Arquitectura

Tanto en Windows como en Amazon Linux, cada WorkSpace está asociado a una nube virtual privada (VPC) y a un directorio en el que se guarda y se administra la información de los WorkSpaces y de los usuarios. Los directorios se administran a través de AWS Directory Service, que ofrece las siguientes opciones: Simple AD, AD Connector o AWS Directory Service para Microsoft Active Directory, también denominado AWS Managed Microsoft AD.

Amazon WorkSpaces utiliza un directorio, ya sea AWS Directory Service o AWS Managed Microsoft AD, para autenticar a los usuarios. Los usuarios obtienen acceso a los WorkSpaces mediante una aplicación cliente desde un dispositivo compatible o, en el caso de los WorkSpaces de Windows, un navegador web, e inician sesión con sus credenciales de directorio. La información de inicio de sesión se envía a una gateway de autenticación, que reenvía el tráfico al directorio para el escritorio de WorkSpaces. Una vez que el usuario está autenticado, se inicia el tráfico de streaming a través de la gateway de transmisión.

Las aplicaciones cliente utilizan HTTPS a través del puerto 443 para todas las sesiones de autenticación y la información relacionada. Las aplicaciones cliente utilizan el puerto 4172 para la transmisión de píxeles al escritorio de WorkSpaces y para las comprobaciones de estado de la red.

Cada escritorio de WorkSpaces tiene dos interfaces de red elástica (ENI) asociada: una para la administración y la transmisión (eth0) y una ENI principal (eth1). La ENI principal tiene una dirección IP proporcionada por la VPC, de las mismas subredes que utiliza el directorio. De este modo se garantiza que el tráfico del WorkSpace alcanza el directorio. El acceso a los recursos de la VPC se controla mediante los grupos de seguridad asignados a la ENI principal.

Fuente: https://docs.aws.amazon.com/es_es/workspaces/latest/adminguide/amazon-workspaces.html