VMWARE CLOUD™ ON AWS

Operations Model White Paper

November 2017

DISCLAIMER: Some features described in this paper have been released in preview to gather feedback, and may not be available to all applicable customers or in all AWS regions. We cannot guarantee that features that are in 'Preview' will become available within any particular time frame or at all. Make your purchase decisions only on the basis of features that are available. For the most current set of features, please see https://cloud.vmware.com/vmc-aws/features.

vmware®

Index

VMware Cloud™ on AWS

VMware Cloud on AWS brings VMware's enterprise-class Software-Defined Data Center software to the AWS Cloud, enabling customers to run production applications across VMware vSphere®-based private, public, and hybrid cloud environments. Delivered, sold, and supported by VMware as an on-demand service, customers can also leverage AWS's breadth of services, including storage, databases, analytics, and more. IT teams manage their cloud-based resources with familiar VMware tools — all without the hassles of learning new skills or utilizing new tools.

VMware Cloud on AWS integrates VMware's flagship compute, storage, and network virtualization products (vSphere, vSAN, and NSX) along with vCenter management, and optimizes it to run on 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 benefits from use of the AWS and VMware hybrid cloud experience, including:

- IT teams manage their cloud-based resources with familiar VMware tools – without the challenges of learning new skills or utilizing new tools. However, administrative responsibilities for the vSphere cluster deployed as part of the Cloud Software-Defined Data Center (SDDC) will be shared between the VMware Cloud on AWS service and the on-premises administrator.
- This paper will describe the differences between running the VMware SDDC software on-premises vs. in VMware Cloud on AWS, and will go over the new operation model that administrators will need to adopt when using this service.

PROVISIONING INFRASTRUCTURE

A Customer Can Deploy Multiple Cloud SDDCs

Each deployment of a cloud SDDC contains at least a single vSphere HA and DRS cluster that runs all management virtual machines and customer workload virtual machines. The initial cluster contains four ESXi hosts. Each ESXi host provides 36 cores running at 2.3 GHz, 512 GB RAM and 16 TB all-flash NVMe devices to the cluster. The workload virtual machines running inside the SDDC cluster consume a dedicated cluster-wide vSAN datastore. A cluster can be expanded up to 32 hosts, all of which have identical hardware capabilities.

Each ESXi host provides 25 GB/s of network bandwidth within the Cluster SDDC. Network I/O Control prioritizes the bandwidth between the several network traffic streams if contention occurs. The SDDC cluster leverages native NSX technology that integrates AWS networking infrastructure. The customer can create logical networks to provide VMs network connectivity to other networks and the Internet if preferred. The management virtual machines, such as the vCenter, NSX Manager, and NSX Edge virtual machines run inside the cluster and are grouped in a separate vSphere DRS resource pool.

A cloud SDDC cluster is dedicated to a single customer. Existing AWS controls ensure customer segregation using dedicated AWS accounts and AWS Virtual Private Connections (VPC) for each cloud SDDC deployment. Because vSAN is built out of instance local storage and each ESXi host is dedicated to a single customer, there is no sharing of resources across different customers inside the SDDC compute, network or storage layers.

Permissions Management Overview
The VMware Cloud on AWS service retains administrator rights on the vCenter server deployed as part of the cloud SDDC. This is required to allow the service to monitor and manage the lifecycle of the cloud SDDC software stack. The VMware Cloud on AWS service retains the administrative rights on the SDDC to deploy and configure the AWS infrastructure and the SDDC software deployment. It is responsible for adding and removing hosts and networks due to a failure or if cluster-scaling operations require more or fewer resources. The VMware Cloud on AWS service is responsible for cloud SDDC software patching and applying updates.

The VMware Cloud on AWS services introduce new roles to the traditional vCenter user model and extend the roles and permissions scheme. This is simply to ensure that the Cloud SDDC infrastructure is configured in prescriptive deployment architecture and that the customer cloud administrator cannot reconfigure the management appliances. Within this model, the customer cloud administrator has full control over their workload while having a read-only view of management workloads and infrastructure.

Cluster Settings Overview
A Cloud SDDC can contain up to 10 clusters. VMware manages the vSphere HA, DRS, and vSAN settings for the customer so the customer cloud administrator has read-only view of the cluster configuration settings. This model does not provide the option to configure per-VM HA and DRS settings and it also doesn't allow configuration of DRS affinity rules settings such as VM-VM and VM-Host affinity rules.

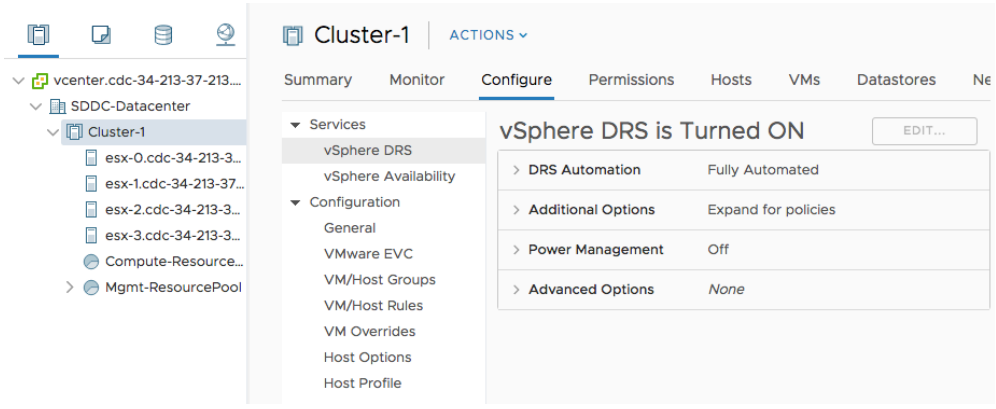

Figure 1: Read-Only View vSphere Cluster

In a cluster, two vSphere DRS resource pools are created. The resource pool named *MGMT-ResourcePool* contains the management virtual machines and is configured with a CPU and memory resource reservation. The customer cloud administrator has a read-only view of the virtual machine and resource pool settings of the management resource pool.

Customer workload virtual machines are placed in the resource pool named *Compute-ResourcePool*. By default, this customer workload resource pool is not configured with CPU and memory resource reservations, giving the customer cloud administrator full control access rights over this resource pool.

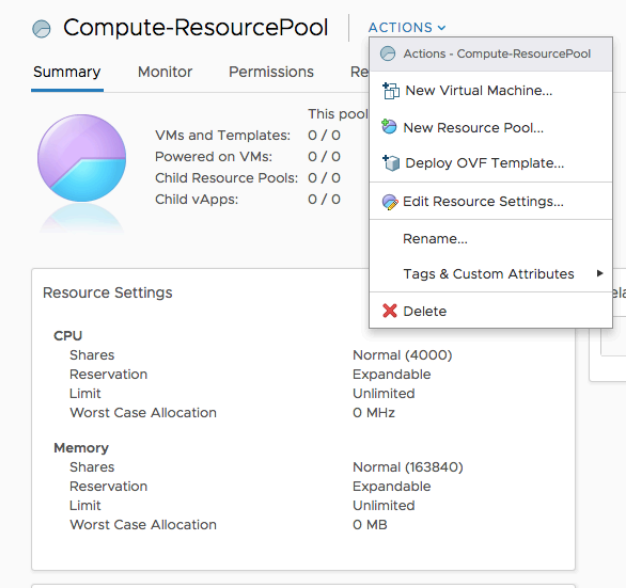

Figure 2: Customer Workload Resource Pool Configuration

COMPONENT	VMWARE CLOUD™ ON AWS SDDC SETTING
Cluster Configuration Settings	Read-only view
Per-VM HA/DRS Settings	Not-Available
DRS Affinity Rules	Not-Available
Management Resource Pool	Read-only view
Workload Resource Pool	Full VM and RP Permissions
Nested Resource Pools	Available*

Table 1: VMware Cloud on AWS SDDC Cluster Setting

*Nested resource pools should not be used as a substitute for a folder structure in the inventory view. The technical paper "DRS Cluster Management with Reservation and Shares" provides guidance on how to structure nested resource pools.

Multiple Cluster Support
By default, a Cloud SDDC contains a single cluster. If the customer chooses to create a new cluster of four hosts inside the Cloud SDDC, the additional cluster will then be created in the same AWS Availability Zone.

ESXi Host Settings Overview

In this model, the customer is expected to focus on consuming cloud resources and move away from an infrastructure focused operational model. No direct access to ESXi host resources is provided to the customer cloud administrator. SSH is disabled, and the customer cloud administrator will not receive any ESXi host credentials.

Additionally, the customer cloud administrator cannot install any third-party software on the Cloud SDDC ESXi hosts. ESXi host reporting, such as host logs, and core dumps are unavailable to the customer cloud administrator. Read-only host operations are mediated through vCenter such as vSphere API calls and the execution of PowerCLI and ESXCLI commands.

Network Settings Overview

VMware NSX is a key ingredient for VMware Cloud on AWS. All virtual machine networking in VMware Cloud on AWS is provided by NSX and provides compatibility with NSX and vSphere products used on-premises. The networking technologies used in VMware Cloud on AWS represent a jointly engineered solution between VMware and Amazon that allows vSphere and NSX to optimally work in the AWS environment.

Amazon has enhanced AWS infrastructure to enable the VMware Cloud on AWS service. Similar to every other key infrastructure component of the Cloud SDDC, it is delivered as a service cloud model and allows frequent introductions of additional networking capabilities. The customer is not required to run NSX on-premises to connect to the Cloud SDDC. NSX in the Cloud SDDC connects the ESXi hosts to the AWS infrastructure and abstract AWS VPC networks for the customer cloud administrator.

With VMware Cloud on AWS, the customer connects to VMware Cloud on AWS by using a L3 VPN IPSEC Connection, L2 VPN, or AWS Direct Connect. Layer 2-network connectivity enables customers to migrate workload without changing IP addresses of virtual machines, enabling support for vMotion (bandwidth and latency permitting) migration both to and from the Cloud SDDC clusters. L2 VPN connectivity provided by VMware Cloud on AWS follows a prescriptive infrastructure model, which is offered by the Simplified Mode.

AWS Direct Connect

AWS Direct Connect is supported to connect the customer on-premises data center to the in-cloud SDDC. AWS Direct Connect offers high bandwidth and low latency connectivity which can be used for ESXi management and vMotion traffic. Direct Connect allows live migration of larger and/or more virtual machines faster than a VPN connection.

Simplified Mode Networking

The goal of Simplified Mode Networking is to allow everyone that uses vSphere to consume VMware Cloud on AWS as easy as possible. VMware Cloud on AWS is designed from the ground up to provide an easy method of resource consumption. To avoid any steep learning curve for network management for an on-premises network and cloud administrator unfamiliar with NSX operations, simplified mode conveniently provides basic networking services.

In this mode, network topology and its components are preconfigured and cannot be changed by the customer; this is referred to as a prescriptive network topology. The on-premises administrators only need to specify subnets and IP-ranges.

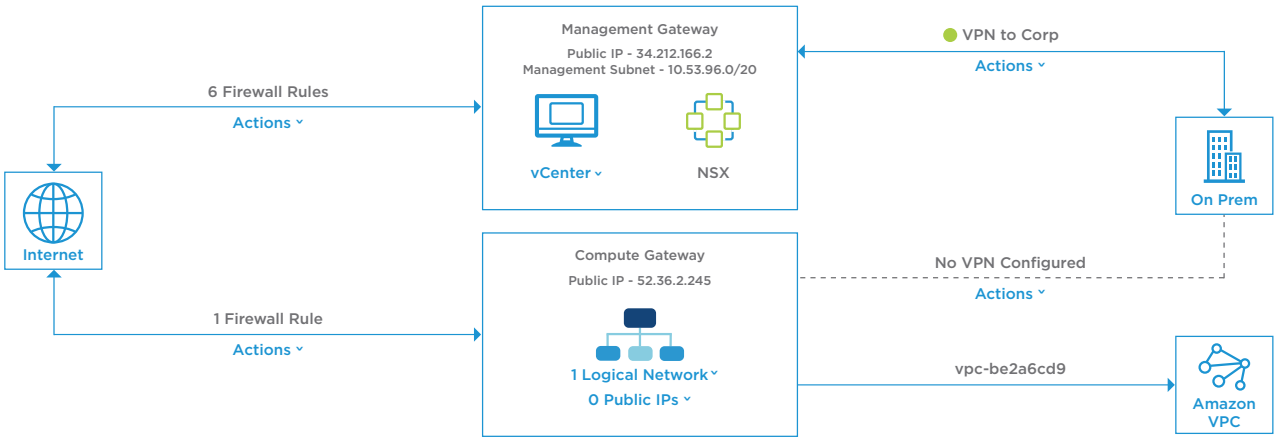

Figure 3: VMC Network Connectivity Diagram

A VMware Cloud on AWS Service Console (Portal) is developed for end-user access. The connectivity to and from the Cloud SDDC is managed through the VMware Cloud on AWS portal. The customer cloud network admin logs into the VMware Cloud on AWS portal and configures the network. The customer cloud network admin can then establish VPN connectivity and configure the access rules of the firewall.

The customer cloud administrator logs into vCenter with the vSphere web client and consumes the networks that the cloud network admin created. The customer cloud administrator can create logical networks, connect virtual machines, and permit traffic through the firewall and across the VPN networks.

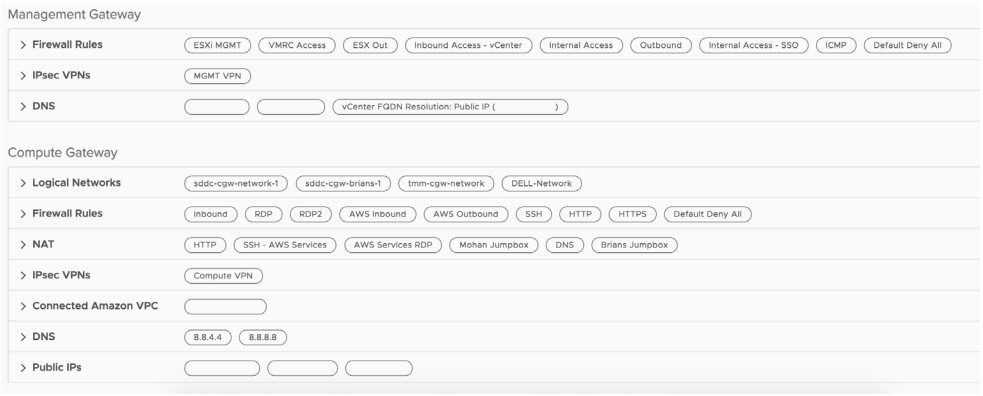

Figure 4: VMware Cloud on AWS Networking Configuration in VMware Cloud on AWS Portal

vSphere Networking Settings

NSX allows ease of management by providing logical networks to virtual machines. When the cluster is scaled out, NSX automatically connects the new hosts to the logical networks and the VMkernel networks.

The customer cloud administrator is unable to configure or add and remove VMkernel networks which provide infrastructure services, but they have full control over logical networks. The NSX logical network construct is the Cloud SDDC equivalent to the on-premises SDDC distributed switch port group.

COMPONENT	VMWARE CLOUD™ ON AWS SDDC SETTING
VMkernel Networks	Read-only view
Management Logical Networks	Read-only view
Pre-Provisioned Workload Logical Network	Network Assigned Permissions
Provisioning Additional Logical Networks	Full Access

NETWORK CONFIGURATION OPERATION	VMWARE CLOUD™ ON AWS PORTAL
Create firewall rules for the management and compute gateways	X
Configure VPN settings for IPsec VPN connections between Cloud SDDC and on-premises SDDC	X
Configure DNS settings for the management and compute gateways	X
Configure inbound NAT and create public IP addresses for your compute gateway	X
Provisioning Additional Logical Networks	X

Table 2: Component Setting and Network Configuration Operation

Storage Settings Overview

vSAN provides the storage capacity and storage services to the virtual machines. vSAN consumes eight local NVMe device per ESXi host and is comprised of two disk groups. The customer cloud administrator has read-only view to the configuration of the vSAN datastore.

vSAN Datastore

All virtual machines running inside the Cloud SDDC consume storage capacity and leverage storage services from vSAN. Management workloads and the workloads belonging to a single VMware Cloud on AWS customer, are located on the same vSAN cluster. However, a new vSAN capability is being introduced to Cloud SDDC, providing

two logical datastores instead of one. One of these datastores will be used to store the management virtual machines and the other datastore will be used for the customer virtual machines..

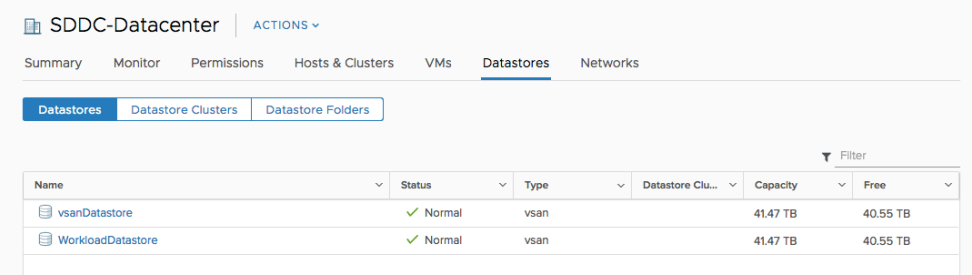

Figure 5: Cloud SDDC vSAN Datastores

The customer cloud administrator has read-only view to the management virtual machines datastore to browse the datastore space. The customer cloud administrator can allocate space and browse the workload datastore. By default, the default storage policy is applied to both the management virtual machines datastore and the customer WorkloadDatastore.

vSAN Health Services

VMware monitors the health and performance of the vSAN datastore, as a result vSAN Health Monitoring and vSAN Performance Service are not available to the Cloud Administrator.

vSAN Storage Policies

The storage policies are applied to virtual machines and their objects. There is a default policy set on the VSAN datastore. This policy is applied to all new virtual machines that do not have a specific policy assigned to them.

IN CLOUD VSAN STORAGE POLICY FEATURE	SETTING
Primary level of failures to tolerate	1
Number of disk stripes per object	1
Flash read cache reservation, or flash capacity used for read cache	0
Object space reservation	0
Force provisioning	0

Table 3: Default vSAN Storage Policies for Workload Virtual Machines

Figure 6 shows how the total raw capacity of a single host cluster is consumed to provide the final usable capacity when all virtual disks are configured with the storage policy of RAID 5/6.

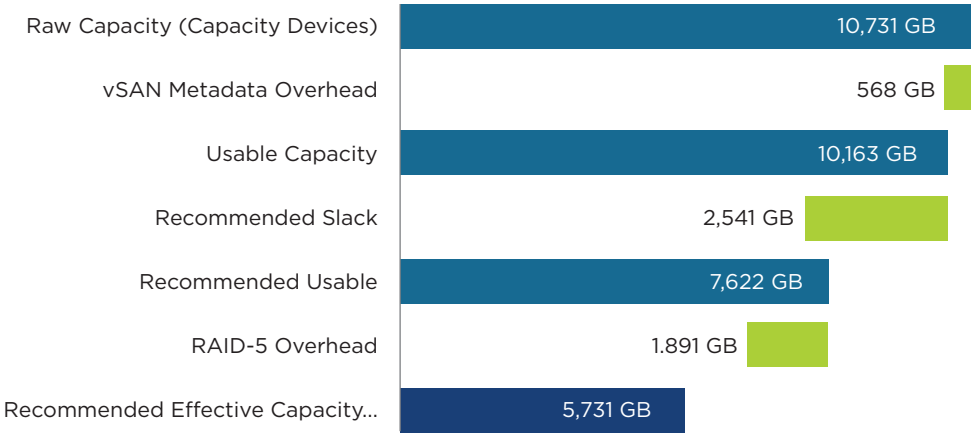

Figure 6: Calculation of vSAN Effective Capacity of a single host with all RAID5

The customer cloud administrator is unable to reconfigure the storage policies set to the management virtual machines. Instead of using RAID-1, the vSAN storage policy of management VMs is configured with the RAID 5/6 Fault Tolerance Method. This reduces the capacity footprint of the management virtual machines, preserving the most available datastore capacity for workload virtual machines. The primary level of failures to tolerate for management virtual machines is adjusted if the ESXi host count inside the Cloud SDDC is six or more.

IN CLOUD VSAN STORAGE POLICY FEATURE	4/5 NODE CLUSTER	6+ NODE CLUSTER
Primary level of failures to tolerate	1	2
Fault Tolerance Method	**Raid 5 (Erasure Coding) - Capacity**	**Raid 6 (Erasure Coding) - Capacity**
Object Space Reservation	100%	100%

Table 4: Default vSAN Storage Policies for Management VMs

The customer cloud administrator is able to create a storage policy with the required failure tolerance method for the vSAN datastore storing the workload virtual machines. With four hosts, the default is set to RAID-5 for the initial cluster configuration. If the SDDC cluster contains six ESXi hosts, the RAID-6 erasure coding fault tolerance method is supported. The new storage policy can act as the default storage policy of the WorkloadDatastore.

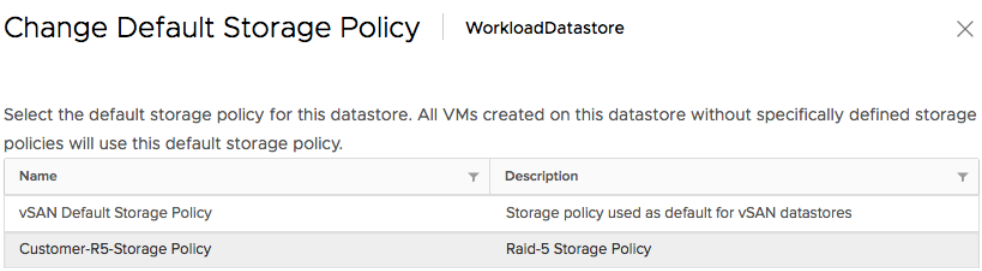

Figure 7: Custom Storage Policy for the WorkloadDatastore

ENSURING SECURITY

Storage Encryption

To provide data security, all local storage NVMe devices are encrypted at the firmware level by AWS. The encryption keys for NVMe encryption are managed by AWS and are not exposed or controlled by VMware or the VMware Cloud on AWS customers. vSphere virtual machine encryption and vSAN datstore encryption is not available at this time.

vMotion Encryption

Encrypted vMotion was introduced in VMware vSphere 6.5. It does not require a third-party key manager. It is set on a per-VM basis as part of the virtual machines Options. Encrypted vMotion encrypts the data going over the vMotion network, not the network itself. As such, it requires no special configuration other than enabling it in the virtual machine options. Encrypted vMotion is available at VMware Cloud on AWS between hosts inside the Cloud SDDC.

Audit Quality Logging

VMware is the internal operator with the administrator ownership and is responsible for audit, compliance, and troubleshooting the infrastructure. The customer cloud administrator is responsible for virtual machine troubleshooting and the auditing of operations they perform on the Cloud SDDC.

Identity Sources

VMware Cloud on AWS supports both OpenLDAP server or an Active Directory as LDAP server as an identity source. Multiple identity sources are supported. Ensure the DNS is configured for your management gateway so that it can resolve the FQDN for the identity source.

Role-Based Access Control

In order to support the adjusted role-based access control, a new CloudAdmins User Group is created that contains a new user named CloudAdmin. The Cloud SDDC also contains new role definitions:

ROLE	PRIVILEGES
CloudAdmin	**Privileges for vCenter-managed entities (e.g., Virtual machines, resource pools, datastores, networks)**
GlobalCloudAdmin	**Global privileges (e.g., Content Library, Tagging, Storage Profiles, Read-Only)**

Table 5: Roles and Privileges

The *CloudAdmin* group is granted the *GlobalCloudAdmin* role on all global permissions. The *CloudAdmin* group granted *CloudAdmin* permissions on:

- Workloads Virtual Machines Folder
- Workloads Resource Pool
- Compute Gateway Logical Network
- vSAN Datastore
- Content Library
- Tagging Services

The *CloudAdmin* user is granted a read-only global permission, enabling this user to view all physical resources and management infrastructure components. Additionally, the *VMware Cloud on AWS Getting Started* guide contains a detailed overview of the role privileges of the CloudAdmin user and the GlobalCloudAdmin user group.

DEPLOYING VIRTUAL MACHINES

Customers can design and consume cluster resources as required, deciding how many virtual machines to run inside a cluster. Virtual machines storage policies determine the fault tolerant method of the virtual machine data and the degree of storage capacity consumption. A default resource pool is created at the same level as the management virtual machines resource pool and supports child resource pools.

The customer cloud administrator has full virtual machine and resource pool permission to configure the resource pools to align with their business requirements; they can create, edit, and delete virtual machines.

The Cloud SDDC contains a group of virtual machine folders. By default, Workload VMs are provisioned in the “Workloads” folder.

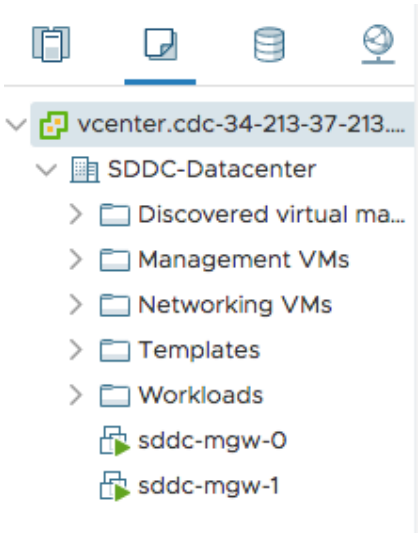

Figure 8: Cloud SDDC Workload Folders

vMotion
Live Migration with vMotion allows virtual machines to be migrated while still powered on. This requires a stretched Layer-2 network to be configured, either over VPN or Direct Connect. Please note that the firewall rules must be configured to allow inbound and outbound connectivity with the on-premises vCenter and ESXi hosts.

Virtual Machines provisioned in Cloud SDDC with a hardware version 13 configuration. This can impact hybrid cloud operations if the on-premises SDDC cluster containing hosts running ESXi 6.0 or older.

Content Library
vCenter Content Library is one of the primary means to copy virtual machine content, such as OVA and ISO images, from the on-premises data center to a Cloud SDDC deployment, and maintain the same versions of these files in both places. In addition, it can be used to synchronize these types of files, and also virtual machine templates, among different Cloud SDDCs.

The customer cloud administrator has full permissions to manage the Content Library. The recommended setup during on boarding of VMware Cloud on AWS is to use on-premises Content Library and publish the content to the Cloud SDDC. The Cloud SDDC acts as a subscriber to the on-premises Content Library.

Hybrid Cloud Extension
Hybrid Cloud Extension, which is an add-on service, enables customers to link on premises environments to VMware Cloud on AWS, to facilitate a hybrid-cloud architecture. Once in place the Hybrid Cloud Extension hybrid interconnect facilitates seamless migration and hybrid scenarios with no retrofit/re-architecture of the source sites.

Hybrid Cloud Extension enables high throughput, secure network extension without the need for NSX on premises, enabling workloads to be moved in bulk and on a schedule, without changing IP or MAC address. It also works with legacy versions of vSphere, thus allowing migration to VMware Cloud on AWS without the need to upgrade the on premises vSphere deployment.

Disaster Recovery

The VMware Site Recovery service expands and simplifies traditional disaster recovery operations by delivering on-demand site protection across a common, vSphere-based operating environment from on-premises to the cloud. The service protects workloads between on-premises data centers and VMware Cloud on AWS, as well as between different instances of VMware Cloud on AWS.

Built on top of enterprise-grade recovery plan automation (VMware Site Recovery Manager) and native hypervisor-based replication capabilities (vSphere Replication), the service provides an end-to-end disaster recovery solution that reduces the requirements for a secondary DR site, accelerates time to protection, and simplifies DR operations. This service is natively integrated into VMware Cloud on AWS, and provides support for multiple vSphere versions on-premises

SIMPLIFYING ADMINISTRATIVE SERVICES

Hybrid Cloud Linked Mode

Hybrid Linked Mode allows you to link your VMware Cloud on AWS vCenter Server instance with an on-premises vCenter Server instance.

Using Hybrid Linked Mode, you can:

- Log in to the vCenter Server instance in your SDDC using your on-premises credentials.
- View and manage the inventories of both your on-premises and Cloud SDDC from a single vSphere Client interface.
- Cold migrate workloads between your on-premises data center and Cloud SDDC.

Due to the adjusted operational model, Hybrid Linked Mode will not replicate all objects and permissions from the on-premises SDDC to the Cloud SDDC.
For example:

- Tags will be uni-directional from on-premises to VMware Cloudon AWS
- Certificates are bi-directional
- Lookup is uni-directional from on-premises to VMware Cloud on AWS

Hybrid Cloud Linked Mode supports embedded and external VMware Platform Services Controller (PSC) on-premises. If the on-premises workload is distributed across multiple vSphere SSO domains, it is recommended to consolidate these workloads into an infrastructure managed by one vSphere SSO domain.

Hybrid Linked Mode supports on-premises deployment of multiple vCenters configured in a single sign-on domain. vCenters version must be VCSA 6.5 patch D and above. Hybrid Linked Mode extends the on-premises vSphere Single Sign-On domain to the VMware Cloud on AWS, providing the ability to use the same identity used on-premises.

Command Line Interface and API

Management of the Cloud SDDC can be done via the user interface using Application Programming Interface (API) or PowerCLI. Due to the adjusted role based access control, the customer cloud administrator cannot configure infrastructure components such as hosts or vCenter via API calls or PowerCLI commands. They can only use the API calls to retrieve information about these components. However, the cloud administrator is able to use API calls or PowerCLI commands to deploy new VM workloads in the SDDC.

Due to the DRS resource pool structure, virtual machines folder structure, and vSAN datastore structure it is necessary to specify these elements during virtual machines-focused commands. Please review existing scripts and adjust them accordingly.

Read-only host operations are mediated through vCenter such as vSphere API calls and the execution of PowerCLI and ESXCLI commands.

The vSphere API Explorer is operational through the vCenter Server. Access the vSphere Automation API methods through API Explorer, Datacenter CLI, PowerCLI (Get-CisService), vSphere Automation SDKs (Python, Ruby, Perl, .NET, Java, REST). In addition, the vSphere SOAP APIs are functional, along with the SOAP-based SDKs and Managed Object Browser.

Please note that the API is limited to basic operational tasks, including inventory operations focused on cluster/datastore/folder/host/network, basic virtual machines administration (create, delete, modify, power on/off).

The service REST API endpoint exists here. Functionality includes:

ELEMENT	FUNCTIONALITY
SDDC	Create/show/delete SDDC
ESXi Host	Add/remove host
VPN	Create/show/modify/remove
Firewall Rules	Create/show/modify/delete/reorder
Public IP	Allocate/show/remove

Table 6: VMware Cloud on AWS Service Operations

NSX API Access for Automation

VMware Cloud on AWS provides customers' access to a subset of the VMware NSX APIs for automation of Network and Security tasks. Customers can easily automate provisioning of the SDDC, establish VPN tunnels, and configure firewall rulesets through the NSX API set. Once configuration of the SDDC is complete, the NSX API set allows customers to create new logical networks, connect virtual machines to logical networks, and provide external access to VMs.

MANAGING SERVICE LIFECYCLE

VMware Cloud on AWS is a service and therefore VMware handles all patching. The customer cloud administrator does not have access to patch or upgrade the underlying infrastructure. VMware has developed automated workflows that are optimized for managing many Cloud SDDCs at scale. Wherever sensible, existing products, such as vSphere Update Manager, are leveraged as components of the overall management framework. This is largely transparent to customers using the VMware Cloud on AWS service.

SDDC Version Control

The version of ESXi that makes up the foundation of your SDDC on VMware Cloud on AWS is a variant of the traditional vSphere release, but completely compatible from the application point of view. ESXi running on VMware Cloud on AWS may have a more frequent update cadence so that customers can take advantage of regular service enhancements. VMware controls the ESXi and component versions. There are no plans to offer customer-selectable version options for the underlying infrastructure components. This consistency enables VMware to operate at scale.

VM Tools Version Control

VMware will provide installers for a designated release of VMware Tools for all supported guest operating systems, and will keep those regularly updated. The customer cloud administrators will have the option of specifying their own repository of VMware Tools installers so that a particular release can be standardized between on-premises and VMware Cloud on AWS. This configuration will be available through a new documented API.

Maintenance Windows

When the Cloud SDDC is scheduled for updating, a one-week window is presented to the customer cloud administrator. This notification is sent via email, and a banner is also displayed on the VMware Cloud on AWS portal. The customer cloud administrator has the option to have the update begin immediately or schedule the update to begin at a particular time during the next week. Workloads are able to continue to run during Cloud SDDC software updates.

ESXi Host Patching

When VMware Cloud on AWS hosts are patched, vMotion enables zero-downtime migration of virtual machines so that these updates can be executed transparently. Customers are not required to maintain N+1 capacity—the upgrade workflow will automatically provision additional resources as needed in order to support the customer applications without negatively impacting performance.

An additional ESXi host is provisioned to avoid ESXi host resource reduction during maintenance operations. Note that data is not evacuated during maintenance operations to avoid performance regression and bandwidth consumption.

Management Components Patching

All elements of the SDDC are considered when implementing update workflows. Dependencies, such as vCenter Server updates, are all resolved and executed as part of an overall maintenance workflow. Customers can expect short periods of service unavailability due to the nature of certain types of upgrades, but none of these will impact the availability of virtual machines and applications running on VMware Cloud on AWS.

Whenever a Cloud SDDC update is scheduled, an advanced maintenance notification email is sent to the customer. This maintenance notification can be expected usually one week ahead for regular updates. In case of an emergency update, a notification email is sent one to two days ahead of the scheduled update.

When the maintenance begins, a notification is sent and the control plane process is initiated. During the control plane update, it's possible that vCenter is not available for customer connections. Once the control plane update is complete a notification is sent to the customer and the data plane update begins. As mentioned, an additional host is added to the cluster to maintain the same level of host resources. Once the data plane update is complete, a notification is sent to the customer.

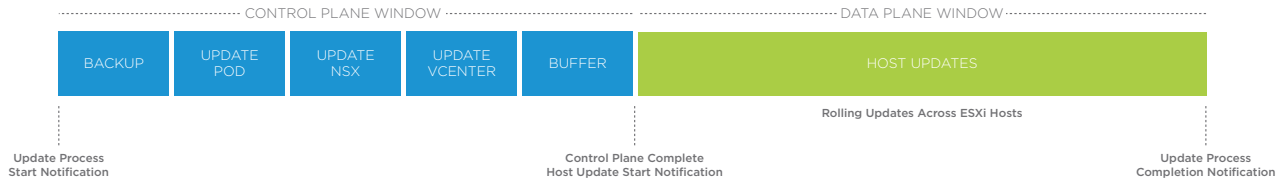

Figure 9: Update Process SDDC Timeline

Maintenance Cadence

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

IN CLOSING

Want to Learn More About VMware Cloud AWS?

For more information on how VMware Cloud for AWS, the best-in-class hybrid cloud solution, could help your organization enjoy more consistent, seamless management of cloud-based resources as well as more agile application development and seamless migration, visit https://cloud.vmware.com/vmc-aws/resources. You can also follow us on Twitter or subscribe to the VMware Cloud on AWS video playlist on YouTube.

About VMware

VMware, a global leader in cloud infrastructure and digital workspace technology, accelerates digital transformation by enabling unprecedented freedom and flexibility in how our customers build and evolve IT environments. With VMware solutions, organizations are improving business agility by modernizing data centers and integrating public clouds, driving innovation with modern apps, creating exceptional experiences by empowering the digital workspace, and safeguarding customer trust by transforming security. VMware is a member of the Dell Technologies family of businesses.

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