VMware Cloud on AWS Frequently Asked Questions

Table of contents

VMware Cloud on AWS Frequently Asked Questions

General

What is VMware Cloud on AWS?

VMware Cloud™ on AWS brings VMware's enterprise-class SDDC software to the AWS Cloud with optimized access to AWS services. Powered by VMware Cloud Foundation, VMware Cloud on AWS integrates VMware compute, storage and network virtualization products (VMware vSphere®, vSAN™ and NSX®) along with VMware vCenter management, optimized to run on dedicated, elastic, bare-metal AWS infrastructure.

Where is VMware Cloud on AWS available today?

VMware Cloud on AWS is available in AWS regions world-widelisted in the documentation. Please note that some regions require customers to explicitly opt-in to link their own AWS account to SDDCs.

What are the features included in VMware Cloud on AWS?

Please visit the VMware Cloud on AWS Roadmap page for the latest information on features.

What do you mean by "SDDC?"

SDDC stands for Software-Defined Data Center. A deployment of vSphere, vSAN, NSX, and more inside VMware Cloud on AWS is encapsulated into a unit we refer to as an SDDC, which is roughly equivalent to a vSphere cluster in the on-premises world. You can create multiple SDDCs and each SDDC is composed of clusters which are in turn composed of hosts.

Can workloads running in a VMware Cloud on AWS SDDC integrate with AWS services?

Yes. VMware Cloud on AWS SDDC is running directly on AWS elastic bare metal infrastructure, with high bandwidth, low latency network connectivity to AWS services. This connectivity provides access to over 200 AWS services.

How do I sign up for the service?

Please contact your VMware account team, AWS account team or AWS partner network. You can learn more about the onboarding process with our Quick Start.

How does VMware protect customer data in VMware Cloud on AWS?

VMware Cloud on AWS is designed with multiple layers of protection. The service inherits all of the physical and network protections of the AWS infrastructure and adds dedicated compute and storage along with the security capabilities built into vSphere, vSAN and NSX. All data transmitted between your customer site and the service can be encrypted via VPN. All data between the VMware Cloud on AWS service and your SDDCs is encrypted. Data at rest is encrypted. The VMware Cloud on AWS infrastructure is monitored and regularly tested for security vulnerabilities and hardened to enhance security. Learn more about security at the VMware Trust Center.

What VMware SDDC products do I need to have on-premises for VMware Cloud on AWS?

There are no requirements for an on-premises environment to use VMware Cloud on AWS. At the same time, many customers extend their on-premises VMware environment to the cloud with VMware Cloud on AWS for a variety of use cases including data center evacuations and disaster recovery DR. Currently supported versions of VMware vSphere are supported for hybrid cloud connectivity and migrations. Please refer to the VMware Compatibility Guide for more information.

Is there localized language support for the international regions?

VMware Cloud on AWS now supports language and regional format settings in French, Spanish, Korean, Simplified Chinese and Traditional Chinese, in addition to German, Japanese, and English. These languages are supported in the VMware Cloud on AWS Console and in Cloud Service Platform features such as Identity & Access Management, Billing & Subscriptions, and some areas of the Support Center. You can change your display language before you login to the VMware Cloud on AWS console or in your account settings. See How Do I Change My Language and Regional Format for more information.

How is VMware Cloud on AWS deployed?

VMware Cloud on AWS infrastructure runs on dedicated, single tenant hosts provided by AWS in a single account, provisioned through the VMware Cloud Console. There are different host instance types to choose from based on your sizing requirements. Sizing and differences between the instance types can be found in our brief on SDDC host types. See Feature Brief: SDDC Host Types for more information.

Each host can run many virtual machines (tens to hundreds depending on their compute, memory, and storage requirements). Clusters can range from a minimum of two (2) hosts up to a maximum of sixteen (16) hosts per cluster. A single VMware vCenter Server is deployed per SDDC.

While VMware Cloud on AWS customers need to have an AWS account associated with their deployments, customers do not need to provision hardware directly with AWS. Provisioning and configuration is done automatically through the VMware Cloud Console.

Industry & Compliance

What compliance certifications has VMware Cloud on AWS achieved?

VMware Cloud on AWS has been independently verified to comply with many leading compliance programs, including but not limited to ISO 27001, ISO 27017, ISO 27018, SOC 2, HIPAA, PCI-DSS, OSPAR, IRAP. Check VMware Cloud Trust Center for more information.

Is VMware Cloud on AWS SDDCs compliant with PCI-DSS (PCI)

The VMware Cloud on AWS cloud platform has successfully been assessed to meet PCI compliance as a level 1 service provider.

What regions are available to run PCI compliant workloads on VMware Cloud on AWS?

Regions that can host PCI-compliant SDDCs can be found in the documentation.

If a customer migrates their VMs into a PCI Compliant SDDC, does that mean that their VMs/Applications are automatically also PCI Compliant?

No. The whitepaper “Migrating PCI Workloads to VMware Cloud on AWS” illustrates how the Shared Responsibility Model relates to PCI compliance. The responsibilities are shared between VMware and Customers. VMware handles PCI compliance of the VMware Cloud on AWS cloud service and cloud platform. Similarly, customer workloads running in VMware Cloud on AWS must pass an entirely separate PCI assessment solely managed by the customer. Customers must hire a Qualified Security Assessor (QSA) to assess and verify their PCI SDDC configuration and must verify that the workloads are PCI-compliant.

Can a standard SDDC be upgraded to a PCI SDDC?

Yes, a standard SDDC can be retrofitted with PCI compliance hardening through the SDDC settings.

What is the difference between a standard SDDC and a PCI SDDC?

PCI SDDCs will have the following major differences from a standard SDDC to prevent non-compliant services from impacting their PCI compliance status:

- SDDC components (vCenter, vSAN, ESXi) are "Security Hardened" based on VMware security standards incorporated from GovCloud. NSX appliances are security hardened using NSX Hardening guidelines.
- PCI Customers must use the local NSX Manager to manage SDDC networking and security. This is accomplished by disabling the Networking & Security Tab in the VMC Console.
- Although customers can use non-compliant VMware Cloud on AWS Add-ons during the setup of their SDDC, our PCI auditors determined that customers must disable VMware HCX and Site Recovery Add-ons (These Add-ons are not currently PCI compliant and must be disabled by the customer administrator in the VMC Console).

Can I continue using HCX in a PCI DSS Compliant SDDC?

HCX can be used to migrate/re-locate virtual machines between SDDCs (ie from onprem to VMware Cloud on AWS) however HCX must be removed upon completion in order to maintain a PCI compliant environment.No, this Add-on is not PCI compliant.

Can a PCI Compliant SDDC be deployed on any host type?

Yes. All PCI configurations are done at the SDDC layer and are independent of the underlying physical hosts.

Which auditor is VMware using for the PCI Audit?

Crowe is VMware Cloud on AWS PCI QSA. The PCI Compliance report can be found here https://www.vmware.com/products/trust-center/certificate.html?family=PCI-DSS by selecting the VMware Cloud on AWS “DOWNLOAD” option

Will customers need to buy any additional VMware Cloud on AWS licenses in order to deploy a PCI Compliant SDDC?

No, the published pricing for bare metal VMware Cloud on AWS hosts is all that is required from a cost perspective. There are no additional charges for PCI SDDCs.

How many SDDCs will customers need for Development, Production, and PCI workloads?

System sizing and design is ultimately a customer-driven activity, though VMware can help. Many organizations choose to limit the scope of compliance and compliance audits by deploying separate SDDCs for PCI-DSS workloads.

Will PCI Compliant SDDCs be upgraded similar to standard SDDC's?

Yes, patching and upgrading will be automatically handled by the VMware Operations team via standard lifecycle processes.

Can APIs and/or automation like PowerCLI or Terraform be used to configure a PCI SDDC?

Yes. Terraform and APIs can be used to configure a PCI SDDC.

If customer’s business requirements get changed, can they revert back to the previous non-PCI compliant configuration?

Yes, this can be done but not through the VMC console. Please contact VMware Support to make this request.

How do customers log into the local NSX Manager to create network segments, manage DFW micro-segmentation rules, etc.?

Customers can use the VMware NSX Manager URL and local VMware NSX account credentials. That information is found in the SDDC Settings tab.

What connectivity differences are there in a PCI Compliant SDDC?

All the same connectivity options are available to a PCI-compliant SDDC as with a standard SDDC.

What are the steps to provision a PCI DSS compliant SDDC from the VMC console for a customer:

A customer would need to perform the following steps:

- Identify an Org or create a new Org where a PCI SDDC will be created
- Create a ticket with VMware Support to request enabling PCI for the Organization.
- Confirm that the change has been implemented by VMware
- Deploy a new SDDC
- Prepare SDDC to host PCI workloads. Configure a network connection to on-premises.
- Create firewall rules on the Management Gateway Firewall to enable access to the local NSX Manager and validate access was setup correctly.
- Disable Networking & Security Tab using the Components Control section of the VMC console
- Disable Site Recovery and/or HCX Add-ons using the Components Control section of the VMC console
- Complete successful customer PCI DSS audit with a QSA
- The customer QSA will confirm when customers can start running PCI DSS Compliant VMs, applications and production cardholder data.

How can I request approval for penetration testing applications and systems in my SDDC?

VMware has a comprehensive vulnerability management program that includes third-party vulnerability scanning and penetration testing. VMware conducts regular security assessments to maintain VMware Cloud on AWS compliance programs and continuously improve cloud platform security controls and processes. While the requirements to conduct penetration testing vary by industry compliance regulations, customer environments benefit greatly with penetration testing to measure the security effectiveness within their virtual infrastructure (SDDCs) and applications. To notify VMware that you plan to conduct penetration testing, please use this Request Form to provide us relevant information about your test plans. VMware will respond with an approval by email. Penetration testing must be conducted in accordance with our Penetration Testing Rules of Engagement

Support

Where can I take advantage of the chat support feature?

In-service chat support is available for all features of VMware Cloud on AWS, including hybrid solutions such as vCenter Hybrid Linked Mode and vCenter Cloud Gateway. Chat support is available 24x5 in English directly within the VMC Console across all global regions but is not currently available for on-premises-only solutions.

Can I set my own notification preferences in VMC Console?

Yes, please navigate to the left menu in the VMC Console and click “Notification Preferences” to pick and choose which notifications you’d like to receive. Ensure you click “Save Changes” when satisfied with your selections.

Who can control my notification preferences?

For now, these are enabled at the user level. What is meant by that is each user is responsible for setting their own notification preferences and only you have control over those settings. Changes you make within your own VMC Console will not affect other users.

What roles do I need to be able to set my notification preferences?

To access the Notification Preferences, you must be a part of the associated Organization as either an Organization Owner or Organization User. You must also be assigned one of the following Service Roles:

- VMware Cloud Admin
- VMware NSX Cloud Admin
- VMware NSX Cloud Auditor

Single Host SDDC

What is the Single Host SDDC offering?

With the new time-bound Single Host SDDC starter configuration, you can now purchase a single host VMware Cloud on AWS environment with the ability to seamlessly scale the number of hosts up within that time period, while still retaining your data. The service life of the Single Host SDDC starter configuration is limited to 60-day intervals. This single host offering applies to customers who want a lower-cost entry point for proving the value of VMware Cloud on AWS in their environments.This is a great way to get started with VMware Cloud on AWS with a Proof-of-Concept.

How is Single Host SDDC priced?

Single Host SDDC is available on-demand only. Where is the Single Host SDDC available today?

The Single Host SDDC is available across all the supported regions.

What are the features included in the Single Host SDDC?

Features that do not require more than one host are included in the Single Host SDDC offering, including hybrid operations between on-premises and VMware Cloud on AWS. However, any operations or capabilities that require more than one host would not work. For example, High Availability (HA) and stretched clusters across two AWS AZ. Due to the nature of single host, if your host fails, your data would be lost. VMware does not currently offer patching or upgrades to a Single Host SDDC.

Single Host SDDC highlights:

- Accelerated onboarding
- Migration capabilities between on-premises and VMware Cloud on AWS – VMware HCX for large-scale rapid migration, VMware vMotion for live migration and lastly cold migration.
- Seamless high-bandwidth, low latency access to native AWS services
- Disaster Recovery – Evaluate VMware Site Recovery, the cloud-based DR service optimized for VMware Cloud on AWS. VMware Site Recovery is purchased separately as an add-on service on a per-VM basis.
- Expert support – Single Host SDDC receives the same unlimited 24/7 VMware Global Support Services as well as 24/5 live chat support
- Hybrid Linked Mode support – Single logical view of on-premises and VMware Cloud on AWS resources
- All-Flash vSAN storage – All Flash vSAN configuration, using flash for both caching and capacity, delivers maximum storage performance.

How many Single Host SDDCs can I provision?

You may provision no more than one Single Host SDDC at a time.

Can I run a Single Host SDDC indefinitely?

A Single Host SDDC will be deleted after 60 days. All data on the SDDC will be lost. You can scale up a Single Host SDDC into a 2 host SDDC and retain all your data. A 2 host SDDC is not time-bound.

Can I extend the lifetime of my Single Host SDDC beyond 60 days?

No, but you may create a new Single Host SDDC if you are under your Single Host SDDC limit, and use migration techniques such as Cross-vCenter vMotion to move workloads.

Can I add hosts to a Single Host SDDC?

Yes, a Single Host SDDC can be non-disruptively scaled up to a 2-host SDDC at any point within the 60-day period.

Can I upgrade from Single Host to a production SDDC?

Yes.By adding at least 1 additional host your cluster becomes a full production SDDC with all the features and capabilities available with the VMware Cloud on AWS service.

How do I scale up to a production SDDC?

You can simply click on the "Add host" optionto scale up to the standard production SDDC service. Your data will be retained..

Do I have to connect my Single Host SDDC to an AWS account?

Yes, but It is possible to defer account linking for Single Host SDDCs for up to 14 days, but it is not possible to scale-up your Single Host SDDC to a production configuration (2+ hosts) without connecting to an AWS account.

Can I convert my standard 2-host SDDC into a Single Host SDDC?

No, a Single Host SDDC must be created as a single host. You cannot scale down from a 2 host to Single Host SDDC.

What support would I get with this offering?

Single Host SDDC receives the same unlimited 24/7 VMware Global Support Services as well as 24/5 live chat support via the VMware Cloud on AWS Console and via vSphere Client.

What service level agreement (SLA) do you offer for a Single Host SDDC?

We offer no SLA for the Single Host SDDC. In case of a component or host failure, you may lose your data.

2-Host SDDC Cluster

What is the 2-host cluster capability?

The 2-host cluster capability enables a customer to provision a persistent production cluster with just 2-hosts in VMware Cloud on AWS. Previously a customer needed 3-hosts to spin up a persistent cluster in VMware Cloud on AWS. This offering is a great place to start for customers who do not need the full 3-host Production cluster due to smaller size workloads or wish to prove the value of VMware Cloud on AWS for a longer duration than the Single Host SDDC can offer today.

How is the 2-host cluster priced?

The cost per host is the same as the 3+ host pricing. For a cluster, this means that the 2-host cluster results in a 33% lower cost of entry with a persistent, full production environment.

Does the 2-host cluster support Custom Core Counts?

Yes, secondary 2-host clusters within existing SDDCs can use custom core counts.

In which regions is the 2-host cluster available today?

The 2-Host cluster is available in all regions where VMware Cloud on AWS is available today.

What are the features included in the 2-host cluster?

Features included in the 2-Host cluster are the same as a 3+ host Production SDDC, except for Optimized Elastic DRS policies (optimize for cost, optimize for performance and rapid scale-out).

How many 2-host clusters can I provision?

You may provision as many 2-host clusters as you wish up to the limit of the SDDC, currently 20 clusters. You can mix an SDDC with a 2-host cluster and 3+ host clusters.

Can I run a 2-host cluster beyond 60 days (unlike the Single Host offering?)

Yes, there is no limitation to the lifetime of a 2-host cluster.

What support is available for 2-Host Clusters?

The 2-Host cluster has the same level of support as all other production SDDCs.

What (service level agreement) SLA do you offer for the 2-host cluster?

The 2-host has the same SLA as other production SDDCs clusters. SLA details can be reviewed here.

Can I scale up from 2-hosts to 3-hosts?

Yes. Not only does the 2-host cluster offer the Default Elastic DRS Policy, but manual scale-up is also available at any time from the VMC Console. .

Can I scale down from 3+ hosts back to 2-hosts?

Yes. 3-host Production SDDCs can be scaled down to a 2-host cluster.

What Add-ons are compatible with 2-Host Clusters?

All add-ons supported for production SDDCs are compatible with 2-Host clusters.

Can I use a Stretched Clusters with the 2-host cluster?

Yes, stretched deployments are available for the 2-Host cluster, in a 1-1 configuration, with 99.9% SLA. For information on stretched cluster configuration options: https://vmc.techzone.vmware.com/vmc-arch/docs/compute/vmc-aws-stretched-cluster

Can I use all of the Optimized EDRS policies with the 2-host cluster?

No. Only the Default Storage EDRS policy is currently available.

How can I purchase the 2-host cluster?

The 2-host cluster can be purchased in the same manner as any other SDDC and can typically be spun up in less than 2 hours in a similar fashion to the Single Host SDDC and 3-host SDDC. Once provisioned, it can be scaled up in a matter of minutes to a 3+ host SDDC.

How many VM’s can I run on a 2-node Cluster?

While a 2-node cluster supports the same number of VMs per host as any other configuration, due to Admission Control, a 2-node I3.metal cluster can power on no more than 35 workload VMs at a time. This is to ensure vSphere HA will be able to restart any running workload in case of a failure. You can find more details on TechZone.

VMware Site Recovery

Where can I find information about VMware Cloud Disaster Recovery?

VMware Live Recovery offers ransomware recovery and disaster recovery leveraging two technology stacks:

- VMware Live Cyber Recovery (formerly known as VMware Cloud Disaster Recovery)
- VMware Live Site Recovery (formerly known as VMware Site Recovery Manager)

However, VMware Live Site Recovery cannot be used with VMware Cloud on AWS. Instead, VMare Site Recovery is available for VMware Cloud on AWS customers.

You can find detailed FAQs for VMware Live Recovery here

VMware Site Recovery

Where can I find more information about VMware Site Recovery?

You can find detailed FAQs for VMware Site Recovery here

Workload Migration

What is vSphere vMotion between on-premises and VMware Cloud on AWS and what does it require?

VMware vSphere vMotion enables live migration of powered on VMs between hosts and environments. This includes on-premises hosts to VMware Cloud on AWS SDDCs, and offers zero downtime for the application, continuous service availability, and complete transaction integrity.
vMotion has several options: regular vMotion, the Advanced Cross-vCenter vMotion, and Hybrid Cloud eXtension (HCX) which also uses vMotion logic. (see Workload Migration - HCX section below).
By enabling certain advanced configurations vMotion can be enabled across different vSphere Distributed Switch versions. Requirements include:

- **Connectivity between on-premises data centers and VMware Cloud on AWS using AWS Direct Connect (over Private VIF) and/or VMware NSX Layer 2 VPN**
- **On-premises vSphere version must be in support.**
- **Sustained bandwidth of 250 Mbps or more is required for optimal performance.**
- **No greater than 150ms of round-trip (RTT) latency.**

To help ensure success it is recommended that source environments be running the latest updates to that major vSphere version.

What are the different ways to orchestrate vMotion between on-premises and VMware Cloud on AWS?

Single VM vMotion:

- UI – Hybrid Linked Mode needs to be set-up for orchestrating vMotion via the HTML5 client.
- PowerCLI – Support via API directly with PowerCLI.

Bulk vMotion:

- UI – Hybrid Cloud Extension can enable bulk migration through UI.
- PowerCLI – Sample scripts here, to allow bulk migration scenarios.

Is encrypted vMotion supported from on-premises to VMware Cloud on AWS?

Yes, encrypted vMotion works out-of-box. No additional set-up action is required beyond the base vMotion requirements.

Can I vMotion from VMware Cloud on AWS back to on-premises?

Yes, you can vMotion from VMware Cloud on AWS back to on-premises as long as the on-premises hosts are compatible. Enhanced vMotion Compatability (EVC) mode does not work across clusters and there is a possibility that, while in VMware Cloud on AWS, the VM goes through a power cycle and begins running on a new hardware version in VMware Cloud on AWS. In such scenarios, the host on-premises might be on an older version and live migration will not be supported.

Is Enhanced vMotion Compatibility (EVC) setting available for VMware Cloud on AWS?

EVC is disabled in VMware Cloud on AWS. All hosts in VMware Cloud on AWS are homogeneous and hence a compatibility check is not required.

How is per-VM EVC different from cluster EVC?

As the name suggests, per-VM EVC abstracts this setting from a cluster to a VM level. By doing so, the EVC mode now can persist through a power cycle of the VM.

What are the requirements for per-VM EVC to work?

Per-VM EVC requires VM hardware version 14 or later. Per-VM EVC requires the VM to be powered off to enable the settings.

Can EVC setting be changed via UI or is it an API only feature?

Settings can be altered with both methods. There is an edit setting attribute at a per-VM level that can be changed to set the specific EVC mode. But it can also be automated and set for a batch of VMs via a script that uses the API.

How does per-VM EVC interact with cluster EVC while they co-exist?

Cluster EVC is not enabled in VMware Cloud on AWS. Only Per-VM EVC can be set.

Are all hosts in VMware Cloud on AWS homogeneous? How does per-VM EVC mode help there?

Yes, all hosts in VMware Cloud on AWS are homogeneous. The per-VM EVC setting comes into play when migrating back from VMware Cloud on AWS to on-premises to ensure there are no compatibility issues.

Workload Migration - HCX

What is VMware HCX?

VMware HCX is an offering that provides application mobility and infrastructure hybridity across different vSphere versions, on-premises and in the cloud. Learn more here

What does VMware HCX offer?

The VMware HCX service offers bi-directional application mobility and data center extension capabilities. VMware HCX includes vMotion, bulk migration, high throughput network extension, WAN optimization, traffic engineering, load balancing, automated VPN with strong encryption (Suite B) and secured data center interconnectivity with built-in hybrid abstraction and hybrid interconnects. VMware HCX enables cloud onboarding without retrofitting source infrastructure, supporting migration from any vSphere version with production support to VMware Cloud on AWS without introducing application risk and complex migration assessments. Learn more here

What is Infrastructure Hybridity?

VMware HCX abstracts vSphere-based on-premises and cloud resources and presents them to the applications as one continuous resource, creating infrastructure hybridity. At the core of this hybridity is a secure, encrypted, high throughput, WAN-optimized, load balanced and traffic engineered interconnect that provides network extension. This allows support for hybrid services, such as app mobility, on top of it. Apps are made oblivious to where they reside over this infrastructure hybridity, making them independent of the hardware and software underneath. Learn more here

What are usage scenarios for VMware HCX?

Here are few examples:

- Extend on-premises data centers to cloud
- Enable SDDC transformation
- Live and bulk VM migration
- Use ongoing hybridity for application landscape transparency and distributed app components.

Learn more here

Does VMware HCX support multisite interconnect? What are good usage scenarios of it?

Yes. VMware HCX supports multisite interconnect. Here are two example use cases:

- Consolidate small DCs to VMware Cloud on AWS
- Extend to multiple VMware Cloud on AWS with separate geo-locations.

Learn more here

Does VMware HCX support NSX SDDCs?

VMware HCX supports all capabilities in VMware NSX SDDCs. VMware NSX SDDCs also support the ability to leverage the Direct Connect Private VIF option for the VMware HCX interconnects. If you are leveraging the Internet and would like to shift your HCX interconnects to the Private VIF option, please reach out to VMware via support to get assistance in switching the interconnect configuration.

Does VMware HCX need VMware NSX on-premises?

It is not required if the destination environment is an HCX-enabled public cloud. NSX is needed if the destination vSphere environment is also private/on-premises. Optionally, NSX can be installed in the source environment to access the NSX Logical Switch Network Extension feature.

Where can I find pricing for VMware HCX for VMware Cloud on AWS?

VMware HCX is included with all VMware Cloud on AWS SDDCs.

How do I sign up for VMware HCX?

VMware HCX is included with your VMware Cloud on AWS subscription. To activate, login to VMware Cloud Services portal and enable HCX for your VMware Cloud on AWS SDDCs. VMware HCX is integrated with the vSphere Client so you can use the same management environment for day-to-day operations.

What is Cloud Motion with vSphere Replication?

Cloud Motion with vSphere Replication is a new and innovative way to enable mass migration of workloads from on-premises to VMware on AWS. With Cloud Motion with replication, you can migrate VMs at large scale with minimal or no downtime.

How is Cloud Motion with vSphere Replication different than existing HCX migration options?

Previously, there were two ways to migrate with HCX:

1. vMotion-based — vMotion based migration is live (no downtime) but is serial in nature. Due to vSphere concurrency and cross-cloud limitations, only a handful of VMs could be vMotioned. at the same time. While vMotion is a live migration option, it did not support large scale mobility
2. Warm migration — Warm migration is a large-scale migration where VMs can move at scale, but the migration needs a VM reboot.

Cloud Motion with vSphere Replication combines the best of both worlds. VMs are replicated to the destination using replication technology, and once the VMs are replicated, the final migration is done via vMotion. This enables large scale migration without the need for reboot. This feature lets you move applications at scale live, without any reboot or reload.

How can Cloud Motion with vSphere Replication help with cloud migrations?

Cloud motion with replication simplifies migration planning and operations in three ways:

- Traditionally, you would have to plan for a maintenance window wherein applications would be rebooted. Maintenance windows are fairly tedious to manage and maintain and there is additional complexity when dealing with application reloads/reboots. With Cloud Motion, migrations can be done at scale from source to VMware Cloud on AWS without scheduling any maintenance windows.

- Cloud Motion eliminates detailed analysis, dependency mappings and elongated migration planning projects.
- Cloud Motion lets you schedule the failover. This enables predictability as to when the application will migrate. In the case of vMotion, there is no predictability since the VMs would move as soon as the vMotion related activities were done. The combination of live migrations at scale with a predictable schedule brings in a paradigm shift in the migration process planning and operations.

What on-premises versions of vSphere are supported with Cloud Motion with vSphere Replication?

This feature requires a vSphere version that is supported on-premises. See the Product Lifecycle Matrix for more information.

How do I get more information about VMware HCX?

Learn more here. Try the Hands-on-Lab for VMware HCX.

When should I change my VMware HCX FQDN resolution to private?

You can choose to use HCX over the internet or using private network connectivity such as AWS Direct Connect. When using private connectivity, private IP address resolution is required.

How Can I change my HCX FQDN resolution?

For instructions, please refer to the VMware Cloud on AWS documentation

Compute

Is this service running nested virtualization?

No, ESXi is running directly on bare-metal AWS infrastructure. There is no nested virtualization.

How can I on-board virtual machines to my SDDC on VMware Cloud on AWS?

There are numerous ways to bring VMs and templates into a VMware Cloud on AWS SDDC, including:

- **Build new templates and redeploy**
- **Publish vSphere Content Libraries with Templates/OVF/OVA/ISOs, subscribe the SDDC**
- **Import templates and VMs as OVF/OVA**
- **Cold vMotion (powered off VM)**
- **Cross-vCenter vMotion**
- **VMware HCX (cloud migration and related methods)**

Tools such as PowerCLI can help automate creation and deployment of workloads wherever you wish to run them.

How can VM template support in VMware Cloud on AWS Content Library help me?

VM templates enable consistency and ease of VM content management. You can add a VM template to Content Library, delete it, rename it, update notes, or create a new VM from it.more

What can I not do with a VM template in Content Library?

You can't add a VM template into a published library, because the synchronization (data distribution) between Published and Subscribed libraries for VM templates is not supported yet. Also, you can't convert a VM template into a VM via Content Libraries; however, the same template with all capabilities is available for you in VMware vCenter Server Inventory/Folders.

How many ESXi hosts do I need (minimum) in VMware Cloud on AWS?

The minimum size SDDC that you can create in VMware Cloud on AWS is singlehost environment with the Single Host SDDC option. However, singlehost SDDCs do not offer anSLA, are limited lifespan (60 days), and are not intended for production use. For more details, refer to the Single Host SDDC FAQ section above.
2-Host Clusters are the smallest production SDDC configurations that are fully supported and offer an SLA

Is there any functional difference between a three host and a four host SDDC?

Yes. With three hosts you cannot implement a "RAID 5" storage policy based management (SPBM) policy. That requires a minimum of four hosts. The only storage redundancy available with 3 hosts is RAID 1.

Can I add a cluster to an existing SDDC?

Yes. Each SDDC can scale to 20 clusters.

What is the maximum supported cluster size in VMware Cloud on AWS?

The maximum cluster size is 16 ESXi hosts.

Can I increase or decrease the size of my cluster after I provision an SDDC on VMware Cloud on AWS?

Yes. You can add additional hosts on-demand or you can use EDRS to automatically scale-out hosts. You can also remove hosts on-demand or let EDRS scale-down automatically. Scaling down depends on multiple factors including storage availability policies and storage consumption below 80%.Learn more in the “Elastic DRS” section below.What is the maximum number of clusters supported?

VMware Cloud on AWS supports a maximum of 20 clusters per SDDC and each cluster supports up to 16 hosts. There fore each SDDC supporrts upwards of 320 hosts. Your organization may have lower cluster "soft" limits set. If you wish to have your limits raised, please contact the VMware support team. If you need to scale beyond a single SDDC, you can create multiple SDDCs

With multi-cluster support, how do I move VM's to the new cluster?

Once the new cluster is provisioned, you can cold migrate or vMotion VMs to this cluster via vCenter the same way you would move VMs on premises.

With multi-cluster support, can I remove the original cluster created when the SDDC was created?

No. Only additional clusters can be removed. You must have one cluster in your SDDC and this cluster must be the original cluster deployed when the SDDC was created. THis is because the management components including vCenter and NSX Manager, among others, reside on the original cluster.

Can a customer create multiple SDDCs?

In VMware Cloud on AWS, you can provision multiple SDDCs and can connect to multiple AWS accounts.

Can the SDDCs reside in different regions?

Yes, the SDDCs can reside in any region where VMware Cloud on AWS is available.

Do I have to connect all my SDDCs to an AWS account?

Yes. A VMware Cloud on AWS SDDC must be connected to an AWS account. It is possible to defer account linking for Single Host SDDCs for up to 14 days, but it is not possible to scale-up your Single Host SDDC without connecting to an AWS account.

What are the benefits of connecting to an AWS account?

Establishing a connection to an AWS account creates a high-bandwidth, low-latency connection between your SDDC and your AWS resources, and allows consuming AWS services with no cross-AZ charges. By delaying account linking, you will not be able to choose which availability zone (AZ) your SDDC will be deployed in.

How do I connect my SDDC to an AWS account?

When creating your SDDC, select Connect to a New AWS Account from the Choose an AWS Account drop down in step number one of creating an SDDC.

Can I connect SDDCs from different Organizations to the same AWS account?

This is not supported.

How do I provision an SDDC in a newly available region?

Select the newly available region when creating your SDDC. It is that simple. You can provision an SDDC in a newly available region in a similar manner to the way you provision an SDDC in other available regions. The region selector will now have another option for the new region. The SDDCs you create in the new region will appear on your dashboard along with your other SDDCs. Further, you can deploy, view, and manage, SDDCs from different regions together in the VMC Console

Do I need to access region specific endpoints to access my SDDCs?

No, you use the same endpoints to access the VMware Cloud on AWS API and VMware Cloud on AWS Console regardless of the region your SDDCs are in.

Which version of VMware ESXi is available on VMware Cloud on AWS?

The version of ESXi running on VMware Cloud on AWS is optimized for cloud operations and is compatible with the standard vSphere releases. ESXi running on VMware Cloud on AWS may have a more frequent update cadence so that you can take advantage of regular service enhancements . For more information on versions see Correlating VMware Cloud on AWS SDDC Versions With Their vSphere Components.

Can I choose the version of VMware ESXi running in my VMware Cloud on AWS SDDC?

Not directly. Versions of ESXi follow the SDDC versions your organization is configured to deploy. You can view the SDDC version in the Support information for that SDDC and then correlate SDDC versions to vSphere component versions.

Can I run nested ESXi VMs on VMware Cloud on AWS for testing and training purposes?

VMware does not support nested ESXi VMs running on VMware Cloud on AWS.

Can I use the vCenter Server in my SDDC to manage my on-premises ESXi hosts?

Through Hybrid Linked Mode, you can connect your VMware vCenter Server running in VMware Cloud on AWS to your on-premises VMware vCenter Server to get a single inventory view of both your cloud and on-premises resources.
The SDDC vCenter Server cannot be used to directly manage non-SDDC hosts.

What is Compute Policy?

Compute Policy is a new framework to allow you the flexibility, control, and policy-based automation required to keep up with the demands of your business. You can configure simple VM-Host affinity and anti-affinity, as well as disable DRS vMotion.

How does Compute Policy differ from DRS rules?

DRS operates at the cluster level.As the environment grows (number of clusters, hosts, VMs), it becomes difficult to manage, replicate and update the static rules (laid down in the beginning). Similarly, the intent (the why and what) for which the rules were created is lost over a period of time. To get around this, Compute Policy provides a higher level of abstraction to capture the customer intent at a SDDC level rather than at a cluster level at which DRS operates. As a result, a single policy can apply to multiple clusters within the SDDC at the same time. It aims to provide a framework to not only allow placement and load balancing decisions for VMs, but also to handle entire workloads.

What is the difference between a mandatory or preferential policy?

Mandatory policies are equivalent to the DRS “must” rules, while preferential policies are similar to the DRS “should” rules. Preferential policies cannot block a host from entering into maintenance mode. However, a policy cannot be violated for fixing cluster imbalance or host over-utilization.

Is VM-Host Affinity a mandatory or preferential policy?

Mandatory policies are not available in a VMware Cloud on AWS environment. As a result, VM-Host affinity is a preferential policy.

What if I delete tags?

If tags associated with a policy are deleted, the policy is no longer in effect, and is deleted.

How many policies can I create?

Compute Policy can support a total of 100 policies per SDDC.

Are some policies preferred over others?

No. All defined policies (except Disable DRS vMotion) are treated the same, and no one policy is preferred over the other. As a result, one policy cannot be violated to remediate another.

How are the interactions between the various policies handled?

In the current implementation there is no conflict detection. This means that if a user configures two policies that conflict with each other, no user error or warning will be generated. DRS will enforce all the policies in the best manner it can, as described below.

Can I choose the AZ in which my VMs run with VM-Host Affinity?

Yes. When defining a VM-Host affinity policy, you can select hosts tagged with the required Availability Zone.

Can I use the VM-Host affinity policy to address my software licensing needs?

VM-Host affinity is a preferential policy. Please discuss with your ISV vendor whether preferential policies are acceptable as per the terms of your licensing agreements.

Are there any scenarios where a VM may not run on a designated host?

In VMware Cloud on AWS, the Virtual Machine power status, maintenance and availability have a higher priority over policy enforcement, and policy enforcement has a higher priority over host utilization. As a result, there are scenarios where a VM may not run on a designated host. For example: If a host goes down due to any failure, and if HA is enabled, the recovering VM may get restarted on any available host in the cluster.

Similarly, if reservations are used, and if a compliant host cannot satisfy a VM's reservations, the VM will get started on any available (even non-compliant) host that can satisfy the reservation.

If there is no compliant host (i.e. if no host has the Host-tag specified by the policy), the VM will be started on any available host.

If the user configures multiple VM-Host affinity policies that are conflicting, the policies will be ignored and the VM shall be started on a suitable host chosen by DRS. In such cases, Compute Policy will keep trying to move the VMs back to the compliant hosts.

How does the VM-VM Anti-Affinity policy work?

Enforcing a VM-VM anti-affinity policy implies that DRS will try to ensure that it keeps each VM (that has the policy's VM tag) on different hosts. This anti-affinity relation between the VMs will be considered by DRS during VM power-on, host maintenance mode and load balancing. If a VM is involved in a VM-VM anti-affinity policy, then DRS will always prefer those candidate hosts which do not have any powered-on VM that has the policy's VM tag.

Are there any scenarios in which the VM-VM Anti-Affinity policy may not be enforced?

One scenario is when any provisioning operation issued by its corresponding API call specifies a destination host is allowed to violate a policy. However, DRS will try to move the VM in a subsequent remediation cycle. If it is not possible to place a VM as per its VM-VM anti-affinity policies, then the policy is dropped and the operation (power-on or host enter MM) continues. This means that first DRS tries to place the VM such that policy can be satisfied, but if that is not possible then DRS will continue to find the best host per other factors, even if it violates the policy. Other scenarios where VMs may not be placed as per the policy could be:

- Every host in the cluster has at least one VM with the tag specified by VM-VM anti-affinity policy.
- None of the policy preferred host can satisfy VM's CPU/memory/vNIC reservation requirements.

What is the behavior if there are more VMs than available hosts in an anti-affinity rule?

DRS will first try to place as many VMs on different hosts as possible, which in this case will be equal to the number of hosts available in the cluster. After that, the policy shall not be enforced, i.e. the remaining VMs will be placed based on the other factors DRS, which may result in multiple VMs on the same host. To remedy this violation, additional hosts can be added to the cluster. Once the hosts are added, DRS will move the VMs that are violating the policy to the newly added hosts.

How does the VM-VM Affinity policy work?

Enforcing a VM-VM affinity policy means that DRS will try to ensure that it keeps each VM that has the policy's VM tag on the same host. This affinity relation between the VMs will be considered by DRS during VM power-on, host maintenance mode and load balancing.

How does the Disable DRS vMotion policy work?

This policy indicates that DRS would not migrate or load balance a virtual machine away from the host on which it was powered-on, except for the case when the host is being put into maintenance mode. This policy can be useful for applications that may be sensitive to vMotion, such as large transactional databases. The VMs subjected to this policy are identified using vSphere tags, and this policy is not applicable for a power-on operation. However, once a VM is powered on, and is subjected to this policy, it will not be moved to remediate a VM-Host affinity or VM-VM Anti-affinity policy.

Can I create my own custom roles in the vCenter running in VMware Cloud on AWS?

Yes, you can create custom roles in addition to the CloudAdmin role that is provided out of the box. Users that have the Authorization.ModifyRoles privilege can create/update/delete roles. Users with the Authorization.ModifyPermissions privilege can assign roles to users/groups.

Are users able to modify other vCenter roles as well, or only roles that they've created?

Users will only be able to modify or delete any roles that have lesser than or equal to the privileges of their current role.

Can I view management objects?

Yes, you can only view management objects. You can assign the read only role to the management objects for other users and groups as well.

What is a Partition Placement Group?

Partition Placement Groups (PPG) are AWS contructs that VMware Cloud on AWS is able to use due VMware’s joint-engineering efforts with AWS. Essentially PPGs attempt to place hosts in a given cluster across logical partitions, typically racks or sets of racks, in AWS data centers. This is an instance placement strategy that helps reduce the likelihood of co-related host failures due to hardware failures. PPGs increase availability of applications by placing hosts in different logical partitions that do not share the same underlying hardware. Partition placement groups follow a “best effort” algorithm to automatically deploy hosts across as many different partitions as there are available within an AZ. Each partition within a placement group has its own set of racks, and each rack has its own network and power source. No two partitions within a placement group share the same racks, which allows for isolating host failures within an SDDC cluster. VMware Cloud on AWS automatically enables Partition Placement groups for new SDDC, cluster and host provisioning operations.

With partition placement groups automatically enabled, what happens when a host is removed or replaced?

When a host is removed, the preference is to remove a host that is not inside a partition; new hosts are added into partitions whenever possible. In this way, SDDCs will benefit from more partitions over time.

How can I view partitions for my SDDC?

Partition placement is not configurable or viewable by customers.

Will there be in-cluster conversion from existing i3/i3en cluster to i4i?

Yes, VMware will provide an in-cluster conversion service for qualified clusters in the upcoming releases. Details of in-cluster conversion are available here.

Custom Core Count

Does VMC on AWS support Custom core counts?

Yes. Custom cores are only supported on physical cores. The custom core counts supported will depend on each host type. See Custom CPU Core Count for more information and host specific capabilities. Can I use custom core counts in the primary cluster?

No, custom core counts are not supported in the primary cluster due to the need for cores to run management VMs.

Can I use custom core counts in the secondary (workload) cluster?

Yes. However, the number of custom core counts supported in the secondary cluster depends on the size of the secondary cluster. For a 2-node secondary cluster, the custom core counts supported will be from 16 and above. For a 3-host and above secondary cluster, the custom core counts outlined in the table above are supported.

How do I use Custom CPU Core Count feature?

Go to the VMware Cloud on AWS Console, click on your SDDC, and select Add Cluster. Under the section “Cluster to Be Added” you will see that you can specify the Number of CPU Cores Per Host. Select the value that works best for your workloads and finish the action

What are the current limitations of Custom CPU Core Count capability?

Cluster-0 must have all cores enabled, and this is an at "Add Cluster" deployment time decision only. Core Count cannot be changed after deployment except by deleting and redeploying an SDDC. All hosts in the cluster must have the same number of CPU cores, including Add/Remove Host operations.

Do I get a price discount on the hosts with lower CPU core count?

No, changing the number of cores does not affect the price of the host.

How do I control my licensing, while leveraging Custom CPU Core Count capability?

To preserve the number of licensed CPU cores, it is highly recommended that you leverage VMware Cloud on AWS Compute Policies (Simple VM-Host Affinity) to tag all applicable VMs and all the original hosts in the cluster, so that the compute policy can keep these VMs on those hosts. During regular VMware Cloud on AWS patch and upgrade operations, an additional host is added to a cluster. Therefore, you may need to include the license for this additional host in your initial licensing contract, making it N+1 since day one.

When I specify the lower number of CPU cores, does it impact the performance?

Reducing core count affects the compute capacity of the hosts, which may affect overall performance for both workloads and internal vSphere, NSX, and vSAN processes that execute on the hosts.

Where can I find more information about Custom Core Count?

Check the VMware Cloud Tech Zone article for more information about the feature.

Stretched Clusters

What are Stretched Clusters for VMware Cloud on AWS?

Stretched clusters facilitate zero RPO infrastructure availability for applications. This enables you to failover workloads within clusters spanning two AWS Availability Zones (Availability Zones). It also enables developers to focus on core application requirements and capabilities, instead of infrastructure availability. With this feature, you can deploy a single SDDC across two Availability Zones. Using the vSAN Stretched Cluster feature, it allows us to guarantee synchronous writes across two Availability Zones in a single SDDC cluster. This feature also extends workload logical networks to support vMotion between Availability Zones. In the case of an Availability Zone failure, vSphere HA will attempt to restart your VMs on the surviving Availability Zone.

How many AZs can I stretch my cluster across?

Two. When you provision your SDDC in the VMC Console you enable stretched clusters with a single check box and select the Availability Zones. The stretched cluster will be automatically deployed withinyour SDDC across these two Availability Zones.

Can I have more than one stretched cluster?

You can create multiple stretched clusters in an SDDC.

Can I create stretched clusters and non-stretched clusters in the same SDDC?

No. Cluster types cannot be mixed. An SDDC can only have stretched clusters or non-stretched clusters.

Can I convert a non-stretched cluster to a stretched cluster?

No. The decision to deploy a stretched or a non-stretched cluster is made when the SDDC is created and cannot be changed afterwards.

Is it possible to configure Custom CPU Core Count with multiple stretched clusters?

Yes. Custom CPU Core COuntcan be configured in an SDDC that has two or more stretched clusters. However, Custom CPU Core Count cannot be configured in the first stretched cluster.

What is the smallest stretched cluster I can make?

The smallest supported stretched cluster is two hosts, 1 in each AZ, and provides a 99.9% SLA. At six hosts, 3 in each AZ, the service increases the SLA to 99.99%.

Can I add hosts to a stretched cluster?

Yes. Just like a regular cluster, you can add and remove hosts at any time. However, in a stretched cluster these hosts must be added and removed in pairs. You must have the same number of hosts on each side at all times. Thus, you can grow a cluster from 6 to 8, 10, 12, etc.

What is the largest stretched cluster that would be supported?

We support cluster sizes of up to 16 hosts.

What about the witness?

In addition to the hosts you request, we always provision one additional ESXi host for stretched clusters to act as a witness node. This is to prevent issues such as split brain in the case of a network partition. You will see this host in the UI, but it will not be a member of the cluster and you cannot run guest VM's on that host. This host is a special version of ESXi that runs as a guest. This allows us to charge less for the service since the witness ESXi does not consume an entire physical host.

Are stretched clusters a good way to implement Disaster Recovery?

No. Stretched clusters improve availability within an AWS region but are not intended for DR. AWS regions are composed of multiple AZs in a geographic area.. A disaster affecting a geographical area could take out multipleAZs in an AWS region.If you wish to protect against a regional failure, please consider a DR solution such as VMware Cloud Live Recovery - more information below.

Do you support ESXi as a guest now?

No. The witness host VM is a special case and does not run guest workloads.

Can I downgrade a stretched cluster SDDC to a single AZ SDDC?

No. Enabling stretched cluster is a deployment time decision. You cannot downgrade a stretched cluster to a non-stretched cluster. You can deploy a new cluster and use vMotion or other migration techniques to move to it.

Can I migrate workloads from a single AZ cluster to a stretched cluster?

Yes, using your preferred workload migration method.

Can I choose the AZ in which my VMs run?

Yes. When deploying a VM you can choose a VMware ESXi host in the desired Availability Zone. In case of failure, the VM will stay in its original Availability Zone if possible. You can also enforce the VM placement using Compute Policies.

Can a stretched cluster span across AWS regions?

No. A stretched cluster spans across 2 AZs within the same AWS region. If you wish to protect against a regional failure, please use a DR tool such as VMware Cloud Live Recovery.

Is there a performance impact when running VMs in a stretched cluster?

Yes. As with any stretched cluster or synchronous mirroring deployment, writes across two Availability Zones will incur additional latency overhead.

How many failures can be tolerated in an AZ using a stretched cluster?

This depends on your SPBM settings. By default, VMs are configured to survive the failure of all the hosts in a single AZ without data loss.

What happens when an AZ fails and when it comes back after a failure when using a stretched cluster?

The servicewill re-synchronize the vSAN datastore. This resync time will depend on how much data you have stored and how long the systems have been segmented. This operation is automatic and monitored by our operations team. You can learn more on Tech Zone.

How much does it cost to run Stretched Clusters?

There are no additional charges to use the Stretched Clusters feature. Stretched Clusters Cross-AZ traffic charges are also waived for up to 10 petabytes per month. Usage will be monitored and for instances where a customer's usage exceeds this limit, VMware reserves the right to inform the customer of the issue and charge the full amount.

What instance types are supported with the ability to create multiple stretched clusters?

Currently host types using vSAN are supported, host types requiring external storage are not. See Stretched Clusters for VMware Cloud on AWS for more information.

Can I mix Stretched Clusters using different host types in the same SDDC?

Yes.

Can I have mix of different host types within the same Stretched Cluster?

No, a single Stretched Cluster can only consist of hosts of the same instance type.

Elastic DRS

What is Elastic DRS (EDRS)?

Elastic DRS (EDRS) is a feature that uses the resource management features of vSphere to analyze the load running in your SDDC to scale your clusters up or down. Using this feature, you can enable VMware Cloud on AWS to manage your cluster sizes without manual intervention.

When will EDRS scale up?

EDRS will automatically scale up when your cluster reaches a capacity threshold, based on policies you set and the EDRS Baseline Policy

What is the Elastic DRS baseline policy ?

Elastic DRS Baseline Policy is automatically configured for every cluster deployed within your SDDC to protect the cluster from running out of storage capacity. The maximum usable capacity of your vSAN datastore is 80%; when that threshold is reached, EDRS will automatically start the process of adding a host to your cluster and expanding your vSAN datastore. Please note that even if you free up enough storage to fall below the threshold, the cluster will not scale-down automatically. You will need to manually remove host(s) from the cluster.

How quickly does EDRS scale my cluster?

It takes about 10-15 minutes to add a host to an existing cluster. EDRS will make a scaling recommendation approximately every five minutes.

Will EDRS scale my clusters down also?

Yes. When your cluster is lightly loaded, EDRS will also scale down automatically once you have configured EDRS scale-in policies.

How do I control my budget with EDRS?

When configuring EDRS, you configure the minimum and maximum allowed cluster size. EDRS will only scale within the limits you set.

Will EDRS just keep adding hosts? Are there any limits to that?

No, EDRS will not add hosts sequentially. EDRS is throttled to prevent runaway cluster scaling. The system is also monitored by our operations team to ensure that scale operations are conducted correctly.

What happens if I have an SPBM policy of RAID 6 set and EDRS tries to scale down to four hosts?

If you have an SPBM policy that requires a minimum number of hosts (such as RAID 6), EDRS will not scale down below that minimum number. To allow scale-down, reconfigure SPBM to use a policy without that restriction such as RAID 1.

How does EDRS affect my bill?

You are billed per host per hour on VMware Cloud on AWS. EDRS simply changes the number of hosts you have running in your SDDC. It is the same as if you manually added hosts to your SDDC.

Do my workloads get automatically re-balanced onto the new host?

Yes. DRS will automatically re-balance your workloads.

How long does a scale-down operation take?

This depends on how heavily loaded your host is. A lightly loaded host will take only a few minutes to remove from the cluster. A very heavily loaded host could take many hours. In the case of EDRS, we only remove hosts which are lightly loaded so we expect this operation to be on the lower end of this spectrum. However, your actual evacuation time largely depends on how many VMs are running and how much data must be evacuated from the host so your times will vary.

If I know that I am about to bring up many workloads suddenly, as in the case of a DR event, should I rely on EDRS?

No. Because EDRS is throttled, it's not designed for very sudden load spikes such as caused by a DR event. In this case, you should script the host addition process as part of your DR runbook. After the DR workload is started, you can rely on EDRS to maintain the correct number of hosts in your cluster.

Is EDRS turned on by default?

Elastic DRS (EDRS) is enabled by default and cannot be disabled in VMware Cloud on AWS. VMware has pre-configured Elastic DRS thresholds across all available policies to ensure SDDC availability. One of the Elastic DRS policies listed in Select Elastic DRS Policy is always active.

What is the scope of EDRS?

EDRS is enabled on a per-cluster basis.

Would I get notified when hosts are added to my SDDC automatically?

Yes, you will get notified via email and in-console notification once any cluster is within 5% of any storage scale-out event. You will also be notified immediately after any hosts are added.

What is EDRS Rapid Scale Out?

EDRS Rapid Scale-Out causes EDRS to react faster and to add hosts in parallel to allow a cluster to scale out more quickly during a DR event for VDI or other workloads.

How do I enable EDRS Rapid Scale Out?

EDRS Rapid Scale-Out is enabled through the UI as a new EDRS policy type or via the EDRS policy API.

What thresholds are used with EDRS Rapid Scale Out?

EDRS Rapid Scale Out maximum thresholds are the same as the thresholds for the EDRS performance policy. The minimum thresholds are 0%; this means scale-in must be performed manually.

How many hosts could be selected for EDRS scale out per cluster?

You can select 4,8 or 12-Hosts to be deployed in parallel.

What EDRS policies are supported with Stretched Clusters?

All EDRS policies - Cost, Performance and Rapid Scale Out - are supported with Stretched Clusters, in addition to the Storage-only default policy.

How does EDRS decide to scale out when capacity (Storage/CPU/Memory) exceeds a threshold in only one of the Availability Zones?

EDRS monitors utilization in each Availability Zone. A scale-out event is triggered when a threshold is exceeded in either Availability Zone. Scale-in, on the other hand, occurs only when utilization goes below the threshold in both Availability Zones.

Storage

What type of storage can I use with my SDDC on VMware Cloud on AWS?

VMware Cloud on AWS SDDC leverages VMware vSAN as a primary datastore. A single cluster-wide vSAN datastore is automatically configured for you when you deploy each cluster in your SDDC. In your first cluster, all management virtual machines are hosted on the vSAN datastore and cannot be moved. You can extend the storage capacity of a cluster by adding hosts or using external storage options such as VMware Cloud Flex Storage. Learn more about storage options here.

Can I use any hybrid vSAN storage (Flash + Spinning Disk)?

We currently do not offer a hybrid storage solution. All hosts are equipped with NVME SSD Storage.

Can I expand my storage without adding additional hosts?

Yes. VMware Cloud on AWS now offers support for external NFS datastores. Customers can use a VMware managed solution – VMware Cloud Flex Storage, or an AWS managed solution – Amazon FSx for NetAPP ONTAP as your external NFS datastore to extend storage capacity without adding additional hosts.

What vSAN policies can be configured?

The following subset of vSAN policies can be configured by the user:

Failures-To-Tolerate (FTT): Configured on a per vSAN Object basis.

- Customers have a choice of Fault Tolerance Methods (FTM) and Failures-To-Tolerate configurations for their VMs. To optimize for cost, performance & availability, it is recommended to use FTM = RAID 1 and FTT= 1 for 3-node cluster and FTM = RAID 5 (Erasure Coding) and FTT=1 for clusters of size 4 & 5 nodes and the FTM = RAID 6 and FTT=2 for clusters of size 6 nodes and higher.
- IOPS Limits: Limit IOPS consumption per VM to better manage performance SLAs for different workloads. Eliminates noisy neighbor Issues.
- Checksum: Enabled by default.
- Disk stripes: The number of disk stripes per object can be up to a maximum of 12, but may be limited by certain cluster configurations (FTT, FTM choices, number of nodes, etc.).
- Force provisioning: Enable provisioning of VMs even when the storage policy cannot be fully satisfied.

What is a storage policy and why is it important? How is “Managed Storage Policy” different?

Storage policies define levels of protection or performance for your VMs or VMDKs. Typically, a user manually sets a policy for one or more VMs and these are then managed by VMware vCenter Server. With Managed Storage Policy for improved data availability, we will automatically set the policy for you based on the number of nodes in your VMware Cloud on AWS cluster.

How does Managed Storage Policy benefit me?

VMware Cloud on AWS provides a 99.9% availability commitment as per the SLA for a standard SDDC. If an SLA event occurs i.e. a service component is unavailable, you will be eligible for SLA credits, provided that your cluster meets certain protection requirements that are set by storage policies. By allowing VMware Cloud on AWS to automatically set these policies for you, the criteria required to be eligible for these credits is already taken care of while ensuring that your clusters have the optimal level of protection.

If I add more hosts to a cluster and this increases the number of hosts beyond 5, will my policy change automatically with Automatic adjustment of vSAN policy feature?

Yes, we will automatically change the policy for your cluster

Can I manually override the function of Automatic adjustment of vSAN policy and set my own policy?

Yes, you can override this function of Automatic adjustment of vSAN policy and set your own policies.

What does the monitoring and alerting enhancement for managed storage policy do?

This feature scans a customers' environment for VMs and objects which have SLA non-compliant policies and notifies a VMware Cloud on AWS customers about the same. VMware Cloud on AWS customers will receive an email notification which contains details of all the non-compliant policies and which VMs/objects they are mapped to for their VMware Cloud on AWS ORG. Customers will also be able to view the entire list of VMs with non-compliant policies within the VMware Cloud console and will be able to move to a managed storage policy with the click of a single button.

What does SLA compliant/non-compliant policies mean?

SLA compliance is required to ensure that your workloads are protected and that you are eligible for credits should a failure occur (Click here to learn more about the VMware Cloud on AWS SLA). SLA compliant policies are policies which follow the VMware Cloud on AWS SLA guidance and non-compliant policies are policies which are different from what is stated in the VMware Cloud on AWS SLA document.

How will I be notified about SLA non-compliant policies?

You will be notified via email about which VMs have non-compliant policies. The email will include a link which re-directs you to the VMware Cloud console where you can view the entire list of VMs and objects with SLA non-compliant policies for your ORG.

How frequently is the scan performed and how often will I be notified?

The scan is performed daily and if there are new non-compliant policies, you will only be notified about these policies. Previously notified non-compliant policies will not be included in an email but they will be listed in the inventory view if they haven't been remediated.

Do I have to remediate all the VMs?

No. In the VMware Cloud console inventory view, you will have the option to select which VMs you want to change to a compliant policy. You will have the option to either select specific VMs you want to remediate or remediate the entire inventory. VMs that have not been moved to a SLA compliant policy will remain in the inventory.

Can I mute the notifications?

Yes. You can use NGW to mute the emails notifications. There will be tiles within each cluster window to indicate which clusters have non-compliant policies.

How does Compression work in VMware Cloud on AWS?

The compression algorithm is applied after deduplication has occurred, but before the data is written to the capacity tier. To avoid the inefficient use of compute resources for the allocation map overhead of compression, vSAN only stores compressed data if a unique 4K block can be reduced to 2K or less. Otherwise, the block is written uncompressed.

vSAN Compression is available on all host types with integrated storage. Deduplication is only active on i3 hosts.

Deduplication removes redundant data blocks, whereas compression removes additional redundant data within each data block. These techniques work together to reduce the amount of physical storage required to store the data. VMware vSAN applies deduplication followed by compression as it moves data from the cache tier to the capacity tier.

Deduplication occurs inline when data is destaged from the cache tier to the capacity tier. The deduplication algorithm utilizes a 4K-fixed block size to provide a good balance of efficiency and performance and is performed within each disk group. Redundant copies of a block within the same disk group are reduced to one copy, but redundant blocks across multiple disk groups are not deduplicated.

How much storage is saved with the Compression feature in VMware Cloud on AWS?

Storage savings resulting from Compression and Deduplication is highly dependent on the workload data. For example:

Operating system files across multiple virtual machines experience great benefit from Deduplication VDI workloads obtain good Deduplication savings.
Video files do not compress well.

Although some customers using vSAN on-premises report savings up to 7x for VDI workloads, we generally see storage savings on the average of 2x based on the current deployments.

Can I apply Compression selectively for each volume?

No, deduplication or compression cannot be enabled individually, it is a cluster-wide setting. Also, all the vSAN datastores in VMware Cloud on AWS are automatically enabled for Compression without any user configuration and cannot be turned off. In addition, all vSAN datastores in i3.metal clusters are enabled for Deduplication.

Is there a performance impact due to Deduplication and Compression?

Although vSAN Deduplication & Compression are very efficient, users may experience some impact. For most workloads the impact is minimal.

Does Deduplication and Compression work with vSAN Encryption?

Yes. vSAN encrypts all data at rest both in the caching and capacity tiers, while preserving the storage efficiencies from deduplication and compression.

How does data encryption at rest work on VMware Cloud on AWS?

Customer data at rest is natively encrypted by vSAN. vSAN uses the AWS Key Management Service to generate the Customer Master Key (CMK). While CMK is acquired from AWS, two additional keys are generated by vSAN. Those keys are an intermediate key, referred as Key Encryption Key (KEK) and Disk Encryption Key (DEK).

The Customer Master Key (CMK) wraps the Key Encryption Key (KEK) and the KEK in turn wraps the Disk Encryption Key (DEK). The CMK never leaves AWS control, and encryption and decryption of the Key Encryption (KEK) is offered via an standard AWS API call.

One Customer Master Key (CMK) and Key Encryption Key (KEK) is required per cluster and one Disk Encryption Key (DEK) for every disk in the cluster.

Can I turn on or turn off vSAN Encryption selectively?

vSAN Data-at-Rest Encryption is on by default for all SDDCs and cannot be deactivated.

How does data-at-rest encryption work in VMware Cloud on AWS?

All customer data at rest will be natively encrypted by vSAN. vSAN will use AWS Key Management Service to generate the Customer Master Key (CMK). While CMK is acquired from AWS, two additional keys are generated by vSAN. Those keys are an intermediate key, referred as Key Encryption Key (KEK) and Disk Encryption Key (DEK). The Customer Master Key (CMK) wraps the Key Encryption Key (KEK), and the Key Encryption Key (KEK) in turn wraps the Disk Encryption Key (DEK). The CMK never leaves AWS control. Encryption and decryption of the Key Encryption Key (KEK) is offered via standard AWS API call. One Customer Master Key (CMK) and one Key Encryption Key (KEK) is required per cluster and one Disk Encryption Key (DEK) is required for every disk in the cluster.

Is there any performance impact because of encryption?

There is always overhead from use of encryption, but the effect on workloads tends to be minimal for environments adequately sized for CPU and I/O. vSAN encryption uses an efficient AES-XTS-256 cipher and leverages CPU-based AES-NI cryptographic instructions for performance.

What provisions are available to rotate the keys used for data at rest encryption in VMware Cloud on AWS?

Customers have the option to change the KEK (Key Encryption Key) either through vSAN API or through the vSphere UI. This process is called shallow rekey. Note, shallow rekey doesn’t change the Disk Encryption Key (DEK) or the Customer Master Key (CMK). Changing the Disk Encryption Key (DEK) and Customer Master Key (CMK) is not supported. In rare situations, if there is a need to change the DEK or CMK, users have the option to set up a new cluster with new CMK and storage vMotion the data from the existing cluster.

Are there any other options for customers to bring their own keys for data at rest encryption?

The Customer Master Key (CMK) is only sourced from the AWS Key Management Service.

Why does vSAN require “slack space?”

Like any storage system, vSAN uses unused, or “slack,” space to maintain the health of the system. This space is used for rebalancing capacity, deduplication, and for recovering from hardware failures.

How are slack space requirements enforced if I turn on EDRS?

EDRS is aware of vSAN and VMware ESXi capacity requirements and will automatically add or remove hosts to be certain that your SDDC remains healthy. EDRS is the best way to ensure that your SDDC is always sized correctly.

Are data compression and deduplication capabilities available on I3en.metal instances?

Compression is available on I3en bare metal instances. Deduplication will not be supported in I3en instances.

What are the policy settings which will be set by Automatic adjustment of vSAN policy for improved data availability?

For Standard Cluster:
=< 5 hosts: Failure to tolerate 1 - Raid-1 >= 6 hosts: Failure to tolerate 2 - Raid-6

For Stretched Cluster:
Dual Site Mirroring, Failure to tolerate 1– Raid-1

What is TRIM/UNMAP?

TRIM/UNMAP is a vSAN feature that allows the guest OS to issue TRIM/UNMAP commands so that vSAN can remove unused blocks inside virtual machines. This benefits thin-provisioned VMDKs as unused blocks can be reclaimed automatically and delivers much better storage capacity utilization.

How does the TRIM/UNMAP feature work?

The guest OS will issue these commands and will continue to run in the background until all the unused blocks are reclaimed.

What benefit do I get from enabling the TRIM/UNMAP feature?

This process carries benefits of freeing up storage space but also has other secondary benefits:

Faster repair - Blocks that have been reclaimed do not need to be rebalanced, or re-mirrored in the event of a device failure.
Removal of dirty cache pages - Read Cache can be freed up in the DRAM client Cache

How is the TRIM/UNMAP feature enabled for my SDDC?

As this feature is being released as a preview, we will enable the feature on a per cluster basis, based on your preference. Please contact your account team to have this feature enabled for your cluster.

What is the performance impact of TRIM/UNMAP feature?

This process does carry some performance impact. It is recommended that TRIM/UNMAP processes be triggered periodically inside the guest OS, versus running continuously.

TRIM/UNMAP operations will be throttled in the SDDC if they consume more than a predefined amount of storage bandwidth capacity.

What is Cloud Native Storage?

Cloud Native Storage (CNS) is a VMware Cloud on AWS and Kubernetes (K8s) feature that makes K8s aware of how to provision storage on VMware Cloud on-demand in a fully automated, scalable fashion as well as providing visibility for the administrator into container volumes through the CNS UI within VMware vCenter Server. Cloud Native Storage on VMware Cloud is supported with TKG and TKG Plus.

How does Cloud Native Storage work?

Cloud Native Storage (CNS) comprises of two parts: A Container Storage Interface (CSI) plugin for K8s and the CNS Control Plane within VMware vCenter Server. There is nothing to install or configure within the service to get this integration working. Simply deploy Kubernetes with the vSphere CSI.

Are data compression and deduplication capabilities available on I4i.metal instances?

Compression is available on I4i bare metal instances. Deduplication is not supported in I4i instances.

How much vSAN storage comes with VMware Cloud on AWS with different host types?

With the I3.metal host instance, each VMware ESXi host comes with NVMe SSD storage. A 3 VMware ESXi host cluster running vSAN provides approximately 15 TiB usable storage and 4 VMware ESXi host cluster running vSAN provides approximately 21 TiB usable storage, with all virtual machines protected against a single host failure (FTT=1). With the I3en.metal host instance, each VMware ESXi host comes with NVMe SSD Storage as well. A 3 host VMware ESXi cluster running vSAN provides approximately 60 TiB of usable storage. The newly-launched I4i.metal instance provides approximately 30 TiB of raw local NVMe flash storage across a 3 node cluster (2x compared to I3.metal). Please note that exact usable storage will vary depending on the effective storage policy, cluster size, site tolerance. All virtual machines are protected against a single host failure (FTT=1). In addition, you can also use external NFS datastores with your VMware Cloud on AWS deployment with all host types to extend your storage capacity for more storage intensive workloads, without provisioning additional hosts.

How much external storage can I have on an SDDC?

When you are using an external NFS datastore you can configure the volume size up to the configuration limit of the NFS server. Please consult VMware Flex Storage FAQs and Amazon FSx for NetAPP ONTAP FAQs for more details.

Can I still use vSAN storage in an SDDC that has external NFS datastores?

Yes. The VMware Cloud on AWS vSAN local storage is still available when external storage is attached.

What are the use cases that are suitable for external storage access from a VMware Cloud on AWS based guest operating system?

In addition to the ability to mount an external NFS datastore to a vSphere cluster in your SDDC, you can also directly add external storage to a virtual machine, running on VMware Cloud on AWS. Storage provided from an EC2 based virtual storage array to a VMware Cloud on AWS guest OS is ideal for a variety of use cases, including test and development, elasticity for big data workloads and user/home directories. Both block and file protocols are supported.

What external virtual storage arrays are supported on VMware Cloud on AWS?

VMware Cloud on AWS now supports external NFS datastores such as the VMware-managed – VMware Cloud Flex Storage, or an AWS managed solution – Amazon FSx for NetAPP ONTAP to extend storage capacity without adding additional hosts. VMware Cloud on AWS can also support a variety of AWS EC2 based virtual storage arrays and general-purpose operating systems that export storage volumes or LUNs. Our storage partners will independently test and provide documentation for their respective solutions.

Which Managed Service Providers (MSPs) offer external storage with VMware Cloud on AWS?

Faction and Rackspace are currently supported Managed Service Providers (MSPs) that offer external storage for VMware Cloud on AWS.

Are there any functional differences or caveats I should be aware of when using external storage through the Managed Service Provider (MSP)?

Please check the VMware Cloud on AWS release notes for a list of caveats and limitations related to the usage of external storage through the Managed Service Provider (MSP). Also, please check with the Managed Service Provider (MSP) for additional details.

Can I storage vMotion workloads between NFS Datastore and the VMware Cloud vSAN datastore?

Yes. Storage vMotion is supported.

How many external datastores can I attach to a single cluster in my SDDC?

Each cluster can have up to four datastores attached. The size of the datastore depends on the storage target.

What is the minimum software version of VMware Cloud on AWS SDDC to support the external NFS datastore feature?

Your SDDC must be version 1.20 or above to use the external NFS datastore feature.

Where can I find more information about the external NFS datastore support?

For further technical information about VMware Cloud on AWS integration with Amazon FSx for NetApp ONTAP please visit the page: https://vmc.techzone.vmware.com/fsx-ontap and check FAQ: https://vmc.techzone.vmware.com/fsx-ontap-faq.

Storage – Cloud Flex Storage

What is VMware Cloud Flex Storage?

Our vision for VMware Cloud Flex Storage is to deliver an enterprise-class storage-and data management-as-a-service for the multi-cloud. We plan to support a broad range of workloads by enabling multi-dimensional scaling of compute, storage performance, and storage capacity, while delivering a seamless and consistent data management experience across clouds.

VMware Cloud Flex Storage is built on a mature, enterprise-class filesystem that has been developed and production-hardened over many years, dating back to Datrium’s D¬HCI storage product, which VMware acquired in July 2020. It is the same filesystem that has been backing the VMware Cloud Disaster Recovery service. The filesystem has a two-tier design that allows for independent scaling of storage performance and capacity, using a Log-Structure Filesystem (LFS) design. The combination of LFS with a 2-tier design, along with efficient snapshots and immutability, makes this a multi-purpose filesystem that unlocks many use cases, such as backup, disaster recovery, ransomware protection, and recovery. With VMware Cloud Flex Storage, we are extending this proven technology to primary storage and making it available in the public cloud, where it delivers exceptional storage performance, scalability, and cost efficiency for traditional and modern workloads.

In the initial release, we are delivering a new approach to help VMware Cloud on AWS customers better align their cloud resources with the needs of their applications and data. Customers will be able to purchase a disaggregated cloud storage and data management service that if fully managed by VMware. It is scalable, elastic, and natively integrated into VMware Cloud on AWS. With just a few clicks in the VMware Cloud Console, customers can scale their storage environment without adding hosts, and elastically adjust their storage capacity up or down as needed for every application. Customers also benefit from a simple pay-as-you-go consumption model. We are offering VMware Cloud Flex Storage as supplemental storage to vSAN. Together with vSAN, VMware Cloud Flex Storage offers more flexibility and customer value in terms of resilience, performance, scale, and cost In the cloud.

Is VMware Cloud Flex Storage managed by VMware?

Yes, the service is fully managed by VMware.

In which AWS regions is VMware Cloud Flex Storage available?

At launch, VMware Cloud Flex Storage will be available in AMER, EMEA and LATAM. APAC support is expected in subsequent release. VMware Cloud Flex Storage will be available in all AWS regions that support VMware Cloud and VMware Cloud DR.

What are the key use cases of VMware Cloud Flex Storage?

- Providing workload datastores for the disaggregated m7i Host. m7i comes without any local NVMe storage. Any m7i cluster requires external storage for workload virtual machines.
- Seamless and cost-effective cloud migration: For customers who are looking to use VMware Cloud on AWS for a seamless and cost-effective cloud migration, VMware Cloud Flex Storage delivers true enterprise-class storage. It reduces complexity and time-to-value by supporting the lift and shift of virtual machines without a need to rework the data layer or re-architect the storage design. Customers can also simplify their operations with a storage solution that is natively built into the VMware Cloud on AWS service and readily available without manual configurations.
- Elastic data center extension: Customers who are looking to use VMware Cloud on AWS for data center extension can use VMware Cloud Flex Storage for easy access to additional storage capacity with dynamic scaling of resources. Common scenarios include high performance burst capacity, on-demand scaling for data analytics, or cost-effective long-term storage of data repositories in the cloud. This gives customers the choice of keeping their data where it best serves their consumption needs, across their data centers and the public cloud. As a result, customers benefit from a VMware-consistent, enterprise-grade hybrid cloud environment with a single pane of glass management through the VMware VMware vCenter Server console.
- Scaling of storage-intensive workloads: For customers who are running certain workloads on VMware Cloud on AWS using local instance storage with VMware vSAN, but have other workloads that are storage bound, VMware Cloud Flex Storage offers a

disaggregated storage service that allows them to independently, seamlessly, and optimally scale their performance and storage capacity to fit every workload individually. VMware Cloud Flex Storage is an ideal solution for scaling large volumes of data in an agile, flexible, and cost-effective way.

How can I learn more about VMware Cloud Flex Storage?

For more information on this service, please visit the VMware Cloud Flex Storage page on https://www.vmware.com/products/cloud-flex-storage.html for more information on this service, and/or please contact your sales representative or partner for more information on this service and how VMware Cloud Flex Storage can help your business.

Networking - General

How do I connect to the VMware vCenter Server in my SDDC on VMware Cloud on AWS?

By default, there is no external access to the VMware vCenter Server system in your SDDC on VMware Cloud on AWS. Open access to your VMware vCenter Server system by configuring a firewall rule on the Management Gateway Firewall to allow access to the VMware vCenter Server system.

Is there connectivity from the AWS VPC to VMware vCenter Server and ESX host?

Yes, you can configure connect from an EC2 instance deployed in the Connected AWS VPC to VMware vCenter Server.

What are the management and compute gateways?

When you deploy an SDDC in VMware Cloud on AWS, it is configured with two networks: a management network and a compute network. The management network handles network traffic for the SDDC hosts, VMware vCenter Server, VMware NSX Manager, and other management functions. The compute network handles network traffic for your workload VMs. The gateways allow users to access these networks from Internet, on-premises , and connected AWS VPC. The VMware NSX edge acts as the gateway.

How many traffic types exist in VMware Cloud on AWS SDDC?

There are three traffic groups in VMware Cloud on AWS:

- VMkernel Traffic (ESX Management, vMotion)
- Management Appliance Traffic (VMware vCenter Server, SRM, vSphere Replication Appliance, VMware NSX Manager)
- Workload VM Traffic

How does connectivity between the overlay network and the VMware NSX management appliances work with VMware NSX?

By default, the Compute Gateway and Management Gateways are connected through a logical segment. You can control communication through the firewall policy on the Management Gateway.

What is the change in default logical network?

As you deploy a 3 or higher host SDDC, a default logical network will not be created. It is the responsibility of the user to create a network with appropriate CIDR before deploying virtual machines

What is the reason for not creating default logical network for 3+ nodes SDDC?

There were many incidents where default logical network CIDR (192.168.1.0/24) overlapped with on-premises networks and caused connectivity issues. These issues are very difficult to troubleshoot.

Will default logical network be created for one node SDDC?

Yes. A default logical network will be created in one node SDDC. Customers must make sure that there is no overlap with CIDR 192.168.1.0/24

What is IPFIX and is it available with VMware Cloud on AWS?

IPFIX is a standard that allows virtual or physical switches to export flow information going through the switch to collector tools. Customers may decide to monitor all flows on a particular logical switch or set of logical switches. IPFIX is available with VMware Cloud on AWS.

Where can I find additional information about IPFIX?

You can find more information about IPFIX in VMware Cloud on AWS product documentation. What is Port Mirroring?

Port Mirroring is a networking feature on virtual or physical switches that allows users to capture all packets from a port and send it to a destination device. In VMware Cloud on AWS, port mirroring is configurable on virtual switches only.

What type of port mirroring is supported in VMware Cloud on AWS?VMware Cloud on AWS supports Encapsulated Remote SPAN.Can only one vNIC of a virtual machine be selected as part of the port mirror session?

Yes, a single vNIC can be configured in a port mirroring source group.

What are DNS Zones?

DNS Zones allows users to specify different DNS servers based on different domains (FQDN).

How many DNS Zones are supported?

5 zones are supported.

How would I forward requests to DNS servers deployed in VMware Cloud on AWS as well as on-premises DNS servers?

You can configure up to 5 DNS zones. Out of those, one should be with on-premises domain (FQDN) pointing to on-premises DNS server. And the other should be with AWS domain (FQDN) pointing to the DNS server in AWS.

Does VMware Cloud on AWS provide DHCP Relay functionality?

Yes, VMware Cloud on AWS provides both native DHCP capabilities and DHCP Relay.

How can I configure DHCP Relay?

This can be configured under Networking & Security tab under System→DHCP.

Can I use both DHCP Server for some Logical segments and DHCP Relay for other Logical segments?

No, either native DHCP capabilities can be used or DHCP Relay. Users will not be able to use DHCP Relay if there are any network segments using native DHCP capabilities; the respective network segments will have to be deleted first.

Are all VMware NSX APIs in VMware Cloud on AWS available under Developer Center?

Yes, you can find all available VMware NSX APIs for VMware Cloud on AWS in API Explorer.

What is the difference between "VMware NSX VMware Cloud Policy" API and "VMware NSX VMware Cloud AWS Integration" API?

VMware NSX VMware Cloud Policy API includes all the VMware NSX Networking and Security APIs for the VMware NSX capabilities within the SDDC. VMware NSX VMware Cloud AWS Integration API includes APIs that are specific to AWS like Direct Connect.

What is the benefit of using API Explorer for VMware NSX APIs?

VMware NSX APIs can easily be found and used within the VMware Cloud on AWS SDDC’s API Explorer. Furthermore, customers can even perform a search on keywords. Customers can easily lookup and test VMware NSX APIs directly from API Explorer before including them in larger scripts or applications.

How can I use API Explorer with VMware NSX APIs?

Go to API Explorer, which can be found under the Developer Center. From API Explorer, select your Organization and SDDC, and you will see both "VMware NSX VMware Cloud Policy" API and "VMware NSX VMware Cloud AWS Integration" API. Click on the one you would like to use. You will see a list of relevant VMware NSX APIs. You can put in the requested information and click the Execute button to execute the API.

How can I request approval for penetration testing applications and systems in my SDDC?

VMware has a comprehensive vulnerability management program that includes third-party vulnerability scanning and penetration testing. VMware conducts regular security assessments to maintain VMware Cloud on AWS compliance programs and continuously improve cloud platform security controls and processes. While the requirements to conduct penetration testing vary by industry compliance regulations, customer environments benefit greatly with penetration testing to measure the security effectiveness within their virtual infrastructure (SDDCs) and applications. To notify VMware that you plan to conduct penetration testing, please use this Request Form to provide us relevant information about your test plans. VMware will respond with an approval by email. Penetration testing must be conducted in accordance with our Penetration Testing Rules of Engagement.

How can I utilize Jumbo Frames on Direct Connect Network?

VMware Cloud on AWS supports Jumbo Frames for networking traffic on Direct Connect. To fully benefit from Jumbo Frames and avoid fragmentation, you must ensure that the Direct Connect interface MTU is set equal to the end to end path MTU from your SDDC to your Data Center over Direct Connect. On the AWS Account, the Direct Connect private VIF must be created with this MTU size. On the SDDC, the Intranet uplink MTU must be set to 8900.

Can I use Jumbo Frames over VPN?No, only traffic over Direct Connect, VMware Transit Connect, or across the Connected VPC can leverage Jumbo Frames.

What is the maximum value for the Jumbo frame with VMware Cloud on AWS SDDC?See the VMware Cloud on AWS configuration maximums page for details.

Networking - Advanced

What is Multi-CGW?

Multi-CGW enables customers to create additional CGWs(T1s) and manage the lifecycle for those CGWs.

Which use cases are enabled by the Multi-CGW?

Multi-CGW will enable the following use cases:

· Multi-tenancy within an SDDC

· Overlapping IPv4 address space across CGWs

· Support for static routes on customer managed CGW

· Deployment of Isolated test 'segments' for Disaster Recovery (DR) testing or “sandbox” environments.

What are the different types of Multi-CGWs (MCGW) supported?

Three types of MCGWs are supported:

· Routed – Segments behind a routed CGW are part of the SDDC’s routing table

· NATted – Segments behind a NATted CGW are reachable only via NAT configuration and are not part of the SDDC’s routing table.

· Isolated – Segments behind an Isolated CGW are not available to the rest of the SDDC.

Can the Multi-CGW type be changed after creation?

Yes, Multi-CGW configuration can be changed to meet customer network requirements.

Does each Multi-CGW have a gateway firewall?

Yes. Each Multi-CGW has its own gateway firewall.

Which NAT options does the Multi-CGW feature support?

Multi-CGW supports multiple NAT options

· Source NAT (SNAT) – Changes Source IP

· Destination NAT (DNAT) – Changes Destination IP

· Reflexive NAT – Stateless NAT

· No SNAT

· No DNAT

Can VPNs be terminated directly on the Multi-CGWs?

Yes. IPSec policy and route-based VPNs as well as L2 VPN are supported on the Multi-CGWs.

Is Route Aggregation necessary for Multi-CGW feature?

For any Multi-CGW connected segment to communicate with Direct Connect, VMware Transit Connect, or the VMware ESXi management network, Route Aggregation must be configured. Route aggregation is not required for Internet via the SDDC's Internet Gateway.

Which route types are supported on the Multi-CGWs?

Static routes can be configured on the Multi-CGWs. Non-default static routes can be configured on any type of Multi-CGW (Routed, NATted, or Isolated). The default route (0.0.0.0/0) can only be configured on Isolated Multi-CGWs.

How do I configure default drop firewall rule in the Multi-CGW gateway firewall?

In SDDC version 1.18, you cannot change the default firewall from Allow to Drop or Reject. You can add a rule to drop all traffic before the default rule of Allow.

What version of SDDC do I need to use Multi-CGW feature?

The minimum SDDC version required to use Multi-CGW feature is 1.18.

Are additional licenses required to use Multi-CGW feature?

No additional licenses are required to use the Multi-CGW feature.

How many CGWs are supported in Multi-CGW feature?

Please refer to ConfigMax for current scale information.

What is Route Aggregation feature and why do we need it?

Route Aggregation summarizes individual CIDRs into a smaller number of advertisements. This is useful to address scale issues caused by the default underlay constraints in the cloud. Route Aggregation can also help improve convergence as fewer API calls are needed to program tables during network changes.

Route Aggregation is also required for Multi-CGW feature. For any multi-CGW connected segment to communicate with Direct Connect (DX), VMware Transit Connect, or the ESXi management network.

Is the AWS Managed Prefix List Mode required for the Route Aggregation feature?

Route Aggregation for Connected VPC can't be used without enabling AWS Managed Prefix List Mode.

What does enabling AWS Managed Prefix List Mode do?

When AWS Managed Prefix List Mode is enabled, a VMware managed prefix list is created and maintained by the SDDC and shared to the Connected VPC's AWS account. This simplifies customer routing configuration and improves network convergence. Additionally, it enables the ability for customers to use the prefix list to support multiple route tables and prefix list based AWS Security Groups in the Connected VPC.

Is an aggregate route suppressed when there are no member routes?

No. Aggregate route will be advertised even if there are no member routes.

Will the prefix for a segment be advertised if there is no aggregate route that covers that segment?

For any segment behind a Multi-CGW, there must be an aggregate route that covers that segment. Otherwise, that segment will not be reachable. For any segment behind the default CGW, if there is no aggregate route that covers that segment, that individual prefix will be advertised.

Is the management CIDR suppressed if an aggregate route covers the management CIDR?

If an aggregate route includes the management CIDR, the management CIDR will still be advertised as a discrete CIDR.

What happens if inaccurate CIDR is configured?

When an incorrect CIDR is configured due to typos or incorrect subnetting, system will normalize inaccurate CIDRs before applying the aggregate prefix. Please check if the applied configuration meets your expectation.

What are the additional considerations when using the Route Aggregation feature?

Here are few additional things to remember when using the Route Aggregation feature:

- Incorrect aggregation can impact reachability to networks on-premises or in other SDDCs
- NAT CIDRs need to be included in the aggregation if you want them to be reachable
- Creation of multiple aggregations is possible for non-contiguous networks

What version of SDDC do I need to use Route Aggregation feature?

The minimum SDDC version required to use Route Aggregation feature is 1.18.

Are additional licenses required to use Route Aggregation feature?

No additional licenses are required to use the Route Aggregation feature.

Networking - Firewall

Will my security policy and services migrate when the VM is live migrated to the VMware Cloud on AWS SDDC using vMotion?

No. You are responsible for moving the security policy and services.

What is Distributed Firewall?

The NSX Distributed Firewall enables micro-segmentation (granular control over East-West traffic) for application workloads running in the VMware Cloud on AWS SDDC.

What is the default Distributed Firewall policy?

The default security policy is allow all. Users can create deny polices as part of the different sections created by default.

How many default sections are created in the DFW?

There are 5 default sections : Ethernet, Emergency, Infrastructure, Environment, and Application.

What is Inventory and why is it used with DFW policies?

Inventory provides the list of VMs deployed in the vCenter. It allows user to create security polices using VM context instead of IP address and these policies are easy to configure and manage.

What is Grouping?

Grouping construct enables users to create identifiable group of objects and create security policies using those objects. For example, you can create group of VMs called as "web" and "app" and "db" and then use those objects to create FW policy between Web and App and App and DB layers.

What is Tagging?

Tagging allows user to assign tags to virtual machines. These tagged virtual machines can be automatically made part of a group that is used for firewall policies.

What is Firewall Logging?

Firewall Logging enables customers to log packets for specific firewall rules. The captured packet logs help in troubleshooting or security monitoring activities.

Where do the Packet Logs forwarded?

Packet Logs are forwarded to the Log Intelligence service.

Do I have to purchase the ARIA Log Insight Cloud service to see the packet logs?

Yes. Customers will get a free 60 day trial for checking packet logs, but then they have to purchase the service to continue to have access to the packet logs.

Can I enable FW logging for Compute Gateway, Management Gateway, and Distributed Firewall?

Yes. You can enable logging for Compute and Management gateway, and DFW rules.

What information is available on firewall statistics?

Administrators can now access firewall statistics directly from the Networking and Security console. When the user clicks on the graph icon on the right-hand side of the rule, he/she can see: Hit Count Packet Count Session Count Byte Count Popularity Index Max Popularity Index Max Session Count Total Session Count.

Can the default Distributed Firewall policy be changed?

Users can change the default DFW behavior from its default permit model (allowing all the traffic through and denying specific traffic with the security rules) to drop model (only allowing specific traffic through the security rules and dropping everything else).

Can I limit the scope of a Firewall rule?

The Firewall or Distributed Firewall scope can now more specific with the "Applied-To" feature. Users can now apply a security rule to a specific group instead of across all the workloads.

What is the DFW Exclusion List?

The DFW Exclusion List keeps a list of virtual machines excluded from consideration from the Distributed Firewall. This is to ensure administrators don't block access to key management platforms by applying a strict security policy. By default, vCenter, NSX Manager ands NSX Controllers are on the Exclusion List but this option now adds the ability to add more VMs to it.

How can I use Groups?

Inventory Groups make it easier to create and apply security policies. Users can create Groups using Virtual Machine name, tag, OS name, logical segment and IP set as membership criteria. It's particularly useful for customers that need the ability to dynamically micro-segment virtual machines based on these criteria. Nesting of Groups is supported - users can now create groups nested inside other groups (also called 'nested groups'). This gives users the ability to apply security policies encompassing wider groups but also more granular rules. This enables administrators to have security policies as close as business and compliance policies. Refer to the VMware Cloud on AWS ConfigMax page for specific scale attributes.

Do I need to modify firewall policy to allow SDDCs that are a member of a SDDC Group to communicate?

Yes, firewall policy must be updated to allow SDDCs that are in a group to communicate. The SDDC Grouping construct enables network connectivity but does not dictate security policy. The SDDC group does automatically create groups that can be used to simplify the definition of security policy.

Networking - Direct Connect

What is AWS Direct Connect?

AWS Direct Connect makes it easy to establish a dedicated network connection from your premises to AWS. Using AWS Direct Connect (DX), you can establish private connectivity between AWS and your data center, office, or colocation environment, which in many cases can reduce your network costs, increase bandwidth throughput and provide a more consistent network experience than Internet-based connections.

What is required while establishing an AWS Direct Connect connection?

You must create an AWS virtual interface (VIF) to begin using your AWS Direct Connect connection. There are two types of virtual interfaces. You can create a Private Virtual Interface to connect to a VPC, or you can create a Public Virtual Interface to connect to AWS public services. The Public Virtual Interface also allows VPN traffic to travel over your Direct Connect.

What are the pre-requisites for connecting to your VMware Cloud on AWS SDDCs with AWS Direct Connect using a private VIF?

You must have established AWS Direct Connect link from on-premises data center to an AWS region. Then create a private VIF and assign the ownership to your VMware Cloud on AWS SDDC. Accept the attachment to the private VIF through the VMware Cloud on AWS Console.

What are the pre-requisites for connecting to your VMware Cloud on AWS SDDCs with AWS Direct Connect using a public VIF?

You must have established AWS Direct Connect link from an on-premises data center to an AWS region. You need to create a public VIF and have to establish IPSec VPN tunnel to the SDDC over the public VIF. There is no configuration required on the VMware Cloud on AWS Console. You need to ensure that you can route your IPSec VPN gateway traffic over the public VIF.

How are the traffic charges handled when a Private VIF is connected to VMware Cloud on AWS SDDC?

AWS Direct Connect traffic charges will be applied to the VMware Cloud on AWS account. You will see those charges on your VMware Cloud on AWS bill.

Can I attach multiple private VIFs to a VMware Cloud on AWS SDDC?

Yes. You can attach multiple private VIFs to provide redundancy and higher throughput.

How is the Direct Connect Integration with NSX SDDC?

Direct connect integration with NSX allows all traffic from VMware Cloud on AWS to On-premises over Private VIF

Does Direct Connect support management appliances and workload traffic?

Yes. With NSX, SDDCs management appliances and workload traffic is carried over DX Private VIF. Management appliances and workload network routes are published to on-premises over existing BGP sessions. As long as the BGP configuration on the on-premises router allows these new routes, you will have the connectivity for these traffic types.

What routes are advertised from the SDDC over Direct Connect Private VIF?

Management Appliance CIDR, ESX CIDR, Logical segments CIDRs. Refer to the VMware Cloud on AWS ConfigMax page for specific scale attributes.

Do you support Private or Public ASN with Direct Connect Private VIF?

By default public ASN is used. However, if you need to utilize private ASN, you can work with support team for that configuration.

What is BGP ASN (Autonomous System Number) and do I need one to use AWS Direct Connect?

Autonomous System numbers are used to identify networks that present a clearly defined external routing policy to the Internet. AWS Direct Connect requires an ASN to create a public or private virtual interface.

Which ASN can be used for Private VIF connection to VMware Cloud on AWS SDDC?

You can pick any private ASN number between 64512 to 65535 range.

Is the ASN common to all Private VIF attached to VMware Cloud on AWS SDDC?

Yes, the ASN is common to all the Private VIFs attached to the SDDC.

Can I change the ASN after the Private VIFs are attached to SDDC?

You have to delete all connected Private VIFs before you can change the ASN.

What BGP Local ASN Configuration do I need with AWS Direct Connect Private VIF?

Direct Connect connection to SDDC now uses BGP Local ASN as 64512. This BGP local ASN is editable and any private ASN from the range 64512 – 65534 can be used.

Can I use Public ASN with a new Direct Connect Private VIF connection?

No, you cannot use Public ASN value while configuring the BGP Local ASN on VMware Cloud on AWS SDDC.

Will you continue to support existing Direct Connect Private VIF configuration that uses Public ASN?

Yes. We will continue to support existing Direct Connect configurations.

What do I need to do if I want to change existing Direct Connect Private VIF configuration from Public to Private ASN ?

You have to first delete the Direct Connect Private VIF connection with public ASN. Then you can choose a Private ASN number from the range 64512-65534 and enter it in the BGP Local ASN field in VMware Cloud on AWS. After that, take the configured Private ASN number and AWS account ID and go to AWS account to create a new Hosted Private VIF with these values.

Networking - VPN

What is NSX L2 VPN?

NSX L2 VPN is a tunnel that enables extending layer 2 networks across geographic sites. Extended layer 2 networks enable virtual machines to move across sites (vMotion) while keeping their IP addresses the same. L2 VPN allows enterprises to seamlessly migrate workloads backed by VLAN or VXLAN between on-premises and VMware Cloud on AWS.

Do I need NSX on-premises to use NSX L2 VPN between on-premises and VMware Cloud on AWS?

No. You do not need NSX on-premises to use L2 VPN. There are two components of L2 VPN - a client side component and a server side component – with the server side running in VMware Cloud on AWS. In order to configure an L2 VPN between on-premises and VMware Cloud on AWS, you must configure the client side component on-premises. If you do not have NSX on-premises , you can download a standalone NSX edge and configure the client side of L2VPN.

Will NSX L2 VPN layer 2 network extension work with any other vendor device?

No. You need an NSX standalone edge that you can download separately or have NSX on-premises.

What are the key use cases NSX L2 VPN enables?

- One-time migration of applications from on-premises to VMware Cloud on AWS
- Workload migration between on-premises and VMware Cloud on AWS
- Keeping the IP address same during Disaster Recovery

How many networks can you extend over one NSX L2 VPN tunnel?

Refer to the VMware Cloud on AWS ConfigMax page for specific scale attributes.

What are the bandwidth considerations across the NSX L2 VPN tunnel?

Maximum bandwidth supported across an NSX L2 VPN tunnel is 750 Mbps.

What is the download config link in Layer 3 IPSec VPN set up?

You can download the IPSec VPN configuration for VMware Cloud on AWS. The downloaded file captures all the key parameters that need to be configured on the Peer IPSec VPN device. This is a generic parameter file that will expedite the configuration on the remote side by providing all the key parameters in a single file.

How do you achieve resiliency for the L2 VPN Client?

Users can choose to deploy two standalone edge devices and configure them as active and standby for resilience.

What failure scenarios does Active-Standby client deployment protects from?

This protects from the edge failure scenario. If the active edge fails, the standby will take over the tunnel traffic.

How Many L2 VPN tunnels you can create through VMware Cloud on AWS console?

You can create only one L2 VPN tunnel.

Does vMotion traffic flow over L2 VPN tunnel?

No. vMotion traffic doesn't flow through L2 VPN tunnel. This tunnel is for the VMware Cloud on AWS VMs to communicate to on-premises resources. vMotion traffic flows through the AWS Direct Connect (Private VIF). For HCX Live Migration, which also uses vMotion, the traffic is automatically secured and routed by HCX.

What is Tunnel Status Monitor?

Tunnel status monitor allows you to see granular information about the traffic through the tunnel with any errors. This information is useful while troubleshooting or monitoring IPsec and L2 VPN tunnels.

What information is available on the tunnel statistics?

You will be able to see packets in/out and bytes in/out per tunnel as well as error counts per tunnel.

How do I find IPSec and VPN tunnel configuration related errors when i use the tunnel status monitor?

The tunnel status color (green, yellow, red) will indicate the health of the tunnel and when you click on the information you will see the pop up with the details.

What is route-based VPN?

Route Based VPN provides the ability to dynamically publish networks across the VPN tunnel using BGP protocol. It simplifies the deployment for customers compared to the manual and static policy-based VPN.

What protocol is supported for Route Based VPN?

Standard eBGP protocol is supported.

What routes are advertised from the VMware Cloud on AWS SDDC?

Management Infrastructure and Logical segment CIDRs are advertised to the on-premises BGP Peer.

With NSX, do I only have to establish one VPN tunnel for Management and workload traffic?

Yes. With NSX, user needs to establish just one tunnel.

If two tunnels are established, can traffic flow through both tunnels?

Yes, if multiple tunnels are configured between the SDDC and the same remote VPN endpoint, Equal Cost Multipath (ECMP) routing will be used.

Does NSX support redundant tunnels?

Yes. There is support for redundant tunnels. User can establish these tunnels across the different endpoint devices on-premises.

How many VPN tunnels are supported?

Refer to the VMware Cloud on AWS ConfigMax page for specific scale attributes.

How is traffic flow controlled over the tunnel?

Traffic flow is controlled through the BGP parameters on the remote endpoint devices. The example for the BGP parameters include: AS Path, BGP weights, MED.

Does VMware Cloud on AWS support two different endpoints in the SDDC?

No. Support is only available for one endpoint in active-standby mode.

For Policy based VPN, can I create just one tunnel to carry all traffic?

Yes, you may create one tunnel for all traffic. All management and workload subnets must be advertised.

Does NSX-T support Ikev2?

Yes, we now support both IKev1 and Ikev2.

Will I be able to see the BGP routes advertised from on-premises over VPN?

Yes. In the Route based VPN tab, users can now click on "View Routes" to see the advertised networks from on-premises. Users also have choice to "download routes".

What is Source NAT public IP in the Networking Security Topology view ?

Any internet facing communication from the SDDC requires a public IP. By default a public IP is provisioned and Source NAT configuration is done for such communication. Topology view now shows that public IP. This will be useful during any troubleshooting exercise.

Can IPSEC VPN be used as backup to Direct Connect Private VIF?

Yes, this is supported with Route Based IPSEC VPN.

How do I enable Route Based IPSEC VPN as back-up to Direct Connect?

This can be enabled under Networking & Security tab under System→Direct Connect by enabling the option "Use VPN as backup to Direct Connect"

What happens if "Use VPN as backup to Direct Connect" is enabled but no VPN is configured?

The traffic will go over Direct Connect as usual. There will not be any VPN backup to Direct Connect until a route based IPSEC VPN is configured.

Does Route Based IPSEC VPN support ECMP?

Yes, Route Based IPSEC VPN supports both Active/Standby and ECMP.

How do I configure ECMP with IPSEC VPN?

There is no ECMP setting to enable. If there are multiple VPN tunnels, all VPNs tunnels will be used. Whether a tunnel is active/standby for routes is controlled via BGP metric from on-premises or the other side.

Networking - VMware Transit Connect

What is VMware Transit Connect?

VMware Transit Connect is a high bandwidth, low latency connectivity feature for SDDC Groups. It provides network-level connectivity among SDDC Group members by leveraging an AWS Transit Gateway (TGW) in the AWS region. It also enables network connectivity to AWS VPCs and on-premises/colo data centers (via a Direct Connect Gateway).

Can I utilize AWS Transit Gateway in VMware Cloud on AWS?

VMware Transit Connect establishes network connectivity among SDDCs by leveraging an AWS Transit Gateway. It creates a VMware Managed Transit Gateway (VTGW) for SDDC Group Communication.

What connectivity models are supported with Transit Connect?

VMware Transit Connect supports SDDC to SDDC communications within the same region and across regions, SDDC to Native customer-owned AWS VPC communications within the same region, and SDDC to on-premises networks using an AWS Direct Connect Gateway.

Can my Connected VPC that is part of my SDDC also connect to the VTGW?

Yes, Connected VPC can utilize VTGW for communication. The Connected VPC will use the VPC attachment for communications to the SDDC it is associated to. The Connected VPC would use the VTGW attachment to communicate with other SDDCs in the SDDC Group.

I have connected my native AWS VPC to a VTGW. Do I need to make any changes to enable communication?

Yes, you must add routes to the AWS VPC to the CIDRs in the SDDC(s) to use the VTGW through the AWS console.

Can I connect a VPN to the VTGW instead of a Direct Connect Gateway for my on-premises environment?

No, you cannot use a VPN to connect to the VTGW.

I am using VPNs for SDDC to SDDC connectivity today. Can I use Transit Connect to interconnect them?

Yes, the requirement is that the SDDCs are in the same AWS region, you can use Transit Connect to replace your VPN connection and get higher performance connectivity.

What is an SDDC Group?

An SDDC Group is a set of SDDC organized together for a common purpose. It is a logical grouping meant to simplify SDDC operations at scale. SDDC Groups provide customers with the ability to logically organize a set of SDDCs to simplify management at scale, as customers deploy multiple SDDCs within VMware Cloud on AWS. With an SDDC group, customers can manage multiple SDDCs as a single logical entity.

Do the automatically created groups get updated as networks are added or removed from my SDDCs?

Yes, the automatically created groups reflect the current state of networks.

Networking - SDDC Group Connectivity to Transit VPC

What is SDDC Group Connectivity to Transit VPC?

SDDC Group Connectivity to Transit VPC designs enable customers to take advantage of additional flexibility in VMware Cloud on AWS network topologies by providing the ability to configure static routes to control network traffic to external destinations.

What are the use cases for connecting a SDDC Group to a Transit VPC design?

Some common use cases for a Transit VPC design include:

Security VPC where all traffic must be inspected before being routed to the Internet or on-premises Interconnecting different SDDC groups in the same region in either the same VMware Cloud Organization or different ones
A temporary workaround for intra-region Transit Connect to AWS TGW peering

What are the requirements to use SDDC Group Connectivity to a Transit VPC?

The requirements to use SDDC Group Connectivity to a Transit VPC are:

SDDC version 1.12(M12) or higher VMware Transit Connect

Are additional licenses required to use SDDC Group Connectivity to a Transit VPC?

No additional licenses are required.

Are there charges or fees to use SDDC Group Connectivity to a Transit VPC?

The normal VMware Transit Connect fee structure still applies, but there is no incremental cost to use SDDC Group Connectivity to a Transit VPC. Pricing information can be found on the VMware Cloud on AWS pricing page here.

How do I configure SDDC Group Connectivity to a Transit VPC?

The configuration for SDDC Group Connectivity to a Transit VPC is performed at the SDDC Group level on a per-VPC attachment basis through a static route.

How many static routes can be configured on a VPC attachment?

100 static routes can be configured per VPC attachment. Please refer to VMware Cloud ConfigMax for current scale attributes here.

Is it possible to configure a default route (0.0.0.0/0) as the static route?

Yes, a default route can be configured but should be done with a complete understanding of the connectivity to and from the SDDC as all traffic, including VMware ESXi host traffic, will follow the default route unless a more specific route exists.

Networking - Transit Connect Inter-Region

What is Transit Connect Inter-Region Support?

Transit Connect Inter-Region support enables customers to simply make VMware Cloud on AWS SDDCs in different regions members of an SDDC Group. This provides a consistent and simplified network topology while broadening the high speed, resilient interconnectivity between regions.

What are the use cases for Transit Connect Inter-Region?

Some common use cases for Transit Connect Inter-Region include: • Inter-Region disaster recovery

Are additional licenses required to use Transit Connect Inter-Region?

No additional licenses are required to use the Transit Connect Inter-Region feature.

Are there charges or fees to use Transit Connect Inter-Region?

The normal VMware Transit Connect fee structure still applies, but there is no incremental cost to use Transit Connect Inter-Region. Pricing information can be found on the VMware Cloud on AWS pricing page here.

Is Transit Connect Inter-Region available in all commercial regions?

Yes, Transit Connect Inter-Region is available in all AWS commercial regions where VMware Cloud is available.

Can I connect my customer-managed AWS Transit Gateway to the SDDC Group?

It is not possible to connect a customer-managed AWS Transit Gateway to the SDDC Group at this time.

Do all SDDCs that are members of the group need to be in the same VMware Cloud Organization?

Yes, all SDDCs that are members of the group need to be in the same VMware Cloud Cloud Organization.

How many regions are supported in a single SDDC group?

Transit Connect Inter-Region supports groups with members of up to three regions. Please refer to VMware Cloud ConfigMax for current scale attributes.

Can all resources connected to the SDDC Group communicate?

SDDCs connected to the SDDC Group can communicate regardless of region. On-premises connections via Direct Connect Gateway and or External VPC connections can only communicate with SDDCs in their same region.

How many routes can be advertised from a SDDC to the SDDC Group?

The number of routes advertised from a SDDC to the SDDC Group is 250. Please refer to VMware Cloud ConfigMax for current scale attributes here.

Networking - Multi Edge SDDC

What is Multi Edge SDDC?

Multi Edge SDDC is a feature that enhances the overall network capacity of the SDDC by provisioning additional edge resources in the SDDC. Users can utilize this feature by configuring Traffic Groups and mapping specific network traffic to utilize additional resources assigned to the group.

What are the primary use cases for Multi Edge SDDC ?

The primary use cases for Multi Edge SDDC are for traffic flows between the SDDC and destinations connected to a VMware Transit Connect network such as another SDDC, native AWS VPCs and on-premises. Additionally, services in the Connected VPC can take advantage of Multi Edge SDDC's increased capacity.

What type of traffic should be considered a good use case for Multi Edge SDDC ?

While Multi Edge SDDC works with many different types of traffic, we've found that services like data backup, database synchronization and file storage are well suited for mapping into a Traffic Group and taking advantage of the increased network capacity.

What do I need to do to enable Multi Edge SDDC?

Multi Edge SDDC requires large-sized SDDC appliances.

Does Multi Edge SDDC require additional compute resources?

Yes, each Traffic Group configured will require 2 additional hosts in the VMC Management cluster to dedicate to the networking services.

How do I configure my SDDC's traffic to use Multi Edge SDDC?

Multi Edge SDDC uses Source Based Routing to network traffic flows. To identify traffic, configure a prefix-list of subnets or IP addresses to use the Traffic Group and then associate the prefix-list to the Traffic Group.

Does Multi Edge SDDC work with all of my SDDC's traffic?

While Multi Edge SDDC works with all types of IP traffic from workloads, there are some specific flows that are not able to take advantage of Multi Edge SDDC. These specific flows are flows that use Network Address Translation (NAT) including S3, VPN traffic and traffic using an AWS Direct Connect. Management VMs and ESXi hosts are not able to take advantage of Multi Edge SDDC. All of these flows will continue to traverse the default edge.

Can I use Multi Edge SDDC with a 2 host SDDC?

Due to the host requirements for Multi Edge SDDC, 2 node SDDCs are not capable of supporting Multi Edge SDDC and in most cases, don't generate enough traffic to really need it.

What is a Traffic Group?

A Traffic Group is a new VMC construct that creates additional network capacity resources in the form of NSX Edge routers.

What is an IP Prefix List?

An IP Prefix List is how customers define the source IP addresses of traffic that will utilize the new network capacity created by the Traffic Group.

What is an Association Map?

An Association Map is the construct used to bind an IP Prefix List to a Traffic Group.

How many Traffic Groups can I have in my SDDC?

Refer to the VMware Cloud on AWS ConfigMax page for specific scale attributes.

Can I reconfigure the Traffic Group/ Prefix List/ Association Map?

Reconfiguration of the prefix list being used by an association map is not possible. We recommend customers either create a new prefix list with the changes required and apply it in place of the current one, or remove the association map, update the prefix list and re-apply the association map.

Networking - Advanced Firewall

What is the Advanced Firewall Add-On?

The Advanced Firewall Add-On is a new set of capabilities enhancing the security offerings for VMware Cloud on AWS. It features Layer 7 Distributed Firewalling, Fully Qualified Domain Name (FQDN) Filter List, Distributed Intrusion Detection/Prevention Services (D-IDS/IPS), and Active Directory Based Identity Firewalling.

Is the Advanced Firewall Add-On part of the VMware Cloud on AWS offering?

With the introduction of VMware Cloud on AWS Advanced, the Advanced Firewall Add-On is an included service except for Intrusion Detection/Intrusion Prevention that needs to be enabled per SDDC to begin using the additional features. IDS/IPS can be activated separately but is subject to charges. Pricing and billing information can be found on the VMware Cloud on AWS pricing page.

Does the Advanced Firewall Add-On protect East-West and North-South traffic?

Yes, the Advanced Firewall Add-On protects both East-West and North-South traffic based on the user configured policy.

Are the Advanced Firewall Add-On features available for PCI-compliant SDDCs?

No, the Advanced Firewall Add-On features are not available in PCI-compliant SDDCs.

Does the Advanced Firewall Add-On protect against malware?

Yes, the Distributed IDS/IPS feature can protect against malware that matches the curated signatures configured.

In which AWS regions are the Advanced Firewall Add-On available?

The Advanced Firewall Add-On is available in all AWS commercial regions where VMware Cloud is available.

What are the scale attributes for the Advanced Firewall Add-On features?

Please refer to VMware Cloud ConfigMax for current scale attributes.

What level of feature enablement is available for the Distributed IDS/IPS?

The Distributed IDS/IPS is enabled or disabled on a per VMware vCenter Server cluster basis.

Where do I download signatures for Distributed IDS/IPS?

Updated signatures for the Distributed IDS/IPS are obtained from the VMware NSX Threat Intelligence Cloud (NTIC) service. This can be configured for automatic updates to streamline administration and ensure the most current signatures are in place.

What is VMware NSX Threat Intelligence Cloud services?

VMware NSX Threat Intelligence Cloud service is a VMware managed repository of IDS/IPS signatures. It is a cloud based offering hosted in multiple regions across the globe.

Does the ability to perform an offline update of the Distributed IDS/IPS signatures exist?

For customers with isolated SDDCs that cannot automatically update through NTIC, an offline download and upload option exists using APIs.

Where are Distributed IDS/IPS signatures stored?

The signatures for Distributed IDS/IPS are initially downloaded to VMware NSX Manager inside the SDDC, and then automatically placed on each host in a cluster that is configured to use Distributed IDS/IPS.

Can I run the Distributed IDS/IPS in detect only mode?

Yes, when a policy is configured for the Distributed IDS/IPS it can be configured for detect only (IDS) or detect and prevent (IPS) actions.

What is the use case for Identity Firewall (IDFW)?

The primary use case for IDFW is for granular, per user session based firewall policy in Virtual Desktop Infrastructure (VDI) environments.

Does Identity Firewall (IDFW) support Remote Desktop Session Host (RDSH)?

The IDFW supports both VDI and RDSH methods for remote access.

What level of feature enablement is available for the Identity Firewall (IDFW)?

The IDFW is enabled or disabled on a per VMware vCenter Server cluster basis.

Is Guest Introspection required to use the Identity Firewall (IDFW) feature?

Guest Introspection is used by the IDFW feature.

Does Guest Introspection require a dedicated VM to operate?

VMware Cloud on AWS uses a kernel based Guest Introspection engine that does not require a dedicated VM to operation.

Is VMTools required for Identity Firewall (IDFW)?

The IDFW feature requires VMTools 11.x or higher to be installed on the guest VMs.

What are the use cases for Layer 7 Firewalling?

The common use case for Layer 7 Firewalling is to allow granular inspection of traffic inside a given port or protocol. This is frequently used to detect and prevent unauthorized traffic from using commonly allowed ports and protocols. It is also used to ensure specific encryption protocols are used for secure traffic.

Does the Layer 7 Firewalling feature have pre-configured application definitions?

The Layer 7 Firewalling feature has more than 70 pre-configured application definitions based on commonly used enterprise applications, enabling fast deployment of the feature.

Is it possible to define a custom application in the Layer 7 Firewall?

The Layer 7 Firewall uses Context Profiles to define applications. The ability to add custom profiles is available.

What are the use cases for Fully Qualified Domain Name (FQDN) filtering?

The common use cases for FQDN filtering include restricting access to unauthorized URLs or conversely restricting access to specific authorized URLs.

Does the Fully Qualified Domain Name (FQDN) filtering feature require DNS Snooping?

The FQDN Filtering feature uses DNS Snooping on the Distributed Firewall (DFW) to observe and track the DNS requests from guests.

Is it possible to deactivate the Advanced Firewall Add-On?

The Advanced Firewall Add-On can be enabled or disabled by the user at any time.

What happens if I disable the Advanced Firewall Add-On?

If the Advanced Firewall Add-On is disabled, additional policy for Distributed IDS/IPS, FQDN Filtering, IDFW or Layer 7 firewalling cannot be added, and existing policy cannot be edited. Previously configured policy will still be enforced and is retained until deleted by the administrator.

What happens if I re-enable the Advanced Firewall Add-On?

If the Advanced Firewall Add-On is re-enabled, existing policy will become configurable.

Service Operations

Who is responsible for supporting customers when they have issues?

VMware will provide VMware Global Support Services (GSS) and Customer Success team support for customers. You will be able to contact GSS via phone, chat feature in the service portal. VMware's service operations team will handle escalations.

What does VMware manage and operate vs. what is the responsibility for customers?

VMware is responsible for the SDDC software components and the IaaS infrastructure resources. Customers are responsible for their applications and workloads running on the service.

Can you describe the operations and support models for VMware Cloud on AWS?

VMware provides a 24x7 command center that supports the service along with site reliability teams and engineering teams that are on-¬call supporting the service. Service operational readiness and live service operations and support are key activities for the service teams. VMware will actively monitor and maintain the SDDC components and IaaS infrastructure to ensure customers receive a high¬-quality service experience. In addition, fleet SDDC lifecycle management will enable efficient and reliable operations at scale.

How do I install a patch for VMware Cloud on AWS & VMware Cloud on AWS GovCloud (US) SDDC components?

VMware handles all patching, updates, and maintenance for VMware Cloud on AWS & VMware Cloud on AWS GovCloud (US) SDDC components.

Who is responsible for conducting maintenance updates on my SDDC software running in VMware Cloud on AWS & VMware Cloud on AWS GovCloud (US)?

VMware handles all patching, updates, and maintenance for VMware Cloud on AWS & VMware Cloud on AWS GovCloud (US) SDDC components.

What happens during a maintenance update for the SDDC software running on VMware Cloud on AWS & VMware Cloud on AWS GovCloud (US)?

Prior to a maintenance update, you will receive an email notification telling you the date and time of when the update is going to occur. When the update process is initiated, you will receive another email notification. The process occurs in 2 main phases, control plane update and data plane update. During the control plane update, customers are temporarily prevented from gaining access to VMware vCenter Server. Direct access to VMs will still be available during this phase. A backup of VMware vCenter Server and VMware NSX Manager is taken prior to installing the update. The update is then installed. Once the installation is completed, access to VMware vCenter Server is restored and the control plane phase is completed. An email is sent to you once the control plane is completed. In the data plane update phase, an extra VMware ESXi host is temporarily added to each cluster to ensure sufficient capacity to complete the update process. The data plane update process is conducted on a rolling basis, with the hosts being updated one at a time. Each VMware ESXi host is placed into maintenance mode and VMs are migrated to another host in the cluster. Update of the VMware ESXi host is done in-place after

the VMs are migrated. Once all of the hosts are updated, one of the hosts is removed from the cluster to restore the host count to the original number before the update process gets over. An email is sent to customers once the data plane update is completed.

Is there any planned downtime during maintenance updates for SDDC software?

Yes, during the control plane phase of the SDDC maintenance update, access to vCenter will be removed. Once the control plane phase is finished, access will be restored.

Is my SDDC software backed up before the SDDC maintenance updates?

VMware will backup VMware vCenter Server and VMware NSX Manager prior to installing control plane updates. VMware will be able to restore from these backups as needed. VMware does not back up virtual machines and user data, as these are the customer's responsibility.

How often will VMware perform maintenance on my SDDC on VMware Cloud on AWS?

Due to the nature of software updates, this will be done on an as-needed basis. For planning purposes, VMware anticipates monthly updates to infrastructure during the initial rollout and expects to transition to quarterly updates as the service matures.

How does VMware notify me about planned or unplanned SDDC Maintenance?

VMware is responsible for managed delivery of Software Defined Data Center updates and emergency patches. This involves maintaining consistent software versions across the SDDC fleet with continuous delivery of features and bug fixes. Detailed information about the SDDC upgrade and maintenance process is available in SDDC Upgrades and Maintenance page. Typical updates are scheduled based on SDDC regions, outside business hours and are not workload impacting. Major updates occur approximately once a quarter with patch bundles in between. Updates may include new functionality, bug fixes and new operational enhancements, patches include bug fixes and security patches. VMware attempts to provide update notifications several weeks in advance but at a minimum will provide 24 hours of notice. VMware Cloud on AWS has multiple notification mechanisms used to contact customers regarding maintenance and uses all of them to ensure customers are informed about any activity that may affect their use of the service.
1. Within the VMware Cloud on AWS Console is a multi-channel notification service that is used to notify customers for important events. Customers can subscribe to the notification webhook for the events.
2. Maintenance activities are published on the VMware Cloud on AWS status page - https://status.vmware-services.io/. Customers can subscribe to updates on this page and email notifications will be sent by noreply@vmware-services.io.
3. Maintenance communications are sent from the email ID vmc-services-notices@vmware.com to the email addresses of all organization members and organization owners. Additional information about the contents of an update can be found on the Release Notes page: https://docs.vmware.com/vmc/releasenote

Can I change any cluster settings, such as DRS or HA?

DRS and HA settings are fixed to values that provide the best performance and availability for both management components as well as virtual machines you deploy.

Can I rename the hosts in my SDDC on VMware Cloud on AWS?

The names for the hosts are generated automatically and cannot be changed. In addition, if a host is replaced, there is no guarantee that the host name will be the same. You should modify any scripts and other tools so that they do not rely upon fixed hostnames.

Can I add my own VIBs to my SDDC hosts on VMware Cloud on AWS?

You are not able to add any software to the base ESXi image installed on your hosts. Patching and updates will be handled for you by the VMware Cloud service.

What happens when I delete an SDDC on VMware Cloud on AWS?

When you delete an SDDC, your VMs and data are deleted and the hosts and other resources allocated to the SDDC are released for use in other SDDCs.

What Network Time Protocol Server (NTP) is used by VMware Cloud on AWS?

VMware Cloud on AWS uses the Amazon Time Sync Service to keep all logs globally synchronized.

Which version of VMware Tools is available for my VMs running on VMware Cloud on AWS?

VMware will provide installers for a designated release of VMware Tools for all supported guest operating systems and will update those from time to time. You have the option of using a different version of VMware Tools than the one shipped with VMware Cloud on AWS to ensure there is a standardized version between your on-premises and VMware Cloud on AWS environment. You can either upload the desired VMware Tools ISO to vSphere Datastore or you can use Guest Operating System tools to deploy the desired VMware Tools version using Microsoft Windows SCCM, Linux apt-get, etc.

If an AWS region goes down or loses connectivity, will I still be able to access the VMware Cloud on AWS Console, APIs and vCenter Server?

The VMware Cloud on AWS Service, Console and APIs are all located in the AWS US West (Oregon) Region. Only a complete failure of this region would result in a service disruption to the VMware Cloud on AWS Service, Console and APIs. If the region that your SDDCs are deployed in goes down, then you will not have access to vCenter Server and the ability to perform actions on the impacted SDDCs.

Do I need to access region-specific endpoints to access my SDDCs?

No, you use the same endpoints to access the VMware Cloud on AWS API and VMware Cloud on AWS Console regardless of the region your SDDCs are in.

Will VMware ever add hosts to my cluster without my permission?

Yes. As part of our responsibility for maintaining your working SDDC, we may add additional hosts to your SDDC if the health of this SDDC is in danger. Generally, this only occurs when your datastore fills up to an unsafe level. As per our SLA, we require 25% "slack space" in order to support your SDDC.

Will VMware bill me for hosts added automatically?

Yes. You are billed for all hosts in your environment per running host hour.

How do I prevent VMware from adding hosts to my SDDC?

Generally, we advise customers to monitor their capacity and take action when the system passes 70% capacity. At that point, some customer action should be taken. If you take corrective action at 70%, automated remediation by VMware will not occur.

How are my subscriptions affected by an automated scale up event?

We do not automatically add subscriptions to your account. Because scale up events may represent temporary spikes, we do not recommend that you automatically buy a new subscription every time a scale up event causes a host to be added to your SDDC. For most customers, it is more cost effective to buy additional host subscriptions after you have established that baseline capacity. Normally, you want to review your capacity requirements by looking backwards 30 to 60 days and then buy subscriptions based on your minimum capacity requirement for that period. This ensures that you are only buying subscriptions you actually need.

If VMware scales up my cluster due to health concerns, will they then scale it back down?

The best way to ensure that we automatically scale your cluster up or down is to enable EDRS. If EDRS is not enabled, we will only add hosts in an emergency and we will not remove those hosts if usage later drops. So, the only way to ensure that VMware is monitoring your cluster size is to enable EDRS.

API Automation

How can I find the API for VMware Cloud on AWS?

From within the VMware Cloud on AWS Console you will be able to access the RESTful APIs by accessing the Developer Center tab and API Explorer, from within this area you can browse the publicly available APIs and try these out for your given resources.

What is the Developer Center?

Developer Center for VMware Cloud on AWS gives automation experts, DevOps engineers and developers a central portal for getting access to detailed API information, software development kits, code samples and command line interfaces.

• Integrated into the VMware Cloud on AWS Service Console. • Easily learn and execute the VMware Cloud on AWS Service RESTful APIs with the Interactive API Explorer.

• Quickly integrate your workflows and partner solutions with VMware and community code samples for common development languages.

• Obtain open source software development kits (SDK's) and links to getting started guides and documentation that will provide a better developer experience to VMware Cloud on AWS features.

• Automation experts and DevOps engineers can seamlessly tie their business workflows into VMware Cloud with a selection of command line interfaces. Learn about the latest updates to the developer center by reading this blog post.

Which APIs are currently in preview?

The /networks resources and any APIs under this resource are currently marked as preview and may change in the future.

What are simple mode NSX API?

In VMware Cloud on AWS, NSX provides simplified consumption of the networking and security functionality - the set of NSX APIs related to this is referred to as simple mode NSX APIs. With these APIs, you can automate:

- Networking and security functions exposed in the VMware Cloud on AWS Console
- Day 0 tasks include establishing IPSec VPN tunnel, configuring firewall policies to allow vCenter access
- Day 2 tasks include creating a new logical switch, configuring firewall policies to allow access to the Internet, configuring DNS and NAT etc.

Customers can choose VMware Cloud on AWS endpoint over the public internet or NSX manager endpoint over private connection for automation.

Where can I find Software Development Kits (SDKs) and code samples for using the VMware Cloud on AWS Service APIs?

From within the VMware Cloud on AWS Console you will be able to access code samples and SDKs by using the Developer Center tab which has links to the supported SDK's and code samples made available from VMware and the community.

Third Party Technology Solutions

What are the terms of service for third party software and how is third party software supported on VMware Cloud on AWS?

Third party ISV software is handled on third party terms. The current certified list is located here

What additional VMware tools are available in VMware Cloud on AWS?

VMware makes the following optional downloadable tools available at no charge: DCLI and Content Onboarding Assistant. These tools are VMware Software that is governed by our standard EULA

How can I access third party content?

Access third party content through the VMware Solutions Exchange, but please note that not all solutions are directly integrated with VMware Cloud on AWS.

Can I bring my own third party software?

Yes. We don’t restrict what you can install, but they may not always be directly integrated with VMware Cloud on AWS.

From where can I acquire ISV licenses?

VMware Cloud on AWS operates on a Bring Your Own License (BYOL) model. You can procure your licenses through the channels you normally use or desire and utilize those licenses on dedicated VMware Cloud on AWS hosts.

How can I get access to VMware Cloud on AWS for development or testing?

With the latest release, VMware Cloud on AWS is available in 3 host and single host configurations. The single host configuration is ideal for for developing/testing own solutions or for customer POCs. Single host configurations have some limitations.

How can I get support for RedHat Enterprise Linux on VMware Cloud on AWS?

VMware Cloud on AWS is a RedHat Certified Cloud Service Provider that allows customers to bring their existing RedHat Enterprise Linux licenses to VMware Cloud on AWS. Please follow the guidance from RedHat on how to enable this here

How can I get support for RedHat OpenShift Container Platform on VMware Cloud on AWS?

VMware Cloud on AWS is a RedHat Certified Cloud Service Provider that allows customers to bring their existing RedHat OpenShift Container Platform licenses to VMware Cloud on AWS. Please follow the guidance from RedHat on how to enable this here.

VMware Tanzu

What is included in TKG?

TKG includes the core binaries to install a TKG cluster on VMware Cloud on AWS plus Customer Reliability Engineering support & services to assist customers in successfully planning, deploying and maintaining their Kubernetes environment. You can find a detailed list of technologies & services supported in TKG in KB 78173. Some relevant callouts are:

- Patching of critical issues prior to upstream releases
- vSAN Container Storage Interface (CSI)
- NSX Container Plugin (NCP)
- Calico 2.6 and above
- RHEL 7.4 for Node OS
- Ubuntu LTS 16.04 for Node OS
- Contour for ingress

Who is responsible for deploying and managing Tanzu services on VMware Cloud on AWS?

The first offering is a self-service model where Customers are responsible for deploying and managing all aspects of Tanzu on VMware Cloud on AWS. The workflows for deploying and managing TKG infrastructure are the same as those for on-premises. VMware is responsible for the management of SDDC software components and the IaaS infrastructure resources. A minimum of 2 ESXi hosts per cluster is required to use this model of Tanzu. Consult the latest Tanzu Kubernetes Grid Product documentation for more details.

The second offering is a full-managed and integrated model where Customers are responsible for providing and maintaining a basic collection of networks, which are used for deploying both Tanzu infrastructure as well as workloads. VMware is responsible for the management of the Tanzu infrastructure in addition to SDDC software components and the IaaS infrastructure resources. As part of this managed service, VMware also provides tighter integrations in the VMC Console as well as Tanzu Mission Control Essentials. As of VMware Cloud on AWS's 1.16 release, a minimum of 3 ESXi hosts per cluster is required to use this model of Tanzu. Consult Using VMware Tanzu™ Kubernetes Grid™ Service with VMware Cloud on AWS in the VMware Cloud Operations Guide for more details

What are the supported Operating Systems for Kubernetes nodes?

With VMware Tanzu, there are a number of supported operating systems that can be leveraged. Check out the Target Operating Systems section of the Tanzu documentation for the latest options.

Can customers use existing Enterprise PKS or PKS Essentials licenses for TKG on VMware Cloud on AWS deployment?

Existing Enterprise PKS or PKS Essentials do not entitle customers to run TKG on VMware Cloud on AWS. Customers will be required to purchase a TKG subscription license.

Where can I find more information about pricing for TKG on VMware Cloud on AWS?

All VMware Cloud on AWS customers are entitled to Tanzu services (i.e. Tanzu Kubernetes Grid and Tanzu Mission Control Essentials). For pricing on other tiers of Tanzu, Please contact your VMware representative.

How can customers get support for Tanzu on VMware Cloud on AWS?

Customers can get support for Tanzu Kubernetes Grid on VMware Cloud on AWS through a combination of VMware Cloud on AWS Support and Tanzu Support with a valid support contract for the product. For more details, please consult the "**How Do I Get Support**" section from the VMware Cloud Services Product Documentation.

How can I purchase Tanzu Application Service for VMware Cloud on AWS?

Tanzu Application Service is a separate purchase from your VMware Cloud on AWS subscription. Please contact your VMware Sales representative for more information on purchasing Tanzu Application Service licenses for VMware Cloud on AWS

I am currently using Tanzu Application Service in my on-premises datacenter, do I need a separate Tanzu Application Service license for VMware Cloud on AWS?

For deploying Tanzu Application Service on VMware Cloud on AWS you can use your existing license that you are using on-premises

Are there any prerequisites for running Tanzu Application Service on VMware Cloud on AWS?

There are no prerequisites for running Tanzu Application Service on VMware Cloud on AWS. The same technology foundation stack is supported on VMware Cloud on AWS

Do I need NSX-T on-premises to use Tanzu Application Service on VMware Cloud on AWS?

No, NSX-T deployment is not a prerequisite for using Tanzu Application Service on VMware Cloud on AWS.

In which regions is Tanzu Application Service on VMware Cloud on AWS supported?

Tanzu Application Service is supported on all VMware Cloud on AWS regions

How can I get support for Tanzu Application Service deployment on VMware Cloud on AWS?

You can continue to follow the existing Tanzu Application Service support model. On VMware Cloud on AWS, you can also leverage chat support available through VMware Cloud Console to open support tickets with VMware Global Support Services

Who is responsible for deploying and operating Tanzu Application Service on VMware Cloud on AWS?

As a VMware Cloud on AWS customer, you are responsible for deploying, operating and managing the lifecycle of Tanzu Application Service instances on VMware Cloud on AWS

Is there a sizing guideline between running TAS on-premises vs TAS on VMware Cloud on AWS?

You can continue to use the existing sizing guidelines for on-premises deployments for Tanzu Application Service on VMware Cloud on AWS

Can VMware HCX be used for migration of Tanzu Application Service instances to VMware Cloud on AWS?

VMware HCX live migrations are not supported for TAS migrations to VMware Cloud on AWS.

What is VMware Tanzu Mission Control?

VMware Tanzu Mission Control is a centralized Kubernetes management platform for operators to consistently, efficiently and securely manage Kubernetes clusters and applications across teams and clouds, while enabling developers with self-service access to information and resources needed for speedy application development and delivery.

It offers a rich set of capabilities, such as cluster lifecycle management, identity and access management, centralized policy management, centralized visibility across clusters, security and conformance inspection and data protection, to help increase operational efficiency and security while improving developer productivity.

How does Tanzu Mission Control work with VMware Cloud on AWS?

Tanzu Mission Control helps VMware Cloud on AWS customers to centrally operate and manage Kubernetes clusters running on VMware Cloud on AWS.

Any conformant Kubernetes clusters running on VMware Cloud on AWS can be attached and managed by Tanzu Mission Control, so that the Kubernetes operators can use the capabilities provided by the platform to gain the consistency, efficiency and security needed for managing the Kubernetes on VMware Cloud on AWS at scale.

If the customers use Tanzu Kubernetes Grid clusters in VMware Cloud on AWS, Tanzu Mission Control integrates with Tanzu Kubernetes Grid to also enable centralized lifecycle management of the Tanzu Kubernetes Grid clusters in VMware Cloud on AWS environment, including cluster provisioning, upgrading, scaling and deleting via Tanzu Mission Control UI, API and CLI (Note, this capability is not available to non-Tanzu Kubernetes Grid clusters).

What benefits does Tanzu Mission Control offer for VMware Cloud on AWS customers?

With Tanzu Mission Control, customers are able to significantly increase the operational efficiency of managing multiple Kubernetes clusters running in VMware Cloud on AWS environment, and also enhance the security and compliance of their Kubernetes infrastructure on top of VMware Cloud on AWS. In addition, Tanzu Mission Control enables developers with much easier self-service access to Kubernetes resources hence enhancing developer productivity and shortening the time-to-market.

Do I need to purchase Tanzu Mission Control separately when using it with VMware Cloud on AWS?

Yes, Tanzu Mission Control is sold separately.

Does VMware Tanzu Mission Control include Tanzu Kubernetes Grid?

No, Tanzu Mission Control does not include Tanzu Kubernetes Grid. However, VMware offers multiple Tanzu editions via which you can purchase Tanzu Mission Control and Tanzu Kubernetes Grid together. Check here for information about Tanzu editions.

How is VMware Tanzu Mission Control priced?

Tanzu Mission Control has two versions: Tanzu Mission Control Standard and Tanzu Mission Control Advanced. Tanzu Mission Control Standard can only be purchased via purchasing the Tanzu Standard edition. Tanzu Mission Control Advanced can be purchased either Standalone or via purchasing Tanzu for Kubernetes Operations. This feature comparison chart shows which features are included. For pricing details, please contact the VMware sales team.

Where can I learn more about Tanzu Mission Control?

To learn more about Tanzu Mission Control, please go to Tanzu Mission Control website.

What is the difference between the Tanzu standard and Tanzu services?

Tanzu Standard is a self-service model where Customers are responsible for deploying and managing all aspects of Tanzu on VMware Cloud on AWS. VMware remains responsible for managing the SDDC software components and the IaaS infrastructure resources

Tanzu Services is a full-managed and integrated model where Customers are responsible for providing and maintaining a basic collection of networks for Tanzu Workloads while VMware is responsible for the management of the Tanzu infrastructure in addition to SDDC software components and the IaaS infrastructure resources.

For more information, see Who is responsible for deploying and managing Tanzu services on VMware Cloud on AWS? under the FAQ section as well as the TechZone article

What is included in Tanzu Kubernetes Grid?

Tanzu Kubernetes Grid includes the core binaries to enable and install Tanzu Services on a cluster in VMware Cloud on AWS as well as Tanzu support & services to assist customers in providing break-fix support for their Kubernetes environment. You can find a detailed list of technologies & services supported in the Tanzu Kubernetes Grid documentation.

VMware Horizon on VMware Cloud on AWS

What is Horizon on VMware Cloud on AWS?

VMware Horizon on VMware Cloud on AWS delivers a seamlessly integrated hybrid cloud for virtual desktops and applications. It combines the enterprise capabilities of VMware's Software-Defined Data Center, delivered as a service on AWS, with the market leading capabilities of VMware Horizon - for a simple, secure and scalable solution.

Where can I find more information on Horizon on VMware Cloud on AWS?

You can find overview information on our Horizon website. You can also read our announcement blog and our preview blog. A recorded demo video is available here.

Which version of Horizon will support VMware Cloud on AWS?

Full Clone desktop pool and manual RDSH farms will be supported starting with Horizon 7.5 and onwards. We are working towards additional support options.

Will Horizon on VMware Cloud on AWS be at feature parity with Horizon on-premises?

The Horizon architecture is exactly the same whether it's running on-premises or on VMware Cloud. However, there are certain Horizon features we do not plan to support on VMware Cloud on AWS: • View Composer / Linked Clones o This applies to both Linked Clone VDI pool as well as Linked Clone RDSH farms. Customers using Linked Clones on-premises will be asked to use Instant Clones on VMware Cloud. Mixing and matching two CPA Pods where the on-premises Pod has Linked Clones and VMware Cloud Pod has Instant Clones will be supported • Content-Based Read Cache (CBRC) o Given the profile of the storage used in VMware Cloud on AWS hardware, CBRC does not add much benefit • Security Server o Use UAG instead • Unmanaged desktops • Manual desktop pools o Note: Manual RDSH farms will be supported • Persona Management ThinApp • Mirage • Fusion • Workstation

When deploying Horizon across both on-premises and VMware Cloud on AWS in CPA configuration, does the Horizon version on-premises have to match the Horizon version on VMware Cloud on AWS?

No that is not necessary. As long as the version of Horizon running on-premises is v7.0 and above, it can be put into the same CPA configuration as a Horizon running on VMware Cloud on AWS.

Who is responsible for deploying and managing Horizon infrastructure on VMware Cloud on AWS?

You are responsible. The workflows of deploying and managing Horizon infrastructure is the same as on-premises. SDDC infrastructure and hardware management is the responsibility of VMware.

Is Horizon part of VMware Cloud on AWS?

No. Horizon is software that can be deployed by you on the IaaS (infrastructure-a-Service) VMware Cloud on AWS. Ultimately you will be responsible for their Horizon infrastructure, even though your SDDC infrastructure will be managed by VMware.

In what regions is Horizon on VMware Cloud on AWS available?

Horizon on VMware Cloud on AWS is available in all the same regions that VMware Cloud on AWS is available.

What is the difference between Horizon on VMware Cloud on AWS and Horizon Cloud?

The biggest difference is the management model. Horizon on VMware Cloud on AWS is an IaaS model where only the cloud platform/SDDC is fully managed and you must manage your own Horizon infrastructure as well as RDSH farms and desktop pools. For Horizon Cloud, you only have to manage RDSH farms and desktop pools. Horizon Cloud infrastructure as well as the cloud platform/SDDC are fully managed. A significant advantage of Horizon on VMware Cloud on AWS is that it is the same architecture as the Horizon on-premises deployment, and the two can be linked by CPA. For existing on-premises customers who want to build a hybrid VDI cloud, extending Horizon to VMware Cloud on AWS is very easy. Horizon is more customizable than Horizon Cloud. A good example is the desktop model, for example, vCPU and vRAM per VM. With Horizon, you can have any configurations of the vCPU and vRAM. On Horizon Cloud, it is standardized on a limited number of configurations. If you require extensive customized options, you may want to start with Horizon on VMware Cloud on AWS.

Can Horizon also be deployed on VMware Cloud on AWS stand-alone? What are the other ways I can deploy this solution?

Yes. There are two ways you can deploy: • Deploy one or more Horizon pods on VMware Cloud on AWS. You can choose to link them together using CPA (or not). • Deploy one or more Horizon pods on VMware Cloud on AWS and deploy one or more Horizon pods on-premises. You can choose to link them together using CPA (or not).

What is the licensing requirement for Horizon on VMware Cloud on AWS?

There are two main cost components to a Horizon on VMware Cloud on AWS deployment. The first component is the cost of VMware Cloud on AWS infrastructure service. List prices are posted online. The second component is the Horizon license, which is a separate charge from VMware Cloud on AWS. Given that this is a cloud deployment, customers are required to use subscription licenses. There are currently two available options for purchasing Horizon subscription licenses. 1) Workspace ONE Enterprise Subscription License For customers looking for a full digital workspace solution, including Horizon, they can purchase Workspace ONE Enterprise or Workspace ONE Enterprise for VDI. Workspace One Enterprise entitles customers to Workspace ONE Advanced, Workspace One Intelligence, and Horizon Apps. For Horizon customers, this unlocks the RDSH use case. Workspace ONE Enterprise for VDI adds the VDI use case on top of the Workspace ONE Enterprise. In order to use these licenses, the customer would have to connect to cloud vIDM (VMware Identity Manager). 2) Horizon Subscription License Horizon subscription licenses are also available for customers who only want to deploy and pay for Horizon. All subscription licenses can be used for both cloud deployments as well as on-premises deployments.

Can I use existing Horizon perpetual licenses for a Horizon on VMware Cloud on AWS deployment?

Horizon perpetual licenses do not entitle you to run Horizon on VMware Cloud on AWS. You will be required to purchase a Horizon subscription license or Workspace ONE Enterprise subscription license in order to run Horizon on VMware Cloud on AWS.

How do I install Horizon on VMware on AWS?

The installation of Horizon on VMware on AWS is similar to installing Horizon on-premises. More details will be provided in the Horizon 7.5 product documentation.

What are my options for integrating with my enterprise’s AD?

We recommend that you deploy an Active Directory server in your VMware Cloud on AWS environment, and link it with your on-premises Active Directory. While you can certainly extend your on-premises Active Directory to your Horizon on VMware Cloud on AWS deployment, the latency may be unacceptable.

How many desktops can I run on a VMware Cloud on AWS host?

Each host has 2 CPUs, 36 cores, 512GB RAM, NVMe attached flash storage (3.6 TB cache plus 10.7 TB raw capacity tier). How many VMs you can run on the host will depend on the configuration of each VM. For detailed sizing, please refer to the VMware Cloud on AWS Sizer.

What is Horizon Smart Provisioning for VMware Cloud on AWS?

Instant Clones has been enhanced to support Smart Provisioning. Smart Provisioning is the ability for Horizon to choose the best way to provision an instant clone, depending on the environment. In certain cases, instant clones are provisioned to optimize for the speed of clone creation by creating and leveraging parentVMs on each host. In other cases, when speed is not paramount, they can be provisioned in a way that does not require parentVMs, thus freeing up more host memory for desktop workloads. Horizon can seamlessly choose one method or another without the administrator’s involvement, sometimes even in the same pool. This capability makes resource usage even more efficient on VMware Cloud on AWS.

VMware Cloud Marketplace

What is the VMware Cloud Marketplace?

VMware Cloud Marketplace enables VMware customers to discover and deploy validated third-party and open-source solutions on VMware environments such as VMware Cloud on AWS.

Can you purchase third-party solutions on VMware Cloud Marketplace?

No, not at this time. Currently, VMware Cloud Marketplace enables the use of third-party solutions in a bring-your-own-license (BYOL) model. While users will be able to search for, browse, and filter for a third-party solution in the Marketplace catalog, they would need to already have the license key from the third-party vendor in order to utilize commercial third-party solutions on the SDDC(s) of their choice.

How does VMware Cloud Marketplace relate to VMware Solutions Exchange (VSX)?

VSX is a repository of technology solutions that complement, integrate or interoperate with VMware's portfolio of products. On the other hand, VMware Cloud Marketplace is an engineered, curated and managed marketplace where users can discover and enable deployment of third-party and open-source solutions directly from their VMware platform environment. We are working on unifying the two portals

How does VMware ensure that third-party solutions on VMware Cloud Marketplace are validated to work on VMware Cloud on AWS?

All deployable third-party solutions on VMware Cloud Marketplace must receive certifications appropriate for the VMware platform on which they are validated. All of our third-party solutions validated on VMware Cloud on AWS have received either the "Partner Ready" for VMware Cloud on AWS certification and/or the "VMware Ready" certification

How can I learn more about VMware Cloud Marketplace?

For more information on VMware Cloud Marketplace, please visit our website here.

Is VMware Cloud Marketplace specifically designed for VMware Cloud on AWS?

No. VMware Cloud Marketplace is intended to integrate with all VMware platforms. Currently, the Marketplace is integrated with VMware Cloud on AWS as well as four other VMware platforms. Further integrations are planned.

VMware Cloud on AWS GovCloud (US)

What is VMware Cloud on AWS GovCloud (US)?

VMware Cloud on AWS GovCloud (US) is a jointly engineered secure, scalable cloud service that brings VMware’s rich Software-Defined Data Center software to the AWS GovCloud (US) Region. VMware Cloud on AWS GovCloud (US) integrates VMware's compute, storage and network virtualization products (VMware vSphere, VMware vSAN and VMware NSX) along with VMware vCenter Server management, optimized to run on dedicated, elastic, bare-metal AWS infrastructure. With the same architecture and operational experience on-premises and in the cloud, IT teams can now quickly derive instant business value from use of the AWS and VMware hybrid cloud experience.

Who can use VMware Cloud on AWS GovCloud (US)?

VMware Cloud on AWS GovCloud is only accessible to vetted U.S. entities and root account holders who must confirm they are U.S. Persons to gain access to these regions. VMware Cloud on AWS GovCloud customers and partners must obtain an AWS GovCloud account from AWS in order use this instance of the VMware service.

Does the VMware Cloud on AWS GovCloud (US) service have a FedRAMP Authority to Operate (ATO)?

No. VMware Cloud on AWS GovCloud (US) does not currently have a FedRAMP ATO. We are pursuing a FedRAMP High ATO and expect to obtain it around the middle of 2019.

What is FedRAMP?

The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

What is FedRAMP Ready?

This designation indicates that a Third Party Assessment Organization (3PAO) attests to a Cloud Service Provider’s (CSP) readiness for the authorization process, and that a Readiness Assessment Report (RAR) has been reviewed and approved by the FedRAMP PMO. The 3PAO (auditor) reviews the implementation of the top 100 most critical security controls that a CSP is required to implement to achieve a FedRAMP ATO. While becoming FedRAMP Ready is not a guarantee that a CSP will become authorized, achieving FedRAMP Ready status provides a greater likelihood of success in the authorization process as the government has a clearer understanding of a CSP’s technical capabilities.

Is VMware Cloud on AWS GovCloud (US) FedRAMP Ready?

Yes, VMware Cloud on AWS GovCloud (US) is FedRAMP Ready.

What does In-Process High mean? Is the VMware Cloud on AWS GovCloud (US) now FedRAMP In-Process High?

An In-Process designation indicates that a CSP is actively working on the documentation required to achieve a FedRAMP Authorization and that an agency is reviewing that documentation with the intent to provide an ATO. FedRAMP introduced their High Baseline to account for the government’s most sensitive, unclassified data in cloud computing environments, including data that involves the protection of life and financial ruin. Yes. VMware Cloud on AWS GovCloud (US) is now FedRAMP In-Process High with United States Marshals Service as the Agency sponsor.

Is the VMware Cloud on AWS GovCloud (US) listed on the FedRAMP.gov marketplace?

Yes – please visit the marketplace.

Can Federal Agencies run production workloads on VMware Cloud on AWS GovCloud (US)?

Federal, State and Local Agencies and healthcare providers, educational institutions etc. can run production workloads on VMware Cloud on AWS GovCloud (US). They must each evaluate the risk of using the service and determine that VMware has sufficient security in place to support their security requirements of their workloads. Federal Agencies have determined that a Cloud Service with a FedRAMP Ready designation is sufficiently secure and will elect to run specific production workloads on a service with this status.

What is the difference between FedRAMP High ATO and FedRAMP Moderate ATO?

Moderate Impact systems account for nearly 80% of CSP applications that receive FedRAMP authorization and is most appropriate for CSOs where the loss of confidentiality, integrity, and availability would result in serious adverse effects on an agency's operations, assets, or individuals. Serious adverse effects could include significant operational damage to agency assets, financial loss, or individual harm that is not loss of life or physical. High Impact data is usually in Law Enforcement and Emergency Services systems, Financial systems, Health systems, and any other system where loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. FedRAMP introduced their High Baseline to account for the government's most sensitive, unclassified data in cloud computing environments, including data that involves the protection of life and financial ruin. VMware Cloud on AWS GovCloud (US) is pursuing a FedRAMP High ATO.

Does VMware Cloud on AWS GovCloud (US) plan to build a FedRAMP Moderate offering?

At this time, VMware is evaluating the demand for a FedRAMP Moderate offering running on AWS GovCloud US East/West.

What other certifications is VMware Cloud on AWS GovCloud (US) pursuing?

VMware plans to pursue a Provisional Authority from the Defense Information Systems Agency (DISA) to run Impact Level (IL) 4/5 workloads, we plan to complete its U.S. International Traffic in Arms Regulation (ITAR) training and ensure ITAR compliance and we expect that we will leverage our FedRAMP efforts to comply with Criminal Justice Information Services (CJIS).

Is VMware Cloud on AWS GovCloud (US) operated by US Persons on U.S. soil?

Yes, VMware Cloud on AWS GovCloud (US) is operated by VMware employees who are U.S citizens on U.S soil.

What Service Level Agreements does the VMware Cloud on AWS GovCloud (US) service support?

The VMware Cloud on AWS service is expected to be highly available, however Service Level Agreements (SLAs) are not guaranteed until General Availability. At General Availability, it is expected that the SLAs will match the commercial service.

Why should I use VMware Cloud on AWS GovCloud (US)?

VMware Cloud on AWS GovCloud (US) provides a consistent and interoperable infrastructure and services between VMware-based data centers and the AWS cloud, which minimizes the complexity and associated risks of managing diverse environments. VMware Cloud on AWS GovCloud (US) offers native access to AWS services and innovation that extends the value of enterprise applications over their lifecycle. With the same architecture and operational experience on-premises and in the cloud, IT teams can now quickly derive instant business value from use of the AWS and VMware hybrid cloud experience.

Where is VMware Cloud on AWS GovCloud (US) available today?

The service is available exclusively in AWS GovCloud (US-West). VMware expects to make the service available in AWS GovCloud (US-East) based on customer demand.

What are the features included in VMware Cloud on AWS GovCloud (US)?

Please visit the VMware Cloud on AWS GovCloud page for the most comprehensive and updated feature list.

Can workloads running in a VMware Cloud on AWS GovCloud (US) instance integrate with AWS services?

Yes. VMware Cloud on AWS GovCloud (US) SDDC is directly connected to your VPC using Elastic Network Interface (ENI) and therefore has access to AWS services. Virtual machine workloads can access public API endpoints for AWS services such as AWS Lambda, Amazon Simple Queue Service (SQS), Amazon S3 and Elastic Load Balancing, as well as private resources in the customer's Amazon VPC such as Amazon EC2, and data and analytics services such as Amazon RDS, Amazon DynamoDB, Amazon Kinesis and Amazon Redshift. Customers can now enjoy the newest generation of VPC Endpoints designed to access AWS services while keeping all the traffic within the AWS network.

How do I sign up for the VMware Cloud on AWS GovCloud(US) service?

Please contact your VMware account team or VMware partners for more information.

How does VMware protect customer data in VMware Cloud on AWS GovCloud (US)?

VMware Cloud on AWS GovCloud (US) is designed with multiple layers of protection. The service inherits the physical and network security controls from the AWS infrastructure and adds dedicated compute and storage along with the security capabilities derived from vSphere, vSAN and NSX. The VMware Cloud on AWS GovCloud (US) infrastructure is monitored 24x7 and regularly tested for security vulnerabilities and hardened to enhance security.

How is Data Encrypted on VMware Cloud on AWS GovCloud (US)?

All data-in-transit between the customer site and the service can be transmitted over a Direct Connect and/or encrypted via VPN. Data at rest is encrypted by VMware vSAN encryption which is FIPS 140-2 compliant and leverages the FIPS 140-2 compliant AWS KMS service. VMware vSAN stores customer data on local self-encrypting NVMe Drives.

What VMware SDDC products do I need to have on-premises for VMware Cloud on AWS GovCloud (US)?

The more software-defined you are with VMware technologies on-premises, the more value you can derive out of VMware Cloud on AWS GovCloud (US). However, you can still move workloads to and from VMware Cloud on AWS GovCloud (US) by doing cold migrations of the VMs. No conversion or modification is required. You can also just run VMware Cloud on AWS GovCloud (US) standalone with only a web browser.

How is VMware Cloud on AWS GovCloud (US) deployed?

VMware Cloud on AWS GovCloud (US) infrastructure runs on dedicated, single tenant host clusters within a dedicated AWS VPC associated with a single AWS account. Clusters can range from a minimum 2 hosts up to a maximum of 16 hosts per cluster. A single VMware vCenter server is deployed within each SDDC environment.

How do I manage resources on VMware Cloud on AWS GovCloud (US)?

You can use the same management tools you use today. A vCenter Server instance is deployed as part of every VMware Cloud on AWS GovCloud (US) SDDC. You may connect to this vCenter Server instance to manage their VMware Cloud on AWS GovCloud (US) clusters. A VMware Cloud Web Console is provided which allows for common tasks such as add/remove hosts, configure firewalls and other basic networking settings. It is important to note that tools that require plug-ins or extensive vSphere permissions may not function properly in VMware Cloud on AWS GovCloud (US). VMware Cloud on AWS GovCloud (US) uses a least privilege security model in which the customer (and therefore their tools) do not have full administrative access.

Can I migrate existing vSphere VMs to my VMware Cloud on AWS GovCloud (US) deployment?

Yes. There are multiple ways to migrate existing vSphere VMs to VMware Cloud on AWS GovCloud (US) such as cold migration, live migration of vSphere VMs via vMotion etc.

How can I purchase the VMware Cloud on AWS GovCloud (US) service?

VMware Cloud on AWS GovCloud (US) is available on-demand or in 1-year and 3-year subscriptions. Please contact your VMware account team or VMware partners for more information.

How will customers be charged for this service?

This service is delivered, sold and supported by VMware and VMware will send you a bill each month. You will get a single bill that includes the total charges for using the VMware Cloud on AWS GovCloud (US) service including the VMware SDDC software and the underlying AWS resources. Note that for any AWS GovCloud (US) resources that you directly provision using an AWS Console or AWS API (i.e., without using VMware management, APIs or orchestration tools), will be billed directly through your AWS account.

How is VMware Cloud on AWS GovCloud (US) priced?

VMware Cloud on AWS GovCloud (US) is available on-demand or in 1-year and 3-year subscriptions.

Do 1-year and 3-year subscriptions auto-renew at the end of the term?

No, subscriptions do not auto-renew. You are free to purchase additional subscriptions at any time. Any workloads running at the end of the subscription term will be billed at an on-demand rate.

Who delivers billing and support for VMware Cloud on AWS GovCloud (US)?

VMware will sell, deliver and support VMware Cloud on AWS GovCloud (US). Billing for the VMware Cloud on AWS GovCloud (US) service will be directly billed to you by VMware. You will only receive a bill from AWS directly for AWS native services used in your own AWS accounts.

Do I also need to purchase AWS Support for VMware Cloud on AWS GovCloud (US) service?

No, VMware Cloud on AWS GovCloud (US) is supported by VMware. However, you can choose to purchase AWS support for the additional AWS services you use that are not provided by VMware Cloud on AWS GovCloud (US).

Will I need an AWS GovCloud (US) account for VMware Cloud on AWS GovCloud (US) service?

Yes, you will need an active AWS GovCloud (US) customer account that will be linked to the VMware Cloud on AWS GovCloud (US) service. If you don't have an existing AWS GovCloud customer account, you will be asked to create one as part of the onboarding process. One of the key benefits of this offering is seamless integration with other AWS services such as Amazon S3, Redshift and other Amazon EC2 instances. VMware will bill you for what you use in the VMware Cloud on AWS GovCloud (US) and separately, AWS will bill the customer for any AWS services they use within their own AWS GovCloud (US) account.

What storage options are available for VMware Cloud on AWS GovCloud (US)?

VMware Cloud on AWS GovCloud (US) includes VMware's vSAN storage technology that provides a single name space shared datastore (vSAN datastore) for VM storage. Each SDDC cluster will utilize an "all flash" vSAN storage solution built on NVMe backed instance storage that offers high performance, and low latency.

Can I use AWS Elastic File System (EFS) volumes as vSphere datastores?

Yes, you can mount Amazon EFS to their VMware VM's running on VMware Cloud on AWS GovCloud (US).

Is data encrypted on vSAN storage?

Yes, data is encrypted at rest by vSAN Encryption and again on each self-encrypting NVMe flash device backing the vSAN datastore in each host.

How does data at rest encryption work in VMware Cloud on AWS GovCloud (US)?

Customer data at rest will be natively encrypted by vSAN. vSAN will use AWS Key Management Service (KMS) to generate the Customer Master Key (CMK). While CMK is acquired from AWS, two additional keys are generated by vSAN. Those keys are an intermediate key, referred as Key Encryption Key (KEK) and Disk Encryption Key (DEK). The CMK wraps the KEK and the KEK in turn wraps the DEK. The CMK never leaves AWS control. Encryption and decryption of the KEK is offered via standard AWS API call. One CMK and one KEK is required per cluster and one DEK for every disk in the cluster.

What provisions are available to rotate the keys?

You have the option to change the KEK (Key Encryption Key) either through vSAN API or through the vSphere UI. This process is called rekey. Note, shallow rekey doesn't change the Disk Encryption Key (DEK) or the Customer Master Key (CMK). Changing the DEK and CMK is not supported. In rare situations, if there is a need to change the DEK or CMK, users have the option to set up a new cluster with new CMK and can Storage vMotion the data from existing cluster.

Can I turn on or turn off vSAN encryption selectively?

Similar to D&C (Deduplication & Compression), vSAN encryption at rest cannot be turned on or off for individual clusters. It is a cluster-wide setting that is always on by default when a cluster is provisioned in the SDDC.

Are there other options for customers to bring their own keys?

For vSAN encryption, the Customer Master Key (CMK) is sourced from AWS Key Management Service and this is the only option available. Customers may run any security or encryption software they choose within the guest operating systems and use their own keys and KMI to manage the in-guest software.

How are VMware Cloud on AWS GovCloud (US) SDDCs connected to my on-premises environment?

When you deploy an SDDC using VMware Cloud on AWS GovCloud (US), it is configured with two networks: a management network and a compute network. The management network handles network traffic for the SDDC hosts, vCenter Server, NSX Manager, and other management functions. The compute network handles network traffic for your workload VMs. Two VMware NSX edge devices serve as gateways for the VMware virtualized networking environment. The Management Gateway (MGW) connects the SDDC management infrastructure to your on-premises environment. The Compute Gateway (CGW) provides connectivity for all workload virtual machines. Traffic can be directed to your on-premises environment using a L3 VPN connection or to your AWS VPC via an Elastic Network Interface (ENI).

Security and Privacy

What Personally Identifiable Information (PII) is collected by VMware Cloud on AWS and how is it used?

The only Personally Identifiable Information (PII) that the VMware Cloud on AWS service collects is the customer administrators' first name, last name, email address and IP address. This information is required in order to operate the VMware Cloud on AWS service and for security and support purposes - e.g. logging who created/deleted an SDDC, added/removed a host, changed a firewall rule, copied a virtual machine, etc. The PII collected by the VMware Cloud on AWS service is used exclusively for the purposes outlined in the VMware Products and Services Privacy Notice. VMware may require additional account information to be provided in connection with the creation or administration of a customer account, including names, usernames, phone numbers, email addresses, and billing information. This is managed by VMware back office systems and VMware handles account information in accordance with our Privacy Notice.

What is Customer Content?

Customer Content is any content you, as a customer, upload into a Service Offering as further specified in the VMware Cloud Service Offerings Terms of Service. This includes all text, sound, video, or image files, and software (including machine images), or other information that you or any of your end users upload into the VMware Cloud on AWS service for processing, storage, or hosting in connection with your account with us. Account information, including names, usernames, phone numbers, and billing information associated with your account, is not included in the definition of “Customer Content”, nor is any information we collect in connection with your use of the service. VMware will handles account information in accordance with our Privacy Notice.

Who owns Customer Content?

You always retain ownership of your Customer Content. VMware will not access or use your Customer Content for any purpose except as necessary to provide the VMware Cloud on AWS Service to you and as set forth and permitted in our Terms of Service with you.

Where is "Customer Content" physically located?

VMware Cloud on AWS is deployed in AWS data centers in multiple regions throughout the world. You select the AWS region where your SDDC will be deployed, and your Customer Content will persist in that data center.

How does VMware protect "Customer Content"?

VMware maintains an information security management program that is aligned with the ISO 27001 standard (as applicable), which is reviewed at least annually to ensure appropriate controls, practices and procedures are in place.

What is "Service Operations Data" and "Usage Data"?

Service Operations Data and Usage Data is information VMware collects in connection with the provisioning and delivery of the VMware Cloud on AWS service. It includes information from VMware’s software or systems hosting the service, and from the customer systems, applications and devices that are used to access the service. The Service Operations Data is used to facilitate the delivery of the service to customers, including managing and monitoring the infrastructure, and providing support, and the Usage Data is used for VMware’s own analytics and product improvement purposes. The data collected is generally technical information, with limited individually identifying information such as email address, IP/MAC address of the VMware Cloud on AWS administrator's devices, and identifiers (including cookies). The information may include the following types of data: Account Information: Information that a customer provides to us in connection with the creation or administration of a customer account, including names, usernames, phone numbers, email addresses, and billing information. Configuration Data: Technical data about how a customer organization has configured VMware Cloud on AWS and related environment information. Feature Usage Data:

Feature usage data relates to how a customer organization uses VMware Cloud on AWS features. Authentication Data: Information that is used to provide access to the Services, such as username and passwords (for local authentication only). Performance Data: Performance data relates to how the VMware Cloud on AWS Services are performing. Examples include metrics of the performance and scale of the Services, response times for user interfaces and API calls. Service Logs: Service logs are automatically generated by the Services. Typically, these logs record system events and state during the operation of the Services in a semi-structured or unstructured form. Security Logs: Security logs come from multiple sources including Intrusion Detection and Prevention Software (IDS/IPS), firewalls, vulnerability scanners, file Integrity monitoring systems, anti-virus solutions, access control systems, vSphere, and AWS Infrastructure. Diagnostic Information: Diagnostic information may be contained in log files, event files and other trace and diagnostic files. Support Data: Support data relates to information that has been provided by a customer to VMware or is otherwise processed in connection with support facilities such as chat and service support tickets. Survey Data: Survey data relates to a customer's Net Provider Score ("NPS") and other similar in-Service surveys or feedback in relation to a customer's use of the relevant Services. The main difference between Usage Data and Services Operations Data are the purposes for which we use the data. When collecting both Usage Data and Services Operations Data, we always aim to collect the minimum amount of personal information necessary to fulfill these respective purposes.

Where is "Service Operations Data" and "Usage Data" physically located?

The Service Operations Data and the Usage Data, including customer SDDC configuration information, persists in the AWS US-West (Oregon) data center location, but may be replicated to other AWS regions to ensure availability of the VMware Cloud on AWS service.

Where can the "Service Operations Data" and "Usage Data" be accessed from?

This information may be accessed by engineering, operations or support teams distributed globally.

How long does VMware retain "Service Operations Data" and "Usage Data"?

VMware retains information that we collect in connection with the customer's use of the VMware Cloud on AWS service for as long as is needed to fulfill the obligations of the VMware Cloud on AWS Terms of Service or where we have another business or legal reason to do so. When we have no justifiable business need to process this information, we will either delete or anonymize it, or, if this is not possible (for example, because the information has been stored in backup archives), then we will securely store the information and isolate it from any further processing until deletion is possible.

Is the "Service Operations Data" and "Usage Data" aggregated and anonymized?

VMware Cloud on AWS provisions a Software Defined Data Center for each customer. This architecture requires that VMware retains the Service Operations Data and Usage Data from the dedicated environments in its original form with identifying customer and user information such as Org ID, SDDC ID, and email address of the administrator who added a host or changed a firewall rule. The non-aggregated data is only used by VMware for the purposes outlined in the VMware Products and Services Privacy Notice. Unless explicit permission is granted to VMware by the customer, Service Operations Data and Usage Data is never shared outside of VMware, its affiliates and suppliers without being anonymized and aggregated e.g, "215 customers are using this feature", or "4 customers have experienced this problem".

How does VMware Cloud on AWS comply with the EU General Data Protection Regulation (GDPR)?

Under the EU General Data Protection Regulation ("GDPR"), VMware is the "processor" with respect to any Personal Data that may be contained within the Customer Content. VMware's obligations and commitments as a processor under GDPR are set forth in VMware's Data Processing Addendum. VMware has achieved Binding Corporate Rules ("BCR") approval for Personal Data it processes. Evidence of approval of VMware's BCRs is available on the European Commission's website.

How does VMware Cloud on AWS comply with the California Consumer Privacy Act (CCPA)?

The California Consumer Privacy Act (“CCPA”), which comes into effect on January 1, 2020, applies to businesses that provide services to consumers in California. It gives individuals certain rights regarding the processing of their personal data. Under the CCPA, VMware acts as a “service provider” with respect to any Personal Data contained within Customer Content, and we will not access or use the Customer Content for any purpose except as necessary to provide the VMware Cloud on AWS service, and as set forth and permitted in our Terms of Service. VMware will assist you, as a customer, in responding to data subject access requests under the CCPA as set forth in our Data Processing Addendum.

What sub-processors does VMware Cloud on AWS use?

VMware Cloud on AWS utilizes other companies to provide certain services on its behalf. The list of sub-processors who may process Customer Content (as defined in the Terms of Service) are listed in our VMware Cloud on AWS Sub-Processors list. As set forth in the Data Processing Addendum, VMware has adequate data transfer mechanisms in place with each sub-processor. There are currently two categories of companies on this list of sub-processors. The first category is the cloud infrastructure provider which manages the physical hardware used to deliver the cloud service. Since Customer Content physically resides on hardware operated by the third-party infrastructure provider, that party qualifies as a sub-processor even though there are no circumstances where the infrastructure provider actually accesses Customer Content. The second category of sub-processors provides supporting functionality for the VMware Cloud on AWS service (e.g., in-product chat, CRM/Customer Success Management, customer surveys, etc.). None of these companies ever have access to Customer Content unless the customer explicitly enters or uploads screenshots containing sensitive information (passwords, Personally Identifiable Information (PII), Personal Health Information (PHI), credit card numbers, etc.) into these product interfaces. In most cases this would be considered Confidential Information, but VMware's privacy team has taken a very conservative approach and has identified this category of service providers as sub-processors in order to ensure that our customers have complete transparency and the most stringent privacy protections. If you would like to receive notification of updates to this sub-processor list, please register here. Notifications are sent at least 60 days prior to the changes taking effect unless the customer have the ability to choose to use a new feature powered by the sub-processor (e.g., a new AWS region becomes available), in which case the VMware Cloud on AWS Sub-Processor list is updated concurrently with the release of the new feature.

What compliance certifications and attestations does VMware Cloud on AWS have?

VMware is committed to delivering a cloud service that meets a comprehensive set of international and industry-specific security and compliance standards. VMware adheres to very rigorous secure development and operational standards and actively conducts third-party audits in order to expand the list of certifications, attestations and adoptions of frameworks. The current list of certifications and attestations that the VMware Cloud on AWS service has achieved is published here. Compliance certificates and auditor's reports not published on this page can be obtained from your VMware account representative.

How does VMware Cloud on AWS segregate customers' environments?

VMware Cloud on AWS has three independent and comprehensive isolation layers in place to segregate customers' environments. A Software Defined Data Center (SDDC) is deployed in a dedicated AWS Virtual Private Cloud (VPC) that is owned by an AWS Account created exclusively for the customer. Amazon Accounts and Amazon VPC's are the mechanisms implemented by AWS to logically isolate sections of the AWS Cloud for each customer. Each SDDC is deployed on dedicated bare metal hardware - providing physical isolation between customers' environments. Dedicated hardware means that customers do not share the physical processor, memory or storage with anyone else. VMware vSphere is deployed in each SDDC which allows customers to logically isolate their Customer Content by creating resource pools and configuring vSphere permissions to control who has access to Customer Content within their own organization.

What is a "Shadow Account" or "Shadow VPC"?

A Software Defined Data Center (SDDC) is deployed in a dedicated AWS Virtual Private Cloud (VPC) that is owned by an AWS Account created by the VMware Cloud on AWS service exclusively for the customer. Amazon Accounts and Amazon VPC's are the mechanisms implemented by AWS to logically isolate sections of the AWS Cloud for each customer. The customer dedicated Account and VPC is referred to as the Shadow Account or Shadow VPC. A single Shadow Account can hold multiple SDDCs across all AWS regions where the VMware Cloud on AWS service is offered. Upon termination of the customer's VMware Cloud on AWS account, all resources held in the Shadow Account will be released and the Shadow Account is retired from use.

What is Account Linking?

In order to allow the SDDC to access resources in a customer’s existing AWS account (and vice versa), VMware employs a workflow called Account Linking that grants the VMware Cloud on AWS service limited permissions in a customer’s account to help select the optimal deployment zone(s), set up cross-account networking via Cross-Account ENIs (X-ENI), and update route table information. This is done via a template-based workflow that allows the customer to grant these permissions in a few clicks. The set of permissions is maintained by an AWS-controlled policy, with cross-account access granted via role assumption from specific VMware Cloud on AWS accounts.

Is Account Linking Required?

Account linking is required. One of the major benefits of using VMware Cloud on AWS is the access to native AWS services (EBS, RDS, Lambda etc.). Linking accounts early in the provisioning processes ensures that a VMware Cloud on AWS account has been configured correctly to enable access to native AWS services before workloads are migrated and created and configuration changes become more difficult.

Is my data Encrypted at Rest?

VMware Cloud on AWS provides customers with multiple layers of encryption to protect their Content. Self-Encrypting Drives The i3.metal, i3en.metal and i4i.metal instances used by VMware Cloud on AWS each contain eight local self-encrypting NVME drives. The Self-Encrypting Drives (SED) use AWS 256-bit XTS encryption and the keys for these drives are securely generated by the firmware on the drive itself. This process is handled by the AWS API interface that VMware calls when allocating or de-allocating hosts to a cluster. Encryption keys are generated in the SED controller and they never leave the drive. Whenever a host machine is removed from a cluster the data encryption keys used by the self encrypting drives are destroyed. This cryptographic erasure ensures that there is no Customer Content on the drives before returning the server to the pool of available hardware. VMware vSAN Encryption VMware Cloud on AWS utilizes VMware vSAN for all Content storage. VMware vSAN is a software-defined storage (SDS) product developed by VMware that pools together direct-attached storage devices across a VMware vSphere cluster to create a distributed, shared data store. VMware vSAN implements storage protection policies to ensure data is tolerant to the failure of one or more physical drives and hosts in a cluster. VMware vSAN also de-duplicates, compresses and encrypts data. vSAN Encrypts data with an XTS AES 256 cipher using Intel AES-NI hardware acceleration, in both the cache and capacity tiers of vSAN datastores. VMware has integrated VMware vSAN with the AWS Key Management Service, (KMS) to provide customers with a highly secure, highly-available and cost-effective method of generating encryption keys. The AWS KMS service uses FIPS 140-2 validated hardware security modules (HSMs) to protect the confidentiality and integrity of all customer keys. Whenever desired, VMware Cloud on AWS customers can rotate the key encryption keys through the vSAN API or the vSphere user interface. In-Guest Encryption Customers may also choose to implement encryption or security software within their guest operating system or applications. This enables a customer to use the same security software they use in their own data centers and utilize their own Key Management Infrastructure.

Is my data Encrypted in Transit?

All access to the VMware Cloud on AWS console and the VMware Virtual Center Web Client is protected using TLS 1.2. Connection to these interfaces via all earlier protocols has been disabled. All data to and from VMware Cloud on AWS and the customer's data center can be encrypted via an IPSec VPN. In the VMware Cloud on AWS Console, the customer is can configure either a Policy-Based or Route-Based VPN. The default encryption mechanism is AES-256. and the customer is in control of the pre-shared keys. VMware Cloud on AWS has enabled Encrypted vMotion by default for all migrations of a virtual machine between hosts within an SDDC. Encrypted vMotion relies on the AES-GCM (Advanced Encryption Standard / Galois Counter Mode) encryption algorithms to provide complete confidentiality, integrity, and authenticity of the data transferred.

What happens if VMware receives a court order or legal request to access Customer Content?

If we are required by a subpoena, court order, agency action, or any other legal or regulatory requirement to disclose any of Your Content we will provide you with notice and a copy of the demand as soon as practicable, unless we are prohibited from doing so pursuant to applicable law. If you request, we will, at your expense, take reasonable steps to contest any required disclosure. We will limit the scope of any disclosure to only the information we are required to disclose. As an additional layer of protection, VMware Cloud on AWS customers may also choose to implement encryption or security software within their guest operating system or applications. This enables a customer to use the same security software they use in their own data centers and utilize their own Key Management Infrastructure to further protect their content from VMware, VMware Cloud on AWS sub-processors and legal entities.

Does VMware perform vulnerability and penetration testing?

VMware has a comprehensive vulnerability management program that includes regular internal and third-party security assessments to continuously improve our cloud platform security controls and processes, and to meet the requirements of the VMware Cloud on AWS compliance programs. Industry standard practice and VMware corporate policy does not allow sharing vulnerability and penetration reports or the findings with our customers. Sharing security testing reports would result in disclosing potential service vulnerabilities to customers before they have been remediated. The vulnerability management program, the reports and the handling of issues found are carefully reviewed by our third-party auditors as part of our compliance programs.

Can Customers run their own Vulnerability and Penetration Tests?

All VMware Cloud on AWS customers are encouraged to perform their own vulnerability and penetration testing to ensure the effectiveness of the security controls within their virtual infrastructure (SDDCs) and applications. VMware requires customers to submit the Penetration Request Form at least 10 business days before your planned test start date. Please use this Request Form to provide us relevant information about your test plans. Note: Any penetration testing requests that require testing above the standard 1Gbps peak bandwidth limit, or outside of these guidelines, will require an additional time for the VMware Cloud on AWS Team to request an approval from AWS. Penetration testing must be conducted in accordance with our Penetration Testing Rules of Engagement: a. Acceptable testing activities include utilizing tools to conduct port scans, vulnerability assessments and fuzzing against virtual machines and applications running within SDDCs that are only owned by you. b. All penetration and/or vulnerability testing must be focused on the VMware Cloud on AWS SDDC dedicated to the customer, and must not target any VMware Cloud on AWS shared infrastructure components or VMware Cloud on AWS resources dedicated to other customers. c. None of your activities will attempt to access another customer’s environment or data. d. All testing activities must not generate traffic that would exceed the 1Gbps bandwidth limit without explicit approval. e. All testing activities must not include utilizing any tools or services in a manner that perform Denial-of-Service (DoS) attacks or simulate any type of DoS attack, or any “load testing” or any flood testing against any VMware Cloud on AWS asset or SDDC/VM assets owned by you. f. Attempts to conduct phishing or other social engineering attacks against VMware employees or anyone else involved in operating the VMware Cloud on AWS service is prohibited. g. You are responsible for any damage to the VMware Cloud on AWS platform or other VMware Cloud on AWS customers that are caused by your testing activities or by failing to abide by these rules of engagement. h. You are responsible for ensuring any contracted third parties performing penetration and/or vulnerability testing do not violate these rules. VMware reserves the right to respond to any actions on the platform networks that appear to be malicious. Various automated risk mitigation mechanisms are employed throughout the VMware Cloud on AWS platform that may trigger a security or operations response to customer penetration and/or vulnerability testing activities that may lead to a disruption of service.

How quickly does VMware respond to Security Vulnerabilities?

The VMware Security Response Center (VSRC) leads the analysis and remediation of software security issues in VMware products and services. VSRC works with internal teams, customers and the security research community to address these issues and provide customers with actionable security information in a timely manner. VSRC tracks internally discovered vulnerabilities, directly receives external reports, and monitors the ecosystem for discussions of security issues in VMware products and services. After validating a report, VSRC works with the VMware Cloud on AWS team to share with our customers the details of the security issue, any mitigation options and the plans to address the root cause. The VSRC team concurrently works with the VMware Engineering teams to develop a solution and schedule releases that address the issue. The VMware Cloud on AWS team provides customers with regular updates on the security issue until the issues has been resolved. Upon closure, all security issues are tracked and publicly disclosed by the VSRC team via a VMware Security Advisory. For further details on the process and VMware's commitment to customers, see the VMware Security Response Policy.

Can VMware access my SDDC and Customer Content?

All cloud service providers need to have the necessary access to support their infrastructure. To protect against abuse, VMware has access control, logging, monitoring, and policies in place to ensure the security of our customers' content. The VMware cloud on AWS Site Reliability Engineering (SRE) team is responsible for the availability, security, integrity and performance of the service. VMware's support operations are focused on supporting the service and the underlying physical and virtual infrastructure, and the functionality of the virtual appliances used to run the virtual infrastructure contained within the "Mgmt-ResourcePool" in the Software Defined Data Center (SDDC). Although very rare, the SRE team may be required to respond to a ticket for a problem in a customer SDDC. Typically, this is required to diagnose and resolve problems related to the application of patches and upgrades of a customer SDDC. Automated runbooks have been developed that address issues that have been previously encountered which can be used to resolve problems without requiring the SRE team to access to the customer's environment. Execution of these automated runbooks is logged and can be traced to the specific individual who ran them. In cases where an automated remediation is unavailable and access to a customer SDDC is required, a senior VMware engineer with the appropriate credentials, training and background checks can gain access to a customer environment via a Delegated Access mechanism. Delegated Access is only granted to a very select and tightly controlled number of VMware engineers. The Delegated Access process requires the engineer with the appropriate permissions and training to authenticate using Multi-Factor Authentication (MFA) to a system that generates a one-time use certificate and credentials that are user-specific and good for only eight hours of access to a specific SDDC. For security and auditing purposes, this access must be tied to a system generated or customer generated support ticket. Since VMware Cloud on AWS gives customers access to vCenter and the virtual infrastructure management system, customers have unprecedented visibility into any activity performed on their virtual infrastructure. All activities performed by VMware using Delegated Access are logged in the customer's vCenter logs and are visible to the customer. These activities should not require access to the Compute-ResourcePool, where customer virtual machines are managed. Customers who are concerned about VMware accessing their information can take additional security measures and ingest the vSphere logs into their own SIEM tools to continuously monitor for any such activity. VMware Engineers cannot copy, move or export customer VMs out of the customer environment since the only Management Gateway connections that exist are established in the VMware Cloud on AWS console by the customer between their VMware Cloud on AWS SDDC and their own data centers. There are no connections from the SDDC to another vSphere environment or datastore that VMware personnel have access to, therefore, there is no destination available to which a copy of a virtual machine can be stored. Creation of a new Management Gateway by a VMware Engineer would be visible to the customer in their Activity Logs. VMware's Security Operations Center (SOC) continuously monitors for any VMware employees access to a customer's SDDC and any suspicious activities are investigated by the Incident Response Team. VMware has strict data handling policies and these policies include termination for mishandling of sensitive data. The SOC is organizationally separate from the VMware Cloud on AWS Engineering and SRE teams and has independence from the business unit to ensure regulatory compliance. Finally, VMware Engineers cannot access the customer virtual machines via the console interface since they will not have the necessary credentials to log into the customer owned virtual machines. These credentials are created and managed by customers and only the customer can provide a VMware Engineer with an account. Given the importance of the Delegated Access process, this process and the security controls associated with it have been extensively reviewed by our third-party auditors as part of our compliance programs.

Can AWS access my Customer Content?

Foremost, AWS does not have programmatic or remote access to customers SDDCs. Customer Content resides on physical servers that reside in data centers operated by AWS. However, there are multiple protection mechanisms in place that make it extremely difficult for AWS to access Customer Content. In order for an AWS employee with access to the physical disks to gain access to Customer Content, the individual would first have to identify which servers were part of the logically defined cluster of servers that make up a Software Defined Data Center (SDDC). Since VMware is the registered owner for all VPCs for all customers created by the VMware Cloud on AWS service, and VMware controls which servers in a VPC make up a specific SDDC, there is a level of segregation that makes it extraordinarily difficult for anyone at Amazon to identify which servers contain data for a particular customer and a particular SDDC. If it was possible for an AWS employee to identify all of the necessary hardware, they would need access to all of the physical drives from all of the servers and would need a means to circumvent the encryption built into the Self-Encrypting Drives (SEDs) used to store Customer Content. Additionally, the Customer Content residing on the SEDs has been handled by vSAN and striped, de-duped, compressed and encrypted across all of these disks. The algorithms used for these operations are proprietary to VMware and are not shared with AWS. Customers who deploy their own security technologies in-guest have an added layer of protection. (See the "Is my data Encrypted at Rest? FAQ).

What Audit and Security logs are available to VMware Cloud on AWS Customers?

Audit and Security Logs are available via the Log Intelligence interface available for use with VMware Cloud on AWS. With Log Intelligence these logs can be queried, alerts can be created and the logs can be forwarded to an on-premises or cloud instance of a SIEM tool. The logs include activities such as the creation, deletion or modification of SDDCs, Virtual Machines, Firewall Rules, VPNs, NATs and logical networks as well as Virtual Machine activities and information like the number of failed logins to the VMware Cloud on AWS service. Firewall packet logs can also be forwarded to the Log Intelligence service to enable customers to analyze and troubleshoot application flows through visibility into packets matching specific NSX firewall rules.

What logs does VMware collect and what is VMware monitoring?

VMware Cloud on AWS logging and monitoring systems cover the SaaS infrastructure (VMware Cloud on AWS Console) and the Software Defined Data Center (SDDC) to ensure the availability, performance, and security of the service. VMware does not monitor customers' workloads or the contents of their network traffic. To ensure the availability and performance of the VMware Cloud on AWS service, the Site Reliability Engineering team collects logs from many sources and employs multiple monitoring and alerting solutions to notify our engineers when the service is not operating normally and could impact a customer's experience. The tools used for monitoring and logging are continuously evolving to improve the detection and response time of production issues, however, they include the use of VMware's Log Intelligence and VMware Tanzu Observability products and third party products and services and are used to do event monitoring, metrics collection, log aggregation, telemetry reading and white box testing. Some of the areas that the VMware SRE team monitors include: a. The physical infrastructure including CPU, Memory, storage and networking availability, utilization and performance. b. The virtual infrastructure components and services for availability and responsiveness, including ESXi, Virtual Center, NSX appliances and AWS services. c. System events like host disconnects, port disconnects, HA fail-overs, and hypervisor crashes. d. Response times for VMware Cloud on AWS and Virtual Center APIs. To ensure the security of the service VMware monitors for security events involving the underlying infrastructure servers, storage, networks, and information systems used in the delivery of the service. The contents of customers' virtual machines and contents of customers' network traffic are not monitored. The VMware Security Operations Center (SOC) continuously aggregates logs, events and alerts into a centralized SIEM system that is monitored 24x7. The logs collected and the tools used for security monitoring are continuously evolving to improve the security of the VMware Cloud on AWS service. The logs come from multiple sources including Intrusion Detection and Prevention Software (IDS/IPS), firewalls, vulnerability scanners, file Integrity monitoring systems, anti-virus solutions, access control systems, vSphere, and AWS Services like Cloudtrail, VPC Flow Logs, GuardDuty etc. The SOC looks for abuse, port scans, brute force attempts, DDOS attacks, access control violations, unusual activities, unauthorized changes, data breaches, malicious insider activity, Hyperjacking etc. The AWS Security team also monitors the AWS infrastructure and has a direct line of communication with the VMware SOC if they detect any suspicious activity.

What Network Time Protocol Server (NTP) is used by VMware Cloud on AWS?

VMware Cloud on AWS uses the Amazon Time Sync Service to keep all logs globally synchronized.

What Corporate Security Policies does VMware have in place?

The VMware Chief Information Security Officer is responsible for defining and implementing our corporate security program and its associated policies and procedures. The corporate policies and procedures are proprietary and confidential and are not shared publicly. The policies were built in alignment with NIST and ISO 27002 standards. Policies are reviewed and revised as necessary on an as-needed basis and at least annually. the policies are made available for reference to all employees and contract resources via VMware's intranet and critical portions of the policies are included in mandatory annual training. VMware Corporate Policies and Procedures include: Acceptable Use Policy Authentication & Password Policy Access Control Policy Backup Policy Business Continuity Policy Change Management Policy Data Classification Policy Encryption Policy Human Resources Information Security Policy Incident Management Policy Information Security Governance Policy Infrastructure Security Policy IT Asset Management Policy Mobile Device Policy Monitoring and Logging Policy Operations Security Policy Physical & Environmental Security Policy Production Control Policy Remote Access Policy Security Compliance Policy System Acquisition, Development & Maintenance Policy Third Party Management Policy Vulnerability Management Policy The contents of these policies, along with the maintenance and implementation of the policies within the VMware Cloud on AWS Service are reviewed by our third-party auditors as part of our compliance programs.

How do I get notified about a security incident with the VMware Cloud on AWS Service?

If the VMware Security Operations Center (SOC) detects or is notified by AWS about suspicious activity that potentially affects the VMware Cloud on AWS service or one of its customers, the VMware Incident Response team immediately investigates to determine if a security incident occurred. If VMware has reasonable suspicion or confirmation of a security incident that affects a customer, the VMware Incident Response team and the VMware Cloud on AWS Operations team will contact the customer directly via email from vmc-services-notices@vmware.com to the email addresses of all organization owners.

What is the Breach Notification Process?

Upon becoming aware of a Personal Data Breach, the VMware Incident Response team and the VMware Cloud on AWS Operations team will contact the customer directly via email from vmc-services-notices@vmware.com to the email addresses of all organization owners. VMware will use reasonable endeavors to assist Customer in mitigating, where possible, the adverse effects of any Personal Data Breach.

What Incidental Software can be used with VMware Cloud on AWS?

There is no Third-Party Content included in the VMware Cloud on AWS service or required to use the service. VMware does run the VMware Solution Exchange (VSX) that provides customers with a centralized resource for finding technology solutions that complement, integrate or interoperate with VMware’s portfolio of products.

Service Availability and Service Updates

If there is an Availability issue, does the entire Service Offering fail?

The architecture of VMware Cloud on AWS is distributed and designed to be highly available. Availability of the components of the VMware Cloud on AWS Console is separate, and completely independent from the availability of the SDDC Infrastructure and the availability of the SDDC Management. The Management and Infrastructure of one SDDC is independent from that of other SDDCs in separate AWS Availability Zones. For instance, the VMware Cloud on AWS Console could be unavailable, but customers can still log into Virtual Center and manage their workloads. Virtual Center could be temporarily unavailable, but customer workloads would continue to run unaffected, or the NSX Management interface could be unavailable, but virtual networking would continue to operate and the NSX APIs could continue to be available. Additionally, a specific AWS Availability Zone could be experiencing availability issues but SDDCs running in other AWS Regions or AWS Availability Zones should be unaffected. An availability issue in one SDDC does not affect any other SDDC unless both SDDCs are located in the same AWS datacenter or Availability Zone (AZ) and the Availability issues is caused by a widespread problem with the AWS infrastructure.

What happens if AWS has Infrastructure availability issues?

Availability of the VMware Cloud on AWS service is dependent on and subject to availability of the AWS infrastructure on which it is hosted. The VMware Cloud on AWS Console and APIs are all located in the AWS US West (Oregon) Region. Only a complete failure of this region would result in a service disruption to the VMware Cloud on AWS Console and APIs. If the AWS Availability Zone that your SDDCs are deployed in has an availability issue, then you may lose access to Virtual Center and the SDDCs running in that region may be impacted. VMware has processes in place to restore operations to the VMware Cloud on AWS service if an AWS Availability Zone or an AWS Region becomes unavailable. Customers are responsible for their own contingency plans including backups of their workloads and alternative hosting locations. Customers with workloads that need to be resilient of AWS infrastructure availability events should deploy workloads using stretched clusters and run workloads in multiple AWS Regions.

What is the VMware Cloud on AWS Service Level Agreement (SLA)?

The Service Level Agreement for VMware Cloud on AWS is published online here. VMware is committed to use commercially reasonable efforts to ensure that, during any given billing month of the Subscription Term, availability of each component of the Service Offering ("service component") meets the “Availability Commitment” specified in the Service Level Agreement.

How is Availability calculated?

Availability in a given billing month is calculated according to the following formula: “Availability” = ([total minutes in a billing month – total minutes Unavailable] / total minutes in a billing month) x 100 Unavailability and SLA Events Example: For a billing month of August 20th -September 20th there are 44640 total minutes ((44640 total minutes - 5 minutes that a Service Component is Unavailable) / 44640) x 100 = 99.98879% Available The total minutes that the service component is Unavailable for a particular SLA Event is measured from the time that the SLA Event has occurred, as validated by VMware, until the time that the SLA Event is resolved such that the service component is no longer Unavailable If the Availability of the service component is less than the associated Availability Commitment, then you may request an SLA Credit.

How is it determined that a Service Component is Unavailable?

A service component will be considered “Unavailable” if VMware’s monitoring tools determine that the Service Component is not performing as described in the Service Level Agreement (SLA). For instance, For the SDDC Infrastructure, if none of your VMs can access storage for four consecutive minutes this would be considered an SLA event.

Why must ALL VMs encounter an SLA Event in order for it to count towards receiving a SLA Credit?

Although a single VM losing network connectivity or access to storage is a serious problem, it is not considered to be an SLA Event since the SLA is designed to cover infrastructure availability. It would be highly unlikely that a single VM in a cluster would lose network connectivity or access storage while other VMs can successfully send/receive packets or perform read/write operations. If vSAN is not available, all VMs in the SDDC will lose access to storage. The same holds true for the NSX service - all of the VMs in the SDDC will lose connectivity. In VMware's experience, a single VM losing connectivity or storage access it is caused by an invalid configuration setting affecting the specific VM. If a customer believes it has experienced an SLA Event that affects a single VM, the customer should contact VMware to assist in the investigation.

Why must the duration of an SLA Event be 4 minutes before it counts towards receiving a SLA Credit?

Service availability impacting events can cause serious problems even if they only last a couple of seconds. However the VMware Cloud on AWS SLA requires an SLA event to exceed 4 minutes for both technical and practical reasons. 1. There are situations that a customer can create that can make a component appear to be unavailable, such as bandwidth or IOPS saturation, maximum utilization of system resources, or DR fail-overs. Typically these conditions remedy themselves relatively quickly but it could appear to a customer or monitoring tool that the component is down. Through operational experience, VMware has determined that a four minute window helps to avoid reporting false outages caused by these situations. 2. The monitoring tools used by VMware poll the critical components frequently, but it is not practical to poll every instance of every component, every second. Therefore, VMware needs a window during which multiple availability tests can be run across components and on each component more than once to determine that there is an actual SLA Event. 3. If a component fails, it switches over to a redundant or backup instance or is remediated by an automated system - typically within seconds. However, recovery of a workload and system after the component is restored can take several minutes (workloads restarted, traffic rerouted etc.). This recovery is not counted as an SLA Event unless the recovery time exceeds four minutes.

Are maintenance outages eligible for a SLA Credit?

Scheduled Maintenance outages are not counted towards the service's stated availability metric, if you have been notified at least 24 hours in advance. Upgrades are scheduled in advance and may limit availability of specific services or capabilities such as Virtual Center access for a short period of time, but the maintenance process used by VMware Cloud on AWS does not typically impact the availability of a customer's workload. Customers' workloads should continue to run during upgrades of the physical hardware, drivers, hypervisor, virtual networking, and management systems. In the extremely rare case that an upgrade has the potential to impact a customer's workloads, this will be carefully coordinated with customers by the VMware Cloud on AWS operations team.

Are network outages eligible for a SLA Credit?

Depending on the cause of the outage, you may be eligible for an SLA credit. As stated in the VMware Cloud on AWS SLA, "If all of your virtual machines ("VMs") running in a cluster do not have any connectivity for four consecutive minutes" you could be eligible for an SLA credit. If the cause of this outage is determined to be caused by the failure of NSX or one of the NSX components then you are eligible for an SLA credit. If the network connectivity issue is due to AWS Direct Connect being unavailable, then you can contact AWS for credit based on the Direct Connect SLA provided by AWS.

Are there any other requirements to be eligible for an SLA Credit?

The specific requirements that must be met to be eligible for an SLA Credit are documented in the VMware Cloud on AWS SLA. You must be operating your SDDC as a production environment. For instance, Failures to Tolerate (FTT) and VM Storage Policies must be configured appropriately and sufficient storage capacity must be available.

What is a SLA Credit?

Each “SLA Credit” is an amount equal to a portion of the monthly recurring or metered subscription amount (net of any discounts) for the billing month in which the SLA Event occurred. The SLA Credit is calculated based on the scope of the Availability issue and how close to the Availability Commitment the component or service met for the month. An SLA Event that impacts an entire SDDC would result in an SLA credit for a portion of the entire SDDC monthly subscription or metered bill. If one or more SLA events within a billing month resulted in the Monthly Uptime Percentage falling below the Availability Commitment thresholds defined in the VMware Cloud on AWS SLA a greater portion of the customer's bill would be returned in the SLA Credit.

How do I request a SLA Credit?

To request an SLA Credit for VMware Cloud on AWS, you must file a support request at https://my.vmware.com within sixty (60) days after the suspected SLA Event. Dates and times of the SLA event(s) Org ID SDDC ID Description of the event and any related support incident ticket numbers. VMware will review the request and issue an SLA Credit when VMware validates the SLA Event based on VMware’s data and records.

How is the SLA Credit issued?

SLA Credits will be issued to the person or entity that VMware invoices for VMware Cloud on AWS, as a separate credit memo that can be applied towards a future VMware Cloud on AWS invoice.

Does VMware Cloud on AWS have a Business Continuity and Disaster Recovery Plan?

VMware's executive leadership sponsored the launch of an Enterprise Resiliency program in 2015 focused on improving the company’s resiliency and preparedness toward potentially business-disrupting events. The Enterprise Resiliency Program brings together the company’s business continuity, disaster recovery, emergency response, and crisis management programs under a common governance framework. The program focuses on aligning key stakeholders and driving development of business continuity plans, emergency management, and response plans to address identified risks and ensure that VMware is adequately prepared for a critical business disruption so that its people, processes, systems, facilities, and other assets are able to respond, recover, and resume operations safely and efficiently; and make sure that there is effective communication with all stakeholders. For VMware Cloud on AWS, Crisis Management, Business Continuity and Disaster Recovery plans are reviewed on an annual basis and undergo regular testing. Testing of the plans include everything from evaluations using a variety of disrupting scenarios including infrastructure issues, malware attacks, system corruption, insider threats, natural disasters etc. to global integrated exercises to identify any gaps in documentation or processes. In the event of a disruption, VMware employees will be dedicated to restoring customer services as quickly as possible. Teams are globally located and can continue operations in the event the primary offices are unavailable. Procedures are also in place to relocate employees if needed. A Pandemic Plan that is aligned with the guidelines of the World Health Organization has been implemented across VMware.

What are the RTO and RPO of the VMware Cloud on AWS Service?

In the event of a disaster, VMware Cloud on AWS has automated systems, business continuity plans, operational procedures and run books in place to restore service as quickly as possible. The scenarios covered include everything from component Availability issues, malware attacks and insider threat scenarios to natural disasters that require the VMware Cloud on AWS Console to be restored in a new AWS region and responding to AWS Infrastructure failures where the AWS RTO exceeds a couple of hours or is unknown. There are, however, an incalculable number of events or circumstances that could result in a significant business disruption and their impact may vary in size, scope, duration, severity, and geographic location. As well, significant business disruptions may result in degrees of harm to human life and regional / national infrastructure (power, transportation, communications, etc...) which could impact VMware’s recovery efforts. While we are diligent in our efforts to plan for unexpected events, it is impossible to consider every possible scenario and develop detailed responses to each of these events. To this end, VMware, in its sole discretion, reserves the right to flexibly respond to any disruption in a situation-specific and prudent manner. There are no guarantee or warranty regarding the actions or performance of VMware, its services, systems, or its personnel in the event of a significant business disruption. In the event of an actual declared disaster (including a force majeure event), and that disaster is not fully addressed in the Company’s Business Continuity/Disaster Recovery Plan, VMware will use commercially reasonable efforts to restore the VMware Cloud on AWS service as quickly as possible. VMware Cloud on AWS backs up system configuration data every 4 hours and has a target Recovery Point Objective (RPO) of 4 hours. The information that is backed up includes the configuration and settings that define a customer organization. In a catastrophic event, any organizations created or configuration settings changed since the last backup will be lost. VMware does not back up customer workloads. In the event of a catastrophic loss of the physical environment hosting a customers's SDDC, the customers will need to select a new AWS Availabiltiy Zone to re-create their SDDC and restore their workloads from their own backup. Depending on the nature of the disaster, recover time is typically a couple of hours. VMware Cloud on AWS has a Recovery Time Objective (RTO) of 24 hours for foreseeable disasters.

How does VMware notify me about planned or unplanned SDDC Maintenance?

VMware is responsible for managed delivery of Software Defined Data Center updates and emergency patches. This involves maintaining consistent software versions across the SDDC fleet with continuous delivery of features and bug fixes. Detailed information about the SDDC upgrade and maintenance process is available in SDDC Upgrades and Maintenance page. Typical updates are scheduled based on SDDC regions, outside business hours and are not workload impacting. Major updates occur approximately once a quarter with patch bundles in between. Updates may include new functionality, bug fixes and new operational enhancements, patches include bug fixes and security patches. VMware attempts to provide update notifications several weeks in advance but at a minimum will provide 24 hours of notice. VMware Cloud on AWS has multiple notification mechanisms used to contact customers regarding maintenance and uses all of them to ensure customers are informed about any activity that may affect their use of the service. 1. Within the VMware Cloud on AWS Console is a multi-channel notification service that is used to notify customers for important events. Customers can subscribe to the notification webhook for the events. 2. Maintenance activities are published on the VMware Cloud on AWS status page - https://status.vmware-services.io/. Customers can subscribe to updates on this page and email notifications will be sent by noreply@vmware-services.io. 3. Maintenance communications are sent from the email ID vmc-services-notices@vmware.com to the email addresses of all organization members and organization owners. Additional information about the contents of an update can be found on the Release Notes page: https://docs.vmware.com/vmc/releasenote

How does VMware notify me about the status of service availability issues?

VMware Cloud on AWS has multiple notification mechanisms used to contact customers about individual service availability issues. Depending on the scope and severity of the issue one or multiple mechanisms may be used. For service availability issues that affect multiple customers, VMware Cloud on AWS maintains a publicly available status page - https://status.vmware-services.io/. Information about the availability of VMware Cloud on AWS service, components and supported AWS Regions is published here along with status updates of current availability issues and information on past incidents. For issues that affect a single customer, VMware uses the Notification Service within the VMware Cloud on AWS console (Customers can subscribe to the notification webhook for the events.) and the VMware Cloud Operations team will send availability communications from the email ID vmc-services-notices@vmware.com to the email addresses of all affected organization members and organization owners.

How does VMware Cloud on AWS notify customers about changes to the VMware Cloud on AWS service?

Updates to the VMware Cloud on AWS service may include new functionality, bug fixes and new operational enhancements, patches include bug fixes and security patches. Detailed information about the contents of an update can be found on the Release Notes page: https://docs.vmware.com/vmc/releasenote. Communication about new releases are sent from the email ID vmc-services-notices@vmware.com to the email addresses of all organization members and organization owners.

What is Service Offering Documentation and how does VMware Cloud on AWS notify customers about changes to the Service Offering Documentation?

Service Offering Documentation includes the VMware Terms of Service and the VMware Data Processing Addendum along with the VMware Cloud on AWS Service Description, Support Policy, and Service Level Agreement. Updates to this documentation are typically done along with updates to the VMware Cloud on AWS Service to accommodate new features and functionality and communication of major changes will be included in the release communications. The latest versions of the Service Offering Documentation are available on the VMware website: [https://www.vmware.com/download/eula.html(https://www.vmware.com/download/eula.html).

How does VMware Cloud on AWS notify customers about a Material Degradation of either the Service or Service Offering Documentation?

In the unlikely event that VMware makes a material, detrimental change to the Service Offering or the Service Offering

Documentation, VMware will notify you prior to the effective date of that change. Notification of a Material Degradation of the service or Service Offering Documentation will be sent from the email ID vmc-services-notices@vmware.com to the email addresses of all organization members and organization owners.

Does a subscription auto-renew upon expiration?

Unless you purchase a new subscription, upon expiration of a committed subscription term, if you continue to use the Service Offering after expiration of your committed subscription term, all services will continue to operate on an on-demand basis, and you will be billed at the then current on-demand rate for those services until you cancel your on-demand use.

VMware and AWS Partnership

What does it mean when it says AWS is VMware's preferred partner?

The relationship we have with AWS is a mutual and strategic partnership that runs both ways. AWS is VMware’s preferred public cloud partner for all VMware vSphere-based workloads. Conversely, VMware Cloud on AWS is the preferred public cloud service recommended by AWS for all VMware vSphere based workloads.

Will VMware by Broadcom continue to support VMware Cloud on AWS?

Yes, VMware by Broadcom is fully committed to VMware Cloud on AWS and to the partnership with AWS. See this blog article for more details.

What is the distinction in what AWS gets versus the other public cloud partners?

There are two clear areas of distinction in the AWS relationship. The first is that VMware Cloud on AWS is the only public cloud service delivered, operated and supported by VMware. Additionally, as strategic and preferred partners, there is a deeper level of engineering and joint go to market investment that we have with AWS. The services offered by other hyperscalers are VMware Cloud Verified services are developed, sold, and supported by those partners.

How has VMware’s relationships with AWS changed as new partnerships have emerged?

There are no changes in our partnerships with either AWS or any of our hyperscale cloud partners. AWS remains VMware’s preferred public cloud partner for all vSphere-based workloads, and VMware Cloud on AWS is VMware’s preferred solution for public cloud infrastructure as a service supporting VMware workloads. That said, VMware believes in and supports customer choice in the cloud. The expanded set of relationships we’ve built with all major hyperscale cloud providers gives customers the freedom to choose the VMware-based cloud offering the best suites to meet their application or business needs.

Commerce

What is a Seller?

Seller is a Billing Account for an org. In simpler words, the company that would send the bill to the customer. It indicates which legal entity or person is identified as the Seller of Record for a specific product to the end consumer. The Seller of Record also often assumes the responsibility for accounting for a transaction tax on that particular transaction. Sellers have their own set of commerce attributes that may or may not be unique to that seller such as Payment Method, Terms of Service, Offer catalog, Pricing, Regions, Currencies accepted, and Billing engines with different invoice templates and billing business rules.

What aspects does the seller concept apply to?

They can choose the seller while creating new subscriptions and SDDCs.

How do I know a product offering is supported by a seller?

A list of VMware product offerings supported by AWS and VMware within the VMC Console or elsewhere on a VMware property is available here.

Is 'Multiple Sellers in one org' feature available for all customers?

It is available for any VMware Cloud on AWS commercial customer that has two sellers established. Please consult with your account team prior to setting up and using multiple sellers and have them contact product management resources as necessary.

Can the customers move their subscriptions from one seller to another?

No. This is not possible.

Can a customer convert VMware SPP Funds to EDP Credits and vice versa?

No. This is not possible.

Is creating a fund equivalent to creating a subscription?

No, adding a fund and creating a subscription are two separate disjoint activities. Customers shouldn't be in the notion that adding new funds would get translated to subscriptions. They would need to create subscriptions in VMC Console.

Can one seller's subscription cover other sellers too?

No, A subscription can only cover hosts within that seller. Example: If you have 2 SDDCs with 4 hosts each, 1 with VMware, 1 with AWS, and a three-year term subscription for four hosts with VMware as the seller. In that case, the 4 host SDDC with AWS as the seller would be charged on demand.

Can a single SDDC have 2 Sellers?

No, An org can have 2 sellers, but the SDDC under the orgs can have only 1 seller for 1 SDDC.