Guía de Seguridad de las TIC
CCN-STIC 887E

Guía de configuración segura para Amazon WorkSpaces

Marzo 2024

MINISTERIO DE DEFENSA

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN centro criptológico nacional
CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2024.03.26 16:57:00 +01'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-24-123-X

Fecha de Edición: marzo de 2024

LIMITACIÓN DE RESPONSABILIDAD
El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

ÍNDICE

1. GUÍA DE CONFIGURACIÓN SEGURA PARA AMAZON WORKSPACES

1.1 DESCRIPCIÓN DEL USO DE ESTA GUÍA

El objetivo de la presente guía es documentar las recomendaciones de seguridad para la implementación segura del servicio Amazon WorkSpaces. Las recomendaciones incluidas en esta guía son específicas para esta solución y se deberán, en su caso, complementar con los requisitos y recomendaciones de seguridad explicados, para cualquier entorno AWS en la guía ***CCN-STIC 887A – Guía de Configuración Segura para AWS***, especialmente cuando se busque el cumplimiento del Esquema Nacional de Seguridad en el sistema desplegado en AWS.

Es por ello por lo que el uso de esta guía se recomienda para aquellas entidades que utilicen el servicio Amazon WorkSpaces.

Los asuntos relacionados con la seguridad y la conformidad son una responsabilidad compartida entre AWS, la cual puede ser consultada en la guía CCN-STIC 887A Guía de Configuración Segura para AWS en la sección 1.3.

1.2 DEFINICIÓN DEL SERVICIO

Amazon WorkSpaces es un servicio que permite aprovisionar escritorios virtuales de Microsoft Windows, Amazon Linux o Ubuntu conocidos como WorkSpaces basados en la nube. Este servicio elimina la necesidad de adquirir e implementar hardware o de instalar software pesado. Amazon WorkSpaces puede agregar o eliminar rápidamente usuarios en función de las necesidades. El acceso de los usuarios a los escritorios virtuales se ofrece desde diversos sistemas operativos, dispositivos o navegadores web que se detallan en el siguiente enlace.

Las principales ventajas de Amazon WorkSpaces son:

- Simplificación del escritorio. Ayuda a eliminar tareas administrativas asociadas con el aprovisionamiento y mantenimiento del escritorio. A su vez reduce la cantidad de hardware que hay que administrar.
- Seguridad de los datos. Se implementa dentro de una red virtual privada (VPC) de Amazon. No se almacenan datos de usuario en el dispositivo local, ayudando a mejorar la seguridad de los datos del usuario. Se puede utilizar autenticación multifactor y también es posible el cifrado de datos a través de AWS KMS.
- Administración y escalabilidad. Brinda acceso a escritorios en la nube dondequiera que trabajen los usuarios. Se puede administrar una implementación global desde la consola de AWS. Permite el aprovisionamiento y eliminación de escritorios rápidamente en función de las necesidades.

1.3 DESCRIPCION DE LA ARQUITECTURA

Cada WorkSpace está asociado a una nube virtual privada (VPC) y a un directorio para almacenar y administrar información de los usuarios de Amazon WorkSpaces. Los directorios se administran a través de AWS Directory Service.

Amazon WorkSpaces utiliza el directorio activo para autenticar a los usuarios. Los usuarios acceden a su Amazon WorkSpaces mediante una aplicación cliente desde un dispositivo compatible o, para Windows WorkSpaces, un navegador web, e inician sesión con sus credenciales de directorio. La información de inicio de sesión se envía a un gateway de autenticación, que reenvía el tráfico al directorio de la WorkSpace. Una vez autenticado el usuario, el tráfico de streaming se inicia a través de un Gateway de transmisión.

Las aplicaciones cliente utilizan HTTPS a través del puerto 443 (TCP) para todas las sesiones de autenticación y de trabajo. Las aplicaciones cliente utilizan los puertos 4172 (PCoIP) y 4195 (WSP) para la transmisión de píxeles al WorkSpace y los puertos 4172 y 4195 (TCP/UDP) para las comprobaciones de estado de la red.

Cada WorkSpace tiene dos interfaces elásticas de red: un interfaz de red para la administración y la transmisión (eth0) y un interfaz de red principal (eth1). El interfaz de red principal tiene una dirección IP proporcionada por la VPC, procedente de las mismas subredes que se utilizan en el directorio. De este modo, se garantiza que el tráfico procedente de un WorkSpace pueda llegar fácilmente al directorio. El acceso a los recursos de la VPC se controla mediante los security groups asignados a la interfaz de red principal.

Amazon WorkSpaces utiliza un directorio para almacenar y administrar la información de sus WorkSpaces y usuarios. Las opciones que tiene disponibles son AD Connector, AWS Managed Microsoft AD, Simple AD y Cross trust (Confianza cruzada).

En el siguiente diagrama se muestra la arquitectura de Amazon WorkSpaces y los diferentes pasos que ocurren cuando un usuario de AWS accede a un WorkSpace usando un directorio activo.

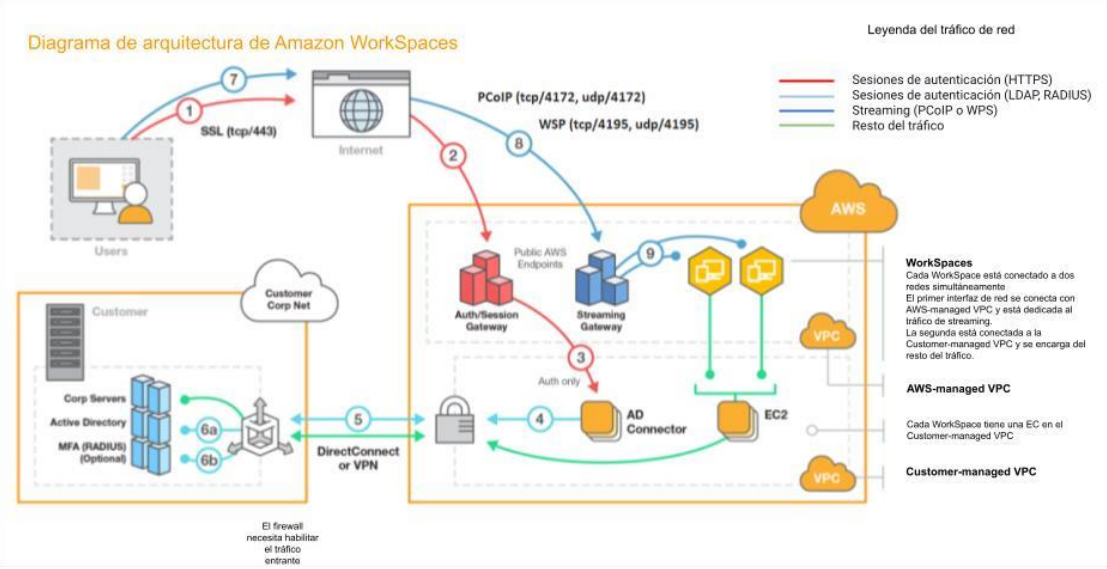

Fig. 2 - Diagrama de una arquitectura de ejemplo de Amazon WorkSpaces

1. El usuario solicita acceso a los WorkSpaces mediante una aplicación cliente desde un dispositivo compatible o para Windows WorkSpaces o un navegador web.
2. La aplicación o navegador web solicita el inicio de sesión a través de un Gateway.
3. La sesión se inicia con las credenciales de directorio (Simple AD, AD Connector, AWS Managed Microsoft Active Directory).
4. La información de inicio de sesión se envía a una pasarela de autenticación.
5. Se reenvía el tráfico al directorio del WorkSpace.
6. Cuando el usuario es autenticado, se inicia el tráfico de streaming a través de la Gateway de streaming.
7. Las aplicaciones cliente utilizan HTTPS a través del puerto 443 para todas las sesiones de autenticación y la información relacionada.
8. Las aplicaciones cliente utilizan el puerto 4172 (PCoIP) y el puerto 4195 (WSP) para la transmisión de píxeles a WorkSpace y los puertos 4172 y 4195 para comprobar el estado de la red.
9. Cada WorkSpace tiene dos interfaces de red elásticas asociadas
    a Interfaz de red para administración y transmisión (eth0)
    b Interfaz de red principal (eth1)

2. RECOMENDACIONES DE SEGURIDAD PARA AMAZON WORKSPACES

En los siguientes aparatados se especifican, por ámbitos de seguridad, las recomendaciones para tener en cuenta para un despliegue y uso seguro de Amazon WorkSpaces.

Adicionalmente, y para una mejor implementación de la seguridad a la hora de trabajar con Amazon WorkSpaces, se recomienda la consulta del documento Prácticas recomendadas para implementar Amazon WorkSpaces.

2.1 CONTROL DE ACCESO

Identificación de usuarios

Tal y como ya se ha anticipado, la identificación de usuarios en Amazon WorkSpaces se basa en servicios de directorio activo para autenticar a los usuarios, concretamente apoyado en el servicio AWS Directory Services. Este servicio ofrece tres opciones de implementación del directorio para el WorkSpace:

- AWS Managed Microsoft AD: Consiste en ejecutar Microsoft AD como un servicio gestionado en la nube por AWS.
- Simple Active Directory: Simple AD proporciona un subconjunto de las funciones que ofrece AWS Managed Microsoft AD, si bien no admite ciertas características tales como las relaciones de confianza con otros dominios o la autenticación multifactor, por lo que es recomendable utilizar preferiblemente AWS Managed Microsoft AD.
- Active Directory Connector: AD Connector es una puerta de enlace de directorio con la que se pueden redirigir las solicitudes del directorio a Microsoft Active Directory local sin almacenar en caché la información en la nube.

Una cuarta opción para la implementación del directorio de WorkSpace es la utilización de un dominio de confianza. Consiste en el establecimiento de una relación de confianza entre el AWS Managed Microsoft AD y el AD del entorno local. En este caso, se establecería una confianza unidireccional o bidireccional para administrar entre ambos directorios y autenticar con usuarios y grupos en Amazon WorkSpaces.

AWS Managed Microsoft AD y AWS Simple Active Directory funcionan sin la necesidad de disponer de un AD propio en el entorno local, mientras que el Active Directory Connector y Simple Active Directory son tecnologías diseñadas para combinarse con el AD local.

Independientemente del servicio de directorio elegido, se recomienda tener en cuenta los requisitos y recomendaciones expuestos en el apartado Identificación [op.acc.1] de la guía ***CCN-STIC 887A – Guía de Configuración Segura para AWS*** en todo lo referente a la gestión de usuarios.

Requisitos de acceso

De forma predeterminada, los usuarios de AWS IAM no tienen permisos para los recursos y las operaciones de Amazon WorkSpaces. Para permitir a los usuarios de AWS IAM administrar recursos de Amazon WorkSpaces, se debe crear una política de AWS IAM que les conceda explícitamente los permisos y asociar la política a los usuarios, grupos o roles de AWS IAM que necesitan esos permisos.

Las políticas de AWS IAM se deberían asignar de modo que los usuarios solamente puedan utilizar los recursos y ejecutar las acciones de Amazon WorkSpaces mínimas para el ejercicio de sus funciones. En este enlace se puede obtener más información sobre las diferentes políticas gestionadas de Amazon WorkSpaces que se pueden utilizar para una correcta asignación de permisos basada en el principio de privilegios mínimos antes de pasar a la creación de políticas por parte del cliente.

Es recomendable que se definan los grupos de usuarios o los roles sobre la base del tipo de acceso y la autenticación del usuario que se requiere como parte del proceso de planificación de los Amazon WorkSpaces. Los roles de usuario definidos mediante los AWS Directory Services pueden servir para la implementación de la estrategia de segmentación y restricción del acceso. No obstante, dado que los WorkSpaces se ejecutan en VPCs, las listas de control de acceso a la red, las tablas de enrutamiento y los grupos de seguridad de VPC también pueden utilizarse para añadir una capa extra de seguridad al control de acceso. Por ejemplo, se puede asignar un grupo de seguridad a todos los WorkSpaces asociados a un AD Connector para especificar que los usuarios requieren una autenticación MFA o decidir si pueden tener acceso de administrador local a sus WorkSpaces.

Además de las políticas de usuarios, con su instalación, Amazon WorkSpaces crea un rol de AWS IAM (workspaces_DefaultRole) para permitir que el servicio Amazon WorkSpaces cree interfaces de red y enumere los directorios.

Por otro lado, los derechos de acceso y acciones relacionadas con Amazon WorkSpaces también deberán contemplar los escenarios en los que se opte por activar el portal de autoservicio. En Amazon WorkSpaces es posible activar un portal de autoservicio para que los usuarios tengan más control sobre su experiencia y, de este modo, reducir la carga de trabajo del equipo de soporte de TI para WorkSpaces. Cuando se habilitan las capacidades de autoservicio, los usuarios pueden realizar una o más de las siguientes tareas directamente desde sus WorkSpaces:

- Almacenar en caché sus credenciales en el cliente. Esto les permite volver a conectarse a su WorkSpace sin volver a introducir sus credenciales.
- Reiniciar su WorkSpace.
- Aumentar el tamaño de los volúmenes raíz y de usuario en su WorkSpace.
- Cambiar el tipo de cómputo (paquete) para su WorkSpace.

- Cambiar el modo de ejecución de su WorkSpace (AlwaysOn, AutoStop).
- Reconstrucción del WorkSpace.

No obstante, es recomendable la restricción de estas opciones, especialmente, el almacenamiento en caché de las credenciales (o, al menos, el establecimiento de la duración máxima de un ticket de Kerberos).

Para ampliar detalles sobre las opciones del portal de autoservicio se puede consultar este enlace.

Mecanismos de autenticación

Los mecanismos de inicio de sesión por parte de los usuarios han de ser robustos, por lo que se recomienda la aplicación de las medidas contenidas en el apartado Mecanismo de autenticación (usuarios de la organización) [op.acc.6] de la guía ***CCN-STIC 887A – Guía de Configuración Segura para AWS*.**

Entre estas medidas de seguridad, es importante tener en cuenta que la autenticación multifactor en el entorno de Amazon WorkSpaces se puede implementar por medio de un servidor RADIUS. El siguiente diagrama muestra los componentes necesarios para esta solución en un entorno que autentica a los usuarios de Amazon WorkSpaces con el directorio del centro de datos local:

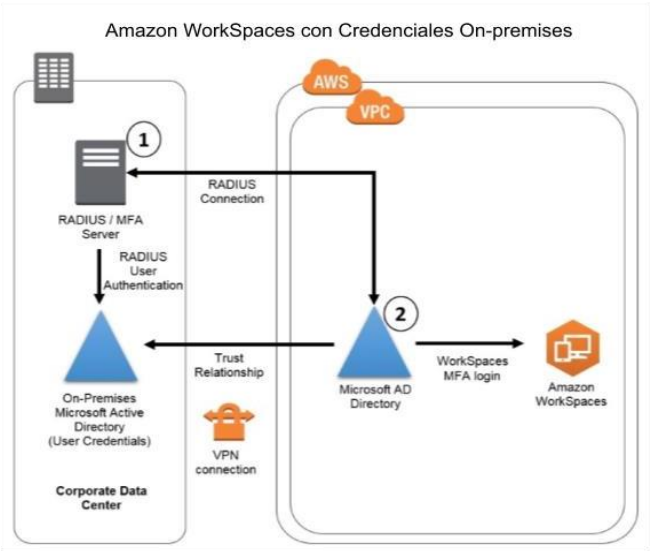

Fig. 3 - Arquitectura de componentes para autenticar usuarios con MFA

El lado izquierdo del diagrama representa el centro de datos de la entidad con el AD local conectado a la infraestructura RADIUS / MFA que proporcionará la autenticación de usuario RADIUS (el servidor RADIUS también podría estar ubicado en AWS). El lado derecho muestra el directorio de Microsoft AD en la nube de AWS conectado al AD local a través de una relación de confianza, y los Amazon WorkSpaces

unidos al directorio de Microsoft AD que exigirán el código MFA cuando autentiquen a los usuarios. Nótese que la autenticación al servicio da acceso al usuario al escritorio sin autenticación adicional.

Acceso remoto

Al tratarse AWS de un servicio de nube gestionado, el acceso a los escritorios se realiza en remoto y nunca en local. Este acceso podría realizarse a través de canales privados desde las redes privadas del usuario o a través de Internet. Este último caso deberá protegerse con filtros de los orígenes que pueden usar el servicio, cuando se desea que el mismo sea restringido y siempre que las circunstancias no lo impidan, como en los casos de uso de trabajo remoto o teletrabajo donde el rango de direcciones origines puede ser muy variable. En AWS esto se implementa con grupos de control de acceso.

Amazon WorkSpaces permite controlar desde qué direcciones IP se puede acceder. Mediante el uso de grupos de control basados en direcciones IP, se puede definir y administrar grupos de direcciones IP de confianza y permitir que los usuarios sólo accedan a sus WorkSpaces cuando están conectados a una red de confianza.

Un grupo de control de acceso a direcciones IP actúa como un firewall virtual que controla las direcciones IP desde las que los usuarios pueden tener acceso a sus escritorios de WorkSpaces. Para especificar los intervalos de direcciones CIDR, se añaden reglas a un grupo de control de acceso con direcciones IP y, a continuación, se asocia el grupo al directorio.

Para conocer el proceso de configuración de esta funcionalidad se puede acceder a este enlace.

Para el acceso de Amazon WorkSpaces se emplea un cliente en el equipo de usuario que esté configurado por defecto para actualizarse de manera automática. Es posible desactivar esta opción manualmente, pero deberá vigilarse que no sea el caso para los usuarios que consuman el servicio. En caso de requerir desactivar el proceso automático será responsabilidad del cliente distribuir e instalar las nuevas versiones del software de cliente. Amazon WorkSpaces también permite el uso de SAML 2.0 como mecanismo de acceso. Se puede consultar cómo integrarlo en el documento- WorkSpaces Integración con SAML 2.0.

2.2 INVENTARIADO DE ACTIVOS

Para disponer de un inventario de activos actualizado que incluya los WorkSpaces, el usuario de AWS deberá apoyarse en las herramientas de terceros o las que proporciona el propio AWS.

AWS Config, es una herramienta que proporciona una vista detallada de los recursos de AWS, es compatible con Amazon WorkSpaces, de modo que se puede utilizar para el inventariado de sus recursos y el seguimiento de sus configuraciones.

Asimismo, AWS Systems Manager permite la visibilidad el tiempo real de la configuración desplegada y de los logs de Amazon WorkSpace, así como automatizar tareas operativas sobre los Amazon WorkSpaces.

Además, se pueden asignar etiquetas (tags)[1] a cada recurso especificando una clave valor por cada etiqueta. El uso de etiquetas es una forma ágil de manejar los recursos de AWS y de organizar la información, incluidos los datos de facturación que aplica para los objetos del servicio Amazon WorkSpaces.

Puede encontrarse más información sobre el uso de estas herramientas para el inventariado de activos en el apartado Inventario de activos [op.exp.1] en la guía ***CCN-STIC 887A – Guía de Configuración Segura para AWS.***

2.3 CONFIGURACIÓN DE SEGURIDAD

Entornos Windows

Para aplicar la configuración para la administración de los Amazon WorkSpaces y de los usuarios que son parte del directorio de Windows WorkSpaces se puede aplicar política de grupo (GPOs). Se recomienda la creación de una unidad organizativa para los objetos de Amazon WorkSpaces equipo y otra para los objetos de Amazon WorkSpaces de usuario.

Para usar las políticas de grupo que son específicas para Amazon WorkSpaces, se tienen que instalar la plantilla administrativa de la política de grupo para el protocolo o protocolos que se usan, tanto PCoIP o WorkSpaces Streaming Protocol (WSP).

Instalación de la plantilla administrativa de la política de grupo para PCoIP

Para utilizar la configuración de la directiva de grupo específica de Amazon WorkSpaces cuando se utiliza el protocolo PCoIP, deberá instalarse la plantilla administrativa de la directiva de grupo para PCoIP.

Instalación de la plantilla administrativa de la política de grupo para WSP

Para utilizar la configuración de la Política de Grupo que es específica de Amazon WorkSpaces cuando se utiliza el Protocolo de Streaming de WorkSpaces (WSP), deberá incluir los archivos de plantilla administrativa de la Política de Grupo wsp.admx y wsp.adml para WSP al Almacén Central del controlador de dominio para su directorio de Amazon WorkSpaces.

La configuración de la política de grupo puede afectar a los usuarios del servicio. Para más información sobre configuración de políticas de grupo se puede consultar este enlace.

[1] https://docs.aws.amazon.com/es_es/tag-editor/latest/userguide/tagging.html

Entornos Linux

Al igual que en los entornos Windows, se puede usar el directorio activo de usuarios y grupos para administrar los Amazon WorkSpaces de Linux y dar acceso a nuevos usuarios al mismo. Las instancias Linux no pueden hacer uso de las políticas de grupo, por lo que se deberá usar una solución para aplicar políticas como AWS OpsWorks for Chef Automate, AWS OpsWorks for Puppet Enterprise o Ansible.

Para más información sobre configuración de políticas de grupo se puede consultar este enlace.

2.4 MANTENIMIENTO Y ACTUALIZACIONES DE SEGURIDAD

Amazon WorkSpaces ofrece varias opciones para el mantenimiento de los equipos. Durante este mantenimiento se instalan actualizaciones importantes de Amazon WorkSpaces y se reinicia si es necesario. Si el sistema operativo tiene disponibles actualizaciones, también se ejecutarán durante el periodo de mantenimiento.

Es responsabilidad del usuario el mantener actualizada la aplicación cliente de Amazon WorkSpaces.

La forma de aplicar el mantenimiento depende del modo de ejecución de un WorkSpace. Los modos de ejecución del WorkSpace son:

- AlwaysOn: Con este modo, el uso del WorkSpace es ilimitado y se paga una cuota mensual fijas. Permite la utilización del escritorio principal a tiempo completo.
- AutoStop: Más adecuado para la utilización del WorkSpace por horas. Con este modo, el WorkSpace se detiene tras un periodo definido y se guarda el estado de las aplicaciones y los datos.

El modo de ejecución de un WorkSpace se puede modificar desde el panel de Amazon WorkSpaces (apartado Acciones/modificar modo de ejecución) o desde la AWS CLI utilizando el comando modify-workspace-properties.

Mantenimiento para WorkSpaces AlwaysOn

En el mantenimiento de los Amazon WorkSpaces en modo de ejecución AlwaysOn, la ventana de mantenimiento se define en la configuración del sistema operativo. Por defecto se realiza desde las 00h00 hasta las 04h00, en la zona horaria del WorkSpace y todos los domingos. Por defecto la zona horaria en un WorkSpace AlwaysOn es la misma que la región de AWS donde se encuentra el WorkSpace. Sin embargo, si se conecta al WorkSpace desde otra región y la redirección de zona horaria está activada, la zona horaria del WorkSpace se actualiza con la zona horaria de la región desde la que se ha conectado. Se puede deshabilitar la redirección horaria desde las políticas de grupo.

Mantenimiento para WorkSpaces AutoStop

Los Amazon WorkSpaces en modo de ejecución AutoStop son iniciados automáticamente una vez al mes para instalar actualizaciones importantes. A partir del tercer lunes del mes y durante un máximo de dos semanas, la ventana de mantenimiento se abre cada día desde las 00h00 hasta las 05h00, en la zona horaria de la región de AWS donde se encuentre el WorkSpace.

Durante este tiempo el estado del WorkSpace aparecerá en mantenimiento. Se puede deshabilitar el mantenimiento del WorkSpace. En caso de deshabilitar esta opción (no recomendado), el WorkSpace no se reiniciará y tampoco entrará en estado de mantenimiento.

Mantenimiento Manual

Amazon WorkSpaces también ofrece la posibilidad de mantenimiento manual. Durante el mantenimiento manual, se recomienda cambiar el estado del WorkSpace por “Mantenimiento” y cuando el trabajo ha terminado cambiarlo a “Disponible”.

2.5 CONTINUIDAD DEL SERVICIO

Amazon WorkSpaces proporciona el redireccionamiento entre regiones. Esta característica funciona con las políticas de redireccionamiento del DNS, redirige los WorkSpaces de los usuarios hacia otros alternativos cuando el principal no está disponible, esto permite tener alta disponibilidad y una alternativa durante los periodos de mantenimiento. Amazon Route 53 identifica el estado de un servicio y conmuta el tráfico DNS hacia otra región ante fallos.

Redireccionamiento entre regiones

Con la característica de redireccionamiento entre regiones de Amazon WorkSpaces, se puede utilizar un nombre de dominio completo (FQDN) como código de registro para los WorkSpaces. El redireccionamiento entre regiones funciona con las políticas de direccionamiento del sistema de nombres de dominio (DNS) para redirigir a los usuarios de Amazon WorkSpaces a una alternativa cuando su nodo principal no esté disponible.

Para usar esta característica, se debe configurar Amazon WorkSpaces en dos o más regiones de AWS. También ha de crearse claves de registro especiales basados en FQDN denominados “*alias de conexión*”. Estos alias de conexión sustituyen las claves de registro específicas de la región para los Amazon WorkSpaces.

Para crear un alias de conexión se deberá especificar el FQDN (desktop.ejemplo.com). Para usar el dominio dentro de la redirección de regiones se debe registrar el dominio y configurar el servicio DNS del dominio.

Cada alias de conexión debe ser asociado con los Amazon WorkSpaces en diferentes regiones, una región principal y una o varias regiones de conmutación por error. Para designar las regiones primarias y de conmutación por error, se debe definir la prioridad de la región al configurar sus políticas de enrutamiento de conmutación por error de DNS.

Es importante tener en cuenta que la información del usuario no es persistente entre Amazon WorkSpaces de diferentes regiones. Para asegurar que los usuarios pueden acceder a sus archivos desde diferentes regiones se deberá usar un servicio de compartir archivos como Amazon WorkDocs. Amazon WorkDocs permite almacenar, administrar, compartir y colaborar en archivos con otras personas.

Para ver un ejemplo de configuración paso a paso puede consultar este enlace.

2.6 MONITORIZACIÓN

Para la monitorización de los Amazon WorkSpaces se pueden usar varios servicios incluidos dentro de AWS.

Amazon CloudWatch Metrics

Amazon WorkSpaces envía datos a Amazon CloudWatch sobre sus WorkSpaces. Amazon CloudWatch ofrece métricas que permiten verificar que los WorkSpaces funcionan como se espera.

Las métricas de Amazon CloudWatch para Amazon WorkSpaces están diseñadas para ofrecer información sobre el estado de funcionamiento y de 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. De forma predeterminada están habilitadas las siguientes métricas:

- Available: La cantidad de WorkSpaces que devolvieron un estado saludable.
- Unhealthy: La cantidad de WorkSpaces que devolvieron un estado poco saludable.
- ConnectionAttempt: El número de intentos de conexión.
- ConnectionSuccess: El número de intentos de conexión exitosos.
- ConnectionFailure: El número de conexiones que han producido un error.
- SessionLaunchTime: Tiempo que tarda en iniciarse una sesión de WorkSpaces.
- InSessionLatency: Tiempo de ida y vuelta entre el cliente y el WorkSpace.
- SesionDisconnect: El número de conexiones que se cerraron, incluidas las iniciadas por el usuario y las que produjeron un error.

- UserConnected: La cantidad de WorkSpaces que tienen un usuario conectado.
- Stopped: La cantidad de WorkSpaces que se detienen.
- Maintenance: La cantidad de WorkSpaces que están en mantenimiento.
- TrustedDeviceValidationAttempt: El número de intentos de validación de firmas de autenticación de dispositivos.
- TrustedDeviceValidationSuccess: El número de validaciones de firmas de autenticación de dispositivos satisfactorias.
- TrustedDeviceValidationFailure: El número de validaciones de firma de autenticación de dispositivos que han presentado error.
- TrustedDeviceCertificateDaysBeforeExpiration: Días que quedan antes de que caduque el certificado raíz asociado al directorio.

Para obtener más información sobre las métricas de Amazon WorkSpaces en AWS CloudWatch, puede consultarse este enlace.

Amazon CloudWatch Events

Amazon WorkSpaces puede enviar eventos a Amazon CloudWatch Events, casi en tiempo real, cuando y donde un usuario inicia sesión en un WorkSpace. Amazon CloudWatch Events permite que se pueda actuar cuando ocurren los eventos a través de reglas que activen acciones programáticas.

Para obtener más información sobre la gestión de eventos de WorkSpaces a través de CloudWatch Events, puede consultarse este enlace.

AWS CloudTrail logs

AWS CloudTrail proporciona un registro de las medidas adoptadas por un usuario, rol, o servicio de AWS en Amazon WorkSpaces. La API de Amazon WorkSpaces está integrada con AWS CloudTrail, un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un servicio de AWS en Amazon WorkSpaces. Mediante la información que recopila AWS CloudTrail, permite conocer la IP desde la que se realizó una solicitud, quien la realizó, cuando la realizó y detalles adicionales.

Se recomienda utilizar la solución de AWS CloudTrail ha de ser aprovechada para el registro tanto de intentos de acceso exitoso y los intentos fallidos, si bien AWS CloudTrail ofrece muchas más capacidades.

AWS CloudTrail puede resolver problemas operativos e incidentes de seguridad en los últimos 90 días en la consola de AWS CloudTrail con la característica Event history. Desde aquí se pueden buscar eventos relacionados con la creación, modificación o eliminación de recursos (como usuarios de AWS IAM o instancias de Amazon WorkSpaces) en una cuenta de AWS por región.

Puede encontrarse más información sobre el uso del servicio de AWS CloudTrail y el cumplimiento de las normativas del ENS en la guía ***CCN-STIC 887A – Guía de Configuración Segura para AWS.***

Para obtener más información sobre la gestión de métricas en AWS, puede consultarse este enlace.

2.7 BLOQUEO DEL PUESTO DE TRABAJO

El cliente de Amazon WorkSpaces no admite la configuración del cierre de sesión y la necesidad de volver a autenticar al usuario tras un tiempo de inactividad. Por ello, esta configuración deberá llevarse a cabo a nivel de sistema operativo desplegado en el WorkSpace.

Sin perjuicio de las configuraciones que el equipo virtualizado en Amazon WorkSpaces herede a través de las políticas del directorio del que, en su caso, sea miembro, la forma de configurar el bloqueo del equipo a nivel local dependerá de si se trata de equipos Windows o Linux.

2.8 PROTECCIÓN DE LAS COMUNICACIONES

De conformidad a la normativa de Perímetro seguro [mp.com.1] del ENS, tal y como ya se ha anticipado, cada WorkSpace está asociado a un Amazon VPC y al AWS Directory Service que se haya usado para crearlo. Todas las construcciones del AWS Directory Service necesitan dos redes 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 determinar los tamaños de subred adecuados antes de generar la construcción de Directory Service. Para ello, antes de la creación de las subredes, se deberían tener en cuenta consideraciones como el número de WorkSpaces que se necesitará, los usuarios que se deberá acoger, el número de dominios de AD que se conectarán o la localización de los usuarios.

Amazon WorkSpaces lanza sus WorkSpaces en una nube privada virtual (VPC). Los WorkSpaces deben tener acceso a Internet para que pueda instalar actualizaciones del sistema operativo. Si no se requiere actualizar el sistema operativo, el uso de aplicaciones externas o acceso a internet dentro del escritorio de Amazon WorkSpaces no es necesario que tenga acceso a internet.

Para los servicios que precisan de acceso a internet, se deberá configurar la VPC con una subred pública y dos subredes privadas. Para proporcionar acceso a Internet a los WorkSpaces en una subred privada, se requiere una puerta de enlace NAT en la subred pública. En caso de facilitar el acceso a Internet a través de proxies o redes en el centro de datos corporativo se deberá habilitar conectividad a esta red.

La razón por la que se exigen siempre (al menos) dos subredes, es porque el servicio requiere que se usen dos zonas de disponibilidad, de forma que, si se cae alguna, no se pierda acceso a todos los WorkSpaces.

A continuación, se plasman ejemplos de arquitecturas que se pueden realizar para el despliegue de los diferentes WorkSpaces.

En el siguiente ejemplo se muestra una arquitectura en la cual se usan dos subredes privadas para alojar los WorkSpaces y una pública con una puerta de enlace NAT.

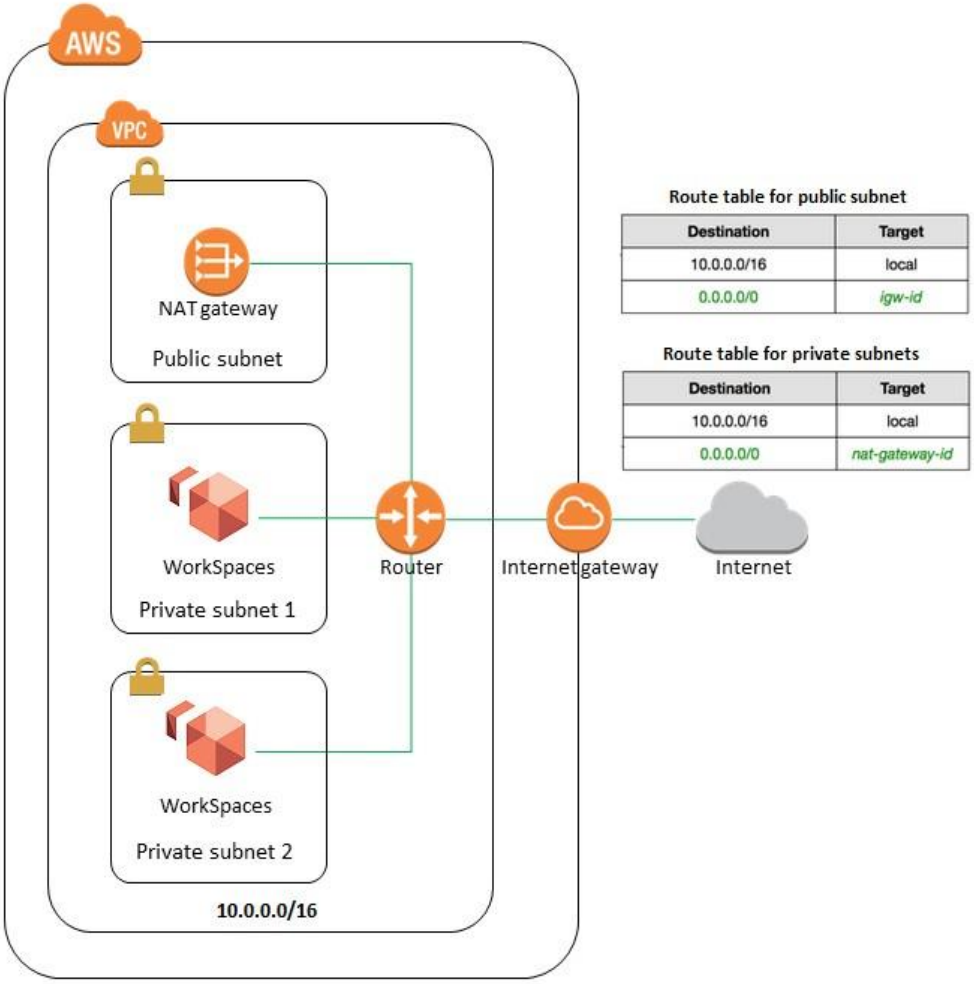

Fig. 4 - Arquitectura de componentes para el despliegue de Amazon WorkSpaceS

En el siguiente ejemplo se muestra una arquitectura con alta disponibilidad, usando el conector AD. El conector de AD actúa solo como un proxy, reenvía las solicitudes de inicio de sesión a los controladores de dominio de AD para la autenticación y proporciona la capacidad para que las aplicaciones consulten datos en el directorio. Esta arquitectura está especialmente recomendada para la segmentación de diferentes perfiles de seguridad en un mismo entorno.

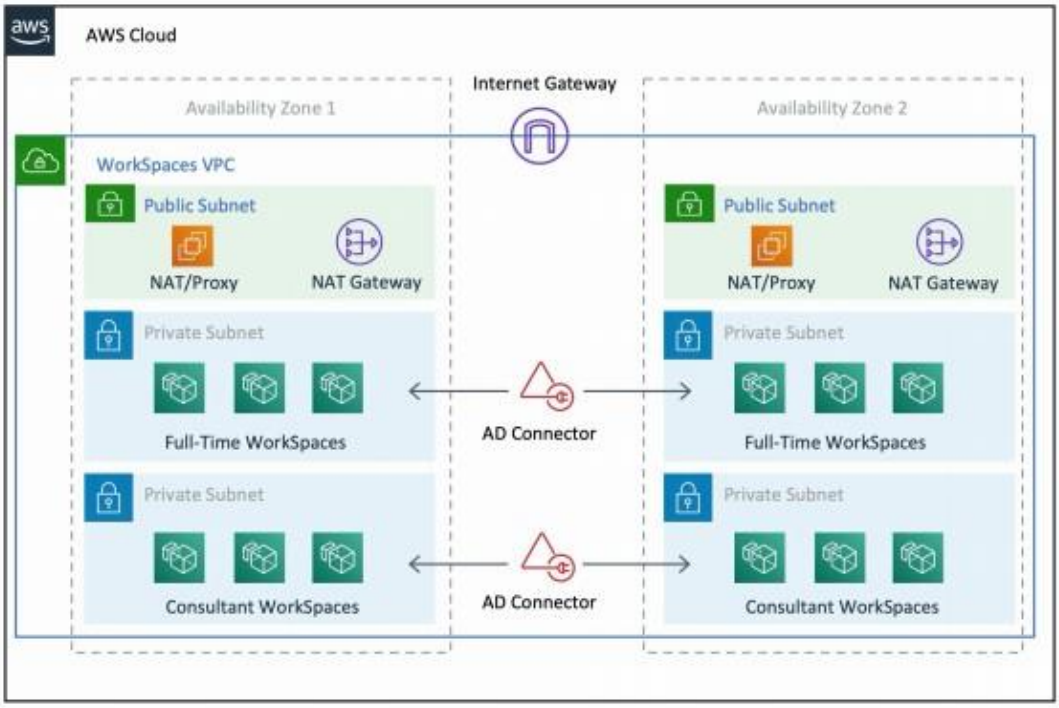

Fig. 5 - Arquitectura de componentes para el despliegue de Amazon WorkSpaces con diferentes perfiles de seguridad

En el siguiente ejemplo se muestra una arquitectura usando AWS Direct Connect para realizar la autenticación con el directorio activo que se encuentre en un entorno fuera de la nube de AWS.

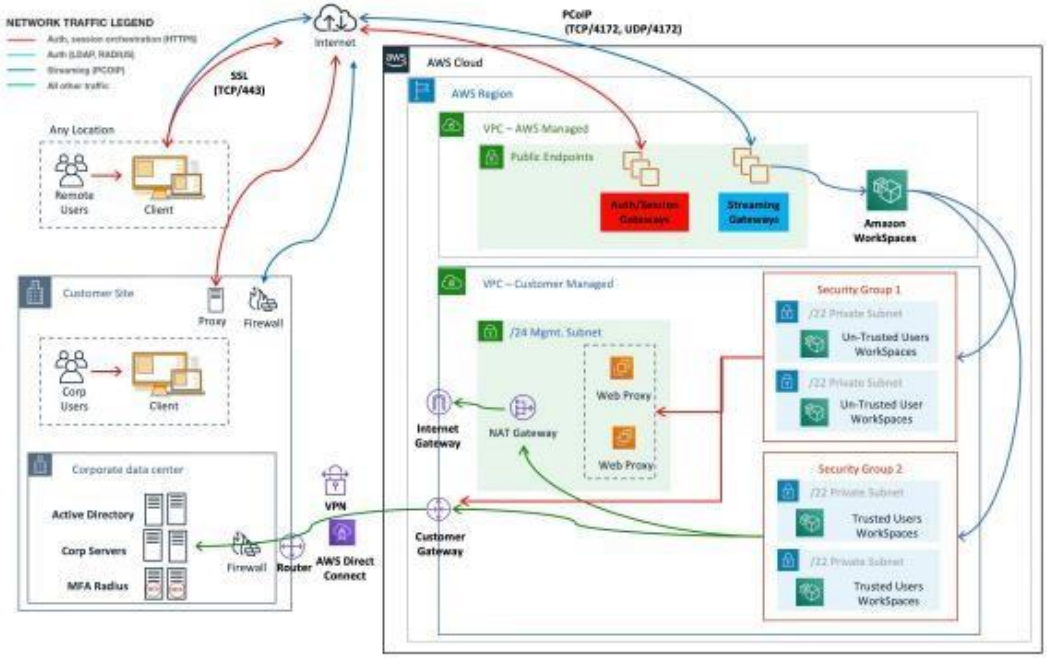

Fig. 6 - Arquitectura de componentes para el despliegue de Amazon WorkSpaces con AWS Direct Connect

Si se necesita más información para configurar la VPC, se puede consultar este enlace.

Con carácter general, las recomendaciones para el diseño de las VPC son:

- Utilizar una VPC, separa específicamente para la implementación de los WorkSpaces. Esto especifica la gobernanza y los procesos de seguridad necesarios específicos para los WorkSpaces.
- Gestionar el tamaño de la subred:
  - Los tamaños de la subred son permanentes y no se pueden cambiar, por lo que se debe dejar un espacio suficiente disponible para el crecimiento futuro. Probablemente en el futuro se desee agregar componentes de administración como servidores. Es recomendable planificar el tamaño para disponer de direcciones IP adicionales en el diseño de la VPC.
  - Especificar un grupo de seguridad predeterminado para el AWS Directory Service elegido. Este grupo de seguridad se aplicará a todos los WorkSpaces asociados a la construcción específica del AWS Directory Service.
  - Se puede hacer que varios servicios de directorio de AWS utilicen la misma subred.

2.9 SEPARACIÓN DE FLUJOS DE INFORMACIÓN DE LA RED

En caso de implementarse el directorio de Amazon WorkSpaces en la nube de AWS de forma independiente utilizando AWS Directory Service, es importante tener en cuenta la separación del tráfico entre el directorio y el propio WorkSpace, por una parte, y la separación del tráfico utilizando diferentes VPCs.

En un primer nivel de separación, se puede implementar la separación del directorio de los WorkSpaces utilizando subredes dedicadas de la misma VPC, tal y como se muestra en el siguiente diagrama:

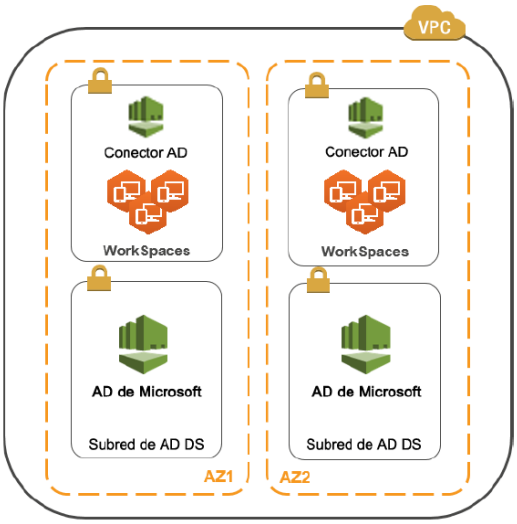

Fig. 7 – Separación de los Amazon WorkSpaces y del AD utilizando subredes de la misma VPC

En un segundo nivel de separación, se pueden utilizar VPCs dedicadas para separar el directorio de los WorkSpaces:

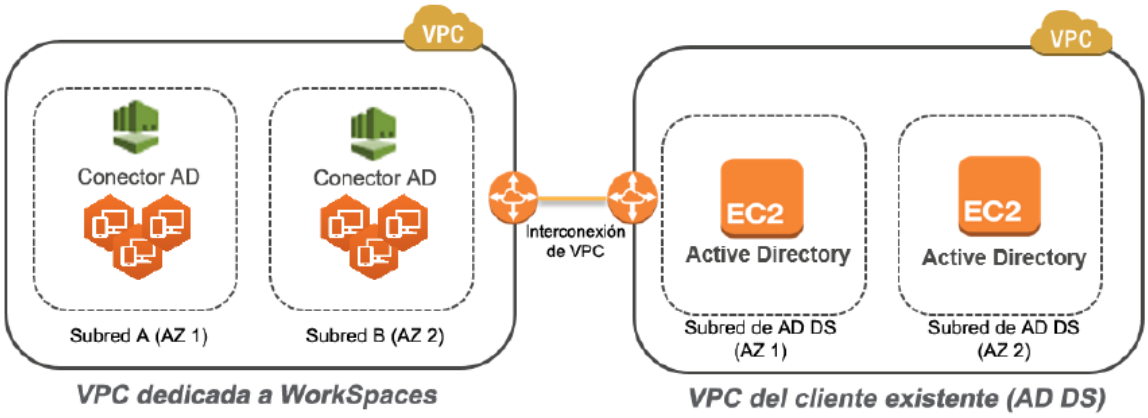

Fig. 8 – Separación de los Amazon WorkSpaces y del AD distintas VPC

En caso de que se disponga de una implementación de Amazon WorkSpaces basada en un AD independiente en la nube utilizando Directory Services, es recomendable escoger esta segunda opción y colocar los WorkSpaces en una VPC dedicada, utilizando una interconexión de la VPC para comunicaciones con el directorio. En cualquier caso, se recomienda restringir las reglas del grupo de seguridad requeridas en las subredes privadas de Amazon WorkSpaces.

Por otro lado, para conectar al WorkSpace, las redes desde las que se conecta a Amazon WorkSpaces deben tener unos puertos concretos abiertos para un rango de IPs para los diversos servicios de AWS.

Puertos para las Aplicaciones Cliente

Puerto	Descripción

443 (TCP)	Este puerto se utiliza para las actualizaciones, el registro y la autenticación de las aplicaciones cliente.
4172 y 4195 (UDP y TCP)	Estos puertos son usados para el streaming del escritorio de WorkSpace y para las comprobaciones de estado. Estos puertos deben estar abiertos para los rangos de IPS de PCoIP y WorkSpaces Streaming Protocol (WSP) y para los servidores de comprobación de estado en la región donde el WorkSpace se encuentra.

Puertos para el Acceso desde Web

Puerto	Descripción
53 (UDP)	Este puerto se utiliza para acceder a los servidores DNS. Debe estar abierto a las direcciones IP de su servidor DNS para que el cliente pueda resolver los nombres de dominio públicos. Este requisito de puerto es opcional si no está utilizando servidores DNS para la resolución de nombres de dominio.
80 (UDP y TCP)	Este puerto se utiliza para las conexiones iniciales a https://clients.amazonworkspaces.com, que luego cambia a HTTPS. Debe estar abierto a todos los rangos de direcciones IP en el subconjunto de Amazon EC2 en la Región en la que se encuentra el WorkSpace.
443 (UDP y TCP)	Este puerto se utiliza para el registro y la autenticación mediante HTTPS. Debe estar abierto a todos los rangos de direcciones IP en el subconjunto de Amazon EC2 en la Región en la que se encuentra el WorkSpace.

Normalmente, el navegador web selecciona aleatoriamente un puerto de origen en el rango alto para utilizarlo en el tráfico de streaming. Amazon WorkSpaces Web Access no tiene control sobre el puerto que selecciona el navegador. Deberá asegurarse de que el tráfico de vuelta a este puerto está permitido.

En este sentido, se recomienda:

- Abrir solo los puertos necesarios para el uso del servicio Amazon WorkSpaces.
- Asociar un grupo de control de acceso IP con un directorio para garantizar que sólo se accede a los Amazon WorkSpaces desde redes de confianza, si aplica para el caso de uso.

Dominios y direcciones IP para añadir a la lista de permitidos

Para que la aplicación cliente de Amazon WorkSpaces pueda acceder al servicio de Amazon WorkSpaces, se deberá añadir los siguientes dominios y direcciones IP a la lista de permitidos en la red desde la que el cliente intenta acceder al servicio.

Se pueden encontrar estos dominios en este enlace.

2.10 CRIPTOGRAFÍA

Cada WorkSpace viene con un volumen de raíz (unidad C:) y un volumen de usuario (unidad D:). La característica de Amazon WorkSpaces cifrados permite cifrar cualquiera de los dos volúmenes o ambos. Concretamente, permite cifrar los datos almacenados en reposo, la E/S del disco al volumen y las instantáneas creadas a partir de volúmenes cifrados.

Amazon WorkSpaces se integra con AWS Key Management Service (AWS KMS). Esto permite cifrar los volúmenes de almacenamiento de Amazon WorkSpaces mediante claves maestras. Al ejecutar CMKs en un WorkSpace, se puede cifrar el volumen raíz y el volumen de usuarios. De este modo se garantiza el cifrado de los datos almacenados.

Al crear WorkSpaces con volúmenes cifrados, Amazon WorkSpaces utiliza Amazon Elastic Block Store (Amazon EBS) para crear y administrar dichos volúmenes. Amazon EBS cifra los volúmenes con una clave mediante el algoritmo AES-256.

Se recomienda emplear Amazon WorkSpaces siempre con cifrado de volúmenes.

Limitaciones a tener en cuenta

- No se puede encriptar un WorkSpace existente. La opción de cifrado debe habilitarse en el momento de crear el WorkSpace.
- No se puede crear una imagen personalizada a partir de un WorkSpace encriptado.
- No es posible desactivar el cifrado de un espacio de trabajo encriptado.
- Los WorkSpaces lanzados con el cifrado del volumen raíz activado pueden tardar hasta una hora en ser aprovisionados.
- Para reiniciar o reconstruir un WorkSpace cifrado, debe asegurar primero que la CMK de AWS KMS esté habilitada; de lo contrario, el WorkSpace quedará inutilizado.

Para saber más sobre el cifrado de Amazon EBS puede consultarse este enlace.

3. GLOSARIO DE TÉRMINOS

A continuación, se describen los términos, acrónimos y abreviaturas relacionados con la tecnología objeto de esta guía con el objeto de facilitar la comprensión de esta.

Término	Definición
AD Connector	Es una puerta de enlace de directorio con la que puede redirigir solicitudes del directorio a Microsoft Active Directory local sin almacenar en caché la información que hay en la nube.
Amazon EBS	Servicio de almacenamiento de bloque de alto rendimiento fácil de usar.
Amazon Route 53	Es un servicio de sistema de nombres de dominio (DNS) escalable y de alta disponibilidad en la nube.
Amazon WorkDocs	Es un servicio completamente administrado y seguro de creación de contenido, almacenamiento y colaboración.
AWS CloudTrail	Servicio de AWS que registra las llamadas a la API de AWS de la cuenta y proporciona archivos de registro.
Amazon CloudWatch	Servicio de AWS que permite monitorizar y administrar diversas métricas- así como configurar acciones de alarma en función de los datos de esas métricas.
ENS	Esquema Nacional de Seguridad.
Directory Service	También conocido como Microsoft Active Directory (AD) administrado en AWS, permite que las cargas de trabajo de directorio y los recursos de AWS utilicen Active Directory (AD) administrado en AWS.
DNS	Sistema de nombres de dominio.
Amazon EC2	Servicio web para lanzar y administrar instancias Linux/UNIX y Windows Server en los centros de datos de Amazon.
FQDN	Un FQDN es un nombre de dominio completo que incluye el nombre de la computadora y el nombre de dominio asociado a ese equipo.
GPOs	Objetos de política de grupo.
HTTPS	Protocolo seguro de transferencia de hipertexto.
AWS IAM	Identity and Access Management (gestión de accesos e identidades)
AWS KMS	Key Management Service. Servicio gestionado de AWS que simplifica la creación y el control de las claves de cifrado que se utilizan para cifrar los datos.
Managed Microsoft AD	Le permite ejecutar Microsoft Active Directory (AD) como un servicio administrado
MFA	Multi-factor Authentication (autenticación multi factor).

PCoIP	PC over IP.
RADIUS	Remote Authentication Dial-In User Service.
Security group	Un grupo de seguridad funciona como un firewall virtual para las instancias EC2 para controlar el tráfico entrante y saliente.
Simple AD	Simple AD es un directorio administrado independiente que utiliza tecnología de un servidor compatible con Active Directory.
TCP	Protocolo de control de transmisión.
UDP	Protocolo de datagramas de usuario.
VPC	Red virtual privada.
WorkSpaces	Escritorio como servicio (DaaS).
WSP	Amazon WorkSpaces Streaming Protocol.

4. GLOSARIO DE SERVICIOS AWS

A continuación, se reúnen los diferentes servicios mencionados a lo largo de esta guía incluyendo enlaces a la documentación concreta de cada uno de ellos.

Servicio	URL de documentación servicio
AD Connector	https://docs.aws.amazon.com/es_es/directoryservice/latest/admin-guide/create_ad_connector.html
Amazon CloudWatch	https://docs.aws.amazon.com/es_es/AmazonCloudWatch/latest/monitoring/cloudwatch_architecture.html
Amazon EC2	https://docs.aws.amazon.com/es_es/AWSEC2/latest/UserGuide/concepts.html
Amazon Elastic Block Store	https://docs.aws.amazon.com/es_es/AWSEC2/latest/UserGuide/AmazonEBS.html
Amazon Route 53	https://docs.aws.amazon.com/es_es/Route53/latest/DeveloperGuide/Welcome.html
Amazon WorkDocs	https://docs.aws.amazon.com/es_es/workdocs/latest/adminguide/what_is.html
Amazon WorkSpaces	https://docs.aws.amazon.com/es_es/workspaces/latest/adminguide/amazon-workspaces.html
AWS CloudTrail	https://docs.aws.amazon.com/es_es/awscloudtrail/latest/userguide/cloudtrail-user-guide.html
AWS Directory Service	https://docs.aws.amazon.com/es_es/directoryservice/latest/admin-guide/what_is.html
AWS Key Management Service	https://docs.aws.amazon.com/es_es/kms/latest/developerguide/overview.html

AWS Managed Microsoft AD	https://docs.aws.amazon.com/es_es/directoryservice/latest/admin-guide/directory_microsoft_ad.html
AWS OpsWorks for Chef Automate	https://docs.aws.amazon.com/es_es/opsworks/latest/userguide/welcome_opscm.html
AWS OpsWorks for Puppet Enterprise	https://docs.aws.amazon.com/es_es/opsworks/latest/userguide/gettingstarted-opspup.html
AWS Organizations	https://aws.amazon.com/es/organizations/
Simple AD	https://docs.aws.amazon.com/es_es/directoryservice/latest/admin-guide/directory_simple_ad.html

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL