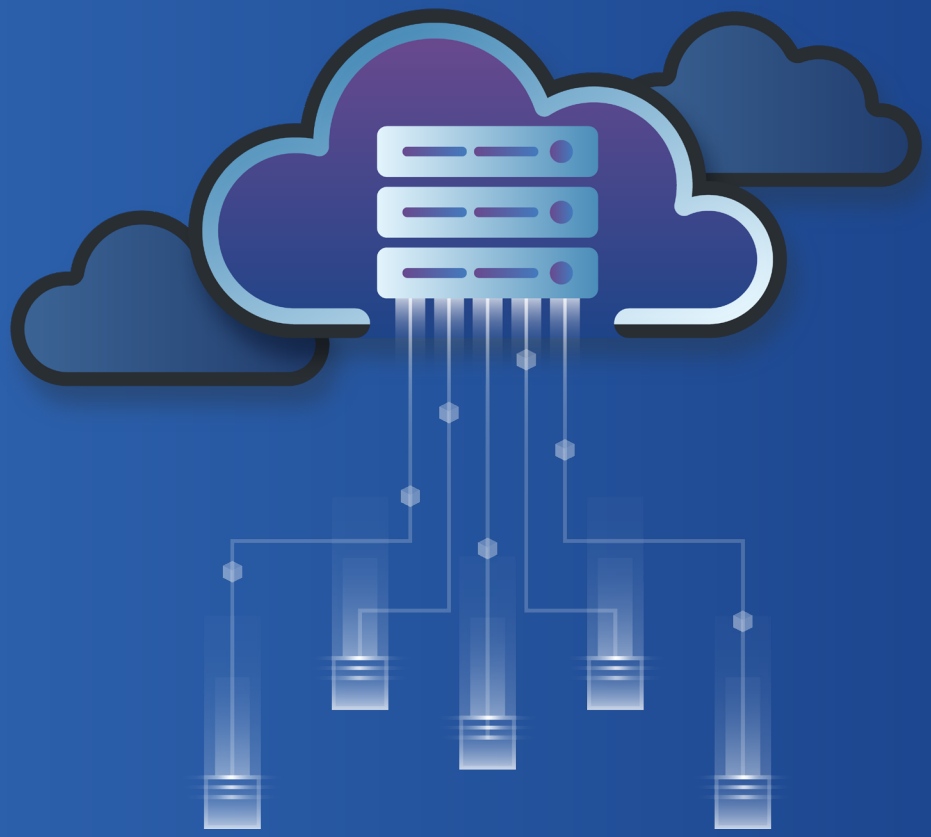
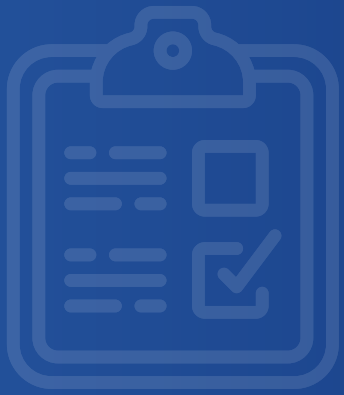
EPLEXITY

The IT Leader's Guide to Remote Working with Amazon WorkSpaces & RDS in AWS



CXOS

Table of Contents



Introduction

Over the last two decades, virtual private networks (VPNs) have enabled organizations to provide employees access to applications and data remotely. Early on, the process was troublesome for end users as connections were slow and some files or applications were too large to access remotely. Latency and file size issues have been addressed to varying degrees as cloud-based applications have come to market.

Still, most large companies require all remote traffic route through the corporate network prior to delivering any data to the end user. Thus, poor performance continues to be an issue for end users. With cloud-based applications readily accessible, employees can now go around the system by accessing applications directly, increasing security risks and creating what is known as shadow IT. This issue is compounded at start-ups and other small organizations that have bring your own device (BYOD) policies.

When employees are allowed to access corporate data and applications remotely, security of wireless networks and concerns about data encryption are paramount. Whether an employee succumbs to a phishing attack or doesn't realize they are on an unsecure wireless network, the companies attack surface grows exponentially when employees are working remotely.

Hiring remote workers can provide a number of benefits to your organization. You have access to a larger qualified pool of candidates for open roles. Not only can this improve your talent level, it can also decrease attrition rates. Providing a strong remote work culture means increased productivity, higher employee engagement, and institutional knowledge stays with the company, reducing the need to hire as often.

Another benefit of remote works is a reduction in overhead costs. Some remote workers may require a co-working space, while others prefer to work from home. The ability to provide options brings down the cost of renting office space and can reduce the cost of travel and commuting expenses with effective teleconferencing tools. Multiple studies have shown that remote workers are more productive and just as engaged as onsite workers. Not surprisingly, remote workers report high satisfaction and morale. Technology has made remote work so efficient and effective that it is not only viable, but a smart business option for many industries.

In this guide we'll discuss two of the best options from Amazon Web Services (AWS) for enabling remote workers, Amazon WorkSpaces and RDS on AWS. Both solutions are highly secure, widely compatible, easily scalable, and provide all of the benefits associated with cloud native applications.

Desktop as a Service (DaaS)

DaaS is a cloud-based solution that enables companies to offer a virtual desktop environment to end users that can be accessed from laptops, pc's, tablets, and some smartphones. DaaS solutions provide access to cloud-based applications, files, and user information, along with the underlying operating system. They are straightforward to purchase and easy to manage for your remote workers.

Virtual Desktop Infrastructure (VDI)

VDI solutions are similar to DaaS solutions with one major difference. VDI solutions are primarily hosted in on-premise data centers and managed by an internal IT team. VDI solutions can reduce capital expenses by utilizing thin client devices that act as terminals only, with no ability to download applications or files to the device itself.

VDI solutions also work with traditional thick client devices such as laptops and PCs. In fact, many start-ups and other small businesses have embraced the bring your own device (BYOD) philosophy. The best way to ensure that these devices don't invite unwanted security breaches is to offer a robust VDI solution. Otherwise, end users will download and run their own software resulting in shadow IT that increases your attack surface.

There is no question that VDI and DaaS solutions improve business agility. However, VDIs have limitations that DaaS solutions don't. IT resources are tight universally. The work associated with adding or removing end users is time consuming and provides little value to the business. Another factor that limits VDIs is the need maintain, update, and patch the system to keep it up to date with the latest software versions and security threats.

Benefits

DaaS solutions improve on traditional VDI deployments in a variety of ways. For example, any device with a browser can access company networks securely, including laptops, PCs, Chromebooks, tablets, and smartphones. And end users don't need to worry about installing and keeping applications up to date.

END USER EXPERIENCE

Remote tools today provide the same digital experience as being in an office. With 5G connectivity growing, the latency experienced on home networks is negligible. End users can connect to office networks from almost anywhere in the world from the device of their choice. Reducing friction for end users improves their productivity and improves your security position.

RESOURCE PRODUCTIVITY

As with all cloud-based solutions, automating low-level tasks frees your IT team to focus on business-critical objectives. For example, there is no need to provision new laptops and load all the appropriate applications each time someone is hired. DaaS solutions quickly set up new devices from a preset virtual desktop. This also means your IT team can take patching, updating, and maintaining these applications and related hardware off of their plate.

DaaS solutions are fully managed by your cloud provider. They are continually updated to the latest version of hardware and systems. And since you no longer need to buy and manage the compute, storage, and network infrastructure, you can reduce costs with the elastic nature of the cloud. Scale up or down as needed in minutes and enable your IT resources to contribute to higher level tasks that drive innovation and revenue.

IMPROVED SECURITY AND COMPLIANCE

The majority of security breaches happen at the edge of your network. DaaS solutions move applications and data to the cloud instead of an end user's device. Even with BYOD devices, you can create security controls regardless of hardware or operating system. Data privacy is one of the top benefits of DaaS solutions. Data can't be downloaded, processed, or stored on an end user's device. Identity and access management (IAM) protocols in the cloud provide even more centralized control over who can access and disseminate data. For companies in regulated industries, many common compliance standards can be met with DaaS solutions. Using cloud-based data centers that are already ISO, PCI, or HIPAA compliant not only helps you meet your compliance requirements, it can also provide you with a competitive advantage.

WorkSpaces and Remote Desktop Services (RDS)

WorkSpaces Overview

Amazon WorkSpaces is a managed, secure DaaS solution. You can use WorkSpaces to provision either Windows or Linux desktops in just a few minutes and quickly scale to provide thousands of desktops to workers across the globe. You can pay either monthly or hourly, just for the WorkSpaces you launch, which helps you save money when compared to traditional desktops and on-premises VDI solutions.

IMPLEMENTING WORKSPACES WILL:

- Help you eliminate many administrative tasks associated with managing your desktop lifecycle including provisioning, deploying, maintaining, and recycling desktops. There is less hardware inventory to manage and no need for complex virtual desktop infrastructure (VDI) deployments that don't scale. A few clicks deploy desktops assigned to each user. You no longer need to operate servers, file shares, network appliances, or third-party solutions. And you can build, patch, and maintain your images with native features.
- Eliminate the need to over-buy desktop and laptop resources by providing on-demand access to cloud desktops that include a range of compute, memory, and storage resources to meet your users' performance needs. Each user receives their own desktop with consistent performance across sessions, no matter how many users are logged on at the same time. You no longer manage complicated multi-session environments.
- Deploy within an Amazon Virtual Private Network (VPC), providing each user with access to persistent, encrypted storage volumes in the AWS Cloud, and integrate with AWS Key Management Service (KMS). No user data is stored on the local device, improving the security of user data and reducing your overall risk surface area.
- Provide access to high performance cloud desktops wherever your teams get work done. You can manage a global deployment of many thousands of WorkSpaces from the AWS console. And you can rapidly provision and de-provision desktops as the needs of your workforce change.
- Provide simple pay-as-you-go pricing with no confusing licensing. Pricing starts at $21 per WorkSpace per month. You can also bring your existing Windows 7 and Windows 10 licenses to maintain license compliance and reduce your cost by $4 per WorkSpace per month.

WorkSpaces and Remote Desktop Services (RDS)

Remote Desktop Service (RDS) Overview

RDS from Microsoft is a platform for building virtualization solutions for customer needs, including delivering individual virtualized applications, providing secure mobile and remote desktop access, and providing end users the ability to run their applications and desktops from the cloud.

RDS offers deployment flexibility, cost efficiency, and extensibility—all delivered through a variety of deployment options. Depending on your environment and preferences, you can set up the RDS solution for session-based virtualization, as a virtual desktop infrastructure (VDI), or as a combination of the two:

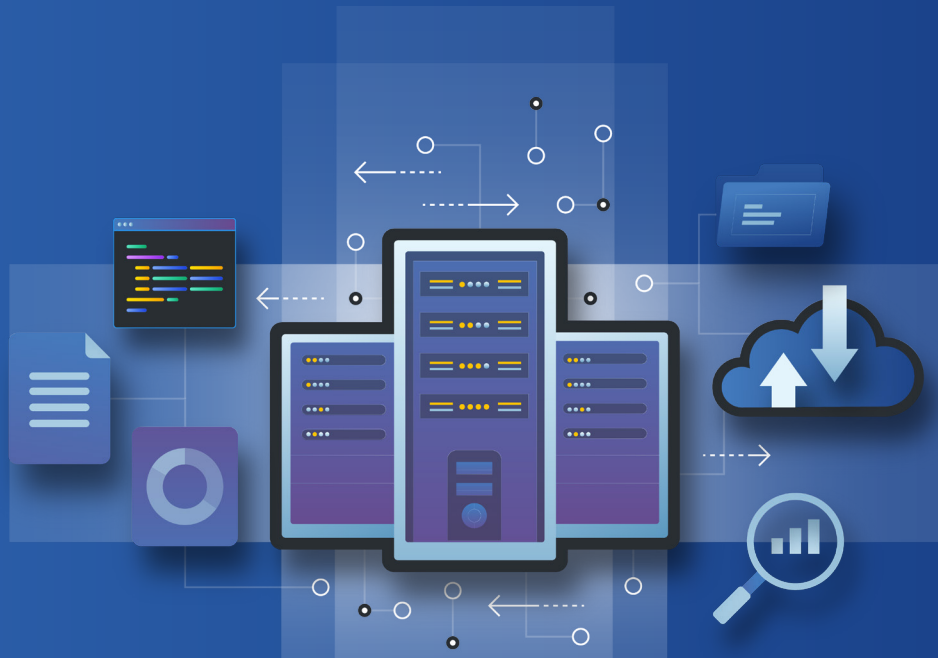
SESSION-BASED VIRTUALIZATION: You can leverage the compute power of Windows Server to provide a cost-effective multi-session environment to drive your users' everyday workloads.

VDI: You can leverage Windows client to provide the high performance, app compatibility, and familiarity that your users have come to expect of their Windows desktop experience.

Within these virtualization environments, you have additional flexibility in what you publish to your users:

DESKTOPS: Give your users a full desktop experience with a variety of applications that you install and manage, which is ideal for users that rely on these computers as their primary workstations or that are coming from thin clients, such as with MultiPoint Services.

REMOTEAPPS: Specify individual applications that are hosted/run on the virtualized machine but appear as if they're running on the user's desktop like local applications. The apps have their own taskbar entry and can be resized and moved across monitors. Ideal for deploying and managing key applications in the secure, remote environment while allowing users to work from and customize their own desktops.



WorkSpaces and Remote Desktop Services (RDS)

Comparison on AWS

WINDOWS BRING-YOUR-OWN-LICENSES (BYOL)

Amazon Workspaces and Microsoft RDS running on EC2 both allow for administrators to purchase licenses through AWS or use the WINDOWS Bring-Your-Own-Licenses (BYOL) program which gives you the option to bring your existing Windows licenses to the cloud, if your Microsoft Licensing Agreement allows it. Customers can run their Amazon Workspaces or Microsoft RDS workloads on dedicated hardware to stay compliant with Microsoft licensing terms. WINDOWS BYOL in AWS enables customers to take advantage of the capabilities of running in the cloud and eliminate costs and maintenance of hardware while still using existing Microsoft licenses.

SECURITY AND COMPLIANCE

Security in AWS is defined by the Shared Responsibility model. AWS is responsible for security of the cloud and the customer is responsible for security IN the cloud. So, for both Amazon Workspaces and Microsoft RDS on EC2, AWS is responsible for the security of the underlying hardware and the customer is responsible for the security of the resources running on that hardware.

Amazon Workspaces offers many different security services to customers including encryption at rest and in transit, MFA, and IP Access Control. The Workspaces client also requires a customer-specific Registration Code be configured during setup. Third party auditors frequently assess Amazon Workspaces security and compliance, and compliance documents are stored and available to download in AWS Artifact. Security patches and updates are automatically applied to Amazon Workspaces during a pre-defined monthly maintenance window.

Microsoft RDS requires external users to go through a Remote Desktop Gateway server in order to connect to a terminal server in a private network by encrypting traffic through HTTPS for secure connections. On the Remote Desktop Gateway server, administrators can create policies that define who is allowed to connect to the server and how they authenticate. Security patches and updates can be manually installed on Remote Desktop servers, or administrators can configure AWS Systems Manager (SSM) to automatically download and install updates.

For both Amazon Workspaces and Microsoft RDS on EC2, AWS Security Groups and Network Access Control List's (NACL's) can be configured to only allow approved IP address or subnets access to AWS resources and add an extra layer of security in the cloud.

WorkSpaces and Remote Desktop Services (RDS)

Comparison on AWS

PRICING

With Amazon Workspaces, you only pay for the resources that you use and can be billed at a monthly or hourly rate. Workspaces with Monthly Pricing are charged a flat monthly fee, while Workspaces with Hourly Pricing have a much lower monthly fee with an additional fee charged per hour the Workspaces are running.

When deciding between monthly or hourly billing, it is important to determine how frequently a Workspace will be used. Workspaces that are only accessed for a few hours a week are great candidates for hourly billing, whereas Workspaces that will used frequently should use the monthly billing option, as a Workspace running 40 hours a week could incur a much higher cost when billed hourly as opposed to monthly.

Additionally, Workspaces are priced based on the bundle and compute resources assigned to the Workspaces. Workspace bundles and compute resources can be configured on a per-user basis so a company can have users running different compute types and are not limited to running the same Workspace bundle for all users in an Organization. The Workspaces bundle and compute resources are not set in stone and can be changed at any time for an individual user or groups of users.

Microsoft RDS on EC2 is priced based on the EC2 cost of the Remote Desktop Gateway server, Remoted Desktop Connection Broker, Remote Desktop Licensing server and Remote Desktop Session hosts, or terminal servers. Amazon EC2 instances are priced based on instance class, size and storage. When deployed in an AWS Auto-Scaling Group, a Microsoft RDS environment can be configured to add or remove Remote Desktop Session Hosts based on the number of users logged into the Remote Desktop Session Hosts for both performance and cost optimization.

A Microsoft RDS deployment allows for multiple users to connect to a single Session Host, however each user and device connecting to a Session Host must have a Client Access License (CAL). It is important to note that while multiple users can connect to a single Session Host, as the number of users logged into the Session Host increases, performance of the Session Host decreases, so it is always recommended to have multiple Session Hosts in a deployment. CAL's can be purchased through the Microsoft Volume Licensing Center and are installed on the Remote Desktop Licensing server.

As we discussed previously, both Amazon Workspaces and Microsoft RDS on EC2 allow administrators to bring their own Windows licenses or purchase the licenses through AWS by selecting an Amazon Workspace or EC2 instance with Windows pre-installed and configured.

WorkSpaces Implementation

Amazon WorkSpaces is a managed desktop computing service in the cloud. Amazon WorkSpaces removes the burden of procuring or deploying hardware or installing complex software and delivers a desktop experience with either a few clicks on the AWS Management Console, using the AWS command line interface (CLI), or by using the APIs. With Amazon WorkSpaces, you can launch a desktop within minutes, and connect to and access your desktop software from on-premises or an external network securely, reliably, and quickly.

Amazon's WorkSpaces service requires three components to deploy successfully:

1 WORKSPACES CLIENT APPLICATION

An Amazon WorkSpaces-supported client device. Find a full list here: Supported Platforms and Devices. You can also use Personal Computer over Internet Protocol (PCoIP) zero clients to connect to WorkSpaces. For a list of available devices, see PCoIP Zero Clients for Amazon WorkSpaces.

2 A DIRECTORY SERVICE TO AUTHENTICATE USERS AND PROVIDE ACCESS TO THEIR WORKSPACE

Amazon WorkSpaces currently works with AWS Directory Service and Active Directory. You can use your on-premises Active Directory server with AWS Directory Service to support your existing enterprise user credentials with WorkSpaces.

3 AMAZON VIRTUAL PRIVATE CLOUD (AMAZON VPC)

In which to run your Amazon WorkSpaces. You'll need a minimum of two subnets for a WorkSpaces deployment because each AWS Directory Service construct requires two subnets in a Multi-AZ deployment.

WorkSpaces Implementation (cont.)

Network Considerations

Each WorkSpace is associated with a specific Amazon VPC and AWS Directory Service construct. All AWS Directory Service constructs (Simple AD, AD Connector, and Microsoft AD) require two subnets to operate, each in different Availability Zones. Subnets are permanently affiliated with a Directory Service construct and can't be modified after an AWS Directory Service is created.

Carefully consider the following before the subnets are created.

- How many WorkSpaces will you need over time?
- What is the expected growth?
- What types of users will you need to accommodate?
- How many Active Directory Domains will you connect?
- Where do your Enterprise User Accounts reside?

We recommend defining user groups, or personas, based on the type of access and the user authentication. Defined user personas can help segment and restrict access using AWS Directory Service, network access control lists, routing tables, and VPC security groups. Each AWS Directory Service construct uses two subnets and applies the same settings to all WorkSpaces that launch from that construct.

AWS Directory Service

Amazon WorkSpaces is underpinned by AWS Directory Service. With AWS Directory Service you can create three types of directories. The first two live in the AWS Cloud:

- AWS Directory Service for Microsoft Active Directory (Enterprise Edition), or Microsoft AD, which is a managed Microsoft Active Directory, powered by Windows Server 2012 R2.
- Simple AD, a standalone, Microsoft Active Directory-compatible, managed directory service powered by Samba 4.
- The third, AD Connector, is a directory gateway that allows you to proxy authentication requests and user or group lookups to your existing on-premises Microsoft Active Directory.

A functional AD DS deployment in the AWS Cloud requires a good understanding of both Active Directory concepts and specific AWS services. Best practices suggest you should deploy AD DS in the AWS Cloud into a dedicated pair of private subnets, across two Availability Zones, and separated from AD Connector or WorkSpaces subnets. This construct provides highly available, low latency access to AD DS services for WorkSpaces, while maintaining separation of roles or functions within the Amazon VPC.

With an Amazon VPC, DHCP services are provided by default for your instances. By default, every VPC provides an internal DNS server that is accessible via the Classless Inter-Domain Routing (CIDR) +2 address space and is assigned to all instances via a default DHCP options set. DHCP options sets are used within an Amazon VPC to define scope options, such as the domain name or the name servers that should be handed to your instances via DHCP. Correct functionality of Windows services within your VPC depends on this DHCP scope option and must be set correctly.

WorkSpaces Implementation (cont.)

Security

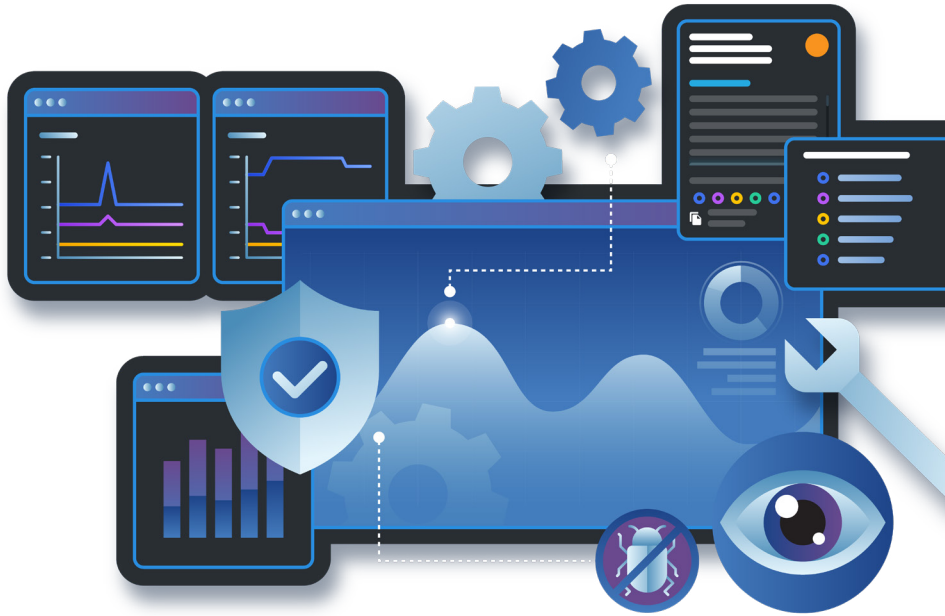
Amazon WorkSpaces uses cryptography to protect confidentiality at different stages of communication (in transit) and also to protect data at rest (encrypted WorkSpaces). The desktop client initiates authentication by sending credentials to the Authentication Gateway. After receiving the credentials from the client, the Authentication Gateway sends an authentication request to AWS Directory Service. The communication from Authentication Gateway to AWS Directory Service takes place over HTTPS, so no user credentials are transmitted in clear text.

A default security group is created per AWS Directory Service and is automatically attached to all WorkSpaces that belong to that specific directory. Additionally, each Amazon WorkSpace is provisioned with a root volume (C: drive) and a user volume (D: drive).

The encrypted WorkSpaces feature enables you to encrypt either volume or both volumes.

Monitoring

Monitoring and logging of WorkSpaces is handled by Amazon CloudWatch. CloudWatch metrics for WorkSpaces provides administrators with additional insight into the overall health and connection status of individual WorkSpaces. Metrics are available per WorkSpace or aggregated for all WorkSpaces in an organization within a given directory and can be viewed in the AWS Management Console (Figure 13), accessed via the CloudWatch APIs.



RDS Implementation

Microsoft RDS is a virtualization solution for customers looking to setup session-based virtualization or Virtual Desktop Infrastructure in on-premises or in the cloud. When running in the AWS cloud you can deliver. Like Amazon Workspaces, RDS removes the burden of procuring or deploying hardware for end-users.

When deploying the Microsoft RDS solution in AWS, four components are required to deploy successfully:

REMOTE DESKTOP GATEWAY SERVER
This server can be deployed in a public or private subnet to allow users on external networks to connect to backend Remote Desktop Session Hosts on a private/corporate network. The Remote Desktop Gateway Server users Remote Desktop Protocol and HTTPS to create a secure, encrypted connection to Session Hosts.

REMOTE DESKTOP SESSION HOSTS
Session Hosts are the backend servers that users will connect to and act as their own desktops in the cloud. Session Hosts are deployed in a Private Subnet behind the Remote Desktop Gateway server, and when deployed in AWS, can be deployed in an Auto-Scaling Group to scale up or down to meet the demand of users logging in.

REMOTE DESKTOP CONNECTION BROKER
Remote Desktop Connection Brokers act as load balancer to balance the load across Session Hosts in a Collection. It is recommended to have multiple Connection Brokers for High Availability.

AMAZON VIRTUAL PRIVATE CLOUD (AMAZON VPC)
in which to run your Microsoft RDS Gateway, Connection Brokers and Session Hosts. You'll need a minimum of two subnets for a Microsoft RDS in AWS deployment, one Public Subnet and one Private Subnet, although it is recommended to have multiple private and public subnets for High-Availability.

RDS Implementation (cont.)

Network Considerations

Microsoft RDS requires connection to on-premises or cloud Domain Controllers in order to allow users to authenticate with their domain credentials. If a Domain Controller does not exist in the same VPC as the RDS environment, a connection will need to be established. For Domain Controllers in AWS, but in a separate VPC, a VPC Peering Connection can be established. If the Domain Controller lives on-premises, a Site-to-Site VPN connection from you on-premises firewall to AWS is recommended.

RDS Collections

It is recommended, but not required, to create multiple RDS Collections for the different business units or groups of users that require specific applications to be installed on their RDS Session hosts or require different compute types. By using multiple Collections, you can install applications for specific business units or groups without having to deploy to all users. Additionally, if you have a group of users that require higher or lower compute resources, you can assign those resources to a specific Collection to allow for more flexibility.

Security

Microsoft RDS uses Remote Desktop Protocol and HTTPS to allow users to login via the Remote Desktop Gateway Server with a secure, encrypted connection. The Remote Desktop Gateway must be configured to allow incoming TCP connections on port 443 as well as UDP connections on port 3391.

AWS Security Groups and Network Access Control Lists add an extra layer of security by giving the customer the ability to allow or restrict access to specific IP address or address ranges.

Monitoring

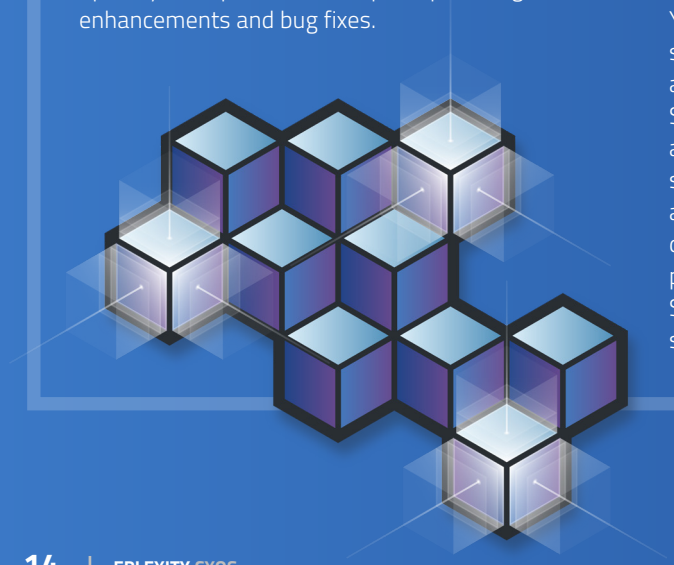
Amazon CloudWatch enables some default monitoring metrics and more detailed metrics can be enabled, although these metrics are performance metrics only and do not monitor the number of users logged in. It is recommended to create a CloudWatch Custom Metric, enable RDS logging or use third-party monitoring for more granular monitoring of the RDS environment.

Why Eplexity

Getting started with WorkSpaces is affordable, fast, and simple with CXOS

CXOS APPLICATION PATTERNS

Application patterns are production ready, workload specific patterns that are engineered to AWS Well Architected Framework standards. Each pattern is proven through hundreds of successful AWS projects utilizing Infrastructure-as-code, Site-Reliability, and Security industry best practices. All CXOS Application patterns are delivered by Eplexity DevOps and AWS experts providing feature enhancements and bug fixes.



CXOS MISSION CONTROL

Once an application pattern is deployed through CXOS, Mission Control provides near real-time metric data and supports operations for each deployed pattern. You'll be able see site-reliability telemetry, security information, and simplified AWS budgets to project and optimize costs for each deployed application pattern.

You'll also receive 24/7/365 cloud managed services support from AWS-certified cloud technicians at the U.S. based Cloud Command Center (C3). Site reliability engineering ensures your deployed application patterns recover quickly from any service disruption. The team monitors utilization and automatically scales your systems up or down depending on need. They take care of security patching and OS upgrades, and you can count on Site Reliability Engineers to monitor and respond to security incidents.

CXOS DEVOPS SERVICE BLOCKS

As you identify new initiatives and take on new projects, you can access AWS DevOps resources to help you get them completed faster. EPLEXITY service blocks include a dedicated Service Delivery Manager to determine daily-to-weekly DevOps work requirements. Flexible contracts allow you to scale to fit your need.

And SLAs give you the peace of mind that work will be completed on time.

EPLEXITY WorkSpaces Case Study

Complete Recovery Corporation (CRC) is a leader in contact call center services including reverse supply chain management and customer experience outsourcing. They help companies manage their customer interactions by providing customer contact service management across multiple channels including telephone, email, letter, text, chat, and social platforms.

To enable their contact call center services, CRC utilized re-furbished computers with support from a local MSP to keep the devices operational. EPLEXITY started working with CRC in 2018 when they decided it was time to adopt a new solution for their core business that would be more flexible, scalable, and reliable, while still delivering value.

The first step was to migrate the application to AWS. EPLEXITY was able to do this quickly and affordably, while still meeting AWS Well Architected Framework best practices. The migration to AWS Workspaces leveraged EPLEXITY's CXOS Managed AWS Service Platform. By starting with the CXOS WorkSpace Application Pattern CRC was able to get their Workspace environment up and running quickly while ensuring Well Architected best practices were being met. Once deployed CXOS's Mission Control provided CRC 24/7/365 support.

The ease of migration and efficiency experienced with AWS encouraged CRC to consider a cloud-based desktop-as-a-service solution with AWS. Anticipating significant growth, CRC wanted a better enterprise business continuity and disaster recovery solution, and reiterated their principles of flexibility, scalability, and reliability as it related to their contact call center workstations.

EPLEXITY advised CRC to pilot AWS WorkSpaces in the Fall of 2019 to determine if it would meet their objectives. CRC customers adhere to strict guidelines related to privacy, information security, and business continuity. The pilot supported CRC's need for rapid scalability and offshore agent support.

The pilot program progressed well. When the COVID-19 outbreak happened, EPLEXITY was able to help CRC deploy WorkSpaces to their entire global agent footprint in Oregon and Colombia without incident. CRC was able to comply immediately with both the Governors stay-at-home directive as well as contractual obligations on business continuity, security, and confidentiality required by their customers. These remote workspaces were able to interface with all CRC applications migrated to AWS as well as a few of the on-premise legacy applications not yet migrated to AWS.

! CRC has seamlessly streamlined and modernized their IT infrastructure. And their contact call centers can confidently operate 24/7/365 whether they are physically in the office or not.

EPLEXITY RDS Case Study

Positronic is a leading manufacturing company that manufactures and supplies electronic connectors for global industries. Although Positronic is headquartered in Springfield, Missouri, the company also has international plants in China, France, India, and Singapore.

To meet the needs of their international workforce without having to provision and deploy physical desktops to employees around the globe, Positronic was running a VMware Horizon Virtual Desktop Infrastructure (VDI) environment. But they were looking for a more reliable, scalable, and elastic solution. EPLEXITY had already been engaged by Positronic to migrate a separate IT infrastructure running in a hosted VMWare environment to AWS.

Based on Positronic's specific needs regarding a cloud-based VDI solution, EPLEXITY recommended a Microsoft RDS infrastructure running on Amazon EC2. The first step in setting up the RDS environment on EC2 was to deploy Remote Desktop Gateway Servers, Connection Brokers, and Session Hosts in AWS to be configured and tested while still running the VMware Horizon solution for their users in parallel. After deploying multiple Remote Desktop Gateways and Connection Brokers for High-Availability, Positronic and EPLEXITY created a separate RDS Collection and installed department-specific applications for each business unit on an Amazon Machine Image (AMI).

! EPLEXITY created an Auto-Scaling Group and Launch Configuration in AWS using the customized AMI for each business unit so that the RD Session Hosts could scale in or out based on the demand of users.

Additionally, EPLEXITY created a Scheduled Action for the Auto-Scaling Groups to proactively scale out just prior to each international location's opening business hours in order to have extra Session Hosts available as users at each plant began working for the day.

For employees at each plant to login to the new Microsoft RDS on EC2 solutions, EPLEXITY and Positronic deployed Thin Clients to all on-site employees with the Remote Desktop Connection pre-configured to point to the Remote Desktop Gateway in AWS.

By using the Microsoft RDS on EC2 solution implemented by EPLEXITY, Positronic can apply OS and application updates, increase or decrease compute resources, and add or remove Session Hosts at any time for their users with no noticeable disruption. Positronic now runs all of their virtual desktops through the Microsoft RDS on EC2 solution, providing high-availability, scalability and reliability for their entire workforce worldwide.

Conclusion

There has been a strategic shift in end-user computing as organizations strive to be more agile, better protect their data, and help their workers be more productive. Many of the benefits already realized with cloud computing also apply to end user computing.

By moving their desktops to the AWS Cloud with Amazon WorkSpaces, organizations can quickly scale as they add workers, improve their security posture by keeping data off devices, and offer their workers a portable desktop with anywhere access from the device of their choice.

Amazon WorkSpaces is designed to be integrated into existing IT systems and processes, providing a cost-effective cloud desktop deployment that scales with your business on the AWS global infrastructure.

Let us help you determine which DaaS solution is right for you.

GET STARTED TODAY

info@eplexity.com
888.501.5979

EPLEXITY

CXOS