Prácticas recomendadas para la implementación de Amazon WorkSpaces

Acceso a la red, servicios del directorio y seguridad

Julio de 2016

Avisos

Este documento se suministra únicamente con fines informativos. Representa la oferta actual de productos y prácticas de AWS a partir de la fecha de publicación de este documento. Dichas prácticas y productos pueden modificarse sin previo aviso. Los clientes son responsables de realizar sus propias evaluaciones independientes de la información contenida en este documento y de cualquier uso de los productos o servicios de AWS, cada uno de los cuales se ofrece "como es", sin garantía de ningún tipo, ya sea explícita o implícita. Este documento no constituye ninguna garantía, representación, compromiso contractual ni condición por parte de AWS, sus filiales, proveedores o licenciantes. Las responsabilidades y obligaciones de AWS con sus clientes se rigen por los acuerdos de AWS, y este documento no forma parte ni supone una modificación de ningún acuerdo entre AWS y sus clientes.

Contenido

Resumen

En este documento técnico se describen algunas de las prácticas recomendadas para la implementación de Amazon WorkSpaces. En el presente documento se abordan consideraciones de la red, servicios de directorio y autenticación del usuario, seguridad y monitorización y registro.

Está dividido en cuatro categorías para permitir un acceso más rápido a la información relevante. Además, está dirigido a ingenieros de redes, ingenieros de directorio o ingenieros de seguridad.

Introducción

Amazon WorkSpaces es un servicio administrado de informática de escritorio en la nube. Con Amazon WorkSpaces se elimina la necesidad de adquirir o implementar hardware o de instalar un software complejo. Ofrece una experiencia de escritorio con tan solo unos clics en la Consola de administración de AWS mediante el uso de la interfaz de línea de comandos (CLI, Command Line Interface) de AWS o mediante API. Con Amazon WorkSpaces, puede lanzar un escritorio en cuestión de minutos y conectarse y acceder a su software de escritorio desde las instalaciones o desde una red externa de manera segura, confiable y rápida. Puede hacer lo siguiente:

- Aprovechar su Microsoft Active Directory (AD) existente en las instalaciones mediante el uso de AWS Directory Service: conector AD
- Ampliar su directorio en la nube de AWS
- Elaborar un directorio administrado con AWS Directory Service: AD de Microsoft o AD simple, a fin de administrar usuarios y WorkSpaces

Además, puede aprovechar su servidor RADIUS ubicado en las instalaciones o alojado en la nube a través del Conector AD para proporcionar una autenticación multifactor (MFA, Multi-factor Authentication) a sus WorkSpaces.

Puede automatizar el aprovisionamiento de Amazon WorkSpaces mediante el uso de CLI o API, lo cual le permite integrar Amazon WorkSpaces a sus flujos de trabajo de suministro existentes.

Por cuestiones de seguridad, además del cifrado de red integrado que ofrece el servicio de WorkSpaces, también puede activar el cifrado en el resto de sus WorkSpaces (consulte Espacios de trabajo cifrados en la sección sobre seguridad).

Puede implementar aplicaciones en sus WorkSpaces mediante el uso de sus herramientas existentes en las instalaciones, como Microsoft System Center Configuration Manager (SCCM) o el aprovechamiento de Amazon WorkSpaces Application Manager (Amazon WAM).

En las siguientes secciones hay información detallada sobre Amazon WorkSpaces, se explica cómo funciona el servicio, se describe lo que necesita para ejecutar el servicio y figuran las opciones y características disponibles.

Requisitos de WorkSpaces

Para ejecutar correctamente el servicio Amazon WorkSpaces, se necesitan tres componentes:

- **Aplicación del cliente de WorkSpaces**. Dispositivo del cliente compatible con Amazon WorkSpaces. Encuentre una lista completa aquí: Plataformas y dispositivos compatibles.

  También puede usar los clientes cero de la computadora personal sobre protocolo de Internet (PCoIP, Personal Computer over Internet Protocol) para conectarse a WorkSpaces. Para ver una lista de los dispositivos disponibles, consulte Clientes cero de PCoIP de Amazon WorkSpaces.

- **Servicio de directorio para autenticar usuarios y proporcionar acceso a su WorkSpace**. Amazon WorkSpaces actualmente funciona con AWS Directory Service y Active Directory. Puede utilizar el servidor de Active Directory en las instalaciones con AWS Directory Service para poder usar sus credenciales de usuario empresariales existentes con WorkSpaces.

- **Amazon Virtual Private Cloud (Amazon VPC) donde se ejecutará Amazon WorkSpaces**. Necesitará dos subredes como mínimo para una implementación de WorkSpaces, porque cada creación de AWS Directory Service necesita de dos subredes en un despliegue Multi-AZ.

Consideraciones de red

Cada WorkSpace está asociado a un Amazon VPC y al AWS Directory Service que usó para crearlo. Todas las construcciones de AWS Directory Service (AD simple, Conector AD y AD de Microsoft) necesitan dos subredes para funcionar, cada una en una zona de disponibilidad diferente. Las subredes se relacionan permanentemente con una construcción de Directory Service y no se pueden modificar después de la creación de un AWS Directory Service. Por lo tanto, es fundamental que determine los tamaños de subred adecuados antes de generar una construcción de Directory Services. Tenga muy en cuenta lo siguiente antes de crear las subredes:

- ¿Cuántos WorkSpaces necesitará con el paso del tiempo? ¿Cuál es el crecimiento previsto?
- ¿Qué tipos de usuarios deberá acoger?
- ¿Cuántos dominios de Active Directory conectará?
- ¿En dónde se encuentran sus cuentas de usuarios empresariales?

Amazon recomienda que defina los grupos de usuarios, o los roles, sobre la base del tipo de acceso y la autenticación del usuario que requiere como parte de su proceso de planificación. Estas respuestas son útiles cuando necesita limitar el acceso a determinadas aplicaciones o recursos. Los roles de usuario definidos pueden ayudarlo a segmentar y a restringir el acceso mediante el uso de AWS Directory Service, las listas de control de acceso a la red, las tablas de enrutamiento y los grupos de seguridad de la nube privada virtual (VPC, Virtual Private Cloud). Cada construcción de AWS Directory Service usa dos subredes y aplica las mismas configuraciones a todos los WorkSpaces que se ejecutan desde esa construcción. Por ejemplo, puede usar un grupo de seguridad que se aplique a todos los WorkSpaces asociados a un conector de AD para especificar si se requiere una autenticación MFA o si el usuario final puede tener acceso de administrador local a sus WorkSpaces.

> **Tenga en cuenta que** cada conector de AD se conecta a una unidad organizacional (OU, Organizational Unit) de Microsoft Active Directory. Debe construir su Directory Service para incluir los roles de usuarios, de modo que pueda aprovechar esta capacidad.

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

Diseño de la VPC

Estos son algunos de los 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 (ACL, Access Control Lists) de la red para su Amazon WorkSpaces, de modo que pueda crear su entorno de WorkSpaces en función de la escala, la seguridad y la fácil administración:

- **VPC**. Le recomendamos que use una VPC por separado específicamente para la implementación de sus WorkSpaces. Con una VPC por separado, puede especificar la gobernanza y los procesos de seguridad necesarios para sus WorkSpaces al crear una separación del tráfico.
- **Directory Services**. Cada construcción de AWS Directory Service requiere de un par de subredes que proporcionen una división altamente disponible de los servicios del directorio entre las zonas de disponibilidad (AZ, Availability Zones) de Amazon.
- **Tamaño de la subred**. Las implementaciones de los WorkSpaces están relacionadas con la construcción de un directorio y se encuentran en las mismas subredes de la VPC que el AWS Directory Service que eligió. Algunas consideraciones:
  - Los tamaños de la subred son permanentes y no se pueden cambiar, por lo que debe dejar un espacio suficiente disponible para el crecimiento futuro.
  - Puede especificar un grupo de seguridad predeterminado para el AWS Directory Service que eligió; este grupo se aplica a todos los WorkSpaces asociados a la construcción específica del AWS Directory Service.

— Puede hacer que varios servicios de directorio de AWS usen la misma subred.

Tenga en cuenta los planes futuros cuando diseñe su VPC. Por ejemplo, probablemente desee agregar componentes de administración como un servidor antivirus, un servidor de administración de revisiones o un servidor de Active Directory o de MFA RADIUS. Vale la pena planificar para direcciones de IP adicionales disponibles en el diseño de su VPC para cumplir con este tipo de requisitos.

Para obtener más instrucciones y consideraciones para el diseño de la VPC y el tamaño de la red, consulte la presentación sobre **re:Invent** Cómo se está moviendo Amazon.com a Amazon WorkSpaces.

Interfaces de red

En cada WorkSpace hay dos interfaces elásticas (ENI, Elastic Network Interfaces), una interfaz de red de administración (eth0) y una interfaz de red primaria (eth1). AWS utiliza la interfaz de red de administración para administrar WorkSpace; esta es la interfaz en la que finaliza la conexión de su cliente. Para esta interfaz, AWS aprovecha un intervalo de direcciones IP privadas. Para que el enrutamiento de red funcione adecuadamente, no puede usar este espacio de dirección privado en ninguna red que pueda comunicarse con su VPC de WorkSpaces.

Para obtener una lista de los intervalos de IP privados que usamos según la región, consulte Detalles de Amazon WorkSpaces.

Nota: Amazon WorkSpaces y sus interfaces de red de administración asociadas no se encuentran en su VPC, y no puede ver la interfaz de red de administración ni la identificación de la instancia de Amazon Elastic Compute Cloud (Amazon EC2) en su Consola de administración de AWS (consulte Figura 4, Figura 5 y Figura 6). Sin embargo, puede ver y modificar las configuraciones del grupo de seguridad de la interfaz de red primaria (eth1) en la Consola de administración de AWS. Además, la interfaz de red primaria de cada WorkSpace no se cuenta en los límites de recursos de la interfaz de red elástica (ENI, Elastic Network Interface) de Amazon EC2. Para implementar WorkSpaces repetidas veces, necesitaría abrir un vale de soporte a través de la Consola de administración de AWS para aumentar los límites de la ENI.

Flujo del tráfico

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

- El tráfico entre el dispositivo del cliente y el servicio de Amazon WorkSpace
- El tráfico entre el servicio de Amazon WorkSpace y el tráfico de red del cliente

En la siguiente sección, abordaremos estos dos componentes.

Dispositivo del cliente a WorkSpace

El dispositivo en el que se ejecuta el cliente de Amazon WorkSpaces, independientemente de su ubicación (en las instalaciones o remoto), usará los mismos dos puertos para conectarse al servicio de WorkSpaces. El cliente utiliza HTTPS sobre el puerto 443 para toda la información relacionada con la autenticación y la sesión, y utiliza el puerto 4172 (puerto PCoIP) con TCP y UDP para la transmisión por secuencias de píxeles a un WorkSpace determinado y para realizar verificaciones del estado de la red. El tráfico en ambos puertos está cifrado. El tráfico del puerto 443 se usa para la información de autenticación y sesión y utiliza la seguridad de la capa de transporte (TLS, Transport Layer Security) para cifrar el tráfico. El tráfico de la transmisión por secuencias de píxeles aprovecha el cifrado del estándar de cifrado avanzado (AES, Advanced Encryption Standard) de 256 bits para establecer una comunicación entre el cliente y el eth0 del WorkSpace a través de la puerta de enlace de transmisión por secuencias. Encuentre más información al respecto en la sección Seguridad que figura más adelante en este documento.

Publicamos intervalos de IP según la región de nuestras puertas de enlaces de transmisión por secuencias PCoIP y los puntos de conexión de verificación del estado de la red. Puede limitar el tráfico de salida en el puerto 4172 desde su red corporativa a la puerta de enlace de transmisión por secuencias de AWS y a los puntos de conexión de verificación del estado de la red al permitir únicamente el tráfico de salida en el puerto 4172 a las regiones de AWS específicas en las que usa Amazon WorkSpaces. Para obtener más información sobre los intervalos de IP y los puntos de conexión de verificación del estado de la red, consulte Intervalos de IP de la puerta de enlace PCoIP de Amazon WorkSpaces.

El cliente de Amazon WorkSpaces tiene una verificación del estado de la red integrada. Mediante este servicio, los usuarios pueden saber si su red podrá establecer una conexión a través de un indicador de estado ubicado en la parte inferior derecha de la aplicación. Se puede acceder a una vista más detallada del estado de la red al seleccionar **Red** en la parte inferior derecha del cliente. El resultado aparece en la Figura 1.

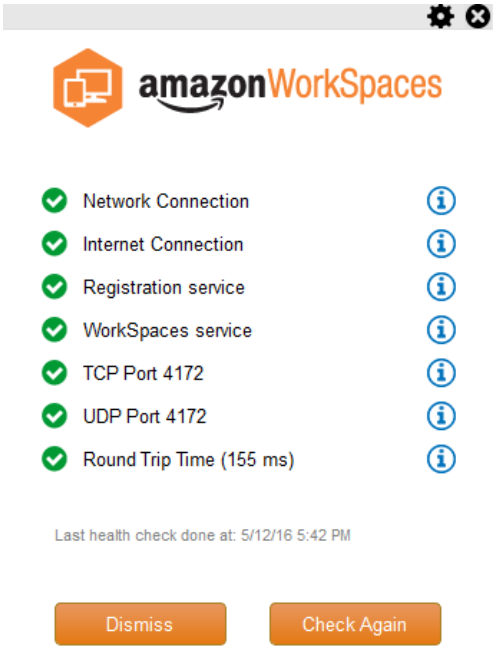

Figura 1: cliente de WorkSpaces: verificación de red

Un usuario inicia una conexión desde su cliente al servicio WorkSpaces al proporcionar su información de inicio de sesión del directorio que utiliza la construcción de Directory Service, que es generalmente su directorio corporativo. La información de inicio de sesión se envía a través de HTTPS a las puertas de enlace de autenticación del servicio Amazon WorkSpaces en la región donde se encuentra el WorkSpace. Entonces la puerta de enlace de autenticación del servicio de Amazon WorkSpaces reenvía el tráfico a la construcción específica del servicio AWS Directory Service asociada a su WorkSpace. Por ejemplo, cuando se usa el conector de AD, este reenvía la solicitud de autenticación directamente a su servicio de Active Directory, que puede estar en las instalaciones o en una VPC de AWS (consulte Escenarios de implementación de AD DS). El conector de AD no almacena ninguna información de autenticación y funciona como un proxy sin estado. Como resultado, es fundamental que el conector de AD pueda conectarse a un servidor de Active Directory. El conector de AD determina el servidor de Active Directory con el que establece conexión a través de los servidores DNS que define cuando crea el conector de AD.

Si está utilizando un conector de AD y tiene la MFA activada en el directorio, se verificará el token de MFA antes que la autenticación del servicio del directorio. En caso de que falle la validación de la MFA, la información de inicio de sesión del usuario no se reenviará a su AWS Directory Service.

Una vez que se autenticó un usuario, comienza el tráfico de transmisión por secuencias al aprovechar el puerto 4172 (puerto PCoIP) a través de la puerta de enlace de transmisión por secuencias de AWS al WorkSpace. Aun así, se intercambia la información relacionada con la sesión a través de HTTPS durante la sesión. El tráfico transmitido usa la primera ENI en el WorkSpace (eth0 en el WorkSpace) que no está conectada a su VPC. AWS se encarga de administrar la conexión de red desde la puerta de enlace de transmisión por secuencias a la ENI. En caso de que se produzca una falla de conexión desde las puertas de enlace de transmisión por secuencias a la ENI de transmisión por secuencias de WorkSpaces, se generará un evento en CloudWatch (consulte la sección Monitorización o registro mediante el uso de Amazon CloudWatch en este documento técnico).

La cantidad de datos que se envían entre el servicio Amazon WorkSpaces y el cliente depende del nivel de actividad de píxeles. Para garantizar una experiencia óptima para los usuarios, le recomendamos que el tiempo de ida y vuelta (RTT, Round Trip Time) entre el cliente de WorkSpaces y la región de AWS donde se encuentran sus WorkSpaces estén ubicados a menos de 100 ms. Por lo general, esto significa que su cliente de WorkSpaces se encuentra a menos de dos mil millas de la región donde se aloja el WorkSpace. Proporcionamos una página web de verificación del estado de conexión que puede consultar para determinar la región de AWS más óptima para el servicio Amazon WorkSpaces.

Servicio Amazon WorkSpaces a VPC

Luego de la autenticación de una conexión desde un cliente a un WorkSpace y del inicio del tráfico de transmisión por secuencias, su cliente de WorkSpaces mostrará un escritorio de Windows (su WorkSpace) conectado a su VPC y su red debería indicar que se estableció la conexión. La ENI primaria de WorkSpace, identificada como eth1, tendrá asignada una dirección IP desde el servicio del protocolo de configuración dinámica de host (DHCP, Dynamic Host Configuration Protocol) proporcionada por su VPC, generalmente desde las mismas subredes que el AWS Directory Service. La dirección IP permanecerá en el WorkSpace mientras este dure. La ENI que se encuentra en su VPC tiene acceso a cualquier recurso en el VPC y a cualquier red que ha conectado a esta (a través de la interconexión de VPC, una conexión de AWS Direct Connect o una conexión de VPN).

El acceso de la ENI a sus recursos de la red está determinado por el grupo de seguridad predeterminado (consulte más información sobre los grupos de seguridad aquí) que su AWS Directory Service configura para cada WorkSpace y cualquier grupo de seguridad adicional que asigne a la ENI. Puede agregar grupos de seguridad a la ENI orientados a la VPC como desee mediante el uso de la Consola de administración de AWS o la interfaz de línea de comandos (CLI, Command Line Interface). Además de los grupos de seguridad, puede utilizar su firewall basado en host preferido en un determinado WorkSpace para limitar el acceso por la red a los recursos que se encuentran en la VPC.

En la Figura 4 en Escenarios de implementación de AD DS, más adelante en este documento técnico, se muestra el flujo de tráfico descrito anteriormente.

Ejemplo de una configuración típica

Veamos un escenario en el que hay dos tipos de usuarios y en el que su AWS Directory Service utiliza un Active Directory centralizado para la autenticación de usuarios:

- **Trabajadores que necesitan acceso completo desde cualquier parte** (por ejemplo, los empleados de tiempo completo). Estos usuarios tendrán acceso completo a Internet y a la red interna y pasarán por un firewall desde la VPC a la red en las instalaciones.

- **Trabajadores que solo deberían tener acceso restringido desde el interior de la red corporativa** (por ejemplo, los contratistas y los asesores). Estos usuarios tienen acceso restringido a Internet a través de un servidor proxy (a sitios web específicos) en la VPC y tendrán acceso limitado a la red en la VPC y en la red de las instalaciones.

Querrá otorgarles a los empleados de tiempo completo la capacidad de tener acceso de administrador local en sus WorkSpaces para instalar software y querrá imponer una autenticación de dos factores con MFA. También querrá permitir que los empleados de tiempo completo tengan acceso ininterrumpido a Internet desde sus WorkSpaces.

En el caso de los contratistas, querrá bloquear el acceso de administrador local para que solo puedan utilizar aplicaciones específicas instaladas previamente. Es conveniente aplicar controles de acceso a la red muy restrictivos a través de los grupos de seguridad para estos WorkSpaces. Debe abrir los puertos 80 y 443 en sitios web internos específicos únicamente y bloquear su acceso a Internet.

En este escenario, hay dos tipos de roles de usuario completamente diferentes con diferentes requisitos en cuanto al acceso a la red y al escritorio. Una de las prácticas recomendadas es administrar y configurar sus WorkSpaces de manera diferente. Para ello, deberá crear dos conectores de AD, uno para cada rol del usuario. Cada conector de AD requiere de dos subredes que necesitan las direcciones IP suficientes para cumplir con los cálculos estimados de crecimiento de uso de sus WorkSpaces.

> **Nota:** Cada subred de la VPC de AWS consume cinco direcciones IP (las primeras cuatro y la última dirección IP) por cuestiones de administración, y cada conector de AD consume una dirección de IP en cada subred en la que persiste.

Las otras consideraciones relacionadas con este escenario son las siguientes:

- Las subredes de la VPC de AWS deben ser subredes privadas, de modo que el tráfico, como el acceso a Internet, se pueda controlar a través de una puerta de enlace NAT o un servidor proxy NAT en la nube, o se redirija de nuevo al sistema de administración de tráfico en las instalaciones.
- Se instaló un firewall para todo el tráfico de la VPC para la red en las instalaciones.
- El servidor de Microsoft Active Directory y los servidores MFA RADIUS se encuentran en las instalaciones (consulte Escenario 1: uso del conector AD para asignar autenticación al AD DS **en las instalaciones**) o forman parte de la implementación en la nube de AWS (consulte los escenarios 2 y 3, Escenarios de implementación de AD DS).

Debido a que se les otorgará algún tipo de acceso a Internet a todos los WorkSpaces y dado que se alojarán en una subred privada, también debe crear subredes públicas que puedan acceder a Internet por una puerta de enlace de Internet. Necesitará una puerta de enlace NAT para los empleados de tiempo completo, que les permitirá acceder a Internet, y un servidor proxy NAT para los asesores y contratistas, a fin de limitar su acceso a sitios web internos específicos. Para planificar fallas, diseñar para una alta disponibilidad y limitar los costos por tráfico cruzado en AZ, debe tener dos puertas de enlace NAT y servidores NAT o proxy en dos subredes diferentes en un despliegue Multi-AZ. Las dos AZ que seleccione como subredes públicas coincidirán con las dos AZ que usará para las subredes de sus WorkSpaces en las regiones que tienen más de dos AZ. Puede dirigir todo el tráfico desde cada AZ de los WorkSpaces a la subred pública correspondiente para limitar los costos por tráfico cruzado en AZ y ofrecer una administración más fácil. En la Figura 2 se muestra la configuración de la VPC.

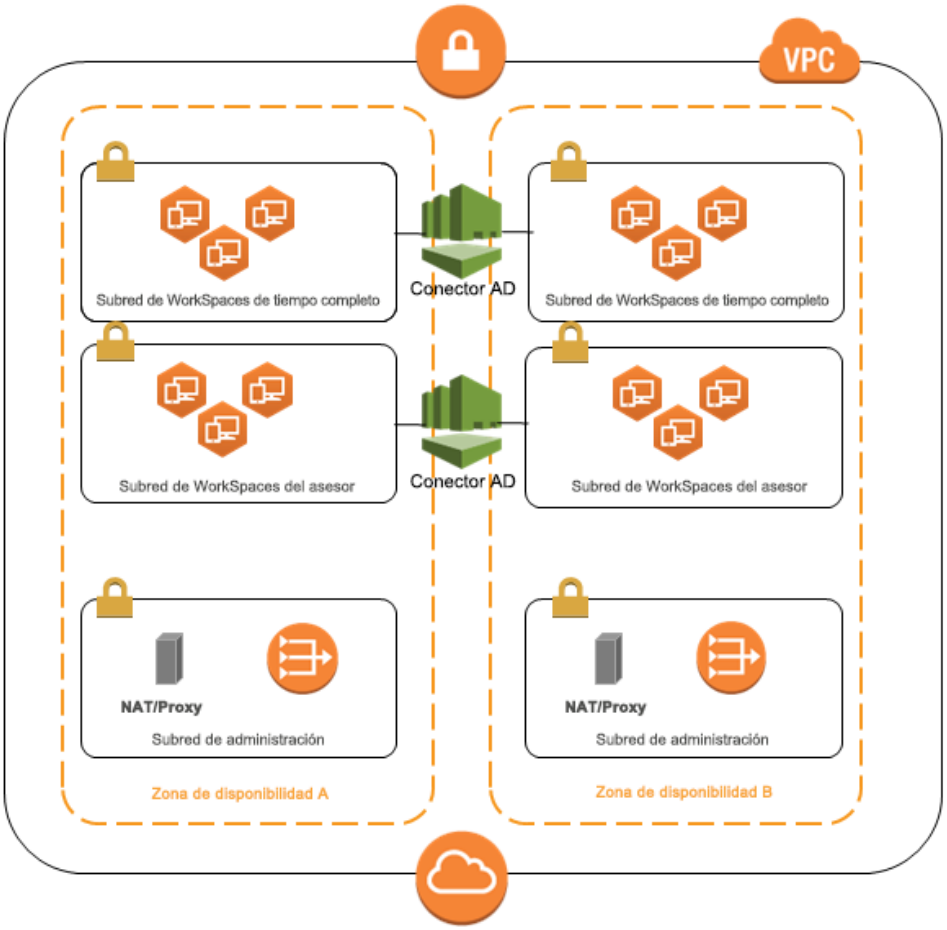

Figura 2: diseño de la VPC de alto nivel

La siguiente información describe cómo configurar los dos tipos de WorkSpaces diferentes descritos anteriormente.

- **Empleados de tiempo completo:** en la Consola de administración de Amazon WorkSpaces, seleccione la opción **Directorios** en la barra del menú, seleccione el directorio donde se alojan los empleados de tiempo completo y luego seleccione **Configuración del administrador local**. Al activar esta opción, cualquier WorkSpace creado recientemente tendrá privilegios de administrador local. Para otorgar acceso a Internet, debe configurar la traducción de direcciones de red (NAT, Network Address Translation) para el acceso a Internet saliente desde su VPC. Para activar la MFA, debe especificar un servidor RADIUS, un IP de servidor, puertos y una clave compartida previamente.

Para los WorkSpaces de los empleados de tiempo completo, el tráfico entrante al WorkSpace se limitaría a un protocolo de escritorio remoto (RDP, Remote Desktop Protocol) desde la subred de asistencia técnica al aplicar un grupo de seguridad predeterminado a través de las configuraciones del conector de AD.

- **Contratistas y asesores:** en la Consola de administración de Amazon WorkSpaces, desactive **Internet Access** y el **Local Administrator Setting**. Luego, agregue un grupo de seguridad en la sección de configuración de **Security Group** para establecer un grupo de seguridad para todos los WorkSpaces nuevos creados en ese directorio.

  En el caso de los WorkSpaces de los asesores, limite el tráfico de entrada y de salida a los WorkSpaces al aplicar un grupo de seguridad predeterminado configurando el Conector AD a todos los WorkSpaces asociados a este. Con el grupo de seguridad se impediría el acceso de salida de los WorkSpaces a cualquier elemento que no sea el tráfico HTTP o HTTPS y el tráfico de entrada al protocolo de escritorio remoto (RDP, Remote Desktop Protocol) desde la subred de asistencia técnica en la red de las instalaciones.

> **Nota:** El grupo de seguridad solo se aplica a la interfaz de red elástica (ENI, Elastic Network Interface) que se encuentra en la nube privada virtual (VPC, Virtual Private Cloud) (eth1 en el WorkSpace), y el acceso al WorkSpace desde el cliente de WorkSpaces no se restringe como resultado de un grupo de seguridad. En la Figura 3 se muestra el diseño final de la VPC de WorkSpaces que se describió anteriormente.

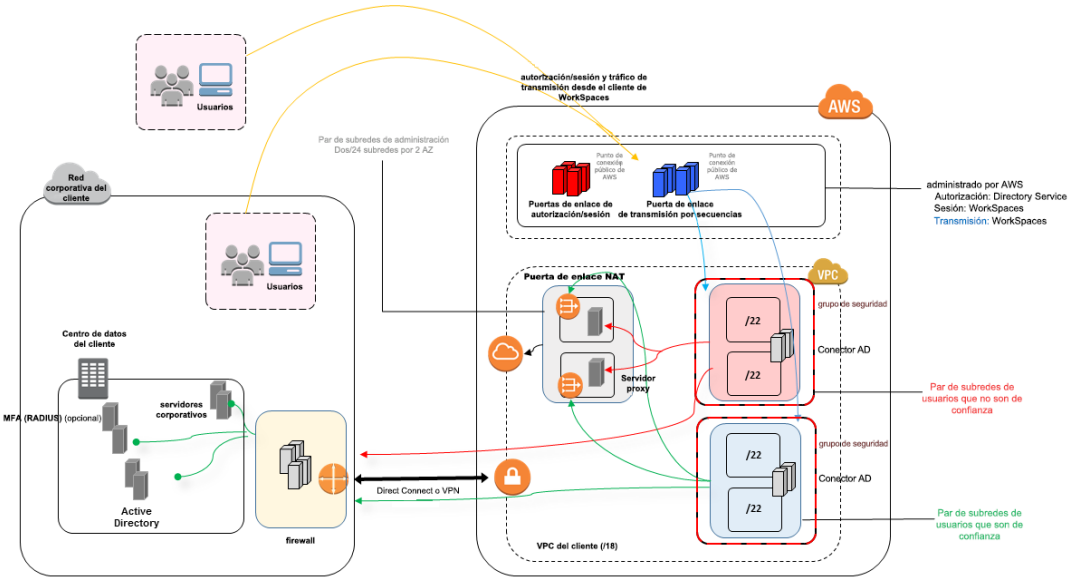

Figura 3: diseño de WorkSpaces con roles del usuario

AWS Directory Service

Como se mencionó en la Introducción, Amazon WorkSpaces está respaldado por AWS Directory Service. Con AWS Directory Service puede crear tres tipos de directorios. Los primeros dos se encuentran en la nube de AWS:

- AWS Directory Service para Active Directory de Microsoft (edición empresarial) o **AD de Microsoft**, un Active Directory de Microsoft administrado, con tecnología de Windows Server 2012 R2.
- **AD simple**, servicio de directorio administrado independiente compatible con Active Directory de Microsoft y con tecnología Samba 4.

La tercera, **Conector AD,** es una puerta de enlace de directorio que le permite asignar solicitudes de autenticación y búsquedas del usuario o del grupo a su Active Directory de Microsoft existente en sus instalaciones.

En la siguiente sección se describen los flujos de comunicación para la autenticación entre el servicio de intermediario de Amazon WorkSpaces y el AWS Directory Service, las prácticas recomendadas para implementar WorkSpaces con AWS Directory Service y los conceptos avanzados como la autenticación multifactor (MFA, Multi-factor authentication). También abordaremos los conceptos de arquitectura de infraestructura para Amazon WorkSpaces en escala, los requisitos para la VPC de Amazon y el AWS Directory Service, incluida la integración con los Servicios de dominio de Active Directory (AD DS) de Microsoft en las instalaciones.

Escenarios de implementación de AD DS

El respaldo de Amazon WorkSpaces en AWS Directory Service y el diseño y la implementación adecuados del servicio del directorio es fundamental. Los siguientes tres escenarios se basan en la *guía de inicio rápido* de *los Servicios de dominio de Active Directory de Microsoft*, en la que se detallan las opciones de implementación de las prácticas recomendadas para AD DS, específicamente para su integración con WorkSpaces. En la sección *Consideraciones sobre* el diseño de este capítulo se abordan los requisitos específicos y las prácticas recomendadas del uso del Conector AD para WorkSpaces, que forma una parte integral del concepto de diseño general de WorkSpaces.

- **Escenario 1: uso del conector AD para asignar autenticación al AD DS en las instalaciones.** En este escenario, la conectividad a la red (red privada virtual [VPN, Virtual Private Network]/Direct Connect [DX]) se encuentra en el cliente, con toda la autenticación asignada a través del AWS Directory Service (Conector AD) al AD DS del cliente en las instalaciones.
- **Escenario 2: ampliación del AD DS de las instalaciones a AWS (réplica).** Este escenario es similar al escenario 1, pero aquí se implementa una réplica del cliente AD DS en AWS junto con el Conector AD, lo cual reduce la latencia de las solicitudes de autenticación/consulta al AD DS y el catálogo global de AD DS.
- **Escenario 3: implementación independiente aislada mediante el uso de AWS Directory Service en la nube de AWS.** Este es un escenario aislado y no incluye la conectividad de vuelta al cliente para su autenticación. En este enfoque se usan el AWS Directory Service (AD de Microsoft) y el Conector AD. Aunque este escenario no depende de la conectividad con el cliente para la autenticación, no proporciona el tráfico de la aplicación sobre VPN o DX cuando es necesario.

Escenario 1: uso del conector AD para asignar autenticación al AD DS en las instalaciones

Este escenario es para los casos en que los clientes que no desean ampliar su AD DS de las instalaciones en AWS o en que una nueva implementación del AD DS no es una opción. Figura 4: conector AD a Active Directory en las instalaciones muestra en un alto nivel cada uno de los componentes y el flujo de autenticación del usuario.

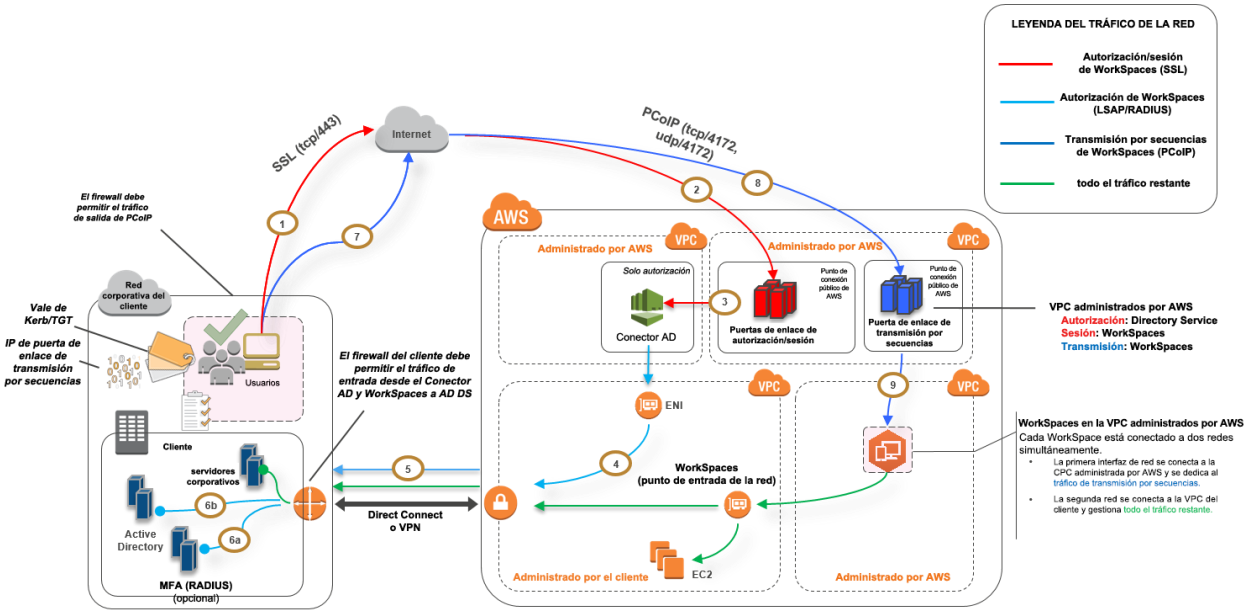

Figura 4: conector AD a Active Directory en las instalaciones

En este escenario, se usa AWS Directory Service (Conector AD) para la autenticación de todos los usuarios o MFA que se asigna a través del Conector AD al AD DS en las instalaciones del cliente (Figura 5). Para obtener detalles sobre los protocolos o el cifrado utilizado para el proceso de autenticación, consulte la sección Seguridad en este documento técnico.

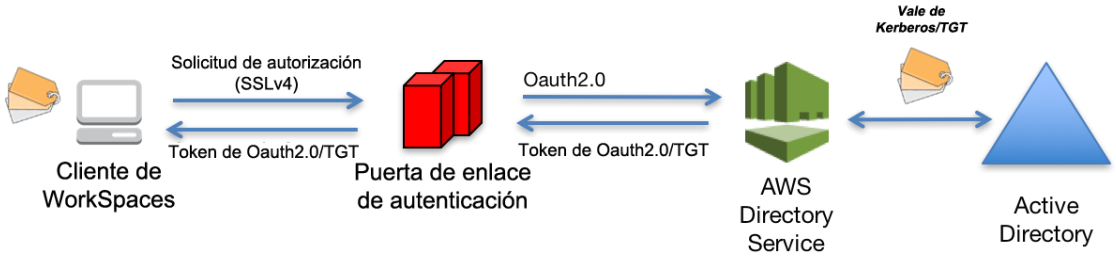

Figura 5: autenticación del usuario a través de la puerta de enlace de autenticación

En el escenario 1 se muestra una arquitectura híbrida donde el cliente posiblemente ya tenga recursos en AWS y recursos en un centro de datos en las instalaciones a los que se podría acceder a través de WorkSpaces. El cliente puede aprovechar el AD DS en las instalaciones y los servidores RADIUS existentes para la autenticación de usuarios y MFA.

Esta arquitectura utiliza los siguientes componentes o principios.

Amazon Web Services:

- **VPC de Amazon:** creación de una VPC de Amazon con al menos dos subredes privadas en dos zonas de disponibilidad.
- **Conjunto de opciones del protocolo de configuración dinámica de host (DHCP, Dynamic Host Configuration Protocol):** creación de un conjunto de opciones del DHCP de la VPC de Amazon. Esto permite la definición de un nombre de dominio especificado por el cliente y de los servidores de nombres de dominio (DNS, Domain Name Servers) (servicios en las instalaciones). (Para obtener más información, consulte Conjuntos de opciones de DHCP).
- **Puerta de enlace privada virtual de Amazon:** permite la comunicación con su propia red sobre un túnel de VPN IPsec o una conexión de AWS Direct Connect.
- **AWS Directory Service**: el Conector AD se implementa en un par de subredes privadas de la VPC de Amazon.
- **Amazon WorkSpaces:** los WorkSpacess se implementan en las mismas subredes privadas que el Conector AD (consulteConsideraciones sobre el diseño Conector AD).

Cliente:

- **Conectividad de la red:** VPN corporativa o puntos de conexión de Direct Connect.
- **AD DS:** AD DS corporativo.
- **MFA (opcional):** servidor RADIUS corporativo.
- **Dispositivos del usuario final:** dispositivos del usuario final corporativos o de tipo traiga su propia licencia (BYOL, Bring Your Own License) (como tabletas Windows, Mac, iPad o Android, Zero Client, Chromebook), que se usan para acceder al servicio Amazon WorkSpaces (consulte Plataformas y dispositivos compatibles).

Si bien esta solución es ideal para los clientes que no desean implementar AD DS en la nube, tiene sus desventajas.

- **Confiabilidad en la conectividad:** si se pierde la conectividad con el centro de datos, ningún usuario podrá iniciar sesión en su respectivo WorkSpace y las conexiones existentes permanecerán activas durante la vida útil de Kerberos/TGT.
- **Latencia:** si existe una latencia a través de la conexión (esto sucede más en el caso de VPN que en el de DX), la autenticación de los WorkSpaces y cualquier actividad relacionada con el AD DS, como la aplicación de la política de grupo (GPO, Group Policy), llevarán más tiempo.
- **Costos de tráfico:** todas las actividades de autenticación deberán atravesar el vínculo de VPN o DX, lo que significa que esto depende del tipo de conexión. Se trata de una transferencia de datos desde Amazon EC2 a Internet o de una transferencia de datos (DX).

> **Nota:** El Conector AD es un servicio proxy. No almacena ni conserva en la caché las credenciales del usuario. En su lugar, su Active Directory gestiona todas las actividades de autenticación y búsqueda y las solicitudes de administración. Se requiere una cuenta con privilegios de delegación en su servicio de directorio que tenga derechos de lectura de toda la información del usuario y de conexión de un equipo al dominio.

Para obtener información detallada sobre cómo configurar un usuario en su directorio para el Conector AD, consulte Delegación de privilegios de conexión.

En líneas generales, la experiencia con WorkSpaces depende considerablemente del elemento 5 que figura en Figura 4.

Escenario 2: ampliación del AD DS de las instalaciones a AWS (réplica)

Este escenario es similar al escenario 1, pero en el escenario 2 se implementa una réplica del cliente AD DS en AWS junto con el Conector AD. Esto reduce la latencia de la autenticación o las solicitudes de consulta a AD DS. Figura 6 muestra una vista de alto nivel de cada uno de los componentes y el flujo de autenticación del usuario.

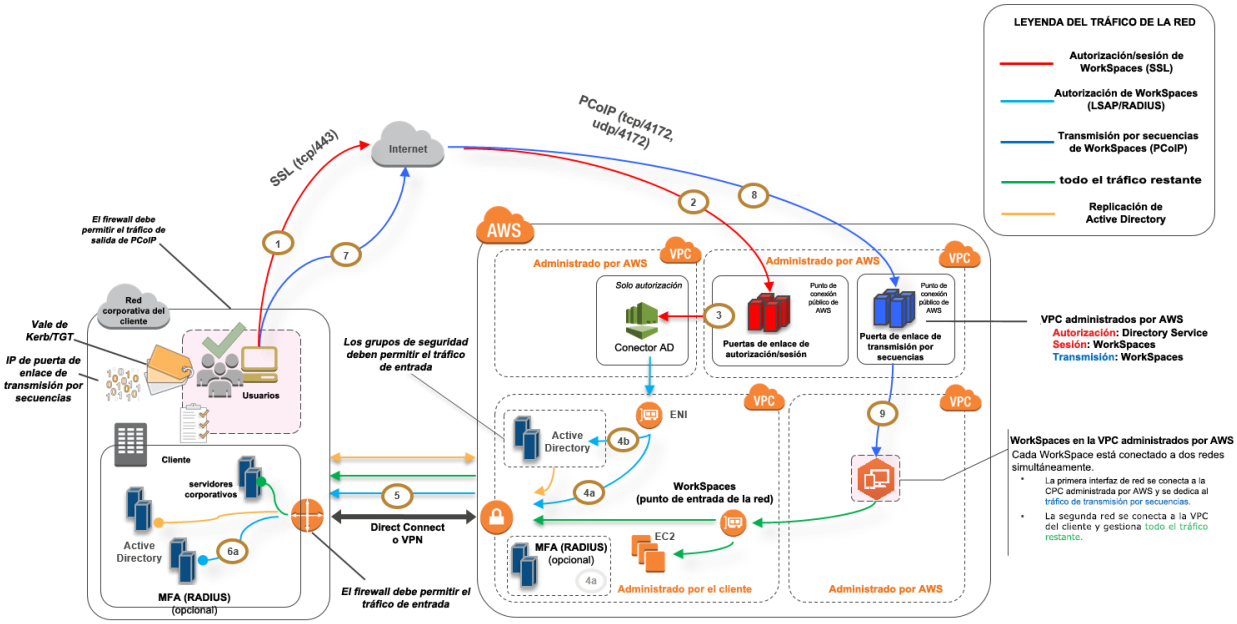

Figura 6: ampliación del dominio de Active Directory del cliente a la nube

Como en el escenario 1, el Conector AD se usa para la autenticación de todos los usuarios o MFA, lo cual, en consecuencia, se asigna al AD DS del cliente (Figura 5). En el escenario 2, el AD DS del cliente se implementa en las zonas de disponibilidad en las instancias de Amazon EC2 que se promueven como controladores de dominio en el bosque de Active Directory de las instalaciones del cliente y que se ejecutan en la nube de AWS. Cada uno de los controladores de dominio se implementa en las subredes privadas de la VPC para que AD DS quede altamente disponible en la nube de AWS. Para ver las prácticas recomendadas de implementación de AD DS en la nube de AWS, consulte Consideraciones de diseño más adelante en este documento técnico.

Una vez que las instancias de WorkSpaces se implementan, tienen acceso a los controladores de dominio basados en la nube para los servicios de directorio seguros y de baja latencia y el DNS. Todo el tráfico de la red, incluida la comunicación de AD DS, las solicitudes de autenticación y la replicación de Active Directory se asegura dentro de las subredes privadas o a través del túnel de VPN o DX del cliente.

Esta arquitectura utiliza los siguientes componentes o principios.

Amazon Web Services:

- **VPC de Amazon:** creación de una VPC de Amazon con al menos cuatro subredes privadas en dos zonas de disponibilidad (dos para el AD DS del cliente, dos para el Conector AD o WorkSpaces).
- **Conjunto de opciones del protocolo de configuración dinámica de host (DHCP, Dynamic Host Configuration Protocol):** creación de un conjunto de opciones del DHCP de la VPC de Amazon. Esto le permite definir un nombre de dominio especificado por el cliente y DNS (AD DS local). Para obtener más información, consulte Conjuntos de opciones de DHCP.
- **Puerta de enlace privada virtual de Amazon:** permite la comunicación con su propia red sobre un túnel de VPN IPsec o una conexión de AWS Direct Connect.
- **Amazon EC2:**
  - Controladores de dominio de AD DS corporativos del cliente implementados en las instancias de Amazon EC2 en subredes de VPC privadas dedicadas.
  - Servidores RADIUS "opcionales" del cliente para MFA.
- **AWS Directory Services**: el Conector AD se implementa en un par de subredes privadas de VPC de Amazon.
- **Amazon WorkSpaces:** los WorkSpacess se implementan en las mismas subredes privadas que el Conector AD (consulte Consideraciones sobre el diseño Conector AD).

Cliente:

- **Conectividad de la red:** VPN corporativa o puntos de conexión de AWS Direct Connect.
- **AD DS:** AD DS corporativo (requerido para la replicación).
- **MFA "opcional":** servidor RADIUS corporativo.

- **Dispositivos del usuario final:** dispositivos del usuario final corporativos o de tipo traiga su propia licencia (BYOL, Bring Your Own License) (como tabletas Windows, Mac, iPad o Android, Zero Client, Chromebook), que se usan para acceder al servicio Amazon WorkSpaces (consulte Plataformas y dispositivos compatibles).

A diferencia del escenario 1, esta solución no tiene las mismas desventajas. Por lo tanto, WorkSpaces y AWS Directory Service no dependen de la conectividad establecida.

- **Dependencia de la conectividad:** si se pierde la conectividad con el centro de datos del cliente, los usuarios finales pueden continuar trabajando, porque la autenticación y la MFA "opcional" se procesan localmente.
- **Latencia:** con la excepción del tráfico de replicación (consulte *Consideraciones sobre* el diseño*:* sitios y servicios de AD DS), toda la autenticación es local y de baja latencia.
- **Costos del tráfico:** en este escenario, la autenticación es local y solo la replicación de AD DS debe atravesar el vínculo de VPN o DX, lo cual reduce la transferencia de datos.

En líneas generales, se mejora la experiencia con WorkSpaces y esta no depende considerablemente del elemento 5, como se muestra en Figura 6. Esto se da de manera aun más significativa si desea ampliar la capacidad de WorkSpaces a miles de escritorios, especialmente en relación con las consultas del catálogo global de AD DS, ya que este tráfico permanece local en el entorno de WorkSpaces.

Escenario 3: implementación independiente aislada mediante el uso de AWS Directory Service en la nube de AWS

En este escenario, que figura en Figura 7, AD DS se implementó en la nube de AWS en un entorno independiente aislado. AWS Directory Service se usa exclusivamente en este escenario. En vez de administrar por completo AD DS usted mismo, depende del AWS Directory Service para realizar tareas como la creación de una topología de directorio altamente disponible, la monitorización de los controladores de dominio y la configuración de las copias de seguridad y las instantáneas.

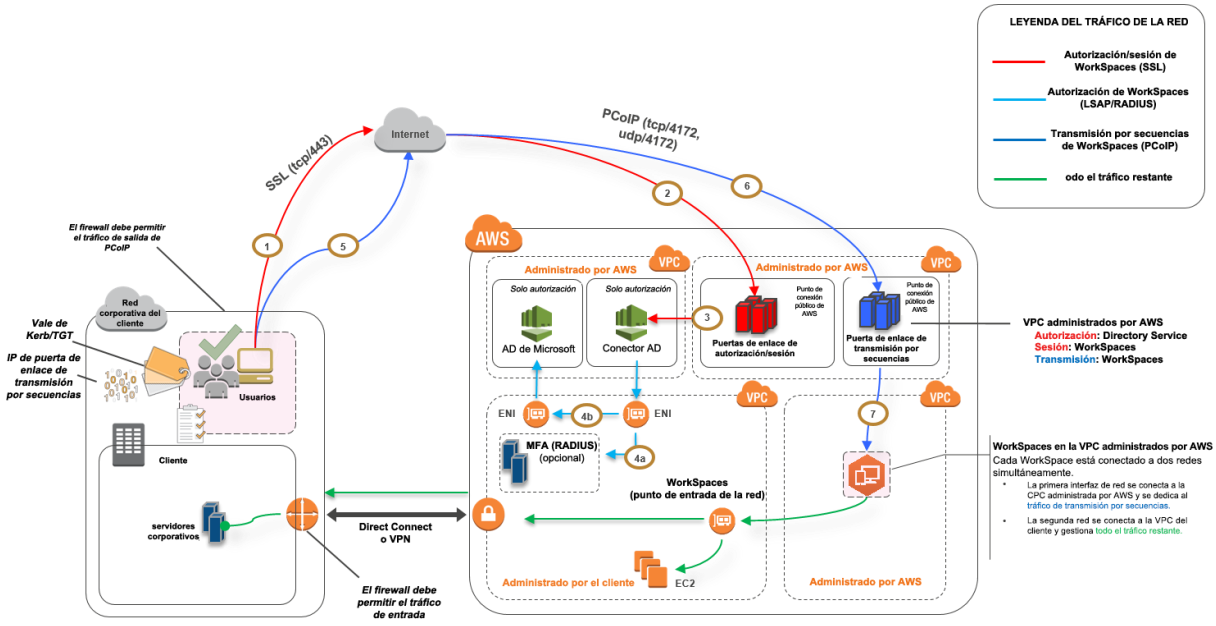

Figura 7: AWS Directory Services (AD de Microsoft) administrados únicamente en la nube

Como en el escenario 2, el AD DS (AD de Microsoft) se implementa en subredes dedicadas que distribuyen dos zonas de disponibilidad, lo cual hace que AD DS quede altamente disponible en la nube de AWS. Además del AD de Microsoft, se implementa el Conector AD (en los tres escenarios) para la autenticación de WorkSpaces o MFA. Esto garantiza una separación de roles o funciones dentro de la VPC de Amazon, que es una mejor práctica estándar (consulte la sección *Consideraciones sobre* el diseño: Redes con particiones).

En el escenario 3, observamos una configuración estándar de todo incluido que funciona bien para los clientes que desean que AWS administre la implementación, las revisiones, la alta disponibilidad y la monitorización de AWS Directory Service. Debido a su modo de aislamiento, además de la producción, el escenario también funciona bien para las pruebas de conceptos y los entornos de laboratorio.

Además del establecimiento de AWS Directory Service, Figura 7 muestra el flujo de tráfico desde un usuario a un espacio de trabajo y la manera en que el espacio de trabajo interactúa con el servidor de AD y el servidor de MFA.

Esta arquitectura utiliza los siguientes componentes o principios.

Amazon Web Services:

- **VPC de Amazon:** creación de una VPC de Amazon con al menos cuatro subredes privadas en dos zonas de disponibilidad (dos para el AD DS *AD de Microsoft*, dos para el Conector AD o WorkSpaces). "*Separación de roles*".
- **Conjunto de opciones del DHCP:** creación de un conjunto de opciones del DHCP de la VPC de Amazon. Esto le permite definir un nombre de dominio especificado por el cliente y DNS (AD de Microsoft). Para obtener más información, consulte Conjuntos de opciones de DHCP.
- **Opcional: puerta de enlace privada virtual de Amazon:** permite la comunicación con su propia red sobre un túnel de VPN IPsec (VPN) o una conexión de AWS Direct Connect. Se usa para acceder a los sistemas de back end en las instalaciones.
- **AWS Directory Service:** el AD de Microsoft se implementa en un par dedicado de subredes de VPC (Servicio administrado de AD DS).
- **Amazon EC2:** servidores RADIUS "opcionales" del cliente para MFA.
- **AWS Directory Services**: el Conector AD se implementa en un par de subredes privadas de la VPC de Amazon.
- **Amazon WorkSpaces:** los WorkSpacess se implementan en las mismas subredes privadas que el Conector AD (consulte Consideraciones sobre el diseño Conector AD).

Cliente:

- **Opcional: conectividad de la red:** VPN corporativa o puntos de conexión de AWS Direct Connect.
- **Dispositivos del usuario final:** dispositivos del usuario final corporativos o de tipo traiga su propia licencia (BYOL, Bring Your Own License) (como tabletas Windows, Mac, iPad o Android, Zero Client, Chromebook), que se usan para acceder al servicio Amazon WorkSpaces (consulte Plataformas y dispositivos compatibles).

Como en el escenario 2, con esta solución no se presentan problemas en cuanto a la dependencia de la conectividad al centro de datos de las instalaciones, la latencia o los costos de transferencias de datos (excepto cuando se habilita el acceso a Internet para WorkSpaces dentro de la VPC) debido a que, por su diseño, este es un escenario aislado o en la nube únicamente.

Consideraciones sobre el diseño

Una implementación funcional del AD DS en la nube de AWS requiere comprender bien los conceptos de Active Directory y los servicios específicos de AWS. En esta sección, abordaremos las consideraciones sobre diseño principales en el momento de implementar AD DS para WorkSpaces, las prácticas recomendadas de la VPC para AWS Directory Service, los requisitos del DHCP y DNS, los aspectos específicos del Conector AD y los sitios y servicios de Active Directory.

Diseño de la VPC

Como abordamos en la sección Consideraciones de red de este documento y mencionamos anteriormente en los escenarios 2 y 3, debe implementar AD DS en la nube de AWS en un par dedicado de subredes privadas, a través de dos zonas de disponibilidad, y por separado del Conector AD o las subredes de WorkSpaces. Mediante este principio, se ofrece un acceso altamente disponible y de baja latencia a los servicios de AD DS para WorkSpaces, mientras se conservan las prácticas recomendadas estándares de separación de roles o funciones dentro de la VPC de Amazon.

En la Figura 8 se muestra la separación de AD DS y el Conector AD en subredes privadas dedicadas (escenario 3). En este ejemplo, todos los servicios se encuentran en la misma VPC de Amazon.

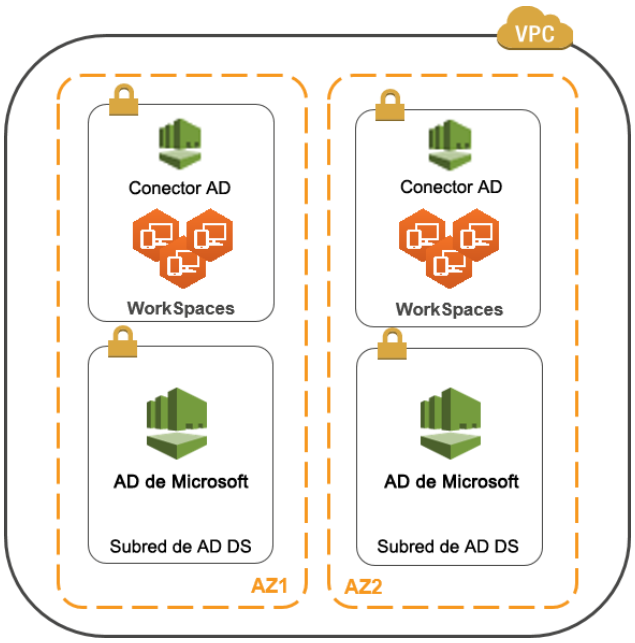

Figura 8: segregación de la red AD DS

En la Figura 9, se muestra un diseño similar al escenario 1. Sin embargo, en este escenario la parte de las instalaciones se encuentra en una VPC de Amazon dedicada.

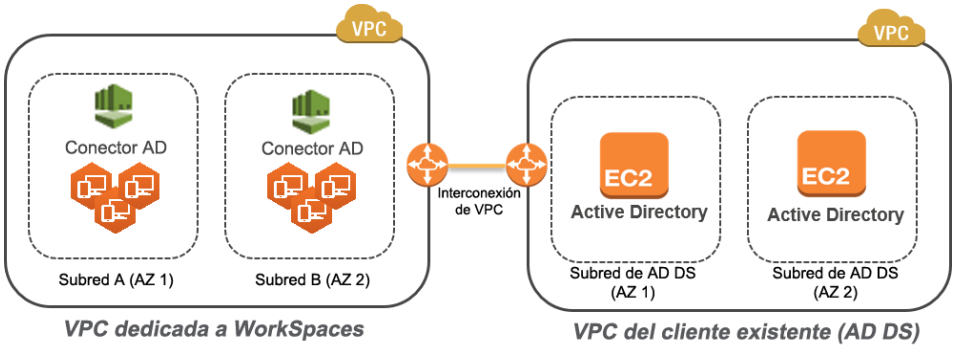

Figura 9: VPC de WorkSpaces dedicada

> **Nota:** Para los clientes que tienen una implementación de AWS existente en la que se usa un AD DS, le recomendamos que coloque sus WorkSpaces en una VPC dedicada y que use una interconexión de la VPC para las comunicaciones del AD DS.

Además de la creación de subredes privadas dedicadas para el AD DS, los controladores de dominio y los servidores de miembro requieren de varias reglas de grupos de seguridad para permitir el tráfico a los servicios, como la replicación del AD DS, la autenticación del usuario, los servicios de Hora de Windows y el sistema de archivos distribuidos (DFS, Distributed File System).

> **Nota:** Una de las prácticas recomendadas es restringir las reglas del grupo de seguridad requeridas en las subredes privadas de WorkSpaces y, en el caso del escenario 2, permitir comunicaciones de AD DS bidireccionales en las instalaciones hacia o desde la nube de AWS, como se muestra en la siguiente tabla.

Protocolo	Puerto	Uso	Destino
tcp	53, 88, 135, 139, 389, 445, 464, 636	Autorización (primaria)	Active Directory (centro de datos privado o EC2)*
tcp	49152 – 65535	Puertos altos de RPC	Active Directory (centro de datos privado o EC2)**
tcp	3268-3269	Confianzas	Active Directory (centro de datos privado o EC2)*
tcp	9389	Microsoft Windows PowerShell remoto (opcional)	Active Directory (centro de datos privado o EC2)*
udp	53, 88, 123, 137, 138, 389, 445, 464	Autorización (primaria)	Active Directory (centro de datos privado o EC2)*
udp	1812	Autorización (MFA) (opcional)	RADIUS (centro de datos privado o EC2)*

* Consulte Requisitos de puerto de Active Directory y de los servicios de dominio de Active Directory.

**Consulte Descripción general del servicio y requisitos del puerto de la red para Windows.

Para obtener instrucciones paso por paso 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 la VPC: DHCP y DNS

Con la VPC de Amazon, se brindan los servicios de DHCP de manera predeterminada para sus instancias. De manera predeterminada, cada VPC proporciona un servidor DNS interno al que se puede acceder a través del espacio de dirección +2 del enrutamiento entre dominios sin clases (CIDR, Classless Inter-Domain Routing) y se asigna a todas las instancias a través de un conjunto de opciones del DHCP predeterminado.

Los conjuntos de opciones del DHCP se usan dentro de la VPC de Amazon para definir las opciones del ámbito, como el nombre de dominio o los servidores de nombre que deberían entregarse a sus instancias a través del DHCP. La correcta funcionalidad de los servicios de Windows dentro de su VPC depende de esta opción de ámbito del DHCP y debe configurarla correctamente. En cada uno de los escenarios definidos anteriormente, crearía y asignaría su propio ámbito que definiría su nombre de dominio y sus servidores de nombre. Esto garantiza que las instancias de Windows unidas por dominios o los WorkSpaces se configuren para usar el DNS de Active Directory. La siguiente tabla es un ejemplo del conjunto personalizado de opciones del ámbito del DHCP que debe crearse para que WorkSpaces y los servicios de directorio de AWS funcionen correctamente.

Parámetro	Valor
Etiqueta del nombre	Crea una etiqueta con una clave = **nombre** y **valor** configurados en una cadena específica Ejemplo: exampleco.com
Nombre del dominio	exampleco.com
Servidores del nombre del dominio	Direcciones del servidor DNS, separados por comas. Ejemplo: 10.0.0.10, 10.0.1.10
Servidores NTP	Dejar este campo en blanco.
Servidores del nombre NetBIOS	Ingrese las mismas IP separadas por comas por servidores de nombre del dominio. Ejemplo: 10.0.0.10, 10.0.1.10
Tipo de nodo NetBIOS	2

Para obtener detalles sobre cómo crear un conjunto de opciones del DHCP y asociarlo con su VPC de Amazon, consulte Trabajar con conjuntos de opciones del DHCP que figura en la *Guía del usuario de la red privada virtual de Amazon*.

En el escenario 1, el ámbito del DHCP estaría en el DNS en las instalaciones o en el AD DS. Sin embargo, en el escenario 2 o 3, este sería el servicio de directorio implementado localmente (AD DS en Amazon EC2 o los servicios de directorio de AWS: AD de Microsoft). Le recomendamos que haga que cada controlador de dominio que se encuentre en la nube de AWS sea un catálogo global y un servidor DNS integrado del directorio.

Active Directory: sitios y servicios

Para el escenario 2, los sitios y los servicios son componentes fundamentales par el correcto funcionamiento del AD DS. La topología del sitio controla la replicación de Active Directory entre los controladores de dominio dentro del mismo sitio y a través de los límites del sitio. En el escenario 2, hay al menos dos sitios, en las instalaciones y AWS WorkSpaces en la nube. Definir la topología correcta del sitio garantiza una afinidad con el cliente, lo que significa que los clientes (en este caso, WorkSpaces) usan su controlador de dominio local preferido.

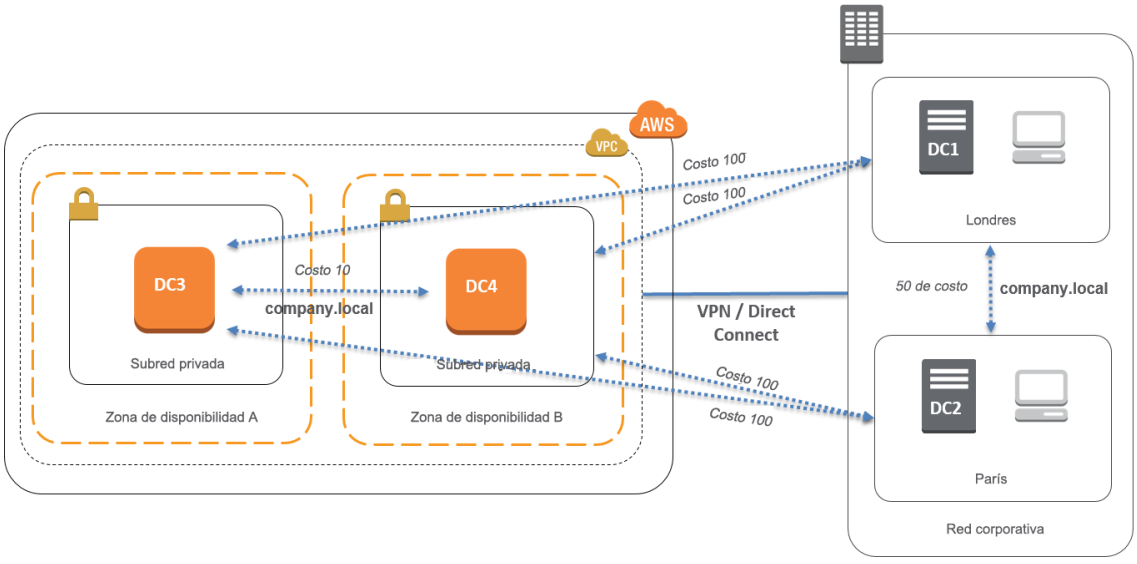

Figura 10: sitios y servicios de Active Directory: afinidad del cliente

Mejor práctica Definir un costo alto para los vínculos del sitio entre el AD DS del sitio y la nube de AWS. En la Figura 10 se ejemplifican los costos que se deben asignar a los vínculos del sitio (100 de costo) para garantizar una afinidad del cliente independiente del sitio.

Mediante estas asociaciones se ayuda a garantizar que el tráfico, como la replicación de AD DS y la autenticación del cliente, use la ruta más eficaz hacia un controlador de dominio. En el caso de los escenarios 2 y 3, esto ayuda a garantizar una menor latencia y un tráfico de vínculo cruzado.

Autenticación multifactor (MFA)

Implementar la MFA requiere que la infraestructura de WorkSpaces utilice un Conector AD como su AWS Directory Service y tenga un servidor RADIUS. Aunque en este documento no se aborde la implementación de un servidor RADIUS, en la sección anterior, Escenarios de implementación de AD DS, se detalla el establecimiento de RADIUS en cada escenario.

MFA: autenticación de dos factores

Amazon WorkSpaces es compatible con la MFA a través del AWS Directory Service: el Conector AD y un servidor RADIUS *de propiedad del cliente*. Una vez habilitada, los usuarios deben ingresar un **nombre de usuario**, una **contraseña** y un **código de MFA** al cliente WorkSpaces para la autenticación en sus escritorios de WorkSpaces correspondientes.

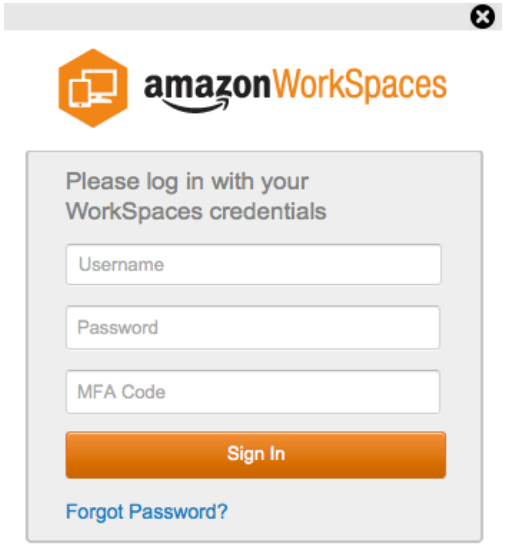

Figura 11: cliente WorkSpaces con MFA habilitada

> **Regla fija** Para implementar la autenticación MFA necesita usar un Conector AD. El Conector AD no es compatible con la MFA "por usuario" selectiva, ya que esta es una configuración global por Conector AD. Si necesita una MFA "por usuario" selectiva, debe separar a los usuarios según el Conector AD.

La MFA de WorkSpaces requiere de un servidor RADIUS o más. Generalmente, estas son soluciones existentes, por ejemplo RSA, o bien los servidores se pueden implementar dentro de la VPC (consulte Escenarios de implementación de AD DS). Si está usando una nueva solución RADIUS, existen varias implementaciones en la industria actualmente, como FreeRADIUS y servicios en la nube como Duo Security.

Para obtener una lista de los requisitos previos para implementar la MFA con Amazon WorkSpaces, consulte la *Guía de administración de Amazon WorkSpaces*, Preparación de la red para un directorio de Conector AD. El proceso para configurar su Conector AD para MFA se describe en Administración de un directorio de Conector AD: autenticación multifactor, en la *Guía de administración de Amazon WorkSpaces*.

Seguridad

En esta sección, se explica cómo asegurar datos a través del cifrado cuando usa los servicios de Amazon WorkSpaces. Describiremos el cifrado en tránsito y en reposo además de la utilización de los grupos de seguridad para proteger el acceso desde la red a los WorkSpaces. Puede encontrar más información sobre la autenticación (incluida la compatibilidad con MFA) en la sección AWS Directory Service.

Cifrado en tránsito

Amazon WorkSpaces utiliza la criptografía para proteger la confidencialidad en diferentes etapas de la comunicación (en tránsito) y también para proteger los datos en reposo (WorkSpaces cifrados). Los procesos que forman parte de cada etapa del cifrado que usa Amazon WorkSpaces en tránsito se describen en las siguientes secciones. Para obtener información sobre el cifrado en reposo, consulte la sección WorkSpaces cifrados que figura más adelante en este documento técnico.

Registro y actualizaciones

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

Etapa de autenticación

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

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

Luego de recibir las credenciales del cliente, la puerta de enlace de autenticación envía una solicitud de autenticación al AWS Directory Service. La comunicación desde la puerta de enlace de autenticación al AWS Directory Service se lleva a cabo sobre HTTPS, de modo que no se transmite como texto sin cifrar ninguna de las credenciales del usuario.

Autenticación: Conector AD

El Conector AD utiliza Kerberos para establecer una comunicación autenticada con el AD en las instalaciones, por lo que puede vincularse con el protocolo ligero de acceso a directorios (LDAP, Lightweight Directory Access Protocol) y ejecutar las consultas de LDAP subsiguientes. En este momento, el AWS Directory Service no es compatible con LDAP con TLS (LDAP). Sin embargo, no se transmite ninguna credencial del usuario en texto sin cifrar en ningún momento. Para aumentar la seguridad, puede conectar su VPC de WorkSpaces con su red en las instalaciones (donde se encuentra su AD) a través de una conexión de VPN. Cuando utiliza una conexión VPN de hardware de AWS, configurará el cifrado en tránsito mediante el uso de una IPSEC estándar (intercambio de claves por red [IKE, Internet Key Exchange] y SA de IPSEC) con las claves de cifrado simétricas AES-128 o AES-256, SHA-1 o SHA-256 para el hash de integración y los 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 uso de PFS.

Etapa de intermediario

Luego de recibir el token OAuth 2.0 (de la puerta de enlace de autenticación, si la autenticación se realizó con éxito), el cliente de escritorio consultará los servicios de Amazon WorkSpaces (administrador de conexión del agente) mediante HTTPS. El cliente de escritorio se autentica al enviar el token OAuth 2.0 y, como resultado, el cliente recibirá la información del punto de conexión de la puerta de enlace de transmisión por secuencias de WorkSpaces.

Etapa de transmisión por secuencias

El cliente de escritorio solicita que se abra una sesión de computadora personal sobre protocolo de Internet (PCoIP, Personal Computer over Internet Protocol) con la puerta de enlace de transmisión por secuencias (mediante el uso del token OAuth 2.0). Esta sesión está cifrada a través de aes256 y usa el puerto PCoIP para el control de la comunicación (es decir, 4172/tcp).

Mediante el uso del token OAuth2.0, la puerta de enlace de transmisión por secuencias solicita la información de los WorkSpaces específicos del usuario desde el servicio WorkSpaces, sobre HTTPS.

La puerta de enlace de transmisión por secuencias también recibe el TGT del cliente (que está cifrado mediante el uso de la contraseña del usuario del cliente) y, mediante la transmisión TGT de Kerberos, la puerta de enlace comienza un inicio de sesión de Windows en el WorkSpace utilizando la TGT de Kerberos obtenida del usuario.

El WorkSpace luego comienza una solicitud de autenticación del AWS Directory Service configurado, mediante el uso de la autenticación estándar de Kerberos.

Luego de que el WorkSpace inició sesión correctamente, comienza la transmisión por secuencias de la PCoIP. El cliente comienza la conexión en el puerto tcp 4172 con el tráfico de retorno en el puerto udp 4172. Además, la conexión inicial entre la puerta de enlace de transmisión por secuencias y su escritorio de WorkSpaces por la interfaz de administración se realiza a través de UDP 55002 (Consulte la documentación de Amazon WorkSpaces, Detalles de Amazon WorkSpaces. El puerto UDP de salida inicial es el 55002). La conexión de transmisión por secuencias, mediante el uso del puerto 4172 (tcp y udp), se cifra con los códigos cifrados AES 128 y de 256 bits, pero la opción predeterminada es de 128 bits. Puede cambiar esto a 256 bits activamente a través de una política de grupo (GPO, Group Policy) específica de Active Directory de PCoIP (pcoip.adm).

Interfaces de red

En cada Amazon WorkSpace hay dos interfaces de red llamadas interfaz de red primaria e interfaz de red de administración.

La interfaz de red primaria proporciona conectividad a los recursos dentro de su VPC, como acceso al servicio de directorio de AWS, Internet y su red corporativa. Se pueden adjuntar grupos de seguridad a esta interfaz de red primaria (como haría con cualquier interfaz de red elástica [ENI, Elastic Network Interface]). Conceptualmente, marcamos una diferencia entre los grupos de seguridad adjuntos a esta ENI sobre la base del ámbito de la implementación: grupo de seguridad de WorkSpaces y grupos de seguridad de ENI.

Interfaz de red de administración

No puede controlar la interfaz de red de administración a través de los grupos de seguridad, pero puede aprovechar un firewall basado en un host en su WorkSpace para bloquear los puertos y controlar el acceso. No recomendamos que aplique restricciones en la interfaz de red de administración. Si decide agregar reglas de firewall basadas en un host para administrar esta interfaz, debe mantener abiertos algunos puertos para que el servicio de WorkSpace pueda administrar el estado y la accesibilidad al WorkSpace como se define en la Guía de administración de Amazon WorkSpaces.

Grupo de seguridad de WorkSpaces

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

Como sucede con cualquier otro grupo de seguridad, es posible modificar las reglas de un grupo de seguridad de WorkSpaces. Los resultados entran en vigencia inmediatamente después de que se aplican los cambios.

También se puede cambiar el grupo de seguridad de WorkSpaces predeterminado por un AWS Directory Service al cambiar la asociación del grupo de seguridad de WorkSpaces.

> **Nota:** Se adjuntará un grupo de seguridad recientemente asociado a los WorkSpaces que se crearon o volvieron a construir luego de la modificación.

Grupos de seguridad de la ENI

Debido a que la interfaz de red primaria es una ENI regular, puede administrar su configuración mediante el uso de diferentes herramientas de administración de AWS (consulte Interfaz de red elástica [ENI]). Particularmente, busque el IP del WorkSpace (en la página WorkSpaces en la consola de Amazon WorkSpaces) y luego use esa dirección IP como filtro para encontrar la ENI correspondiente (en la sección Interfaces de red de la consola de Amazon EC2).

Una vez que encontró la ENI, puede administrar los grupos de seguridad directamente desde allí. Al asignar manualmente grupos de seguridad a la interfaz de red primaria, tenga en cuenta los requisitos de puerto de Amazon WorkSpaces como se explica en Detalles de Amazon WorkSpaces.

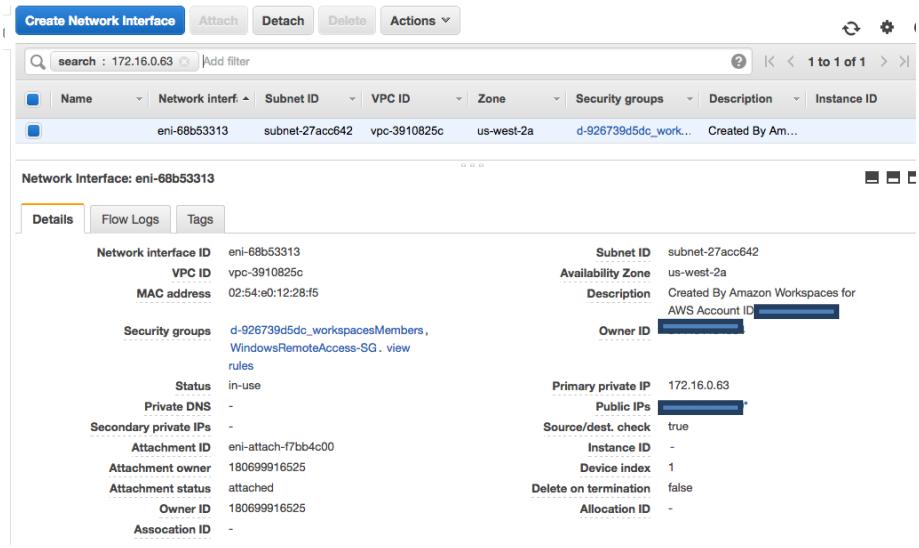

Figura 12: Administración de asociaciones del grupo de seguridad

WorkSpaces cifrados

Cada Amazon WorkSpace viene con un volumen de raíz (unidad C:) y un volumen de usuario (unidad D:). La característica de WorkSpaces cifrados le permite cifrar cualquiera de los volúmenes o ambos.

¿Qué es lo que se cifra?

Se cifran los datos almacenados en reposo, la E/S del disco al volumen y las instantáneas creadas a partir de volúmenes cifrados.

¿Cuándo se realiza el cifrado?

Debe especificar el cifrado de un WorkSpace al ejecutar (crear) WorkSpace. Los volúmenes de los WorkSpaces se pueden cifrar únicamente en el momento de la ejecución, ya que luego de esta no puede cambiar el estado de cifrado de un volumen. En la Figura 13 se muestra la página de la consola de Amazon WorkSpaces para seleccionar el cifrado durante la ejecución de un nuevo WorkSpace.

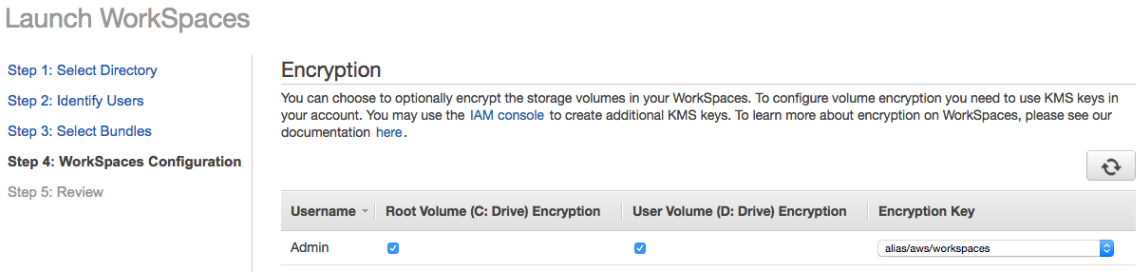

Figura 13: cifrado de volúmenes de WorkSpaces

¿Cómo se cifra un nuevo WorkSpace?

Puede seleccionar la opción Encrypted WorkSpaces en la consola de Amazon WorkSpaces o en la interfaz de línea de comandos (CLI, Command Line Interface) de AWS, o mediante el uso de la API de Amazon WorkSpaces cuando ejecute un nuevo WorkSpace.

Para cifrar los volúmenes, Amazon WorkSpaces usa una clave maestra del cliente (CMK, Customer Master Key) del AWS Key Management Service (KMS). Se crea una CMK de AWS KMS la primera vez que se ejecuta un WorkSpace en una región (las CMK tienen un ámbito de región). También puede crear una CMK administrada por el cliente para usarla con los WorkSpaces cifrados. La CMK se usa para cifrar las claves de datos que usa el servicio Amazon WorkSpaces para cifrar los volúmenes (en sentido estricto, el servicio Amazon Elastic Block Store [Amazon EBS] será el encargado de cifrar los volúmenes). Cada CMK puede utilizarse para cifrar claves de hasta 30 WorkSpaces.

> **Nota:** Actualmente, no es compatible la creación de imágenes personalizadas desde un WorkSpace cifrado. Además, los WorkSpaces que se ejecutan con un cifrado de volumen de raíz habilitado pueden demorar hasta una hora para llevarse a cabo.

Para obtener una descripción detallada sobre el proceso de cifrado de WorkSpaces, consulte Descripción general del cifrado de Amazon WorkSpaces mediante el uso de AWS KMS. Para obtener más información sobre las claves maestras del cliente y las claves de datos de AWS KMS, consulte Conceptos de AWS Key Management Service.

Monitorización y registro mediante Amazon CloudWatch

La monitorización es una parte integral de cualquier infraestructura, ya sea una red, servidores o registros. Los clientes que usan Amazon WorkSpaces deben monitorizar sus implementaciones, específicamente el estado de funcionamiento y conexión general de los WorkSpaces individuales.

Métricas de Amazon CloudWatch para WorkSpaces

Las métricas de CloudWatch para WorkSpaces están diseñadas para ofrecerles a los administradores más información sobre el estado de funcionamiento y conexión general de los WorkSpaces individuales. Las métricas se encuentran disponibles por WorkSpace o se agregan para todos los WorkSpaces en una organización dentro de un determinado directorio (*Conector AD, consulte Identidad*).

Estas métricas, como todas las métricas de CloudWatch, se pueden ver en la Consola de administración de AWS (Figura 13) y se puede acceder a ellas a través de las API de CloudWatch. Además, se pueden monitorizar a través de las alarmas de CloudWatch y herramientas de terceros.

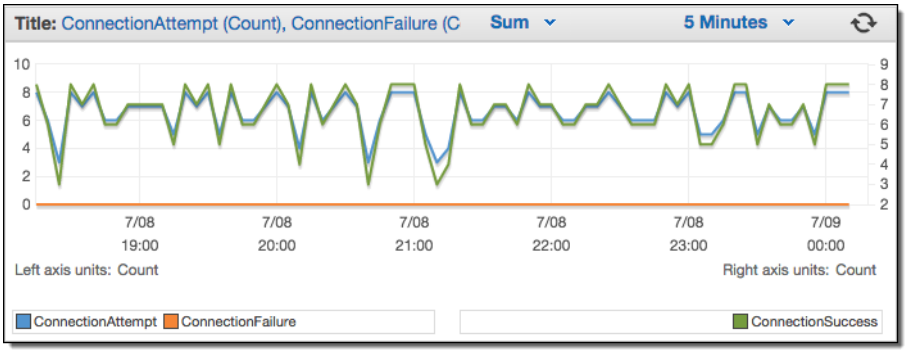

Figura 14: métricas de CloudWatch: ConnectionAttempt/ConnectionFailure

Las siguientes métricas están habilitadas de manera predeterminada y se encuentran disponibles sin costo adicional:

- **Disponible**: se cuentan en esta métrica los WorkSpaces que responden a una verificación de estado.
- **Mal funcionamiento**: se cuentan en esta métrica los WorkSpaces que no responden a la misma verificación de estado.
- **ConnectionAttempt**: la cantidad de intentos de conexión a un WorkSpace.
- **ConnectionSuccess**: la cantidad de intentos de conexión correctos.
- **ConnectionFailure**: la cantidad de intentos de conexión incorrectos.
- **SessionLaunchTime**: el tiempo que se demora en iniciar una sesión, según las mediciones del cliente de WorkSpaces.
- **InSessionLatency**: el tiempo de ida y vuelta entre el cliente de WorkSpaces y los WorkSpaces, según las mediciones e informes del cliente.
- **SessionDisconnect**: la cantidad de sesiones iniciadas por el usuario y cerradas automáticamente.

Además, se pueden crear alarmas, como se muestra en la Figura 15.

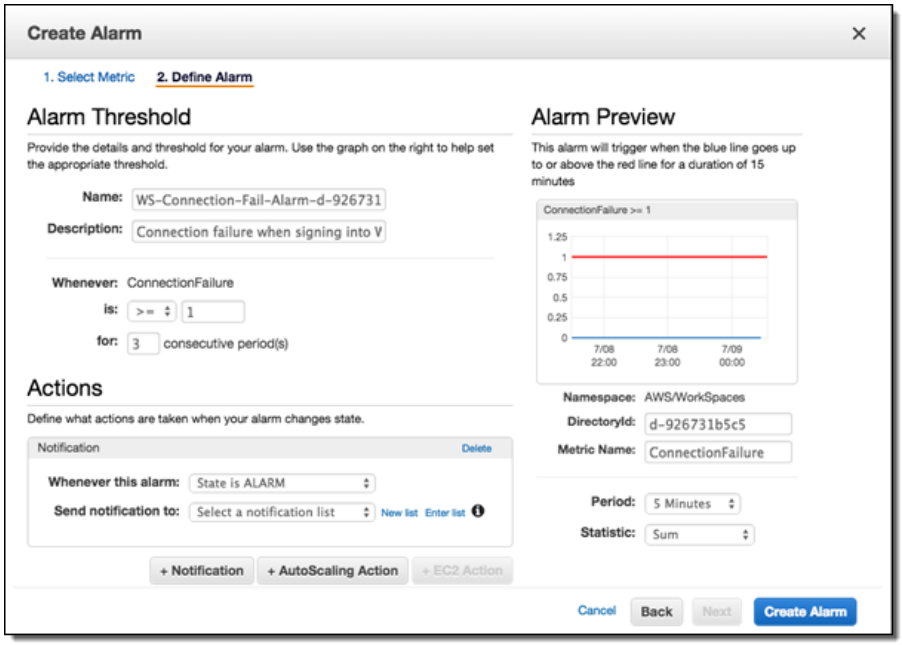

Figura 15: creación de alarma de CloudWatch para los errores de conexión de WorkSpaces

Resolución de problemas

Se pueden encontrar los problemas más comunes de la administración y el cliente, como "Aparece el siguiente mensaje de error: 'Su dispositivo no se puede conectar al servicio de registro de WorkSpaces'" o "No puedo conectarme a un WorkSpace con un banner de inicio de sesión interactivo", en las páginas de resolución de problemas del cliente y de administración en la *Guía de administración de Amazon WorkSpaces*.

El Conector AD no puede conectarse a Active Directory.

Para que el Conector AD pueda conectarse a su directorio en las instalaciones, el firewall de su red en las instalaciones debe tener determinados puertos abiertos en el enrutamiento entre dominios sin clases (CIDR, Classless Inter-Domain Routing) para ambas subredes en la VPC (consulte Conector AD). Para probar si se cumplen las condiciones, siga los siguientes pasos.

Para verificar la conexión

1. Ejecute una instancia de Windows en la VPC y conéctese a esta sobre el protocolo de escritorio remoto (RDP, Remote Desktop Protocol). Los pasos restantes se llevan a cabo en la instancia de VPC.
2. Descargue la aplicación de prueba DirectoryServicePortTest y descomprímala. Se incluyen el código fuente y los archivos del proyecto de Visual Studio para que pueda modificar la aplicación de prueba, si así lo desea.
3. Desde un símbolo del sistema de Windows, ejecute la aplicación de prueba DirectoryServicePortTest 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*>

Nombre de dominio completamente calificado que se usa para probar el bosque y los niveles funcionales del dominio. Si excluye el nombre del dominio, no se probarán los niveles funcionales.

<*server_IP_address*>

Dirección IP de un controlador de dominio en su dominio en las instalaciones. Se evaluarán los puertos frente a esta dirección IP. Si excluye la dirección IP, no se probarán los puertos.

Mediante esto se determinará si los puertos necesarios están abiertos desde la VPC a su dominio. Con la aplicación de prueba también se verifica el bosque mínimo y los niveles funcionales del dominio.

Cómo verificar la latencia en la región de AWS más cercana

En octubre de 2015, Amazon WorkSpaces lanzó el sitio web Connection Health Check. Mediante el sitio web, se verifica rápidamente si puede obtener todos los servicios requeridos para usar WorkSpaces. También se realiza una verificación de rendimiento en cada región de AWS donde se ejecuta WorkSpaces, lo cual permite a los usuarios saber cuál será el más rápido para ellos.

Conclusión

Estamos observando un cambio estratégico en la informática del usuario final mientras 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 informática en la nube también se aplican a la informática del usuario final. Al mover sus escritorios a la nube de AWS con Amazon WorkSpaces, las organizaciones pueden ampliar la capacidad rápidamente a medida que agregan trabajadores, mejorar su posición respecto de la seguridad al quitar los datos del dispositivo y ofrecer a sus trabajadores un escritorio portátil con acceso en cualquier lugar desde el dispositivo de su elección.

Amazon WorkSpaces está diseñado para integrarse a sistemas y procesos de TI existentes y en este documento técnico se describen las prácticas recomendadas para lograrlo. El resultado de las siguientes instrucciones en este documento técnico es la implementación de un escritorio en la nube rentable que escala con sus negocios en la infraestructura global de AWS.

Colaboradores

Las siguientes personas participaron en la elaboración de este documento:

- Justin Bradley, arquitecto de soluciones, Amazon Web Services
- Mahdi Sajjadpour, asesor sénior, Servicios Profesionales de AWS
- Mauricio Munoz, arquitecto de soluciones, Amazon Web Services

Documentación adicional

Para obtener ayuda adicional, consulte las siguientes fuentes:

- Resolución de problemas de administración del AWS Directory Service
- Resolución de problemas de administración de Amazon WorkSpaces
- Resolución de problemas del cliente de Amazon WorkSpaces
- Guía de administración de Amazon WorkSpaces
- Guía del desarrollador de Amazon Workspaces
- Plataformas y dispositivos compatibles
- Cómo Amazon WorkSpaces utiliza AWS KMS
- Referencia de comando AWS CLI: WorkSpaces
- Monitorización de las métricas de Amazon WorkSpaces