VMware Cloud on AWS Operations Guide

16 January 2020

VMware Cloud on AWS

vmware®

You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

If you have comments about this documentation, submit your feedback to

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

About VMware Cloud on AWS Operations

The *VMware Cloud on AWS Operations Guide* provides information about configuring advanced SDDC features that support ongoing operation of your VMware Cloud on AWS SDDC, including storage management, provisioning, and seamless interoperation with your on-premises data center.

Intended Audience

This guide is primarily for VMware Cloud on AWS organization members who have the CloudAdmin role or another role that includes administrative rights over objects owned by your organization. It covers operational areas like provisioning your SDDC with content from your on-premises datacenter, using AWS services like S3 and Direct Connect, and integrating VMware Cloud on AWS with other VMware and Amazon tools.

We assume you already have experience using an SDDC with a management network as described in the VMware Cloud on AWS *Getting Started* guide. Experience configuring and managing vSphere in an on-premises environment and familiarity with virtualization concepts are assumed. In-depth knowledge of Amazon Web Services is useful, but is not required.

About Software-Defined Data Centers

1

A VMware Cloud on AWS Software-Defined Data Center (SDDC) includes compute, storage, and networking resources.

Each SDDC runs in an Amazon Virtual Private Cloud (VPC) and provides a full VMware stack, including vCenter Server, NSX-T software-defined networking, vSAN software-defined storage, and one or more ESXi hosts that provide compute and storage resources to your workloads.

This chapter includes the following topics:

Supported SDDC Versions

A given version of the SDDC software is supported only for a specific period of time. Updates to the SDDC software are necessary to maintain the health and availability of the service, and are mandatory.

Each version of the SDDC software has an expiration date. SDDCs whose software version is past the expiration date are not guaranteed support from VMware.

To find the version of your SDDC software, see Get Support.

Table 1-1. Lifecycle Support for SDDC Software Versions

SDDC Version	Expiration Date
1.8	TBD
1.7	Feb 28, 2020
1.6	October 31, 2019

Configuration Maximums for VMware Cloud on AWS

There are maximums and minimums associated with many features in VMware Cloud on AWS.

All limits listed are hard limits unless otherwise indicated. A hard limit cannot be changed. Any limit described as a soft limit may be increased upon request. Contact VMware Support to request an increase to a soft limit.

SDDC Maximums

Maximum	Value	Description
Number of SDDCs per Organization	2	Number of SDDCs per organization. This is a soft limit.
Number of linked VPCs	1	Maximum number of linked AWS VPCs per SDDC.
Public IP Addresses (Elastic IPs)	75	Maximum number of elastic IP addresses per SDDC. This is a soft limit.
Minimum hosts per cluster for full SLA	3	This is the minimum number of ESXi per vSphere cluster to be supported at the full SLA.
Minimum hosts per cluster for no SLA	1	This is the minimum number of ESXi hosts per vSphere cluster with no SLA.
Maximum hosts per cluster, including stretched clusters	16	The maximum number of ESXi hosts per vSphere cluster. This limit applies to both single-AZ clusters and stretched clusters.
Maximum clusters	20	Maximum number of vSphere clusters per SDDC.

vCenter Server Maximums

Maximum	Value	Description
Maximum hosts per SDDC	32 (soft limit) 300 (hard limit)	Maximum number of ESXi hosts per SDDC
Maximum VMs per SDDC	4000	Maximum number of virtual machines per SDDC.
VMs per host	200	Maximum number of VMs per host.

Networking and Security Maximums

Maximum	Value	Description
ARP entries per Edge Node	5000	Maximum number of ARP entries.
IPSec VPN Tunnel	16	Maximum number of IPsec VPN tunnels created per SDDC.
Logical Segment	200	Maximum number of logical segments per SDDC.
Logical Ports	1000 per logical segment	Maximum number of ports on a logical segment.
MGW Firewall Rule	200	Maximum number of Management Gateway firewall rules.
CGW Firewall Rule	950	Maximum number of Compute Gateway firewall rules.
CGW NAT Rule	500	Maximum number of Compute Gateway NAT rules.
Logical segment advertised over DX private VIF	16	Maximum number of logical segments advertised over Direct Connect Private VIF. This is a soft limit.
Number of L2 VPN Clients	1	Maximum number of sites connecting to L2 VPN server per SDDC.
Extended Network	100 per L2 VPN	Maximum number of logical segments extended from on-premises.
Distributed Firewall Grouping Objects	10000	Maximum number of grouping objects (security groups).
Ports with Grouping Objects Applied	1000	Maximum number of ports with grouping objects (security groups) applied.
Distributed Firewall Sections	100	Maximum number of distributed firewall sections.
Distributed Firewall Rules Across All Section Groups	10000	Maximum total number of distributed firewall rules across all sections groups (Emergency Rules, Infrastructure Rules, and so on).
Distributed Firewall Rules Per Section Group	10000	Maximum number of distributed firewall rules per section group.
Distributed Firewall Sections Per Section Group	100	Maximum number of distributed firewall sections per section group (Emergency Rules, Infrastructure Rules, and so on).
Distributed Firewall Sections Across All Section Groups	100	Maximum number of distributed firewall sections across all section groups.
IPs per IP Set	4000	Maximum number of IP addresses that can be included in an IP set.
Distributed Firewall Rules per Grouping Object	512	Maximum number of distributed firewall rules per grouping object (security group).
Security Tags per VM	25	Maximum number of security tags per VM.
VMs per Grouping Object	5	Maximum number of VMs per grouping object (security group).
Port Mirroring Source VMs per session	5	Maximum number of source VMs in a port mirroring session.
Port Mirroring Destination VMs per session	1	Maximum number of destination VMs in a port mirroring session.

Maximum	Value	Description
IPFIX Collectors	4	Maximum number of IPFIX Collectors configured.
IP Discovery ARP Snooping	1	Maximum IPs detected by ARP snooping on a VM.
IP Discovery VM Tools	1024 (with VMware Tools 10.3.x on a VM)	Maximum IPs detected by VMware Tools 10.3.x on a VM.
Direct Connect Private VIF Connection per SDDC	4	Maximum number of private virtual interfaces attached to one SDDC.
Number of VIFs/Ports per host	400	Maximum number of VIFs or ports per host.

vSAN Maximums

Maximum	Value	Description
Maximum datastore capacity that can be utilized	75%	You can use up to 75% of available datastore capacity. Usage beyond this point creates a non-compliant environment as described in Service Level Agreement for VMware Cloud on AWS
Datastore capacity requiring remediation plan	70%	You should prepare a remediation plan when capacity utilization nears 70%. Either add hosts to augment datastore capacity, or reduce storage utilization.
VMs per vSAN Hosts	200	Maximum number of VMs per ESXi host in a vSAN cluster.

Site Recovery Maximums

Maximum	Value	Description
VMs per SDDC (NSX-T based networking)	1500	This is the supported limit for NSX-T and takes into account both incoming and outgoing replications. Bidirectional protection: The total number of protected VMs across both sites cannot exceed this limit.
VMs per protection group	500	Maximum number of VMs per protection group.
Number of recovery plans	250	Maximum number of recovery plans.
Protection groups per recovery plan	250	Maximum number of protection groups per recovery plan.
VMs per recovery plan	1500	Maximum number of VMs per recovery plan.
Concurrent recoveries	1500	Total number of VM recoveries that you can start simultaneously across multiple recovery plans.
Multiple-site deployment limits	10	With VMware Site Recovery, you can connect multiple protected and recovery sites to a single SDDC. A single SDDC can support a maximum of 10 paired remote sites.

HCX Maximums

Maximum	Value	Description
Site Pairs	10	Registered destination HCX sites (SDDCs) per source HCX Manager
Service Meshes	1	One per source and destination Compute Profile pair
HCX Interconnect Appliances	1	One per Service Mesh
HCX WAN Optimization Appliances	1	One per Service Mesh
HCX Network Extension Appliances	50	Per HCX Manager
Concurrent HCX Bulk Migration Operations	100	Per HCX Manager
Concurrent HCX vMotion Operations	1	Per Service Mesh. Subsequent operations are queued, up to a maximum of 100.
Concurrent HCX Cold Migration Operations	8	Per Service Mesh. Subsequent operations are queued, up to a maximum of 100.
Concurrent HCX vMotion w/vSphere Replication (Replication Assisted vMotion)	100	Scheduled switchover is serial. Switchovers are queued with HCX vMotions.
Maximum HCX Virtual Machine Protections	500	Maximum number of HCX Virtual Machine Protections.
Maximum Network Extensions to NSX-T SDDCs	8	Maximum number of on-premises networks that can be extended to an NSX-T cloud SDDC. 10 Network Extension appliance interfaces minus uplink/management
Maximum Network Extensions with Cisco Nexus 1000v at the Source Site	8	10 Network Extension appliance interfaces minus uplink/ management.
Network Extension Throughput	4-6 Gbps	4-6+ Gbps per HCX Network Extension Appliance. 1+ Gbps per traffic flow. Performance varies depending on: MTU, Latency, Environment Traffic, Network Bandwidth, CPU, Memory resources
Virtual Machine Hardware Version	HW version 7 or higher is required for Bulk migration Hardware version 9 or higher is required for HCX vMotion, RAV migrations, and cold migrations.	Minimum virtual machine hardware versions required for migration.

Maximum	Value	Description
Maximum Virtual Machine Disk Size for HCX Bulk Migration and Replication Assisted vMotion	62 TB with ESXi 5.5 or later. 2 TB with ESXi 5.0 to 5.1	Maximum VM disk size for bulk migration and Replication Assisted vMotion.
Maximum Virtual Machine Disk size for HCX vMotion	Reference the VMDK limitations for the destination site data store	Maximum VM disk size for HCX vMotion.

Horizon Maximums

Maximum	Value	Description
Number of desktops per SDDC	2500	For knowledge worker as defined by Login VSI and WQHD display Actual customer workload might have different characteristics than the benchmark workload used in testing. Therefore, results might vary.

VMware Cloud Services Identity Maximums

Maximum	Value	Description
Logins per Identity Provider	250 users/minute	Each VIDM tenant has a limitation of 250 users max performing login in a minute.
Refresh Auth Token flow	9500 users/minute	Maximum number of users that can exchange an API token for an authentication token using the following API: https://console.cloud.vmware.com/csp/gateway/am/api/swagger-ui.html#/Authentication/getAccessTokenByApiRefreshTokenUsingPOST.
Users in Organizations	no limit	There is no limit to the number of users in an Organization.
AD Connections	no limit	There is no limit to the number of open AD connections.

Deploying and Managing a Software-Defined Data Center

Deploying a Software-Defined Data Center (SDDC) is the first step in making use of the VMware Cloud on AWS service. After you deploy the SDDC, you can view information about it and perform management tasks.

There are a number of factors to consider before deploying your SDDC.

Connected AWS account

When you deploy an SDDC on VMware Cloud on AWS, it is created within an AWS account and VPC dedicated to your organization and managed by VMware. You must also connect the SDDC to an AWS account belonging to you, referred to as the customer AWS account. This connection allows your SDDC to access AWS services belonging to your customer account.

If you are deploying a Single Host SDDC, you can delay linking your customer AWS account for up to two weeks. You cannot scale up a Single Host SDDC to a multiple host SDDC until you link an AWS account. If you are deploying a multiple host SDDC, you must link your customer AWS account when you deploy the SDDC.

AWS VPC Configuration and Availability Requirements

The VPC, subnet, and AWS account you use to must meet several requirements:

- The subnet must be in an AWS Availability Zone (AZ) where VMware Cloud on AWS is available. Start by creating a subnet in every AZ in the AWS Region where the SDDC will be created. That way, you can identify all AZs where an SDDC can be deployed and select the one that best meets your SDDC placement needs, whether you want to keep your VMC workloads close to or isolated from your AWS workloads running in a particular AZ. See Creating a Subnet in Your VPC in the AWS documentation for information about how to use the Amazon VPC console to create a subnet in your VPC.
- The AWS account being linked must have sufficient capacity to create a minimum of 17 ENIs per SDDC in each region where an SDDC is deployed. Although you cannot provision more than 16 hosts in a cluster, SDDC operations including planned maintenance and Elastic DRS can require us to temporarily add as many as 16 more hosts, so we recommend using an AWS account that has sufficient capacity for 32 ENIs per SDDC per region.
- We recommend dedicating a /26 CIDR block to each SDDC and not using that subnet for any other AWS services or EC2 instances. Because some of the IP addresses in this block are reserved for internal use, a /26 CIDR block is the smallest subnet that can accommodate the 33 addresses required for an SDDC.
- Any VPC subnets on which AWS services or instances communicate with the SDDC must be associated with the main route table of the connected VPC. Use of a custom route table or replacement of the main route table is not supported.
- If necessary, you can link multiple SDDCs to a VPC as long as the VPC subnet used for ENI connectivity has a large enough CIDR block to accommodate them. Because all SDDCs in a VPC use the same main route table, make sure that network segments in those SDDCs don't overlap with each other or the VPC's primary CIDR block. Workload VMs on routed SDDC networks can communicate with all subnets in the VPC's primary CIDR block, but are unaware of other CIDR blocks that might exist in the VPC.

Single Host SDDC starter configuration for VMware Cloud on AWS

You can jump start your VMware Cloud on AWS experience with a Single Host SDDC starter configuration. This is a time-limited offering designed for you to prove the value of VMware Cloud on AWS in your environment. The service life of a Single Host environment is limited to 30 days. At any point during the service life of a Single Host SDDC, you can scale it up to a production configuration with three or more hosts with no loss of data. If you don't scale up the Single Host SDDC before the end of the service life, the SDDC is deleted along with all the workloads and data it contains.

Stretched Clusters for VMware Cloud on AWS

You can create an SDDC with a cluster that spans two availability zones. A stretched cluster uses vSAN technology to provide a single datastore for the SDDC and replicate the data across both availability zones. If service in one availability zone is disrupted, workload VMs in the SDDC are brought up in the other availability zone.

The following restrictions apply to stretched clusters:

- The linked VPC must have two subnets, one in each AZ occupied by the cluster.
- A given SDDC can contain either standard (single availability zone) clusters or stretched clusters, but not a mix of both.
- You can't convert a stretched cluster to a standard cluster, or vice versa.
- You need a minimum of six hosts (three in each AZ) to create a stretched cluster. Hosts must be added in pairs.

For additional limitations that can affect stretched clusters, see Configuration Maximums for VMware Cloud on AWS.

Connecting to the SDDC and Configuring SDDC Networks

Before you can migrate your workload VMs and manage them in VMware Cloud on AWS, you'll need to connect your on-premises data center to your SDDC. You can use the public Internet, AWS Direct Connect, or both for this connection. You'll also need to set up one or more Virtual Private Networks (VPNs) to secure network traffic to and from your SDDC, and configure SDDC networking and security features like firewall rules, DNS, and DHCP. The VMware Cloud on AWS Networking and Security guide has more information about how to do that.

Deploy an SDDC from the VMC Console

Deploy an SDDC to host your workloads in the cloud.

To create an SDDC, pick an AWS region to host it, give the SDDC a name, and specify how many ESXi hosts you want the SDDC to contain. If you don't already have an AWS account, you can still create a starter configuration SDDC that contains a single ESXi host.

Procedure

1 Log in to the VMC Console at https://vmc.vmware.com.

2 Click **Create SDDC**.

3 Configure SDDC properties.

a Select the AWS region in which to deploy the SDDC.

The following regions are available:

- US West (Oregon)
- US East (N. Virginia)
- Europe (London)
- Europe (Frankfurt)
- Asia Pacific (Sydney)
- Asia Pacific (Tokyo)
- Europe (Ireland)
- US West (N. California)
- US East (Ohio)
- Asia Pacific (Singapore)
- Canada (Central)
- Europe (Paris)
- Asia Pacific (Mumbai)
- Asia Pacific (Seoul)
- South America (São Paulo)
- Europe (Stockholm)

b Select deployment options.

Option	Description
Single Host	Select this option to create Single Host Starter Configuration SDDC. Single Host Starter Configuration SDDCs expire after 30 days. For more information, see Deploying a Single Host SDDC Starter Configuration.
Multi-Host	Select this option to create an SDDC with three or more hosts.
Stretched Cluster	If you create a multiple-host SDDC, you also have the option to create a stretched cluster that spans two availability zones. The multiple availability zone stretched cluster provides fault tolerance and availability in the event that there is a problem with one of the availability zones. You must have a minimum of six hosts in a stretched cluster, and you must deploy an even number of hosts. **Note** The US West (N. California), Canada (Central), and South America (São Paulo) regions do not currently support Stretched Clusters.

c Enter a name for your SDDC.

You can change this name later if you want to. See Rename an SDDC in the *VMware Cloud on AWS Operations Guide*.

d Select the host type.

Option	Description
i3 (Local SSD)	Provision hosts with a fixed amount of local SSD storage per host.
R5 (EBS)	Provision hosts with EBS-based storage. When provisioning R5 hosts, you can select the storage capacity per host. This allows you to provision greater capacity for workloads requiring large storage capacities.

e If you selected R5 (EBS) hosts, select the storage capacity per host.

The value you select is used for all hosts in the cluster, including any hosts you add to the cluster after creation.

f If you are creating a multiple host SDDC, specify the initial **Number of Hosts** you want in the SDDC.

You can add or remove hosts later if you need to.

Note Storage capacity, performance, and redundancy are all affected by the number of hosts in the SDDC. See Storage Capacity and Data Redundancy for more information.

Host Capacity and **Total Capacity** update to reflect the number of hosts you've specified.

4 Connect to an AWS account.

See AWS VPC Configuration and Availability Requirements for important information about requirements for the AWS account and subnets you create in it.

Option	Description
Skip for now	If you don't have an AWS account or don't want to connect to one you have now, you can postpone this step for up to 14 days. This option is currently available for Single Host SDDCs only.
Use an existing AWS account	From the **Choose an AWS account** drop-down, select an AWS account to use an AWS account that was previously connected to another SDDC. If no accounts are listed in the drop-down, you must **Connect to a new AWS account**.
Connect a new AWS account	From the **Choose an AWS account** drop-down. select **Connect to a new AWS account** and follow the instructions on the page. The VMC Console shows the progress of the connection.

5 (Optional) Click **NEXT** to configure the Management Subnet in the SDDC.

Enter an IP address range for the management subnet as a CIDR block or leave the text box blank to use the default, which is 10.2.0.0/16. You can't change these values after the SDDC has been created, so consider the following when you specify this address range:

- Choose a range of IP addresses that does not overlap with the AWS subnet you are connecting to. If you plan to connect your SDDC to an on-premises data center, the IP address range of the subnet must be unique within your enterprise network infrastructure. It cannot overlap the IP address range of any of your on-premises networks.
- If you are deploying a single-host SDDC, the IP address range 192.168.1.0/24 is reserved for the default compute gateway logical network of the SDDC. If you specify a management network address range that overlaps with 192.168.1.0/24, single-host SDDC creation fails. If you are deploying a multi-host SDDC, no compute gateway logical network is created during deployment, so you'll need to create one after the SDDC is deployed.

  The entire address range 100.64.0.0/10 (reserved for carrier-grade NAT per RFC 6598) is reserved by VMware Cloud on AWS for internal use. You cannot access any remote (on-premises) networks in that address range from workloads in the SDDC, and you cannot you use any addresses in that range within the SDDC. In addition, CIDR blocks 10.0.0.0/15 and 172.31.0.0/16 are reserved for internal use. The management network CIDR block cannot overlap either of these ranges.
- CIDR blocks of size 16, 20, or 23 are supported, and must be in one of the "private address space" blocks defined by RFC 1918 (10.0.0.0/8, 172.16.0.0/12, or 192.168.0.0/16). The primary factor in choosing a Management CIDR block size is the anticipated scalability requirements of the SDDC. The management CIDR block cannot be changed after the SDDC has been deployed, so a /23 block is appropriate only for SDDCs that will not require much growth in capacity.

CIDR block size	Number of hosts (Single AZ)	Number of hosts (Multi AZ)
23	27	22
20	251	246
16	See Configuration Maximums for VMware Cloud on AWS.	

6 Acknowledge that you understand and take responsibility for the costs you incur when you deploy an SDDC, then click **DEPLOY SDDC** to create the SDDC.

Charges begin when you click **DEPLOY SDDC**. You cannot pause or cancel the deployment process after it starts. You won't be able to use the SDDC until deployment is complete. Deployment typically takes about two hours.

What to do next

After your SDDC is created, do the following:

- Configure a VPN connection to the management gateway.

- For full-scale SDDCs, you must configure a logical segment for workload VM networking. Single host SDDCs have a default logical segment. A banner is displayed on the SDDC card after creation is complete to indicate whether you need to create a logical segment. See Create a Network Segment .
- For single host SDDCs, a banner is displayed on the SDDC card to indicate that a default logical segment has been created for this SDDC. If this default segment causes a conflict, delete it and create a new segment. See Create a Network Segment.

Rename an SDDC

You can rename an existing SDDC.

SDDC names are limited to 128 characters. They are not required to be unique.

Procedure

1. Log in to the VMC Console at https://vmc.vmware.com.
2. On the card for the SDDC you want to rename, click **Actions > Rename SDDC**.
3. Type the new SDDC name and click **RENAME**.

Delete an SDDC

Deleting an SDDC terminates all running workloads and destroys all SDDC data and configuration settings including public IP addresses. Deletion of an SDDC cannot be undone.

Procedure

1. Log in to the VMC Console at https://vmc.vmware.com.
2. On the card for the SDDC you want to remove, click **Actions > Delete SDDC**
3. Confirm that you understand the consequences of deleting an SDDC.

   Select all of the following:

   - All workloads in this SDDC will be terminated.
   - You will lose all data and configuration settings in this SDDC.
   - You will lose all UI and API access to this SDDC.
   - All public IP addresses for this SDDC will be released.
   - All direct connect virtual interfaces will be deleted.

   or click **CANCEL** to cancel the process without affecting the SDDC.
4. Click **DELETE SDDC**.

SDDC Upgrades and Maintenance

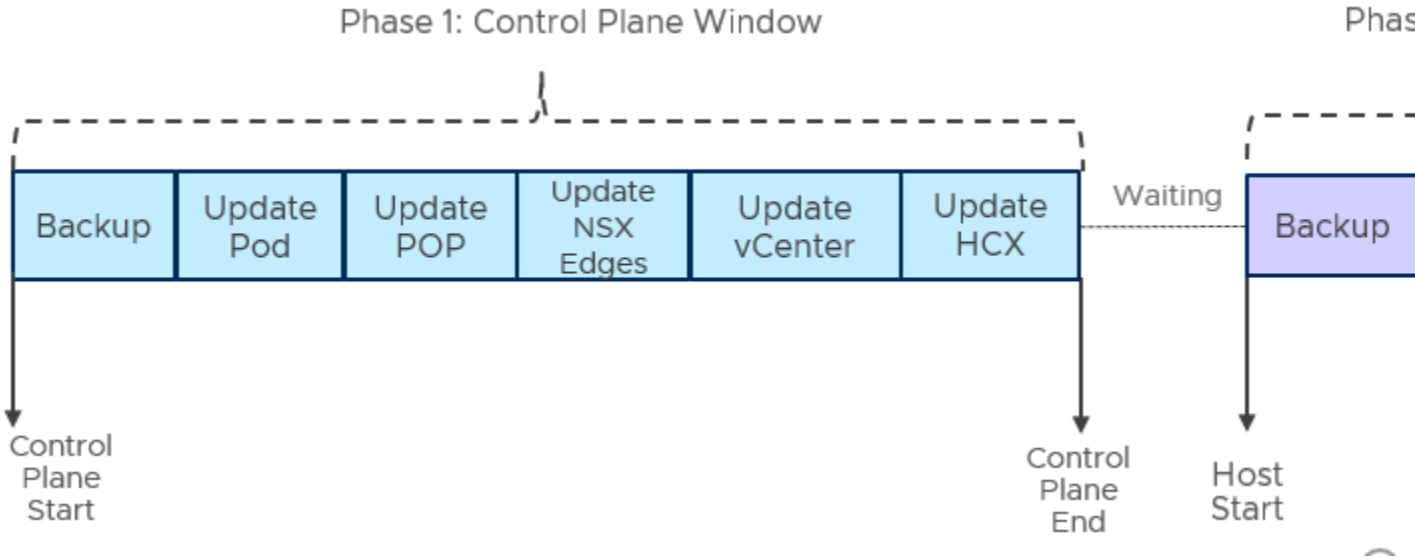
VMware Cloud on AWS regularly performs updates on your SDDCs. These updates ensure continuous delivery of new features and bug fixes, and maintain consistent software versions across the SSDC fleet.

Updates to the SDDC software are mandatory and must be done in a timely manner. When an SDDC update is upcoming, VMware sends a notification email to you. Typically, this occurs 7 days before a regular update and 1-2 days before an emergency update. Delays to upgrades could result in your SDDC running an unsupported software version. See Supported SDDC Versions.

You also receive notifications by email when each phase of the update process starts, completed, is rescheduled, or is canceled. To ensure that you receive these notifications, whitelist vmc-services-notices@vmware.com.

Upgrade Process for SDDCs Using NSX-T

The figure below shows the upgrade process for SDDCs with networking based on NSX-T.



Important During upgrades:

- Do not perform hot or cold workload migrations. Migrations fail if they are started or in progress during maintenance.
- Do not perform workload provisioning (New/Clone VM). Provisioning operations fail if they are started or in progress during maintenance.
- Do not make changes to Storage-based Policy Management settings for workload VMs.
- Ensure that there is enough storage capacity (> 30% slack space) in each cluster.

Maintenance is performed in three phases.

Phase 1: Host Networking Updates. These are the updates to the host networking software (NSX-T) in the SDDC. An additional host is temporarily added to the SDDC to provide enough capacity for the update. vMotion and DRS activities occur to facilitate the update. During this time, your workloads and other resources function as usual subject to the constraints outlined above.

You will receive a notification when Phase 1 starts. After Phase 1 is complete, there is a waiting period until Phase 2 starts. Phase 2 is initiated at a designated start time that is usually days after the Phase 1 start time. This allows for enough time for Phase 1 to finish successfully.

Phase 2: Control Plane Updates. These are the updates to vCenter Server. During this time you do not have access to vCenter Server or other management VMs in your SDDC, but workloads and other resources function as usual subject to the constraints outlined above. However, there is a short downtime of 10-20 seconds for North-South network routes when NSX-T Edges are updated. This downtime usually occurs 45 to 75 minutes after the start of the control plane update.

When Phase 2 is complete, you receive a notification. Phase 3 begins immediately after the Phase 2 update is complete. Therefore, it does not have a designated start time.

Phase 3: Host Updates. These are the updates to the ESXi hosts in the SDDC. As in Phase 1, an additional host is temporarily added to your SDDC to provide enough capacity for the update. vMotion and DRS activities occur to facilitate the update. During this time, your workloads and other resources function as usual subject to the constraints outlined above.

When Phase 3 is complete, you receive a notification.

When an SDDC upgrade for your SDDC is scheduled, you can see information about upcoming or ongoing maintenance in the Maintenance Tab of the VMC Console. For more information, see View an SDDC Maintenance Schedule Reservation.

Updates for VMware Hybrid Cloud Extension (HCX)

For customers using HCX:

- The VMware Hybrid Cloud Extension (HCX) for the SDDC managers will be upgraded to the latest release.
- Avoid starting HCX migrations that might overlap with the SDDC upgrade window. HCX bulk migration processes might be halted, and HCX vMotion migrations might fail.
- For more details, see the *VMware HCX User Guide* at https://docs.vmware.com/en/VMware-NSX-Hybrid-Connect/index.html.

Updates for the VMware vCenter Cloud Gateway

For customers using the VMware vCenter Cloud Gateway:

- The VMware vCenter Cloud Gateway will be updated to the latest release.
- The user interface for the VMware vCenter Cloud Gateway might be inaccessible during the upgrade of the appliance.

- For more information, see the documentation for the vCenter Cloud Gateway Appliance at https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vsphere.vmc-aws-manage-data-center.doc/GUID-58C1AC46-3F99-4F93-BB1F-FD1878B49374.html.

Updates for Horizon Enterprise

For information about the impact of an SDDC upgrade on a Horizon Enterprise installation running on VMware Cloud on AWS, see https://kb.vmware.com/s/article/74599.

View an SDDC Maintenance Schedule Reservation

You can specify a day and time range for scheduled SDDC maintenance. You can also reschedule upcoming maintenance.

VMware periodically schedules software maintenance for its services, including VMware Cloud on AWS. During maintenance, your workload VMs will remain online, but you won't be able to view or modify your vCenter Server and SDDC networking.

VMware periodically schedules software maintenance for its services, including VMware Cloud on AWS. During maintenance, your workload VMs will remain online, but you won't be able to view or modify your vCenter Server and SDDC networking. If you don't specify a date and time preference, the maintenance takes places on a default schedule.

Note You cannot specify a start time for critical patches.

Prerequisites

This operation is restricted to users who have the CloudAdmin role.

Procedure

1. Log in to the VMC Console at https://vmc.vmware.com.
2. Navigate to the **Maintenance** tab of your SDDC.

   If maintenance is scheduled for this SDDC, you'll see an **Upcoming maintenance** card showing a date and time range for the maintenance.
3. (Optional) Reschedule upcoming maintenance.
   a. On the an **Upcoming maintenance** card, click **RESCHEDULE** to see a list of available days and start times for the upcoming maintenance.
   b. Choose a maintenance day and start time and click **SAVE**.

      All available start times are listed. Some times might not be available because they have already been taken by other SDDCs.

4 (Optional) Choose a preferred maintenance day and start time.

The **Maintenance window preference** card displays your current maintenance window preference.

a Click **EDIT PREFERENCE** to open the **Edit Maintenance Schedule Preference** page.

b Choose a preferred maintenance day and start time and click **SAVE**.

All available start times are listed. Some times might not be available because they have already been taken by other SDDCs. Changes in preference do not affect your existing reservations.

The system updates your maintenance window preferences and displays the updated preferences.

Convert UTC Time to Local Time

Maintenance windows are scheduled using UTC time. You can convert this to your local time.

Procedure

- Calculate your local time from a UTC time using one of the following methods.

Option	Description
Use a time zone calculator	Use the time zone calculator at https://www.timeanddate.com/worldclock/converter.html to convert from UTC time to your time.
Compute local time using UTC offset	a Determine the time offset from UTC time for your local time zone. See https://en.wikipedia.org/wiki/List_of_UTC_time_offsets. b Add the time offset to the UTC time (expressed in 24-hour time). c If daylight saving time is in effect in your local time zone, adjust for daylight saving time.

View Billing Information

Billing for VMware Cloud on AWS is handled through VMware Cloud services.

Your billing cycle begins on the day of the month when the first service for your organization was set up. For example, if you set up the first service in your organization on the 15th of the month, your billing cycle runs from the 15th of the month through the 14th of the following month.

Host usage for VMware Cloud on AWS is tracked in alignment with your billing cycle. The host usage shown on your bill is the entirety of your host usage during the billing period.

Other types of usage, including data transfer out, IP address usage and remaps, and EBS usage are received on the 5th of each month and include usage up to the last day of the previous month. For these types of usage, there is a time lag between when the usage occurs and when it shows up on your bill. The amount of time lag depends on where the beginning of your billing cycle is in relation to the 5th of the month.

For example, consider two users, Alice and Bob. Alice's billing cycle begins on the 3rd of the month, while Bob's billing cycle begins on the 12th.

Alice's bill on the 3rd of June shows:

- Host usage from May 3 through June 2
- Other usage from April 1 through April 30

Bob's bill on the 12th of June shows:

- Host usage from May 12 through June 11
- Other usage from May 1 through May 31

Procedure

- View your bill as described in https://docs.vmware.com/en/VMware-Cloud-services/services/Using-VMware-Cloud-Services/GUID-B57490E3-1916-4214-B193-9D9E7AF3B10A.html.

Roles and Permissions in the SDDC

Every SDDC defines a role named CloudAdmin. An organization member in this role has administrative rights over all objects owned by the organization.

SDDC Roles

CloudAdmin	The CloudAdmin role has the necessary privileges for you to create and manage workloads on your SDDC. However, you cannot access or configuring the certain management components that are supported and managed by VMware, such as hosts, clusters, and management virtual machines.
CloudGlobalAdmin	The CloudGlobalAdmin role is associated with global privileges and allows you to create and manage content library objects and perform some other global tasks.

Understanding Authorization in vSphere in *Managing the VMware Cloud on AWS Data Center* has more information about roles and rights in the system.

The CloudAdmin is responsible for creating users, groups, and roles in the SDDC, typically by using vCenter Single Sign-On and Hybrid Linked Mode. For the majority of use cases, rights and roles in the SDDC vCenter can be configured the same way that they are in an on-premises vCenter linked to the SDDC with Hybrid Linked Mode, so that your organization's workflows can benefit from having the same access controls in both environments.

Because it is a service, VMware Cloud on AWS limits access by all tenants (organization members) to vSphere resources that must remain under the control of the service provider (VMware). It also places limitations on the rights you can associate with roles you create, and prevents you from modifying the CloudAdmin role or any roles that have more rights than the CloudAdmin role. The service provider is granted super-user rights over all users, groups, rights, roles, and inventory objects in your organization.

Note The CoudGlobalAdmin role, which has a subset of the privileges granted to the CloudAdmin role, is deprecated as of SDDC version 1.7.

See Understanding Authorization in vSphere in the *VMware vSphere Documentation* for more information about roles and rights in the system.

AWS Roles

To create an SDDC, VMware must add several required AWS roles and permissions to your AWS account. Most permissions are removed from these roles after the SDDC has been created. The others remain with the roles in your AWS account.

Important You must not change any of the remaining AWS roles and permissions. Doing so will render your SDDC inoperable.

For more information, see AWS Roles and Permissions

Managing SDDC Hosts and Clusters

2

You can add and remove clusters and hosts from your cloud SDDC, as long as this would not bring your SDDC below the minimum or above the maximum number of allowed clusters and hosts.

The initial cluster created during SDDC creation is named Cluster-1. Additional clusters that you create are numbered sequentially, Cluster-2, Cluster-3, and so on.

When you add hosts to an SDDC with multiple clusters, you can select the cluster to add them to.

This chapter includes the following topics:

VMware Cloud on AWS Host Types

VMware Cloud on AWS provides different host types for use in your SDDC.

A given cluster in your SDDC must contain hosts of the same type.

Some host types might not be available within a particular region or availability zone.

i3	The i3 host type is the default host type. i3 hosts have a fixed compute, memory, and storage allocation of 36 cores, 512GB RAM, and 10.7TB per host.
r5	When you create an SDDC or add an additional cluster, you have the option to select the r5 host type. r5 hosts use EBS-based storage. When you create a cluster using this host type, you can select the storage

capacity per host. These hosts are ideal for workloads requiring large storage capacities.

Add a Cluster

You can add clusters to a cloud SDDC up to the maximum configured for your account.

Additional clusters are created in the same availability zone or availability zones as the initial SDDC.

When you deploy an additional cluster, whether it is a single availability zone cluster or stretched cluster, you do not have to select the same host type used in the initial cluster created for the SDDC. However, all hosts in a given cluster must be of the same type.

Logical networks you have created for your SDDC are automatically shared across all clusters. Compute and storage resources are configured similarly for all clusters. For example:

- Each cluster contains a Compute-ResourcePool and a Mgmt-ResourcePool, with the same permissions that these have in the initial SDDC cluster.
- Each cluster contains a vsanDatastore and a workloadDatastore, with the same permissions that these have in the initial SDDC cluster.

Procedure

1. Log in to the VMC Console at https://vmc.vmware.com.
2. On the card for the SDDC you want to add a cluster to, select **Actions > Add Cluster**.
3. Select the host type.

Option	Description
i3 (Local SSD)	Provision hosts with a fixed amount of local SSD storage per host.
R5 (EBS)	Provision hosts with EBS-based storage. When provisioning R5 hosts, you can select the storage capacity per host. This allows you to provision greater capacity for workloads requiring large storage capacities.

4. Specify the number of CPU cores to enable for each host in the cluster.

   All CPU cores are enabled by default on each host in the cluster. If you'd like to disable some of the cores to save on licensing costs for applications that are licensed on a per-core basis, you can enable a subset of the available cores. This subset applies to all hosts in the cluster. Other cores on each host are disabled and remain disabled for the lifetime of the host.

   Important Reducing core count affects the compute performance of all workloads on the host and increases the likelihood of system performance degradation. For example, vCenter and vSAN overhead can become more noticeable, and operations like adding clusters and hosts can take longer to complete.

5. Select the number of hosts in the cluster.

6 If you selected R5 (EBS) hosts, select the storage capacity per host.

The value you select is used for all hosts in the cluster, including any hosts you add to the cluster after creation.

7 click **Add Cluster**.

A progress bar shows the progress of cluster creation.

Remove a Cluster

You can remove any cluster in an SDDC except for the initial cluster, Cluster-1.

When you delete a cluster, all workload VMs in the cluster are immediately terminated and all data and configuration information is deleted. You lose API and UI access to the cluster. Public IP addresses associated with VMs in the cluster are released.

Currently deleting a cluster from an SDDC deployed with a multiple availability zone cluster is not supported.

Prerequisites

- Migrate any workload VMs that you want to keep to another cluster in the SDDC.
- Make a copy of any data that you want to retain.

Procedure

1 Log in to the VMC Console at https://vmc.vmware.com.

2 Click on the SDDC and then click **Summary**.

3 On the card for the cluster you want to remove, click **Delete Cluster**.

Before you can delete the cluster, you must select all of the check boxes to confirm that you understand the consequences of this action. When all the check boxes are selected, the **Delete Cluster** button is enabled. Click it to delete the cluster.

Add Hosts

Add hosts to your SDDC to increase the amount of computing and storage capacity available in your SDDC.

You can add hosts to your SDDC as long as you do not exceed the maximum number of hosts allotted to your account.

Procedure

1 Log in to the VMC Console at https://vmc.vmware.com.

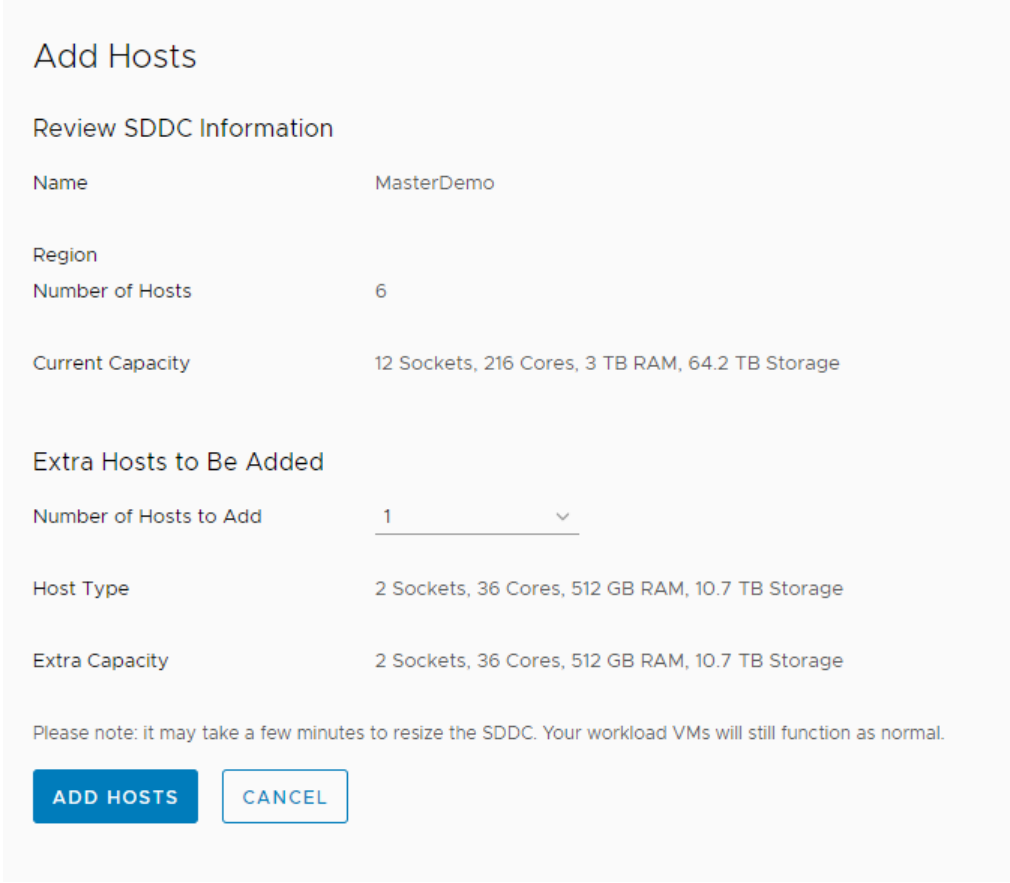
2 Click on the SDDC and then click **Summary**.

3 Select where to add the hosts.

- If the SDDC has only one cluster, select **Actions > Add Hosts** from the SDDC card.

- If the SDDC has more than one cluster, select **Actions > Add Hosts** from the card for the cluster where you want to add the hosts.

The Add Hosts page is displayed.



4 Select the number of hosts to add, and click **Add Hosts**.

If you are adding hosts to a multiple availability zone cluster, you must add them in multiples of two hosts at a time.

One or more hosts are added to your SDDC cluster.

Remove Hosts

You can remove hosts from your SDDC as long as the number of hosts in your SDDC cluster remains above the minimum.

The minimum number of hosts for a single availability zone cluster is 3. The minimum number for a multiple availability zone cluster is 6.

Whenever you reduce cluster size, storage latency increases due to process overhead introduced by host removal. The duration of this overhead varies with the amount of data involved. It can take as little as an hour, though an extreme case could require more than 24 hours. While cluster-size reduction (scale-in) is underway, workload VMs supported by the affected clusters can experience significant increases in storage latency.

When you remove a host, VMs running on that host are evacuated to other hosts in the SDDC cluster. The host is placed into maintenance mode and then removed.

Prerequisites

Ensure that you have sufficient capacity in your cluster to hold the workload VMs that will be evacuated from the hosts that you remove.

Procedure

1. Log in to the VMC Console at https://vmc.vmware.com.
2. Click on your SDDC and then click **Summary**.
3. Select **Actions > Remove Hosts**
   - If the SDDC has only one cluster, select **Actions > Remove Hosts** from the SDDC card.
   - If the SDDC has more than one cluster, select **Actions > Remove Hosts** from the card for the cluster from which you want to remove the hosts.
4. Select the number of hosts you want to remove.

   If you are removing hosts from a multiple availability zone cluster, you must remove them in multiples of two.

   Note All vSAN storage policies have requirements for a minimum number of hosts. If you attempt to reduce the number of hosts below this minimum, the operation fails. See vSAN Policies in *Managing the VMware Cloud on AWS Data Center*.
5. Select the **I understand that this action cannot be undone** check box.
6. Click **Remove**.

About Elastic DRS

Elastic DRS uses an algorithm to maintain an optimal number of provisioned hosts to keep cluster utilization high while maintaining desired CPU, memory, and storage performance.

Elastic DRS monitors the current demand on your SDDC and applies an algorithm to make recommendations to either scale-in or scale-out the cluster. A decision engine responds to a scale-out recommendation by provisioning a new host into the cluster. It responds to a scale-in recommendation by removing the least-utilized host from the cluster.

Elastic DRS is not supported for the following types of SDDCS:

- SDDCs deployed with multiple availability zone stretched clusters.
- Single host starter SDDCs

When the Elastic DRS algorithm initiates a scale-out, all Organization users receive a notification in the VMC Console and through email.

How the Elastic DRS Algorithm Works

The Elastic DRS algorithm monitors resource utilization in a cluster over time. After allowing for spikes and randomness in the utilization, it makes a recommendation to scale out or scale in a cluster and generates an alert. This alert is processed immediately by provisioning a new host or removing a host from the cluster.

The algorithm runs every 5 minutes and uses the following parameters:

- Minimum and maximum number of hosts the algorithm should scale up or down to.
- Thresholds for CPU, memory and storage utilization such that host allocation is optimized for cost or performance. These thresholds, which we list on the Select Elastic DRS Policy page, are predefined for each DRS policy type and cannot be altered by user.

Scale-out Recommendation

A scale-out recommendation is generated when any of CPU, memory, or storage utilization remains consistently above thresholds. For example, if storage utilization goes above the high threshold but memory and CPU utilization remain below their respective thresholds, a scale-out recommendation is generated. A vCenter Server event is posted to indicate the start, completion, or failure of scaling out on the cluster.

Scale-in Recommendation

A scale-in recommendation is generated when CPU, memory, and storage utilization all remain consistently below thresholds. The scale-in recommendation is not acted upon if the number of hosts in the cluster is at the minimum specified value. A vCenter Server event is posted to indicate the start, completion, or failure of the scaling in operation on the cluster.

Note Whenever you reduce cluster size, storage latency increases due to process overhead introduced by host removal. The duration of this overhead varies with the amount of data involved. It can take as little as an hour, though an extreme case could require more than 24 hours. While cluster-size reduction (scale-in) is underway, workload VMs supported by the affected clusters can experience significant increases in storage latency.

Time Delays Between Two Recommendations

A safety check is included in the algorithm to avoid processing frequently generated events and to provide some time to the cluster to cool off with changes due to last event processed. The following time intervals between events are enforced:

- A 30 minute delay between two successive scale-out events.
- A three hour delay to process a scale-in event after scaling out the cluster.

Interactions of Recommendations with Other Operations

The following operations might interact with Elastic DRS recommendations:

- User-initiated addition or removal of hosts.

Normally, you would not need to manually add or remove hosts from a cluster with Elastic DRS enabled. You can still perform these operations, but an Elastic DRS recommendation might revert them at some point.

If a user-initiated add or remove host operation is in progress, the current recommendation by the Elastic DRS algorithm is ignored. After the user-initiated operation completes, the algorithm may recommend a scale-in or scale-out operation based on the changes in the resource utilization and current selected policy.

If you start an add or remove host operation while an Elastic DRS recommendation is being applied, the add or remove host operation fails with an error indicating a concurrent update exception.

- Planned Maintenance Operation

  A planned maintenance operation means a particular host needs to be replaced by a new host. While a planned maintenance operation is in progress, current recommendations by the Elastic DRS algorithm are ignored. After the planned maintenance completes, the algorithm runs again and fresh recommendations are applied. If a planned maintenance event is initiated on a cluster while an Elastic DRS recommendation is being applied to that cluster, the planned maintenance task is queued. After the Elastic DRS recommendation task completes, the planned maintenance task starts.

- Auto-remediation

  During auto-remediation, a failed host is replaced by a new host, and its host tags are applied to the replacement host. While auto-remediation is in progress, the current recommendations by the Elastic DRS algorithm are ignored. After auto-remediation completes, the algorithm runs again and fresh recommendations are applied. If an auto-remediation event is initiated for a cluster while an Elastic DRS recommendation is being applied to that cluster, the auto-remediation task is queued. After the Elastic DRS recommendation task completes, the auto-remediation task starts.

- SDDC maintenance window

  If an SDDC is undergoing maintenance or is scheduled to undergo planned maintenance in the next 6 hours, EDRS recommendations are ignored.

Select Elastic DRS Policy

Set the Elastic DRS policy on a cluster to optimize for either cost or performance.

Elastic DRS is set to **Scale Up for Storage Only** by default. In this mode, Elastic DRS adds hosts only when storage utilization exceeds the threshold of 75%.

When you enable Elastic DRS, you must choose a DRS policy. Each policy has its own set of resource utilization thresholds. Scale-out is triggered when a cluster reaches the high threshold for any resource. Scale-in is triggered only after all of the low thresholds have been reached.

Table 2-1. Optimize for Best Performance

Resource	High Threshold	Low Threshold
CPU	90% utilization	50% utilization
Memory	80% utilization	50% utilization
Storage	70% utilization	20% utilization

Table 2-2. Optimize for Lowest Cost

Resource	High Threshold	Low Threshold
CPU	90% utilization	60% utilization
Memory	80% utilization	60% utilization
Storage	70% utilization	20% utilization

Procedure

1. Log in to the VMC Console at https://vmc.vmware.com.
2. Click on the SDDC and then click **Summary**.
3. On the card for the SDDC or cluster, click **Edit EDRS Settings**.
4. Select the Elastic DRS policy you want to use.

Option	Description
Scale Up for Storage Only	This is the default setting. Elastic DRS adds hosts only when storage utilization exceeds 75%. No scale in operations are performed.
Optimize for Best Performance	Select the **Minimum cluster size** and **Maximum cluster size**. Elastic DRS adds hosts more quickly and removes hosts more slowly in order to provide best performance.
Optimize for Lowest Cost	Select the **Minimum cluster size** and **Maximum cluster size**. Elastic DRS adds hosts more slowly and removes hosts more quickly in order to provide the lowest cost.

5. Click **Save**.

Using Policies and Profiles

A CloudAdmin user can establish policies and profiles in the SDDC that govern the placement of workload VMs.

Creating and Managing Compute Policies

Compute policies provide a way to specify how the vSphere Distributed Resource Scheduler (DRS) should place VMs on hosts in a resource pool. Use the vSphere client Compute Policies editor to create and delete compute policies.

You can create or delete, but not modify, a compute policy. If you delete a category tag used in the definition of the policy, the policy is also deleted. The system does not check for policy conflicts. If, for example, multiple VMs subject to the same VM-Host affinity policy are also subject to a VM-VM anti-affinity policy, DRS will be unable to place the VMs in a way that complies with both policies.

Note Affinity policies in your VMware Cloud on AWS SDDC are not the same as the vSphere DRS affinity rules you can create on premises. They can be used in many of the same ways, but have significant operational differences. A compute policy applies to all hosts in an SDDC, and cannot typically be enforced in the same way that a DRS "must" policy is enforced. The policy create/delete pages have more information about operational details for each policy type.

Monitoring Compliance

Open the VM Summary page in the vSphere client to view the compute policies that apply to a VM and its compliance status with each policy.

Create or Delete a VM-Host Affinity Policy

A VM-Host affinity policy describes a relationship between a category of VMs and a category of hosts.

VM-Host affinity policies can be useful when host-based licensing requires VMs that are running certain applications to be placed on hosts that are licensed to run those applications. They can also be useful when virtual machines with workload-specific configurations require placement on hosts that have certain characteristics.

A VM-Host affinity policy establishes an affinity relationship between a category of virtual machines and a category of hosts. After the policy is created, the placement engine in your SDDC deploys VMs in the category covered by the policy on hosts in the category covered by the policy.

To prevent a VM-Host affinity policy from blocking the upgrade of a host or cluster, VM-Host affinity policies are constrained in several ways.

- A policy cannot prevent a host from entering maintenance mode.
- A policy cannot prevent a host configured for HA from executing a failover. VMs with an affinity for the failed host can be migrated to any available host in the cluster.
- A policy cannot prevent a VM from powering-on. If a VM subject to a host affinity policy specifies a resource reservation that no host can meet, it is powered on on any available host.

These constraints are lifted as soon as a compliant host becomes available.

Prerequisites

This operation is restricted to users who have the CloudAdmin role.

Procedure

1 Create a category and tag for VMs that you want to include in a VM-Host affinity policy.

  Pick a category name that describes common characteristics, such as license requirements, of VMs you plan to tag as members of that category.

2 Create a category and tag for hosts that you want to include in a VM-Host affinity policy.

   You can use existing tags and categories or create new ones specific to your needs. See vSphere Tags and Attributes for more about creating and using tags.

3 Tag the VMs and hosts that you want to include in a VM-Host affinity policy.

4 Create a VM-Host affinity policy.

   a In your SDDC, click **OPEN VCENTER**.

   b From the vSphere Client Home, click **Policies and Profiles > Compute Policies**.

   c Click **Add** to open the **New Compute Policy** Wizard.

   d Fill in the policy **Name** and choose **VM-Host affinity** from the **Policy type** drop-down control.

      The policy **Name** must be unique within your SDDC.

   e Provide a **Description** of the policy, then use the **VM tag** and **Host Tag** drop-down controls to choose a **Category** and **Tag** to which the policy applies.

      Unless you have multiple VM tags associated with a category, the wizard fills in the VM tag after you select the tag **Category**.

   f Click **Create** to create the policy.

5 (Optional) To delete a compute policy, open the vSphere Web Client, click **Policies and Profiles > Compute Policies** to show each policy as a card. Click DELETE to delete a policy.

Create or Delete a VM-Host Anti-Affinity Policy

A VM-Host anti-affinity policy describes a relationship between a category of VMs and a category of hosts.

A VM-Host anti-affinity policy can be useful when you want to avoid placing virtual machines that have specific host requirements such as a GPU or other devices, or capabilities such as IOPS control, on hosts that can't support those requirements. After the policy is created, the placement engine in your SDDC avoids deploying VMs covered by the policy on hosts covered by the policy.

To prevent a VM-Host anti-affinity policy from blocking the upgrade of a host or cluster, these policies are constrained in several ways.

- A policy cannot prevent a host from entering maintenance mode.
- A policy cannot prevent a host configured for HA from executing a failover. VMs with an anti-affinity for the failed host can be migrated to any available host in the cluster.
- A policy cannot prevent a VM from powering-on. If a VM subject to a VM-Host anti-affinity policy specifies a resource reservation that no host can meet, it is powered on on any available host.

These constraints are lifted as soon as a compliant host becomes available.

Prerequisites

This operation is restricted to users who have the CloudAdmin role.

Procedure

1. Create a category and tag for VMs that you want to include in a VM-Host anti-affinity policy.

   Pick a category name that describes common characteristics of VMs you plan to tag as members of that category.

2. Create a category and tag for hosts that you want to include in a VM-Host anti-affinity policy.

   You can use existing tags and categories or create new ones specific to your needs. See vSphere Tags and Attributes for more about creating and using tags.

3. Tag the VMs and hosts that you want to include in a VM-Host anti-affinity policy.

4. Create a VM-Host anti-affinity policy.

   a. In your SDDC, click **OPEN VCENTER**.

   b. From the vSphere Client Home, click **Policies and Profiles > Compute Policies**.

   c. Click **Add** to open the **New Compute Policy** Wizard.

   d. Fill in the policy **Name** and choose **VM-Host anti-affinity** from the **Policy type** drop-down control.

      The policy **Name** must be unique within your SDDC.

   e. Provide a **Description** of the policy, then use the **VM tag** and **Host Tag** drop-down controls to choose a **Category** and **Tag** to which the policy applies.

      Unless you have multiple tags associated with a VM or host in a given category, the wizard fills in the VM tag and Host tag after you select the tag **Category**.

   f. Click **Create** to create the policy.

5. (Optional) To delete a compute policy, open the vSphere Web Client, click **Policies and Profiles > Compute Policies** to show each policy as a card. Click DELETE to delete a policy.

Create or Delete a VM-VM Affinity Policy

A VM-VM affinity policy describes a relationship between members of a category of VMs.

VM-VM affinity policies can be useful when two or more VMs in a category can benefit from locality of data reference or where placement on the same host can simplify auditing.

A VM-VM affinity policy establishes an affinity relationship between virtual machines in a given category. After the policy is created, the placement engine in your SDDC attempts to deploy all VMs in the category covered by the policy on the same host.

Prerequisites

This operation is restricted to users who have the CloudAdmin role.

Procedure

1. Create a category and tag for each group of VMs that you want to include in a VM-VM affinity policy.

   You can use existing tags and categories or create new ones specific to your needs. See vSphere Tags and Attributes for more about creating and using tags.
2. Tag the VMs that you want to include in each group.
3. Create a VM-VM affinity policy.
   a. In your SDDC, click **OPEN VCENTER**.
   b. From the vSphere Client Home, click **Policies and Profiles > Compute Policies**.
   c. Click **Add** to open the **New Compute Policy** Wizard
   d. Fill in the policy **Name** and choose **VM-VM affinity** from the **Policy type** drop-down control.

      The policy **Name** must be unique within your SDDC.
   e. Provide a **Description** of the policy, then use the **VM tag** drop-down control to choose the **Category** and **Tag** to which the policy applies.

      Unless you have multiple VM tags associated with a category, the wizard fills in the VM tag after you select the tag **Category**.
   f. Click **Create** to create the policy.
4. (Optional) To delete a compute policy, open the vSphere Web Client, click **Policies and Profiles > Compute Policies** to show each policy as a card. Click DELETE on the policy card to delete the policy.

Create or Delete a VM-VM Anti-Affinity Policy

A VM-VM anti-affinity policy describes a relationship among a category of VMs.

A VM-VM anti-affinity policy discourages placement of virtual machines in the same category on the same host. This kind of policy can be useful when you want to place virtual machines running critical workloads on separate hosts, so that the failure of one host does not affect other VMs in the category. After the policy is created, the placement engine in your SDDC attempts to deploy VMs in the category on separate hosts.

Enforcement of a VM-VM anti-affinity policy can be affected in several ways:

- If the policy applies to more VMs than there are hosts in the SDDC, or if it's not possible to place a VM on a host that satisfies the policy, DRS attempts to place the VM on any suitable host.
- If a provisioning operation specifies a destination host, that specification is always honored even if it violates the policy. DRS will try to move the VM to a compliant host in a subsequent remediation cycle.

Prerequisites

This operation is restricted to users who have the CloudAdmin role.

Procedure

1. Create a category and tag for each group of VMs that you want to include in a VM-VM anti-affinity policy.

   You can use existing tags and categories or create new ones specific to your needs. See vSphere Tags and Attributes for more about creating and using tags.
2. Tag the VMs that you want to include in each group.
3. Create a VM-VM anti-affinity policy.
   a. In your SDDC, click **OPEN VCENTER**.
   b. From the vSphere Client Home, click **Policies and Profiles > Compute Policies**.
   c. Click **Add** to open the **New Compute Policy** Wizard.
   d. Fill in the policy **Name** and choose **VM-VM anti affinity** from the **Policy type** drop-down control.

      The policy **Name** must be unique within your SDDC.
   e. Provide a **Description** of the policy, then use the **VM tag** drop-down control to choose the **Category** and **Tag** to which the policy applies.

      Unless you have multiple VM tags associated with a category, the wizard fills in the VM tag after you select the tag **Category**.
   f. Click **Create** to create the policy.
4. (Optional) To delete a compute policy, open the vSphere Web Client, click **Policies and Profiles > Compute Policies** to show each policy as a card. Click DELETE to delete a policy.

Create or Delete a Disable DRS vMotion Policy

A DisableDRSvMotion policy applied to a VM prevents DRS from migrating the VM to a different host unless the current host fails or is put into maintenance mode.

This type of policy can be useful for a VM running an application that creates resources on the local host and expects those resources to remain local. If DRS moves the VM to another host for load-balancing or to meet reservation requirements, resources created by the application are left behind and performance can be degraded when locality of reference is compromised.

A Disable DRS vMotion policy takes effect after a tagged VM is powered on, and is intended to keep the VM on its current host as long as the host remains available. The policy does not affect the choice of the host where a VM is powered on.

Prerequisites

This operation is restricted to users who have the CloudAdmin role.

Procedure

1. Create a category and tag for each group of VMs that you want to include in a DisableDRSvMotion policy.

2 Tag the VMs that you want to include in each group.

   You can use existing tags and categories or create new ones specific to your needs. See vSphere Tags and Attributes for more about creating and using tags.

3 Create a Disable DRS vMotion policy.

   a In your SDDC, click **OPEN VCENTER**.

   b From the vSphere Client Home, click **Policies and Profiles > Compute Policies**.

   c Click **Add** to open the **New Compute Policy** Wizard.

   d Fill in the policy **Name** and choose **Disable DRS vMotion** from the **Policy type** drop-down control.

      The policy **Name** must be unique within your SDDC.

   e Provide a **Description** of the policy, then use the **VM tag** drop-down control to choose the VM category to which the policy applies.

      Unless you have multiple VM tags associated with a category, the wizard fills in the VM tag after you select the tag category.

   f Click **Create** to create the policy.

4 (Optional) To delete a compute policy, open the vSphere Web Client, click **Policies and Profiles > Compute Policies** to show each policy as a card. Click DELETE to delete a policy.

Working With SDDC Add-On Services

3

When you log in to the VMC Console, you'll see cards for **My Services** and **More Services**. You can add services from the **More Services** list to your **My Services** list to make them available in your SDDC.

This chapter includes the following topics:

Using the vRealize Log Insight Cloud Add-On

The vRealize Log Insight Cloud collects and analyzes logs generated in your SDDC.

A trial version of the vRealize Log Insight Cloud is enabled by default in a new SDDC. The trial period begins when a user in your organization accesses the vRealize Log Insight Cloud add-on and expires in thirty days. After the trial period, you can choose to subscribe to this service or continue to use a subset of service features at no additional cost. For more information about using vRealize Log Insight Cloud, see the vRealize Log Insight Cloud Documentation.

SDDC Audit Log Events

vRealize Log Insight Cloud classifies SDDC events matching the following rules as audit data.

ESXi Audit Events

```
"text=(esx AND audit)"
"text =(hostd AND vmsvc AND vm AND snapshot)"
"text =(vim.event.HostConnectionLostEvent)"
```

vCenter Audit Events

```
"text = (vpxd AND event AND vim AND NOT originator)"
```

NSX-T Audit Events

```
"text = (nsx AND audit AND true AND comp AND reqid)"
```

NSX-T Firewall and Packet Log Events

```
"text = (nsx AND firewall AND inet)"
"text = (firewall_pktlog AND inet)"
```

Getting Templates, ISOs, and Other Content into Your SDDC

4

You might have a variety of `.vmtx` templates, OVF and OVA templates, ISO images, scripts, and other content that you want to use in your SDDC.

Content Type	How to transfer it to your SDDC
`.vmtx` template	■ Use the Content Onboarding Assistant to transfer the template to your SDDC. ■ Clone the templates to OVF template in an on-premises Content Library and subscribe to the Content Library from your SDDC.
OVF template	■ Add the template to an on-premises Content Library and subscribe to the content library from your SDDC. ■ Create a local Content Library in your SDDC, and upload the OVF template to it. ■ Deploy the OVF template directly from a client machine to your SDDC in the vSphere Web Client. Right-click the **Compute-ResourcePool** resource pool and select **Deploy OVF template**.
OVA template	Deploy the OVA template directly from a client machine to your SDDC using the vSphere Web Client. Right-click the **Compute-ResourcePool** resource pool and select **Deploy OVF template**
ISO image	■ Upload the ISO image to the workloadDatastore. ■ Import the ISO image into an on-premises Content Library and subscribe to the Content Library from your SDDC. ■ Create a local Content Library in your SDDC, and upload the ISO image to it. ■ Use the Content Onboarding Assistant to transfer the ISO image to your SDDC.
scripts or text files	■ Import the file into an on-premises Content Library and subscribe to the Content Library from your SDDC. ■ Create a local Content Library in your SDDC and upload the file to it. ■ Use the Content Onboarding Assistant to transfer the file to your SDDC.

This chapter includes the following topics:

Use the Content Onboarding Assistant to Transfer Content to Your SDDC

The Content Onboarding Assistant automates the transfer of `.vmtx` templates, ISO images, scripts, and other files to your cloud SDDC.

You have two options for how the Content Onboarding Assistant transfers `.vmtx` templates to your SDDC

- Convert these templates to OVF templates in the SDDC Content Library. This option takes less time.
- Transfer these templates as `.vmtx` templates in the vCenter Server inventory. In this case, the templates undergo an intermediate conversion to OVF and then back to `.vmtx` templates.

You can use the Content Onboarding Assistant on any MacOS, Linux, or Windows machine that has network access to your on-premises data center and your SDDC.

If you use the Content Onboarding Assistant to transfer content to your SDDC, and then find that there are additional items you want to transfer, you can run the Content Onboarding Assistant again. The Content Onboarding Assistant recognizes which `.vmtx` templates have already been transferred and does not allow you to select those to be transferred again. It also recognizes ISO images and script files that have been transferred, and will only transfer new ISO images and scripts.

Prerequisites

Before you run Content Onboarding Assistant, do the following:

- Make sure that your on-premises data center is running vCenter Server 6.0 or later.
- Install the Java Runtime Environment (JRE) 1.8 or later. You can download the Java Runtime installer from the Oracle website at http://www.oracle.com/technetwork/java/javase/downloads/jre8-downloads-2133155.html.
- Set the `$JAVA_HOME` environment variable to the location where you installed the JRE.
- Set up a VPN connection between your on-premises data center and your SDDC. See "Configuring VPNs and Gateways" in *Getting Started With VMware Cloud on AWS*.

Procedure

1. Prepare scripts and ISO images for addition to the Content Library by moving them into a single folder in your on-premises data center.

   `.vmtx` templates need no special preparation.

2. Download the Content Onboarding Assistant from the download location.

3 In the terminal or command line, switch to the directory where you placed the `Content-Onboarding-Assistant.jar` file and enter the command
`java -jar` ***`jar_file_name`*** **`--cfg`** ***`full_path_to_config_file`***.

In the configuration file, specify each parameter on its own line, and follow it with a space and the value. For example

```
onpremServer vcenter.onprem.example.com
onpremInfraServer psc.onprem.example.com
```

You can also specify many parameters on the command line by specifying them as **`--`*`parameter parameter_value`***. Type **`java --jar`** ***`jar_file_name`*** **`--help`** to see a full list of parameters, or consult the table below.

Parameter	Description
`onpremServer` *`server`*	The host name of the vCenter Server for your on-premises data center.
`onpremInfraServer` *`psc-server`*	The host name of the on-premises Platform Services Controller. This is optional for embedded configurations.
`onpremUsername` *`username`*	The user name used to log in to the on-premises vCenter Server.
`location` *`foldername`*	The location of files such as scripts or ISO images on the on-premises datastore. Use the format `datastore-name:folder/`.
`cloudServer` *`server`*	The host name of the cloud SDDC vCenter Server.
`cloudInfraServer` *`infra-server`*	The host name of the cloud SDDC vCenter Server. This is optional.
`cloudFolderName` *`foldername`*	The name of the vCenter Server folder on the cloud SDDC where `.vmtx` templates will be stored.
`cloudRpName` *`resource-pool-name`*	The resource pool on the cloud SDDC for the `.vmtx` templates.
`cloudNetworkName` *`network-name`*	The distributed virtual port group on the cloud SDDC for the `.vmtx` templates.
`sessionUpdate` *`value`*	The time in milliseconds between session update calls. The default value is 60000 ms (10 minutes). If you experience issues with sessions timing out while the Content Onboarding Assistant is running, decrease this value.

4 Enter the passwords for the on-premises data center and the cloud SDDC when you are prompted.

Content Onboarding Assistant tests the connections to the on-premises data center and SDDC, and then displays a table showing all the `.vmtx` templates it has discovered.

5 Enter the numbers for the templates you want to transfer.

You can enter single numbers separated by commas, or a range separated by a dash.

6 Confirm that the folder for ISO images and scripts is correct.

7 Select how to transfer your `.vmtx` templates.
   - Select option 1 to transfer the templates as OVF templates in the SDDC Content Library.
   - Select option 2 to transfer the templates as `.vmtx` templates in the vCenter Server inventory.

The Content Onboarding Assistant does the following:

- Copies `.vmtx` templates from your on-premises data center to your SDDC, using the options you specified.
- Creates a Content Library in your on-premises data center, adds the ISO images and scripts to that Content Library, and publishes it.
- Creates a subscribed Content Library in your SDDC and synchronizes the ISO images and scripts to the SDDC.

What to do next

You can now use the `.vmtx` templates and ISO images to create virtual machines in your SDDC.

Use a Content Library to Import Content into Your SDDC

If you have a Content Library in your on-premises data center, you can create a Content Library in your SDDC that subscribes to it, then publish it to import library items into your SDDC.

This method works for transferring OVF templates, ISO images, scripts, and other files.

Prerequisites

- You must have a Content Library in your on-premises data center. See Create a Library
- Set up a VPN connection between your on-premises data center and your SDDC. See "Configuring VPNs and Gateways" in *Getting Started With VMware Cloud on AWS*.

Procedure

1 Add your templates, ISO images, and scripts to the on-premises Content Library.

   All `.vmtx` templates are converted to OVF templates.

2 Publish your on-premises Content Library.

3 In your SDDC, create a Content Library that subscribes to the one you published in Step 2. Content is synchronized from your on-premises data center to your SDDC in VMware Cloud on AWS.

Upload Files or Folders to your SDDC

You can use the vSphere Client to upload files or folders to your SDDC.

You can upload content to your SDDC's WorkloadDatastore. The vsanDatastore is managed by VMware.

Prerequisites

You must have the CloudAdmin role on the datastore.

Procedure

1. In the vSphere Client, select the Storage icon and select WorkloadDatastore and click **Files**.
2. You can create a new folder, upload files, or upload a folder.

Option	Description
To create a new folder	a Select the WorkloadDatastore or an existing folder. b Select **New Folder**.
To upload a file	a Select a folder. b Click **Upload Files**. c Select a file and click **OK**.
To upload a folder	a Select a folder. b Select **Upload Folder**. c Select a folder and click **OK**.

Migrating Virtual Machines

5

VMware Cloud on AWS supports several ways to migrate your workload VMs from your on-premises hosts to the ones in your SDDC and back again, as well as across hosts in your SDDC. The method you choose should be based on your tolerance for workload VM downtime, the number of VMs you need to move, and your on-premises networking configuration.

Migration within the SDDC

Migration within SDDC refers to migrating virtual machines in your SDDC vCenter Server from one host or cluster to another. For information about migrations like this, see Migrating Virtual Machines in the *VMware vSphere Product Documentation*.

For a guided migration experience to help you use HCX to migrate VMs from your on-premises data center to the cloud SDDC, you can use the VMware Cloud Migration solution, Integrated Experiences for your Hybrid Cloud.

Hybrid Migration

Hybrid migration refers to migrating virtual machines between two different vSphere installations: one that's in your on-premises data center and another that's in your VMware Cloud on AWS SDDC. Because these two vSphere installations might have different versions, configurations, or both, hybrid migration use cases typically carry additional prerequisites and configuration that ensure both compatibility of the virtual machines and appropriate network bandwidth and latency. VMware Cloud on AWS supports a variety of tools and methods for hybrid migration.

- Hybrid Migration With VMware HCX

  VMware HCX, a multi-cloud app mobility solution, is provided free to all SDDCs and facilitates migration of workload VMs from your on-premises data center to your SDDC.

- Hybrid Migration with vMotion

  Migration with vMotion, also known as hot migration or live migration, moves a powered-on VM from one host or datastore to another. Migration with vMotion is the best option for migrating small numbers of VMs without incurring any downtime.

- Hybrid Cold Migration

  Cold migration moves powered-off VMs from one host or datastore to another. Cold migration is a good option when you can tolerate some VM downtime during the migration process.

Hybrid Migration With VMware HCX

VMware HCX, a multi-cloud app mobility solution, is provided free to all SDDCs and facilitates migration of workload VMs from your on-premises data center to your SDDC.

For more information about using HCX for hybrid migration, see the VMware HCX User Guide and the VMware Cloud Migration solution at https://vmc.vmware.com/solutions.

Hybrid Migration with HCX Checklist

This checklist describes end to end the requirements and configurations needed for migration using the VMware Hybrid Cloud Extension (HCX).

Requirement	Description
Networking speed	Migration with vMotion using HCX requires a minimum of 100 Mbps throughput between source and destination.
On-premises vSphere version	■ For vMotion: vSphere 5.5, 6.0, 6.5, 6.7 ■ For bulk migration: vSphere 5.0, 5.1, 5.5, 6.0, 6.5, 6.7 ■ For cold migration: vSphere 5.5, 6.0, 6.5, 6.7
On-premises virtual switch configuration	vSphere Distributed Switch
	Cisco Nexus 1000v
	vSphere standard switch
Installation of VMware HCX Manager in the on-premises data center	Install and configure the VMware HCX Manager appliance as described in "VMware HCX Manager Installation" in https://hcx.vmware.com/content/docs/vmware-hcx-user-manual.pdf.
Establish the HCX Interconnect with you SDDC	Pair the VMware HCX Manager with your VMware Cloud on AWS SDDC as a remote site as described in "Building the HCX Interconnect" in https://hcx.vmware.com/content/docs/vmware-hcx-user-manual.pdf.
L2 VPN	Extend a network from your on-premises datacenter to your VMware Cloud on AWS SDDC as described in "Extending Networks with VMware HCX" in https://hcx.vmware.com/content/docs/vmware-hcx-user-manual.pdf.
VMware Cloud on AWS firewall rules	Create firewall rules to open the ports used by HCX as described in "HCX Network Ports" in https://hcx.vmware.com/content/docs/vmware-hcx-user-manual.pdf.

Requirement	Description
On-premises firewall rules	Create firewall rules to open the ports used by HCX as described in "HCX Network Ports" in https://hcx.vmware.com/content/docs/vmware-hcx-user-manual.pdf.
Virtual machine hardware and settings	Ensure that these requirements are met for virtual machine hardware. ■ Virtual machine hardware version 9. ■ EVC is not supported in the VMware Cloud on AWS SDDC. ■ VMs that are created in the cloud SDDC or that have been power-cycled after migration to the cloud SDDC can't be migrated back to the on-premises data center with vMotion unless the on-premises EVC baseline is Broadwell. You can relocate these VMs after powering them off, as long as their virtual machine hardware version is compatible with the on-premises data center. The following virtual machines are not supported: ■ VMs with hard disks larger than 2TB. ■ VMs with shared `.vmdk` files. ■ VMs with virtual media or ISOs attached.

Hybrid Migration with vMotion

Migration with vMotion, also known as hot migration or live migration, moves a powered-on VM from one host or datastore to another. Migration with vMotion is the best option for migrating small numbers of VMs without incurring any downtime.

To implement migration with vMotion, you can configure hybrid linked mode and use the vSphere client. You can also use command-line (PowerShell) or API automation.

Summary of Supported Configurations

Your on-premises vSphere installation must be one of the following:

- vSphere 6.7U2 or higher.
- vSphere 6.5P03 or higher.

See VMware Knowledge Base article 56991 for more information.

Restrictions on VMs Migrated with vMotion

The restrictions on migration with vMotion that apply to VMs previously migrated from on-premises data centers are as follows:

- VMs that use standard virtual switches for networking cannot be migrated back to an on-premises data center after being migrated to the cloud SDDC.
- Any VM that has been power-cycled in the cloud SDDC can only be migrated back to an on-premises host or cluster with the Broadwell chipset or EVC mode.

- If your on-premises hosts haven't been patched to address vulnerability to side channel analysis due to speculative execution (also referred to as the Spectre Variant 2 vulnerability), this may affect vMotion compatibility as shown in . To find the correct patch for your on-premises hosts, see https://kb.vmware.com/s/article/52245. All hosts in VMware Cloud on AWS SDDCs have been patched.

Table 5-1. vMotion Compatibility Effects of Spectre patch

On-premises Host Processor Family and Patch Status	Virtual Machine Hardware Version	Has the VM been power-cycled in VMware Cloud on AWS SDDC?	vMotion from On-premises to VMware Cloud on AWS	vMotion from VMware Cloud on AWS to On-premises
Broadwell (SPECTRE patched)	< 9	No	Supported	Supported
		Yes	Supported	Supported
	9-13	No	Supported	Supported
		Yes	Supported	Supported
Broadwell (Not SPECTRE patched)	< 9	No	Supported	Not supported
		Yes	Supported	Not supported
	9-13	No	Supported	Supported
		Yes	Supported	Not supported
Non-Broadwell	< 9	No	Not supported	Supported
		Yes	Not supported	Not supported
	9-13	No	Supported	Supported
		Yes	Supported	Not supported

Note You can find the Virtual Machine Hardware Version on the **Summary** tab for the virtual machine. You can find the host processor type on the **Summary** tab for the host. For a list of processor types in the Broadwell processor family, see https://ark.intel.com/products/codename/38530/Broadwell.

These restrictions don't apply to cold migration.

Hybrid Migration with vMotion Checklist

This checklist describes end to end requirements and configurations needed for migration with vMotion between your on-premises data center and your cloud SDDC.

Note HCX-based vMotion has a different set of requirements. See Hybrid Migration with HCX Checklist.

Table 5-2. vMotion Requirements for SDDCs With NSX-T

Requirement	Description
Networking speed and latency	Migration with vMotion requires sustained minimum bandwidth of 250 Mbps between source and destination vMotion vMkernel interfaces, and a maximum latency of 100 ms round trip between source and destination.
On-premises vSphere version	Your on-premises vSphere installation must be one of the following: ■ vSphere 6.7U2 or higher. ■ vSphere 6.5P03 or higher. See VMware Knowledge Base article 56991 for more information.
On-premises DVS version	6.0 or higher.
On-premises NSX version	any **Note** SDDCs configured with NSX-T do not support hot vMotion to or from on-premises VXLAN encapsulated networks (NSX for vSphere) or Geneve Datacenter Overlay networks (NSX-T).
IPsec VPN	Configure an IPsec VPN for the management gateway. See "Configuring VPNs and Gateways" in *Getting Started With VMware Cloud on AWS*.
Direct Connect	Direct Connect over a private virtual interface between your on-premise datacenter and your VMware Cloud on AWS SDDC is required for migration with vMotion. See Using AWS Direct Connect with VMware Cloud on AWS.
Hybrid Linked Mode	Hybrid Linked Mode is required to initiate migration from the vSphere Client. It is not required to initiate migration using the API or PowerCLI. See "Hybrid Linked Mode" in *Managing the VMware Cloud on AWS Data Center*.
L2 VPN	Configure a Layer 2 VPN to extend virtual machine networks between your on-premises data center and cloud SDDC. Routed networks are not supported. See *VMware Cloud on AWS Networking and Security*.
VMware Cloud on AWS firewall rules	Ensure that you have created the necessary firewall rules as described in Required Firewall Rules for vMotion.

Table 5-2. vMotion Requirements for SDDCs With NSX-T (continued)

Requirement	Description
On-premises firewall rules	Ensure that you have created the necessary firewall rules as described in Required Firewall Rules for vMotion.
Virtual machine hardware and settings	Ensure that these requirements are met for virtual machine hardware. ■ Virtual machine hardware version 9 or later is required for migration with vMotion from the on-premises data center to the cloud SDDC. ■ EVC is not supported in the VMware Cloud on AWS SDDC. ■ VMs that are created in the cloud SDDC or that have been power-cycled after migration to the cloud SDDC can't be migrated back to the on-premises data center with vMotion unless the on-premises EVC baseline is Broadwell. You can relocate these VMs after powering them off, as long as their virtual machine hardware version is compatible with the on-premises data center. ■ Migration of VMs with DRS or HA VM overrides is not supported. For more information on VM overrides, see Customize an Individual Virtual Machine.

Important Source switch configurations (including NIOC, spoofguard, distributed firewall, and Switch Security) and runtime state are not applied at the destination as part of migration in either direction. Before you initiate vMotion, apply the source switch configuration to the destination network.

Required Firewall Rules for vMotion

This topic summarizes the firewall rules required for migration with vMotion, both in your on-premises and cloud data centers.

VMC on AWS Firewall Rules for vMotion

Ensure that the following firewall rule are configured in the VMC Console.

Use Cases	Source	Destination	Service
Provide access to vCenter Server from the on premises. Use for general vSphere Client access as well as for monitoring vCenter Server	remote (on-premises) vSphere Client IP address	vCenter	HTTPS
Allow outbound vCenter Server access to on-premises vCenter Server.	vCenter	remote (on-premises) vCenter Server IP address	Any (All Traffic)
Allow SSO vCenter Server	remote (on-premises) Platform Services Controller IP address	vCenter	SSO (TCP 7444)

Use Cases	Source	Destination	Service
ESXi NFC traffic	remote (on-premises) ESXi VMkernel networks used for NFC.	ESXi	Provisioning (TCP 902)
Allow outbound ESXi access to on-premises .	ESXi	remote (on-premises) ESXi management VMkernel networks	Any (All Traffic)
Allow vMotion traffic.	remote (on-premises) ESXi vMotion VMkernel networks	ESXi	vMotion (TCP 8000)

On-Premises Firewall Rules for vMotion

Ensure that the following firewall rules are configured in your on-premises firewall.

Rule	Action	Source	Destination	Service	Ports
On-premises to vCenter Server	Allow	remote (on-premises) vSphere Client subnet	VMware Cloud on AWS vCenter Server IP address	HTTPS	443
Remote to ESXi provisioning	Allow	remote (on-premises) subnet		TCP 902	902
Cloud SDDC to on-premises vCenter ServerAllow	Allow	CIDR block for cloud SDDC management network	On-premises vCenter Server, PSC, Active Directory subnet	HTTPS	443
Cloud SDDC toESXi Remote Console	Allow	CIDR block for cloud SDDC management network	VMware Cloud on AWS vCenter Server IP address		
Cloud SDDC to Remote LDAP	Allow	CIDR block for cloud SDDC management network	Remote LDAP Server	TCP	389, 636
Cloud SDDC to ESXi vMotion	Allow	CIDR block for cloud SDDC management network	Remote ESXi host subnet	TCP	8000

Bulk Migration with vMotion

While you can use vMotion with the vSphere client to migrate VMs between your on-premises data center and your SDDCs, use of an automation solution like PowerCLI or the vMotion APIs becomes increasingly necessary as the number of migrated VMs grows. There's no formal definition of how many VMs constitute a "bulk" migration, but for most cases, assume that if you can't count the VMs on the fingers of one hand, a bulk migration solution is appropriate.

To implement bulk migration, you can use command-line (PowerShell) or API automation, described in the Multicloud Workload Migration whitepaper. For additional GUI and REST API options, download the Cross vCenter Workload Migration Utility.

Summary of Supported Configurations

The following table summarizes the supported configurations for hybrid bulk migration.

Table 5-3. Summary of Supported Configurations for Hybrid Bulk Migration

On-premises vSphere Version	Network Connectivity	VDS version on-premises
vSphere 5.0, 5.1, 5.5, 6.0, and 6.5	Internet or AWS Direct Connect and L2 VPN created through HCX	Any VMware Distributed Switch, vSphere standard switch, or Cisco Nexus 1000v

Hybrid Cold Migration

Cold migration moves powered-off VMs from one host or datastore to another. Cold migration is a good option when you can tolerate some VM downtime during the migration process.

To implement cold migration, you can configure hybrid linked mode and use the vSphere client. You can also use command-line (PowerShell) or API automation.

Summary of Supported Configurations

The following table summarizes the supported configurations for hybrid cold migration.

Table 5-4. Supported Configurations for Hybrid Cold Migration

On-premises vSphere Version	Network Connectivity	VDS version on-premises
vSphere 6.0u3	AWS Direct Connect or IPsec VPN	VMware Distributed Switch version 6.0
vSphere 6.5 patch d	AWS Direct Connect or IPsec VPN	VMware Distributed Switch version 6.0 or 6.5
vSphere 5.5, 6.0, and 6.5	Internet or AWS Direct Connect and L2 VPN created through HCX	Any VMware Distributed Switch, vSphere standard switch, or Cisco Nexus 1000v

Hybrid Cold Migration Checklist

This checklist describes end to end the requirements and configurations needed for cold migration between your on-premises data center and your cloud SDDC.

Requirement	Description
On-premises vSphere version	vSphere 6.5 patch d and later
	vSphere 6.0 update 3 and later
On-premises virtual switch configuration	Standard switches, vSphere Distributed Switch 6.0, or vSphere Distributed Switch 6.5
IPsec VPN	Configure an IPsec VPN for the management gateway. See "Configuring VPNs and Gateways" in *Getting Started With VMware Cloud on AWS*.

Requirement	Description
Hybrid Linked Mode	Hybrid Linked Mode is required to initiate migration from the vSphere Client. It is not required to initiate migration using the API or PowerCLI. See "Hybrid Linked Mode" in *Managing the VMware Cloud on AWS Data Center*.
VMware Cloud on AWS and on-premises firewall rules	Ensure that you have created the necessary firewall rules as described in Required Firewall Rules for Cold Migration.
On-premises DNS configuration	Ensure that your on-premises DNS server can correctly resolve the address for the cloud vCenter Server.

Required Firewall Rules for Cold Migration

SDDC Management Gateway Firewall Rules for Cold Migration

Ensure that the following SDDC management gateway firewall rules are configured. See Add or Modify Compute Gateway Firewall Rules in *VMware Cloud on AWS Networking and Security*.

Use Cases	Source	Destination	Service
Provide on-premises vSphere Client and monitoring access to the SDDC vCenter Server.	remote (on-premises) vSphere Client IP address	vCenter	HTTPS
Allow outbound vCenter Server access to on-premises vCenter Server.	vCenter	remote (on-premises) vCenter Server IP address	Any (All Traffic)
Allow SSO to vCenter Server	remote (on-premises) Platform Services Controller IP address	vCenter	SSO (TCP 7444)
ESXi NFC traffic	remote (on-premises) ESXi VMkernel networks used for NFC.	ESXi	Provisioning (TCP 902)
Allow outbound ESXi access to on-premises ESXi	ESXi	remote (on-premises) ESXi management VMkernel networks	Any (All Traffic)

On-Premises Firewall Rules for Cold Migration

Ensure that the following rules are configured in your on-premises firewall.

Rule	Action	Source	Destination	Service	Ports
On-premises to vCenter Server	Allow	remote (on-premises) vSphere Client subnet	VMware Cloud on AWS vCenter Server IP address	HTTPS	443
Remote to ESXi provisioning	Allow	remote (on-premises) subnet	SDDC management subnet	TCP	902
Cloud SDDC to on-premises vCenter Server	Allow	CIDR block for cloud SDDC management network	On-premises vCenter Server	HTTPS	443
Cloud SDDC to ESXi Remote Console	Allow	CIDR block for cloud SDDC management network	VMware Cloud on AWS vCenter Server IP address	TCP	902
Cloud SDDC to Remote LDAP (Required for HLM only)	Allow	CIDR block for cloud SDDC management network	Remote LDAP Server	TCP	389, 636

Working with the Developer Center

6

The Developer Center is a single point of entry for developers that provides tools to manage API structure and to capture user actions to translate them into executable code.

The VMware Cloud on AWS Developer Center provides tools for automation experts, devops engineers, and developers to find the resources needed to automate and integrate with the VMware Cloud on AWS service. These tools include:

- Overview of the APIs and tooling available.
- Interactive API Explorer for the VMware Cloud on AWS RESTful APIs enabling the ability to learn and execute the APIs.
- Access to VMware and community code samples for common development languages and API tooling.
- Access to download the supported Open Source software development kits (SDKs) and links to getting started guides and documentation.
- Developer and Automation downloadable tools and interfaces for working with these APIs.
- Code Capture to record actions performed during a user session and translate them into PowerCLI.

This chapter includes the following topics:

Using Code Capture

Code Capture records user actions and translates them into executable code.

Code Capture gives you the ability to record actions taken in the VMware Cloud on AWS service and output them as usable PowerCLI code. You can then copy the code or download it as a script and use it in a PowerShell session to execute the task.

Record Actions Using Code Capture

You can use Code Capture to record actions taken in a VMware Cloud on AWS session to produce a PowerCLI code output.

Note Calls made on operations regarding roles, privileges, tags, content libraries, and storage policies are not recorded. Sensitive data such as passwords is not recorded.

Prerequisites

To use Code Capture to record a session, you must first enable Code Capture.

Procedure

1. From the home sidebar menu, click **Developer Center** and go to the **Code Capture** tab.
2. (Optional) If Code Capture is not enabled, click the toggle to enable Code Capture.
3. To start a recording, navigate to your desired pane and click the red record button in the top pane. To start recording immediately, click **Start Recording**.

   While a recording is in progress, the red record button in the top pane blinks.
4. (Optional) To clear the code captured in a previous session and start a new session, click **Clear and Start Another**.
5. To stop a recording, click the red record button in the top pane, or navigate to the **Code Capture** tab in the Developer Center and click **Stop Recording**.

   The recorded code appears in the code pane.
6. (Optional) Click **Copy** to copy the code or **Download** to download it as a PowerCLI script.
7. To clear the current code and start another recording, click **Clear and Start Another** or navigate to your desired pane and click the red record button in the top pane.

The recorded code appears in the code pane. You can copy the code, download it, or clear the code to start another recording.

Accessing AWS Services

7

During SDDC deployment, you connected your SDDC to an Amazon VPC in your AWS account, creating a high-bandwidth, low-latency interface between your SDDC and services in the Amazon VPC.

Using this connection, you can enable access between VMs in your SDDC and services in your AWS account, such as EC2 and S3.

This chapter includes the following topics:

Access an EC2 Instance

You can deploy an EC2 instance in your connected Amazon VPC and configure AWS security policies and compute gateway firewall rules to allow a connection between VMs in your SDDC and that instance.

The default AWS Security Group in the connected VPC controls traffic from EC2 instances in the VPC to VMs in the SDDC. This traffic must also pass through the Compute Gateway firewall (and the Distributed Firewall if you're using that). All of these controls must allow the intended traffic for a connection to be established.

When you deploy an EC2 instance, the EC2 Launch Wizard associates it with a new Security Group unless you have specified another group. A new AWS Security Group allows all outbound traffic from the instance and no inbound traffic to it. To allow a connection between an EC2 instance and a VM in your SDDC, you typically need only create inbound rules.

- To allow traffic to be initiated from the EC2 instance to a VM in the SDDC, create an inbound rule on the default Security Group.
- To allow traffic to be initiated from the VM to the EC2 instance, create an inbound rule on the Security Group applied to the EC2 instance.

Bear in mind that when you use the default AWS Security Group with the instance, its inbound rules are applied to traffic both when it transits the EC2 instance, and when it transits the SDDC. To allow traffic initiated by either the VM in the SDDC or the EC2 instance to reach other, inbound rules must allow inbound traffic from both the EC2 instance and the VM.

Prerequisites

To complete this task, you need the following information:

- The CIDR blocks of the network segments the VMs in your SDDC are connected to. Click **Segments** on the **Networking & Security** tab to list all segments.
- The connected Amazon VPC and subnet. Click **Connected VPC** in the **System** category on the **Networking & Security** tab to open the **Connected Amazon VPC** page, which provides this information under **VPC ID** and **VPC Subnet**.

Procedure

1. Deploy the EC2 instance in your AWS account.

   Keep in mind the following when creating the EC2 instance:

   - The EC2 instance must be in the VPC that you selected during deployment of your SDDC, or a connection can't be established over a private IP address.
   - The EC2 instance can be deployed in any subnet within the VPC, but you might incur cross-AZ traffic charges if it is a different AZ than the one you selected during SDDC deployment.
   - If possible, select a Security Group for your EC2 instance that already has an inbound traffic rule configured as described in Step 2.
   - The VPC subnet(s) used for the SDDC, as well as any VPC subnets on which AWS services or instances communicate with the SDDC must all be associated with the VPC's main route table.
   - Workload VMs in the SDDC can communicate over the ENI connection with all subnets in the primary CIDR block of the connected VPC. VMC is unaware of other CIDR blocks in the VPC.

2. Add inbound rules to the Security Group applied to the instance. Select the EC2 instance that you deployed in Step 1 and configure its Security Group to allow inbound traffic from the logical network or IP address associated with the VM in your SDDC.

   a. Select the instance that you deployed in Step 1.

   b. In the instance description, click the instance's Security Group and click the **Inbound** tab.

   c. Click **Edit**.

   d. Click **Add Rule**.

   e. In the **Type** dropdown menu, select the type of traffic that you want to allow.

   f. In the **Source** text box, select **Custom** and enter the IP addresses or CIDR block of VMs in the SDDC that need to communicate with the instance.

g (Optional) Add rules as needed for additional CIDR blocks or traffic type you want to connect to the instance from VMs in your SDDC.

h Click **Save**.

3 (Optional) If you need to allow traffic initiated by the instance that you deployed in Step 1 to a VM in your SDDC, edit the default Security Group for the connected Amazon VPC to add inbound rules that identify the instances by CIDR block or Security Group.

a In the AWS console, select the default Security Group for the Connected Amazon VPC and click the **Inbound** tab.

b Click **Edit**.

c Click **Add Rule**.

d In the **Type** dropdown menu, select the type of traffic that you want to allow.

e In the **Source** text box, select **Custom** and enter the IP addresses or CIDR block of VMs in the SDDC that need to communicate with the instance.

If all the VMs are associated with the same SDDC Inventory Group, you can specify that Group as the **Source** rather than using an IP address or CIDR block.

f (Optional) Add rules as needed for additional CIDR blocks or traffic type you want to connect to the instance from VMs in your SDDC.

g Click **Save**.

4 Configure the necessary compute gateway firewall rules.

See Add or Modify Compute Gateway Firewall Rules in *VMware Cloud on AWS Networking and Security*.

- To allow inbound traffic from the instances in the connected Amazon VPC, create a rule where the **Source** is **Connected VPC Prefixes** and the **Destination** is an inventory group containing the VMs that require inbound access from the instance.
- To allow outbound traffic to instances in the connected Amazon VPC, create a rule where the **Source** is an inventory group containing the VMs that require outbound access to the instance and the **Destination** is **Connected VPC Prefixes**.

Note In either case, you can limit traffic to or from a subset of EC2 instances by defining a workload inventory group in your SDDC that includes only the IP addresses or CIDR blocks for those instances.

5 (Optional) Configure distributed firewall rules.

If any of the VMs that communicate with the instance is protected by distributed firewall, you might need to adjust the rules for that firewall to allow the expected traffic. See Add or Modify Distributed Firewall Rules.

Access an S3 Bucket Using an S3 Endpoint

You can access an S3 bucket in your connected AWS VPC by creating an S3 endpoint.

Procedure

1 Create an S3 endpoint.

See Gateway VPC Endpoints and Endpoints for Amazon S3 in the *Amazon Virtual Private Cloud User Guide*.

a For **Service category**, select AWS services.

b Under **Service Name**, select a `com.amazonaws.`*region-AZ*`.s3` service of type **Gateway** where *region-AZ* matches the region and AZ your SDDC is in. For example, `com.amazonaws.us-west-2.s3`.

c In the **VPC** drop down, select the VPC that is connected to your SDDC.

d Under **Configure route tables**, select the **Route Table ID** where the value in the **Main** column is **Yes**. This Route Table is used by the SDDC and should also be associated with the VPC subnet the SDDC is connected to.

e Under **Policy** select the default Full Access policy or create a more restrictive one. See Endpoints for Amazon S3 in the *Amazon Virtual Private Cloud User Guide*. Traffic to S3 from the SDDC will have its source IP NATted to an IP from the subnet selected at SDDC deployment, so any policy must allow traffic from that subnet.

f Click **Create Endpoint** to create the endpoint and add routes for the S3 public IP ranges in the region to the main route table.

2 (Optional) Configure the security group for your connected Amazon VPC to allow outbound traffic to the network segment associated with the VM in your SDDC.

The default security group allows this traffic, so you won't need to take this step unless you previously customized the default security group.

a In the AWS console, select the default Security Group for the Connected Amazon VPC and click the **Outbound** tab.

b Click **Edit**.

c Click **Add Rule**.

d In the **Type** dropdown menu, select **HTPPS**.

e In the **Destination** text box, select **Anywhere**.

f Click **Save**.

3 Ensure that access to S3 through the elastic network interface is enabled.

By default, S3 access through the elastic network interface in the connected Amazon VPC is enabled. If you disabled this access to allow S3 access through the internet gateway, you must re-enable it.

a Log in to the VMC Console at https://vmc.vmware.com.

b Click **> Connected VPC**

c Under **Service Access**, click **Enable** next to **S3 Endpoint**.

4 From the VMC Console, create a compute gateway firewall rule to allow https access to the connected Amazon VPC.

a Under **Compute Gateway**, click **Firewall Rules**.

b Add a compute gateway firewall rule with the following parameters.

Option	Description
Source	The CIDR block for the logical network that the VM in your SDDC is connected to.
Destination	Select **S3 Prefixes**.
Service	Select **HTTPS**.
Applied to	Clear **All Uplinks** and select **VPC Interface**.

Workload VMs in your SDDC can access files in the S3 bucket over an https connection.

Access an S3 Bucket Using the Internet Gateway

If you don't want to use an S3 Endpoint to access an S3 bucket, you can access it using the internet gateway. For example, you might do this

Procedure

1 Ensure that the access permissions for the S3 bucket permit access from your cloud SDDC from the internet.

See Managing Access Permissions to Your Amazon S3 Resources for more information.

2 Enable access to S3 through the internet gateway.

By default, S3 access goes through the S3 endpoint of your connected Amazon VPC. You must enable access to S3 over the internet before you can use it.

a Log in to the VMC Console at https://vmc.vmware.com.

b **View Details**

c **Networking & Security**

d Click **Connected Amazon VPCs**, and then click **Disable** next to **S3 Endpoint**.

3 From the VMC Console, create a compute gateway firewall rule to allow https access to the internet.

   a Under **Compute Gateway**, click **Firewall Rules**.

   b Add a compute gateway firewall rule with the following parameters.

Option	Description
Source	The CIDR block for the logical network that the VM in your SDDC is connected to.
Destination	**Any**
Service	Select **HTTPS**.

VMs in your SDDC can now access files on the S3 bucket using their https paths.

Use AWS CloudFormation to Create an SDDC

AWS CloudFormation is a text-based modeling tool that enables you to create templates that describe all the features of an VMware Cloud on AWS SDDC or any other AWS infrastructure.

To introduce this capability to VMware Cloud on AWS customers, VMware has made a CloudFormation SDDC template available on code.vmware.com. Use this template as a starting point for working with AWS CloudFormation tools to create a CloudFormation stack and an AWS Lambda function that you can run to deploy an SDDC based on the template. For a more detailed explanation of this procedure, see VMware Cloud on AWS Integrations with CloudFormation on the *VMware {code}* blog and https://github.com/vmwaresamples/vmware-cloud-on-aws-integration-examples/blob/master/CloudFormation/README.md.

Procedure

1 Log in to the AWS console and go to the **US West (Oregon)** region.

   Log in with an AWS identity authorized to view and deploy CloudFormation templates.

2 Retrieve the CloudFormation Create SDDC Template from the *vmwaresamples* repository on Github.

3 Open the AWS **CloudFormation** service and click **Create new stack**.

4 Upload the template you retrieved in Step 2.

   In the AWS **CloudFormation > Stacks > Create stack** window, click **Upload a template to Amazon S3** and choose the `vmc-aws-cloud-cf-template.txt` template. Click **Next**.

5 Specify a name for the new stack, then click **Next** and **Create**.

6 Specify SDDC variables for use by the AWS Lambda function.

   In the AWS **CloudFormation > Stacks > Stack Detail** window. In the Resources section, you can see an IAM role and a Lambda Function. Click the **Physical ID** value of the Lambda function and enter the Environment variables that provide configuration details for the SDDC.

Table 7-1. Environment Variables for Cloud Formation SDDC Stack

Name	Description
connected_account_id	The Amazon account ID used to connect the SDDC. Returned by the VMC API request `GET /orgs/{org}/account-link/connected-accounts` as the value of `id`.
customer_subnet_ids	This is the ID of the subnet (not the actual subnet address). Returned by the VMC API request `GET /orgs/{org}/account-link/compatible-subnets` as the `subnet_id` of the `subnet_cidr_block` that you want to use.
Email	currently unimplemented
vpc_cidr	Subnet CIDR block for management traffic. Default is 10.2.0.0/16
name	The name of the SDDC to be created
numOfHosts	The number of hosts initially added to the SDDC
orgId	Can be found in the VMware Cloud on AWS API or as part of the UI under an existing SDDC connection and the **Support Info** tab
region	Must be `US_WEST_2`
user_refresh_token	Can be found in the VMware Cloud on AWS UI by clicking on your name at the top right and then the **Oauth Refresh Token** button.

7 Save and run the AWS Lambda function to create the SDDC from the template.

Click Save, then click Test to open the **Configure test event** window. Give the test event a name and click **Create**.

The AWS Lambda function runs and creates an SDDC based on the template and environment variables you supplied. You can monitor the SDDC creation process on the **SDDCs** tab of the VMC Console or use the AWS Tasks API.

AWS Roles and Permissions

To create an SDDC, VMware must add several required AWS roles and permissions to your AWS account.

Permissions Statement

Initial permissions required to create the SDDC are shown in italics. These permissions are removed from the role after the SDDC has been created. The others remain with this role in your AWS account.

Important You must not change any of the remaining AWS roles and permissions. Doing so will render your SDDC inoperable.

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
```

```
"Action": [
"ec2:DescribeRouteTables",
"ec2:CreateRoute",
"ec2:DeleteRoute",
"ec2:ReplaceRoute"
],
"Resource": [
"*"
]
},
{
"Effect": "Allow",
"Action": [
"ec2:DescribeNetworkInterfaces",
"ec2:CreateNetworkInterface",
"ec2:DeleteNetworkInterface",
"ec2:CreateNetworkInterfacePermission",
"ec2:ModifyNetworkInterfaceAttribute",
"ec2:DescribeNetworkInterfaceAttribute",
"ec2:DescribeVpcs",
"ec2:DescribeSubnets"
],
"Resource": [
"*"
]
},
{
"Effect": "Allow",
"Action": [
"ec2:AssignPrivateIpAddresses",
"ec2:UnassignPrivateIpAddresses"
],
"Resource": [
"*"
]
},
{
"Effect": "Allow",
"Action": [
"cloudformation:CreateStack",
"cloudformation:DescribeStacks",
"cloudformation:DescribeStackEvents",
"cloudformation:DescribeStackResource",
"cloudformation:DescribeStackResources",
"cloudformation:GetTemplateSummary",
"cloudformation:ListStackResources",
"cloudformation:GetTemplate",
"cloudformation:ListChangeSets",
"cloudformation:GetStackPolicy"
],
"Resource": "*"
},
{
"Effect": "Allow",
"Action": [
```

```
  "iam:CreateRole",
  "iam:CreatePolicy",
  "iam:AttachRolePolicy",
  "iam:GetRole",
  "iam:PassRole",
  "iam:PutRolePolicy",
  "lambda:CreateFunction",
  "lambda:InvokeFunction",
  "lambda:GetFunctionConfiguration",
  "cloudformation:DescribeStackResource",
  "cloudformation:DescribeStackResources"
 ],
 "Resource": "*"
 }
 ]
}
```

To see the associated Policy Permissions document, log into the AWS Console and open `https://console.aws.amazon.com/iam/home?region=us-east-1#/policies/arn:aws:iam::aws:policy/AmazonVPCCrossAccountNetworkInterfaceOperations$jsonEditor`. Here's the summary description of that policy.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeRouteTables",
                "ec2:CreateRoute",
                "ec2:DeleteRoute",
                "ec2:ReplaceRoute"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeNetworkInterfaces",
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface",
                "ec2:CreateNetworkInterfacePermission",
                "ec2:DeleteNetworkInterfacePermission",
                "ec2:DescribeNetworkInterfacePermissions",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeNetworkInterfaceAttribute",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets"
            ],
            "Resource": [
                "*"
```

```
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:UnassignPrivateIpAddresses"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

Using On-Premises vRealize Automation with Your Cloud SDDC

8

You can use your on-premises vRealize Automation with your VMware Cloud on AWS SDDC.

Currently vRealize Automation 7.2, 7.3, and 7.4 are supported for use with VMware Cloud on AWS.

This chapter includes the following topics:

Prepare Your SDDC to Work with vRealize Products

Before you connect vRealize Automation to your VMware Cloud on AWS SDDC, you must configure networking and firewall rules for your SDDC.

Procedure

1. Configure a VPN connection over the public Internet or AWS Direct connect.

   See Configure VPN Connectivity to the On-Premises Data Center and Configure AWS Direct Connect for VMware Cloud on AWS in *VMware Cloud on AWS Networking and Security*.

2. Verify that the vCenter Server FQDN is resolvable at a private IP address on the management network.

   See Set vCenter Server FQDN Resolution Address in *VMware Cloud on AWS Networking and Security*.

3. Configure additional firewall rules if necessary.

   vRealize Automation requires the following Management Gateway firewall rules.

Table 8-1. Management Gateway Firewall Rules Required by vRealize Automation

Name	Source	Destination	Service
vCenter	CIDR block of on-premises data center	vCenter	Any (All Traffic)
vCenter Ping	Any	vCenter	ICMP (All ICMP)

Table 8-1. Management Gateway Firewall Rules Required by vRealize Automation (continued)

Name	Source	Destination	Service
On Premises to ESXi Ping	CIDR block of on-premises data center	ESXi Management Only	ICMP (All ICMP)
On Premises to ESXi Remote Console and Provisioning	CIDR block of on-premises data center	ESXi Management Only	TCP 902
On-Premises to SDDC VM	CIDR block of on-premises data center	CIDR block of SDDC logical network	Any (All Traffic)
SDDC VM to On-Premises	CIDR block of SDDC logical network	CIDR block of on-premises data center	Any (All Traffic)

See Add or Modify Management Gateway Firewall Rules in *VMware Cloud on AWS Networking and Security*.

Connect vRealize Automation to Your SDDC

You can connect vRealize Automation to your cloud SDDC and create blueprints allowing users to deploy VMs.

Prerequisites

- Ensure that you have completed all the steps in Prepare Your SDDC to Work with vRealize Products.
- Ensure that all vRealize Automation VMs are configured to use TLS 1.2.

Procedure

1. In vRealize Automation, select **Infrastructure > Endpoints**.
2. Select **New > Virtual > vSphere (vCenter)**.
3. Specify the vCenter Server URL in the format `https://fqdn/sdk`.
4. Specify the cloud admin credentials.
5. (Optional) If you are using vRealize Automation 7.3 or 7.4, click **Test Connection** and **Accept Certificate**.
6. Create a Fabric Group.
   a. Add the cloud admin as the fabric administrator.
   b. Add the default SDDC cluster Cluster-1 to the Compute Resources.

   For more information on creating a Fabric Group, see Create a Fabric Group.
7. Create reservations for the components that the cloud admin has access to.

Option	Description
Resource Pool	Compute-ResourcePool
Datastore	WorkloadDatastore

Option	Description
VM & Template Folder	Workloads
Network	Use the logical network that you created as part of the prerequisites

Important Because VMware Cloud on AWS places VMs provisioned for vRealize Automation Business Groups in a non-standard folder, you must set the vRealize Automation custom property `VMware.VirtualCenter.Folder` to reference the workloads folder (**VM & Template Folder**). See the vRealize Automation Custom Properties Reference.

8 Create a Network Profile for the logical network you created as part of the prerequisites.

For more information on creating a network profile, see Create a Network Profile.

9 Create a Blueprint.

For more information on Blueprints, see Providing Service Blueprints to Users.

What to do next

If you plan to access the Remote Console from vRealize Automation, follow the steps in Enable vRealize Automation Access to the Remote Console.

Enable vRealize Automation Access to the Remote Console

To access the Remote Console from vRealize Automation, you must add the host management IP address of the ESXi hosts to the `/etc/hosts` file in the vRealize Automation appliance.

Procedure

1 For each ESXi host in your SDDC, determine the IP address of the host management network.

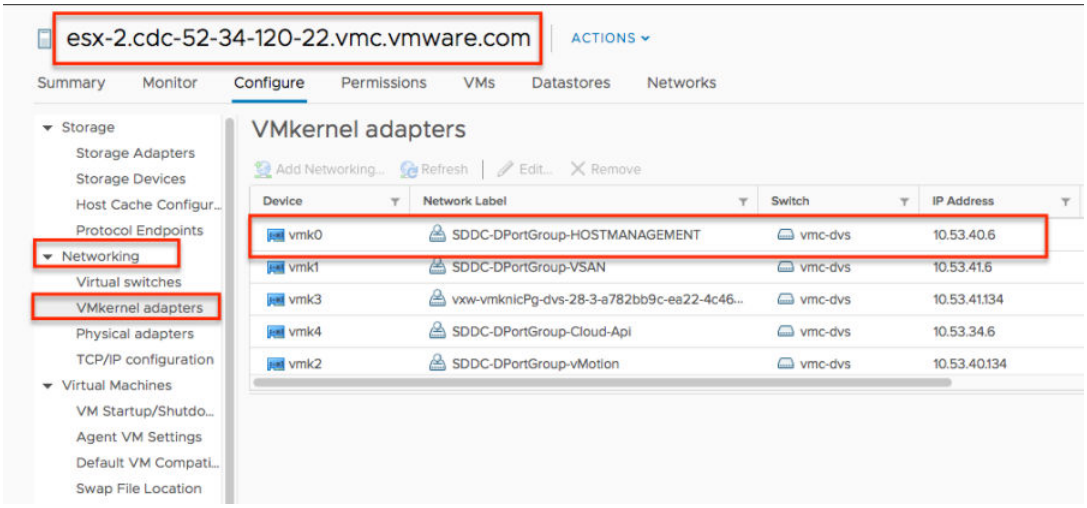
a Log in to the vSphere Client for your SDDC.

b In the Hosts and Clusters inventory list, select the host.

c Click the **Configure** tab.

d Under **Networking**, click **VMkernel Adapters**.

e Note the FQDN for the host and the IP address for the vmk0 device.



2 Connect to the vRealize Automation appliance using ssh.

3 Edit the `/etc/hosts` file and add a line for each host as shown.

```
host-management-ip esxi-host-name
```

VMC Console Settings

9

You can modify VMC Console settings to change the function of the console.

This chapter includes the following topics:

- Set Language for the VMC Console

Set Language for the VMC Console

The VMC Console supports a number of languages, based on the language setting of your web browser.

The VMC Console UI supports English, French, German, Japanese, Korean, Spanish, Simplified Chinese, and Traditional Chinese.

To set the language used by the VMC Console, set your language preferences in your VMware Cloud Services account.

For more information, see https://docs.vmware.com/en/VMware-Cloud-services/services/Using-VMware-Cloud-Services/GUID-FD81BC5E-D940-459A-99CC-FBBC202BBC9D.html.

Procedure

1. From the VMC Console, click the services icon () and select **Cloud Services Console**.
2. In the Cloud Services Console, click your user name and select **My Account**.
3. Click **Preferences**.
4. Next to **Language and Regional Format**, click **Edit**.
5. Select the language and regional format and click **Save**.

Service Notifications and Activity Log

10

VMware periodically sends notifications to keep you informed of upcoming maintenance and other events that impact your VMware Cloud on AWS service.

Outages and other service-wide events are reported on the VMware Cloud Services status page. See View and Subscribe to the Service Status Page for more information.

Notifications for events such as SDDC deployment, removal, upgrades, and maintenance are included in the Activity Log. See View the Activity Log.

For events such as customer-specific outages, upgrades, and maintenance, VMware also sends email notifications to all organization owners and organization members. To ensure that you receive these email notifications, whitelist donotreply@vmware.com.

This chapter includes the following topics:

View the Activity Log

The Activity Log contains a history of significant actions in your organization, such as SDDC deployments and removals, as well as notifications sent by VMware for events such as SDDC upgrades and maintenance.

Procedure

1. Log in to the VMC Console at https://vmc.vmware.com.
2. Click **Activity Log**.

   Entries are displayed in reverse chronological order, with the newest entries at the top.
3. (Optional) If an entry indicates that a task failed, click to expand the task to show the error message.

View and Subscribe to the Service Status Page

VMware publishes service operational status and maintenance schedules at status.vmware-services.io.

Subscribe to the status page to get real-time email or SMS notifications on the service status.

Procedure

1. Go to https://status.vmware-services.io to view the service status dashboard and incidents.
2. Click **Subscribe to Updates**.
3. Select the notification methods you prefer to subscribe to for the service.

Troubleshooting

11

You have a number of options for getting help and support for your VMware Cloud on AWS environment.

This section also documents a number of known issues and workarounds that can help you resolve problems.

This chapter includes the following topics:

Get Support

VMware Cloud on AWS customers can get support by opening the **VMware Cloud Services** console.

Procedure

1. Before you contact VMware for support, have the support information for your SDDC ready.
   a. Log in to the VMC Console at https://vmc.vmware.com.
   b. Click **View Details** on the SDDC card.
   c. Click **Support** to view the support information.
2. See How Do I Get Support for more information about using VMware Cloud Services in-product support.

Unable to Connect to VMware Cloud on AWS

Problem

You might experience problems connecting to resources on VMware Cloud on AWS. For example:

- You log in to the VMC Console and see only a blank screen.
- You try to log in to the vSphere Client or vSphere Web Client and see the error message, `User name and password are required`.

Cause

This error is caused by a problem with the site cookies.

Solution

- You can resolve this issue either by deleting the site cookies or opening an incognito or private browsing window in your browser.

Option	Description
Delete cookies	Follow the instructions for your browser. If you want to delete only specific cookies, delete ones with "vmware" and "vidm" in the name. ■ Google Chrome: See https://support.google.com/chrome/answer/95647 ■ Mozilla Firefox: See https://support.mozilla.org/en-US/kb/delete-cookies-remove-info-websites-stored ■ Microsoft Internet Explorer: https://support.microsoft.com/en-us/help/17442/windows-internet-explorer-delete-manage-cookies ■ Microsoft Edge: https://support.microsoft.com/en-us/help/10607/microsoft-edge-view-delete-browser-history ■ Safari: https://support.apple.com/kb/PH21411?locale=en_US
Open an incognito or private browsing window	Follow the instructions for your browser: ■ Google Chrome: Click the menu button and select **New incognito window**. ■ Mozilla Firefox: Click the menu button and select **New Private Window**. ■ Microsoft Internet Explorer: Click the tools button and select **Safety > InPrivate Browsing**. ■ Microsoft Edge: Click the More icon, and select **New InPrivate window**. ■ Safari: Select **File > New Private Window**.

Unable to Connect to vCenter Server

You are unable to connect to the vSphere Client interface for your SDDC.

Problem

When you click the link on the connection tab to open the vSphere Client interface to vCenter Server, your browser reports that the site cannot be reached.

Cause

By default, the management gateway firewall is set to deny all traffic between the internet and vCenter Server. Verify that the appropriate firewall rules are in place.

Solution

- Create the following firewall rules.

Table 11-1. Firewall Rules Required for vCenter Access

Use Cases	Service	Source	Destination
Provide access to vCenter Server from the internet. Use for general vSphere Client access as well as for monitoring vCenter Server	HTTPS	public IP address	vCenter
Provide access to vCenter Server over VPN tunnel. Required for Management Gateway VPN, Hybrid Linked Mode, Content Library.	HTTPS	IP address or CIDR block from on-premises data center	vCenter
Provide access from cloud vCenter Server to on-premises services such as Active Directory, Platform Services Controller, and Content Library.	Any	vCenter	IP address or CIDR block from on-premises data center.

Unable to Select Subnet When Creating SDDC

While creating your SDDC and connecting a VPC and subnet to connect to in your AWS account, you are unable to select a subnet.

Problem

While deploying an SDDC, there is a step in which you select an Amazon VPC and subnet in your AWS account to connect to your SDDC. You might be unable to select a subnet during this step. A message in the UI indicates that you do not have capacity in any of your current subnet AZs.

Cause

You must select a subnet in the same availability zone (AZ) as your SDDC. Currently, it isn't possible to ensure which AZ your SDDC will match up to. If you have only created a single subnet, it might be in the incorrect AZ and not available for selection in this step.

Solution

- Create an appropriate subnet in each availability zone in your Amazon VPC.

Unable to Copy Changed Password Into vCenter Login Page

Problem

You changed the cloudadmin@vmc.local for a vCenter Server system from the vSphere Client. Now you no longer remember the password, so you use the Copy icon on the Default vCenter Credentials page and paste the password into the VMware vCenter Single Sign-On Login Screen. The login process fails.

Cause

When you change the password for your SDDC from the vSphere Client, the new password is not synchronized with the password that is displayed on the Default vCenter Credentials page. That page shows only the Default credentials. If you change the credentials, you are responsible for keeping track of the new password.

Solution

Contact Technical Support and request a password change. See Get Support.

Compute Workloads Are Unable to Reach an On-Premises DNS Server

Compute workloads connected to a user-created logical network using DHCP are unable to reach an on-premises DNS server.

Problem

If you selected a non-default logical network when creating your compute gateway VPN, and that network uses DHCP, workload VMs might be unable to reach an on-premises DNS server.

Cause

The problem occurs if the compute gateway VPN has not been configured to allow DNS requests over the VPN.

Solution

1. Configure the VMware Cloud on AWS side of the VPN tunnel to allow DNS requests over the VPN.
   a. Log in to the VMC Console at https://vmc.vmware.com.
   b. Navigate to the Networking tab of your SDDC.
   c. Under **Compute Gateway** and click **VPN**.
   d. Select **Actions > Edit**.
   e. Under **Local Network**, select **cgw-dns-network**.
   f. Click **Save**.
2. Configure the on-premises side of the tunnel of connect to *local_gateway_ip*/32 in addition to the Local Gateway IP address. This allows DNS requests to be routed over the VPN.