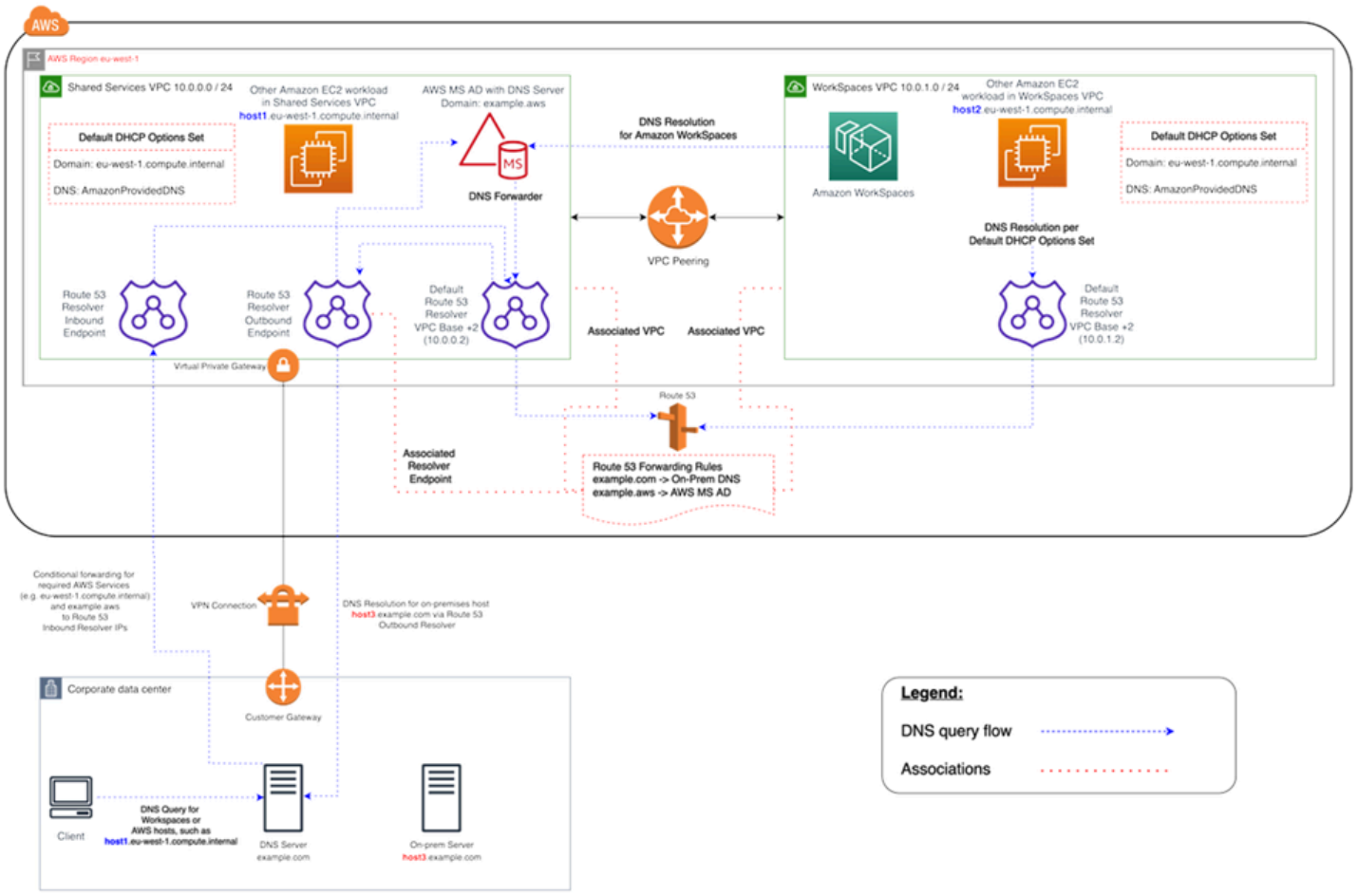

Figura 2: Ejemplo de resolución de WorkSpaces DNS con puntos finales de Route 53

- Amazon WorkSpaces utilizará el servicio DNS AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD) para la resolución de DNS. El servicio AWS Managed Microsoft AD DNS resuelve el `example.aws` dominio y reenvía todas las demás consultas de DNS al solucionador de DNS de Route 53 predeterminado en la dirección IP base CIDR de la VPC +2 para habilitar la resolución de DNS.

  La VPC de Shared Services contiene un punto final de resolución de salida de Route 53, que está asociado a dos reglas de reenvío de Route 53. Una de estas reglas reenvía las consultas de DNS del `example.com` dominio a los servidores DNS locales. La segunda regla reenvía las consultas de DNS de su AWS Managed Microsoft AD dominio `example.aws` al servicio DNS de Active Directory en la VPC de Shared Services.

  Con esta arquitectura, Amazon WorkSpaces podrá resolver las consultas de DNS para lo siguiente:

  - Tu AWS Managed Microsoft AD dominio`example.aws`.
  - Las instancias EC2 del dominio configuradas con el conjunto de opciones de DHCP predeterminado (por ejemplo`host1.eu-west-1.compute.internal`), así como otros AWS servicios o puntos finales.
  - Los hosts y los servicios de su dominio local, como. `host3.example.com`
- • Las demás cargas de trabajo de EC2 de la VPC de Shared Services (`host1.eu-west-1.compute.internal`) y de la WorkSpaces VPC (`host2.eu-west-1.compute.internal`) pueden utilizar las mismas resoluciones de DNS que las suyas WorkSpaces, siempre que las reglas de reenvío de Route 53 estén asociadas a ambas VPC. En este caso, la resolución de DNS del `example.aws` dominio pasará por el solucionador de DNS de Route 53 predeterminado en la dirección IP base CIDR de la VPC +2, que, según las reglas de reenvío de Route 53 configuradas y asociadas, la reenviará a través del punto de enlace saliente de Route 53 Resolver al WorkSpaces servicio DNS de Active Directory.
- • Por último, un cliente local también puede realizar la misma resolución de DNS, ya que el servidor DNS local está configurado con reenviadores condicionales para los `eu-west-1.compute.internal` dominios `example.aws` y, que reenvían las consultas de DNS de estos dominios a las direcciones IP del punto final entrante de Route 53 Resolver.

Ejemplo de una configuración típica

Consideremos un escenario en el que tiene dos tipos de usuarios y su AWS Directory Service utiliza un AD centralizado para la autenticación de los usuarios:

- Trabajadores que necesitan acceso total desde cualquier lugar (por ejemplo, empleados a tiempo completo): estos usuarios tendrán acceso total a Internet y a la red interna, y pasarán a través de un firewall desde la VPC a la red local.
- Trabajadores que solo deberían tener acceso restringido desde dentro de la red corporativa (por ejemplo, contratistas y consultores): estos usuarios han restringido el acceso a Internet a través de un servidor proxy a sitios web específicos de la VPC y tendrán acceso limitado a la red en la VPC y a la red local.

Le gustaría ofrecer a los empleados a tiempo completo la posibilidad de tener acceso de administrador local WorkSpace para instalar el software, y le gustaría aplicar la autenticación de dos factores con MFA. También quieres permitir que los empleados a tiempo completo accedan a Internet sin restricciones por parte de sus empleados. WorkSpace

En el caso de los contratistas, es mejor bloquear el acceso de los administradores locales para que solo puedan utilizar determinadas aplicaciones preinstaladas. Para ello WorkSpaces, desea aplicar controles restrictivos de acceso a la red mediante grupos de seguridad. Debe abrir los puertos 80 y 443 únicamente para acceder a sitios web internos específicos y desea bloquear por completo su acceso a Internet.

En este escenario, hay dos tipos de usuarios completamente diferentes con requisitos diferentes de acceso a la red y al escritorio. Se recomienda administrarlos y configurarlos de WorkSpaces forma diferente. Deberá crear dos conectores AD, uno para cada persona de usuario. Cada AD Connector requiere dos subredes que tengan suficientes direcciones IP disponibles para cumplir con sus estimaciones de crecimiento WorkSpaces de uso.

> **Note**
>
> Cada subred de AWS VPC consume cinco direcciones IP (las cuatro primeras y la última dirección IP) con fines de administración, y cada AD Connector consume una dirección IP en cada subred en la que persiste.

Otras consideraciones para este escenario son las siguientes:

- AWS Las subredes de VPC deben ser subredes privadas, de modo que el tráfico, como el acceso a Internet, pueda controlarse mediante una puerta de enlace de traducción de direcciones de red (NAT), un servidor proxy-NAT en la nube o enrutarse a través del sistema de administración de tráfico local.
- Hay un firewall para todo el tráfico de VPC destinado a la red local.
- El servidor AD de Microsoft y los servidores RADIUS de MFA son locales (consulte el Escenario 1: Uso del conector AD para la autenticación mediante proxy para AD DS local en este documento) o forman parte de la implementación en la AWS nube (consulte el Escenario 2 y el Escenario 3, Escenarios de implementación de AD DS, en este documento).

Dado que a todos WorkSpaces se les concede algún tipo de acceso a Internet y que están alojados en una subred privada, también debe crear subredes públicas que puedan acceder a Internet a través de una puerta de enlace a Internet. Necesita una puerta de enlace NAT para los empleados a tiempo completo, que les permita acceder a Internet, y un servidor proxy NAT para los consultores y contratistas, a fin de limitar su acceso a sitios web internos específicos. Para evitar fallos, diseñar para una alta disponibilidad y limitar las tarifas de tráfico entre zonas de disponibilidad, debería

disponer de dos puertas de enlace NAT y servidores NAT o proxy en dos subredes diferentes en una implementación con varias zonas de disponibilidad. Las dos AZ que seleccione como subredes públicas coincidirán con las dos AZ que utilice para sus WorkSpaces subredes, en regiones que tengan más de dos zonas. Puede enrutar todo el tráfico de cada zona de disponibilidad WorkSpaces a la subred pública correspondiente para limitar los cargos por tráfico entre zonas de disponibilidad y facilitar la administración. En la siguiente figura se muestra la configuración de la VPC.

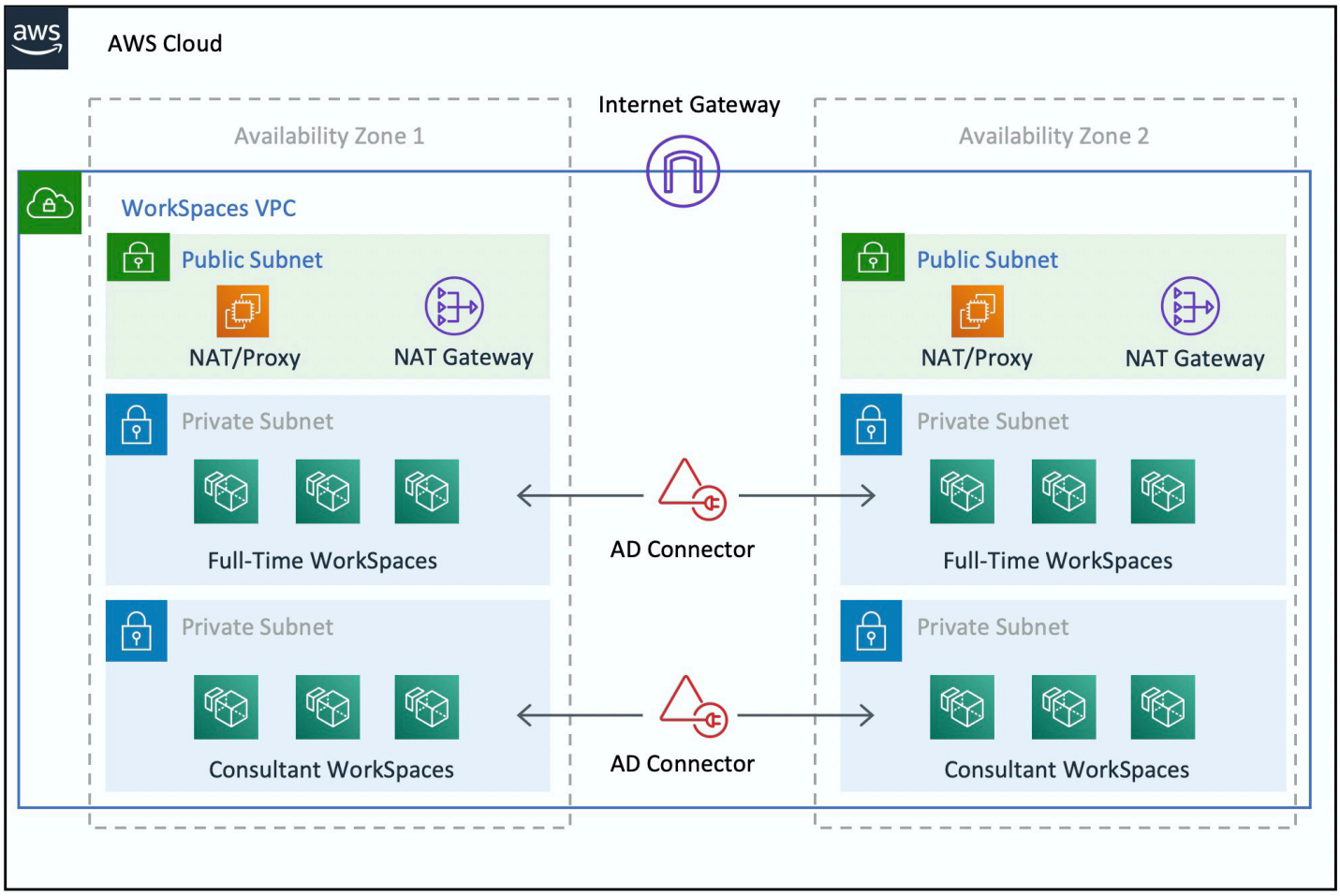

Figura 3: Diseño de VPC de alto nivel

La siguiente información describe cómo configurar los dos WorkSpaces tipos diferentes:

Para configurarlo WorkSpaces para empleados a tiempo completo:

1. En Amazon WorkSpaces Management Console, selecciona la opción Directorios en la barra de menús.
2. Elija el directorio que aloja a sus empleados a tiempo completo.
3. Elija la configuración de administrador local.

Al activar esta opción, cualquier persona recién creada WorkSpace tendrá privilegios de administrador local. Para conceder acceso a Internet, configure la NAT para el acceso saliente a Internet desde su VPC. Para habilitar la MFA, debe especificar un servidor RADIUS, direcciones IP de servidor, puertos y una clave previamente compartida.

Para los empleados a tiempo completo WorkSpaces, el tráfico entrante al Protocolo de Escritorio Remoto (RDP) desde la subred del Helpdesk WorkSpace puede limitarse al Protocolo de Escritorio Remoto (RDP) mediante la aplicación de un grupo de seguridad predeterminado a través de la configuración del AD Connector.

Para configurarlo para contratistas y consultores WorkSpaces :

1. En Amazon WorkSpaces Management Console, deshabilite el acceso a Internet y la configuración de administrador local.
2. Añada un grupo de seguridad en la sección de configuración del grupo de seguridad para aplicar un grupo de seguridad a todos los nuevos que WorkSpaces se creen en ese directorio.

En el caso de los consultores WorkSpaces, limite el tráfico entrante y saliente al aplicando un grupo de seguridad predeterminado WorkSpaces mediante la configuración del Conector AD a todos los WorkSpaces asociados al Conector AD. El grupo de seguridad impide el acceso saliente desde cualquier lugar que no sea el WorkSpaces tráfico HTTP y HTTPS, así como el tráfico entrante a RDP desde la subred del Helpdesk de la red local.

> **Note**
>
> El grupo de seguridad solo se aplica al ENI que se encuentra en la VPC (`eth1`en la WorkSpace) y el acceso al mismo WorkSpace desde el WorkSpaces cliente no está restringido como resultado de un grupo de seguridad. En la siguiente figura se muestra el diseño final de la WorkSpaces VPC.

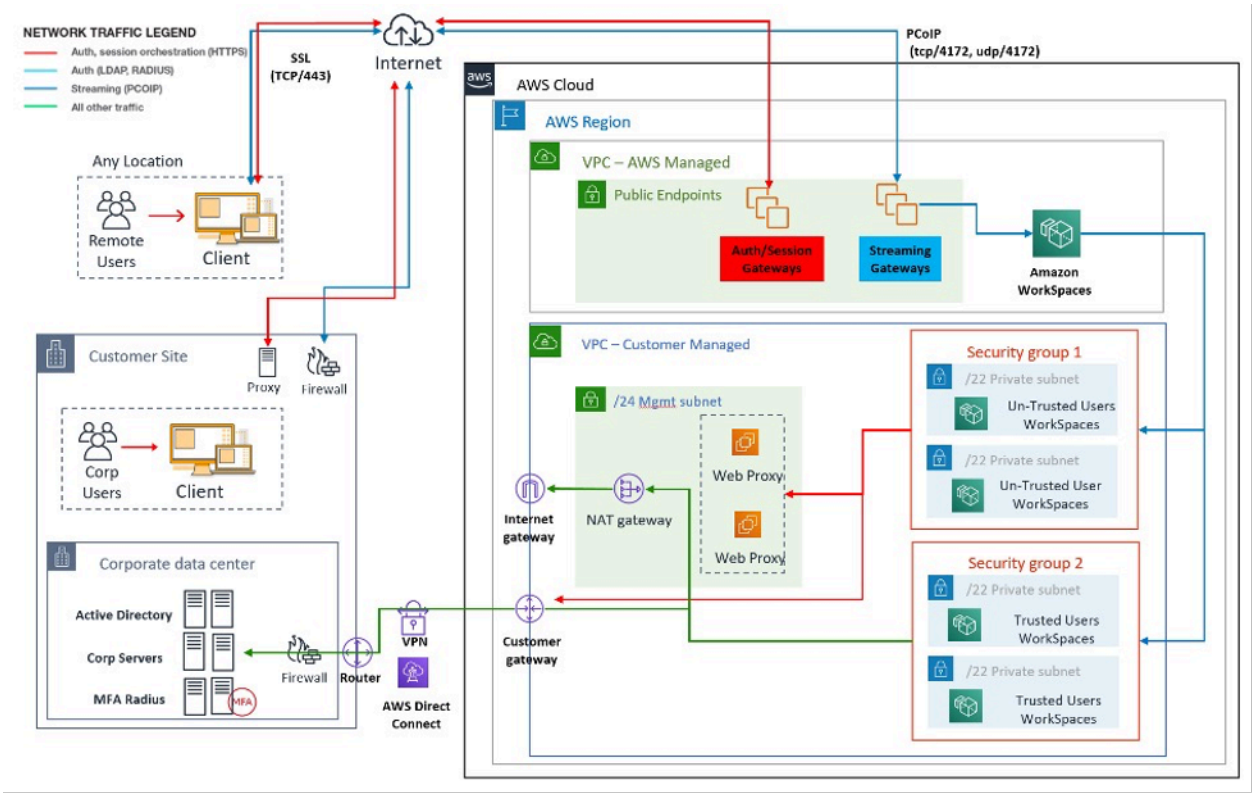

Figura 4: WorkSpaces diseño con personas de usuario

AWS Directory Service

Como se mencionó en la introducción, AWS Directory Service es un componente fundamental de Amazon WorkSpaces. Con AWS Directory Service, puede crear tres tipos de directorios con Amazon WorkSpaces:

- AWS Managed Microsoft AD es un Microsoft AD administrado, con tecnología Windows Server 2012 R2. AWS Managed Microsoft AD está disponible en las ediciones Standard o Enterprise.
- Simple AD es un servicio de directorio gestionado independiente, compatible con Microsoft AD y con tecnología Samba 4.
- AD Connector es un proxy de directorio para redirigir las solicitudes de autenticación y las búsquedas de usuarios o grupos a su Microsoft AD local existente.

En la siguiente sección se describen los flujos de comunicación para la autenticación entre el servicio de WorkSpaces corretaje de Amazon y AWS Directory Service, las prácticas recomendadas para la implementación WorkSpaces con AWS Directory Service y los conceptos avanzados, como el MFA. También analiza los conceptos de arquitectura de infraestructura para Amazon WorkSpaces a

escala, los requisitos de Amazon VPC y AWS Directory Service, incluida la integración con Microsoft AD Domain Services (AD DS) locales.

Escenarios de implementación de AD DS

El respaldo de Amazon WorkSpaces es el AWS Directory Service, y el diseño e implementación adecuados del servicio de directorio son fundamentales. Los seis escenarios siguientes se basan en los servicios de dominio de Active Directory de la guía de inicio AWS rápido y describen las mejores prácticas para las opciones de implementación de AD DS cuando se usa con Amazon WorkSpaces. La sección Consideraciones de diseño de este documento detalla los requisitos específicos y las mejores prácticas para usar AD Connector for WorkSpaces, que es una parte integral del concepto de WorkSpaces diseño general.

- Escenario 1: Uso de AD Connector como proxy de la autenticación en AD DS local: en este escenario, la conectividad de red (VPN/Direct Connect) está instalada con el cliente y toda la autenticación se envía mediante proxy mediante AWS Directory Service (AD Connector) al AD DS local del cliente.
- Escenario 2: Ampliar AD DS local a AWS (réplica): este escenario es similar al escenario 1, pero aquí se implementa una réplica del AD DS del cliente AWS en combinación con AD Connector, lo que reduce la latencia de las solicitudes de autenticación/consulta a AD DS y al catálogo global de AD DS.
- Escenario 3: Despliegue aislado independiente mediante AWS Directory Service en la AWS nube: se trata de un escenario aislado y no incluye la conectividad con el cliente para la autenticación. Este enfoque utiliza AWS Directory Service (Microsoft AD) y AD Connector. Si bien este escenario no depende de la conectividad con el cliente para la autenticación, sí prevé el tráfico de aplicaciones cuando sea necesario a través de VPN o Direct Connect.
- Escenario 4: AWS Microsoft AD y una confianza transitiva bidireccional hacia el entorno local: este escenario incluye el servicio gestionado de AWS Microsoft AD (MAD) con una confianza transitiva bidireccional hacia el bosque de Microsoft AD local.
- Escenario 5: AWS Microsoft AD usa una VPC de Shared Services: este escenario usa AWS Microsoft AD administrado en una VPC de Shared Services para usarlo como dominio de identidad para varios servicios (AWS Amazon EC2, Amazon WorkSpaces, etc.) mientras se usa el AD Connector para enviar por proxy las solicitudes de autenticación de usuarios del Protocolo ligero de acceso a directorios (LDAP) a los controladores de dominio de AD.
- Escenario 6: AWS Microsoft AD, VPC de Shared Services y confianza unidireccional para AD local: este escenario es similar al escenario 5, pero incluye dominios de identidad y recursos dispares que utilizan una confianza unidireccional para el entorno local.

Debe tener en cuenta varias consideraciones al seleccionar el escenario de implementación de los Servicios de dominio de Active Directory (ADDS). En esta sección se explica la función del AD Connector en Amazon WorkSpaces y se abordan algunas consideraciones importantes a la hora de seleccionar un escenario de despliegue de ADDS. Para obtener más información sobre el diseño y la planificación de ADDS on AWS, consulte la Guía de AWS diseño y planificación de los servicios de dominio de Active Directory.

El papel del AWS AD Connector en Amazon WorkSpaces

El AWS AD Connector es un AWS Directory Service que actúa como un servicio proxy para un Active Directory. No almacena ni almacena en caché ninguna credencial de usuario, sino que reenvía las solicitudes de autenticación o búsqueda a Active Directory, ya sea local o local. AWS A menos que lo utilices AWS Managed Microsoft AD, también es la única forma de registrar tu Active Directory (local o ampliado AWS) para usarlo con Amazon WorkSpaces (WorkSpaces).

Un AD Connector puede apuntar a su Active Directory local, a un Active Directory extendido a AWS (controladores de dominio de AD en Amazon EC2) o a un. AWS Managed Microsoft AD

El AD Connector desempeña un papel importante en la mayoría de los escenarios de implementación que se describen en las siguientes secciones. El uso del AD Connector con WorkSpaces ofrece una serie de ventajas:

- Cuando apunta a su Active Directory corporativo, permite a los usuarios usar sus credenciales corporativas existentes para iniciar sesión en WorkSpaces y otros servicios, como Amazon WorkDocs.
- Puede aplicar de forma coherente las políticas de seguridad existentes (caducidad de contraseñas, bloqueos de cuentas, etc.) tanto si sus usuarios acceden a los recursos de su infraestructura local como si están en ella Nube de AWS, por ejemplo. WorkSpaces
- El AD Connector permite una integración sencilla con su infraestructura de MFA basada en RADIUS existente para proporcionar una capa adicional de seguridad.
- Permite la segregación de los usuarios. Por ejemplo, permite configurar varias WorkSpaces opciones por unidad de negocio o persona, ya que varios conectores AD pueden apuntar a los mismos controladores de dominio (servidores DNS) de Active Directory para la autenticación de los usuarios:
  - Dominio o unidad organizativa de destino para la aplicación específica de los objetos de política de grupo (GPO) de Active Directory

- Diferentes grupos de seguridad para controlar el flujo de tráfico hacia/desde WorkSpaces
- Diferentes opciones de control de acceso (dispositivos cliente permitidos) y grupos de control de acceso IP (limitan el acceso a los rangos de IP)
- Habilitación selectiva de los permisos de administrador local
- Diferentes permisos de autoservicio
- Aplicación selectiva de la autenticación multifactor (MFA)
- Colocación de las interfaces de red WorkSpaces elásticas (ENI) en diferentes VPC o subredes para aislarlas

Los conectores AD múltiples también permiten admitir una mayor cantidad de usuarios, si está alcanzando el límite de rendimiento de un solo conector AD pequeño o grande. Consulte la Dimensionamiento de AWS Managed Microsoft AD sección para obtener más información.

El uso de AD Connector con WorkSpaces es gratuito, siempre que tenga al menos un WorkSpaces usuario activo en un AD Connector pequeño y al menos 100 WorkSpaces usuarios activos en un AD Connector grande. Para obtener más información, consulta la página de precios de los servicios de AWS directorio.

La importancia de conectar su red AWS con un Active Directory local

WorkSpaces se basa en la conectividad con su Active Directory. Por lo tanto, la disponibilidad del enlace de red a su Active Directory es de suma importancia. Por ejemplo, si su enlace de red en el escenario 1 está inactivo, los usuarios no podrán autenticarse y, en consecuencia, no podrán usar el suyo WorkSpaces.

Si se va a utilizar un Active Directory local como parte del escenario, tendrá que tener en cuenta la resistencia, la latencia y el coste del tráfico de su enlace de red. AWS En una WorkSpaces implementación multirregional, esto puede implicar varios enlaces de red en diferentes AWS regiones o varios AWS Transit Gateway s con el emparejamiento establecido entre ellos para enrutar el tráfico de AD a la VPC con conectividad a su AD local. Estas consideraciones sobre los enlaces de red se aplican a la mayoría de los escenarios descritos en las siguientes secciones, pero son especialmente importantes en aquellos casos en los que el tráfico de AD procedente de los conectores de AD WorkSpaces necesita atravesar el enlace de red para llegar a tu Active Directory local. El escenario 1 destaca algunas de las advertencias.

Uso de la autenticación multifactor con WorkSpaces

Si planea usar la Autenticación Multi-Factor (MFA) WorkSpaces con, debe usar un AD AWS Connector o AWS Managed Microsoft AD un, ya que solo estos servicios permiten el registro del directorio para su uso WorkSpaces con RADIUS y su configuración. Para la ubicación de los servidores RADIUS, se aplican las consideraciones sobre los enlaces de red que se describen en la La importancia de conectar su red AWS con un Active Directory local sección.

Separar la cuenta y el dominio de recursos

Por motivos de seguridad o para mejorar la capacidad de administración, podría ser conveniente separar el dominio de la cuenta del dominio de los recursos. Por ejemplo, coloque los objetos WorkSpaces informáticos en un dominio de recursos independiente, mientras que los usuarios formen parte del dominio de la cuenta. Una implementación como esta se puede utilizar para permitir que una organización asociada administre el WorkSpaces uso de las políticas de grupo de AD en el dominio de recursos, sin ceder el control ni conceder acceso al dominio de la cuenta. Esto se puede lograr mediante el uso de dos Active Directory con una confianza de Active Directory configurada. En las siguientes secciones se describe este tema con más detalle:

- Escenario 4: AWS Microsoft AD y una confianza transitiva bidireccional hacia el entorno local
- Escenario 6: AWS Microsoft AD, VPC de servicios compartidos y confianza unidireccional con el entorno local

Implementaciones de Active Directory de gran tamaño

Debe asegurarse de que los sitios y servicios de Active Directory estén configurados en consecuencia. Esto es especialmente importante si su Active Directory consta de una gran cantidad de controladores de dominio en diferentes ubicaciones geográficas. Sus Windows WorkSpaces utilizan el mecanismo estándar de Microsoft para detectar su controlador de dominio para el sitio de Active Directory al que están asignados. Este proceso de DC Locator se basa en el DNS y puede prolongarse considerablemente en caso de que se devuelva una larga lista de controladores de dominio con una prioridad y un peso inespecíficos en la fase inicial del proceso de DC Locator. Y lo que es más importante, si WorkSpaces se queda «anclado» a un controlador de dominio que no sea el óptimo, todas las comunicaciones posteriores con este controlador de dominio pueden verse afectadas por un aumento de la latencia de la red y una reducción del ancho de banda al atravesar enlaces de red de área amplia. Esto ralentizará cualquier comunicación con el controlador de dominio, incluido el procesamiento de un número potencialmente elevado de objetos

de política de grupo (GPO) y las transferencias de archivos desde el controlador de dominio. Según la topología de la red, también puede aumentar el costo de la red, ya que los datos intercambiados entre los controladores de dominio WorkSpaces y los controladores de dominio podrían atravesar innecesariamente una ruta de red más costosa. Consulte Consideraciones sobre el diseño las secciones Diseño de VPC y para obtener información sobre DHCP y DNS con el diseño de la VPC y los sitios y servicios de Active Directory.

Uso de Microsoft Azure Active Directory o Active Directory Domain Services con WorkSpaces

Si piensa usar Microsoft Azure Active Directory con WorkSpaces, puede usar Azure AD Connect para sincronizar su identidad con su Active Directory local o con su Active Directory activado AWS (controlador de dominio en Amazon AWS Managed Microsoft AD EC2 o). Sin embargo, esto no le permitirá unirse WorkSpaces a su Azure Active Directory. Para obtener más información, consulte la documentación de Microsoft Hybrid Identity en la documentación de Microsoft Azure.

Si desea unirlo WorkSpaces a su Azure Active Directory, necesitará implementar los servicios de dominio de Microsoft Azure Active Directory (Azure AD DS), establecer la conectividad entre Azure AWS y Azure y usar un conector AWS AD que apunte a los controladores de dominio de Azure AD DS. Para obtener más información sobre cómo configurarlo, consulte la entrada del blog Agregar su WorkSpaces dispositivo a Azure AD mediante los servicios de dominio de Azure Active Directory.

Cuando AWS Directory Service utilices s with WorkSpaces, tendrás que tener en cuenta el tamaño de la WorkSpaces implementación y el crecimiento esperado para poder dimensionarla AWS Directory Service adecuadamente. En esta sección se proporcionan instrucciones sobre cómo dimensionar el dispositivo AWS Directory Service para usarlo con WorkSpaces. También le recomendamos que consulte las AWS Managed Microsoft AD secciones Prácticas recomendadas para AD Connector y Prácticas recomendadas de la Guía de AWS Directory Service administración.

Dimensionamiento del conector AD con WorkSpaces

El conector de Active Directory (conector AD) está disponible en dos tamaños, pequeño y grande. Si bien no se imponen límites de usuario o conexión, recomendamos utilizar un AD Connector pequeño para un máximo de 500 usuarios WorkSpaces autorizados y un conector AD grande para un máximo de 5000 usuarios WorkSpaces autorizados. Puede distribuir las cargas de aplicaciones en varios conectores AD Connector para adaptarlas a sus necesidades de rendimiento. Por ejemplo, si necesita dar soporte a 1500 WorkSpaces usuarios, puede distribuirlo WorkSpaces equitativamente entre tres AD Connector pequeños, cada uno de los cuales admite 500 usuarios. Si todos los

usuarios residen en el mismo dominio, todos los AD Connector pueden apuntar al mismo conjunto de servidores DNS que resuelven su dominio de Active Directory.

Tenga en cuenta que si comenzó con un conector AD pequeño y su WorkSpaces implementación crece con el tiempo, puede solicitar un ticket de soporte para cambiar el tamaño de su AD Connector de pequeño a grande para poder gestionar la mayor cantidad de usuarios WorkSpaces autorizados.

Dimensionamiento de AWS Managed Microsoft AD

AWS Managed Microsoft ADle permite ejecutar Microsoft Active Directory como un servicio gestionado. Puede elegir entre la Edición Estándar y la Edición Empresarial al lanzar el servicio. La edición estándar se recomienda para pequeñas y medianas empresas con un máximo de 5000 usuarios y admite hasta unos 30 000 objetos de directorio, como usuarios, grupos y ordenadores. La edición Enterprise está diseñada para admitir hasta 500 000 objetos de directorio y también ofrece una función adicional, como la replicación multirregional.

Si necesita admitir más de 500 000 objetos de directorio, considere la posibilidad de implementar controladores de dominio de Microsoft Active Directory en Amazon EC2. Para conocer el tamaño de estos controladores de dominio, consulte el documento de Microsoft sobre la planificación de la capacidad para los servicios de dominio de Active Directory.

Escenario 1: Uso del conector AD para la autenticación mediante proxy en Active Directory Service local

Este escenario es para los clientes que no desean extender su servicio de AD local a AD DS o para los que una nueva implementación de AD DS no es una opción. AWS La siguiente figura muestra, en un nivel superior, cada uno de los componentes y el flujo de autenticación de los usuarios.

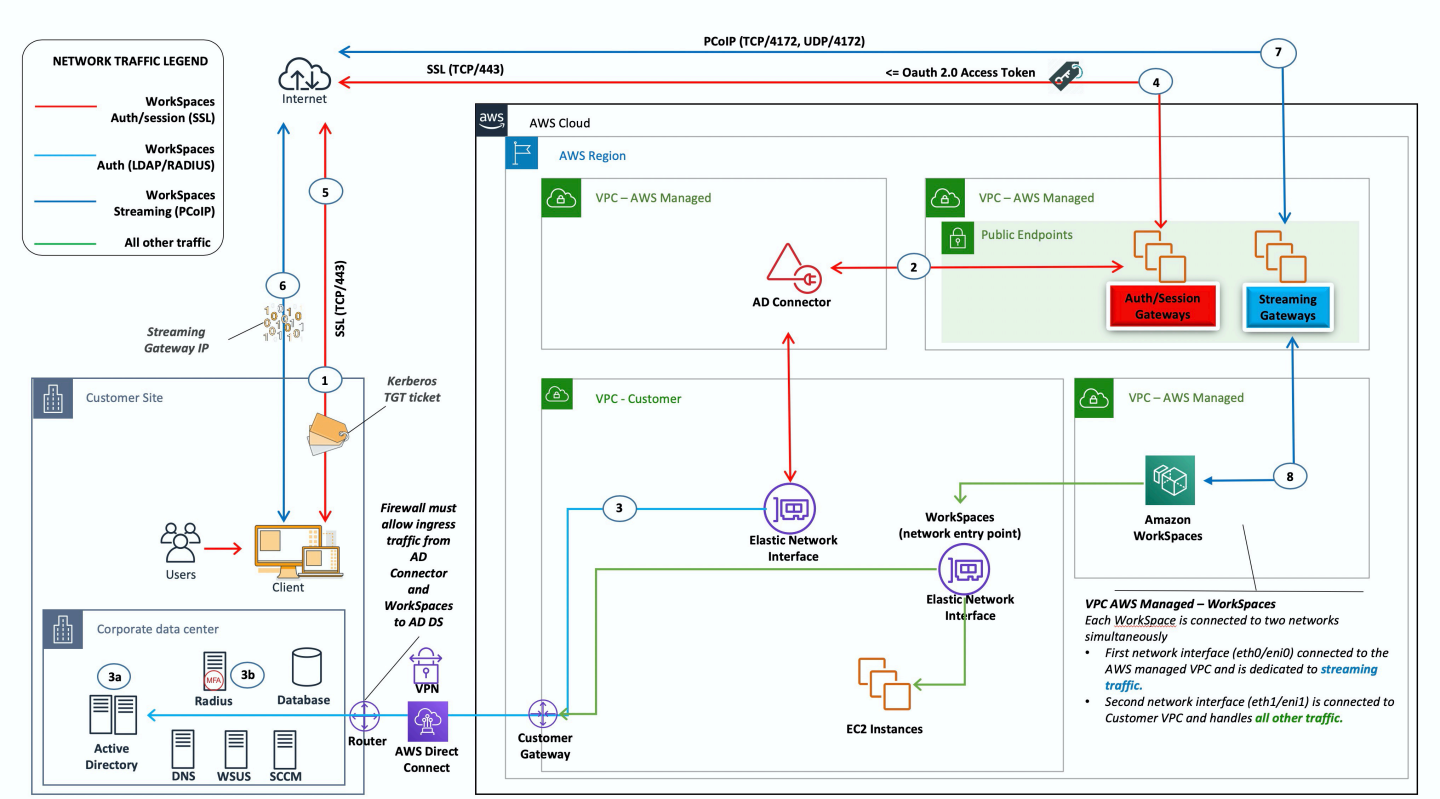

Figura 5: Conector AD para Active Directory local

En este escenario, AWS Directory Service (AD Connector) se utiliza para todas las autenticaciones de usuario o MFA que se envían mediante proxy a través del AD Connector al AD DS local del cliente (se detalla en la siguiente figura). Para obtener más información sobre los protocolos o el cifrado utilizados en el proceso de autenticación, consulte la Seguridad sección de este documento.

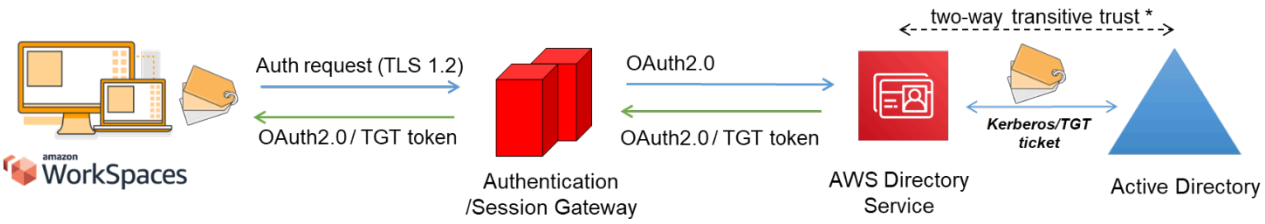

Figura 6: Autenticación de usuarios mediante la pasarela de autenticación

El escenario 1 muestra una arquitectura híbrida en la que es posible que el cliente ya tenga recursos AWS, así como recursos en un centro de datos local al que se puede acceder a través de Amazon WorkSpaces. El cliente puede aprovechar sus servidores AD DS y RADIUS locales existentes para la autenticación de usuarios y MFA.

Esta arquitectura utiliza los siguientes componentes o estructuras:

AWS

- Amazon VPC: creación de una Amazon VPC con al menos dos subredes privadas en dos zonas de disponibilidad.
- Conjunto de opciones de DHCP: creación de un conjunto de opciones de DHCP de Amazon VPC. Esto permite definir el nombre de dominio especificado por el cliente y los servidores de nombres de dominio (DNS) (servicios locales). Para obtener más información, consulte los conjuntos de opciones de DHCP.
- Amazon Virtual Private Gateway: habilita la comunicación con tu propia red a través de un túnel VPN IPsec o una AWS Direct Connect conexión.
- AWS Directory Service: AD Connector se implementa en un par de subredes privadas de Amazon VPC.
- Amazon WorkSpaces: WorkSpaces se implementan en las mismas subredes privadas que el AD Connector. Para obtener más información, consulte la sección Active Directory: sitios y servicios de este documento.

Cliente

- Conectividad de red: puntos finales VPN corporativos o Direct Connect.
- AD DS: AD DS corporativo.
- MFA (opcional): servidor RADIUS corporativo.
- Dispositivos de usuario final: dispositivos de usuario final corporativos o con licencia propia (BYOL) (como Windows, Mac, iPads, tabletas Android, cero clientes y Chromebooks) que se utilizan para acceder al servicio de Amazon. WorkSpaces Consulte esta lista de aplicaciones cliente para ver los dispositivos y navegadores web compatibles.

Si bien esta solución es ideal para los clientes que no desean implementar AD DS en la nube, tiene algunas advertencias:

- Confianza en la conectividad: si se pierde la conectividad con el centro de datos, los usuarios no pueden iniciar sesión en sus respectivos WorkSpaces centros de datos y las conexiones existentes permanecerán activas durante toda la vida útil de Kerberos/Ticket-Granting Ticket (TGT).

- Latencia: si existe latencia a través de la conexión (este es más el caso con la VPN que con Direct Connect), la WorkSpaces autenticación y cualquier actividad relacionada con AD DS, como la aplicación de políticas de grupo (GPO), llevarán más tiempo.
- Costes de tráfico: toda la autenticación debe atravesar el enlace VPN o Direct Connect, por lo que depende del tipo de conexión. Se trata de una transferencia de datos de salida de Amazon EC2 a Internet o de una transferencia de datos de salida (Direct Connect).

> **Note**
>
> AD Connector es un servicio de proxy. No almacena ni almacena en caché las credenciales de usuario. En su lugar, su AD gestiona todas las solicitudes de autenticación, búsqueda y administración. Se requiere una cuenta con privilegios de delegación en el servicio de directorio con derechos para leer toda la información del usuario y unir un equipo al dominio.

En general, la WorkSpaces experiencia depende en gran medida del proceso de autenticación de Active Directory que se muestra en la figura anterior. En este escenario, la experiencia de WorkSpaces autenticación depende en gran medida del enlace de red entre el AD del cliente y la WorkSpaces VPC. El cliente debe asegurarse de que el enlace tenga una alta disponibilidad.

Escenario 2: extender AD DS local a AWS (réplica)

Este escenario es similar al escenario 1. Sin embargo, en este escenario, se implementa una réplica del AD DS del cliente AWS en combinación con AD Connector. Esto reduce la latencia de las solicitudes de autenticación o consulta a AD DS que se ejecuta en Amazon Elastic Compute Cloud (Amazon EC2). La siguiente figura muestra una vista de alto nivel de cada uno de los componentes y del flujo de autenticación de los usuarios.

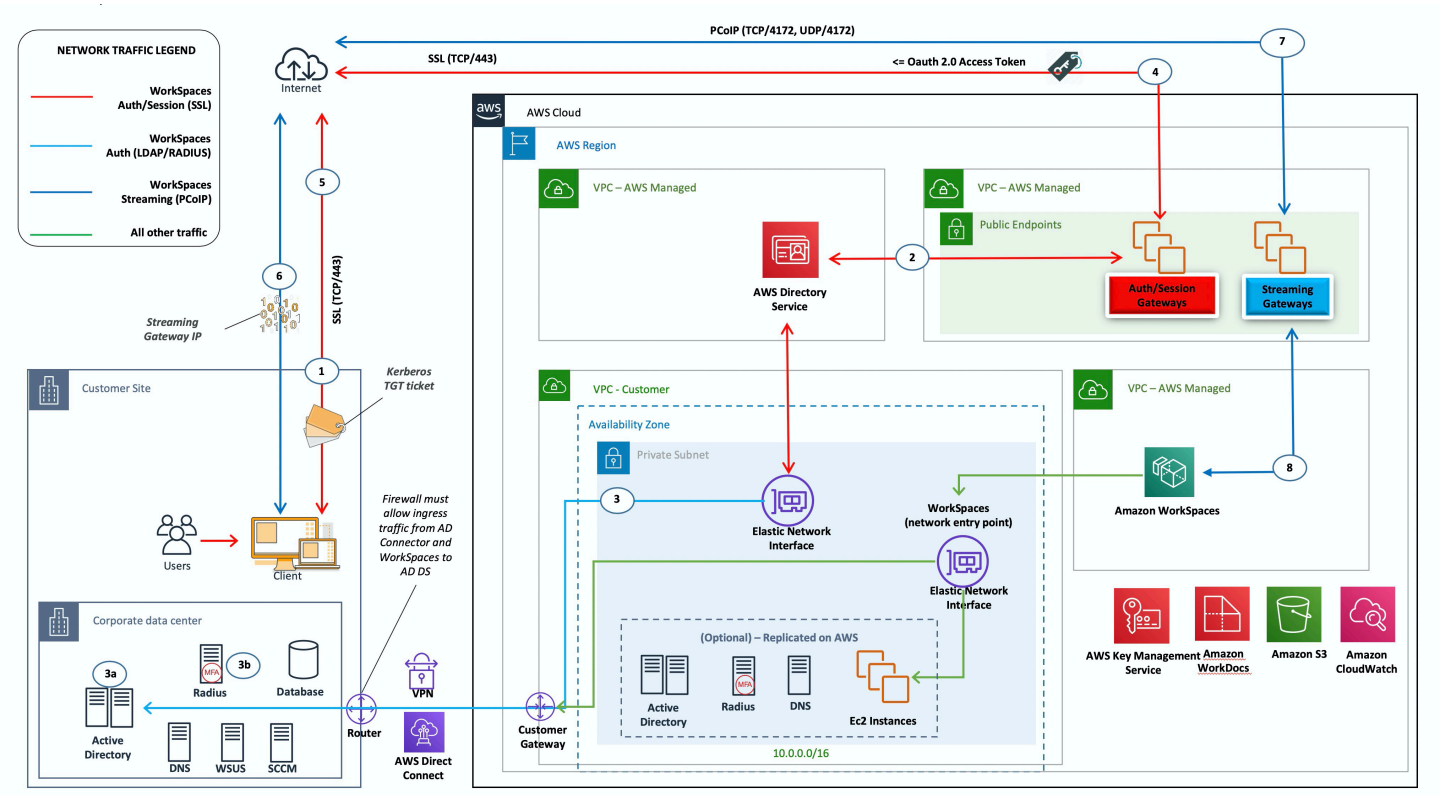

Figura 7: Extienda el dominio de Active Directory del cliente a la nube

Como en el escenario 1, AD Connector se utiliza para todas las autenticaciones de usuario o MFA, que a su vez se envía por proxy al AD DS del cliente (consulte la figura anterior). En este escenario, el AD DS del cliente se implementa en todas las AZ de las instancias de Amazon EC2 que se promocionan como controladores de dominio en el bosque de AD local del cliente, que se ejecuta en la nube. AWS Cada controlador de dominio se implementa en subredes privadas de VPC para que AD DS tenga una alta disponibilidad en la nube. AWS Para conocer las prácticas recomendadas para implementar AD DS en AWS, consulta la sección Consideraciones de diseño de este documento.

Una vez implementadas, las WorkSpaces instancias tienen acceso a los controladores de dominio basados en la nube para ofrecer servicios de directorio y DNS seguros y de baja latencia. Todo el tráfico de red, incluida la comunicación de AD DS, las solicitudes de autenticación y la replicación de AD, está protegido dentro de las subredes privadas o a través del túnel VPN del cliente o Direct Connect.

Esta arquitectura utiliza los siguientes componentes o estructuras:

AWS

- Amazon VPC: creación de una Amazon VPC con al menos cuatro subredes privadas en dos zonas de disponibilidad: dos para el cliente AD DS y dos para AD Connector o Amazon. WorkSpaces
- Conjunto de opciones de DHCP: creación de un conjunto de opciones de DHCP de Amazon VPC. Esto permite al cliente definir un nombre de dominio y un DNS específicos (AD DS local). Para obtener más información, consulte los conjuntos de opciones de DHCP.
- Amazon Virtual Private Gateway: permite la comunicación con una red propiedad del cliente a través de un túnel o conexión VPN IPsec. AWS Direct Connect
- Amazon EC2
  - Controladores de dominio AD DS corporativos del cliente implementados en instancias de Amazon EC2 en subredes de VPC privadas dedicadas.
  - Servidores RADIUS del cliente (opcionales) para MFA en instancias de Amazon EC2 en subredes de VPC privadas dedicadas.
- AWS Servicios de directorio: AD Connector se implementa en un par de subredes privadas de Amazon VPC.
- Amazon WorkSpaces: WorkSpaces se implementan en las mismas subredes privadas que el AD Connector. Para obtener más información, consulte la sección Active Directory: sitios y servicios de este documento.

Cliente

- Conectividad de red: VPN corporativa o AWS Direct Connect puntos finales.
- AD DS: AD DS corporativo (necesario para la replicación).
- MFA (opcional): servidor RADIUS corporativo.
- Dispositivos de usuario final: dispositivos de usuario final corporativos o BYOL (como Windows, Mac, iPads, tabletas Android, cero clientes y Chromebooks) que se utilizan para acceder al servicio de Amazon. WorkSpaces Consulte la lista de aplicaciones cliente para ver los dispositivos y navegadores web compatibles. Esta solución no tiene las mismas advertencias que en el escenario 1. Amazon WorkSpaces y AWS Directory Service no dependen de la conectividad existente.

- Confianza en la conectividad: si se pierde la conectividad con el centro de datos del cliente, los usuarios finales pueden seguir trabajando porque la autenticación y el MFA opcional se procesan localmente.
- Latencia: con la excepción del tráfico de replicación, toda la autenticación es local y de baja latencia. Consulte la sección Active Directory: sitios y servicios de este documento.
- Costos de tráfico: en este escenario, la autenticación es local y solo la replicación de AD DS tiene que atravesar el enlace VPN o Direct Connect, lo que reduce la transferencia de datos.

En general, la WorkSpaces experiencia ha mejorado y no depende en gran medida de la conectividad con los controladores de dominio locales, como se muestra en la figura anterior. Este también es el caso cuando un cliente quiere ampliarse WorkSpaces a miles de escritorios, especialmente en relación con las consultas del catálogo global de AD DS, ya que este tráfico sigue siendo local en el WorkSpaces entorno.

Escenario 3: Implementación aislada e independiente mediante AWS Directory Service en la nube AWS

En este escenario, que se muestra en la siguiente figura, AD DS se implementa en la AWS nube en un entorno aislado e independiente. AWS Directory Service se utiliza exclusivamente en este escenario. En lugar de administrar completamente AD DS, los clientes pueden confiar en AWS Directory Service para tareas como crear una topología de directorios de alta disponibilidad, monitorear los controladores de dominio y configurar copias de seguridad e instantáneas.

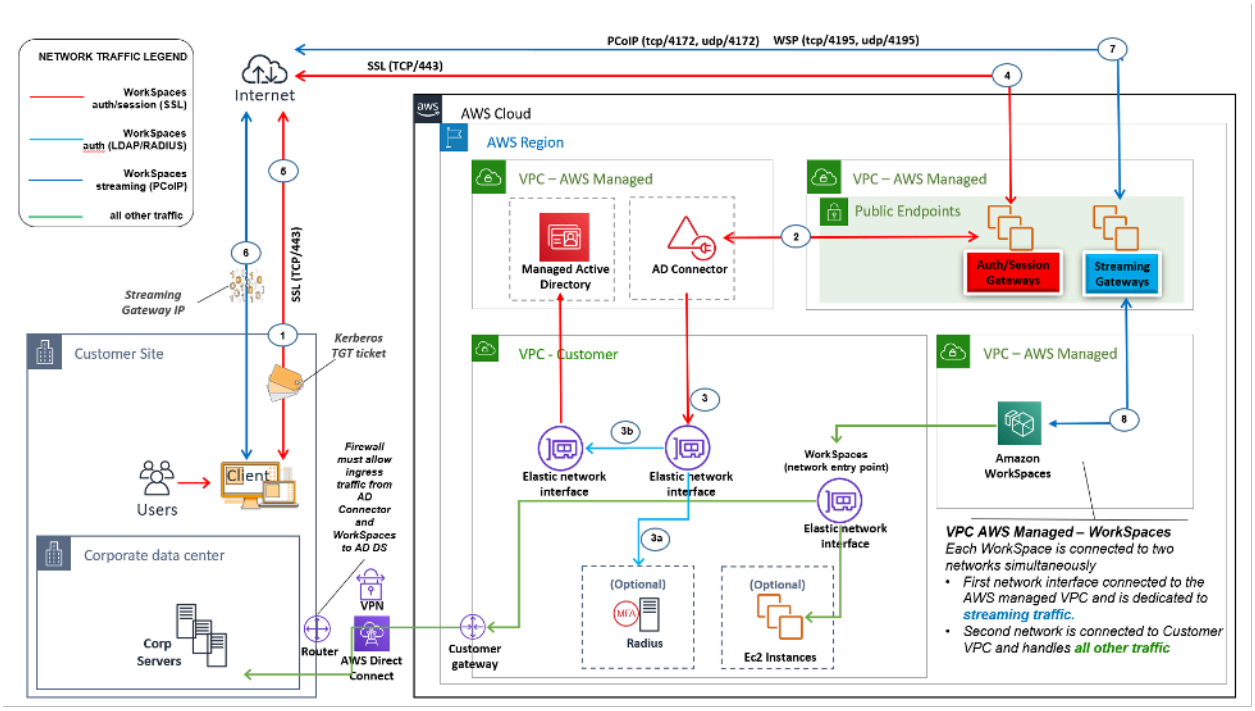

Figura 8: Solo en la nube: servicios de AWS directorio (Microsoft AD)

Como en el escenario 2, el AD DS (Microsoft AD) se implementa en subredes dedicadas que abarcan dos zonas de disponibilidad, lo que hace que AD DS esté altamente disponible en la AWS nube. Además de Microsoft AD, AD Connector (en los tres escenarios) se implementa para la WorkSpaces autenticación o la MFA. Esto garantiza la separación de roles o funciones dentro de Amazon VPC, que es una práctica recomendada estándar. Para obtener más información, consulte la sección Consideraciones de diseño de este documento.

El escenario 3 es una configuración estándar e integral que funciona bien para los clientes que desean AWS gestionar la implementación, los parches, la alta disponibilidad y la supervisión del AWS Directory Service. El escenario también funciona bien para entornos de prueba de concepto y de laboratorio y de producción debido a su modo de aislamiento.

Además de la ubicación de AWS Directory Service, en esta figura se muestra el flujo de tráfico de un usuario a un espacio de trabajo y la forma en que el espacio de trabajo interactúa con el servidor AD y el servidor MFA.

Esta arquitectura utiliza los siguientes componentes o estructuras.

AWS

- Amazon VPC: creación de una Amazon VPC con al menos cuatro subredes privadas en dos zonas de disponibilidad: dos para AD DS Microsoft AD, dos para AD Connector o. WorkSpaces
- Conjunto de opciones de DHCP: creación de un conjunto de opciones de DHCP de Amazon VPC. Esto permite al cliente definir un nombre de dominio y un DNS (Microsoft AD) específicos. Para obtener más información, consulte los conjuntos de opciones de DHCP.
- Opcional: puerta de enlace privada virtual de Amazon: habilita la comunicación con una red propiedad del cliente a través de un túnel VPN (VPN) o una conexión IPSec. AWS Direct Connect Se utiliza para acceder a los sistemas de back-end locales.
- AWS Directory Service: Microsoft AD se implementó en un par dedicado de subredes de VPC (AD DS Managed Service).
- Amazon EC2: servidores RADIUS «opcionales» del cliente para MFA.
- AWS Servicios de directorio: AD Connector se implementa en un par de subredes privadas de Amazon VPC.
- Amazon WorkSpaces: WorkSpaces se implementan en las mismas subredes privadas que el AD Connector. Para obtener más información, consulte la sección Active Directory: sitios y servicios de este documento.

Cliente

- Opcional: conectividad de red: VPN corporativa o AWS Direct Connect puntos finales.
- Dispositivos de usuario final: dispositivos corporativos o BYOL para usuarios finales (como Windows, Mac, iPads, tabletas Android, cero clientes y Chromebooks) que se utilizan para acceder al servicio de Amazon. WorkSpaces Consulte esta lista de aplicaciones cliente para ver los dispositivos y navegadores web compatibles.

Al igual que en el escenario 2, este escenario no presenta problemas relacionados con la conectividad con el centro de datos local del cliente, la latencia o los costos de transferencia de datos salientes (excepto cuando el acceso a Internet está habilitado WorkSpaces dentro de la VPC) porque, por diseño, se trata de un escenario aislado o solo en la nube.

Escenario 4: AWS Microsoft AD y una confianza transitiva bidireccional hacia el entorno local

En este escenario, que se muestra en la siguiente figura, se ha implementado un AD AWS gestionado en la AWS nube, que tiene una confianza transitiva bidireccional hacia el AD local del cliente. Los usuarios y WorkSpaces se crean en el AD gestionado, y la confianza de AD permite acceder a los recursos en el entorno local.

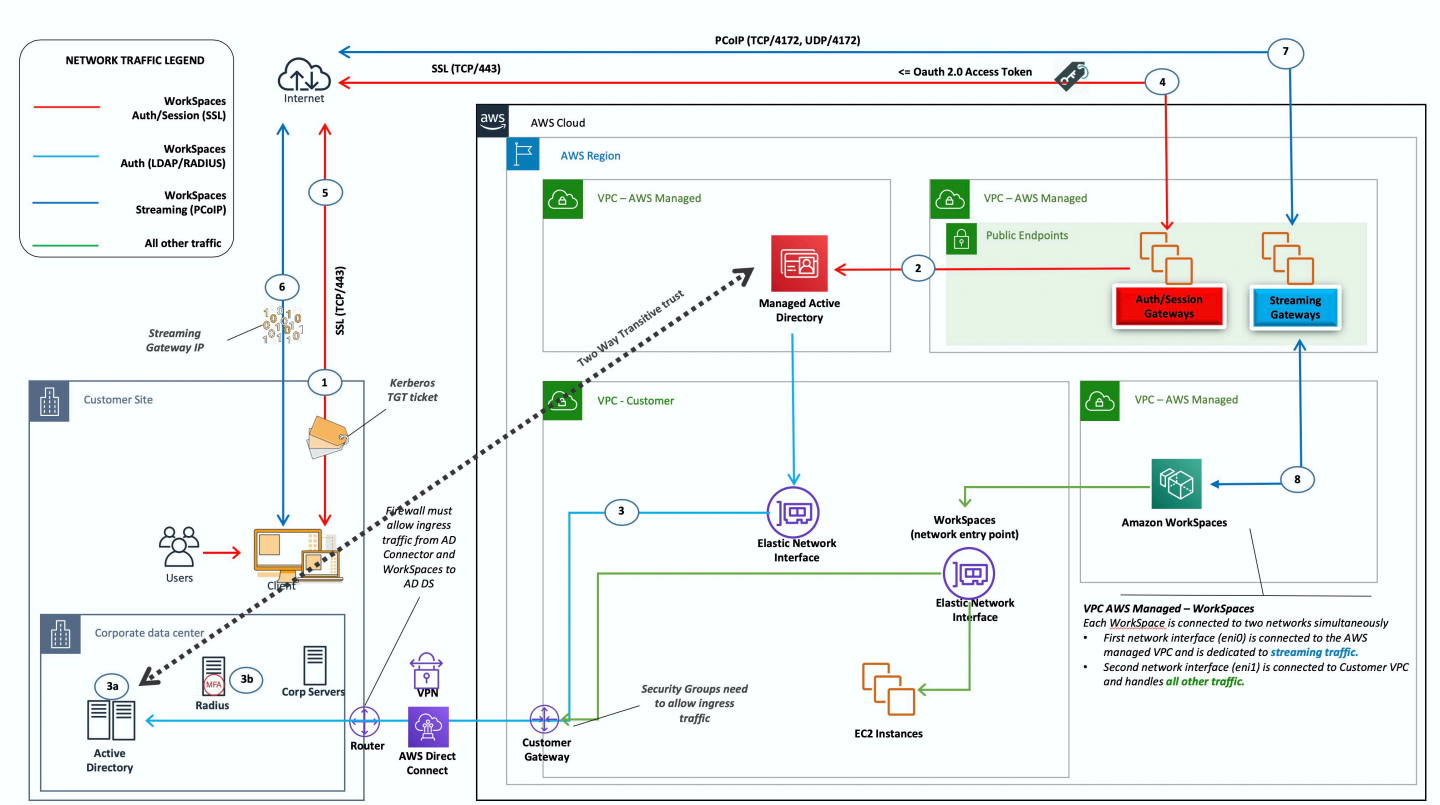

Figura 9: AWS Microsoft AD y una confianza transitiva bidireccional hacia el entorno local

Como en el escenario 3, el AD DS (Microsoft AD) se implementa en subredes dedicadas que abarcan dos zonas de disponibilidad, lo que hace que AD DS tenga una alta disponibilidad en la AWS nube.

Este escenario funciona bien para los clientes que desean tener un AWS Directory Service totalmente gestionado, que incluya la implementación, la aplicación de parches, la alta disponibilidad y la supervisión de su AWS nube. Este escenario también permite a WorkSpaces los usuarios acceder a los recursos unidos a AD en sus redes existentes. Este escenario requiere que exista una confianza de dominio. Los grupos de seguridad y las reglas de firewall deben permitir la comunicación entre los dos directorios activos.

Además de la ubicación de AWS Directory Service, la figura anterior describe el flujo de tráfico de un usuario a un espacio de trabajo y la forma en que el espacio de trabajo interactúa con el servidor AD y el servidor MFA.

Esta arquitectura utiliza los siguientes componentes o componentes.

AWS

- Amazon VPC: creación de una Amazon VPC con al menos cuatro subredes privadas en dos zonas de disponibilidad: dos para AD DS Microsoft AD, dos para AD Connector o. WorkSpaces
- Conjunto de opciones de DHCP: creación de un conjunto de opciones de DHCP de Amazon VPC. Esto permite al cliente definir un nombre de dominio y un DNS (Microsoft AD) específicos. Para obtener más información, consulte los conjuntos de opciones de DHCP.
- Opcional: puerta de enlace privada virtual de Amazon: habilita la comunicación con una red propiedad del cliente a través de un túnel VPN (VPN) o una conexión IPSec. AWS Direct Connect Se utiliza para acceder a los sistemas de back-end locales.
- AWS Directory Service: Microsoft AD se implementó en un par dedicado de subredes de VPC (AD DS Managed Service).

- Amazon EC2: servidores RADIUS opcionales para MFA por parte del cliente.
- Amazon WorkSpaces: WorkSpaces se implementan en las mismas subredes privadas que el AD Connector. Para obtener más información, consulte la sección Active Directory: sitios y servicios de este documento.

Cliente

- Conectividad de red: VPN corporativa o AWS Direct Connect puntos finales.
- Dispositivos de usuario final: dispositivos corporativos o BYOL para usuarios finales (como Windows, Mac, iPads, tabletas Android, cero clientes y Chromebooks) que se utilizan para acceder al servicio de Amazon. WorkSpaces Consulte la lista de aplicaciones cliente para ver los dispositivos y navegadores web compatibles.

Esta solución requiere conectividad con el centro de datos local del cliente para permitir que funcione el proceso de confianza. Si WorkSpaces los usuarios utilizan los recursos de la red local, es necesario tener en cuenta los costes de latencia y de transferencia de datos salientes.

Escenario 5: AWS Microsoft AD utiliza una Nube Privada Virtual (VPC) de servicios compartidos

En este escenario, que se muestra en la siguiente figura, se implementa un AD AWS gestionado en la AWS nube, que proporciona servicios de autenticación para cargas de trabajo que ya están alojadas AWS o que se prevé que formen parte de una migración más amplia. La mejor práctica recomendada es tener Amazon WorkSpaces en una VPC dedicada. Los clientes también deberían crear una unidad organizativa AD específica para organizar los objetos de la WorkSpaces computadora.

Para realizar la implementación WorkSpaces con una VPC de servicios compartidos que aloje un AD gestionado, implemente un AD Connector (ADC) con una cuenta de servicio de ADC creada en el AD gestionado. La cuenta de servicio requiere permisos para crear objetos de ordenador en la OU WorkSpaces designada en el AD gestionado de servicios compartidos.

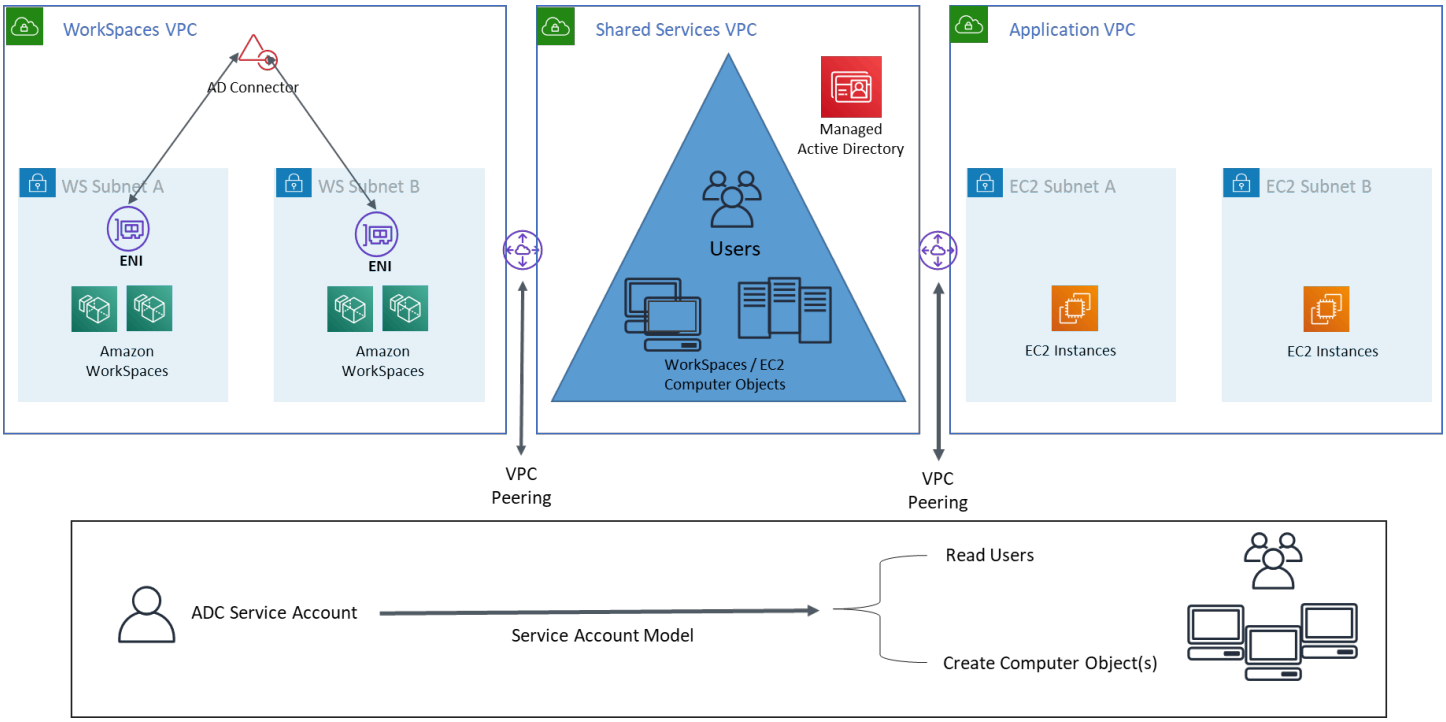

Figura 10: AWS Microsoft AD mediante una VPC de servicios compartidos

Esta arquitectura utiliza los siguientes componentes o construcciones.

AWS

- Amazon VPC: creación de una Amazon VPC con al menos dos subredes privadas en dos zonas de disponibilidad (dos para AD Connector y). WorkSpaces
- Conjunto de opciones de DHCP: creación de un conjunto de opciones de DHCP de Amazon VPC. Esto permite al cliente definir un nombre de dominio y un DNS (Microsoft AD) específicos. Para obtener más información, consulte los conjuntos de opciones de DHCP.
- Opcional: puerta de enlace privada virtual de Amazon: habilita la comunicación con una red propiedad del cliente a través de un túnel VPN (VPN) o una conexión IPSec. AWS Direct Connect Se utiliza para acceder a los sistemas de back-end locales.
- AWS Directory Service: Microsoft AD implementado en un par dedicado de subredes de VPC (AD DS Managed Service), AD Connector
- AWS Emparejamiento de Transit Gateway/VPC: habilite la conectividad entre la VPC de Workspaces y la VPC de Shared Services
- Amazon EC2: servidores RADIUS opcionales para MFA por parte del cliente.
- Amazon WorkSpaces: WorkSpaces se implementan en las mismas subredes privadas que el AD Connector. Para obtener más información, consulte la sección Active Directory: sitios y servicios de este documento.

Cliente

- Conectividad de red: VPN corporativa o AWS Direct Connect puntos finales.
- Dispositivos de usuario final: dispositivos corporativos o BYOL para usuarios finales (como Windows, Mac, iPads, tabletas Android, cero clientes y Chromebooks) que se utilizan para acceder al servicio de Amazon. WorkSpaces Consulte la lista de aplicaciones cliente para ver los dispositivos y navegadores web compatibles.

Escenario 6: AWS Microsoft AD, VPC de servicios compartidos y confianza unidireccional con el entorno local

Este escenario, como se muestra en la siguiente figura, utiliza un Active Directory local existente para los usuarios e introduce un Active Directory administrado independiente en la AWS nube para alojar los objetos informáticos asociados al. WorkSpaces Este escenario permite que los objetos

informáticos y las políticas de grupo de Active Directory se administren de forma independiente del Active Directory corporativo.

Este escenario resulta útil cuando un tercero quiere administrar Windows WorkSpaces en nombre de un cliente, ya que permite que el tercero defina y controle las políticas asociadas a él WorkSpaces y las políticas asociadas a él, sin necesidad de conceder al tercero acceso al AD del cliente. En este escenario, se crea una unidad organizativa (OU) específica de Active Directory para organizar los objetos WorkSpaces informáticos del AD de Shared Services.

> **Note**
>
> Amazon Linux WorkSpaces requiere que exista una confianza bidireccional para poder crearlos.

Para implementar Windows WorkSpaces con los objetos informáticos creados en la VPC de Shared Services que aloja Active Directory administrado con usuarios del dominio de identidad del cliente, implemente un conector de Active Directory (ADC) que haga referencia al AD corporativo. Utilice una cuenta de servicio ADC creada en el AD (dominio de identidad) corporativo que tenga permisos delegados para crear objetos informáticos en la unidad organizativa (OU) que se configuró para Windows WorkSpaces en el AD administrado de Shared Services y que tenga permisos de lectura en el Active Directory corporativo (dominio de identidad).

Para garantizar que la función de localización de dominios pueda autenticar a WorkSpaces los usuarios en el sitio de AD deseado para el dominio de identidad, asigne el mismo nombre a los sitios de AD de ambos dominios para las WorkSpaces subredes de Amazon, tal como se indica en la documentación de Microsoft. Se recomienda tener controladores de dominio AD tanto del dominio de identidad como del dominio de Shared Services en la misma AWS región que Amazon WorkSpaces.

Para obtener instrucciones detalladas sobre cómo configurar este escenario, consulta la guía de implementación para configurar una confianza unidireccional para Amazon WorkSpaces con AWS Directory Services

En este escenario, establecemos una confianza transitiva unidireccional entre la VPC AWS Managed Microsoft AD de Shared Services y el AD local. La figura 11 muestra la dirección de la confianza y el acceso, y cómo AWS AD Connector utiliza la cuenta de servicio AD Connector para crear objetos de equipo en el dominio de recursos.

Según las recomendaciones de Microsoft, se utiliza una confianza forestal para garantizar que se utilice la autenticación Kerberos siempre que sea posible. WorkSpaces Recibirá objetos de política de grupo (GPO) de su dominio de recursos en. AWS Managed Microsoft AD Además, debe WorkSpaces realizar la autenticación Kerberos con su dominio de identidad. Para que esto funcione de forma fiable, se recomienda ampliar el dominio de identidad al que AWS ya se ha explicado anteriormente. Le sugerimos que consulte la guía de implementación de Deploy Amazon WorkSpaces using a One-Way Trust Resource Domain con una guía de AWS Directory Service implementación para obtener más detalles.

Tanto el AD Connector como el WorkSpaces suyo deben poder comunicarse con los controladores de dominio de su dominio de identidad y su dominio de recursos. Para obtener más información, consulta los requisitos de dirección IP y puerto WorkSpaces en la Guía de WorkSpaces administración de Amazon.

Si usa varios conectores AD, se recomienda que cada uno de los conectores AD use su propia cuenta de servicio de AD Connector.

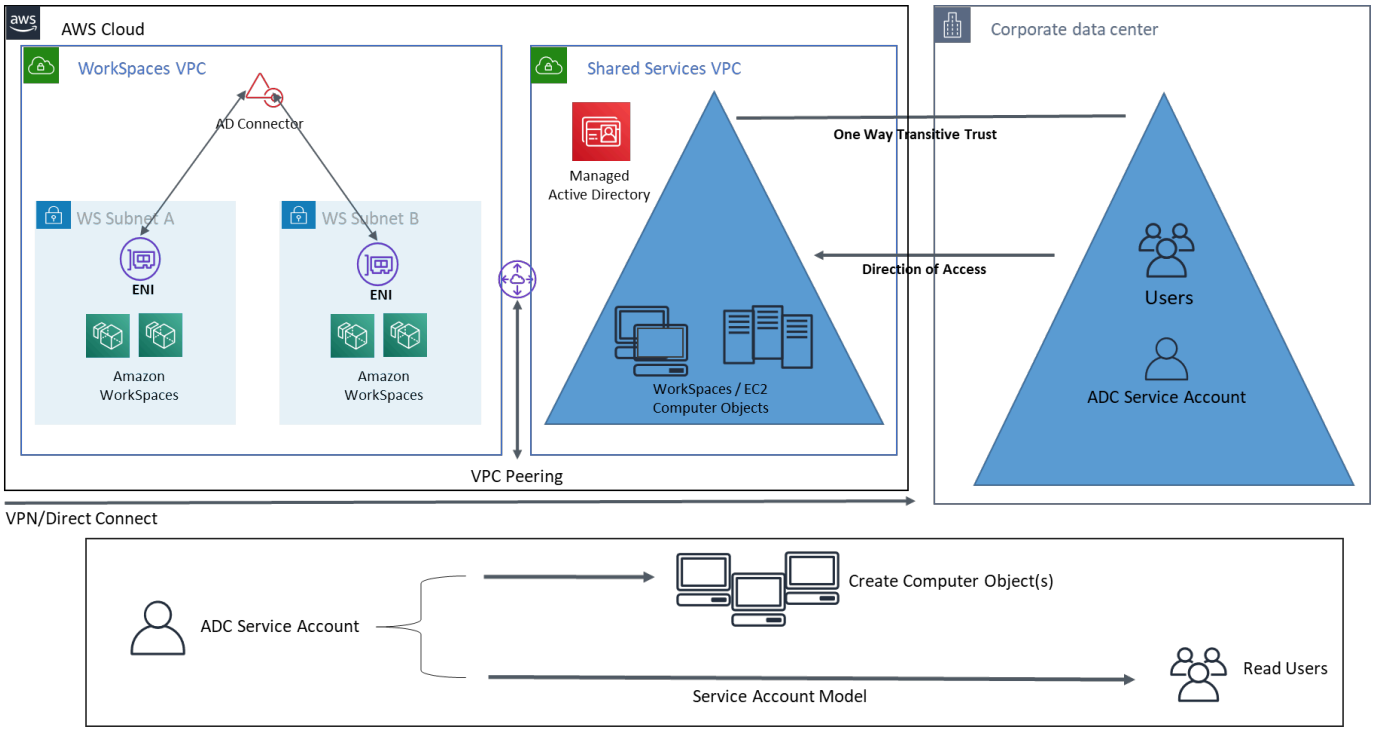

Figura 11: AWS Microsoft, VPC de servicios compartidos y confianza unidireccional con AD local

Esta arquitectura utiliza los siguientes componentes o estructuras:

AWS

- Amazon VPC: creación de una Amazon VPC con al menos dos subredes privadas en dos zonas de disponibilidad (dos para AD Connector y. WorkSpaces
- Conjunto de opciones de DHCP: creación de un conjunto de opciones de DHCP de Amazon VPC. Esto permite al cliente definir un nombre de dominio y un DNS (Microsoft AD) específicos. Para obtener más información, consulte los conjuntos de opciones de DHCP.
- Opcional: puerta de enlace privada virtual de Amazon: habilita la comunicación con una red propiedad del cliente a través de un túnel VPN (VPN) o una conexión IPSec. AWS Direct Connect Se utiliza para acceder a los sistemas de back-end locales.
- AWS Directory Service: Microsoft AD se implementó en un par dedicado de subredes de VPC (AD DS Managed Service), AD Connector.
- Emparejamiento de Transit Gateway/VPC: habilite la conectividad entre la VPC de Workspaces y la VPC de Shared Services.
- Amazon EC2: servidores RADIUS «opcionales» del cliente para MFA.
- Amazon WorkSpaces: WorkSpaces se implementan en las mismas subredes privadas que el AD Connector. Para obtener más información, consulte la sección Active Directory: sitios y servicios de este documento.

Cliente

- Conectividad de red: VPN corporativa o AWS Direct Connect puntos finales.
- Dispositivos de usuario final: dispositivos corporativos o BYOL para usuarios finales (como Windows, Mac, iPads, tabletas Android, cero clientes y Chromebooks) que se utilizan para acceder al servicio de Amazon. WorkSpaces Consulte esta lista de aplicaciones cliente para ver los dispositivos y navegadores web compatibles.

Uso de Active Directory AWS gestionado en varias regiones con Amazon WorkSpaces

AWS Directory Service for Microsoft Active Directory (MAD) es un Active Directory (AD) de Microsoft totalmente gestionado que se puede combinar con Amazon WorkSpaces. Los clientes eligen AWS Managed Microsoft AD porque incorpora alta disponibilidad, supervisión y copias de seguridad. AWS La edición gestionada Microsoft AD Enterprise añade la capacidad de configurar la replicación

multirregional. Esta función configura automáticamente la conectividad de redes entre regiones, implementa controladores de dominio y replica todos los datos de Active Directory en varias regiones, lo que garantiza que las cargas de trabajo de Windows y Linux que residen en esas regiones puedan conectarse a AWS MAD y utilizarla con baja latencia y alto rendimiento. Las regiones MAD replicadas no se pueden registrar directamente; sin embargo WorkSpaces, se puede registrar un directorio MAD replicado WorkSpaces configurando un AD Connector (ADC) para que apunte a los controladores de dominio replicados.

La mejor práctica al implementar AD Connectors con MAD es crear un conector AD para cada unidad de negocio de su WorkSpaces entorno. Esto le permitirá alinear cada unidad de negocio con una unidad organizativa específica dentro de Active Directory. A continuación, puede asignar objetos de política de grupo de AD a nivel de unidad organizativa que se alineen directamente con la unidad de negocio en cuestión.

Arquitectura

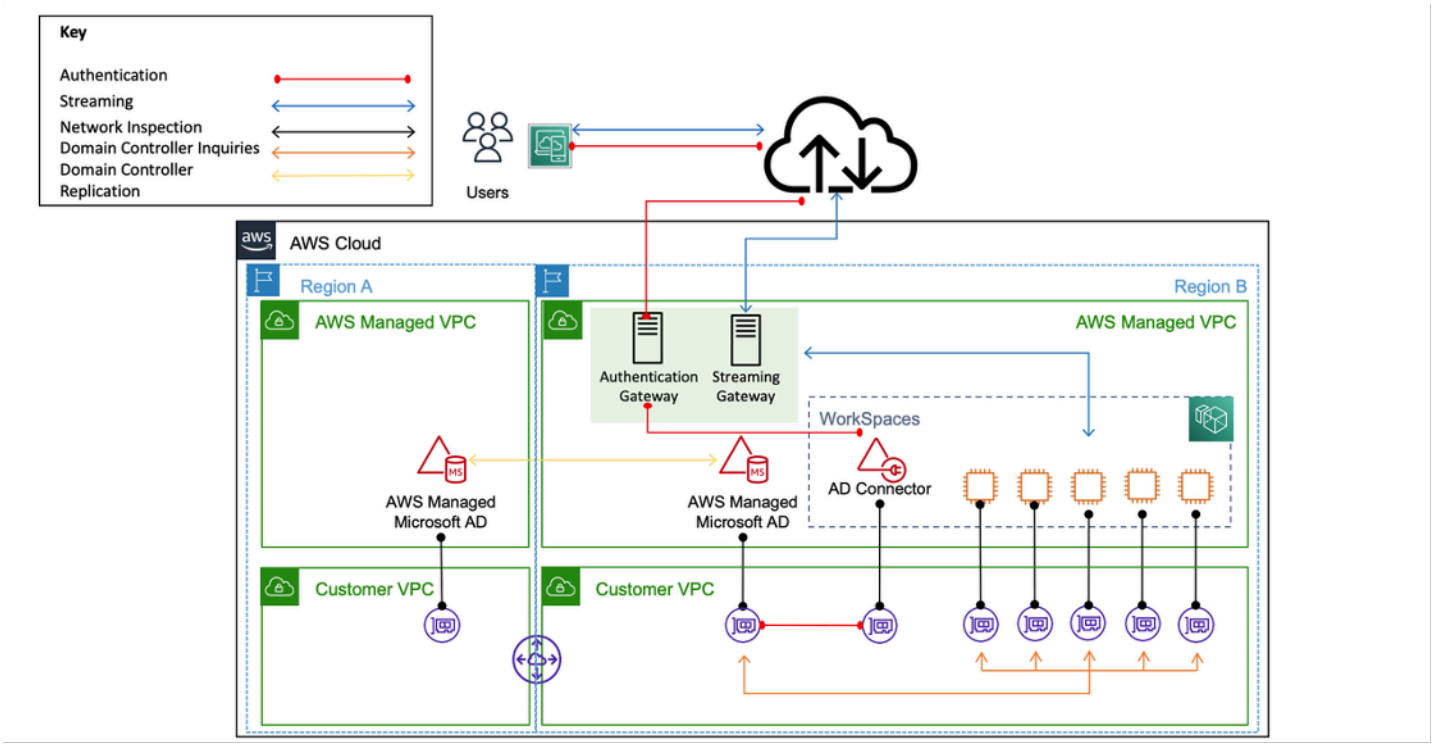

Figura 12: Ejemplo de arquitectura para registrar una región MAD replicada en un WorkSpace

Implementación

Para registrar su región MAD replicada WorkSpaces, necesitará crear un conector AD que apunte a las IP de su controlador de dominio MAD. Para encontrar las direcciones IP de su controlador de

dominio MAD, vaya al panel de navegación de la consola de AWS Directory Service, seleccione Directorios y, a continuación, elija el ID de directorio correcto. Para crear estos conectores AD, sigue esta guía. Una vez creados, puede registrarlos en WorkSpaces. Antes de realizar la implementación WorkSpaces en la nueva región, asegúrese de haber actualizado el conjunto de opciones de DHCP de la VPC.

Consideraciones sobre el diseño

Una implementación funcional de AD DS en la AWS nube requiere una buena comprensión tanto de los conceptos de Active Directory como de los servicios específicos. AWS En esta sección se analizan las principales consideraciones de diseño a la hora de implementar AD DS para Amazon WorkSpaces, las prácticas recomendadas de VPC para AWS Directory Service, los requisitos de DHCP y DNS, las especificaciones de AD Connector y los sitios y servicios de AD.

Diseño de VPC

Como se mencionó anteriormente en la sección Consideraciones sobre la red de este documento y se documentó anteriormente para los escenarios 2 y 3, los clientes deben implementar AD DS en la AWS nube en un par dedicado de subredes privadas, en dos AZ y separado del AD Connector o las WorkSpaces subredes. Esta construcción proporciona acceso de alta disponibilidad y baja latencia a los servicios de AD DS y WorkSpaces, al mismo tiempo, mantiene las mejores prácticas estándar de separación de roles o funciones dentro de Amazon VPC.

La siguiente figura muestra la separación de AD DS y AD Connector en subredes privadas dedicadas (escenario 3). En este ejemplo, todos los servicios residen en la misma Amazon VPC.

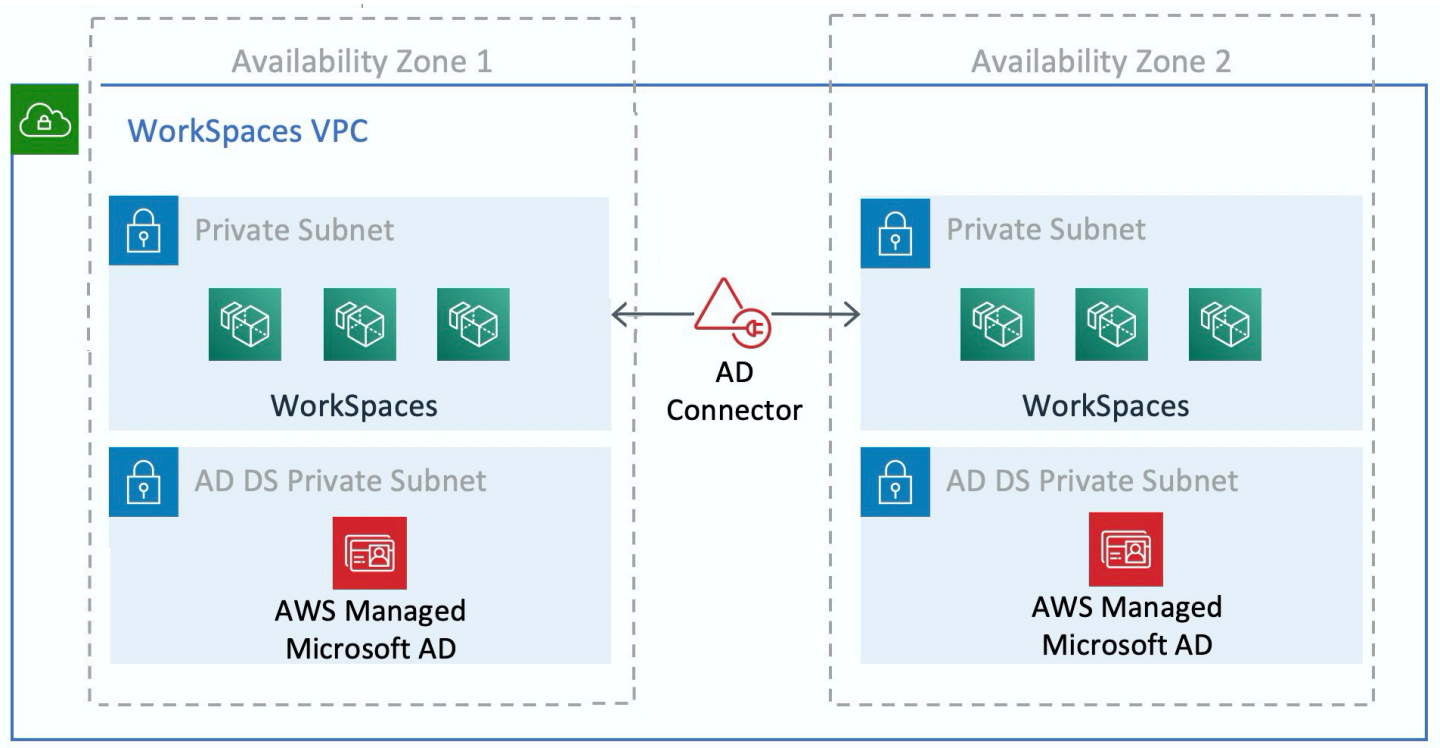

Figura 13: Separación de redes de AD DS

La siguiente figura muestra un diseño similar al escenario 1; sin embargo, en este escenario, la parte local reside en una Amazon VPC dedicada.

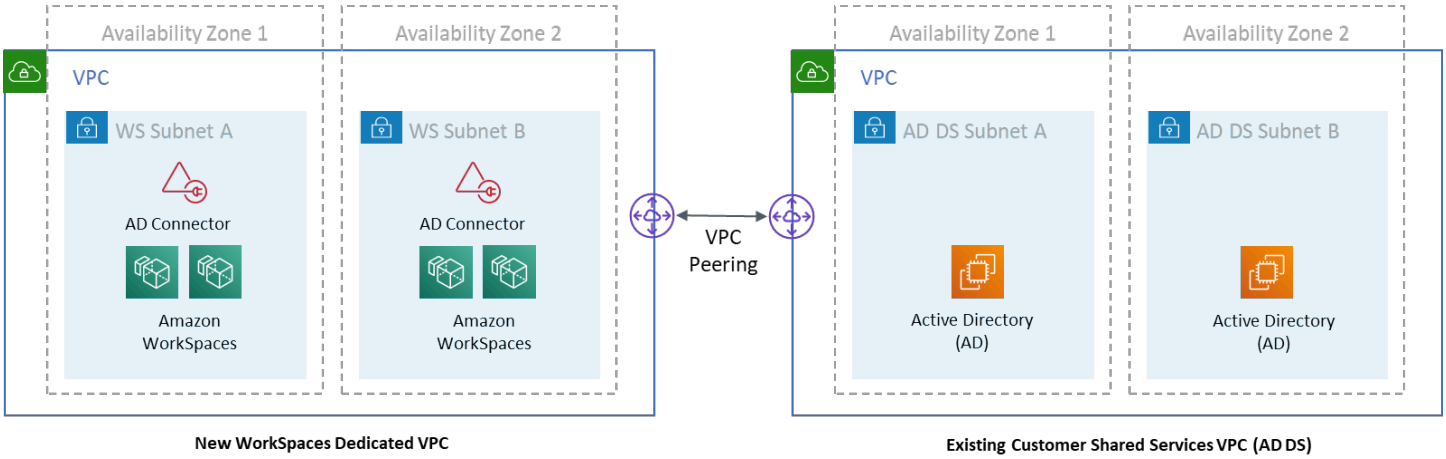

Figura 14: WorkSpaces VPC dedicada

> **Note**
>
> Para los clientes que tienen una AWS implementación existente en la que se usa AD DS, se recomienda que la ubiquen WorkSpaces en una VPC dedicada y utilicen la interconexión de VPC para las comunicaciones de AD DS.

Además de crear subredes privadas dedicadas para AD DS, los controladores de dominio y los servidores miembros requieren varias reglas de grupos de seguridad para permitir el tráfico de los servicios, como la replicación de AD DS, la autenticación de usuarios, los servicios Windows Time y el sistema de archivos distribuido (DFS).

> **Note**
>
> La mejor práctica es restringir las reglas de grupo de seguridad requeridas a las subredes WorkSpaces privadas y, en el caso del escenario 2, permitir las comunicaciones bidireccionales de AD DS locales hacia y desde la AWS nube, como se muestra en la siguiente tabla.

Tabla 1: Comunicaciones bidireccionales de AD DS hacia y desde la nube AWS

Protocolo	Puerto	Uso	Destino
TCP	53, 88, 135, 139, 389, 445, 464, 636	Autenticación (principal)	Active Directory (centro de datos privado o Amazon EC2) *
TCP	49152 — 65535	Puertos RPC High	Active Directory (centro de datos privado o Amazon EC2) **
TCP	3268-3269	Confías	Active Directory (centro de datos privado o Amazon EC2) *
TCP	9389	Microsoft Windows remoto PowerShell (opcional)	Active Directory (centro de datos privado o Amazon EC2) *
UDP	53, 88, 123, 137, 138, 389, 445, 464	Autenticación (principal)	Active Directory (centro de datos privado o Amazon EC2) *
UDP	1812	Auth (MFA) (opcional)	RADIUS (centro de datos privado o Amazon EC2) *

Para obtener más información, consulte los requisitos de puertos y la descripción general del servicio y los requisitos de puertos de red para los servicios de dominio de Active Directory y Active Directory para Windows

Para obtener step-by-step orientación sobre la implementación de reglas, consulte Cómo agregar reglas a un grupo de seguridad en la Guía del usuario de Amazon Elastic Compute Cloud.

Diseño de VPC: DHCP y DNS

Con una Amazon VPC, los servicios del Protocolo de configuración dinámica de host (DHCP) se proporcionan de forma predeterminada para sus instancias. De forma predeterminada, cada VPC proporciona un servidor de sistema de nombres de dominio (DNS) interno al que se puede acceder mediante el enrutamiento entre dominios sin clase (CIDR) +2 espacios de direcciones y se asigna a todas las instancias mediante un conjunto de opciones de DHCP predeterminado.

Los conjuntos de opciones de DHCP se utilizan en una VPC de Amazon para definir las opciones de alcance, como el nombre de dominio o los servidores de nombres que deben entregarse a las instancias de los clientes a través de DHCP. La funcionalidad correcta de los servicios de Windows en una VPC del cliente depende de esta opción de ámbito de DHCP. En cada uno de los escenarios definidos anteriormente, los clientes crean y asignan su propio ámbito que define el nombre de dominio y los servidores de nombres. Esto garantiza que las instancias de Windows unidas a un dominio o WorkSpaces estén configuradas para usar el DNS de AD.

La siguiente tabla es un ejemplo de un conjunto personalizado de opciones de ámbito de DHCP que se deben crear para que Amazon WorkSpaces y AWS Directory Services funcionen correctamente.

Tabla 2: Conjunto personalizado de opciones de ámbito de DHCP

Parámetro	Valor
Name tag (Etiqueta de nombre)	Crea una etiqueta con la clave = nombre y valor establecidos en una cadena específica Ejemplo: example.com
Nombre del dominio	example.com
Domain name servers	Dirección del servidor DNS, separada por comas Ejemplo: 192.0.2.10, 192.0.2.21
NTP servers	Deje este campo en blanco
NetBIOS name servers	Introduzca las mismas IP separadas por comas que en los servidores de nombres de dominio

Parámetro	Valor
	Ejemplo: 192.0.2.10, 192.0.2.21
NetBIOS node type	2

Para obtener más información sobre la creación de un conjunto de opciones de DHCP personalizado y su asociación a una VPC de Amazon, consulte Trabajo con conjuntos de opciones de DHCP en la Guía del usuario de Amazon Virtual Private Cloud.

En el escenario 1, el ámbito de DHCP sería el DNS local o el AD DS. Sin embargo, en los escenarios 2 o 3, este sería el servicio de directorio implementado localmente (AD DS en Amazon EC2 o AWS Directory Services: Microsoft AD). Se recomienda que cada controlador de dominio que resida en la AWS nube sea un catálogo global y un servidor DNS integrado en un directorio.

Active Directory: sitios y servicios

En el escenario 2, los sitios y los servicios son componentes fundamentales para el correcto funcionamiento de AD DS. La topología del sitio controla la replicación de AD entre controladores de dominio dentro del mismo sitio y entre los límites del sitio. En el escenario 2, hay al menos dos sitios: el local y Amazon WorkSpaces en la nube.

Definir la topología de sitio correcta garantiza la afinidad con los clientes, lo que significa que los clientes (en este caso WorkSpaces) utilizan su controlador de dominio local preferido.

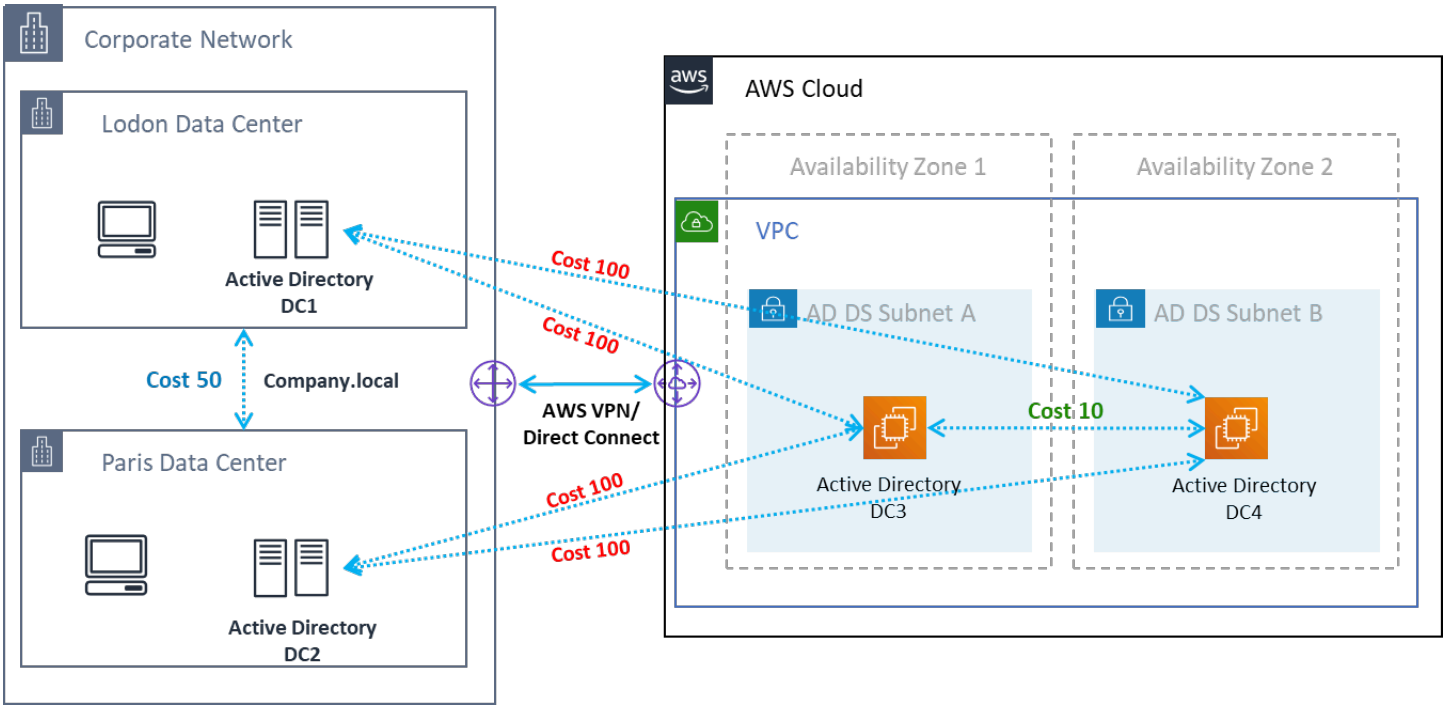

Figura 15: Sitios y servicios de Active Directory: afinidad con el cliente

Práctica recomendada: Defina el alto costo de los enlaces de sitios entre AD DS locales y la AWS nube. En la siguiente figura se muestra un ejemplo del coste de asignar los enlaces a sitios (coste de 100€) para garantizar una afinidad con los clientes independiente del sitio.

Estas asociaciones ayudan a garantizar que el tráfico, como la replicación de AD DS y la autenticación de clientes, utilice la ruta más eficiente hacia un controlador de dominio. En el caso de los escenarios 2 y 3, esto ayuda a garantizar una latencia y un tráfico de enlaces cruzados más bajos.

Protocolo

Amazon WorkSpaces Streaming Protocol (WSP) es un protocolo de streaming nativo de la nube que permite una experiencia de usuario uniforme a través de distancias globales y redes poco fiables. El WSP desvincula el protocolo del protocolo descargando el análisis métrico, la WorkSpaces codificación, el uso y la selección de códecs. El WSP utiliza el puerto TCP/UDP 4195. A la hora de decidir si utilizar o no el protocolo WSP, hay varias preguntas clave que deben responderse antes de la implementación. Consulte la siguiente matriz de decisiones:

Pregunta	AVISPA	PCoIP
¿Necesitarán los WorkSpaces usuarios identificados audio o vídeo bidireccionales?	•	
¿Se utilizará cero clientes como punto final remoto (dispositivo local)?		•
¿Se utilizará Windows o macOS como punto final remoto?	•	•
¿Se usará Ubuntu 18.04 como punto final remoto?		•
¿Los usuarios accederán a Amazon WorkSpaces a través del acceso web?		•
¿Es necesaria la compatibi lidad con tarjetas inteligentes (PIC/CAC) antes o durante la sesión?	•	
¿Se WorkSpaces utilizará en la región de China (Ningxia)?		•
¿Será necesaria la autentica ción previa con tarjeta inteligente o la asistencia durante la sesión?	•	
¿Los usuarios finales utilizan conexiones poco fiables, de alta latencia o con poco ancho de banda?	•	

Las preguntas anteriores son fundamentales para determinar el protocolo que se debe utilizar. Puede consultar información adicional sobre los casos de uso del protocolo recomendados aquí. El protocolo utilizado también se puede cambiar más adelante mediante la función Amazon WorkSpaces Migrate. Puede consultar más información sobre el uso de esta función aquí.

Al realizar la implementación WorkSpaces mediante WSP, las pasarelas WSP deben añadirse a una lista de dispositivos permitidos para garantizar la conectividad con el servicio. Además, para los usuarios que se conecten a un WSP WorkSpaces mediante un WSP, el tiempo de ida y vuelta (RTT) debe ser inferior a 250 ms para obtener el mejor rendimiento. Las conexiones con un RTT de entre 250 ms y 400 ms se degradarán. Si la conexión del usuario se degrada constantemente, se recomienda implementar Amazon WorkSpaces en una región compatible con el servicio más cercana al usuario final, si es posible.

Multi-Factor Authentication (MFA)

La implementación de la MFA requiere WorkSpaces que Amazon esté configurado con un Active Directory Connector (AD Connector) o un AWS Microsoft AD administrado (MAD) como servicio de directorio, y que disponga de un servidor RADIUS al que pueda acceder desde la red el Directory Service. El Active Directory simple no admite MFA.

Consulte la sección anterior, donde se describen las consideraciones sobre la implementación de Active Directory y los servicios de directorio para AD y las opciones de diseño de RADIUS en cada escenario.

MFA: autenticación de dos factores

Una vez habilitada la MFA, los usuarios deben proporcionar su nombre de usuario, contraseña y código MFA WorkSpaces al cliente para la autenticación en sus escritorios respectivos. WorkSpaces

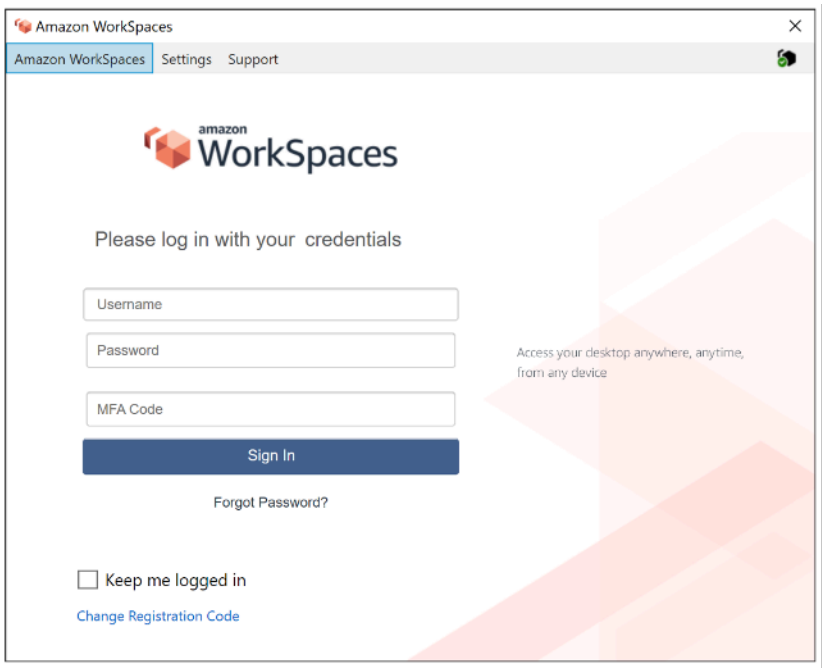

Figura 16: WorkSpaces cliente con MFA activado

> **Note**
>
> AWS Directory Service no admite la MFA selectiva por usuario o contextual: se trata de una configuración global por directorio. Si se requiere un MFA selectivo «por usuario», los usuarios deben estar separados por un conector AD, que puede apuntar a la misma fuente de Active Directory.

WorkSpaces La MFA requiere uno o más servidores RADIUS. Por lo general, se trata de soluciones existentes que quizás ya haya implementado, por ejemplo, RSA o Gemalto. Como alternativa, los servidores RADIUS se pueden implementar dentro de la VPC en las instancias EC2 (consulte la sección Escenarios de implementación de AD DS de este documento para ver las opciones de arquitectura). Si está implementando una nueva solución RADIUS, existen varias implementaciones, como FreeRADIUS, junto con ofertas de SaaS como Duo Security o Okta MFA.

Se recomienda aprovechar varios servidores RADIUS para garantizar que la solución sea resistente a los fallos. Al configurar su Directory Service para MFA, puede introducir varias direcciones IP separándolas con una coma (por ejemplo, 192.0.0.0,192.0.0.12). La función MFA de los servicios de directorio probará con la primera dirección IP especificada y pasará a la segunda dirección IP en caso de que no se pueda establecer la conectividad de red con la primera. La configuración de RADIUS para una arquitectura de alta disponibilidad es única para cada conjunto de soluciones; sin

embargo, la recomendación general es colocar las instancias subyacentes de la capacidad RADIUS en diferentes zonas de disponibilidad. Un ejemplo de configuración es Duo Security y, para el MFA de Okta, puede implementar varios agentes de servidor RADIUS de Okta de la misma manera.

Para ver los pasos detallados para habilitar su AWS Directory Service para MFA, consulte AD Connector y Managed AWS Microsoft AD.

Recuperación ante desastres y continuidad empresarial

WorkSpaces Redirección entre regiones

Amazon WorkSpaces es un servicio regional que proporciona a los clientes acceso remoto al escritorio. En función de los requisitos de continuidad empresarial y recuperación ante desastres (BC/DR), algunos clientes requieren una conmutación por error sin contratiempos a otra región en la que el WorkSpaces servicio esté disponible. Este requisito de BC/DR se puede cumplir con la opción de redireccionamiento entre regiones. WorkSpaces Permite a los clientes utilizar un nombre de dominio completo (FQDN) como código de registro. WorkSpaces

Una consideración importante es determinar en qué punto debe producirse una redirección a una región de conmutación por error. Los criterios para tomar esta decisión deben basarse en la política de la empresa, pero deben incluir el objetivo de tiempo de recuperación (RTO) y el objetivo de punto de recuperación (RPO). Un diseño de arquitectura de WorkSpaces Well-Architected debe incluir la posibilidad de que se produzca una falla en el servicio. La tolerancia temporal para la recuperación normal de las operaciones comerciales también influirá en la decisión.

Cuando los usuarios finales inician sesión WorkSpaces con un FQDN como código de WorkSpaces registro, se resuelve un registro TXT de DNS que contiene un identificador de conexión que determina el directorio registrado al que se dirigirá el usuario. A continuación, se presentará la página de inicio de sesión del WorkSpaces cliente en función del directorio registrado asociado al identificador de conexión devuelto. Esto permite a los administradores dirigir a sus usuarios finales a diferentes WorkSpaces directorios en función de sus políticas de DNS para el FQDN. Esta opción se puede usar con zonas DNS públicas o privadas, suponiendo que las zonas privadas se puedan resolver desde la máquina cliente. La redirección entre regiones puede ser manual o automática. Estas dos conmutaciones por error se pueden lograr cambiando el registro TXT que contiene el identificador de conexión para que apunte al directorio deseado.

Al desarrollar su estrategia de BC/DR, es importante tener en cuenta los datos del usuario, ya que la opción de redireccionamiento WorkSpaces entre regiones no sincroniza ningún dato de usuario ni sincroniza las imágenes. WorkSpaces Sus WorkSpaces despliegues en distintas regiones

son entidades independientes. AWS Por lo tanto, tendrá que tomar medidas adicionales para garantizar que sus WorkSpaces usuarios puedan acceder a sus datos cuando se produzca un redireccionamiento a una región secundaria. Hay muchas opciones disponibles para la replicación de datos de usuario WorkSpaces, como Windows FSx (DFS Share) o utilidades de terceros para sincronizar los volúmenes de datos entre regiones. Del mismo modo, tendrá que asegurarse de que la región secundaria tenga acceso a las WorkSpaces imágenes requeridas, por ejemplo, copiándolas de una región a otra. Para obtener más información, consulta Redireccionamiento entre regiones para Amazon WorkSpaces en la Guía de WorkSpaces administración de Amazon y el ejemplo del diagrama.

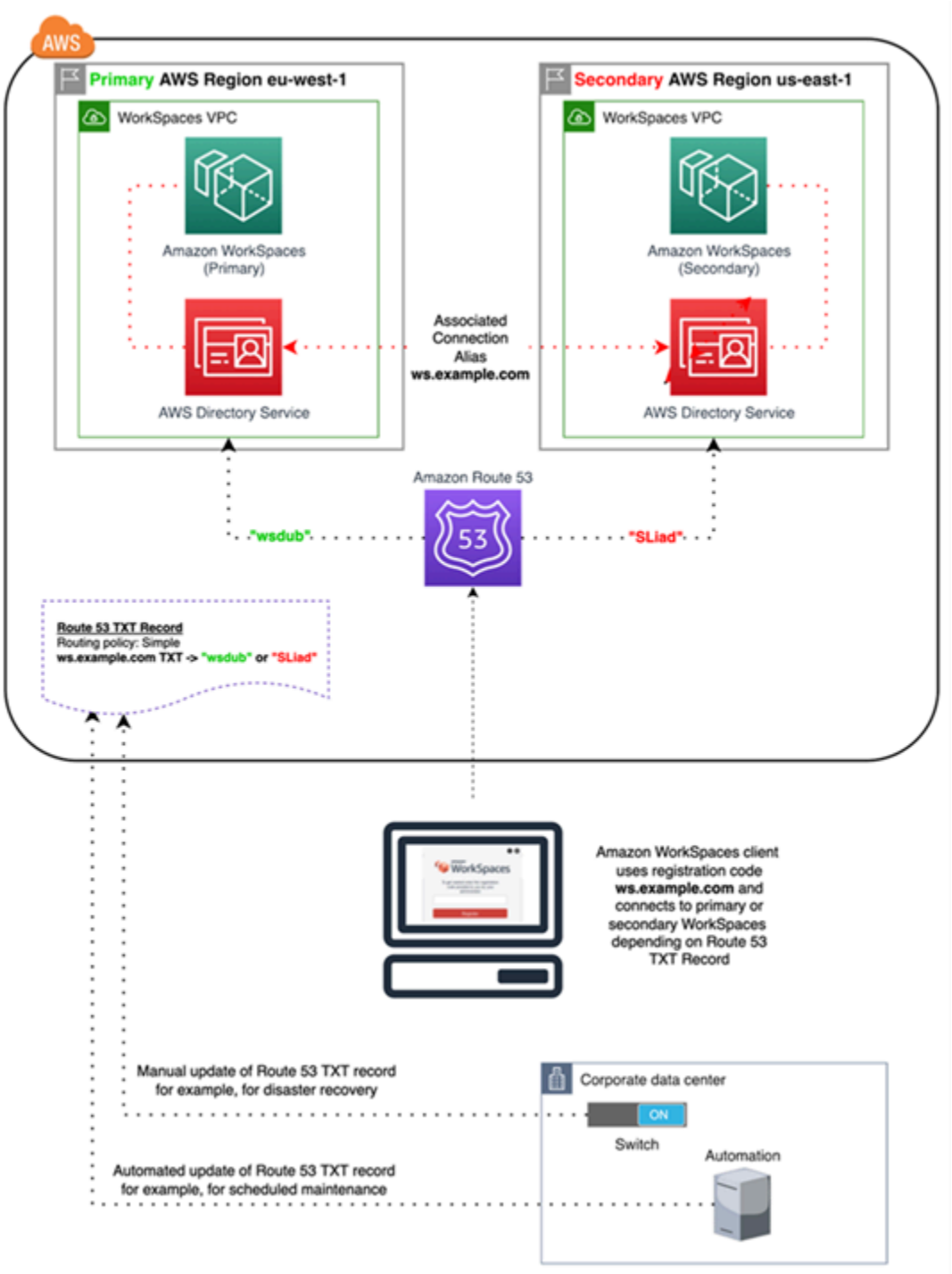

Figura 17: Ejemplo de redireccionamiento WorkSpaces entre regiones con Amazon Route 53

WorkSpaces Punto final de interfaz VPC (AWS PrivateLink): llamadas a la API

Las API WorkSpaces públicas de Amazon son compatibles con AWS PrivateLink. AWS PrivateLink aumenta la seguridad de los datos compartidos con aplicaciones basadas en la nube al reducir la exposición de los datos a la Internet pública. WorkSpaces El tráfico de la API se puede proteger dentro de una VPC mediante un punto final de interfaz, que es una interfaz de red elástica con una dirección IP privada del rango de direcciones IP de la subred que sirve como punto de entrada para el tráfico destinado a un servicio compatible. Esto le permite acceder de forma privada a los servicios de la WorkSpaces API mediante direcciones IP privadas.

El uso PrivateLink con API WorkSpaces públicas también le permite exponer de forma segura las API de REST a los recursos que solo se encuentran dentro de su VPC o a aquellos que están conectados a sus centros de datos a través de ellos. AWS Direct Connect

Puede restringir el acceso a Amazon VPC y puntos de enlace de VPC seleccionados, y habilitar el acceso entre cuentas mediante políticas específicas de recursos.

Asegúrese de que el grupo de seguridad asociado a la interfaz de red de puntos finales permita la comunicación entre la interfaz de red de puntos finales y los recursos de la VPC que se comunican con el servicio. Si el grupo de seguridad restringe el tráfico HTTPS entrante (puerto 443) de los recursos de la VPC, es posible que no pueda enviar tráfico a través de la interfaz de red de punto de enlace. Un punto de conexión de interfaz solo admite tráfico TCP.

- Los puntos de enlace solo son compatibles con el tráfico IPv4.
- Al crear un punto de enlace, puede asociar una política de punto de enlace que controle el acceso al servicio al que se va a conectar.
- Hay una cuota en el número de puntos de enlace que puede crear por VPC.
- Los puntos finales solo se admiten en la misma región. No puede crear un punto final entre una VPC y un servicio en una región diferente.

Cree una notificación para recibir alertas sobre los eventos del punto final de la interfaz: puede crear una notificación para recibir alertas sobre eventos específicos que se produzcan en el punto final de la interfaz. Para crear una notificación, debe asociar un tema de Amazon SNS con la notificación. Suscribiéndose al tema de SNS recibirá una notificación por correo electrónico cuando se produzca el evento en el punto de conexión.

Cree una política de puntos de enlace de VPC para Amazon WorkSpaces: puede crear una política para los puntos de enlace de VPC de Amazon WorkSpaces para especificar lo siguiente:

- La entidad principal que puede realizar acciones.
- Las acciones que se pueden realizar.
- Los recursos en los que se pueden llevar a cabo las acciones.

Conecte su red privada a su VPC: para llamar a la WorkSpaces API de Amazon a través de su VPC, debe conectarse desde una instancia que esté dentro de la VPC o conectar su red privada a su VPC mediante una red privada virtual (VPN) de Amazon o. AWS Direct Connect Para obtener información sobre Amazon VPN, consulte las conexiones VPN en la Guía del usuario de Amazon Virtual Private Cloud. Para obtener más información AWS Direct Connect, consulte Crear una conexión en la Guía del AWS Direct Connect usuario.

Para obtener más información sobre el uso de la WorkSpaces API de Amazon a través de un punto final de interfaz de VPC, consulta Infrastructure Security in Amazon. WorkSpaces

Compatibilidad con tarjetas inteligentes

La compatibilidad con tarjetas inteligentes está disponible tanto para Microsoft Windows como para Amazon Linux WorkSpaces. La compatibilidad con tarjetas inteligentes mediante la tarjeta de acceso común (CAC) y la verificación de identidad personal (PIV) están disponibles exclusivamente a través de Amazon WorkSpaces mediante el Protocolo de WorkSpaces transmisión (WSP). La compatibilidad con tarjetas inteligentes del WSP WorkSpaces ofrece una mayor seguridad para autenticar a los usuarios en puntos de conexión aprobados por la organización con un hardware específico, en forma de lectores de tarjetas inteligentes. Es importante familiarizarse primero con el alcance del soporte disponible para las tarjetas inteligentes y determinar cómo funcionarían las tarjetas inteligentes en las WorkSpaces implementaciones actuales y futuras.

Se recomienda determinar qué tipo de compatibilidad con tarjetas inteligentes es necesaria: la autenticación previa a la sesión o la autenticación durante la sesión. En el momento de escribir este artículo, la autenticación previa a la sesión solo está disponible en AWS GovCloud (EE. UU. Oeste), EE. UU. Este (Virginia del Norte), EE. UU. Oeste (Oregón), Europa (Irlanda), Asia Pacífico (Tokio) y Asia Pacífico (Sídney). La autenticación mediante tarjeta inteligente durante la sesión suele estar disponible teniendo en cuenta algunas consideraciones, como las siguientes:

- ¿Cuenta su organización con una infraestructura de tarjetas inteligentes integrada con Windows Active Directory?

- ¿Su respondedor del Protocolo de estado de certificados en línea (OCSP) tiene acceso público a Internet?
- ¿Los certificados de usuario se emiten con el nombre principal del usuario (UPN) en el campo Nombre alternativo del sujeto (SAN)?
- Se detallan más consideraciones en las secciones sobre la sesión y antes de la sesión.

La compatibilidad con tarjetas inteligentes se habilita mediante la política de grupo. Se recomienda añadir la plantilla administrativa de la política de WorkSpaces grupo de Amazon para WSP al almacén central del dominio de Active Directory que utilizan Amazon WorkSpaces Directory. Al aplicar esta política a una WorkSpaces implementación existente de Amazon, todas WorkSpaces requerirán la actualización de la política de grupo y un reinicio para que el cambio surta efecto para todos los usuarios, ya que se trata de una política basada en computadoras.

CA raíz

La naturaleza de la portabilidad del WorkSpaces cliente y el usuario de Amazon exige la obligación de entregar de forma remota el certificado CA raíz de terceros al almacén de certificados raíz de confianza de cada dispositivo que los usuarios utilizan para conectarse a Amazon. WorkSpaces Los controladores de dominio de AD y los dispositivos de usuario con tarjetas inteligentes deben confiar en las CA raíz. Consulte las directrices proporcionadas por Microsoft para habilitar las CA de terceros para obtener más información sobre los requisitos exactos.

En los entornos unidos a un dominio de AD, estos dispositivos cumplen este requisito mediante la política de grupo que distribuye los certificados de CA raíz. En los casos en los que Amazon WorkSpaces Client se utiliza desde non-domain-joined dispositivos, se debe determinar un método de entrega alternativo para las CA raíz de terceros, como Intune.

Durante la sesión

La autenticación durante la sesión simplifica y asegura la autenticación de las aplicaciones una vez que las sesiones de los WorkSpaces usuarios de Amazon ya se han iniciado. Como se mencionó anteriormente, el comportamiento predeterminado de Amazon WorkSpaces deshabilita las tarjetas inteligentes y debe habilitarse mediante una política de grupo. Desde la perspectiva de WorkSpaces la administración de Amazon, la configuración es necesaria específicamente para las aplicaciones que transfieren la autenticación (como los navegadores web). No es necesario realizar cambios en los conectores y directorios de AD.

Las aplicaciones más comunes que requieren soporte de autenticación durante la sesión se utilizan a través de navegadores web como Mozilla Firefox y Google Chrome. Mozilla Firefox requiere una configuración limitada para admitir tarjetas inteligentes durante la sesión. Amazon Linux WSP WorkSpaces requiere una configuración adicional para poder admitir tarjetas inteligentes durante la sesión tanto en Mozilla Firefox como en Google Chrome.

Se recomienda asegurarse de que las CA raíz estén cargadas en el almacén de certificados personales del usuario antes de solucionar el problema, ya que es posible que el WorkSpaces cliente de Amazon no tenga permisos para acceder al ordenador local. Además, utilice OpenSC para identificar los dispositivos de tarjetas inteligentes al solucionar cualquier posible problema de autenticación durante la sesión con tarjetas inteligentes. Por último, se recomienda utilizar un respondedor del Protocolo de estado de certificados en línea (OCSP) para mejorar la seguridad de la autenticación de las aplicaciones mediante una comprobación de la revocación de certificados.

Antes de la sesión

Support para la autenticación previa a la sesión requiere Windows WorkSpaces Client 3.1.1 y versiones posteriores, o WorkSpaces clientes macOS 3.1.5 y posteriores. La autenticación previa a la sesión con tarjetas inteligentes es fundamentalmente diferente a la autenticación estándar, ya que requiere que el usuario se autentique mediante una combinación de la inserción de la tarjeta inteligente y la introducción de un código PIN. Con este tipo de autenticación, la duración de las sesiones del usuario está limitada por la duración del vale Kerberos. Puede encontrar una guía de instalación completa aquí.

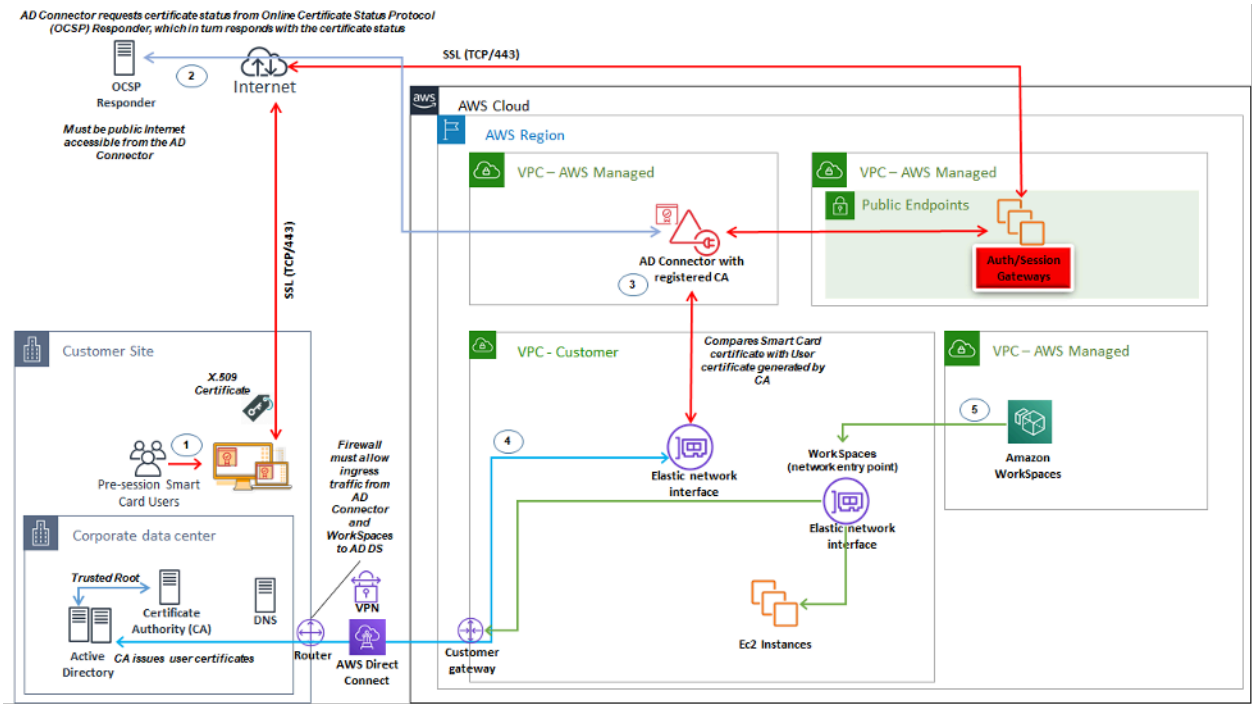

Figura 18: Descripción general de la autenticación previa a la sesión

1. El usuario abre Amazon WorkSpaces Client, inserta la tarjeta inteligente e introduce su PIN. Amazon WorkSpaces Client utiliza el PIN para descifrar el certificado X.509, que se envía por proxy al AD Connector a través de la puerta de enlace de autenticación.
2. AD Connector valida el certificado X.509 con la URL del respondedor OCSP de acceso público especificada en la configuración del directorio para garantizar que el certificado no se haya revocado.
3. Si el certificado es válido, el WorkSpaces cliente de Amazon continúa con el proceso de autenticación y solicita al usuario que introduzca su PIN por segunda vez para descifrar el certificado X.509 y el proxy del AD Connector, donde, a continuación, se compara con los certificados raíz e intermedio del AD Connector para su validación.
4. Una vez que la validación del certificado coincide correctamente, el AD Connector utiliza Active Directory para autenticar al usuario y se crea un vale de Kerberos.
5. El ticket de Kerberos se pasa a Amazon del usuario WorkSpace para autenticarse e iniciar la sesión de WSP.

El OCSP Responder debe ser de acceso público, ya que la conexión se realiza a través de la red AWS administrada y no de la red administrada por el cliente; por lo tanto, no hay enrutamiento a redes privadas en este paso.

No es necesario introducir el nombre del usuario, ya que los certificados de usuario presentados a AD Connector incluyen el userPrincipalName UPN del usuario en el campo subjectAltName (SAN) del certificado. Se recomienda automatizar todos los usuarios que requieren la autenticación previa a la sesión con tarjetas inteligentes y actualizar sus objetos de usuario de AD para autenticarse con el UPN previsto en el certificado que utilizan PowerShell, en lugar de hacerlo de forma individual en las consolas de administración de Microsoft.

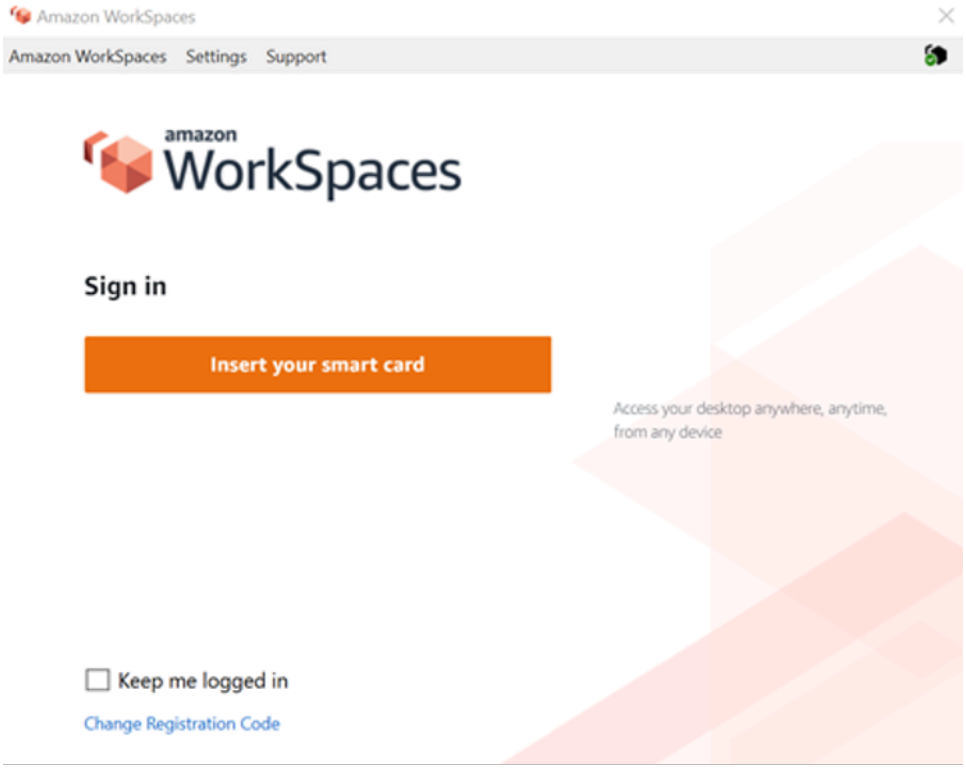

Figura 19: consola de WorkSpaces inicio de sesión

Despliegue de clientes

El Amazon WorkSpaces Client (versión 3.X+) utiliza archivos de configuración estandarizados que los administradores pueden utilizar para preconfigurar el cliente de sus usuarios. WorkSpaces La ruta de los dos archivos de configuración principales se encuentra en:

SO	Ruta del archivo de configuración
Windows	C:\Users\USERNAME\AppData\ Local\ Amazon Web Services\ Amazon WorkSpaces

SO	Ruta del archivo de configuración
macOS	/Usuarios/Nombre de usuario/Biblioteca /Soporte de aplicaciones/Amazon Web Services/Amazon WorkSpaces
Linux (Ubuntu 18.04)	/home/ubuntu/.local/share/Amazon Web Services/Amazon/ WorkSpaces

Dentro de estas rutas, encontrará los dos archivos de configuración. El primer archivo de configuración es UserSettings .json, que establecerá aspectos como el registro actual, la configuración del proxy, el nivel de registro y la posibilidad de guardar la lista de registros. El segundo archivo de configuración es RegistrationList .json. Este archivo contendrá toda la información del WorkSpaces directorio que el cliente utilizará para asignarla al WorkSpaces directorio correcto. Al preconfigurar RegistrationList .json, se rellenarán todos los códigos de registro del cliente para el usuario.

> **Note**
>
> Si sus usuarios utilizan la versión 2.5.11 del WorkSpaces cliente, se utilizará proxy.cfg para la configuración del proxy del cliente y client_settings.ini establecerá el nivel de registro, así como la posibilidad de guardar la lista de registro. La configuración de proxy predeterminada utilizará lo establecido en el sistema operativo.

Como estos archivos están estandarizados, los administradores pueden descargar el WorkSpaces cliente, establecer todos los ajustes aplicables y, a continuación, enviar los mismos archivos de configuración a todos los usuarios finales. Para que la configuración surta efecto, el cliente debe iniciarse después de establecer las nuevas configuraciones. Si cambia la configuración mientras el cliente está en ejecución, ninguno de los cambios se establecerá en el cliente.

La última configuración que se puede configurar para WorkSpaces los usuarios es la actualización automática del cliente de Windows. Esto no se controla mediante archivos de configuración, sino mediante el Registro de Windows. Cuando salga una nueva versión del cliente, puede crear una clave de registro para omitir esa versión. Esto se puede configurar creando una cadena de nombres de entradas de registro SkipThisVersion con el valor del número de versión completo en la siguiente ruta: Computer\ HKEY_CURRENT_USER\ Software\ Amazon Web Services. LLC\

Amazon WorkSpaces\ WinSparkle Esta opción también está disponible para macOS; sin embargo, la configuración se encuentra dentro de un archivo plist que requiere un software especial para editarlo. Si aún así deseas realizar esta acción, puedes hacerlo añadiendo una SkippedVersion entrada SU en el dominio com.amazon.workspaces, ubicado en: /Users/username/Library/Preferences

Selección de puntos de WorkSpaces conexión de Amazon

Cómo elegir un punto final para su WorkSpaces

Amazon WorkSpaces ofrece soporte para varios dispositivos de punto final, desde escritorios Windows hasta iPads y Chromebooks. Puede descargar los WorkSpaces clientes de Amazon disponibles desde el sitio web de Amazon Workspaces. Elegir el punto de conexión adecuado para sus usuarios es una decisión importante. Si sus usuarios requieren el uso de audio/vídeo bidireccional y van a utilizar el protocolo de WorkSpaces transmisión, deben usar el cliente de Windows o macOS. Para todos los clientes, asegúrese de que las direcciones IP y los puertos que figuran en los requisitos de direcciones IP y puertos de Amazon se WorkSpaces hayan configurado de forma explícita para garantizar que el cliente pueda conectarse al servicio. Estas son algunas consideraciones adicionales que le ayudarán a elegir un dispositivo de punto final:

- Windows: para utilizar el WorkSpaces cliente Amazon de Windows, el cliente 4.x debe ejecutar el escritorio Microsoft Windows 8.1 y Windows 10 de 64 bits que requiere. Los usuarios pueden instalar el cliente solo para su perfil de usuario sin privilegios administrativos en la máquina local. Los administradores del sistema pueden implementar el cliente en puntos finales administrados con una política de grupo, Microsoft Endpoint Manager Configuration Manager (MEMCM) u otras herramientas de implementación de aplicaciones utilizadas en un entorno. El cliente de Windows admite un máximo de cuatro pantallas y una resolución máxima de 3840 x 2160.
- macOS: para implementar el último WorkSpaces cliente de Amazon para macOS, los dispositivos macOS deben ejecutar macOS 10.12 (Sierra) o posterior. Puede implementar una versión anterior del WorkSpaces cliente para conectarse a PCoIP WorkSpaces si el terminal ejecuta OSX 10.8.1 o una versión posterior. El cliente macOS admite hasta dos monitores con resolución 4K o cuatro monitores con resolución WUXGA (1920 x 1200).
- Linux: el cliente Amazon WorkSpaces Linux requiere Ubuntu 18.04 (AMD64) de 64 bits para ejecutarse. Si sus terminales Linux no ejecutan esta versión del sistema operativo, el cliente Linux no es compatible. Antes de implementar clientes Linux o proporcionar a los usuarios su código de registro, asegúrese de habilitar el acceso a los clientes Linux a nivel de WorkSpaces directorio, ya que está deshabilitado de forma predeterminada y los usuarios no podrán conectarse desde los

clientes Linux hasta que esté habilitado. El cliente Linux admite hasta dos monitores con resolución 4K o cuatro monitores con resolución WUXGA (1920 x 1200).

- iPad: la aplicación cliente Amazon WorkSpaces iPad es compatible con PCoIP WorkSpaces. Los iPads compatibles son el iPad2 o posterior con iOS 8.0 o posterior, el iPad Retina con iOS 8.0 y posterior, el iPad Mini con iOS 8.0 y posterior y el iPad Pro con iOS 9.0 y posterior. Asegúrese de que el dispositivo desde el que se conectarán los usuarios cumpla con esos criterios. La aplicación cliente para iPad admite muchos gestos diferentes. (Consulta la lista completa de los gestos compatibles). La aplicación cliente Amazon WorkSpaces iPad también es compatible con el Swiftpoint GT y PadPoint los ProPoint ratones. El Swiftpoint, el TRACPOINT PenPoint y GoPoint los ratones no son compatibles.
- Android/Chromebook: cuando desee implementar un dispositivo Android o un Chromebook como terminal para sus usuarios finales, hay algunas consideraciones que deben tenerse en cuenta. Asegúrese de que los usuarios a WorkSpaces los que se van a conectar sean PCoIP WorkSpaces, ya que este cliente solo es compatible con PCoIP. WorkSpaces Este cliente solo admite una pantalla única. Si los usuarios necesitan compatibilidad con varios monitores, utilice un terminal diferente. Si quieres implementar un Chromebook, asegúrate de que el modelo que implementes admita la instalación de aplicaciones de Android. La compatibilidad con todas las funciones solo se admite en el cliente de Android, no en el cliente de Chromebook anterior. Por lo general, esto solo se tiene en cuenta en el caso de los Chromebooks fabricados antes de 2019. La compatibilidad con Android se proporciona tanto para tabletas como para teléfonos, siempre que el Android ejecute el sistema operativo 4.4 o posterior. Sin embargo, se recomienda que el dispositivo Android ejecute el sistema operativo OS 9 o superior para utilizar el cliente WorkSpace Android más reciente. Si sus Chromebooks utilizan la versión de WorkSpaces cliente 3.0.1 o superior, sus usuarios ahora pueden aprovechar las funciones de autoservicio. WorkSpaces Además, como administrador, puedes utilizar certificados de dispositivos de confianza para restringir el WorkSpaces acceso a dispositivos de confianza con certificados válidos.
- Acceso web: los usuarios pueden acceder a Windows WorkSpaces desde cualquier ubicación mediante un navegador web. Esto es ideal para los usuarios que deben usar un dispositivo bloqueado o una red restrictiva. En lugar de utilizar una solución de acceso remoto tradicional e instalar la aplicación cliente correspondiente, los usuarios pueden visitar el sitio web para obtener acceso a los recursos de trabajo. Los usuarios pueden utilizar el acceso WorkSpaces web para conectarse a non-graphics-based Windows PCoIP con Windows 10 o WorkSpaces Windows Server 2016 con Desktop Experience. Los usuarios deben conectarse mediante Chrome 53 o una versión posterior, o Firefox 49 o una versión posterior. En el caso de los sistemas basados en WSP WorkSpaces, los usuarios pueden utilizar el acceso WorkSpaces web para conectarse a dispositivos no gráficos basados en Windows. WorkSpaces Estos usuarios deben conectarse

mediante Microsoft Edge 91 o posterior o Google Chrome 91 o posterior. La resolución de pantalla mínima admitida es de 960 x 720 con una resolución máxima admitida de 2560 x 1600. No se admiten varios monitores. Para obtener la mejor experiencia de usuario, siempre que sea posible, se recomienda que los usuarios utilicen una versión de sistema operativo del cliente.

- Cliente cero de PCoIP: puede implementar clientes cero de PCoIP para los usuarios finales a los que se les asigne o se les asignará el WorkSpaces PCoIP. El cliente cero de Tera2 debe tener una versión de firmware 6.0.0 o posterior para conectarse directamente al. WorkSpace Para utilizar la autenticación multifactor con Amazon WorkSpaces, el dispositivo cliente Tera2 zero debe ejecutar la versión de firmware 6.0.0 o posterior. Support y solución de problemas del hardware de cliente cero deben realizarse con el fabricante.
- Sistema operativo IGEL: puede utilizar el sistema operativo IGEL en dispositivos terminales para conectarse a dispositivos basados en PCoIP siempre que la versión del firmware WorkSpaces sea la 11.04.280 o superior. Las funciones compatibles coinciden con las del cliente Linux existente en la actualidad. Antes de implementar los clientes del sistema operativo IGEL o proporcionar a los usuarios su código de registro, asegúrese de habilitar el acceso a los clientes Linux a nivel de WorkSpaces directorio, ya que está deshabilitado de forma predeterminada y los usuarios no podrán conectarse desde los clientes del sistema operativo IGEL hasta que esté habilitado. El cliente LGel OS admite hasta dos monitores con resolución 4K o cuatro monitores con resolución WUXGA (1920 x 1200).

Cliente de acceso web

Diseñado para dispositivos bloqueados, el cliente Web Access proporciona acceso a Amazon WorkSpaces sin necesidad de implementar software de cliente. El cliente de acceso web solo se recomienda en entornos en los que Amazon WorkSpaces sea un sistema operativo (SO) Windows y se utilice para flujos de trabajo de usuarios limitados, como un entorno de quiosco. La mayoría de los casos de uso se benefician del conjunto de funciones disponible en el WorkSpaces cliente de Amazon. El cliente Web Access solo se recomienda en casos de uso específicos en los que los dispositivos y las restricciones de red requieren un método de conexión alternativo.

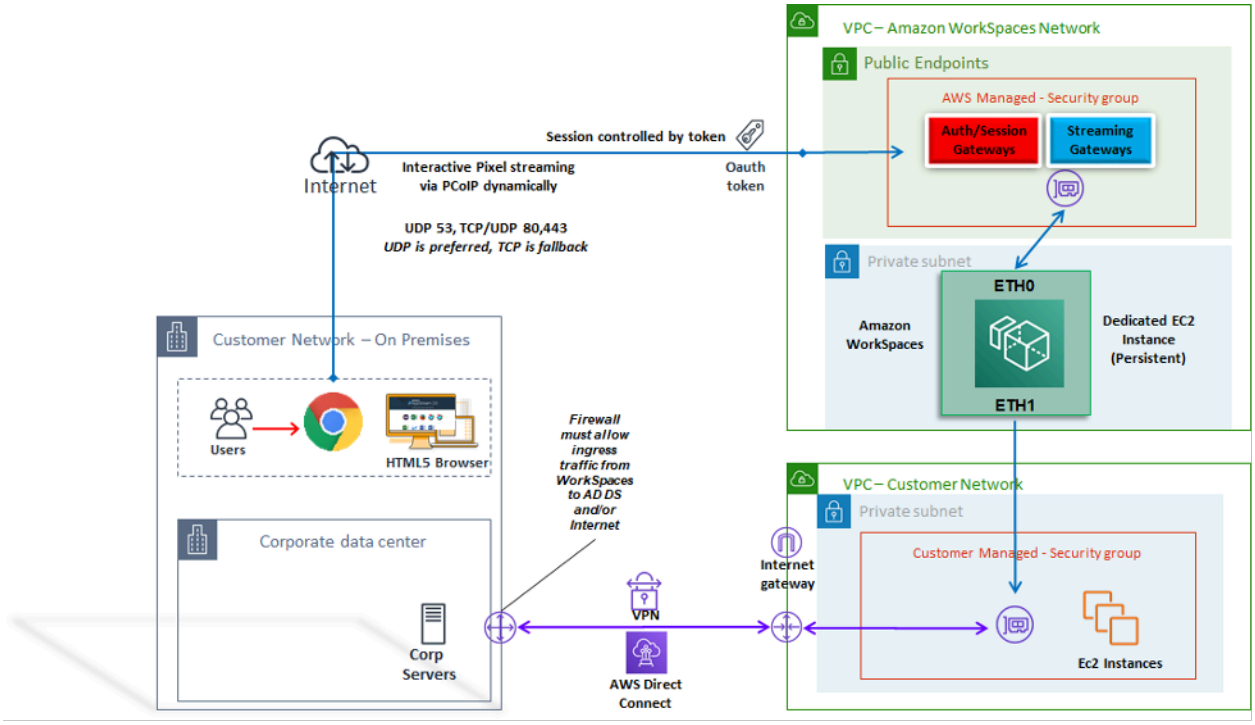

Figura 20: Arquitectura del cliente de acceso web

Como se muestra en el diagrama, el cliente de acceso web tiene diferentes requisitos de red para transmitir la sesión a los usuarios. El acceso web está disponible para Windows WorkSpaces mediante el protocolo PCoIP o WSP. Se requieren DNS y HTTP/HTTPS para la autenticación y el registro en las puertas de enlace. WorkSpaces Para WorkSpaces utilizar el protocolo WSP, es necesario abrir la conexión directa del UDP/TCP 4195 a los rangos de direcciones IP de la puerta de enlace WSP. El tráfico de streaming no se asigna a un puerto fijo como ocurre con el WorkSpaces cliente completo de Amazon, sino que se asigna de forma dinámica. El UDP es preferible para el tráfico de streaming; sin embargo, el navegador web recurrirá al TCP cuando se restrinja el UDP. En entornos en los que el puerto TCP/UDP 4172 está bloqueado y no se puede desbloquear debido a restricciones organizativas, el cliente de acceso web ofrece a los usuarios un método de conexión alternativo.

De forma predeterminada, el cliente de acceso web está deshabilitado en el nivel del directorio. Para permitir que los usuarios accedan a Amazon WorkSpaces a través de un navegador web, usa la AWS Management Console para actualizar la configuración del Directorio o usa la WorkspaceAccessProperties API de forma programática para modificarla DeviceTypeWeb a Permitir. Además, el administrador debe asegurarse de que la configuración de la política de grupo no entre en conflicto con los requisitos de inicio de sesión.

WorkSpaces Etiquetas de Amazon

```
Tags enable you to associate metadata with AWS resources. Tags can be used with Amazon
 WorkSpaces to registered directories,
  bundles, IP Access Control Groups, or images. Tags assist with cost allocation to
 internal cost centers. Before using tags with Amazon WorkSpaces,
  refer to the Tagging Best Practices whitepaper.

Tag restrictions
```

- Número máximo de etiquetas por recurso: 50
- Longitud máxima de la clave: 127 caracteres Unicode
- Longitud máxima del valor: 255 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 los prefijos aws: o aws:workspaces: en los nombres o valores de las etiquetas porque están reservados para su uso. AWS Los nombres y valores de etiquetas que tienen estos prefijos no se pueden editar.

Recursos que puede etiquetar

- Puede añadir etiquetas a los siguientes recursos al crearlos: imágenes WorkSpaces importadas y grupos de control de acceso IP.
- Puede añadir etiquetas a los recursos existentes de los siguientes tipos: directorios registrados WorkSpaces, paquetes personalizados, imágenes y grupos de control de acceso IP.

  Uso de la etiqueta de asignación de costos

Para ver las etiquetas de WorkSpaces recursos en el Cost Explorer, active las etiquetas que ha aplicado a sus WorkSpaces recursos siguiendo las instrucciones de Activación de etiquetas de asignación de costes definidas por el usuario en la AWS Billing and Cost Management Guía del usuario de Cost Management.

Si bien las etiquetas aparecen 24 horas después de la activación, los valores asociados a esas etiquetas pueden tardar de cuatro a cinco días en aparecer en el Cost Explorer. Para que aparezcan

y proporcionen datos de costos en el Cost Explorer, WorkSpaces los recursos que se hayan etiquetado deben incurrir en cargos durante ese tiempo. Cost Explorer muestra solo los datos de costos desde el momento en que se activaron las etiquetas en adelante. No hay datos históricos disponibles en este momento.

Administrar etiquetas

Para actualizar las etiquetas de un recurso existente mediante los comandos AWS CLI create-tags y delete-tags. Para actualizaciones masivas y para automatizar la tarea en una gran cantidad de WorkSpaces recursos, Amazon WorkSpaces añade soporte para AWS Resource Groups Tag Editor. AWS Resource Groups El editor de etiquetas te permite añadir, editar o eliminar AWS etiquetas tanto de tus WorkSpaces recursos como de otros AWS recursos.

Cuotas WorkSpaces de servicio de Amazon

Service Quotas facilita la búsqueda del valor de una cuota en particular, también denominada límite. También puedes buscar todas las cuotas de un servicio en particular.

Para ver tus cuotas de WorkSpaces

1. Navegue a la consola Service Quotas.
2. En el panel de navegación de la izquierda, selecciona AWS servicios.
3. Selecciona Amazon WorkSpaces de la lista o introduce Amazon WorkSpaces en el campo de búsqueda con anticipación.
4. Para ver información adicional sobre una cuota, como su descripción y el nombre de recurso de Amazon (ARN), elija el nombre de la cuota.

Amazon WorkSpaces proporciona diferentes recursos que puedes usar en tu cuenta en una región determinada, como imágenes WorkSpaces, paquetes, directorios, alias de conexión y grupos de control de IP. Cuando crea su cuenta de Amazon Web Services, se establecen cuotas predeterminadas (también denominadas límites) en la cantidad de recursos que puede crear.

Puede usar la consola Service Quotas para ver las cuotas de servicio predeterminadas o para solicitar aumentos de cuota para las cuotas ajustables.

Para obtener más información, consulte Ver las cuotas de servicio y Solicitar un aumento de cuota en la Guía del usuario de Service Quotas.

Automatizar el despliegue de Amazon WorkSpaces

Con Amazon WorkSpaces, puede lanzar un escritorio de Microsoft Windows o Amazon Linux en cuestión de minutos y conectarse a su software de escritorio y acceder a él desde una red local o externa de forma segura, fiable y rápida. Puedes automatizar el aprovisionamiento de Amazon WorkSpaces para poder WorkSpaces integrar Amazon en tus flujos de trabajo de aprovisionamiento existentes.

Métodos de automatización habituales WorkSpaces

Los clientes pueden utilizar una serie de herramientas para permitir una rápida WorkSpaces implementación de Amazon. Las herramientas se pueden utilizar para simplificar la administración WorkSpaces, reducir los costes y crear un entorno ágil que pueda ampliarse y moverse con rapidez.

AWS CLI y API

Existen operaciones de la WorkSpaces API de Amazon que puedes utilizar para interactuar con el servicio de forma segura y a escala. Todas las API públicas están disponibles con el AWS CLI SDK y las herramientas PowerShell, mientras que las API privadas, como la creación de imágenes, solo están disponibles a través del AWS Management Console. Al considerar la gestión operativa y el autoservicio empresarial para Amazon WorkSpaces, ten en cuenta que WorkSpaces las API requieren experiencia técnica y permisos de seguridad para su uso.

Las llamadas a la API se pueden realizar mediante el AWS SDK. AWS Tools for Windows PowerShell y AWS Tools for PowerShell Core son PowerShell módulos basados en la funcionalidad expuesta por el AWS SDK para .NET. Estos módulos le permiten programar operaciones en AWS los recursos desde la línea de PowerShell comandos e integrarlos con las herramientas y los servicios existentes. Por ejemplo, las llamadas a la API permiten gestionar automáticamente el WorkSpaces ciclo de vida mediante la integración con AD para aprovisionar y desmantelar en WorkSpaces función de la pertenencia del usuario a un grupo de AD.

AWS CloudFormation

AWS CloudFormation le permite modelar toda su infraestructura en un archivo de texto. Esta plantilla se convierte en la única fuente de información fiable para su infraestructura. Esto le ayuda a estandarizar los componentes de infraestructura que se utilizan en su organización, lo que permite cumplir con la configuración y agilizar la resolución de problemas.

AWS CloudFormation aprovisiona sus recursos de forma segura y repetible, lo que le permite crear y reconstruir su infraestructura y sus aplicaciones. Puede utilizarla CloudFormation para poner en marcha y desmantelar entornos, lo que resulta útil cuando tiene varias cuentas que quiere crear y desmantelar de forma repetible. Al considerar la gestión operativa y el autoservicio empresarial para Amazon WorkSpaces, ten en cuenta que su uso AWS CloudFormationrequiere experiencia técnica y permisos de seguridad.

Portal de autoservicio WorkSpaces

Los clientes pueden usar comandos de WorkSpaces API integrados y otros AWS servicios para crear un portal de WorkSpaces autoservicio. Esto ayuda a los clientes a optimizar el proceso de implementación y recuperación WorkSpaces a escala. Al utilizar un WorkSpaces portal, puede permitir que sus WorkSpaces empleados dispongan de un flujo de trabajo de aprobación integrado que no requiera la intervención de TI para cada solicitud. Esto reduce los costos operativos de TI y, al mismo tiempo, ayuda a los usuarios finales a empezar con WorkSpaces mayor rapidez. El flujo de trabajo de aprobación integrado adicional simplifica el proceso de aprobación de escritorios para las empresas. Un portal dedicado puede ofrecer una herramienta automatizada para aprovisionar escritorios en la nube Windows o Linux y permitir a los usuarios reconstruir, reiniciar o migrar sus escritorios en la nube WorkSpace, además de proporcionar una función para restablecer las contraseñas.

Hay ejemplos guiados sobre la creación de WorkSpaces portales de autoservicio a los que se hace referencia en la sección de lectura adicional de este documento. AWS Los socios proporcionan portales de WorkSpaces administración preconfigurados a través del AWS Marketplace.

Integración con la gestión de servicios de TI empresariales

A medida que las empresas adoptan Amazon WorkSpaces como su solución de escritorio virtual a gran escala, es necesario implementar o integrarse con los sistemas de administración de servicios de TI (ITSM). La integración de ITSM permite ofrecer ofertas de autoservicio para el aprovisionamiento y las operaciones. El Service Catalog le permite administrar de forma centralizada los AWS servicios que se implementan habitualmente y los productos de software aprovisionados. Este servicio ayuda a su organización a cumplir requisitos de gobernanza y conformidad coherentes y, al mismo tiempo, permite a los usuarios implementar solo los AWS servicios aprobados que necesitan. El Service Catalog se puede usar para habilitar una oferta de administración del ciclo de vida de autoservicio para WorkSpaces Amazon desde herramientas de administración de servicios de TI como. ServiceNow

WorkSpaces Mejores prácticas de automatización del despliegue

Debe tener en cuenta los principios de Well Architected a la hora de seleccionar y diseñar la automatización de la WorkSpaces implementación.

- Diseño para la automatización: diseñe para ofrecer la menor intervención manual posible en el proceso a fin de permitir la repetibilidad y la escalabilidad.
- Diseñe para optimizar los costos: al crear y recuperar automáticamente WorkSpaces, puede reducir el esfuerzo administrativo necesario para proporcionar recursos y evitar que los recursos inactivos o no utilizados generen costos innecesarios.
- Diseñe para lograr la eficiencia: minimice los recursos necesarios para crear y terminar. WorkSpaces Siempre que sea posible, proporcione capacidades de autoservicio de nivel 0 para que la empresa mejore la eficiencia.
- Diseñe para lograr flexibilidad: cree un mecanismo de implementación coherente que pueda gestionar varios escenarios y escalarse con el mismo mecanismo (personalizado con identificadores de perfil y casos de uso etiquetados).
- Diseñe pensando en la productividad: diseñe sus WorkSpaces operaciones para permitir la autorización y la validación correctas a la hora de añadir o eliminar recursos.
- Diseño para la escalabilidad: pay-as-you el modelo móvil que WorkSpaces utiliza Amazon puede generar ahorros de costos al crear recursos según sea necesario y eliminarlos cuando ya no sean necesarios.
- Diseñe pensando en la seguridad: diseñe sus WorkSpaces operaciones para permitir la autorización y la validación correctas a la hora de añadir o eliminar recursos.
- Diseñe para garantizar la compatibilidad: diseñe sus WorkSpaces operaciones de manera que cuenten con mecanismos y procesos de soporte y recuperación no invasivos.

WorkSpaces Parches y actualizaciones in situ de Amazon

Con Amazon WorkSpaces, puede gestionar los parches y las actualizaciones mediante herramientas de terceros existentes, como Microsoft System Center Configuration Manager (SCCM), Puppet Enterprise o Ansible. La implementación local de los parches de seguridad suele mantener un ciclo de parches mensual, con procesos adicionales para escalarlos o implementarlos rápidamente. Sin embargo, en el caso de las actualizaciones locales del sistema operativo o de las funciones, a menudo es necesario tener en cuenta algunas consideraciones especiales.

WorkSpace mantenimiento

Amazon WorkSpaces tiene un período de mantenimiento predeterminado durante el cual WorkSpace instala las actualizaciones de los WorkSpaces agentes de Amazon y cualquier actualización del sistema operativo disponible. WorkSpaces no estará disponible para las conexiones de los usuarios durante el período de mantenimiento programado.

- AlwaysOn WorkSpaces el período de mantenimiento predeterminado es de las 00h00 a las 04h00, en la zona horaria del WorkSpace, todos los domingos por la mañana.

- La redirección de zona horaria está habilitada de forma predeterminada y puede anular la ventana predeterminada para que coincida con la zona horaria local del usuario.
- Puede deshabilitar la redirección de zona horaria para Windows WorkSpaces mediante la política de grupo. Puede deshabilitar la redirección de zonas horarias para Linux WorkSpaces mediante la configuración del agente PCoIP.

- AutoStop WorkSpaces se inician automáticamente una vez al mes para instalar actualizaciones importantes. A partir del tercer lunes del mes y durante un máximo de dos semanas, el período de mantenimiento estará abierto todos los días entre las 00:00 y las 05:00 horas, en la zona horaria de la región correspondiente al AWS . WorkSpace Se WorkSpace puede mantener cualquier día del período de mantenimiento.

- Aunque no puede modificar la zona horaria que se utiliza para el mantenimiento AutoStop WorkSpaces, puede desactivar el período de mantenimiento para usted AutoStop WorkSpaces.

- Los períodos de mantenimiento manual se pueden configurar según la programación que prefiera configurando el estado del en WorkSpace ADMIN_MAINTENANCE.

- El AWS CLI comando se modify-workspace-statepuede utilizar para modificar el WorkSpace estado a ADMIN_MAINTENANCE.

Amazon Linux WorkSpaces

Para conocer las consideraciones, los requisitos previos y los patrones sugeridos para administrar actualizaciones y parches en las imágenes WorkSpaces personalizadas de Amazon Linux, consulte

el documento técnico Mejores prácticas para preparar las imágenes de Amazon WorkSpaces para Linux.

Requisitos previos y consideraciones sobre la aplicación de parches en Linux

- Los repositorios de Amazon Linux están alojados en depósitos de Amazon Simple Storage Service (Amazon S3) a los que se puede acceder a través de puntos de enlace públicos accesibles a Internet o puntos de enlace privados. Si su Amazon Linux WorkSpaces no tiene acceso a Internet, consulte este proceso para hacer que las actualizaciones sean accesibles: ¿Cómo puedo actualizar yum o instalar paquetes sin acceso a Internet en mis instancias EC2 que ejecutan Amazon Linux 1 o Amazon Linux 2?
- No puede configurar el período de mantenimiento predeterminado para Linux. WorkSpaces Si se requiere la personalización de esta ventana, se puede utilizar el proceso de mantenimiento manual.

Parches en Amazon Windows

De forma predeterminada, sus Windows WorkSpaces están configurados para recibir actualizaciones de Windows Update que requieren acceso a Internet desde su WorkSpaces VPC. Para configurar sus propios mecanismos de actualización automática para Windows, consulte la documentación de Windows Server Update Services (WSUS) y Configuration Manager.

Actualización local de Amazon Windows

- Si planea crear una imagen desde un sistema Windows 10 WorkSpace, tenga en cuenta que la creación de imágenes no es compatible con los sistemas Windows 10 que se hayan actualizado desde una versión anterior (una actualización de una función o versión de Windows). Sin embargo, el proceso de creación y captura de WorkSpaces imágenes admite las actualizaciones acumulativas o de seguridad de Windows.

- Las imágenes personalizadas Bring Your Own License (BYOL) de Windows 10 deberían comenzar con la versión más reciente compatible de Windows en una máquina virtual como fuente del proceso de importación BYOL: consulte la documentación de importación de BYOL para obtener más información.

Requisitos previos para la actualización local de Windows

- Si ha aplazado o pausado las actualizaciones de Windows 10 mediante la política de grupo de Active Directory o SCCM, habilite las actualizaciones del sistema operativo para su Windows 10. WorkSpaces
- Si WorkSpace es una AutoStop WorkSpace, cambie el AutoStop tiempo a al menos tres horas para adaptarlo al período de actualización.
- El proceso de actualización in situ recrea el perfil de usuario mediante una copia de Default User (C:\Users\Default). No utilice el perfil de usuario predeterminado para realizar personalizaciones. En su lugar, se recomienda realizar cualquier personalización del perfil de usuario mediante objetos de política de grupo (GPO). Las personalizaciones realizadas a través de los GPO se pueden modificar o revertir fácilmente y son menos propensas a cometer errores.
- El proceso de actualización local sólo permite realizar una copia de seguridad y volver a crear un perfil de usuario. Si tiene varios perfiles de usuario en la unidad D, elimine todos los perfiles excepto el que necesita.

Consideraciones sobre la actualización local de Windows

- El proceso de actualización local utiliza dos scripts de registro (enable-inplace-upgrade.ps1 y update-pvdrivers.ps1) para realizar los cambios necesarios y permitir que se ejecute el proceso de Windows Update. WorkSpaces Estos cambios implican la creación de un perfil de usuario temporal en la unidad C en lugar de en la unidad D. Si ya existe un perfil de usuario en la unidad D, los datos de ese perfil de usuario original permanecen en la unidad D.
- Una vez implementada la actualización local, debe restaurar los perfiles de usuario en la unidad D para asegurarse de que puede reconstruir o migrar los suyos WorkSpaces y evitar posibles problemas con la redirección de las carpetas del shell de usuario. Para ello, utilice la clave de registro PostUpgradeRestoreProfileOnD, tal y como se explica en la página de referencia sobre la actualización de BYOL.

Paquetes de WorkSpaces idiomas de Amazon

WorkSpaces Los paquetes de Amazon que proporcionan la experiencia de escritorio de Windows 10 admiten inglés (EE. UU.), francés (Canadá), coreano y japonés. Sin embargo, puedes incluir paquetes de idiomas adicionales para español, italiano, portugués y muchas más opciones de

idiomas. Para obtener más información, consulte ¿Cómo se crea una nueva WorkSpace imagen de Windows con un idioma de cliente distinto del inglés? .

Gestión de WorkSpaces perfiles de Amazon

Amazon WorkSpaces separa el perfil de usuario del sistema operativo (SO) base redirigiendo todas las escrituras de perfil a un volumen independiente de Amazon Elastic Block Store (Amazon EBS). En Microsoft Windows, el perfil de usuario se almacena en D:\Users\username. En Amazon Linux, el perfil de usuario se almacena en /home. El volumen de EBS se captura automáticamente cada 12 horas. La instantánea se almacena automáticamente en un depósito de S3 AWS gestionado, para utilizarla en caso de que WorkSpace se reconstruya o restaure un Amazon.

Para la mayoría de las organizaciones, disponer de instantáneas automáticas cada 12 horas es mejor que la implementación de escritorio existente sin copias de seguridad para los perfiles de usuario. Sin embargo, los clientes pueden necesitar un control más detallado de los perfiles de usuario; por ejemplo, migrar del escritorio a WorkSpaces un nuevo sistema operativo o AWS región, admitir la recuperación ante desastres, etc. Amazon dispone de métodos alternativos para la gestión de perfiles WorkSpaces.

Redirección de carpetas

Si bien la redirección de carpetas es una consideración de diseño común en las arquitecturas de infraestructura de escritorio virtual (VDI), no es una práctica recomendada ni siquiera un requisito común en los diseños de Amazon. WorkSpaces La razón de esto es que Amazon WorkSpaces es una solución de escritorio como servicio (DaaS) persistente, en la que los datos de las aplicaciones y los usuarios se conservan listos para usar.

Hay situaciones específicas en las que es necesaria la redirección de carpetas para las carpetas del shell de usuario (por ejemplo, D:\Users\username\Desktop redireccionado a\\ Server\ RedirectionShare $\ username\ Desktop), como el objetivo de punto de recuperación inmediata (RPO) para los datos del perfil de usuario en entornos de recuperación ante desastres (DR).

Prácticas recomendadas

Se enumeran las siguientes prácticas recomendadas para una redirección de carpetas sólida:

- Aloje los servidores de archivos de Windows en la misma AWS región y zona en la que WorkSpaces se lanzó Amazon.

- Asegúrese de que las reglas de entrada del grupo de seguridad de AD incluyan el grupo de seguridad del servidor de archivos de Windows o las direcciones IP privadas; de lo contrario, asegúrese de que el firewall local permita ese mismo tráfico basado en los puertos TCP y UDP.
- Asegúrese de que las reglas de entrada de los grupos de seguridad de Windows File Server incluyan TCP 445 (SMB) para todos los grupos de WorkSpaces seguridad de Amazon.
- Cree un grupo de seguridad de AD para que WorkSpaces los usuarios de Amazon autoricen el acceso de los usuarios al recurso compartido de archivos de Windows.
- Utilice el espacio de nombres DFS (DFS-N) y la replicación DFS (DFS-R) para garantizar que su recurso compartido de archivos de Windows sea ágil, no esté vinculado a nadie a un servidor de archivos de Windows específico y que todos los datos de los usuarios se repliquen automáticamente entre los servidores de archivos de Windows.
- Añada «$» al final del nombre del recurso compartido para ocultar el recurso compartido que aloja los datos de los usuarios al navegar por los recursos compartidos de la red en el Explorador de Windows.
- Cree el recurso compartido de archivos siguiendo las instrucciones de Microsoft para las carpetas redirigidas: Implemente la redirección de carpetas con archivos sin conexión. Siga atentamente las instrucciones sobre los permisos de seguridad y la configuración de los GPO.
- Si tu WorkSpaces implementación de Amazon es Bring Your Own License (BYOL), también debes especificar la desactivación de los archivos sin conexión siguiendo las instrucciones de Microsoft: deshabilitar los archivos sin conexión en carpetas individuales redirigidas.
- Instale y ejecute la deduplicación de datos (también denominada «deduplicación») si su servidor de archivos de Windows es Windows Server 2016 o una versión posterior para reducir el consumo de almacenamiento y optimizar los costes. Consulte Instalar y habilitar la deduplicación de datos y Ejecutar la deduplicación de datos.
- Realice copias de seguridad de los archivos compartidos del servidor de archivos de Windows mediante las soluciones de respaldo organizativas existentes.

¿Qué hay que evitar

- No utilice servidores de archivos de Windows a los que solo se pueda acceder a través de una conexión de red de área amplia (WAN), ya que el protocolo SMB no está diseñado para ese uso.
- No utilice el mismo recurso compartido de archivos de Windows que se utiliza en los directorios principales para reducir las posibilidades de que los usuarios eliminen accidentalmente sus carpetas de User Shell.

- Si bien se recomienda habilitar el servicio Volume Shadow Copy (VSS) para facilitar la restauración de archivos, esto por sí solo no elimina la necesidad de hacer copias de seguridad de los recursos compartidos de archivos del servidor de archivos de Windows.

Otras consideraciones

- Amazon FSx for Windows File Server ofrece un servicio gestionado para los recursos compartidos de archivos de Windows y simplifica la sobrecarga operativa de la redirección de carpetas, incluidas las copias de seguridad automáticas.
- Utilice SMB File Share AWS Storage Gateway para hacer copias de seguridad de sus archivos compartidos si no existe una solución de copia de seguridad organizacional existente.

Configuración del perfil

Políticas de grupo

Una práctica recomendada habitual en las implementaciones empresariales de Microsoft Windows consiste en definir la configuración del entorno de usuario mediante la configuración del objeto de política de grupo (GPO) y de las preferencias de política de grupo (GPP). Los ajustes, como los atajos, las asignaciones de unidades, las claves de registro y las impresoras, se definen mediante la Consola de administración de políticas de grupo. Las ventajas de definir el entorno de usuario mediante los GPO incluyen, entre otras, las siguientes:

- Administración centralizada de la configuración
- Perfil de usuario definido por la pertenencia al grupo de seguridad de AD o la ubicación de la unidad organizativa
- Protección contra la eliminación de la configuración
- Automatice la creación y personalización de perfiles en el primer inicio de sesión
- Facilidad de futuras actualizaciones

> **Note**
>
> Siga las prácticas recomendadas de Microsoft para optimizar el rendimiento de las políticas de grupo.

No se deben utilizar las políticas grupales de banners de inicio de sesión interactivos, ya que Amazon WorkSpaces no los admite. Los banners se presentan en el WorkSpaces Cliente de Amazon a través de solicitudes de AWS soporte. Además, los dispositivos extraíbles no deben bloquearse mediante la política de grupo, ya que son necesarios para Amazon WorkSpaces.

Los GPO se pueden usar para administrar Windows WorkSpaces. Para obtener más información, consulte Administre su Windows WorkSpaces.

WorkSpaces Volúmenes de Amazon

Cada WorkSpaces instancia de Amazon contiene dos volúmenes: un volumen del sistema operativo y un volumen de usuarios.

- Amazon Windows WorkSpaces: la unidad C:\ se usa para el sistema operativo (SO) y la unidad D:\ es el volumen de usuarios. El perfil de usuario se encuentra en el volumen de usuario (documentosAppData, imágenes, descargas, etc.).
- Amazon Linux WorkSpaces: en Amazon Linux WorkSpace, el volumen del sistema (/dev/xvda1) se monta como carpeta raíz. El volumen de usuarios es para aplicaciones y datos de usuario; /dev/xvdf1 se monta como /home.

Para los volúmenes del sistema operativo, puede seleccionar un tamaño inicial para esta unidad de 80 GB o 175 GB. Para los volúmenes de usuario, puede seleccionar un tamaño inicial de 10 GB, 50 GB o 100 GB. Se puede aumentar el tamaño de ambos volúmenes hasta 2 TB según sea necesario; sin embargo, para aumentar el volumen de usuarios más allá de los 100 GB, el volumen del sistema operativo debe ser de 175 GB. Los cambios de volumen solo se pueden realizar una vez cada seis horas por volumen. Para obtener información adicional sobre la modificación del tamaño del WorkSpaces volumen, consulte la WorkSpace sección Modificar un volumen de la Guía de administración.

WorkSpaces volúmenes: prácticas recomendadas

Al planificar una WorkSpaces implementación de Amazon, se recomienda tener en cuenta los requisitos mínimos para la instalación del sistema operativo, las actualizaciones in situ y las aplicaciones principales adicionales que se añadirán a la imagen del volumen del sistema operativo. Para el volumen de usuarios, se recomienda empezar con una asignación de disco más pequeña y aumentar gradualmente el tamaño del volumen de usuarios según sea necesario. Al minimizar el tamaño de los volúmenes de disco se reduce el coste de ejecución del WorkSpace.

> **Note**
>
> Si bien se puede aumentar el tamaño de un volumen, no se puede reducir.

WorkSpaces Registro de Amazon

En un WorkSpaces entorno de Amazon, hay muchas fuentes de registro que se pueden capturar para solucionar problemas y supervisar el WorkSpaces rendimiento general.

Amazon WorkSpaces Client 3.x En cada WorkSpaces cliente de Amazon, los registros del cliente se encuentran en los siguientes directorios:

- Windows: %LOCALAPPDATA%\ Amazon Web Services\ Amazon\ logs WorkSpaces
- macOS — ~/Library/"Application Support» /"Amazon Web Services» /"Amazon «/logs WorkSpaces
- Linux (Ubuntu 18.04 o posterior) — /opt/workspacesclient/workspacesclient

Hay muchos casos en los que es posible que se necesiten detalles de diagnóstico o depuración para una sesión desde el lado del cliente. WorkSpaces También se pueden habilitar los registros avanzados de los clientes añadiendo un «-l3» al archivo ejecutable del espacio de trabajo. Por ejemplo:

```
"C:\Program Files (x86)\Amazon Web Services, Inc\Amazon WorkSpaces"
workspaces.exe -l3
```

WorkSpaces Servicio Amazon

El WorkSpaces servicio de Amazon está integrado con Amazon CloudWatch Metrics, CloudWatch Events y CloudTrail. Esta integración permite que los datos de rendimiento y las llamadas a la API se registren en el AWS servicio central.

Al gestionar un WorkSpaces entorno de Amazon, es importante supervisar constantemente determinadas CloudWatch métricas para determinar el estado general del entorno. Métricas

Si bien hay otras CloudWatch métricas disponibles para Amazon WorkSpaces (consulta Monitorea tu WorkSpaces uso de CloudWatch métricas), las tres métricas siguientes te ayudarán a mantener la disponibilidad de las WorkSpace instancias:

- Insalubre: el número de WorkSpaces ellas devolvió un estado no saludable.
- SessionLaunchTime— La cantidad de tiempo que se tarda en iniciar una WorkSpaces sesión.
- InSessionLatency— El tiempo de ida y vuelta entre el WorkSpaces cliente y el WorkSpace.

Para obtener más información sobre las opciones de WorkSpaces registro, consulta Cómo registrar las llamadas a las WorkSpaces API de Amazon mediante el uso CloudTrail. Los CloudWatch eventos adicionales ayudarán a capturar la IP del lado del cliente de la sesión del usuario, cuándo el usuario se conectó a la WorkSpaces sesión y qué punto final se utilizó durante la conexión. Todos estos detalles ayudan a aislar o identificar los problemas notificados por los usuarios durante las sesiones de solución de problemas.

> **Note**
>
> Algunas CloudWatch métricas solo están disponibles con AWS Managed AD.

Subsistema de contenedores y Windows para Linux en Amazon WorkSpaces

Contenedores y Amazon WorkSpaces

Los clientes que desean dar servicio a las cargas de trabajo de contenedores con Amazon WorkSpaces suelen abordar la informática para el usuario final. Si bien es posible, esta no es la solución preferida ni recomendada. Se recomienda encarecidamente a los clientes que deseen aprovechar los posibles ahorros operativos y de costos de los contenedores que evalúen Amazon Elastic Container Service (Amazon ECS) y/o Amazon Elastic Kubernetes Service (Amazon EKS).

En los casos en que los requisitos del cliente exigen habilitar los contenedores con Amazon WorkSpaces, se ha publicado una guía técnica que permite el uso de Docker. Se debe informar a los clientes de que esto requiere otros servicios de seguimiento y que los costes y la complejidad aumentan en comparación con los servicios de contenedores nativos y desacoplados.

Subsistema de Windows para Linux

Con el lanzamiento de Windows Server 2019 como sistema operativo subyacente de Amazon WorkSpaces, los clientes están ansiosos por implementar el Subsistema de Windows para Linux (WSL), específicamente WSL2. Como WSL2 invoca una máquina virtual (Hyper-V) para realizar sus funciones, no puede ejecutarse en Amazon WorkSpaces, que se gestiona mediante hipervisores. AWS Por este motivo, los clientes deben saber que solo estará disponible el WSL1 y comprender las diferencias entre el WSL1 y el WSL2.

Amazon WorkSpaces migrate

La función Amazon WorkSpaces Migrate te permite incorporar tus datos de volumen de usuarios a un nuevo paquete. Puede utilizar esta función para:

- Migre su experiencia WorkSpaces de Windows 7 a la experiencia de escritorio de Windows 10.
- Migre de un PCoIP WorkSpace a un protocolo de WorkSpaces transmisión (WSP). WorkSpace
- Migre WorkSpaces de un paquete público o personalizado a otro. Por ejemplo, puede migrar de paquetes (gráficos y GraphicsPro) habilitados para GPU a paquetes no habilitados para GPU y viceversa.

Proceso de migración

Con la WorkSpaces migración, puede especificar el WorkSpaces paquete de destino. El proceso de migración recrea el WorkSpace uso de un nuevo volumen raíz a partir de la imagen del paquete de destino y el volumen de usuario a partir de la última instantánea del volumen de usuarios original. Durante la migración, se genera un nuevo perfil de usuario para mejorar la compatibilidad. Los datos del perfil de usuario anterior que no se pueden mover al nuevo perfil se almacenan en la carpeta .NotMigrated.

Durante la migración, se conservan los datos del volumen de usuario (unidad D), pero se pierden todos los datos del volumen raíz (C:\ drive). Esto significa que no se conserva ninguna de las aplicaciones, configuraciones ni cambios instalados en el registro. A la antigua carpeta de perfiles de usuario se le cambia el nombre por. NotMigrated sufijo y se crea un nuevo perfil de usuario.

El proceso de migración tarda hasta una hora cada WorkSpace uno. Además, si el flujo de trabajo de migración no completa el proceso, el servicio restablecerá automáticamente el WorkSpace estado original antes de la migración, lo que minimizará cualquier riesgo de pérdida de datos.

Todas las etiquetas asignadas al original WorkSpace se conservan durante la migración. WorkSpace Se conserva el modo de ejecución del. El migrado WorkSpace tiene un nuevo WorkSpace identificador, nombre de equipo y dirección IP. Procedimiento de migración

Puede realizar la migración WorkSpaces a través de la WorkSpaces consola de Amazon, AWS CLI mediante el comando migrate-workspace o la API de Amazon WorkSpaces . Todas las solicitudes de migración se ponen en cola y el servicio reducirá automáticamente el número total de solicitudes de migración si son demasiadas. Límites de migración

- No puede migrar a un paquete de experiencia de escritorio de Windows 7 público o personalizado.
- No puede migrar a paquetes BYOL para Windows 7.
- WorkSpaces Solo puede migrar BYOL a otros paquetes BYOL.
- No puedes migrar un paquete WorkSpace creado de un paquete público o personalizado a un paquete BYOL.
- Actualmente, no se admite la migración WorkSpaces de Linux.
- En AWS las regiones que admiten más de un idioma, puede migrar WorkSpaces entre paquetes de idiomas.
- Los paquetes de origen y destino deben ser diferentes. (Sin embargo, en las regiones que admiten más de un idioma, puede migrar al mismo paquete de Windows 10 siempre que los idiomas sean diferentes). Si quieres actualizar tu paquete WorkSpace usando el mismo paquete, reconstruye el paquete WorkSpace en su lugar.
- No puede migrar de una WorkSpaces región a otra.
- WorkSpaces no se pueden migrar cuando están en modo ADMIN_MAINTENANCE.

Costo

Durante el mes en que se produce la migración, se le cobrarán importes prorrateados tanto para el nuevo como para el original. WorkSpaces Por ejemplo, si migra WorkSpace A a WorkSpace B el 10 de mayo, se le cobrará por WorkSpace A del 1 al 10 de mayo y se le cobrará por WorkSpace B del 11 al 30 de mayo.

WorkSpaces prácticas recomendadas de migración

Antes de migrar un WorkSpace, haga lo siguiente:

- Realice una copia de seguridad de los datos importantes de la unidad C en otra ubicación. Todos los datos de la unidad C se borrarán durante la migración.
- Asegúrese de WorkSpace que la migración tenga al menos 12 horas de antigüedad para asegurarse de que se ha creado una instantánea del volumen de usuarios. En la WorkSpaces página Migrate de la WorkSpaces consola de Amazon, puedes consultar la hora de la última instantánea. Los datos creados después de la última instantánea se pierden durante la migración.
- Para evitar una posible pérdida de datos, asegúrate de que tus usuarios cierren WorkSpaces la sesión y no la vuelvan a iniciar hasta que finalice el proceso de migración.
- Asegúrese de que el estado que WorkSpaces desea migrar sea DISPONIBLE, DETENIDO o ERROR.

- Asegúrese de que tiene suficientes direcciones IP para la WorkSpaces migración. Durante la migración, se asignarán nuevas direcciones IP a. WorkSpaces
- Si utiliza scripts para migrar WorkSpaces, migre los archivos en lotes de no más de 25 WorkSpaces a la vez.

Marco de buena arquitectura

AWS WellArchitected ayuda a los arquitectos de la nube a crear una infraestructura segura, de alto rendimiento, resiliente y eficiente para sus aplicaciones y cargas de trabajo. Describe los conceptos clave, los principios de diseño y las mejores prácticas arquitectónicas para diseñar y ejecutar cargas de trabajo en la nube. Se basa en cinco pilares clave:

- Excelencia operativa
- Seguridad
- Fiabilidad
- Eficiencia del rendimiento
- Optimización de costos

Al diseñar la arquitectura de un WorkSpaces entorno de Amazon, es importante evaluar estos pilares clave para determinar el nivel de madurez del despliegue y descubrir funciones adicionales que se pueden utilizar con Amazon WorkSpaces. Si AWS bien existe una guía general para el marco Well-Architect, a continuación se ofrecen algunas preguntas clave que pueden incluirse en la fase de planificación de la WorkSpaces implementación para garantizar que se tengan en cuenta cada uno de los cinco pilares.

General

- ¿Cuál es el motor empresarial de este proyecto?

Excelencia operativa

- ¿Cómo se segrega el control de acceso entre los usuarios y los diferentes grupos de administradores?

Seguridad

1. ¿Cuáles son los requisitos de seguridad y conformidad que deben tenerse en cuenta WorkSpaces para operar?
2. ¿Hay alguna restricción en el enrutamiento a direcciones IP externas?

3. ¿Se permite el paso de WorkSpaces los puertos necesarios a través del firewall corporativo?
4. ¿Se utiliza o se utilizará la autenticación multifactorial en esta implementación?
5. ¿Cuántas identidades de usuario y solicitudes de autorización se gestionan en la actualidad?

Fiabilidad

1. ¿Cuál es la política de retención de datos para ordenadores de sobremesa?
2. ¿Qué es el objetivo del punto de recuperación (RPO) para los datos de los usuarios finales?
3. ¿Qué es el objetivo de tiempo de recuperación (RTO) de los datos de los usuarios finales?

Optimización de costos

1. ¿Los WorkSpaces paquetes tienen el tamaño adecuado para el caso de usuario y las aplicaciones?
2. ¿Los usuarios consumirán WorkSpaces más de 82 horas al mes?

Si bien las preguntas anteriores no constituyen una lista exhaustiva de los elementos que deben tenerse en cuenta, proporcionan una guía general para ayudarlo con una implementación de Well-Architected Amazon. WorkSpaces

Seguridad

En esta sección se explica cómo proteger los datos mediante el cifrado cuando se utilizan WorkSpaces los servicios de Amazon. Describe el cifrado en tránsito y en reposo, y el uso de grupos de seguridad para proteger el acceso a la red WorkSpaces. En esta sección también se proporciona información sobre cómo controlar el acceso de los dispositivos finales WorkSpaces mediante dispositivos de confianza y grupos de control de acceso IP.

En esta sección encontrará información adicional sobre la autenticación (incluida la compatibilidad con MFA) en AWS Directory Service.

Cifrado en tránsito

Amazon WorkSpaces utiliza la criptografía para proteger la confidencialidad en las diferentes etapas de la comunicación (en tránsito) y también para proteger los datos en reposo (cifrados WorkSpaces). Los procesos en cada etapa del cifrado utilizado por Amazon WorkSpaces en tránsito se describen en las siguientes secciones.

Para obtener información sobre el cifrado en reposo, consulta la WorkSpaces sección Cifrado de este documento.

Registro y actualizaciones

La aplicación cliente de escritorio se comunica con Amazon para las actualizaciones y el registro mediante HTTPS.

Etapa de autenticación

El cliente de escritorio inicia la autenticación enviando las credenciales a la pasarela de autenticación. La comunicación entre el cliente de escritorio y la puerta de enlace de autenticación utiliza HTTPS. Al final de esta etapa, si la autenticación se realiza correctamente, la pasarela de autenticación devuelve un token de OAuth 2.0 al cliente de escritorio, a través de la misma conexión HTTPS.

> **Note**
>
> La aplicación cliente de escritorio admite el uso de un servidor proxy para el tráfico del puerto 443 (HTTPS), para las actualizaciones, el registro y la autenticación.

Tras recibir las credenciales del cliente, la pasarela de autenticación envía una solicitud de autenticación a AWS Directory Service. La comunicación desde la pasarela de autenticación a AWS Directory Service se realiza a través de HTTPS, por lo que no se transmiten las credenciales de usuario en texto plano.

Autenticación: conector de Active Directory (ADC)

AD Connector usa Kerberos para establecer una comunicación autenticada con AD local, de modo que pueda vincularse a LDAP y ejecutar consultas LDAP posteriores. El soporte LDAPS del lado del cliente en ADC también está disponible para cifrar consultas entre Microsoft AD y Applications. AWS Antes de implementar la funcionalidad LDAPS del lado del cliente, revise los requisitos previos del LDAPS del lado del cliente.

El AWS Directory Service también admite LDAP con TLS. No se transmite ninguna credencial de usuario en texto plano en ningún momento. Para aumentar la seguridad, es posible conectar una WorkSpaces VPC a la red local (donde reside AD) mediante una conexión VPN. Al utilizar una conexión VPN de AWS hardware, los clientes pueden configurar el cifrado en tránsito mediante IPSEC estándar (SA de intercambio de claves de Internet (IKE) e IPSEC) con claves de cifrado simétricas AES-128 o AES-256, SHA-1 o SHA-256 para el hash de integridad y grupos DH (2,14-18, 22, 23 y 24 para la fase 1; 1,2,5, 14-18, 22, 23 y 24 para la fase 2) mediante el secreto directo perfecto (PFS).

Etapa de intermediario

Tras recibir el token de OAuth 2.0 (desde la pasarela de autenticación, si la autenticación se realizó correctamente), el cliente de escritorio consulta los WorkSpaces servicios de Amazon (Broker Connection Manager) mediante HTTPS. El cliente de escritorio se autentica mediante el envío del token OAuth 2.0 y, como resultado, el cliente recibe la información del punto final de la pasarela de streaming. WorkSpaces

Etapa de streaming

El cliente de escritorio solicita abrir una sesión PCoIP con la pasarela de streaming (mediante el token OAuth 2.0). Esta sesión está cifrada con AES-256 y utiliza el puerto PCoIP para el control de la comunicación (4172/TCP).

Mediante el token OAuth2.0, la pasarela de streaming solicita la WorkSpaces información específica del usuario al WorkSpaces servicio de Amazon, a través de HTTPS.

La pasarela de streaming también recibe el TGT del cliente (que se cifra con la contraseña del usuario del cliente) y, mediante la transferencia TGT de Kerberos, la puerta de enlace inicia un inicio de sesión de Windows en él, utilizando el TGT de Kerberos recuperado por el WorkSpace usuario.

A WorkSpace continuación, inicia una solicitud de autenticación al AWS Directory Service configurado mediante la autenticación Kerberos estándar.

Una vez que WorkSpace se haya iniciado sesión correctamente, se iniciará la transmisión de PCoIP. El cliente inicia la conexión en el puerto TCP 4172 y el tráfico de retorno en el puerto UDP 4172. Además, la conexión inicial entre la pasarela de streaming y un WorkSpaces ordenador de sobremesa a través de la interfaz de administración se realiza mediante el UDP 55002. (Consulte la documentación para conocer los requisitos de dirección IP y puerto de Amazon WorkSpaces. El puerto UDP de salida inicial es 55002. La conexión de streaming, que utiliza los puertos 4172 (TCP y UDP), se cifra mediante cifrados AES de 128 y 256 bits, pero de forma predeterminada es de 128 bits. Los clientes pueden cambiarlo activamente a 256 bits, ya sea mediante la configuración de política de grupo de AD específica de PCoIP para Windows o con el archivo WorkSpaces pcoip-agent.conf para Amazon Linux. WorkSpaces Para obtener más información sobre la administración de políticas de grupo para Amazon WorkSpaces, consulta la documentación.

Interfaces de red

Cada Amazon WorkSpace tiene dos interfaces de red, denominadas interfaz de red principal e interfaz de red de administración.

La interfaz de red principal proporciona conectividad a los recursos de la VPC del cliente, como el acceso a AWS Directory Service, Internet y la red corporativa del cliente. Es posible conectar grupos de seguridad a esta interfaz de red principal. Conceptualmente, los grupos de seguridad se diferencian adscritos a este ENI en función del alcance del despliegue: grupo de WorkSpaces seguridad y grupos de seguridad ENI.

Interfaz de red de administración

La interfaz de la red de administración no se puede controlar mediante grupos de seguridad; sin embargo, los clientes pueden usar un firewall basado en un host WorkSpaces para bloquear los puertos o controlar el acceso. No recomendamos aplicar restricciones a la interfaz de la red de administración. Si un cliente decide añadir reglas de firewall basadas en el host para administrar esta interfaz, deben estar abiertos algunos puertos para que el WorkSpaces servicio de Amazon pueda gestionar el estado y la accesibilidad de la WorkSpace. Para obtener más información, consulte Interfaces de red en la Guía de administración de Amazon Workspaces.

WorkSpaces grupos de seguridad

Se crea un grupo de seguridad predeterminado por cada AWS Directory Service y se adjunta automáticamente a todos los WorkSpaces que pertenecen a ese directorio específico.

Amazon WorkSpaces, como muchos otros AWS servicios, utiliza grupos de seguridad. Amazon WorkSpaces crea dos grupos de AWS seguridad al registrar un directorio en el WorkSpaces servicio. Uno para los controladores de directorio DirectoryID_Controllers y otro para WorkSpaces el directorio DirectoryID_WorkspacesMembers. No elimine ninguno de estos grupos de seguridad o se verá afectado. WorkSpaces De forma predeterminada, la salida del grupo de seguridad WorkSpaces Members está abierta en 0.0.0.0/0. Puede agregar un grupo de WorkSpaces seguridad predeterminado a un directorio. Después de asociar un nuevo grupo de seguridad a un WorkSpaces directorio, el nuevo grupo de seguridad WorkSpaces que inicie o el existente WorkSpaces que reconstruya tendrá el nuevo grupo de seguridad. También puede agregar este nuevo grupo de seguridad predeterminado a los existentes WorkSpaces sin volver a crearlos. Al asociar varios grupos de seguridad a un WorkSpaces directorio, WorkSpaces agregue las reglas de cada grupo de seguridad en un único conjunto de reglas. Recomendamos condensar las reglas de grupo de seguridad tanto como sea posible. Para obtener más información sobre los grupos de seguridad, consulte Grupos de seguridad para su VPC en la Guía del usuario de Amazon VPC.

Para obtener más información sobre cómo añadir un grupo de seguridad a un WorkSpaces directorio o a uno existente WorkSpace, consulte la guía de administración. WorkSpaces

Algunos clientes desean restringir los puertos y destinos por los que puede salir el WorkSpaces tráfico. Para restringir el tráfico de salida desde allí WorkSpaces, debe asegurarse de dejar los puertos específicos necesarios para la comunicación del servicio; de lo contrario, sus usuarios no podrán iniciar sesión en los suyos. WorkSpaces

WorkSpaces utilice la interfaz de red elástica (ENI) en la VPC del cliente para comunicarse con los controladores de dominio durante el inicio de WorkSpace sesión. Para permitir que sus usuarios inicien sesión WorkSpaces correctamente, debe permitir que los siguientes puertos accedan a sus controladores de dominio o a los rangos de CIDR que incluyen sus controladores de dominio en el grupo de seguridad _WorkspacesMembers.

- TCP/UDP 53: DNS
- TCP/UDP 88: autenticación de Kerberos
- TCP 389 — LDAP
- TCP/UDP 445: SMB

- TCP 3268-3269: catálogo global
- TCP/UDP 464: cambio de contraseña de Kerberos
- TCP 139: Netlogon
- UDP 137-138: Netlogon
- UDP 123: NTP
- TCP/UDP 49152-65535 Puertos efímeros para RPC

Si WorkSpaces necesita acceder a otras aplicaciones, Internet u otras ubicaciones, tendrá que permitir esos puertos y destinos en notación CIDR dentro del grupo de seguridad _WorkspacesMembers. Si no agrega esos puertos y destinos, no WorkSpaces llegarán a ningún otro puerto que no sea el indicado anteriormente. Una última consideración: de forma predeterminada, un nuevo grupo de seguridad no tiene reglas de entrada. Por lo tanto, no se permitirá el tráfico entrante que proceda de otro host a su instancia hasta que no añada reglas entrantes al grupo de seguridad. Los pasos anteriores solo son necesarios si desea restringir la salida WorkSpaces o establecer reglas de entrada restringidas únicamente a los recursos o rangos de CIDR que deberían tener acceso a ellos.

> **Note**
>
> Un grupo de seguridad recién asociado solo se adjuntará si se WorkSpaces crea o se reconstruye después de la modificación.

Grupos de seguridad ENI

Como la interfaz de red principal es una ENI normal, se puede gestionar mediante las diferentes herramientas AWS de gestión. Para obtener más información, consulte Elastic Network Interfaces. Navegue hasta la dirección WorkSpace IP (en la WorkSpaces página de la WorkSpaces consola de Amazon) y, a continuación, utilice esa dirección IP como filtro para encontrar el ENI correspondiente (en la sección Interfaces de red de la consola Amazon EC2).

Una vez localizado el ENI, los grupos de seguridad pueden gestionarlo directamente. Al asignar grupos de seguridad manualmente a la interfaz de red principal, tenga en cuenta los requisitos de puerto de Amazon WorkSpaces. Para obtener más información, consulte Interfaces de red en la Guía de administración de Amazon Workspaces.

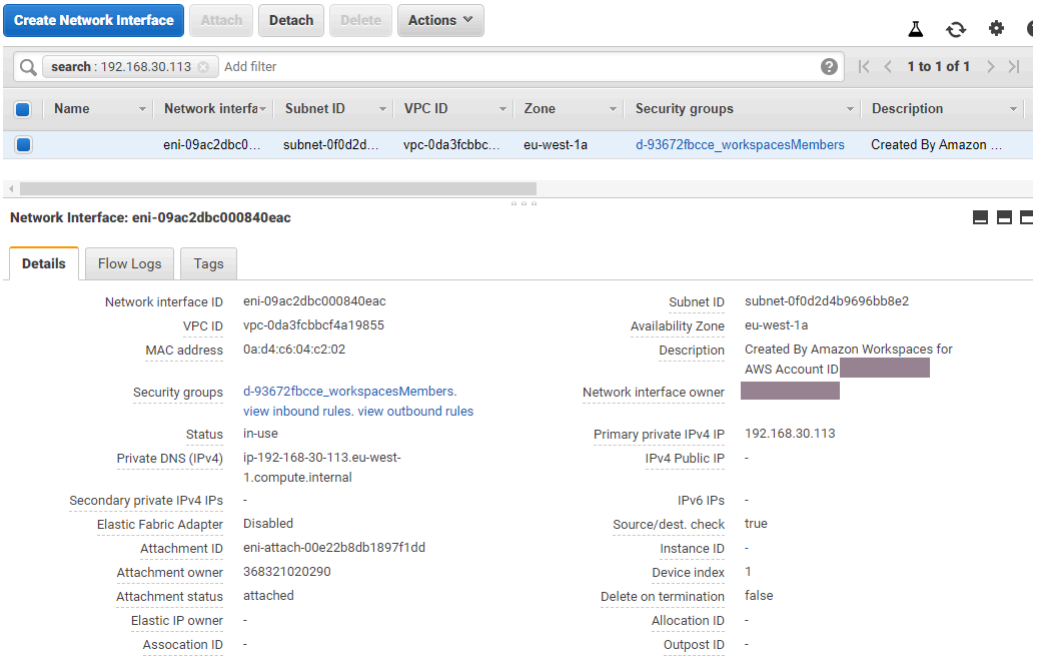

Figura 21: WorkSpaces cliente con MFA activado

Listas de control de acceso (ACL) de red

Debido a la complejidad añadida que supone gestionar otro firewall, las ACL de red se suelen utilizar en despliegues muy complejos y, por lo general, no se utilizan como práctica recomendada. Como las ACL de red están conectadas a las subredes de la VPC, su función se centra en la capa 3 (red) del modelo OSI. Debido a que Amazon WorkSpaces está diseñado en Directory Services, se deben definir dos subredes. Las ACL de red se administran por separado de los servicios de directorio, y es muy probable que una ACL de red se asigne solo a una de las WorkSpaces «subredes» asignadas.

Cuando se requiere un firewall sin estado, las ACL de red son una buena práctica de seguridad. Como práctica recomendada, asegúrese de que cualquier cambio realizado en las ACL de red que supere la configuración predeterminada se valide por subred. Si las ACL de la red no funcionan según lo previsto, considere la posibilidad de utilizar los registros de flujo de la VPC para analizar el tráfico.

AWS Network Firewall

AWS Network Firewall ofrece una funcionalidad superior a la que ofrecen los grupos de seguridad y las ACL de red nativos, pero a un precio. Cuando los clientes ~~solicitaron~~ la posibilidad de aumentar la seguridad en torno a las conexiones de red, como la inspección de nombres de servidores (SNI)

para sitios web basados en HTTPS, la detección y prevención de intrusiones y una lista de nombres de dominio permitidos y rechazados, no les quedó más remedio que buscar firewalls alternativos. AWS Marketplace La complejidad de la implementación de estos firewalls planteaba desafíos que iban más allá de lo que saben hacer los administradores de la EUC estándar. AWS Network Firewall ofrece una AWS experiencia nativa al tiempo que habilita las protecciones de las capas 3 a 7. El uso de AWS Network Firewall junto con NAT Gateway es una buena práctica cuando las organizaciones no disponen de ningún otro medio (se excluyen las licencias locales existentes para firewalls de terceros que se pueden transferir a la nube o los equipos independientes que gestionan los firewalls) para cubrir todas las protecciones de red de la EUC. NAT Gateway también es gratuito con AWS Network Firewall.

Las implementaciones de AWS Network Firewall se diseñan en torno al diseño EUC existente. Los diseños de una sola VPC pueden lograr una arquitectura simplificada con subredes para los puntos finales del firewall y consideraciones de enrutamiento de salida de Internet independientes, mientras que los diseños de múltiples VPC se benefician enormemente de una VPC de inspección consolidada con firewalls y puntos finales de Transit Gateways.

Escenarios de diseño

Escenario 1: Bloqueo de instancias básico

El grupo WorkSpaces de seguridad predeterminado no permite el tráfico entrante, ya que los grupos de seguridad están denegados de forma predeterminada y están en estado activo. Esto significa que no es necesario configurar configuraciones adicionales para proteger aún más las propias WorkSpaces instancias. Tenga en cuenta las reglas de salida que permiten todo el tráfico y si se ajustan al caso de uso. Por ejemplo, puede ser mejor denegar todo el tráfico saliente del puerto 443 a cualquier dirección y rangos de IP específicos que se adapten a los casos de uso de los puertos, como 389 para LDAP, 636 para LDAPS, 445 para SMB, entre otros; aunque tenga en cuenta que la complejidad del entorno puede requerir varias reglas y, por lo tanto, estar mejor atendido a través de ACL de red o un dispositivo de firewall.

Escenario 2: Excepciones entrantes

Si bien no es un requisito constante, puede haber ocasiones en las que el tráfico de red se inicie de entrada a. WorkSpaces Por ejemplo, la clasificación de los casos en los que el WorkSpaces cliente no puede conectarse requiere una conectividad remota alternativa. En estos casos, es mejor habilitar temporalmente el TCP 3389 entrante en el grupo de seguridad del ENI WorkSpace del cliente.

Otro escenario son los scripts organizativos que ejecutan comandos para funciones de inventario o automatización, iniciados por una instancia centralizada. La protección del tráfico de ese puerto desde esas instancias centralizadas específicas de la interfaz entrante se puede configurar de forma permanente. Sin embargo, se recomienda hacerlo en el grupo de seguridad adicional adjunto a la configuración del directorio, ya que se puede aplicar a varias implementaciones de la AWS cuenta.

Por último, hay parte del tráfico de red que no está basado en el estado y requerirá que se especifiquen los puertos efímeros en las excepciones de entrada. Si las consultas y los scripts fallan, se recomienda permitir los puertos efímeros, al menos temporalmente, y determinar la causa principal del fallo de conectividad.

Escenario 3: Inspección de VPC única

Las implementaciones simplificadas de WorkSpaces (como una sola VPC sin planes de escalado) no requieren una VPC independiente para la inspección y, por lo tanto, la conexión a otras VPC se puede simplificar con la interconexión de VPC. Sin embargo, se deben crear subredes separadas para los puntos finales del firewall con el enrutamiento configurado para esos puntos finales, así como el enrutamiento de salida de Internet Gateway (IGW), que de otro modo no necesitaría configurarse. Es posible que las implementaciones existentes no tengan el espacio IP disponible si todas las subredes utilizan todo el bloque CIDR de la VPC. En esos casos, el escenario 4 puede funcionar mejor, ya que la implementación ya ha superado su diseño inicial.

Escenario 4: Inspección centralizada

Suele preferirse en varios despliegues de EUC en una AWS región, lo que simplifica la administración de las reglas con y sin estado del firewall de AWS red. Los pares de VPC existentes se sustituirán por Transit Gateways, ya que este diseño requiere el uso de adjuntos de Transit Gateway, así como el enrutamiento de inspección que solo se puede configurar a través de esos accesorios. También se ejerce un mayor grado de control sobre esta configuración y permite una seguridad que va más allá de la experiencia predeterminada. WorkSpaces

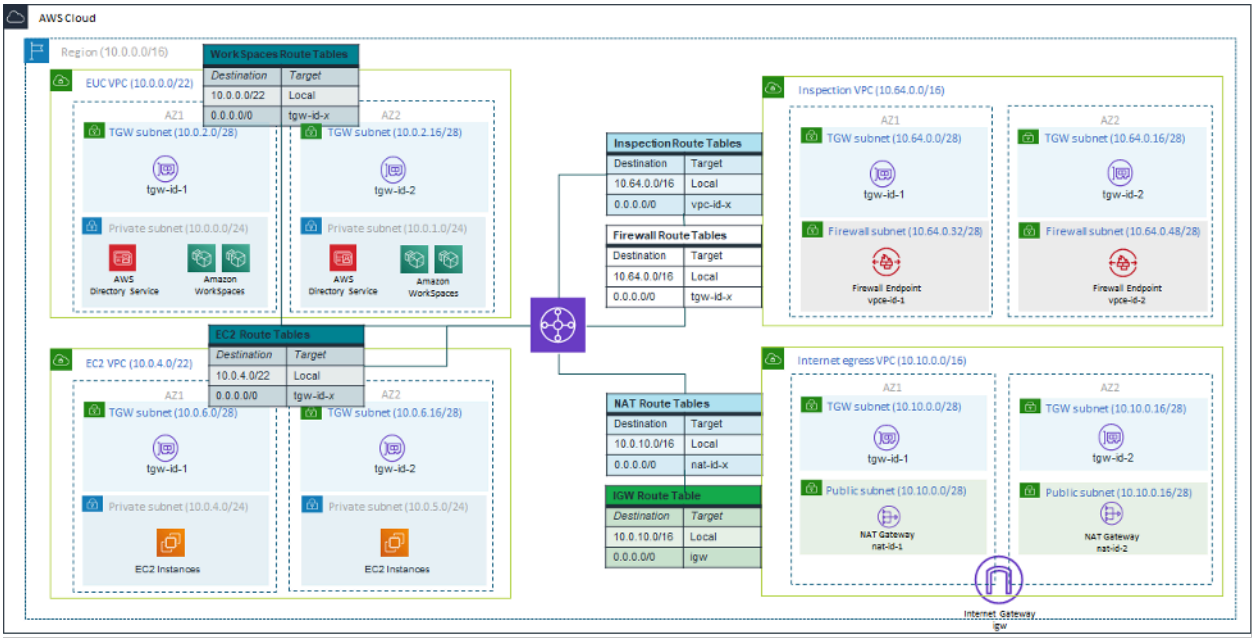

Figura 22: Ejemplo de arquitectura con accesorios Transit Gateway

Cifrado WorkSpaces

Cada Amazon WorkSpace se aprovisiona con un volumen raíz (C: unidad para Windows WorkSpaces, raíz para Amazon Linux WorkSpaces) y un volumen de usuario (D: unidad para Windows WorkSpaces, /home para Amazon Linux WorkSpaces). La WorkSpaces función de cifrado permite cifrar uno o ambos volúmenes.

¿Qué se cifra?

Todos los datos almacenados en reposo, la entrada/salida (E/S) del disco en el volumen y las instantáneas creadas a partir de volúmenes cifrados están cifrados.

¿Cuándo se produce el cifrado?

El cifrado de a WorkSpace debe especificarse al lanzar (crear) el WorkSpace. WorkSpaces los volúmenes solo se pueden cifrar en el momento del lanzamiento: tras el lanzamiento, el estado de cifrado del volumen no se puede cambiar. La siguiente figura muestra la página de la WorkSpaces consola de Amazon para elegir el cifrado durante el lanzamiento de un nuevo WorkSpace.

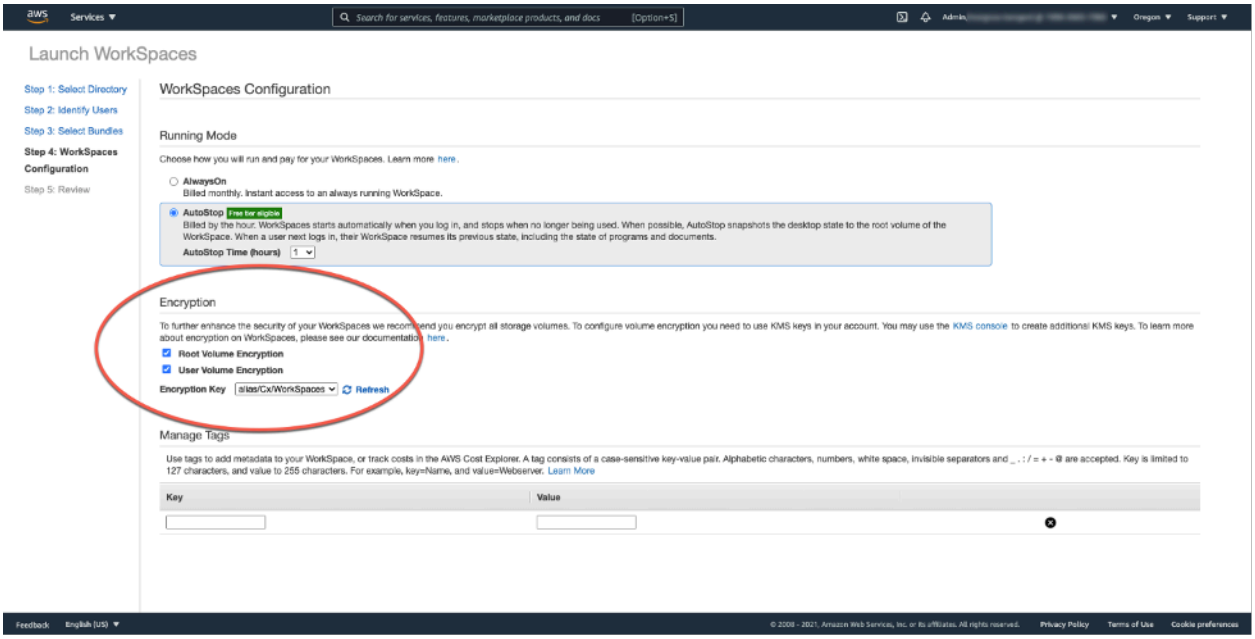

Figura 23: Cifrado WorkSpace de volúmenes raíz

¿Cómo se WorkSpace cifra una nueva?

Un cliente puede elegir la WorkSpaces opción cifrada desde la WorkSpaces consola de Amazon o mediante la WorkSpaces API de Amazon cuando un cliente lanza una nueva WorkSpace. AWS CLI

Para cifrar los volúmenes, Amazon WorkSpaces utiliza una CMK de AWS Key Management Service ()AWS KMS. La primera vez que se lanza a en una región WorkSpace se crea una AWS KMS CMK predeterminada. (Las CMK tienen un ámbito regional).

Un cliente también puede crear una CMK gestionada por el cliente para utilizarla cifrada. WorkSpaces La CMK se utiliza para cifrar las claves de datos que utiliza el WorkSpaces servicio de Amazon para cifrar cada uno de los volúmenes. WorkSpace (En sentido estricto, Amazon EBS cifrará los volúmenes). Para conocer los límites actuales de CMK, consulte Cuotas de recursos. AWS KMS

> **Note**
>
> No se admite la creación de imágenes personalizadas a partir de un archivo cifrado WorkSpace . Además, si WorkSpaces se lanza con el cifrado del volumen raíz activado, el aprovisionamiento puede tardar hasta una hora.

Para obtener una descripción detallada del proceso de WorkSpaces cifrado, consulta Cómo lo WorkSpaces usa Amazon AWS KMS. Ten en cuenta cómo se supervisará el uso de la CMK para garantizar que una solicitud de cifrado WorkSpace se tramite correctamente. Para obtener información adicional sobre AWS KMS las claves y las claves de datos, consulte la AWS KMS página.

Opciones de control de acceso y dispositivos de confianza

Amazon WorkSpaces ofrece a los clientes opciones para gestionar los dispositivos cliente a los que pueden acceder WorkSpaces. Los clientes pueden limitar el WorkSpaces acceso únicamente a dispositivos de confianza. WorkSpaces Se puede permitir el acceso desde ordenadores macOS y Microsoft Windows mediante certificados digitales. También puede permitir o bloquear el acceso para iOS, Android, Chrome OS, Linux y cero clientes, así como para el cliente WorkSpaces Web Access. Con estas capacidades, puede mejorar aún más la postura de seguridad.

Las opciones de control de acceso están habilitadas para las nuevas implementaciones para que los usuarios accedan a sus clientes WorkSpaces desde Windows, macOS, iOS, Android, ChromeOS y Zero Clients. El acceso mediante Web Access o un WorkSpaces cliente Linux no está habilitado de forma predeterminada para una nueva WorkSpaces implementación y será necesario habilitarlo.

Si hay límites en el acceso a los datos corporativos desde dispositivos de confianza (también conocidos como dispositivos gestionados), el WorkSpaces acceso puede restringirse a dispositivos de confianza con certificados válidos. Cuando esta función está habilitada, Amazon WorkSpaces utiliza la autenticación basada en certificados para determinar si un dispositivo es de confianza. Si la aplicación WorkSpaces cliente no puede verificar que un dispositivo es de confianza, bloquea los intentos de iniciar sesión o volver a conectarse desde el dispositivo.

La compatibilidad con dispositivos de confianza está disponible para los siguientes clientes:

- Aplicación Amazon WorkSpaces Android Client en Google Play que se ejecuta en dispositivos Android y Chrome OS compatibles con Android
- Aplicación Amazon WorkSpaces macOS Client que se ejecuta en dispositivos macOS
- Aplicación Amazon WorkSpaces Windows Client que se ejecuta en dispositivos Windows

Para obtener más información sobre cómo controlar los dispositivos a los que se puede acceder WorkSpaces, consulte Restringir el WorkSpaces acceso a dispositivos de confianza.

> **Note**
>
> Los certificados para dispositivos de confianza solo se aplican a los clientes de Amazon WorkSpaces Windows, macOS y Android. Esta función no se aplica al cliente Amazon WorkSpaces Web Access ni a ningún cliente de terceros, incluidos, entre otros, el software PCoIP y los clientes móviles de Teradici, los clientes cero de PCoIP de Teradici, los clientes RDP y las aplicaciones de escritorio remoto.

Grupos de control de acceso IP

Al usar grupos de control basados en direcciones IP, los clientes pueden definir y administrar grupos de direcciones IP confiables y permitir que los usuarios accedan a ellos WorkSpaces solo cuando están conectados a una red confiable. Esta función ayuda a los clientes a tener un mayor control sobre su postura de seguridad.

Los grupos de control de acceso IP se pueden agregar a nivel de WorkSpaces directorio. Hay dos maneras de empezar a utilizar los grupos de control de acceso IP.

- Página de controles de acceso IP: desde la consola de WorkSpaces administración, se pueden crear grupos de control de acceso IP en la página de controles de acceso IP. Las reglas se pueden agregar a estos grupos introduciendo las direcciones IP o los rangos de IP desde los que se WorkSpaces puede acceder. Luego, estos grupos se pueden agregar a los directorios de la página de detalles de la actualización.
- API de espacio de trabajo: WorkSpaces las API se pueden usar para crear, eliminar y ver grupos; crear o eliminar reglas de acceso; o para agregar y eliminar grupos de los directorios.

Para obtener una descripción detallada del uso de grupos de control de acceso IP con el proceso de WorkSpaces cifrado de Amazon, consulte Grupos de control de acceso IP para usted WorkSpaces.

Supervisión o registro mediante Amazon CloudWatch

La supervisión de la red, los servidores y los registros es una parte integral de cualquier infraestructura. Los clientes que despliegan Amazon WorkSpaces necesitan monitorear sus despliegues, específicamente el estado general y de conexión de la persona WorkSpaces.

CloudWatch Métricas de Amazon para WorkSpaces

CloudWatch metrics for WorkSpaces está diseñado para proporcionar a los administradores información adicional sobre el estado general de salud y de conexión de una persona WorkSpaces. Las métricas están disponibles por WorkSpace organización o agregadas para todos WorkSpaces los miembros de una organización dentro de un directorio determinado.

Estas métricas, como todas CloudWatch las métricas, se pueden ver en AWS Management Console (se muestra en la siguiente figura), se puede acceder a ellas a través de las CloudWatch API y se pueden supervisar mediante CloudWatch alarmas y herramientas de terceros.

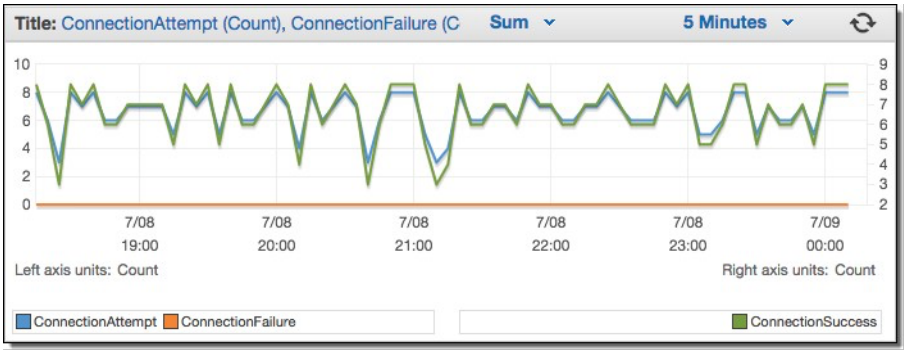

Figura 24: CloudWatch métricas: ConnectionAttempt / ConnectionFailure

De forma predeterminada, las siguientes métricas están habilitadas y están disponibles sin coste adicional:

- Disponibles: las WorkSpaces que responden a una verificación de estado se cuentan en esta métrica.
- En mal estado: los WorkSpaces que no responden a la misma verificación de estado se tienen en cuenta en esta métrica.
- ConnectionAttempt— El número de intentos de conexión realizados a un WorkSpace.
- ConnectionSuccess— El número de intentos de conexión correctos.
- ConnectionFailure— El número de intentos de conexión fallidos.
- SessionLaunchTime— El tiempo que se tarda en iniciar una sesión, medido por el WorkSpaces cliente.
- InSessionLatency— El tiempo de ida y vuelta entre el WorkSpaces cliente y WorkSpaces, medido e informado por el cliente.
- SessionDisconnect— El número de sesiones iniciadas por el usuario y cerradas automáticamente.

Además, se pueden crear alarmas, como se muestra en la siguiente figura.

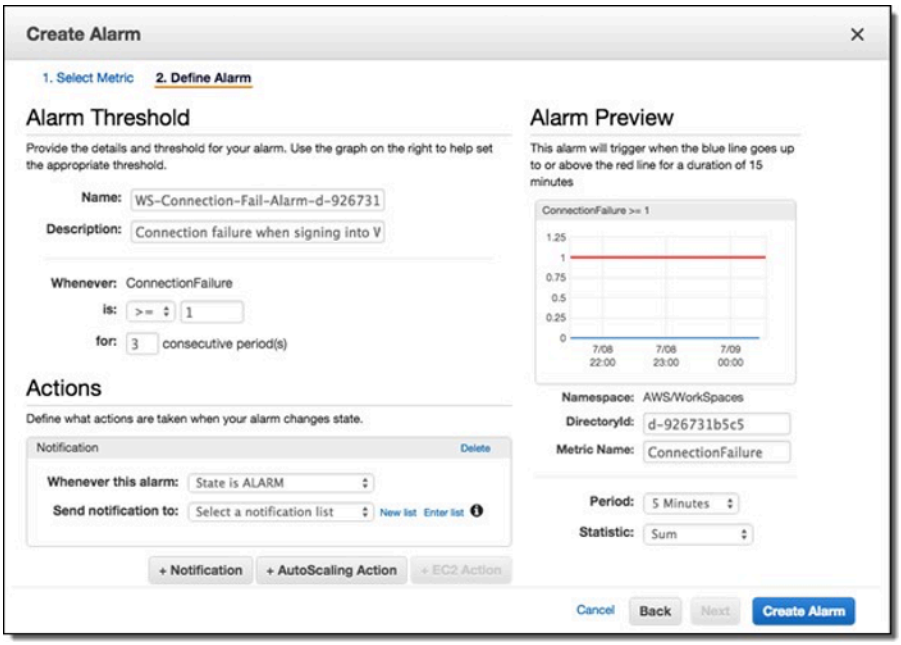

Figura 25: Crear una CloudWatch alarma por errores de WorkSpaces conexión

Amazon CloudWatch Events para WorkSpaces

Los eventos de Amazon CloudWatch Events se pueden usar para ver, buscar, descargar, archivar, analizar y responder a los inicios de sesión correctos. WorkSpaces El servicio puede monitorear las direcciones IP de la WAN del cliente, el sistema operativo, el WorkSpaces ID y la información de ID de directorio para los inicios de sesión de los usuarios. WorkSpaces Por ejemplo, puede usar los eventos para los siguientes fines:

- Guarde o archive los eventos de inicio de WorkSpaces sesión como registros para consultarlos en el futuro, analice los registros para buscar patrones y tome medidas en función de esos patrones.
- Utilice la dirección IP de la WAN para determinar desde dónde han iniciado sesión los usuarios y, a continuación, utilice políticas que permitan a los usuarios acceder únicamente a los archivos o datos desde los WorkSpaces que se cumplan los criterios de acceso que figuran en el tipo de CloudWatch evento de WorkSpaces acceso.
- Utilizar los controles de las políticas para bloquear el acceso a los archivos y aplicaciones desde direcciones IP no autorizadas.

Para obtener más información sobre cómo usar CloudWatch Events, consulta la Guía del usuario de Amazon CloudWatch Events. Para obtener más información sobre CloudWatch Events for WorkSpaces, consulte Supervise su WorkSpaces uso de Cloudwatch Events.

YubiKey soporte para Amazon WorkSpaces

Para añadir una capa de seguridad adicional, los clientes suelen optar por proteger las herramientas y los sitios con autenticación multifactorial. Algunos clientes optan por hacerlo con un YubiKey Yubico. Amazon WorkSpaces admite códigos de acceso de un solo uso (OTP) y el protocolo de autenticación FIDO U2F con. YubiKeys

Amazon admite WorkSpaces actualmente el modo OTP y no se requieren pasos adicionales por parte del administrador o usuario final para utilizar un modo YubiKey con OTP. El usuario puede conectarlos YubiKey a su ordenador, asegurarse de que el teclado esté centrado en el interior del teclado WorkSpace (específicamente en el campo en el que hay que introducir la OTP) y tocar el contacto dorado de la. YubiKey YubiKey Introducirá automáticamente la OTP en el campo seleccionado.

Para utilizar el modo FIDO U2F con YubiKey y WorkSpaces, se requieren pasos adicionales. Asegúrese de que sus usuarios dispongan de uno de estos YubiKey modelos compatibles para poder utilizar la redirección U2F con: WorkSpaces

- YubiKey 4.
- YubiKey 5 NFC
- YubiKey 5 Nano
- YubiKey 5C
- YubiKey Nano 5C
- YubiKey 5 NFC

Para habilitar la redirección USB para U2F YubiKey

De forma predeterminada, la redirección USB está deshabilitada para el PCoIP WorkSpaces; para utilizar el modo U2F con, debe habilitarla. YubiKeys

1. Asegúrese de haber instalado la plantilla administrativa de política de WorkSpacesgrupo más reciente para PCoIP (32 bits) o la plantilla administrativa de política de WorkSpacesgrupo para PCoIP (64 bits) más reciente.

2. En una instancia de administración de directorios WorkSpace o de Amazon EC2 que esté unida a su WorkSpaces directorio, abra la herramienta de administración de políticas de grupo (gpmc.msc) y vaya a Variables de sesión de PCoIP.
3. Para permitir que el usuario anule su configuración, seleccione Valores predeterminados de administrador anulables. De lo contrario, selecciona Valores predeterminados del administrador que no se pueden anular.
4. Abra la opción Activar/desactivar USB en la sesión de PCoIP.
5. Seleccione Habilitada y, a continuación, elija OK.
6. Abra la opción configuración de reglas de dispositivos permitidos y no permitidos de PCoIP USB.
7. Seleccione Habilitado y, en Introducir la tabla de autorización USB (máximo diez reglas), configure las reglas de la lista de dispositivos USB permitidos.
   a. Regla de autorización: 110500407 Este valor es una combinación de un ID de proveedor (VID) y un ID de producto (PID). El formato de una combinación VID/PID es`1xxxxyyyy`, donde `xxxx` está el VID en formato hexadecimal y `yyyy` el PID en formato hexadecimal. Para este ejemplo, 1050 es el VID, y 0407 es el PID. Para obtener más valores de YubiKey USB, consulte los valores de ID de YubiKey USB.
8. En Introduzca la tabla de autorización USB (diez reglas como máximo), configure las reglas de la lista de dispositivos USB bloqueados.
   a. Para Regla de desautorización, establezca una cadena vacía. Esto significa que solo se permiten los dispositivos USB de la lista de autorización.

   > **Note**
   >
   > Puede definir un máximo de 10 reglas de autorización USB y un máximo de 10 reglas de desautorización USB. Utilice el carácter de barra vertical (|) para separar varias reglas. Para obtener información detallada sobre las reglas de autorización/desautorización, consulte Teradici PCoIP Standard Agent para Windows

9. Seleccione Aceptar.
10. El cambio en la configuración de la política de grupo surtirá efecto después de la siguiente actualización de la política de grupo y después de que se reinicie la sesión. WorkSpace WorkSpace Para aplicar los cambios de la directiva de grupo, realice una de las siguientes acciones:
    a. Reinicie el WorkSpace (en la WorkSpaces consola de Amazon, seleccione y WorkSpace, a continuación, elija Acciones, Reiniciar WorkSpaces).

b. En una línea de comandos administrativa, escriba gpupdate /force.

11. Una vez que la configuración surta efecto, se podrá redirigir a todos los dispositivos USB compatibles, a WorkSpaces menos que se configuren las restricciones mediante la configuración de las reglas de los dispositivos USB.

Una vez que hayas activado la redirección USB para YubiKey U2F, podrás utilizar el modo U2F de Fido. YubiKey

Optimización de costos

Capacidades de administración de autoservicio WorkSpace

En Amazon WorkSpaces, las capacidades WorkSpace de administración de autoservicio se pueden habilitar para que los usuarios tengan más control sobre su experiencia. Permitir a los usuarios la capacidad de autoservicio puede reducir la carga de trabajo del personal de soporte de TI para Amazon WorkSpaces. Cuando las capacidades de autoservicio están habilitadas, los usuarios pueden realizar una o más de las siguientes tareas directamente desde su cliente Windows, macOS o Linux para Amazon WorkSpaces:

- Almacene en caché sus credenciales en su cliente. Esto permite a los usuarios volver a conectarse a ellos WorkSpace sin tener que volver a introducir sus credenciales.
- Reinicie sus. WorkSpace
- Aumente el tamaño de los volúmenes raíz y de usuario de sus WorkSpace.
- Cambie el tipo de procesamiento (paquete) de sus WorkSpace.
- Cambie el modo de ejecución de sus WorkSpace.
- Reconstruye sus WorkSpace.

Permitir a los usuarios las opciones de reinicio y reconstrucción para sus usuarios no tiene implicaciones de costo continuas WorkSpaces. Los usuarios deben saber que una reconstrucción suya WorkSpace WorkSpace hará que no estén disponibles durante un máximo de una hora, a medida que se lleve a cabo el proceso de reconstrucción.

Las opciones para aumentar el tamaño de los volúmenes, cambiar el tipo de procesamiento y cambiar el modo de ejecución pueden suponer costes adicionales. WorkSpaces Una práctica recomendada es habilitar el autoservicio para reducir la carga de trabajo del equipo de soporte. El autoservicio para los gastos adicionales debe incluirse en un proceso de flujo de trabajo que garantice que se ha obtenido la autorización para cubrir los gastos adicionales. Esto puede realizarse a través de un portal de autoservicio específico o mediante la integración con los servicios de gestión de servicios de tecnología de la información (ITSM) existentes, por ejemplo. WorkSpaces ServiceNow

Para obtener información más detallada, consulte Cómo habilitar las capacidades de WorkSpace administración de autoservicio para sus usuarios. Para ver un ejemplo que describe cómo habilitar un

portal estructurado para el autoservicio de los usuarios, consulta Automatizar Amazon WorkSpaces con un portal de autoservicio.

Optimizador WorkSpaces de costes de Amazon

La solución Amazon WorkSpaces Cost Optimizer analiza todos tus datos de WorkSpaces uso de Amazon. En función del uso, convierte automáticamente la WorkSpace opción de facturación en la más rentable (por hora o por mes). Esta solución le ayuda a supervisar su WorkSpace consumo y AWS CloudFormation a optimizar los costes, además de aprovisionar y configurar automáticamente los AWS servicios necesarios para analizar el uso cada 24 horas y realizar conversiones individuales WorkSpaces. La última versión, la 2.4, ofrece a los clientes la flexibilidad de implementar la solución en una VPC existente y configurarla de forma opcional para la región y la terminación. También mejoró la precisión de los cálculos de las horas de facturación WorkSpaces y mejoró los metadatos de los informes. Si ya implementó una versión anterior (v2.2.1 o inferior) de esta solución, consulte la documentación de la pila de actualizaciones para actualizar la pila de Amazon WorkSpaces Cost Optimizer CloudFormation y obtener la versión más reciente del marco de la solución.

El modo de ejecución de a WorkSpace determina su disponibilidad y facturación inmediatas. Estos son los modos de WorkSpaces ejecución actuales:

AlwaysOn— Úselo cuando pague una tarifa mensual fija para un uso ilimitado de WorkSpaces. Este modo es el mejor para los usuarios que utilizan su WorkSpace escritorio principal y necesitan acceso instantáneo a una versión WorkSpace en funcionamiento en todo momento.

AutoStop— Úselo cuando pague WorkSpaces por horas. Con este modo, WorkSpaces deténgase después de un período de inactividad específico y se guardará el estado de las aplicaciones y los datos. Para configurar la hora de parada automática, usa AutoStop Hora (horas). Este modo es el mejor para los usuarios que solo necesitan acceder a sus dispositivos a tiempo parcial WorkSpaces.

Una buena práctica es monitorear el uso y configurar el modo WorkSpaces de funcionamiento de Amazon para que sea el más rentable utilizando una solución como Amazon WorkSpaces Cost Optimizer. Esta solución implementa una regla de CloudWatch eventos de Amazon que invoca una AWS Lambdafunción cada 24 horas.

Esta solución puede convertir un modelo WorkSpaces de facturación individual de un modelo de facturación por horas a un modelo de facturación mensual cualquier día después de alcanzar el umbral. Si la solución convierte una WorkSpace facturación por hora en una facturación mensual, no WorkSpace vuelve a convertir la facturación en facturación por horas hasta principios del mes

siguiente y solo si el uso estaba por debajo del umbral. Sin embargo, el modelo de facturación se puede cambiar manualmente en cualquier momento mediante la WorkSpaces API AWS Management Console o Amazon. La AWS CloudFormation plantilla de la solución incluye los parámetros que ejecutarán estas conversiones y permiten ejecutar la solución en modo de ejecución sin procesar para proporcionar informes sobre las recomendaciones.

Optar por no usar etiquetas

Para evitar que la solución convierta a de un modelo de WorkSpace facturación a otro, aplique una etiqueta de recurso al mismo WorkSpace utilizando la clave de etiqueta Skip_Convert y cualquier valor de etiqueta. Esta solución registrará las etiquetas WorkSpaces, pero no las convertirá. WorkSpaces Elimine la etiqueta en cualquier momento para reanudar la conversión automática WorkSpace. Para obtener más información, consulta Amazon WorkSpaces Cost Optimizer.

Optar por regiones

De forma predeterminada, esta solución monitoriza WorkSpaces todas las AWS regiones disponibles buscando directorios registrados WorkSpaces en Amazon en la misma AWS cuenta. Puedes proporcionar una lista separada por comas de AWS las regiones que deseas monitorear en el parámetro de entrada Lista de AWS regiones para limitar las regiones que deseas monitorear.

Implementación en una VPC existente

Esta solución requiere una VPC para ejecutar la tarea de ECS. De forma predeterminada, la solución creará una nueva VPC, pero puede implementarla en una VPC existente proporcionando los ID de subred y el ID del grupo de seguridad como parte del parámetro de entrada. Su subred actual tiene una ruta a Internet para que la tarea de ECS extraiga la imagen de Docker alojada en un repositorio público de Amazon ECR.

Terminación de la no utilizada WorkSpaces

Esta solución le permite cancelar el servicio no utilizado WorkSpaces el último día del mes cuando se hayan cumplido todos los criterios. Puede activar esta función cambiando el parámetro TerminateUnusedWorkSpacesde entrada a la CloudFormation plantilla. Una buena práctica consiste en ejecutar esta función en modo de prueba durante un par de meses y revisar los informes mensuales para revisar lo que WorkSpaces está marcado para ser cancelado.

Optimización de Amazon Connect para Amazon WorkSpaces

La experiencia del usuario final para los agentes del centro de contacto debe ser una prioridad absoluta, ya que si su audio se degrada, se crea una mala experiencia de llamada para el cliente al que atienden. Cuando se ejecuta una solución de contact center en un escritorio remoto, el rendimiento del audio siempre se ve afectado en una escala medible si no se prioriza el tráfico de voz por encima de la conexión de red. Este impacto se debe a que el audio fluye desde el terminal de audio a la sesión virtual y luego se comprime a través del protocolo de transmisión para entregarlo al usuario final. Este enrutamiento adicional hace que el audio tenga un rendimiento degradado debido a los cuellos de botella de la red.

Un método para evitar este comportamiento consiste en dividir el audio fuera de la sesión, lo que significa que todos los recursos del agente del centro de contacto permanecen dentro de la sesión mientras que la transmisión de audio permanece fuera de la sesión. Esta división permite que el audio se transmita desde el terminal de audio directamente al usuario final, mientras que todos los demás recursos de llamada, incluida la PII que está viendo el agente, permanecen en una sesión segura. Esta optimización del audio se considera una buena práctica, ya que garantiza que la experiencia de llamada del cliente sea lo mejor posible.

Amazon Connect ofrece una API de Streams que permite a los administradores personalizar su panel de control de contactos (CCP) para cumplir con sus requisitos empresariales. Una de las opciones que tiene un administrador es controlar si el CCP personalizado puede recibir el audio de la llamada. Estos ajustes nos permiten configurar un CCP dividido: un CCP de solo audio para fuera de la sesión y un CCP sin contenido multimedia para dentro de la sesión. Una vez que los administradores hayan configurado estos CCP personalizados, podrán aprovechar la optimización de audio de Amazon Connect para WorkSpaces. Como los CCP se entregan en el navegador, esta configuración permite a los administradores proporcionar al directorio su URL de CCP de solo audio. WorkSpaces Una vez configurado, cuando los agentes del centro de contacto de WorkSpaces Connect se autentiquen correctamente en sus servidores WorkSpaces, el WorkSpaces cliente abrirá automáticamente la URL CCP de solo audio proporcionada en el navegador local predeterminado del agente. Esta acción permite que el audio fluya directamente a la máquina local del agente, mientras que el CCP, sin medios, se encarga del resto de la sesión segura. WorkSpaces

Diagrama de la arquitectura

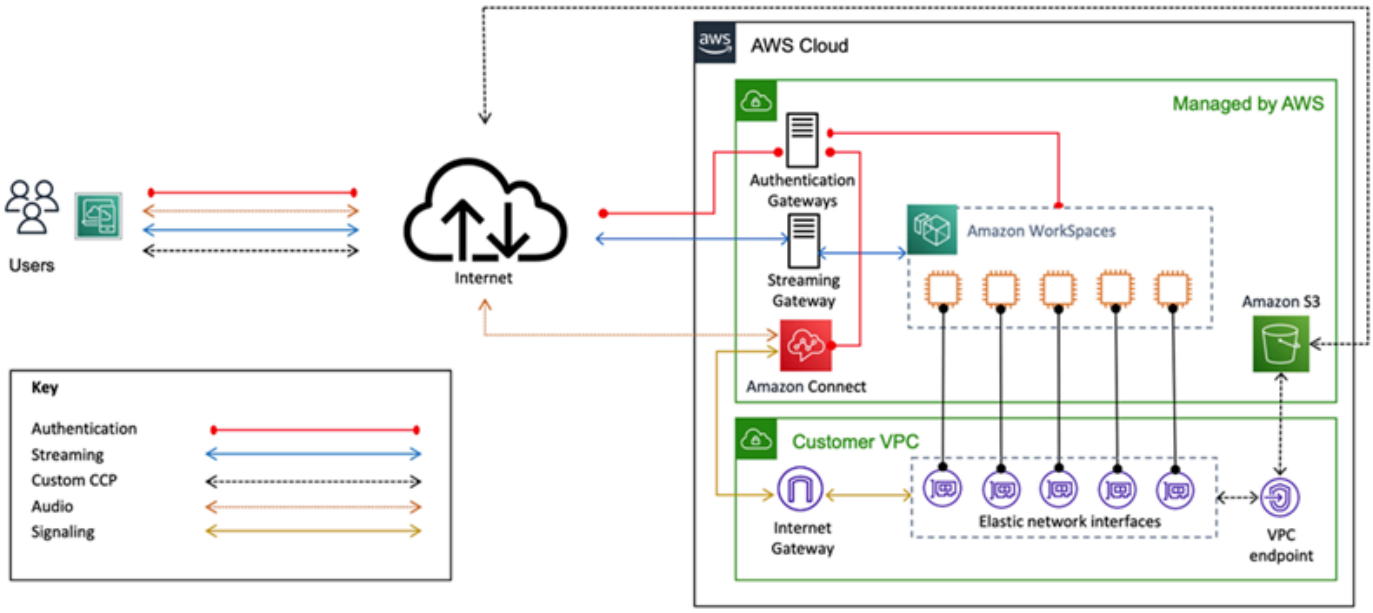

Figura 26: Amazon Connect y diagrama de WorkSpaces arquitectura

Solución de problemas

En las páginas de solución de problemas de clientes y clientes de la Guía de administración de Amazon WorkSpaces se pueden encontrar problemas frecuentes de administración y clientes, como mensajes de error como «Su dispositivo no puede conectarse al servicio de WorkSpaces registro» o «No se puede conectar a un banner de inicio de sesión interactivo». WorkSpace

Temas

- AD Connector no se puede conectar a Active Directory
- Solución de problemas de un error WorkSpace de creación de una imagen personalizada
- Solución de problemas de un Windows WorkSpace marcado como en mal estado
- Recopilación de un paquete de registros de WorkSpaces soporte para la depuración
- ¿Cómo comprobar la latencia en la AWS región más cercana

AD Connector no se puede conectar a Active Directory

Para que AD Connector se conecte al directorio local, el firewall de la red local debe tener ciertos puertos abiertos a los CIDR para ambas subredes de la VPC. Consulte el escenario 1: Uso de AD Connector para la autenticación mediante proxy en el servicio Active Directory Service local. Para comprobar si se cumplen estas condiciones, lleve a cabo los siguientes pasos.

Para probar la conexión:

1. Ejecute una instancia de Windows en la VPC y conéctese a ella a través de RDP. El resto de los pasos deben realizarse en la instancia de VPC.
2. Descarga y descomprime la aplicación de DirectoryServicePortTestprueba. El código fuente y los archivos de proyecto de Microsoft Visual Studio se incluyen para modificar la aplicación de prueba, si se desea.
3. Desde una línea de comandos de Windows, ejecute la aplicación de DirectoryServicePortTest prueba con las siguientes opciones:

```
DirectoryServicePortTest.exe -d <domain_name>
-ip <server_IP_address> -tcp "53,88,135,139,389,445,464,636,49152" -udp
 "53,88,123,137,138,389,445,464" <domain_name>
```

<domain_name>— El nombre de dominio completo, que se utiliza para probar los niveles funcionales del bosque y del dominio. Si se excluye el nombre de dominio, no se probarán los niveles funcionales.

< Server_IP_Address>: la dirección IP de un controlador de dominio del dominio local. Los puertos se comprueban con esta dirección IP. Si se excluye la dirección IP, no se probarán los puertos.

Esta prueba determina si los puertos necesarios están abiertos desde la VPC al dominio. La aplicación de prueba también comprueba los niveles funcionales mínimos del bosque y del dominio.

Solución de problemas de un error WorkSpace de creación de una imagen personalizada

Si se WorkSpace ha lanzado y personalizado un Windows o Amazon Linux, se puede crear una imagen personalizada a partir de ahí WorkSpace. Una imagen personalizada contiene el sistema operativo, el software de la aplicación y la configuración del WorkSpace.

Revise los requisitos para crear una imagen personalizada de Windows o los requisitos para crear una imagen personalizada de Amazon Linux. La creación de imágenes requiere que se cumplan todos los requisitos previos antes de que pueda comenzar la creación de imágenes.

Para confirmar que Windows WorkSpace cumple los requisitos para la creación de imágenes, se recomienda ejecutar el Comprobador de imágenes. El verificador de imágenes realiza una serie de pruebas para determinar WorkSpace cuándo se crea una imagen y proporciona instrucciones sobre cómo resolver cualquier problema que encuentre. Para obtener información detallada, consulte Instalación y configuración del comprobador de imágenes.

Una vez WorkSpace superadas todas las pruebas, aparece el mensaje «La validación se ha realizado correctamente». Ahora puedes crear un paquete personalizado. De lo contrario, resuelva cualquier problema que provoque errores y advertencias en las pruebas y repita el proceso de ejecutar el comprobador de imágenes hasta que supere todas las pruebas. WorkSpace Todos los errores y advertencias deben resolverse antes de poder crear una imagen.

Para obtener más información, siga los consejos para resolver los problemas detectados por el comprobador de imágenes.

Solución de problemas de un Windows WorkSpace marcado como en mal estado

El WorkSpaces servicio de Amazon comprueba periódicamente el estado de un WorkSpace mediante el envío de una solicitud de estado. WorkSpace Se marca como Insalubre si no se recibe una respuesta de WorkSpace él de manera oportuna. Las causas más comunes de este problema son:

- Una aplicación en el bloquea WorkSpace la conexión de red entre el WorkSpaces servicio de Amazon y el WorkSpace.
- Alto uso de la CPU en WorkSpace.
- WorkSpace Se ha cambiado el nombre de la computadora.
- El agente o servicio que responde al WorkSpaces servicio de Amazon no está en estado de ejecución.

Los siguientes pasos de solución de problemas pueden WorkSpace devolverlo a un estado correcto:

- Primero, reiníciala WorkSpace desde la WorkSpaces consola de Amazon. Si el problema no WorkSpace se resuelve al reiniciarlo, utilice RDP o conéctese a Amazon Linux WorkSpace mediante SSH.
- Si no WorkSpace se puede acceder a mediante un protocolo diferente, reconstruya el WorkSpace desde la consola de Amazon WorkSpaces .
- Si no se puede establecer una WorkSpaces conexión, compruebe lo siguiente:

Compruebe el uso de la CPU

Utilice Open Task Manager para determinar si WorkSpace se está produciendo un uso elevado de la CPU. Si es así, prueba cualquiera de los siguientes pasos de solución de problemas para resolver el problema:

1. Detenga cualquier servicio que consuma una gran cantidad de CPU.
2. Cambie el tamaño WorkSpace a un tipo de procesamiento superior al que se utiliza actualmente.
3. Reinicie el WorkSpace.

> **Note**
>
> Para diagnosticar el uso elevado de la CPU y obtener orientación si los pasos anteriores no resuelven el problema del elevado uso de la CPU, consulte ¿Cómo se diagnostica el uso elevado de la CPU en mi instancia EC2 de Windows cuando la CPU no está sobrecargada?

Compruebe el nombre de la computadora WorkSpace

Si se ha cambiado el nombre del ordenador del espacio de trabajo, cámbielo de nuevo por el nombre original:

1. Abre la WorkSpaces consola de Amazon y, a continuación, expande Unhealthy WorkSpace para ver los detalles.
2. Copia el nombre de la computadora.
3. Conéctese al RDP WorkSpace mediante.
4. Abra una línea de comandos y, a continuación, escriba el nombre de host para ver el nombre de la computadora actual.
   a. Si el nombre coincide con el nombre del equipo del paso 2, pase a la siguiente sección de solución de problemas.
   b. Si los nombres no coinciden, escriba sysdm.cpl para abrir las propiedades del sistema y, a continuación, siga los pasos restantes de esta sección.
5. Seleccione Cambiar y, a continuación, pegue el nombre del equipo del paso 2.
6. Introduzca las credenciales de usuario del dominio si se le solicita.
7. Confirme que SkyLightWorkspaceConfigServiceestá en estado de ejecución
   a. En Servicios, compruebe que el WorkSpace servicio SkyLightWorkspaceConfigService se encuentra en estado de ejecución. Si no es así, inicie el servicio.

Compruebe las reglas del firewall

Confirme que el Firewall de Windows y cualquier firewall de terceros que se esté ejecutando tengan reglas que permitan los siguientes puertos:

- TCP entrante en el puerto 4172: establece la conexión de streaming.
- UDP entrante en el puerto 4172: transmite la entrada del usuario.

- TCP entrante en el puerto 8200: administre y configure el. WorkSpace
- UDP saliente en el puerto 55002: transmisión PCoIP.

Si el firewall utiliza un filtrado sin estado, abra los puertos efímeros 49152-65535 para permitir la comunicación de retorno.

Si el firewall utiliza un filtrado con estado, el puerto efímero 55002 ya está abierto.

Recopilación de un paquete de registros de WorkSpaces soporte para la depuración

Al solucionar WorkSpaces problemas, es necesario recopilar el paquete de registros del afectado WorkSpace y del host en el que está instalado el WorkSpaces cliente. Existen dos categorías fundamentales de registros:

- Registros del lado del servidor: El WorkSpace es el servidor en este escenario, por lo que se trata de registros que residen en sí mismos. WorkSpace
- Registros del lado del cliente: se registran en el dispositivo que el usuario final está utilizando para conectarse al. WorkSpace

- Solo los clientes de Windows y macOS escriben registros localmente.
- Los clientes cero y los clientes iOS no registran.
- Los registros de Android se cifran en el almacenamiento local y se cargan automáticamente al equipo de ingeniería del WorkSpaces cliente. Solo ese equipo puede revisar los registros de los dispositivos Android.

Registros del lado del servidor WSP

Todos los componentes del WSP escriben sus archivos de registro en una de estas dos carpetas:

- Ubicación principal: `C:\ProgramData\Amazon\WSP\` y `C:\ProgramData\NICE\dcv\log\`
- Ubicación del archivo: `C:\ProgramData\Amazon\WSP\TRANSMITTED\`

Cambiar la verbosidad del archivo de registro en Windows

Puede configurar el nivel de verbosidad del archivo de registro para WSP Windows a escala configurando la configuración de política de grupo del WorkSpaces nivel de verbosidad del registro.

Para cambiar la verbosidad del archivo de registro individual WorkSpaces, configure la clave mediante el Editor del h_log_verbosity_options Registro de Windows:

1. Abra el Editor del Registro de Windows como administrador.
2. Vaya a \HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Amazon.
3. Si la WSP clave no existe, haga clic con el botón derecho del ratón y seleccione Nuevo > Clave y asígnele un nombre. WSP
4. Vaya a \HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Amazon\WSP.
5. Si el h_log_verbosity_options valor no existe, haga clic con el botón derecho del ratón y seleccione Nuevo > DWORD y asígnele un h_log_verbosity_options nombre.
6. Haga clic en el nuevo h_log_verbosity_options DWORD y cambie el valor a uno de los siguientes números en función del nivel de verbosidad requerido:
   - 0 — Error
   - 1 — Advertencia
   - 2 — Información
   - 3 — Depurar
7. Haga clic en Aceptar y cierre el Editor del Registro de Windows.
8. Reinicie el WorkSpace.

Registros del lado del servidor PCoIP

Todos los componentes del PCoIP escriben sus archivos de registro en una de estas dos carpetas:

- Ubicación principal: C:\ProgramData\Teradici\PCoIPAgent\logs
- Ubicación del archivo: C:\ProgramData\Teradici\logs

A veces, cuando se trabaja con AWS Support un problema complejo, es necesario poner el agente del servidor PCoIP en modo de registro detallado. Para habilitar esto:

1. Abra la siguiente clave de registro: `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Teradici\PCoIP\pcoip_admin_defaults`
2. En la `pcoip_admin_defaults` clave, cree el siguiente DWORD de 32 bits: `pcoip.event_filter_mode`
3. Establezca el valor de `pcoip.event_filter_mode` en «3» (Dec o Hex).

Como referencia, estos son los umbrales de registro que se pueden definir en este DWORD.

- 0 — (CRÍTICO)
- 1 — (ERROR)
- 2 — (INFORMACIÓN)
- 3 — (Depurar)

Si el `pcoip_admin_default` DWORD no existe, el nivel de registro es el 2 predeterminado. Se recomienda restaurar el valor de 2 DWORD cuando ya no necesite registros detallados, ya que son mucho más grandes y consumirán espacio en disco innecesariamente.

WebAccess registros del lado del servidor

Para PCoIP y WSP (versión 1.0+) WorkSpaces, el cliente de acceso WorkSpaces web utiliza el servicio STXHD. Los registros del acceso web se almacenan en WorkSpaces . `C:\ProgramData\Amazon\Stxhd\Logs`

En el caso de WSP (versión 2.0+) WorkSpaces, los registros de WorkSpaces Web Access se almacenan en. `C:\ProgramData\Amazon\WSP\`

Registros del lado del cliente

Estos registros provienen del WorkSpaces cliente con el que se conecta el usuario, por lo que se encuentran en el ordenador del usuario final. Las ubicaciones de los archivos de registro para Windows y Mac son:

- Windows: `"%LOCALAPPDATA%\Amazon Web Services\Amazon WorkSpaces\Logs"`
- macOS: `~/Library/"Application Support"/"Amazon Web Services"/"Amazon WorkSpaces"/logs`
- Linux: `~/.local/share/Amazon Web Services/Amazon WorkSpaces/logs`

Para ayudar a solucionar los problemas que puedan experimentar los usuarios, habilita el registro avanzado que se puede utilizar en cualquier WorkSpaces cliente de Amazon. El registro avanzado está habilitado para cada sesión posterior del cliente hasta que se desactiva.

1. Antes de conectarse a WorkSpace, el usuario final debe habilitar el registro avanzado para su WorkSpaces cliente.
2. A continuación, el usuario final debe conectarse como de costumbre WorkSpace, utilizar el suyo e intentar reproducir el problema.
3. El registro avanzado genera archivos de registro que contienen información de diagnóstico y detalles de depuración, incluidos datos detallados de rendimiento.

Esta configuración se mantiene hasta que se desactive de forma explícita. Una vez que el usuario haya reproducido correctamente el problema con el inicio de sesión detallado, esta configuración debe deshabilitarse, ya que genera archivos de registro de gran tamaño.

Recopilación automática de paquetes de registros del lado del servidor para Windows

El `Get-WorkSpaceLogs.ps1` script es útil para recopilar rápidamente un paquete de registros del lado del servidor para. AWS Support Se puede solicitar el script AWS Support solicitándolo en un caso de soporte:

1. Conéctese al WorkSpace mediante el cliente o mediante el Protocolo de escritorio remoto (RDP).
2. Inicie una línea de comandos administrativa (ejecútela como administrador).
3. Inicie el script desde la línea de comandos con el siguiente comando:

```
powershell.exe -NoLogo -ExecutionPolicy RemoteSigned -NoProfile -File "C:\Program
 Files\Amazon\WorkSpacesConfig\Scripts\Get-WorkSpaceLogs.ps1"
```

4. El script crea un paquete de registros en el escritorio del usuario.

   El script crea un archivo zip con las siguientes carpetas:

   - C: contiene los archivos de programa, archivos de programa (x86) y Windows relacionados con Skylight ProgramData, EC2Config, Teradici, el visor de eventos y los registros de Windows (Panther y otros).

- CliXML: contiene archivos XML que se pueden importar a Powershell mediante el filtrado interactivo. `Import-CliXML` Consulte Import-Clixml.
- Config: registros detallados de cada comprobación que se realiza
- ScriptLogs— Registros sobre la ejecución del script (no son relevantes para la investigación, pero son útiles para depurar lo que hace el script).
- tmp —Carpeta temporal (debe estar vacía).
- Rastros: la captura de paquetes se realiza durante la recopilación de registros.

¿Cómo comprobar la latencia en la AWS región más cercana

El sitio web Connection Health Check comprueba rápidamente si se WorkSpaces puede acceder a todos los servicios necesarios que utilizan Amazon. También comprueba el rendimiento de cada AWS región en la que Amazon WorkSpaces está disponible y permite a los usuarios saber cuál será la más rápida.

Conclusión

Hay un cambio estratégico en la informática para usuarios finales, ya que las organizaciones se esfuerzan por ser más ágiles, proteger mejor sus datos y ayudar a sus trabajadores a ser más productivos. Muchos de los beneficios que ya ofrece la computación en nube también se aplican a la informática para los usuarios finales. Al trasladar sus escritorios Windows o Linux a la AWS nube con Amazon WorkSpaces, las organizaciones pueden escalar rápidamente a medida que añaden trabajadores, mejorar su postura de seguridad al mantener los datos alejados de los dispositivos y ofrecer a sus trabajadores un escritorio portátil, con acceso desde cualquier lugar, mediante el dispositivo que elijan.

Amazon WorkSpaces está diseñado para integrarse en los sistemas y procesos de TI existentes, y en este documento técnico se describen las mejores prácticas para hacerlo. El resultado de seguir las directrices de este documento técnico es una implementación rentable de escritorio en la nube que puede ampliarse de forma segura con su empresa en la infraestructura global. AWS

Colaboradores

Los colaboradores de este documento son:

- Andrew Morgan, arquitecto de soluciones EUC, Amazon Web Services
- Don Scott, consultor sénior especializado en EUC, Amazon Web Services
- Klaus Becker, arquitecto sénior especializado en soluciones EUC, Amazon Web Services
- Naviero Magee, arquitecto principal de soluciones, Amazon Web Services
- Robert Fountain, consultor especializado en EUC, Amazon Web Services
- Stephen Stetler, arquitecto sénior de soluciones EUC, Amazon Web Services

Documentación adicional

Para obtener información adicional, consulte los siguientes recursos:

- Guía de WorkSpaces administración de Amazon
- Guía para WorkSpaces desarrolladores de Amazon
- WorkSpaces Clientes de Amazon
- Administración de Amazon Linux 2 WorkSpaces con Amazon AWS OpsWorks para Puppet Enterprise
- Personalización de Amazon Linux WorkSpace
- Cómo mejorar la seguridad de LDAP en AWS Directory Service con LDAPS del lado del cliente
- Usa Amazon CloudWatch Events con Amazon WorkSpaces y AWS Lambda para una mayor visibilidad de la flota
- Cómo WorkSpaces usa Amazon AWS KMS
- AWS CLI Referencia de comandos: WorkSpaces
- Supervisión de Amazon WorkSpaces Metrics
- Entorno de escritorio MATE
- Solución de problemas de administración de AWS Directory Service
- Solución de problemas de WorkSpaces administración de Amazon
- Solución de problemas con los WorkSpaces clientes de Amazon
- Automatice Amazon WorkSpaces con un portal de autoservicio

Revisiones del documento

Para recibir notificaciones sobre las actualizaciones de este documento técnico, suscríbase a la fuente RSS.

Cambio	Descripción	Fecha
Actualización menor	Contenido actualizado para los servicios de directorio de AD, la recuperación ante desastres, la continuidad empresarial y la redirección entre regiones. Se agregó WorkSpaces y optimizó el audio de Amazon Connect. Actualizaciones menores en el formato.	26 de mayo de 2022
Actualización menor	Corrige el lenguaje no inclusivo.	6 de abril de 2022
Documento técnico actualizado	Contenido actualizado	24 de marzo de 2022
Documento técnico actualizado	Contenido actualizado para AWS Network Firewall, MAD Replicated Directories, YubiKey Support, Containers, WSLv1, Smart Card Support, WorkSpaces Service Quota y Trusted Devices.	20 de diciembre de 2021
Documento técnico actualizado	Contenido actualizado sobre el protocolo de WorkSpaces transmisión, la autenticación con tarjeta inteligente, los diagramas, las implementaciones de clientes, la	28 de abril de 2021

	selección de dispositivos finales y el acceso a la web	
Documento técnico actualizado	Contenido actualizado	1 de diciembre de 2020
Documento técnico actualizado	Se actualizó el contenido desde la primera publicación y se agregaron nuevos diagramas.	1 de mayo de 2020
Publicación inicial	Publicado por primera vez.	1 de julio de 2016

Avisos

Es responsabilidad de los clientes realizar su propia evaluación independiente de la información que contiene este documento. Este documento: (a) tiene únicamente fines informativos, (b) representa las ofertas y prácticas de AWS productos actuales, que están sujetas a cambios sin previo aviso, y (c) no crea ningún compromiso ni garantía por parte de AWS sus filiales, proveedores o licenciantes. AWS los productos o servicios se proporcionan «tal cual» sin garantías, representaciones o condiciones de ningún tipo, ya sean expresas o implícitas. Las responsabilidades y obligaciones de AWS sus clientes están reguladas por AWS acuerdos, y este documento no forma parte de ningún acuerdo entre sus clientes AWS y sus clientes ni lo modifica.

© 2022 Amazon Web Services, Inc. o sus filiales. Todos los derechos reservados.

AWS Glosario

Para obtener la AWS terminología más reciente, consulte el AWS glosario de la Glosario de AWS Referencia.

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.