Amazon WorkSpaces enables you to provision virtual, cloud-based Microsoft Windows, Amazon Linux, or Ubuntu Linux desktops for your users, known as WorkSpaces. WorkSpaces eliminates the need to procure and deploy hardware or install complex software. You can quickly add or remove users as your needs change. Users can access their virtual desktops from multiple devices or web browsers.

Features

Choose your operating system (Windows, Amazon Linux, Ubuntu Linux) and select from a range of hardware configurations, software configurations, and AWS Regions. For more information, see Amazon WorkSpaces Bundles and Create a custom WorkSpaces image and bundle.

Choose your protocol: PCoIP or WorkSpaces Streaming Protocol (WSP).

Connect to your WorkSpace and pick up from right where you left off. WorkSpaces provides a persistent desktop experience.

WorkSpaces provides the flexibility of either monthly or hourly billing for WorkSpaces.

For Windows desktops, you can bring your own licenses and applications, or purchase them from the AWS Marketplace for Desktop Apps.

Create a standalone managed directory for your users, or connect your WorkSpaces to your on-premises directory so that your users can use their existing credentials to obtain seamless access to corporate resources.

Use the same tools to manage WorkSpaces that you use to manage on-premises desktops.

Use multi-factor authentication (MFA) for additional security.

Use AWS Key Management Service (AWS KMS) to encrypt data at rest, disk I/O, and volume snapshots.

Control the IP addresses from which users are allowed to access their WorkSpaces.

Architecture

For Windows and Linux WorkSpaces, each WorkSpace is associated with a virtual private cloud (VPC), and a directory to store and manage information for your WorkSpaces and users. For more information, see Configure a VPC for WorkSpaces. Directories are managed through the AWS Directory Service, which offers the following options: Simple AD, AD Connector, or AWS Directory Service for Microsoft Active Directory, also known as AWS Managed Microsoft AD. For more information, see the AWS Directory Service Administration Guide.

WorkSpaces uses your Simple AD, AD Connector, or AWS Managed Microsoft AD directory to authenticate users. Users access their WorkSpaces by using a client application from a supported device or, for Windows WorkSpaces, a web browser, and they log in by using their directory credentials. The login information is sent to an authentication gateway, which forwards the traffic to the directory for the WorkSpace. After the user is authenticated, streaming traffic is initiated through the streaming gateway.

Client applications use HTTPS over port 443 for all authentication and session-related information. Client applications use port 4172 (PCoIP) and port 4195 (WSP) for pixel streaming to the WorkSpace and ports 4172 and 4195 for network health checks.

Each WorkSpace has two elastic network interfaces associated with it: a network interface for management and streaming (eth0) and a primary network interface (eth1). The primary network interface has an IP address provided by your VPC, from the same subnets used by the directory. This ensures that traffic from your WorkSpace can easily reach the directory. Access to resources in the VPC is controlled by the security groups assigned to the primary network interface.