AUGUST 2020

Deploying Horizon on VMware Cloud on AWS

VMware End User Computing Group

VMware Cloud on AWS Workload Group

Table of Contents

OVERVIEW OF HORIZON ON VMWARE CLOUD ON AWS

You can deploy Horizon on VMware Cloud on AWS to scale Horizon desktops and applications on an elastic cloud platform.

VMware Cloud on AWS allows you to create SDDCs on AWS. These SDDCs include VMware vCenter Server® for Virtual Machine (VM) management, VMware vSAN™ for storage, and VMware NSX® for networking. You can connect an on-premises SDDC to your cloud SDDC and manage both from a single VMware vSphere® Web Client interface. You can leverage HCX to migrate workload between on-premises and your SDDC. Using your connected AWS account, you can access AWS services such as EC2 and S3 from VMs in your SDDC. For more information, see the *VMware Cloud on AWS documentation.*

Introduction

VMware Horizon® for VMware Cloud™ on AWS delivers a seamlessly integrated hybrid cloud for virtual desktops and applications. It combines the enterprise capabilities of the VMware Software-Defined Data Center (SDDC), delivered as a service on Amazon Web Services (AWS), with the market-leading capabilities of VMware Horizon for a simple, secure, and scalable solution. You can address use cases such as on-demand capacity, disaster recovery, and cloud co-location without buying additional data center resources.

For customers who are already familiar with Horizon or have Horizon environment on-premises, deploying Horizon on VMware Cloud on AWS lets you leverage a unified architecture and familiar tools. This means that you use the same expertise you know from VMware vSphere® and Horizon for operational consistency and leverage the same rich feature set and flexibility you expect. By outsourcing the management of the SDDC to VMware, you can simplify operation of Horizon deployments. For more information about VMware Horizon for VMware Cloud on AWS, visit the *Horizon on VMware Cloud on AWS product page.*

The purpose of this guide is to provide VDI administrators and architects with a set of steps and best practices on how to deploy Horizon on VMware Cloud on AWS. This guide is designed to be used in conjunction with *Horizon documentation*, *VMware Workspace ONE and VMware Horizon Enterprise Edition On-premises Reference Architecture* guide, and *VMware Cloud on AWS documentation*.

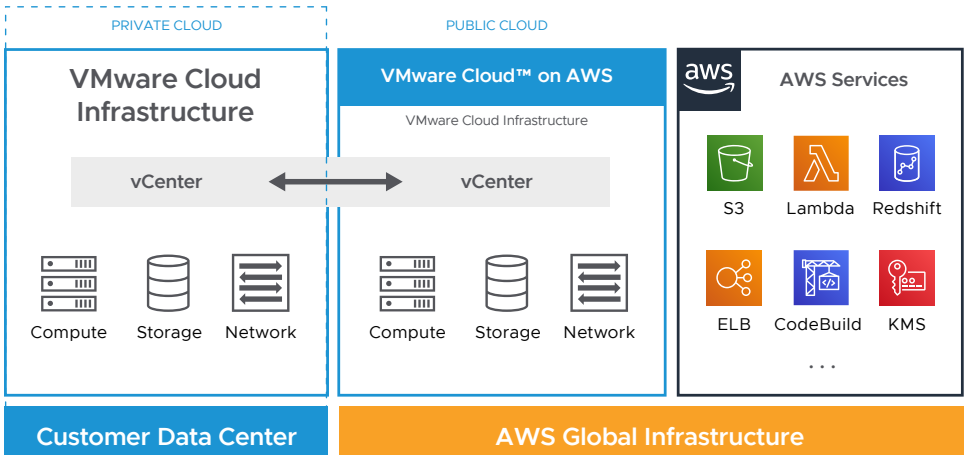


Figure 1. Technical overview

Note: This document references to capabilities of SDDC v. 1.10v3.

Once you have deployed an SDDC on VMware Cloud on AWS, you can deploy Horizon in that cloud environment just like you would in an on-premises vSphere environment. This enables Horizon customers to outsource the management of the SDDC infrastructure to VMware. There is no requirement to purchase new hardware, and you can use the pay-as-you-go option for hourly billing on VMware Cloud on AWS.

Cloud Pod Architecture (CPA) is a Horizon feature that allows you to scale your Horizon deployment across multiple pods and sites for federated management and it's fully supported with VMware Cloud on AWS. You can deploy Horizon in a hybrid cloud environment when you use CPA to interconnect on-premises data centers and VMware Cloud on AWS data centers. You can also stretch CPA across two or more VMware Cloud on AWS data centers. Of course, use of CPA is optional. You can choose to deploy Horizon exclusively in a single VMware Cloud on AWS data center without linking it to any other data center.

Important: A single pod and the Connection Servers in it must be located within a single data center and cannot span locations. Multiple locations must have their own separate pods. These pods can be managed individually or interconnected using CPA.

Since the Horizon architecture is the same on-premises and in VMware Cloud on AWS, the deployment and management experience remain the same across on-premises sites and in the cloud. When using multiple data centers, you must use a storage replication mechanism, such as DFS-R in a hub-spoke topology, for replicating user data (user profiles, shared folders, etc.).

For details on feature parity between Horizon on-premises and Horizon on VMware Cloud on AWS, as well as interoperability of Horizon and VMware Cloud on AWS versions, see the VMware Knowledge Base article *Horizon on VMware Cloud on AWS Support (58539)*.

Horizon deployment scenarios on VMware Cloud on AWS

You can deploy Horizon on VMware Cloud on AWS for the following scenarios:

DATA CENTER EXPANSION / EVACUATION
Use this scenario if you have an existing on-premises Horizon infrastructure and need to expand capacity but don't want to procure additional hardware. Extend the Horizon deployment to VMware Cloud on AWS by using CPA to connect on-premises pods with a pod in VMware Cloud. With this strategy, you can use cloud capacity and still manage on-premises and private cloud deployments in a single federated space. You can also utilize the cloud platform to provide temporary capacity for contractors and seasonal workers. The on-premises deployment is optional. Based on your needs, you can decide to consolidate and move the on-premises deployment completely to VMware Cloud on AWS.
APPLICATION LOCALITY
Use this scenario when you want to move published applications that are latency-sensitive to VMware Cloud on AWS and need virtual desktops and Remote Desktop Session Hosts (RDSH) to be co-located with your published applications. You can also have other published applications that are still on-premises. When you extend your Horizon deployment to VMware Cloud on AWS, you can allow end users to connect to the nearest virtual desktop or RDS host to launch the application regardless of whether the application is on-premises or on VMware Cloud on AWS.
BUSINESS CONTINUITY (BC) AND DISASTER RECOVERY (DR)
The cost of building an on-premises BCDR infrastructure for VDI envirioment can be high. When you use VMware Cloud on AWS, you pay for the use of BCDR infrastructure during those times when the primary infrastructure is down or when you require a small pilot during normal operations for a quick Recovery Time Objective (RTO) during a disaster event. Having a unified Horizon architecture across the primary site on-premises and the BCDR site on VMware Cloud on AWS makes the failover process simple. You can also deploy CPA across multiple VMware Cloud on AWS data centers for BCDR.

Deployment architecture for Horizon on VMware Cloud on AWS

Horizon Pod and building block on-premises

A typical Horizon architecture design on-premises uses a pod strategy. A pod is a unit of organization determined by Horizon scalability limits. Each pod has a separate management UI and therefore the typical design is to minimize the number of pods.

Customers usually include multiple building blocks in a Horizon pod on-premises. A building block is a logical construct and should not be sized for more than the maximum number of desktops tested. See the VMware Knowledge Base article *VMware Horizon sizing limits and recommendations (2150348).*

A building block consists of:

- Physical servers
- One vCenter Server and vSphere infrastructure
- Horizon server components
- Shared storage
- Virtual desktops and/or RDS hosts for end users

Architecting Horizon Cloud pod architecture for VMware Cloud on AWS

CPA is a standard Horizon feature that allows you to connect your Horizon deployment across multiple pods and sites for federated management. It can be used to scale up your deployment, to build hybrid cloud, and to provide redundancy for BCDR. CPA introduces the concept of a global entitlement (GE) that spans the federation of multiple Horizon pods and sites. Any users or user groups belonging to the global entitlement are entitled to access virtual desktops and RDS published apps on multiple Horizon pods that are part of the CPA.

Important: CPA is not a stretched deployment; each Horizon pod is distinct and all Connection Servers belonging to each of the individual pods are required to be located in a single location and run on the same broadcast domain from a network perspective.

Here is a logical overview of a basic two site/ two pod CPA implementation. For VMware Cloud on AWS, Site 1 and Site 2 may be different AWS AZs or Regions, or Site 1 may be on-prem and Site 2 may be on VMware Cloud on AWS.

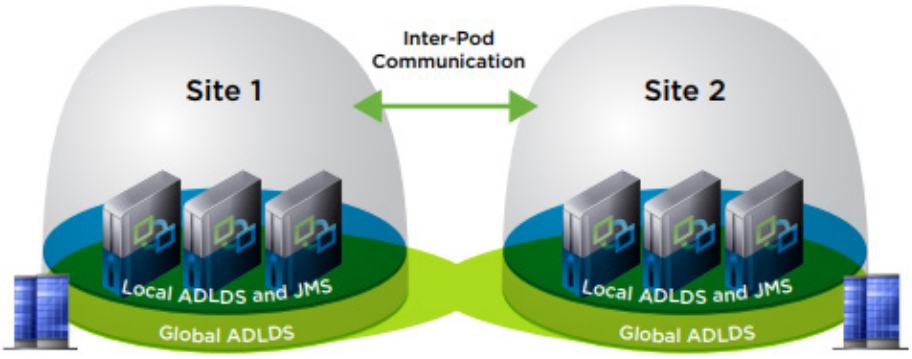


Figure 2. Cloud Pod Architecture technical overview

For the full documentation on how to set up and configure CPA, refer to Administering View CPA in the *Horizon documentation* and *VMware Workspace ONE and VMware Horizon Enterprise Edition On-premises Reference Architecture.*

Understanding key components of Horizon deployment on VMware Cloud on AWS

Horizon deployment on VMware Cloud on AWS leverages the same components as for on-premises deployment and integrates with the management components of your SDDC.

KEY SDDC COMPONENTS	
MANAGEMENT COMPONENTS	• VMware vSphere infrastructure managed by a vCenter Server • NSX-T infrastructure, deployed and managed by VMware
NSX-T COMPONENTS	VMware NSX Data Center is the network virtualization platform for the Software-Defined Data Center (SDDC), delivering networking and security entirely in software, abstracted from the underlying physical infrastructure. The SDDC network topology is shown in Figure 1. • Tier-0 router handles internet, route or policy based IPSEC VPN, AWS Direct Connect and also serves as an edge firewall for the Tier-1 Compute Gateway (CGW). • Tier-1 Compute Gateway (CGW) is an NSX Edge firewall that provides north-south network connectivity and network services including Distributed Firewall (DFW) for virtual machines running in the SDDC. • Tier-1 Management Gateway (MGW) is an NSX Edge firewall that provides north-south network connectivity for the vCenter Server and other management appliances running in the SDDC.

Note: Multiple VLANs can be used to extend a desktop pool on VMware Cloud on AWS.

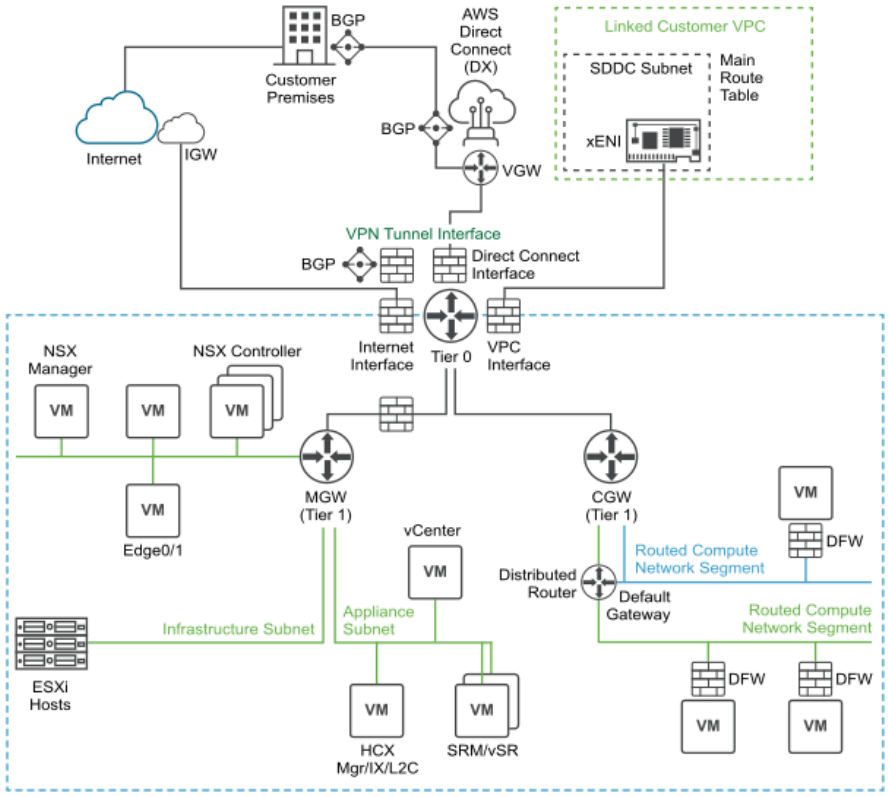


Figure 3. Networking topology on VMware Cloud on AWS for Horizon

KEY HORIZON COMPONENTS	
COMPUTE COMPONENT	The compute component of Horizon includes the following: • Unified Access Gateway appliances • Horizon Connection Servers • Virtual machines • App Volumes
NETWORK COMPONENTS	The following user managed network components are required: • Load balancer

Deploying Horizon pod on VMware Cloud on AWS

Resource pools

A resource pool is a logical abstraction for flexible management of resources. Resource pools can be grouped into hierarchies and used to hierarchically partition available compute (CPU and memory) resources.

Within a Horizon pod on VMware Cloud on AWS, you can use vSphere resource pools to separate management components from virtual desktops or published applications workloads to make sure resources are allocated correctly.

After an SDDC instance on VMware Cloud on AWS is created, two resource pools exist:

- A Management Resource Pool with reservations that contains vCenter Server and NSX deployment, which is managed by VMware
- A Compute Resource Pool within which everything is managed by the customer

We recommend creating two sub–resource pools within the Compute Resource Pool for your Horizon deployments:

- A Horizon Management Resource Pool for your Horizon management components, such as connection servers
- A Horizon User Resource Pool for your desktop pools and published apps

See Figure 4 for schematics of the recommended architecture. Because the management components of Horizon are shared among all virtual machines, you can avoid having any single virtual machine affect overall performance by deploying the management components in a separate resource pool with reservations. Alternatively, you can use different clusters to separate these components.

Note: Consider not mixing VDI and other workloads in the same cluster.

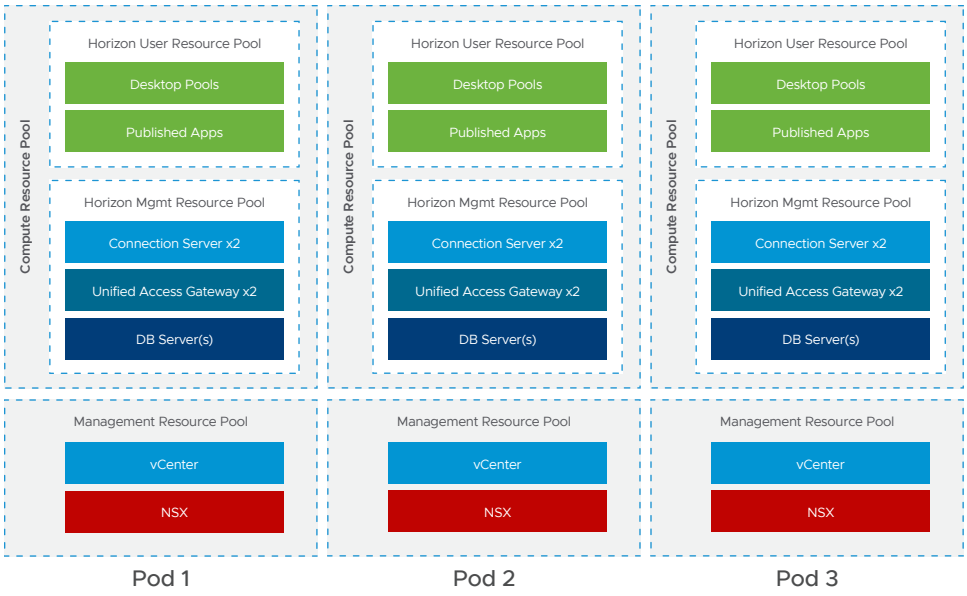


Figure 4. Horizon pod architecture on VMware Cloud on AWS

Horizon Pod architecture considerations on VMware Cloud on AWS

You can set memory and CPU reservations both on the Resource pool and on the VM level. The table below provides a summary of VMware recommended settings.

	RESOURCE POOL LEVEL		VM LEVEL		
	RESERVATION		RESERVATION		SHARES
	Memory	CPU	Memory	CPU	CPU
Management	Full	Full (vCPU *freq)	Full	Full (vCPU *freq)	No
VDI	Full	No	Full	No	Default
RDSH	Full	No	Full	No	By Ratio

Table 1. Reservation and shares overview

Memory reservations

Because sharing of physical memory between virtual machines is not enabled, and because ESXi host swapping or ballooning might have undesirable performance impact, be sure to reserve all memory for all Horizon virtual machines, including management components, virtual desktops, and RDS hosts. You should set memory reservations both on the Resource pool and on the individual VM level.

CPU reservations

CPU reservations are shared when not used, and a reservation specifies the guaranteed minimum allocation for a virtual machine. Any amount of CPU reservations not actively used by the management components will still be available for virtual desktops and RDS hosts when they are not deployed to a separate cluster.

For the management components, the reservations should equal the number of vCPUs, assigned to all management VMs, times the CPU frequency (currently 2300 with VMware Cloud on AWS with i3.metal host type).

VM–level reservations

As well as setting a reservation on the resource pool, be sure to set a reservation at the virtual machine level. This ensures that any VMs that might later get added to the resource pool will not consume resources that are reserved and required for HA failover. These VM-level reservations do not remove the requirement for reservations on the resource pool. Because VM-level reservations are taken into account only when a VM is powered on, the reservation could be taken by other VMs when one VM is powered off temporarily.

Leveraging CPU shares for different workloads

Because RDS hosts can facilitate more users per vCPU than virtual desktops can, a higher share should be given to them. When desktop VMs and RDS host VMs are run on the same cluster, the share allocation should be adjusted to ensure relative prioritization.

As an example, if an RDS host with 8 vCPUs facilitates 28 users and a virtual desktop with 2 vCPUs facilitates a single user, the RDS host is facilitating 7 times the number of users per vCPU. In that scenario, the desktop VMs should have a default share of 1000, and the RDS host VMs should have a vCPU share of 7000 when not deployed to a separate cluster. This number should also be adjusted to the required amount of resources, which could be different for a VDI virtual desktop session versus a shared RDSH-published desktop session.

Note: While implementing resource pool design for your VDI environment, ensure that no individual VMs are provisioned on the same level of hierarchy as a Resource Pool. Doing so would heavily impact resource allocation to your Resource Pools.

Sizing Horizon on VMware Cloud on AWS

Similar to deploying Horizon on-premises, you will need to size your requirements for deploying Horizon on VMware Cloud on AWS to determine the number of hosts you will need to deploy. Compute resources are needed for the following purposes:

- Your virtual desktop or RDS workloads
- Your Horizon infrastructure components such as connection servers, Unified Access Gateways, App Volumes managers, etc.
- SDDC infrastructure components on VMware Cloud on AWS. These components are deployed and managed automatically for you by VMware, but you will need capacity in your SDDC for running them. By default, the mentioned management components will be deployed on the first provisioned cluster in your SDDC.

The methodology for sizing Horizon on VMware Cloud on AWS is exactly the same as for on-premises. What is the different (and simpler) is the fixed hardware configurations on VMware Cloud on AWS. Work with your VMware sales team to determine the correct sizing or use *the online sizing calculator*.

VMware Cloud on AWS configuration maximum

While planning your cloud or hybrid Horizon deployment make sure to check applicable *configuration maximums* including minimum cluster size, maximum number of hosts per cluster, etc.

Note: Horizon can be deployed on a single node SDDC or a multi-node SDDC. However, since a single node does not support HA and has no service SLA, we do not recommend a single node SDDC for production use.

Network configuration for Horizon deployment on VMware Cloud on AWS

The following section describes network configuration in VMware Cloud on AWS using NSX-T.

After you deploy an SDDC instance on VMware Cloud on AWS, two isolated network spaces exist, a management network space and a compute network space. Each has its own NSX Edge Gateway and an NSX Distributed Logical Router for extra networks in the compute section.

The recommended network architecture consists of a double DMZ and a separation between Horizon management components and the RDSH and VDI virtual machines.

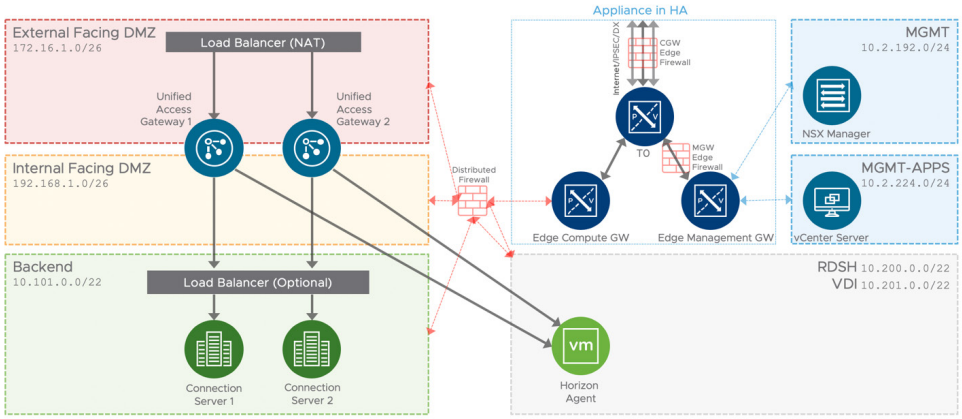


Figure 5. Network configuration for Horizon deployment on VMware Cloud on AWS (subnets are for illustrative purposes only)

Because the Horizon Connection Server must communicate with the vCenter Server, traffic must be allowed on the MGW Edge Firewall.

A third-party load balancer such as F5 LTM or AWS Elastic Load Balancer (ELB) or AVI VMware Load Balancer must be deployed to allow multiple Unified Access Gateway appliances and Connection Servers to be implemented in a highly available configuration.

When direct external access is required, configure a public IP address with destination Network Address Translation (DNAT) towards the Unified Access Gateway virtual IP of the load balancer. AWS egress network fees applies.

For accessing your on-premises resources, create a VPN (Route-based, preferred, or policy-based) or leverage an AWS Direct Connect (DX)

- Route-based VPN uses the routed tunnel interface as the endpoint of the SDDC network to allow access to multiple subnets within the network. Local and remote networks are discovered using BGP advertisements. Route-based VPN can be used as a backup for your AWS DX.
- Policy-based VPN require manual managing of subnets, allowing to communicate from an to VMware Cloud on AWS.
- AWS DX is a service provided by AWS that allows you to create a high-speed, low latency connection between your on-premises data center and AWS services. When you configure AWS DX, VPNs can use it instead of routing traffic over the public Internet. Traffic over Direct Connect is not encrypted. If you want to encrypt that traffic, configure your L3 VPN to use Direct Connect.

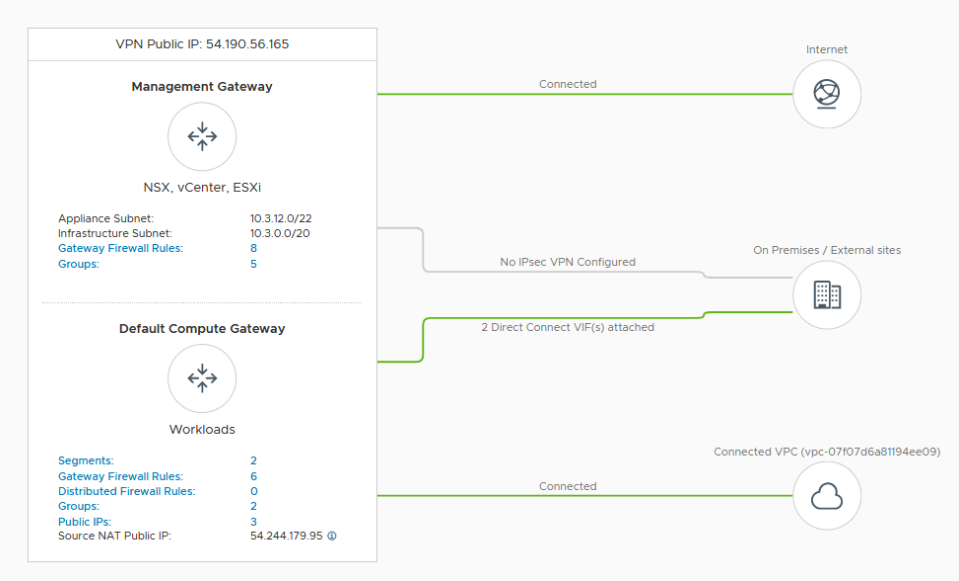


Figure 6. VMware Cloud on AWS network connectivity overview

Using CPA to build hybrid cloud and scale for Horizon

You can deploy Horizon in a hybrid cloud environment when you use CPA to interconnect Horizon on-premises and Horizon pods on VMware Cloud on AWS. You can easily entitle your users to virtual desktop and RDS published apps on-premises and/or on VMware Cloud on AWS. You can configure it such that they can connect to whichever site is closest to them geographically as they roam.

You can also stretch CPA across Horizon pods in two or more VMware Cloud on AWS data centers with the same flexibility to entitle your users to one or multiple pods as desired.

Of course, use of CPA is optional. You can choose to deploy Horizon exclusively in a single VMware Cloud on AWS data center without linking it to any other data center.

Using CPA to provide business continuity (BC) and disaster recovery (DR) for Horizon

Unlike traditional BCDR solution for applications where replication of all data from primary site to secondary site is needed, we recommend a different approach for Horizon, using CPA. Since majority of VDI and RDS deployments use non-persistent and stateless virtual machines that can be created and recreated very quickly, it is senseless to replicate them across sites. CPA can be used across on-premise Horizon pods (primary site) and Horizon pods on VMware Cloud on AWS (secondary site) for the purpose of BCDR. By using VMware Cloud on AWS as a secondary site for BCDR, you can take advantage of the hourly billing option and the pay-as-you-go benefit.

During normal operations, keep a small host footprint on VMware Cloud on AWS where you will deploy your Horizon instance, store your updated golden images and create a small pool of VMs. Note that there is a minimum number of hosts requirement per SDDC.

When the primary site goes down, you can simply create the new virtual desktops as well as new hosts on the secondary site from the exact same golden image. Use Global Entitlements to ensure that your end-users can access desktops on the secondary site.

You will need to keep persistent data such as user profiles, user data, and golden images synced between the two sites by using a storage replication mechanism, such as DFS-R in a hub-spoke topology or another 3rd party file share technology. If you also use App Volumes and User Environment Manager, appstacks and file share data will also need to be replicated from the primary site to the secondary site.

An important consideration in leveraging VMware Cloud on AWS as a secondary site for BCDR involves host availability at the AWS data center when you need your BCDR capacity. While there are usually spare hosts available that can be used to expand your secondary site, depending on your RTO (Recovery Point Objective) and growth requirement, you may not be able to reach your target number right away. The only way to guarantee the number of hosts you need right away is to reserve them ahead of time, but the tradeoff is the high cost. There are things you can do to optimize your availability and cost:

- Segment end-user population into tiers in terms of RTO. Some user segments may require a secondary desktop right away. You should have desktops created and on standby for them. Other user segments may be able to tolerate longer RTO and may require a secondary desktop within hours. In this case, you can wait for new hosts and desktops created. Each new host takes about 10 min to create, assuming the data center has available physical server.
- New hosts in the same cluster are created serially whereas hosts in different clusters are created in parallel. For faster host availability, it is better to have more clusters. Note: the current cluster limit recommended by VMware Cloud on AWS is 16 hosts per cluster.

Work with your VMware sales representative to ensure that you will have adequate BCDR capacity when you need it.

Note: while planning your DR strategy for VDI workload, ensure to accommodate all relevant management components and application required for your users.

Below is an example of how you can set up and configure a BCDR site on VMware Cloud on AWS to protect your primary site. This works similarly regardless of whether the primary site is on-premises or on VMware Cloud on AWS.

In this example, our customer has a 1600 user VDI pod / site on-premise and want to set up a secondary pod/site on VMware Cloud on AWS for the purpose of BCDR. They have determined that they will need 16 hosts on VMware Cloud on AWS for when the entire 1600 users are all using the secondary site. Our customer has also worked with VMware Cloud on AWS team to ensure that there is likely enough spare capacity in the desired region / AZ for the scale up.

They have segmented their users into 2 tiers by their RTO:

- Tier 1 users: these users are essential personnel and need a secondary desktop right away when the primary pod/site goes down. There are 400 of them.
- Tier 2 users: these users will require a secondary desktop within about 2 hours after the primary pod/site goes down. There are 1200 of them.

First create a secondary pod on VMware Cloud on AWS with 4 hosts and pay the reserve instance price. Change Elastic DRS (EDRS) policy to “Optimize for Rapid Scale-out” in VMC console for the cluster designated to host Tier 2 users’ desktops on VMware Cloud on AWS. The policy enables addition of 4 hosts in parallel and allows to rapidly growth the capacity. Check for more details *here.*

Note: “Optimize for Rapid Scale-out” policy does not support automatic scale-in. This task should be done manually after switching back to the main datacenter to reduce costs.

On the 4 hosts, they can deploy 2 connection servers, 2 Load Balancers, 2 Unified Access Gateways, AD Domain Controller, and an event database. Be sure to provision enough infrastructure components for the full BCDR capacity. They also need to store a copy of their golden images in the secondary pod.

Then initialize CPA between their primary pod and secondary pod. Put primary pod in site 1, and secondary pod in site 2.

During normal operations, create 2 pools on the primary pod/site, one for each tier of users, with names of primary_pool_tier1 and primary_pool_tier2. On the secondary pod/site, create 2 pools, one for each tier of users, with names of secondary_pool_tier1 and secondary_pool_tier2. Secondary_pool_tier1 is created with 400 VMs. Secondary_pool_tier2 is created with 1 VM.

Then create 2 global entitlements:

- GE1 consists of primary_pool_tier1 and secondary_pool_tier1, and all of the Tier 1 users.
- GE2 consists of primary_pool_tier2 and secondary_pool_tier2, and all of the Tier 2 users.

When they experience a site-wide outage of the primary site, all users will be automatically logged off. As they try to log back in, the administrator has configured a pre-authentication message to inform them when each tier of users should expect to be able to get a desktop. This prevents users from repeatedly try to log into the secondary site that does not yet have a desktop ready for them. This message must be configured at the pod-level (rather than globally) at this time.

As instructed, the Tier 1 users will try to log back into their desktops right away. Since there's already a pool of 400 VMs ready for these users, they will be transparently connected to their secondary desktops.

In order to accommodate 1200 Tier 2 users the administrator will expand secondary_pool_tier2 from 1 VM to 1200 VMs. This will activate EDRS policy and pool expansion will be done in 4 hosts increment. We expect this process to take 40 to 50 minutes + time to create instant clones (30 min or so). At the pre-specified time, Tier 2 users will start logging into their desktops and be transparently connected to a desktop on the secondary site.

Once the primary site is back online again, users will be automatically connected to their primary desktop the next time they log in. The administrator can simply delete the secondary desktops on the secondary site, and then delete the unused hosts on the secondary site.

Note: The workflow above currently only works with global entitlements involving 2 sites, a primary site and a secondary site. If you have a scenario where you want to use the same DR site for two different primary sites, you still need to create two separate set global entitlements, one set for primary site 1 and secondary site, and another for primary site 2 and secondary site.

You can optionally configure a Global Load Balancer (GSLB) between the two sites and your end-users (such as F5 GTM , AWS Route 53, or others). The global load balancer provides a single-namespace capability that allows the use of a common global namespace when referring to CPA. Using CPA with a global load balancer provides your end users with a single connection method and desktop icon in their Horizon Client or Workspace ONE console. Without the global load balancer and the ability to have a single namespace for multiple environments, end-users will be presented with two different icons (corresponding to the number of pods on which desktops have been provisioned for them), which may potentially get confusing.

Business continuity (BC) and disaster recovery (DR) for Horizon full clone desktops

The BCDR workflow recommended in the previous section works well for non-persistent instant clones. There are some considerations for protection persistent full clone desktops.

First, do your users require the mirror image desktops after a primary site failure? If the answer is yes, then you'll need to replicate your primary full clone desktops periodically to the secondary site. This is the most costly type of protection – for every primary full clone desktop, you'll need an equivalent secondary full clone desktop on VMware Cloud on VMC, running at all times. You'll also need to script the import of secondary desktops into the connection servers on the secondary site as a manual full clone pool.

Most customers find that, given the cost of providing a fully mirrored desktop, it is acceptable to give their persistent full clone desktop users a secondary desktop that is a pristine copy of same golden image. Any user customization or data not saved in a file share and replicated to the secondary site will be lost, so you'll need to ensure that all important user data reside in a file share. You can then use the sample workflow above to provision either an instant clone desktop or a full clone desktop on the secondary site for BCDR purpose.

Configuring VMware Cloud on AWS for Horizon deployment

To deploy Horizon on VMware Cloud on AWS:

1. Create an SDDC instance on VMware Cloud on AWS.
   See the *VMware Cloud on AWS documentation.*
2. Deploy a supported version of Horizon on VMware Cloud on AWS. For more details on supported version of Horizon on VMware Cloud on AWS, see VMware Interoperability Matrix. See the *Horizon product documentation* for more information on Horizon.
3. Set up the Horizon environment on VMware Cloud on AWS. *Check the knowledge base article 58539* for feature parity of Horizon on VMware Cloud on AWS.

Horizon environment on VMware Cloud on AWS

When you set up the Horizon environment on VMware Cloud on AWS, you must install and configure the following components:

- Install and configure Active Directory, DNS, DHCP, and KMS servers according to your design.
- Optionally, install RDS license servers.
- Install Horizon Connection Server and replica connection server for high availability
- You must use cloudadmin@vmc.local for the vCenter Server credentials and select VMware Cloud on AWS when adding the vCenter Server to Horizon.

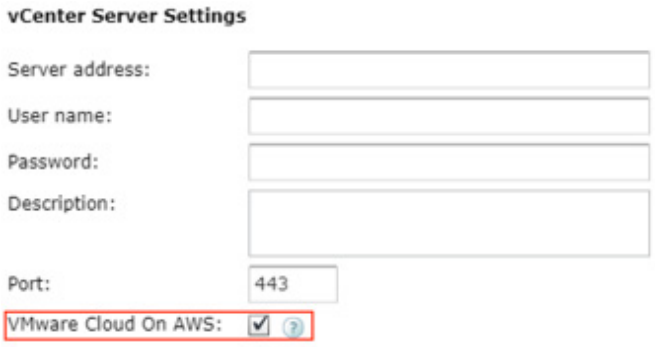


Figure 7. Installing Horizon on VMware Cloud on AWS SDDC

For a single-node cluster, modify the vSAN VM storage policy to "No data redundancy". VMware does not recommend to use a single-node cluster and no data redundancy vSAN policy in production.

Deploy a Unified Access Gateway appliance and connect it to the Connection Server if your deployment supports remote users.

- Use Unified Access Gateway version 3.3.
- Only deploy a single NIC with the OVF Deploy wizard. For multiple NICs, use the PowerShell script to include the password and encode special characters in the .INI configuration file. For more information, see the *Unified Access Gateway documentation*.
- Deploy the NICs to the Compute-ResourcePool, WorkloadDatastore, and Workloads folder.
- Specify netmask0-2 for the NICs.
- Deploy a load balancer if you are using two or more Connection Servers.
- Optionally, install a Horizon event database on Microsoft SQL Server 2016.

Install Horizon Agent on the master images for RDS hosts and VDI virtual desktop VMs. This agent communicates with the Connection Servers.

Deploy Horizon over hybrid cloud

You might already have Horizon environments on-premises. The Horizon pod on-premises and your Horizon pod on VMware Cloud on AWS can be managed separately. Alternatively, you can extend your on-premises Horizon environment to the cloud by linking it with your Horizon on VMware Cloud on AWS environment using CPA. Deploying your Horizon over hybrid cloud enables you to manage your on-premises deployment and your cloud deployment in a single federated space.

For hybrid cloud deployment, follow these steps.

4. Configure network connectivity (VPN or AWS DX) and firewall rules to enable the Connection Server instance on VMware Cloud on AWS to communicate with the Connection Server instance on-premises.
5. Prepare a Microsoft Active Directory (AD) domain controller(s) on your SDDC on VMware Cloud on AWS.
6. Ensure that your on-premises Horizon version is 7.0 or later.
   Note: The Horizon version deployed on-premises does not have to match the Horizon version deployed on VMware Cloud on AWS. However, you cannot mix a Horizon 6 pod (or lower) with a Horizon pod within the same CPA.
7. Use CPA to connect the Horizon pod on-premises with the Horizon pod on VMware Cloud on AWS.
8. For easy sharing of images and ISO, you can use the vCenter Content Library on each vCenter Server.

Network configuration and services for deploying Horizon on VMware Cloud on AWS

To set up a successful hybrid cloud deployment, ensure to understand and configure the following network services.

VMware Cloud on AWS network connectivity

In a preparation for the hybrid deployment you must connect your SDDC with your on-premises data center or with another SDDC. The following connection options can be used:

- VPN (policy- or route-based) over public Internet
- VPN (policy- or route-based) over AWS DX
- AWS DX

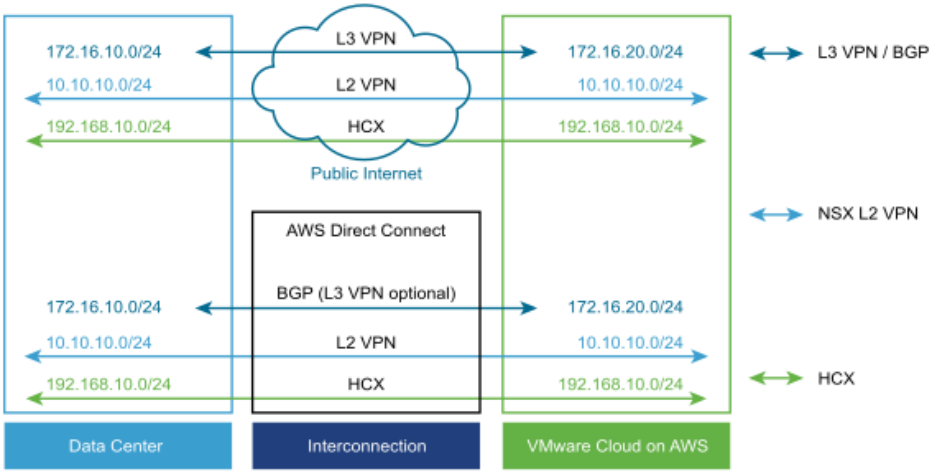


Figure 8. VMware Cloud on AWS network connectivity for Horizon

Depending on the requirements one or another option might be a best fit for you. For a predictable networking experience AWS DX is recommended. Once the connection is established, ensure that routing configuration permits required traffic flow (e.g. all required subnets are correctly announced via BGP to VMware Cloud on AWS for AWS DX and route-based VPNs). Additional network capabilities provided by HCX or L2VPN can be leveraged if needed. Check the *following document for more details.*

DHCP service

It's critical to ensure that all VDI enabled desktops have proper assigned IP address. In most cases you opt for the automatic IP assignment.

VMware Cloud on AWS supports the following ways to assign IP addresses to clients:

- NSX-T based local DHCP service, attached to the Compute Gateway (default).
- DHCP Relay, customer managed.

For better management of IP addresses and possible integration with IP Address Management (IPAM) VMware recommends to use a DHCP Relay for VDI. You will configure the DHCP Relay IP address using VMC console under **Networking and Security – System – DHCP**. See the *following documentation* for the configuration details.

DNS Service

Reliable and correctly configured name resolution is a key for the successful hybrid horizon deployment. While designing your environment make sure to understand *DNS strategies for VMware Cloud on AWS.* You design choice will directly influence the configuration details. You should configure:

- Management Gateway DNS. By default, Google DNS Servers are used. To be able to resolve on-premises resources (on-premises vCenter Server name, ESXi host names, etc.) you will need to specify your own DNS server, capable to resolve names of the mentioned resources.
- Set the DNS resolution of VMware Cloud on AWS vCenter to Private (VMware Cloud on AWS Console, Settings – vCenter FQDN – Resolution Address:)
- Compute Gateway DNS. If you opt to use your own DHCP Relay ensure that DNS Server option is configured correctly on your DHCP server specified as the relay. VMware recommend using local DNS Server (hosted on VMware Cloud on AWS) to reduce dependency on the connection link to on-premises. Choosing AWS native to host your DNS might be another option as described below.

Note: You cannot configure DHCP Relay if the Compute Gateway includes any segments that provide their own DHCP services.

Firewall rules

Firewall Service on VMware Cloud on AWS is based on NSX-T and provides both Distributed (Microsegmentation) and Gateway Firewall Services.

Note: This guide will cover Gateway Firewall Services only. Check *this document* for more information on configuring Distributed Firewall.

To simplify the management of Gateway Firewall VMware recommend using Groups (located under *Networking&Security -- Inventory*) both for Compute and Management. Precreate groups for your on-premises vSphere managements components, VDI components, applications to be accessible from VMware Cloud on AWS. Do the same for VDI components deployed on VMware Cloud on AWS. Groups for vSphere managements components are already precreated by VMware. While creating a group you need to specify IP addresses using CIDR notation. You can include as a member a single host by specifying /32 mask or a continuous range of IPs using relevant CIDR (e.g. /24 to include all IPs within a 24 bit subnet).

Note: Default behavior of both Management and Gateway Firewall is set to deny all traffic not explicitly enabled.

Management Gateway Firewall rules

At minimum you would need to enable the traffic flow between your on-premises vCenter and ESXi hosts and vCenter/ESXi hosts located in VMware Cloud on AWS.

Note: It's a predefined set of Services that you can use while configuring rules for Management Gateway. You cannot add or modify theses services. Each Group (ESXi hosts, vCenter, etc.) has it's own set of services.

You can achieve this by creating the following rules:

NAME	SOURCES	DESTINATIONS	SERVICES	ACTION
SDDC vCenter to on-premises management	vCenter	<On-premises vSphere environment>	Any	Allow
SDDC ESXi hosts to on-premises management	ESXi	<On-premises vSphere environment>	Any	Allow
<On-premises vSphere> to ESXi	<On-premises vSphere>	ESXi	• Provisioning and Remote Console • VMware vMotion • ICMP ALL • HTTPS	Allow
<On-premises vSphere> to vCenter	<On-premises vSphere>	vCenter	• SSO • ICMP ALL • HTTPS	Allow

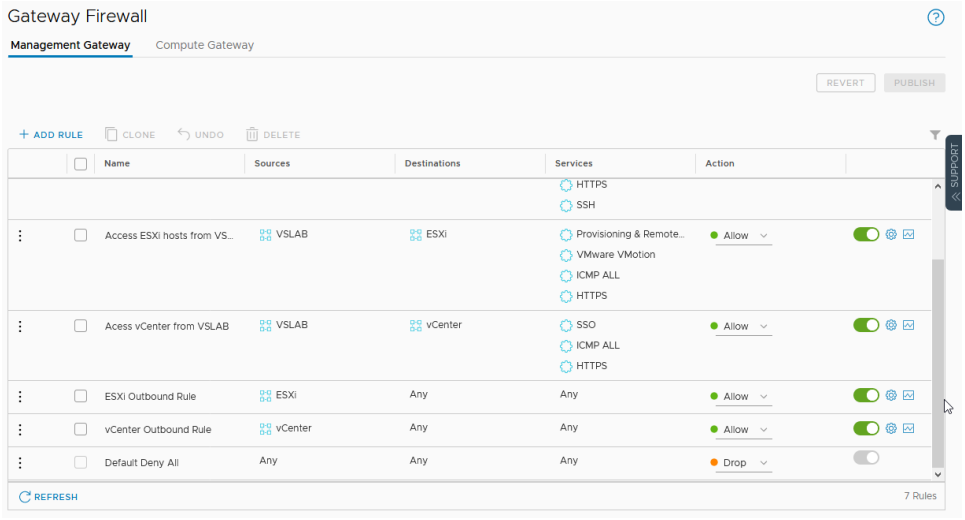


Figure 9. Configure VMware Cloud on AWS Gateway Firewall for Horizon

Compute Gateway Firewall rules

Compute Gateway Firewall controls traffic flow between segments (networks) on VMware Cloud on AWS and between on-premises and segments on VMware Cloud on AWS. Depending on your security requirements you might be able to use a simplified rule(s) enabling all communication between on-premises and VMware Cloud on AWS on subnets basis or create a granular rules for each service (Active Directory, Databases, Applications, etc.). This guide will provide as an example the following set of rule:

1. Enable communication between connection servers to create CPA
2. Enable communication between Active Directory Controllers
3. Enable access to internet for all logical segments used by the VDI workload

This set of rules is neither complete, nor sufficient for a complex deployment—however, gives an example of Compute Gateway configuration. For stricter control and external access, see the Ports and Services chapter in the *VMware Horizon Security* guide.

You will need to prepare the following Compute Groups:

1. **OP-Conn-Servers:** Connection server(s) on-premises. Do not use a Load Balancer IP, use exact IPs of your connection servers
2. **VMC-Conn-Servers:** Connection servers(s) on VMware Cloud on AWS.
3. **OP-AD:** Active Directory Controller(s) on-premises. Ensure to include at least one Global Catalogue and FSMO roles.
4. **VMC-AD:** Active Directory Controllers on VMware Cloud on AWS
5. **VMC-Segments:** VMware Cloud on AWS VDI logical segments. To simplify the configuration use subnets in CIDR notation.

NAME	SOURCES	DESTINATIONS	SVCS	APPLIED TO	ACTION
Connection servers to on-premises	VMC-Conn-Servers	OP-Conn-Servers	All	All Uplinks*	Allow
Connection servers to VMC	OP-Conn-Servers	VMC-Conn-Servers	All	All Uplinks*	Allow
AD to on-premises	VMC-AD	OP-AD	All	All Uplinks*	Allow
AD to VMC	OP-AD	VMC-AD	All	All Uplinks*	Allow
VDI to Internet	VMC-Segments	Any	Any	Internet Interface	Allow

** Applied to fild defines the outbound interface of T1 Compute Gateway and can be set to: All Uplinks (all interfaces), VPC Interface (link to connected VPC and native AWS), Direct Connect Interface (DX based connection to on-premises), Internet interface (Internet connection), VPN Tunnel interface (VPN policy/routed connection to on-premises). Depending on your connection to on-premises you can use direct connect interface or VPN Tunnel instead of all uplinks.

Preparing Active Directory for hybrid cloud deployment

If you are deploying Horizon in a hybrid cloud environment by linking the on-premises pod with the VMware Cloud on AWS pod, you must ensure that desktops clients deployed on VMware Cloud on AWS are able to access the Active Directory environment. VMware recommend to deploy a local domain controller on VMware Cloud on AWS to ensure that the directory service is not dependat on the link to on-premises. You can use a read-only DC, DC with Global Catalog option for the same domain or even a separate domain in the same forest (trust configuration is required in this case). You can also use AWS hosted DC or AWS managed Active Directory.

If you are deploying the Horizon pod on VMware Cloud on AWS as a standalone (that is, not part of a hybrid cloud deployment), you can skip the preparation of the on-premises AD.

Link Horizon Pods on VMware Cloud on AWS

You can use the CPA feature to connect Horizon pods regardless of whether the pods are on-premises or on VMware Cloud on AWS. When you deploy two or more Horizon pods on VMware Cloud on AWS, you can manage them independently or manage them together by linking them with CPA.

- On one Connection Server, initialize CPA and join the Connection Server to a pod federation.
- Once initialized, you can create a global entitlement across your Horizon pods on-premises and on VMware Cloud on AWS.
- Optionally, when you use CPA, you can deploy a global load balancer (such as F5, AWS Route 53, or others) between the pods. The global load balancer provides a single-namespace capability that allows the use of a common global namespace when referring to Horizon CPA. Using CPA with a global load balancer provides your end users with a single connection method and desktop icon in their Horizon Client or Workspace ONE console.

Without the global load balancer and the ability to have a single namespace for multiple environments, end users will be presented with a possibly confusing array of desktop icons (corresponding to the number of pods on which desktops have been provisioned for them). For more information on how to set up CPA, see the *Administering Cloud Pod Architecture in Horizon document.*

Use CPA to link any supported number of Horizon pods on VMware Cloud on AWS. The maximum number of pods must conform to the limits set for pods in CPA. See, the VMware Knowledge Base article *VMware Horizon Sizing Limits and Recommendations (2150348).*

When you connect multiple Horizon pods together with CPA, the Horizon versions for each of the pods can be different from one another. The only limitation is that they all be Horizon v7.0 or higher (i.e. no mixing of Horizon 6 pods).

Shared Content Library

Content Libraries are container objects for VM, vApp, and OVF templates and other types of files, such as templates, ISO images, text files, and so on. vSphere administrators can use the templates in the library to deploy VMs and vApps in the vSphere inventory. Sharing golden images across multiple vCenter Server instances, between multiple VMware Cloud on AWS and/or on-premises SDDCs guarantees consistency, compliance, efficiency, and automation in deploying workloads at scale.

For more information, see *Using Content Libraries* in the vSphere Virtual Machine Administration guide in the *VMware vSphere documentation.*

Note: Management Gateway Firewall should be configured to allow the traffic flow between vCenters sharing content library.

Licensing

For POC or pilot deployment of Horizon on VMware Cloud on AWS, you may use a temporary eval license or your existing perpetual license. However, to enable Horizon for production deployment on VMware Cloud on AWS, you must purchase the new Horizon Subscription License. To obtain the new Horizon Subscription License or for more information on how to upgrade your existing perpetual license to subscription license and associated discounts, please contact your VMware representative.

Different types of Horizon subscription licenses

Horizon Subscription Licenses come in five major flavors:

- Horizon Universal Apps Subscription – deploying RDSH apps only. A single license can be used for deploying on-premises, on VMware Cloud on AWS, on Microsoft Azure or on IBM Softlayer. An on-premise vSphere license is included.
- Horizon Apps Subscription Add-on – deploying RDSH apps only. A single license can be used for deploying on VMware Cloud on AWS only. No on-premise vSphere license is included and therefore this license is lower cost.
- Horizon Universal Subscription – deploying RDSH apps and VDI. A single license can be used for deploying on-premises, on VMware Cloud on AWS, on Microsoft Azure or on IBM Softlayer. An on-premise vSphere license is included.
- Horizon Subscription Add-on – deploying RDSH apps and VDI. A single license can be used for deploying on VMware Cloud on AWS only. No on-premise vSphere license is included and therefore this license is lower cost.
- Workspace One Subscription – deploying Horizon RDSH apps and VDI, as well as Workspace One mobility solution.

Except for Workspace One, all other licenses above have Concurrent User and Named User options.

You can use different licenses (including perpetual licenses) on different Horizon pods whether the pods are connected by CPA or not. You cannot mix different licenses within a pod since each pod only takes 1 type of license. For example, you cannot use both perpetual license and subscription license for a single pod. You also cannot use both the Horizon Universal Apps Subscription license and the Horizon Universal Subscription license for a single pod. Suppose you have two pods deployed, pod A on-premises and pod B on VMware Cloud on AWS and the two pods are connected by CPA, you can use a different license type on each pod. For example, you can use the Horizon Enterprise perpetual license for pod A, and the new Horizon Universal Subscription license for pod B.

The best subscription license you need for your Horizon on VMware Cloud on AWS deployment will depend on your use case. Here are some examples:

- You are setting up a new H7 deployment for 2,000 VDI users on VMware Cloud on AWS. There are no on-premises components. Purchase 2,000-user Horizon Subscription Add-on license in this case.
- You have an existing Horizon pod on-premises for 2,000 users, and you want to deploy a pod on VMware Cloud on AWS for an addition 1,000 users for full time VDI use. The best license type is the Horizon Subscription Add-on for your Horizon pod on VMware Cloud on AWS. You would keep your perpetual license for on-premise pod until renewal and then decided whether to move to Horizon Subscription license for your on-prem pod.
- You have an existing Horizon pod on-premises for 2,000 users, and you want to deploy a pod on VMware Cloud on AWS as BCDR capacity for the 2,000 users on-premise. The best license type is to upgrade your existing 2,000-user perpetual license to 2,000-user Horizon Universal Subscription license. This new license would allow these 2,000 users to connect to virtual desktops either on-premises or on VMware Cloud on AWS. License Enablement

Regardless of whether you are deploying Horizon on-premises or on VMware Cloud on AWS, if you are using any of the subscription licenses, you must install the Horizon Cloud Connector to enable subscription license management for Horizon. The Horizon Cloud Connector is a virtual appliance that connects a Horizon pod with Horizon Cloud Service features.

A MyVMware account from *https://my.vmware.com* is required for Horiozn 7 subscription license. Once you purchase the subscription license, a record will be created in the Horizon Cloud Service using your MyVMware email address, and your subscription license information will be visible to the Horizon Administrator console.

As part of the subscription license fulfillment process, you will receive email with the link to download the Horizon Cloud Connector as an OVA file and follow instructions to deploy the Cloud Connector, from vSphere web client, alongside your new or existing Horizon pods. Once the Cloud Connector is deployed and paired with the Connection Server in the Horizon pod with the Horizon Cloud Service, which manages the Horizon subscription license between connected Horizon pod(s). Unlike the Horizon perpetual license, with a subscription license, you do not need to retrieve or manually enter a license key for Horizon product activation. However, supporting component license keys, e.g., license key for vSphere, license key for App Volumes and others, will be delivered separately and must be manually keyed in to activate the product by the administrator.

Review the Horizon documentation for more details on how to deploy the Horizon Cloud Connector Virtual Appliance. You will need a separate Cloud Connector for each pod.

Deploying desktops on VMware Cloud on AWS with Instant Clone, App Volumes, and User Environment Manager

Instant Clone

In addition to using Full Clones, you can also leverage Instant Clone Technology (starting with VMware Horizon version 7 and above) coupled with App Volumes (starting with App Volumes 2.15) to accelerate the delivery of user-customized and fully personalized desktops. Dramatically reduce infrastructure requirements while enhancing security by delivering a brand-new personalized desktop and application services to end users every time they log in:

- Reap the economic benefits of stateless, nonpersistent virtual desktops served up to date upon each login.
- Deliver a pristine, high-performance personalized desktop every time a user logs in.
- Improve security by destroying desktops every time a user logs out.

When you install and configure Horizon for instant clone for deployment on VMware Cloud on AWS, do the following:

When adding VMware Cloud on AWS vCenter Server to the Horizon configuration, be sure to select the **VMware Cloud on AWS** check box.

- CBRC (Content-Based Read Cache) is not supported or needed on VMware Cloud on AWS. CBRC has been disabled by default.
- On the master image, add the domain's DNS to avoid customization failures.
- When creating Horizon instant-clone pools on VMware Cloud on AWS, use the following settings in the provisioning wizard:
  - **Compute-ResourcePool** resource pool as a parent RP. Create additional RPs according to your design
  - **Workloads** folder as a parent folder. Precreate additional VM folder as needed.
  - **WorkloadDatastore** datastore

Multi-VLAN is not yet supported when creating Horizon instant-clone pools on VMware Cloud.

App Volumes

App Volumes provides real-time application delivery and management, now for on-premise and on VMC:

- Quickly provision applications at scale.
- Dynamically attach applications to users, groups, or devices, even when users are already logged in to their desktop.
- Provision, deliver, update, and retire applications in real time.
- Provide a user-writable volume, allowing users to install applications that follow them across desktops.
- Provide end users with quick access to a Windows workspace and applications, with a personalized and consistent experience across devices and locations.
- Simplify end-user profile management by providing organizations with a single and scalable solution that leverages the existing infrastructure.
- Speed up the login process by applying configuration and environment settings in an asynchronous process instead of all at login.
- Provide a dynamic environment configuration, such as drive or printer mappings, when a user launches an application.

For more information on how to configure, see "*Configuring App Volumes Manager for VMware Cloud on AWS*" in the *App Volumes Administration guide for App Volumes.*

Transfer app volumes from vSphere to VMC

For migration or BCDR purpose, you can transfer your appstacks or user writable volumes from on-premise to the VMware Cloud on AWS environment using your vSphere client in a two-step process.

From the vSphere client on-premises:

1. Create a VM with thin provisioning and attach the volume that you want to transfer to the VM.
2. Select the VM and export it as an OVF template from File > Export to OVF Template.

From vSphere client connected to vCenter managing VMware Cloud on AWS
Click Actions > Deploy OVF Template.

1. Follow on-screen instructions and when you have to select the storage format, select Thin provision.

Note: You also can use HCX or CGA (vMotion) to move a pre-created VM without exporting to OVF.

Once the VM is created, browse the datastore where the OVF was exported and move the VMDK file with its metadata to the cloudvolumes directory. Ensure that you change the template location in the metadata file to point to the new datastore.

User Environment Manager

Use VMware User Environment Manager for application personalization and dynamic policy configuration across any virtual, physical, and cloud-based environment. Install and configure the User Environment Manager on VMware Cloud on AWS just like installing on-premises.

Deploying external storage for user data

User data is an important consideration when thinking about deploying Horizon on VMware Cloud on AWS. For storing user profile and user data, you can either deploy a Windows file share on VMware Cloud on AWS (and use DFS-R to replicate data across multiple sites) or use external storage, such as Dell EMC Unity Cloud Service.

Dell EMC Unity Cloud Edition provides a ready-made solution for storing file data such as user home directories and can be easily deployed alongside Horizon on VMware Cloud on AWS. Dell EMC Unity Cloud Edition also supports Cloud Sync for replicating data between Dell EMC Unity systems on premises and VMware Cloud on AWS.

For deployment details please refer to *Dell EMC Unity Cloud Edition with VMware Cloud on AWS Whitepaper* and *video.*

Estimating data egress cost

Unlike on-premises, deploying Horizon on VMware Cloud on AWS incurs data egress cost based on the amount of data egress traffic your environment will generate. It is important to understand and estimate the data egress traffic.

Understanding different types of data egress traffic

Depending on your deployment use case, you may be incurring cost for some or all of the following types of data egress traffic:

- End-user traffic via Internet - You have configured your environment where your end users will connect to their virtual desktops on VMware Cloud on AWS remotely via the Internet. Any data leaving the VMware Cloud on AWS data center will incur egress charge. Egress data consists of the following components: outbound data from Horizon protocols and outbound data from remote experience features (for example, remote printing). While the former is typically predicable, the latter has more variance and depends on the exact activity of the user.

- End-user traffic via on-premises - You have configured your environment where your end users will connect to their virtual desktops on VMware Cloud on AWS via your on-premise data center. In this case, you will have to link your data center with the VMware Cloud on AWS data center using VPN or AWS DX. Any data traffic leaving the VMware Cloud on AWS data center back to your data center will incur egress charge. And if you have CPA configured between the on-premise environment and the VMware Cloud on AWS environment, you will incur egress charge for any CPA traffic between the two pods (although CPA traffic is typically fairly light).
- External application traffic - You have configured your environment where your virtual desktops on VMware Cloud on AWS has to access applications hosted either in your on-premise environment or in another cloud. Any data traffic leaving the VMware Cloud on AWS data center to these other data centers will incur egress charge.
- Note that data traffic within your VMware Cloud on AWS SDDC or between the SDDC and AWS services in that same region is exempt from egress charge. However, any traffic from the SDDC to another availability zone or to another AWS region will be subject to egress charge.

Data ingress (i.e. data flowing into VMware Cloud on AWS data center) is free of charge.

Estimating data egress traffic with SysTrack from Lakeside

Since the data egress cost is priced per GB, the best way to estimate your data egress cost is to estimate your likely data egress traffic by using a monitoring tool in your existing on-premises environment (whether it's already virtualized or not). Make sure you estimate the different types of data egress traffic listed above separately as applicable. One such monitoring tool is SysTrack from Lakeside Software.

Lakeside's SysTrack workplace analytics solution contains an extensive set of tools to provide relevant planning information for *desktop transformation*. Best of all, this is available at no cost to VMware customers via the *SysTrack Desktop Assessment* (SDA). Through the SDA, customers can collect detailed environmental information, including recommendations for deployment options and resource requirements, with only the need to deploy the SysTrack agent to systems being considered for transformation. For advanced cases, the on-premises version of SysTrack can be used as well. This guide will make the assumption that such a deployment is already in place. For additional setup details or questions about the SDA, the *Quick Start Guide* is a good resource.

Once SysTrack is deployed in the environment, it will immediately begin collecting relevant information from devices on which it's installed. For this guide we'll focus on the most interesting facets of data collection for the network:

- Per device network usage
- Per session protocol bandwidth usage
- Per application (and destination) bandwidth usage

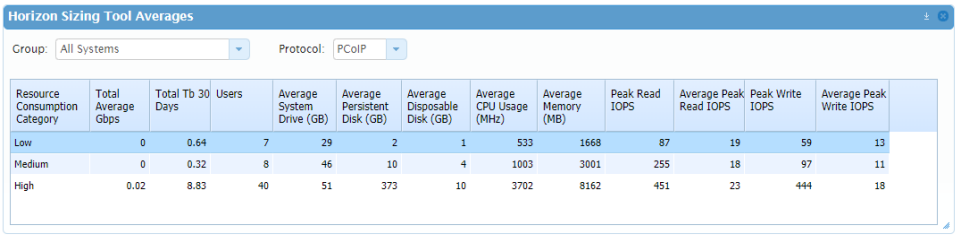
The key is thinking about how best to combine these pieces of information into something that's useful for planning costs. Because the ingress data is free on VMware on AWS, we'll focus on the egress data as observed from the devices in the collection. That will take the form of "transmitted" data from that device to other destinations, and you'll see more details about this as we go into methodology we suggest.

With SysTrack you can make use of two different styles of calculation depending on the level of detail you'd like to see. We've created several dashboards that customers can use to easily visualize this information in SysTrack.

Note: All figures in these dashboards are measured in bits, not bytes.

1. Basic network egress bandwidth calculation
   The Horizon Sizing Tool dashboard provides some basic numbers to help you plan your migration to the VMware cloud. The table below breaks users down into categories based on egress bandwidth consumption. Resource consumption metrics are supplied for each category as well as egress bandwidth consumption for applications and three remote display protocols: ICA, Blast and PCoIP.

   The resource consumption metrics can be fed into some of VMware's sizing tools (Horizon Sizing Tool and Horizon Sizing Estimator). These tools provide guidance on how to plan for the number and size of systems you will be deploying.



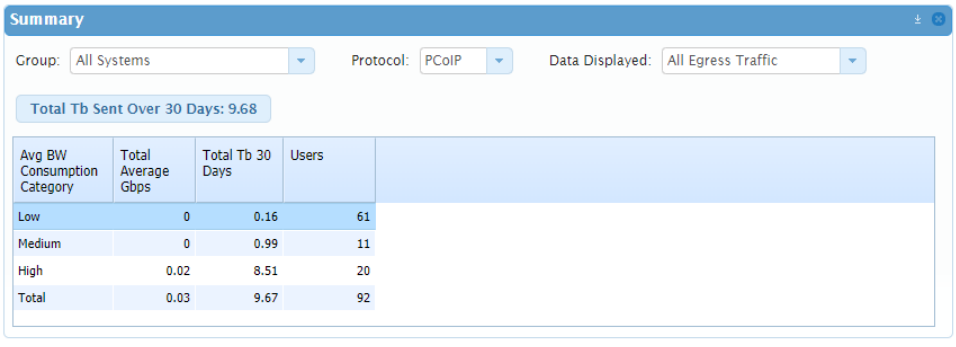
Resource Consumption Category	Total Average Gbps	Total Tb 30 Days	Users	Average System Drive (GB)	Average Persistent Disk (GB)	Average Disposable Disk (GB)	Average CPU Usage (MHz)	Average Memory (MB)	Peak Read IOPS	Average Peak Read IOPS	Peak Write IOPS	Average Peak Write IOPS
Low	0	0.64	7	29	2	1	533	1668	87	19	59	13
Medium	0	0.32	8	46	10	4	1003	3001	255	18	97	11
High	0.02	8.83	40	51	373	10	3702	8162	451	23	444	18

Figure 10. Horizon Sizing Tool dashboard

2. Advanced network egress bandwidth calculation
   The Advanced Horizon Sizing Tool offers advanced sizing calculations which can be used to estimate costs around migrating to the VMware cloud. VMware cloud pricing is based around the level of data transmitted from the cloud back to the client (i.e. egress bandwidth consumption).

   Within the dashboard, each user is put into a category based on egress bandwidth consumption. This can be based on actual SysTrack data if you are migrating from an existing virtual environment or estimated if migrating from a physical environment. You can select the protocol you would like to use to estimate values for users on physical machines, as well as the type of egress data displayed – protocol, application or a combination of both.

   A summary table shows these categories and tells you the total and average for egress bandwidth consumption.



Avg BW Consumption Category	Total Average Gbps	Total Tb 30 Days	Users
Low	0	0.16	61
Medium	0	0.99	11
High	0.02	8.51	20
Total	0.03	9.67	92

Figure 11. Advanced Horizon Sizing Tool dashboard

This same data is also presented in graph form for a more visual presentation:

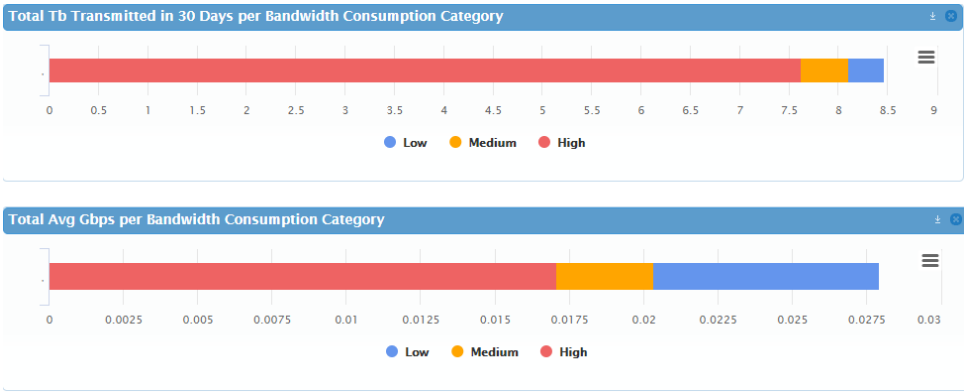
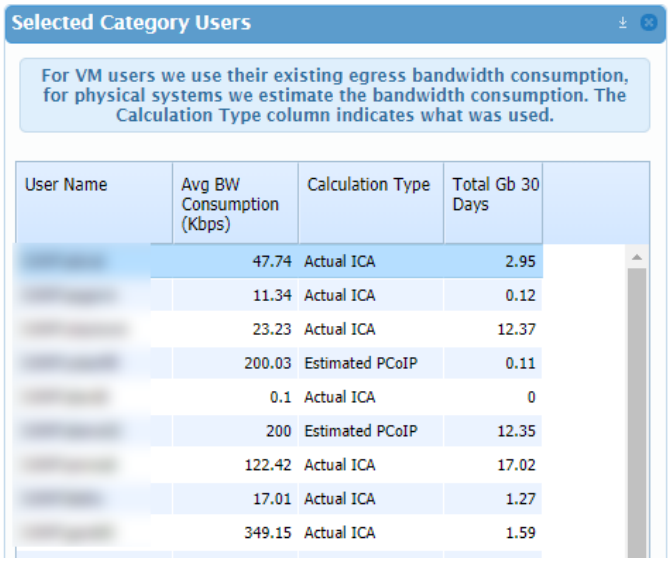


Figure 12. Horizon Sizing Tool dashboard

You can also see more detail on a per user basis depending on the category selected in the summary table. The table below shows total and average bandwidth consumption as well as calculation type, which indicates which data source was used to generate the consumption values. Here is an example of how to determine monthly egress bandwidth per VM in gigabytes.



User Name	Avg BW Consumption (Kbps)	Calculation Type	Total Gb 30 Days
[redacted]	47.74	Actual ICA	2.95
[redacted]	11.34	Actual ICA	0.12
[redacted]	23.23	Actual ICA	12.37
[redacted]	200.03	Estimated PCoIP	0.11
[redacted]	0.1	Actual ICA	0
[redacted]	200	Estimated PCoIP	12.35
[redacted]	122.42	Actual ICA	17.02
[redacted]	17.01	Actual ICA	1.27
[redacted]	349.15	Actual ICA	1.59

Figure 13.Horizon Sizing Tool dashboard - per user view

If you want to simply calculate the egress bandwidth for an average VM, you can take the "Total Tb 30 Days" and "Users" values in the advanced dashboard summary table and perform the following calculation:

Monthly GB egress bandwidth per VM = (([Total Tb 30 Days]/8) * 1024) / [Users]

From the data in Figure 14, the calculation would become this:

Monthly GB egress bandwidth per VM = ((9.67/8) * 1024) / 92 = 13.5 GB

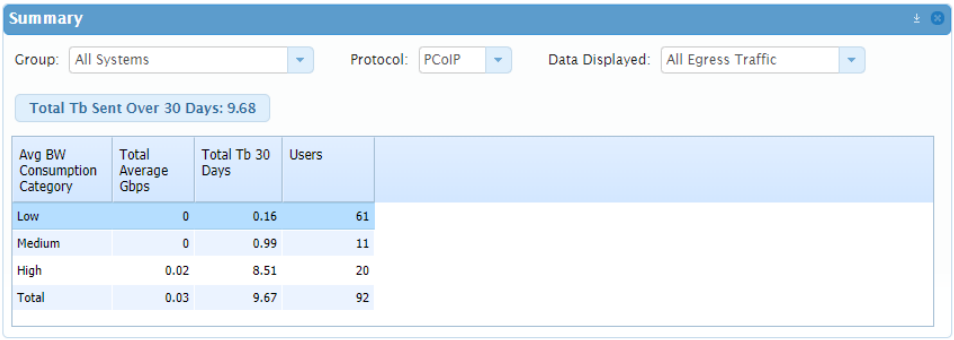


Figure 14.Horizon Sizing Tool dashboard - summary information

Using native AWS services with Horizon on VMware Cloud on AWS

Combining Horizon with native AWS services and VMware Cloud on AWS allows organizations to get the best of both worlds – easily consumed cloud services to provision and operate enterprise applications with a platform that requires few changes to the applications themselves and operational processes.

Utilizing native AWS services like those listed in this section has additional benefits for EUC environments. When deploying Horizon on VMware Cloud on AWS, the management infrastructure is typically deployed in the SDDC alongside the desktops. By utilizing native AWS services, resources that would otherwise be reserved for and consumed by servers can now be utilized for desktops, providing a greater desktop density. The following section explores and details the AWS services that are complimentary to Horizon on VMware Cloud on AWS.

Below are details on how you can seamlessly integrate Horizon on VMware Cloud on AWS with native AWS services:

AWS Direct Connect

Simplify migration and increase interoperability between your data center and VMware Cloud on AWS with AWS Networking Services. **AWS Direct Connect.** This service uses a dedicated, secure network connection to an organization's on-premises data center. AWS Direct Connect can provide a more consistent network experience than VPN connectivity via the public internet.

AWS Direct Connect offers bandwidth flexibility, 1Gbps and 10Gbps are available to suit the requirements of organizations. Additionally, AWS Direct Connect id compatible with all AWS services, including VMware Cloud on AWS.

For Horizon deployments AWS Direct Connect enables users to connect to resources that are yet to migrate to the cloud and are hosted in an on-premise datacenter, and/or to their virtual desktop from an organization's premises with predictable, consistent performance.

Elastic Load Balancing

Elastic Load Balancing automatically distributes traffic across a number of resources for the purposes of performance, scale and availability. AWS offers an **Application Load Balancer** (ALB) and a **Network Load Balancer** (NLB). ALB is suited to web traffic such as HTTP and HTTPS. NLB is aimed at TCP, UDP and TLS where performance is a priority consideration and requirement. These load-balancers can help reduce the complexity of an organization's environment.

In a Horizon environment ALB and NLB can replace existing 3rd party load balancers to scale and protect the Unified Access Gateways and Connection servers. This can reduce cost and complexity of a deployment by eliminating additional 3rd party components and utilizing native AWS Services.

Amazon FSx

Leverage **Amazon FSx** for scalable, elastic VDI workload storage either or on-premises or AWS. Amazon FSx provides the native compatibility of third-party file systems, this reduces the administrative overhead of provisioning and managing file servers and storage. It also automates additional administrative tasks such as hardware provisioning, software configuration, patching, and backups.

Amazon FSx for Windows File Server is built on Microsoft Windows Server and includes full support for the Server Message Block (SMB) protocol, Windows New Technology File System (NTFS), Active Directory integration, and Distributed File System (DFS). It is built on solid state drive (SSD) storage, is fully managed, and comes complete with automated backups.

Amazon FSx for Windows File Server provides a fully managed, native AWS shared file system for in-guest file storage to the Horizon Desktops that reside in your VMware Cloud on AWS SDDC.

File systems ranging from 300 GiB to 65,536 GiB in storage capacity can be created, including throughput capacity ranging from 8 MB/s to 2048 MB/s. There's no need to worry about capturing and storing backups, or how to restore from a backup in a disaster recovery event.

To gain an understanding of how Amazon FSx for Windows File Server can be used within a VMware Horizon, consider the following example. To consolidate data centers and migrate a large Horizon VDI environment to the cloud. A large set of user data are stored in native Windows file shares. To accelerate the migration process, VMware Cloud on AWS is employed to remove the need for re-tooling or re-platforming the VDI environment and Amazon FSx for Windows File Server is utilized to provide the SMB shares required for user home directories and group shared folders.

Amazon Route 53

Seamlessly integrate the **Amazon Route 53** Domain Naming System (DNS) with your virtual desktops and applications to simplify DNS management for VDI. Amazon Route 53 is a scalable, highly available DNS service, designed to give organizations a simple, reliable and cost-effective way to connect users to resources. With Amazon Route 53 Traffic Flow global traffic management id simplified, various routing options are available, such as; Latency Based Routing, Geo DNS, Geo-proximity, and Weighted Round Robin.

Organizations looking to deploy Horizon on VMware Cloud on AWS in multiple AWS Regions, or simply manage a DNS zone can utilize Amazon Route 53. To manage DNS failover between the locations this highly available and scalable cloud DNS service enables organizations to deliver a reliable and cost-effective way to route end users to Horizon deployments, as well as internet applications either on or outside of AWS.

AWS Directory Service for Microsoft Active Directory

Manage Horizon workloads using **AWS Directory Service for Microsoft Active Directory** (also known as AWS Managed Microsoft AD). AWS Managed Microsoft AD provides a managed Active Directory in the AWS Cloud. Built on an actual Active Directory, AWS Managed Microsoft AD does not require the synchronization or replication of data from an existing Active Directory. Standard. AWS Managed Microsoft AD allows for the use of the usual Active Directory administration tools such as, Active Directory User and Computers and Group Policy Management Console.

AWS Managed Microsoft AD enables the simple migration of Horizon workloads without the need to build out a full Active Directory infrastructure whilst still leveraging all the management tools familiar to them. Trust relationships are available into existing Active Directories to extend and leverage the existing user credentials to access Horizon resources. Each Directory is built across multiple Availability Zones, failures are

REFERENCES:

VMware Cloud on AWS Getting Started

VMware Cloud on AWS Networking and Security

Horizon on VMware Cloud on AWS Technical Content

Horizon on VMware Cloud on AWS. Product Resources

automatically detected and failed Domain Controllers replaced. Data replication, backup, patching and updates are all managed.

Amazon Relational Database Service

Accelerate the storage and retrieval of data in your database virtual desktop and virtual application environment using the **Amazon Relational Database Service (Amazon RDS).** Amazon RDS provides a managed database service, management of the underlying EC2 instance and the operating system are abstracted from the organization. Administrative tasks such as provisioning, backup and updates are all managed by AWS.

Several database engines are available for Amazon RDS, these include; Amazon Aurora, Microsoft SQL, ProstgreSQL, MySQL, MariaDB and Oracle.

Amazon RDS is highly scalable, scaling operation take just a few clicks in the AWS console or via a simple API call. With pass On Demand, and Reserved Instance pricing available Amazon RDS offers organizations an inexpensive way to provision their database requirement.

In a Horizon environment Amazon RDS with the Microsoft SQL server database engine can be utilized to host the View Events database. This removes the need for VDI administrators to build-out and manage complex and a costly SQL Server environment.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com