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

https://docs.vmware.com/
Contents

About VMware Cloud on AWS Operations  6

1 About Software-Defined Data Centers  7
   Supported SDDC Versions  7
   Configuration Maximums for VMware Cloud on AWS  8
   Correlating VMware Cloud on AWS with Component Releases  8
   VMware Cloud on AWS Developer Resources  9
   Deploying and Managing a Software-Defined Data Center  9
      Deploy an SDDC from the VMC Console  12
      Rename an SDDC  15
      Delete an SDDC  16
   Creating and Managing SDDC Deployment Groups with VMware Transit Connect™  16
      Create or Modify an SDDC Group  21
      Add Compute Gateway Firewall Rules to Enable SDDC Group Member Workload Connectivity  24
      Attach a Direct Connect Gateway to an SDDC Group  26
      Use vCenter Linking in an SDDC Group  27
   SDDC Upgrades and Maintenance  29
      View an SDDC Maintenance Schedule Reservation  33
      View Maintenance Progress  33
      Convert UTC Time to Local Time  34
      Estimating the Duration of SDDC Maintenance  34
      Actions Taken by VMware to Ensure SDDC Health  35
   View Billing Information  36
   Upsize SDDC Management Appliances  37
   Roles and Permissions in the SDDC  38

2 Managing SDDC Hosts and Clusters  40
   VMware Cloud on AWS Host Types  40
   Add a Cluster  41
   Remove a Cluster  42
   Add Hosts  43
   Remove Hosts  44
   About Elastic DRS  45
      How the Elastic DRS Algorithm Works  46
      Select Elastic DRS Policy  48
   Using Policies and Profiles  49
      Create or Delete a VM-Host Affinity Policy  50
8 Service Notifications and Activity Log 97

View the Activity Log 97
View and Subscribe to the Service Status Page 98
Notifications Available from VMware Cloud on AWS 98

9 Troubleshooting 109

Get Support 109
Unable to Connect to VMware Cloud on AWS 109
Unable to Connect to vCenter Server 110
Unable to Select Subnet When Creating SDDC 111
Unable to Copy Changed Password Into vCenter Login Page 112
Compute Workloads Are Unable to Reach an On-Premises DNS Servers Over a Policy-Based VPN 112
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.
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
- Configuration Maximums for VMware Cloud on AWS
- Correlating VMware Cloud on AWS with Component Releases
- VMware Cloud on AWS Developer Resources
- Deploying and Managing a Software-Defined Data Center
- Creating and Managing SDDC Deployment Groups with VMware Transit Connect™
- SDDC Upgrades and Maintenance
- View Billing Information
- Upsize SDDC Management Appliances
- Roles and Permissions in the SDDC

**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

<table>
<thead>
<tr>
<th>SDDC Version</th>
<th>Expiration Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.10</td>
<td>TBD</td>
</tr>
<tr>
<td>1.9</td>
<td>December 31, 2020</td>
</tr>
<tr>
<td>1.8</td>
<td>November 30, 2020</td>
</tr>
<tr>
<td>1.7</td>
<td>Feb 28, 2020</td>
</tr>
<tr>
<td>1.6</td>
<td>October 31, 2019</td>
</tr>
</tbody>
</table>

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.

For the latest maximums, see VMware Configuration Maximums

Correlating VMware Cloud on AWS with Component Releases

The following table shows the ESXi, vCenter Server, NSX-T, and virtual machine hardware versions associated with each SDDC version.

<table>
<thead>
<tr>
<th>SDDC version</th>
<th>ESXi version</th>
<th>vCenter Server version</th>
<th>NSX-T version</th>
<th>Virtual Machine Hardware version</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.13</td>
<td>7.0.1 (Build 17230216)</td>
<td>7.0.1 (Build 17182107)</td>
<td>3.0.2 (Build 17148774)</td>
<td>17</td>
</tr>
<tr>
<td>1.12v2</td>
<td>7.0.1 (Build 17053012)</td>
<td>7.0.1 (Build 17053011)</td>
<td>3.0.2 (Build 17101807)</td>
<td>17</td>
</tr>
<tr>
<td>1.12</td>
<td>7.0.1 (Build 16862706)</td>
<td>7.0.1 (Build 16862250)</td>
<td>3.0.2 (Build 16837606)</td>
<td>17</td>
</tr>
<tr>
<td>1.11</td>
<td>7.0.0 (Build 16239929)</td>
<td>7.0.0 (Build 16241306)</td>
<td>2.5.1 (Build 16222301)</td>
<td>17</td>
</tr>
<tr>
<td>1.10v8</td>
<td>7.0.0 (Build 16737387)</td>
<td>7.0.0 (Build 16765794)</td>
<td>2.5.1 (Build 16798767)</td>
<td>17</td>
</tr>
<tr>
<td>1.10v7</td>
<td>7.0.0 (Build 16717799)</td>
<td>7.0.0 (Build 16763602)</td>
<td>2.5.1 (Build 16732946)</td>
<td>17</td>
</tr>
<tr>
<td>1.10v6</td>
<td>7.0.0 (Build 16447747)</td>
<td>7.0.0 (Build 16591182)</td>
<td>2.5.1 (Build 16586072)</td>
<td>17</td>
</tr>
<tr>
<td>1.10v5</td>
<td>7.0.0 (Build 16447747)</td>
<td>7.0.0 (Build 16350205)</td>
<td>2.5.1 (Build 16432221)</td>
<td>17</td>
</tr>
<tr>
<td>SDDC version</td>
<td>ESXi version</td>
<td>vCenter Server version</td>
<td>NSX-T version</td>
<td>Virtual Machine Hardware version</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------------</td>
<td>------------------------</td>
<td>---------------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>1.10v4</td>
<td>7.0.0 (Build 16365721)</td>
<td>7.0.0 (Build 16350205)</td>
<td>2.5.1 (Build 16329990)</td>
<td>17</td>
</tr>
<tr>
<td>1.10v3</td>
<td>7.0.0 (Build 16183155)</td>
<td>7.0.0 (Build 15987059)</td>
<td>2.5.1 (Build 15978420)</td>
<td>17</td>
</tr>
<tr>
<td>1.10v2</td>
<td>7.0.0 (Build 15866630)</td>
<td>7.0.0 (Build 15900180)</td>
<td>2.5.1 (Build 15833404)</td>
<td>17</td>
</tr>
<tr>
<td>1.10</td>
<td>7.0.0 (Build 15734104)</td>
<td>7.0.0 (Build 15726776)</td>
<td>2.5.1 (Build 15698959)</td>
<td>17</td>
</tr>
<tr>
<td>VMware Cloud on AWS GovCloud (1.9)</td>
<td>7.0.0 (Build 15423985)</td>
<td>7.0.0 (Build 15424599)</td>
<td>2.5.1 (Build 15419370)</td>
<td>17</td>
</tr>
<tr>
<td>1.9</td>
<td>7.0.0 (Build 15423985)</td>
<td>7.0.0 (Build 15424599)</td>
<td>2.5.1 (Build 15419370)</td>
<td>17</td>
</tr>
<tr>
<td>1.8v3</td>
<td>6.9.1 (Build 15150309)</td>
<td>6.9.1 (Build 14699973)</td>
<td>Build 14698810</td>
<td>15</td>
</tr>
<tr>
<td>1.8v2</td>
<td>6.9.1 (Build 14665869)</td>
<td>6.9.1 (Build 14699973)</td>
<td>Build 14698810</td>
<td>15</td>
</tr>
</tbody>
</table>

**VMware Cloud on AWS Developer Resources**

VMware Cloud on AWS provides an open, extensible framework that enables customers, partners, independent software vendors, and open-source software contributors to create scripts, solutions and services that integrate, extend, and automate SDDC creation, deployment, and management.

Visit the [VMware Cloud on AWS Dev Center](https://devcenter.vmware.com) to find out more about the available APIs, SDKs, CLIs, and other resources. You can also use many of the native vSphere tools that apply to your on-premises vSphere installation to automate vSphere operations in the SDDC. See [Working with the Developer Center](https://pubs.vmware.com/vsphere-7x/topic/com.vmware.vsphere.doc_7.0/vsphere-deploy-center.html) in the [vSphere Documentation](https://pubs.vmware.com/vsphere-7x/topic/com.vmware.vsphere.doc_7.0/vsphere-deploy-center.html).

**Deploying and Managing a Software-Defined Data Center**

Deploying a Software-Defined Data Center is the first step for using the VMware Cloud on AWS service. After you deploy the SDDC, you can view information about it and perform management tasks.

There are several actions to be considered before deploying your SDDC.

**Connected AWS Account**

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

You can deploy one, two or multiple hosts on VMware Cloud on AWS.
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 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. It helps you 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 subnet must exist in the connected AWS account. It cannot be one owned by and shared from another account.

- 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 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 if 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 do not 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 do not 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 cannot convert a stretched cluster to a standard cluster, or conversely.
- 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 VMware Configuration Maximums.

Connecting to the SDDC and Configuring SDDC Networks

Before you can migrate your workload VMs and manage them in VMware Cloud on AWS, you must connect your on-premises data center to your SDDC. You can use the public Internet, AWS Direct Connect, or both for this connection. You must also 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.

Credit Card Payments

If you choose to use a credit card to pay for your VMware Cloud on AWS SDDC, rather than SPP credits or another method, you will incur a one-time $2000 pre-charge the first time you deploy an SDDC. Any SDDC usage in your first 60 days will be charged against this pre-charged amount. If you delete your initial SDDC before using up the $2000, any remaining amount is not refunded, but the usage for any other SDDCs you deploy counts towards this amount. Usage beyond this amount will be charged to your credit card. If you reach the end of the 60 days without consuming the full $2000 pre-charge, you forfeit any remainder. This pre-charge amount can only be used for VMware Cloud on AWS, and not other VMware Cloud services.
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

2. Click Create SDDC.
3. Configure SDDC properties.
    a. Select the AWS region in which to deploy the SDDC.
       See Available AWS Regions for a list of available regions and the features they support.
    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 two or more hosts. Three hosts is the default.                                                      |
       | Stretched Cluster | If you create a multiple-host SDDC, you also have the option to create a stretched cluster that spans two availability zones (AZs). This configuration provides data redundancy in the event that there is a problem with one of the AZs. The system deploys management VMs in the first AZ you select. Both AZs can be used by your workloads. Either can be used for failover. You must have a minimum of six hosts in a stretched cluster, and you must deploy an even number of hosts. |
    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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>i3 (Local SSD)</td>
<td>Provision hosts with a fixed amount of local SSD storage per host.</td>
</tr>
<tr>
<td>i3en (Local SSD)</td>
<td>Provision hosts with a larger amount of local SSD storage per host. i3en</td>
</tr>
<tr>
<td></td>
<td>hosts are currently only available with version 1.10v4 of the SDDC software,</td>
</tr>
<tr>
<td></td>
<td>and are only available in some regions.</td>
</tr>
</tbody>
</table>

e 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 (Optional) Select the size of the SDDC appliances.

By default, a new SDDC is created with medium-sized NSX Edge and vCenter Server appliances. Large-sized appliances are recommended for deployments with more than 30 hosts or 3000 VMs or in any other situation where management cluster resources might be oversubscribed. Large-sized appliances are also required if you want to Configure a Multi-Edge SDDC With Traffic Groups.

To deploy the SDDC with large appliances, click **Show Advanced Configuration** and select **Large** from the drop-down control.

If you create the SDDC with a medium appliance configuration and find that you need additional management cluster resources, you can upsize the configuration to large. See Upsize SDDC Management Appliances.

5 Click **Next** to 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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Skip for now</td>
<td>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.</td>
</tr>
<tr>
<td>Use an existing AWS account</td>
<td>From the Choose an AWS account drop-down, select 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.</td>
</tr>
<tr>
<td>Connect a new AWS account</td>
<td>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.</td>
</tr>
</tbody>
</table>
6  (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 the Management Subnet 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. For a complete list of IPv4 addresses reserved by VMware Cloud on AWS, see [Reserved Network Addresses](#) in the *VMware Cloud on AWS Networking and Security* guide.

- If you are deploying a single-host SDDC, the IP address range 192.168.1.0/24 is reserved for the default compute network of the SDDC. If you specify a management network address range that overlaps that address, 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.

- 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.

<table>
<thead>
<tr>
<th>CIDR block size</th>
<th>Number of hosts (Single AZ)</th>
<th>Number of hosts (Multi AZ)</th>
</tr>
</thead>
<tbody>
<tr>
<td>23</td>
<td>27</td>
<td>22</td>
</tr>
<tr>
<td>20</td>
<td>251</td>
<td>246</td>
</tr>
<tr>
<td>16</td>
<td>See <a href="#">VMware Configuration Maximums</a></td>
<td></td>
</tr>
</tbody>
</table>

7  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.

Available AWS Regions

VMware Cloud on AWS is available in many AWS regions.

AWS Regions that Support VMware Cloud on AWS

Most of the AWS regions that support VMware Cloud on AWS also support stretched clusters.

<table>
<thead>
<tr>
<th>AWS Region Name</th>
<th>Stretched Cluster Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asia Pacific (Mumbai)</td>
<td>Y</td>
</tr>
<tr>
<td>Asia Pacific (Seoul)</td>
<td>Y</td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td>Y</td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td>Y</td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td>Y</td>
</tr>
<tr>
<td>Canada (Central)</td>
<td>Y</td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td>Y</td>
</tr>
<tr>
<td>Europe (Ireland)</td>
<td>Y</td>
</tr>
<tr>
<td>Europe (London)</td>
<td>Y</td>
</tr>
<tr>
<td>Europe (Paris)</td>
<td>Y</td>
</tr>
<tr>
<td>Europe (Stockholm)</td>
<td>Y</td>
</tr>
<tr>
<td>South America (São Paulo)</td>
<td>Y</td>
</tr>
<tr>
<td>US East (N. Virginia)</td>
<td>Y</td>
</tr>
<tr>
<td>US East (Ohio)</td>
<td>Y</td>
</tr>
<tr>
<td>US West (N. California)</td>
<td>N</td>
</tr>
<tr>
<td>US West (Oregon)</td>
<td>Y</td>
</tr>
</tbody>
</table>

Rename an SDDC

You can rename an existing SDDC. SDDC names are limited to 128 characters. They are not required to be unique.

Procedure

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](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**.

### Creating and Managing SDDC Deployment Groups with VMware Transit Connect™

An SDDC deployment group uses VMware Transit Connect to provide high-bandwidth, low-latency connections between SDDCs in the group and to other VPCs in the same region. You can also add a Direct Connect Gateway (DXGW) to provide centralized connectivity to your on-premises SDDCs.

An SDDC deployment group (SDDC Group) is a logical entity designed to simplify management of your organization's VMware Cloud on AWS resources at scale. Collecting SDDCs into an SDDC Group provides a number of benefits to an organization with multiple SDDCs whose workloads need a high-bandwidth, low-latency connection to each other. All network traffic between group members travels over a VMware Transit Connect network. Routing between compute networks of all SDDCs in a group is managed automatically by VMware Transit Connect as subnets are added and deleted. You control network traffic among group member workloads with compute gateway firewall rules.

Any organization member who has a VMC service role of **Administrator** or **Administrator (Delete Restricted)** can create or modify an SDDC Group.
Group Membership

SDDC groups are an organization-level object. An SDDC group cannot contain SDDCs from more than one organization. An SDDC must meet several criteria to be eligible for group membership:

- It must be in the same AWS region as other group members.
- Its management network CIDR block cannot overlap the management CIDR block of any other group member.
- It cannot be a member of another SDDC Group.
- It must be at SDDC version 1.11 or later.

While you can create a group with a single member, most practical applications of SDDC Groups require two or more members.

**Note** Hybrid Linked Mode over a VPN connection is incompatible with SDDC groups. If you add an SDDC that you've configured to use Hybrid Linked Mode over a VPN connection, the connection will fail and you won't be able to use Hybrid Linked Mode with that SDDC. Hybrid Linked Mode over a DX connection is unaffected when an SDDC is added to a group.

Internal Group Connectivity Using VMware Transit Connect

Peer connectivity among SDDC group members requires a VMware Managed Transit Gateway (VTGW). This is an AWS resource owned and managed by VMware. Adding the first member to an SDDC Group creates one of these resources and assigns it to the group. Creation and operation of a VTGW incurs additional charges on your VMware Cloud on AWS bill.
Members can be added to and removed from a group as needed. You cannot remove a group until all members have been removed. Removing the group also destroys the group's VMware Managed Transit Gateway.
Attaching a VPC to an SDDC Group

Attaching a VPC to an SDDC group simplifies network connections between SDDCs in the group and AWS services that run in that VPC. You use the VMC Console to make the VTGW (an AWS resource) available for sharing, then use the AWS console to accept the shared resource and associate it with the VPCs you’d like to attach to the SDDC Group.

Figure 1-2. Using VMware Transit Connect to Attach a VPC to an SDDC Group
External Group Connectivity Using AWS Direct Connect Gateway

To provide network connectivity between the group and external endpoints such as on-premises SDDCs, associate an AWS Direct Connect Gateway with the VMware Managed Transit Gateway created for the group. Unlike the Direct Connect (DX) configuration that you can use to connect your on-premises SDDC with a standalone VMware Cloud on AWS SDDC, the Direct Connect gateway that you associate with the VTGW provides DX-level connectivity to all SDDC group members.

Figure 1-3. An AWS Direct Connect Gateway Connects the SDDC Group to On-Premises SDDCs
Routing and Peering

Compute networks in all group members use the VMware Transit Connect route table. Learned routes from this table are added to the route table of the SDDC's Tier-0 router. To view or download a list of VMware Transit Connect routes learned and advertized by a member SDDC, open the SDDC’s Networking & Security tab and click Transit Connect. See View Routes Learned and Advertised over VMware Transit Connect in the VMware Cloud on AWS Networking and Security guide.

To view the routes learned and advertised by all SDDCs in the group, click the Routing tab. You can use the drop-down control. Select External to view routes between members or Members to view routes between members and external endpoints like VPCs or Direct Connect Gateways.

SDDCs in the group learn routes to the networks advertised by other SDDCs and VPCs in the group, and those advertised over the group’s Direct Connect Gateway. Because AWS imposes a limit of 20 prefixes that can be advertised by a Direct Connect Gateway to an external endpoint like an on-premises SDDC, the CIDR block prefixes of all SDDC group members must fall within a range that can be summarized in a way that won't exceed that limit.

VMware Transit Connect enforces several routing policies:

- Traffic originating from SDDCs can be routed to other SDDCs as well as to VPCs and Direct Connect Gateways attached to the group.
- Traffic originating from VPCs or Direct Connect Gateways attached to the group can be routed only to SDDCs in the group.
- Traffic between VPCs or between a VPC and the Direct Connect Gateway is blocked.

Note When you connect an SDDC to VMware Transit Connect or a Direct Connect Gateway, several aspects of existing SDDC networking change:

- Routes advertised by a route-based VPN are preferred over routes advertised by VMware Transit Connect or a Direct Connect Gateway.
- Use of a route-based VPN as a backup to Direct Connect is unsupported when your SDDC Group includes a Direct Connect Gateway. To disable this configuration in your SDDC, select Networking & Security > Direct Connect and set the Use VPN as backup to Direct Connect switch to Disabled.
- The jumbo MTU size is decreased to 8500 bytes. See Create a Private Virtual Interface for SDDC Management and Compute Network Traffic in the VMware Cloud on AWS Networking and Security guide for information about how to update this value for your SDDC.

Create or Modify an SDDC Group

To create an SDDC Group, give the group a name and description, then select SDDCs from your organization to be members.
Prerequisites

You must be logged into the VMC console as a user with a VMC service role of Administrator or Administrator (Delete Restricted).

Procedure


2. On the Software-Defined Data Centers (SDDC) page, click SDDC Groups.

3. On the SDDC Groups tab, click ACTIONS and select Create SDDC Group.
   Give the group a Name and optional Description, then click NEXT. You can edit the group later to change these values.

4. On the Membership grid, select the SDDCs to include as group members.
   The grid displays a list of all SDDCs in your organization. To qualify for membership in the group, an SDDC must meet several criteria:
   - It must be in the same Location (AWS region) as the other SDDCs you select.
   - It must not have a Management CIDR block that overlaps the management CIDR block of another SDDC in the group.
   - It must not be a member of another SDDC Group.
   - It must be at SDDC version 1.11 or later.

   When you have finished selecting members, click NEXT. You can edit the group later to add or remove members.

5. Acknowledge that you understand and take responsibility for the costs you incur when you create an SDDC group, then click CREATE GROUP to create the SDDC Group and its VMware Transit Connect network.
   Charges begin when you click CREATE GROUP. You cannot pause or cancel the process after it starts. Group members won’t be able to use the group’s VMware Transit Connect network until deployment is complete. Deployment typically takes about fifteen minutes. When deployment is complete, the group’s Connectivity Status changes from PENDING to CONNECTED.

6. (Optional) To modify the group name and description or to add or remove group members, click ACTIONS and select Edit Group.
   You cannot edit the group while its Connectivity Status is PENDING.

What to do next

To view the routes learned and advertised by all SDDCs in the group, click the Routing tab. You can use the drop-down control. Select External to view routes between members or Members to view routes between members and external endpoints like VPCs or Direct Connect Gateways.
To enable network traffic between workloads in member SDDCs, you'll need to create a set of compute gateway firewall rules in each member. See Add Compute Gateway Firewall Rules to Enable SDDC Group Member Workload Connectivity for details. You'll need to do this for each new member you add to the group.

**Attach a VPC to an SDDC Group**

You can use VMware Transit Connect to attach an AWS VPC to an SDDC Group. Doing this simplifies network connections between SDDCs in the group and the AWS services that run in that VPC.

Attaching a VPC to the SDDC group is a multi-step process that requires you to use both the VMC Console and the AWS console. You use the VMC Console to make the VTGW (an AWS resource managed by VMware) available for sharing. You then use the AWS console to accept the shared resource and associate it with the VPCs you'd like to attach to the SDDC Group.

**Procedure**

1. On the Software-Defined Data Centers (SDDC) page of the VMC Console, click SDDC Groups, then click the Name of the group to which you want to attach the VPC.

2. On the VPC Connectivity tab for the group, click ADD ACCOUNT and specify the AWS account that owns the VPC you want to add to the group.

   This enables AWS resource sharing in that account for the VTGW.

3. In the AWS console, open the Resource Access Manager and accept the shared VTGW resource.

   It will be listed under Shared with me, and will have a Name of the form VMC-Group-UUID and a Status of Pending.

4. In the VMC Console, return to the VPC Connectivity tab for the group and wait for Status of the resource share you created in Step 2 to change to ASSOCIATED.

5. In the VMC Console, return to the VPC Connectivity tab for the group and ACCEPT the shared VPC attachment.

   When the VPC status changes to PENDING_ACCEPTANCE, click ACCEPT to accept it. The status changes to AVAILABLE after the acceptance process completes.

**What to do next**

- Update the VPC’s route tables to add the VTGW CIDR as a destination. See Adding and removing routes from a route table in the Amazon Virtual Private Cloud User Guide.

- In the AWS console, create network ACLs to manage traffic between the VPCs you've added to the group and other group members. If you want to access an AWS service running in the VPC, you might need to modify the AWS security policy for the service. See Access an S3 Bucket Using an S3 Endpoint for an example of AWS security policy configuration for the S3 service.
Remove an SDDC Group

To remove an SDDC Group, remove all members from the group, then delete the group.

Removing a member from a group disconnects it from the group’s VTGW but makes no other changes in group properties. Removing an SDDC group destroys the group’s VMware Transit Connect network and any routing information associated with it, along with its VTGW.

Prerequisites

You must be logged into the VMC console as a user with a VMC service role of Administrator or Administrator (Delete Restricted).

Procedure

2. On the Software-Defined Data Centers (SDDC) page, click SDDC Groups and click the group you want to remove.
3. Click the Name checkbox to select all SDDCs in the group, then click REMOVE SDDCS.
   - Confirm that you understand the implications of removing the SDDCs, then click CONTINUE to proceed with the removal. Removal can take several minutes per SDDC.
4. After all the SDDCs have been removed, click ACTIONS > Delete Group to remove the group and its associated AWS resources.
   - Confirm that you understand the effects of removing the group, then click DELETE GROUP to proceed with the removal.

Add Compute Gateway Firewall Rules to Enable SDDC Group Member Workload Connectivity

You must create firewall rules for the Compute Gateway of each SDDC in the group. Without these rules, workloads running on group members cannot use VMware Transit Connect to communicate with each other.

Because all members of an SDDC Group are owned by the same VMware Cloud on AWS organization, network traffic among members of the group can be safely treated as East-West traffic, rather than North-South traffic that might have an external source or destination. But since an SDDC compute gateway’s default firewall rules reject external traffic, you’ll need to create firewall rules allowing that traffic through the compute gateway of each SDDC in the Group. (SDDC Groups do not currently need to route network traffic through members’ management gateways.)

The system defines a set of inventory groups intended for use in Compute Gateway firewall rules that provide high-level control over traffic among group members. These groups contain the prefixes (CIDR blocks) for routes learned over VMware Transit Connect.

Deployment Group DGW Prefixes
Routes learned from the group's Direct Connect Gateway.

**Deployment Group Native VPCs Prefixes**
Routes learned from the group's attached VPCs.

**Deployment Group other SDDCs Prefixes**
Routes learned from other SDDCs in the group.

Prefixes in each of these groups are automatically added, removed, and updated as group membership changes and new routes are learned.

For more information, see Add or Modify Compute Gateway Firewall Rules in the *VMware Cloud on AWS Networking and Security* documentation.

**Procedure**

1. On the **Networking & Security** tab, click **Gateway Firewall**.

2. Define inventory groups as needed to provide sources and destinations for workload traffic.

   The system-defined inventory groups are useful for creating high-level connectivity among group members and attached VPCs. If you need to create finer-grained firewall rules that apply to individual workload segments in member SDDCs, you'll need to create inventory groups that define those segments, as shown in the example below.

3. On the **Gateway Firewall** card, click **Compute Gateway**, then click **ADD RULE**.

   The system-defined inventory groups, along with any compute groups you defined are available as choices in the **Sources** and **Destinations** drop-downs. To enable unrestricted group connectivity, you could add a rule like this one, which allows inbound traffic to this SDDC from other group members.

<table>
<thead>
<tr>
<th>Name</th>
<th>Sources</th>
<th>Destinations</th>
<th>Services</th>
<th>Applied To</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound from other SDDCs</td>
<td>Deployment Group other SDDCs Prefixes</td>
<td>Any</td>
<td>Any</td>
<td>Direct Connect Interface</td>
<td>Allow</td>
</tr>
</tbody>
</table>

   If you have created inventory groups with the CIDR blocks of your local workload segments, you can use them to create rules at a higher precedence that apply finer-grained controls over this traffic.

**Example: CGW Firewall Rules with User-Defined Inventory Groups to Allow Workload Traffic Between Group Members**

**Create the Groups**

On the **Groups** card, click **COMPUTE GROUPS**, then click **ADD GROUP** and create three groups. You can use any names you want for the groups. The ones we show here are just examples.

- A group named **Local Workloads** that includes segment prefixs for the SDDC's own workload segments.
A group named **Peer Workloads** that includes segment prefixes for workload segments of other SDDCs in the group.

- A group named **Peer SDDC vCenters** that includes the private IP address of the vCenter in each SDDC in the group.

For each group, click **Set Members** to open the **Select Members** tool. In this tool, you can click **ADD CRITERA** and enter the **IP Addresses** or **MAC Addresses** of group members. You can also click **ACTIONS > import** to import these values from a file.

### Create the Rules

As shown in **Step 3**, open the **Gateway Firewall** card, click **Compute Gateway**, then click **ADD RULE** to create new rules that use the inventory groups you created for their **Sources** and **Destinations**. You can use any names you want for the rules. The ones we show here are just examples.

<table>
<thead>
<tr>
<th>Name</th>
<th>Sources</th>
<th>Destinations</th>
<th>Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local workload to peer workload</td>
<td>Local Workloads</td>
<td>Peer Workloads</td>
<td>As needed for outbound traffic from local workloads to workloads in other group members</td>
</tr>
<tr>
<td>Peer workload to local workload</td>
<td>Peer Workloads</td>
<td>Local Workloads</td>
<td>As needed for in traffic to local workloads from workloads in other group members</td>
</tr>
</tbody>
</table>

All rules governing SDDC group member traffic through the compute gateway firewall should be applied to **All Uplinks** and have an action of **Allow**.

### Attach a Direct Connect Gateway to an SDDC Group

After you create an SDDC Group, you can attach an AWS Direct Connect Gateway to it to support high-bandwidth, low-latency connections to your on-premises SDDC.

VMware Transit Connect handles all compute and management network traffic among SDDC group members. Many SDDC group members will also need to make network connections to external endpoints such as on-premises SDDCs, VPCs outside the group, and AWS services that run in them. To enable these kinds of connections, associate an AWS Direct Connect Gateway with the group's VMware Managed Transit Gateway.

Attaching a Direct Connect Gateway to the SDDC group is a multi-step process that requires you to use both the VMC Console and the AWS console. You use the VMC Console to make the VTGW (an AWS resource) available for sharing. You then use the AWS console to accept the shared resource and associate it with the Direct Connect Gateway you'd like to attach to the SDDC Group.
Prerequisites

You must create an AWS Direct Connect Gateway. See Creating a Direct Connect gateway in the AWS documentation.

Procedure

1. On the Software-Defined Data Centers (SDDC) page of the VMC Console, click SDDC Groups, then click the Name of the group to which you want to attach the Direct Connect Gateway.

2. On the Direct Connect Gateway tab for the group, click ADD ACCOUNT and specify the AWS account that owns the Direct Connect Gateway you want to add to the group.

   On the Add Direct Connect Gateway page, fill in the following values:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct Connect Gateway ID</td>
<td>The ID value, displayed on the AWS console Direct Connect Gateways page for the gateway object.</td>
</tr>
<tr>
<td>Direct Connect Gateway Owner</td>
<td>The AWS account number that owns the Direct Connect Gateway ID.</td>
</tr>
<tr>
<td>Allowed Prefixes</td>
<td>A comma-separated list of compute network CIDR blocks of SDDC group members.</td>
</tr>
</tbody>
</table>

   Click OK to generate an association proposal in AWS for the specified gateway.

3. In the AWS console, open the Direct Connect Gateways page for the gateway object and accept the association proposal.

   Acceptance can take up to 20 minutes. When it completes:
   - In the AWS console, the gateway will have a State of associated on the AWS Direct Connect Gateways page for the gateway object.
   - In the VMC Console, the gateway will have a Status of Connected in the Direct Connect tab for the group.

4. Attach an AWS Transit VIF between the Direct Connect Gateway and your Direct Connect Location (Direct Connect provider).

   See Transit gateway attachments to a Direct Connect gateway in the AWS VPC documentation.

What to do next

Create any firewall rules needed to allow traffic between the Direct Connect Gateway and the on-premises SDDC.

Use vCenter Linking in an SDDC Group

An organization that includes an SDDC deployment group can link the vCenter Server systems in those SDDCs to enable an administrator to manage their combined inventories in the same vSphere Client view.
When you enable vCenter linking in an SDDC group, a cloud administrator can log in as clouadmin@vmc.local and use the vSphere Client to manage all the vCenter Server systems in the group. If the clouadmin@vmc.local account configures these systems to use single sign-on, then users with accounts in that single sign-on domain can access all the linked systems in the group.

After vCenter linking has been enabled in an SDDC group, the vCenter Server systems in SDDCs added to the group are linked automatically, and vCenter Server systems in SDDCs that are removed from the group are unlinked automatically.

**Prerequisites**

**Networking**

The required L3 networking for this feature is offered by VMware Transit Connect which is already configured as part of the creation of the SDDC Group. Each linked vCenter Server in the group must be able to reach the other linked vCenter Server instances at a private IP address using a route that goes through the group's VMware Transit Connect. Other routing configurations are not supported.

Migration with vMotion of a VM across the vCenter Server instances in a linked SDDC group does not work because VMware Transit Connect only creates L3 connectivity between the group members.

**SDDC Version**

vCenter Linking requires SDDC version 1.12 or higher.

**Service Role**

This operation is restricted to users with a VMC service role of **Administrator** or **Administrator (Delete Restricted)**.

**vCenter Name Resolution**

Each linked vCenter Server in the group must be able to resolve the hostname and FQDN of the other linked vCenter Servers to a private IP address. See Set vCenter Server FQDN Resolution Address in the VMware Cloud on AWS Networking and Security guide.

**Hybrid Linked Mode**

As noted in Creating and Managing SDDC Deployment Groups with VMware Transit Connect™, use of Hybrid Linked Mode over a VPN connection is not supported when the SDDC is a member of an SDDC group. You can configure Hybrid Linked Mode with the Cloud Gateway Appliance over a Direct Connect Gateway (DXG) connection to an SDDC group member and use it to manage that SDDC's vCenter Server even if it is linked with other vCenter Server systems in the group.

**Procedure**

On the **Software-Defined Data Centers (SDDC)** page, click **SDDC Groups**.

This page lists all the SDDC groups in your organization. To create an SDDC group, see **Create or Modify an SDDC Group**.

On the **SDDC Groups** page, choose an SDDC group card, click **VIEW DETAILS**, and open the **vCenter Linking** tab.

This page presents a list of all the SDDCs in the group, their versions, and vCenter Server linking status.

To link all the vCenter Server systems in the list, click **LINK ALL VCENTERs**.

This action links all the vCenter Server systems that have a status of **Unlinked**. Linking vCenter Server systems in an SDDC group is something you do only once. It establishes a group property ensuring that vCenter Server systems in the group are always linked, regardless of the set of member SDDCs, until you deliberately unlink them. After you **LINK ALL VCENTERs** in a group vCenter linking is automatic whenever an SDDC is added to the group. Linked vCenter Server systems are unlinked automatically when their SDDC is removed from the group.

(Optional) Configure a shared identity source for the linked vCenter Server systems.

If you configure the linked vCenter Server systems to use the same identity source, user accounts defined in that identity source can access all linked vCenter Server systems with the privileges defined for their account in the identity source. See **vSphere Authentication with vCenter Single Sign-On** in the **VMware vSphere Documentation** for configuration details. If you don't take this step, cloudadmin@vmc.local can authenticate to all linked vCenter Server systems using the credentials listed on the **Settings** tab of the VMC Console.

To unlink all the vCenter Server systems in the list, click **UNLINK ALL VCENTERs**.

This action unlinks all the vCenter Server systems that have a status of **Linked**. Like linking vCenter Server systems in an SDDC group, unlinking is something you do only once. It establishes a group property ensuring that vCenter Server systems in the group are not linked until you deliberately link them. After you **UNLINK ALL VCENTERs** in a group, vCenter Server systems remain unlinked when an SDDC is added to the group.

**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 SDDC fleet.

Upgrades to even-numbered releases of the SDDC software, such as VMC Version 1.10 or 1.12, will be provided to all SDDCs and are mandatory. Upgrades to odd-numbered releases, such as 1.11 or 1.13, are available to request. If you want to upgrade an SDDC to an odd-numbered release version, contact your VMware TAM, sales, or customer success representative to request an upgrade. The request will be evaluated by VMware and considered based on business need.
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, completes, is rescheduled, or is canceled. To ensure that you receive these notifications, ensure that donotreply@vmware.com is added to your email allow list.

**Upgrade Process for SDDCs Using NSX-T**

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

The impact of the upgrade on different elements of the SDDC infrastructure is shown in the figure below.

---

**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: Control Plane Updates. These are the updates to vCenter Server and NSX Edge. A backup of the management appliances is taken during this phase. If a problem occurs, there is a restore point for the SDDC. A management gateway firewall rule is added during this phase. There is an NSX Edge failover during this upgrade phase, resulting in a brief downtime. You do not have access to NSX Manager and vCenter Server during this phase. During this time, your workloads and other resources function as usual subject to the constraints outlined above.

**Note**  Upgrades from SDDC version 1.8 to version 1.10v2 or higher require NSX appliance configuration changes. This results in an NSX Edge failover that causes an additional downtime of approximately 10 seconds at the end of Phase 1.

Certificates for vCenter Server and NSX Edge are replaced during Phase 1 if the certificates were last replaced more than 14 days ago. If you are using other software that relies on the vCenter Server certificate, such as Horizon Enterprise, vRealize Operations, vRealize Automation, VMware Site Recovery, and many third-party management applications, you must re-accept the vCenter Server and NSX certificates in that software after Phase 1 of the upgrade.

**Note**  VMware HCX and VMware Site Recovery have their own certificates that are not replaced as part of the SDDC Upgrade process.

More information on updating certificates for specific products can be found below:

- AppVolumes: [https://kb.vmware.com/s/article/2150281](https://kb.vmware.com/s/article/2150281)
- Horizon Enterprise: [https://kb.vmware.com/s/article/74599](https://kb.vmware.com/s/article/74599)
- VMware Site Recovery: [https://kb.vmware.com/s/article/74599](https://kb.vmware.com/s/article/74599)

When Phase 1 is complete, you receive a notification. After Phase 1 is complete, there is a waiting period until Phase 2 starts. Phase 2 is initiated at a designated start time.

Phase 2: Host Updates. These are the updates to the ESXi hosts and host networking software in the SDDC. An additional host is temporarily added to your SDDC to provide enough capacity for the update. You are not billed for these host additions. vMotion and DRS activities occur to facilitate the update. The upgrade process has been improved so that only one NSX Edge migration occurs during the update. During this time, your workloads and other resources function as usual subject to the constraints outlined above. When Phase 2 is complete, the hosts that were temporarily added are removed from each cluster in the SDDC.

When Phase 2 is complete, you receive a notification. After Phase 2 is complete, there is a waiting period until Phase 3 starts. Phase 3 is initiated at a designated start time.

Phase 3: These are the updates to the NSX-T appliances. A backup of the management appliances is taken during this phase. If a problem occurs, there is a restore point for the SDDC. A management gateway firewall rule is added during this phase. You do not have access to NSX Manager and vCenter Server during this phase. 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.
For more information on estimating the duration of each phase, see *Estimating the Duration of SDDC Maintenance*.

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 not be upgraded as part of this 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.

**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.

**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.

**Impact of Updates on VMware Site Recovery**

The SDDC upgrade affects the VMware Site Recovery service, because during upgrades inbound management network traffic is stopped, and the vCenter Server instance is restarted. The impact is as follows:

- You cannot open the Site Recovery UI for the SDDC under maintenance. From the remote SDDC Site Recovery UI, this site will appear as disconnected.
- Recovery plan failover operations towards the SDDC under maintenance cannot be initiated. Failover operations in progress might fail when maintenance starts.
Incoming replications are interrupted. Depending on RPO settings and the maintenance duration, RPO violations notification for these replications might appear in the remote Site Recovery UI. RPO violations should disappear automatically sometime after the maintenance is completed, depending on when vSphere Replication manages to sync the accumulated delta. Replications outgoing from the SDDC under maintenance are not affected.

For more information, see the documentation for VMware Site Recovery at https://docs.vmware.com/en/VMware-Site-Recovery/index.html.

**View an SDDC Maintenance Schedule Reservation**

You can view the times scheduled for upcoming SDDC 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.

**Prerequisites**

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

**Procedure**

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.

**View Maintenance Progress**

You can view the progress of ongoing maintenance by clicking on the SDDC card in the VMC Console.

**Procedure**

2. Navigate to the **Maintenance** tab of your SDDC.
   
   If maintenance is ongoing, the maintenance summary shows information about the current phase and step of maintenance.

3. Click **View Details** to see more details on the maintenance steps.
   
   You can see details of the operations performed in each step, as well as start and end times for the steps.

4. (Optional) Click **View Times in Local Time Zone** to view the times in your local time zone rather than UTC time.
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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use a time zone calculator</td>
<td>Use the time zone calculator at <a href="https://www.timeanddate.com/worldclock/">https://www.timeanddate.com/worldclock/</a></td>
</tr>
<tr>
<td></td>
<td>converter.html to convert from UTC time to your time.</td>
</tr>
<tr>
<td>Compute local time using UTC offset</td>
<td>a Determine the time offset from UTC time for your local time zone. See</td>
</tr>
<tr>
<td></td>
<td>b Add the time offset to the UTC time (expressed in 24-hour time).</td>
</tr>
<tr>
<td></td>
<td>c If daylight saving time is in effect in your local time zone, adjust for</td>
</tr>
<tr>
<td></td>
<td>daylight saving time.</td>
</tr>
</tbody>
</table>

Estimating the Duration of SDDC Maintenance

VMware Cloud on AWS performs regular maintenance for your SDDC to keep it up-to-date with new features and capabilities.

The length of maintenance depends on many factors, including but not limited to:

- The number of clusters in the SDDC. Up to 10 clusters can be upgraded concurrently.
- The number of hosts in the SDDC
- The amount of data in vCenter Server, ESXi hosts, and NSX-T databases
- Time required to add and remove hosts. SDDCs used for VDI require additional time to update and remove hosts.
- Time to execute multiple service actions such as backup, pre-update, and post-update actions. When upgrading from SDDC version 1.8 to version 1.9 or higher, additional time is required for NSX appliance configuration changes.
- Transient environmental or infrastructure conditions

The number of factors makes it difficult to provide a precise estimate of the maintenance time. However, the numbers given below are based on historical data and should give you a good idea of the duration of upcoming maintenance for your SDDC.

Phase 1: Control Plane Updates

This phase consists of management appliance backup, updates to the vCenter Server, and updates to NSX Edge.

You can expect this phase to take approximately 3 to 4 hours.

Phase 2: Host Updates

This phase consists of updates to the hosts and host networking software in the SDDC.
Use the table below to estimate the duration of Phase 2.

<table>
<thead>
<tr>
<th>Process</th>
<th>Time</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup</td>
<td>30 minutes</td>
<td>Based on appliances' database size.</td>
</tr>
<tr>
<td>Add Host</td>
<td>30 minutes</td>
<td>Hosts are added to clusters in parallel.</td>
</tr>
<tr>
<td>Update Host</td>
<td>45-60 minutes per host</td>
<td>Clusters are updated in parallel. The duration for Phase 2 depends on the number of hosts in the largest cluster.</td>
</tr>
<tr>
<td>Remove Host</td>
<td>60 minutes</td>
<td>Hosts are removed from clusters in parallel.</td>
</tr>
</tbody>
</table>

Clusters are upgraded in parallel up to ten clusters at a time. If you have ten or fewer clusters, the overall upgrade time is determined by the largest cluster in the SDDC. If you have more than ten clusters, each additional cluster begins upgrading as soon as one of the initial ten clusters completes. In this case, the overall upgrade time is determined by the time required for the largest cluster of the initial ten, plus any additional time required to complete subsequent clusters that started after one of the first ten completed.

**Phase 3: NSX Appliance Updates**

This phase consists of management appliance backups and updates to the NSX Appliance(s). You can expect this phase to take approximately 2 to 4 hours.

**Actions Taken by VMware to Ensure SDDC Health**

VMware constantly monitors customer SDDC environments through automation and a team of Site Reliability Engineers (SRE). The following describes processes that VMware automates to ensure the health of SDDCs.

**VM Operations**

**Orphaned VM(s) Auto-Remediation**

If you use "No data redundancy/VMs w/ FTT=0" as a storage policy, you might experience data loss if there is a failure or if the VM becomes unresponsive. If a failure happens and a VM or VMs become orphaned, VMware performs a cleanup action. You will receive an email notification when this happens.

**vCenter Operations**

**vCenter Sessions (Connections) Maxed Out**

If many sessions are created and not cleared, vCenter Server might become inaccessible. Typically this is caused by automation creating a large number of sessions. This generates an automated alert and VMware will restart vCenter Server. You will receive an email notification when this happens.
A number of different issues might require a reboot of vCenter Server. Some issues might require an immediate reboot for remediation, while others might allow for continued usage with a reboot required in the near future. In the latter case, you will receive an email notification alerting you that a restart will occur in the next 24 hours. After a reboot, ongoing tasks and application connections might need to restart.

**Expired vCenter CA Certificate Removal**

Some product integrations install CA certificates on vCenter. If a CA certificate has expired, it could result in host add failures. Expired CA certificates will be removed.

**NSX Operations**

**Management Plane (NSX Manager) Restart**

A number of different issues might require a restart of NSX Manager. Some issues might require an immediate reboot for remediation, while others might allow for continued usage with a reboot required in the near future. For the short time while NSX Manager is in the process of restarting, you will not be able to access the SDDC Networking and Security UI. You will not receive an email notification for NSX Manager restart events.

**NSX Edge Failover**

If our monitoring system detects that an NSX Edge (active) is close to becoming unhealthy, we will schedule NSX Edge failover at off-peak hours. This scheduled failover is done as a proactive measure to avoid possible disruption from a failover happening at peak hours. If there is a problem with NSX (active) Edge before the scheduled failover, it will automatically failover. You will receive an email notification if we schedule an NSX Edge failover.

**SDDC Operations**

**Single Host SDDC Failure**

The Single Host SDDC starter configuration has no SLA and is appropriate for proof-of-concept or test and development use cases. VMware does not perform any remediation in the event of a Single Host SDDC failure. You will receive an email notification if a Single Host SDDC failure occurs.

**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

**Note** If you purchased through AWS, pricing and payment details are not shown in the VMware Cloud Services Console. Pricing is determined by your agreement with AWS. For more information, see [Purchase Options for VMware Cloud on AWS](https://docs.vmware.com/en/VMware-Cloud-services/services/GUID-B57490E3-1916-4214-B193-9D9E7AF3B10A.html).

**Procedure**


**Upsize SDDC Management Appliances**

When you create an SDDC, you can choose to have it contain medium or large SDDC appliance configurations. If you created the SDDC with a medium appliance configuration and find that you need additional management cluster resources, you can upsize the configuration to large.

By default, a new SDDC is created with medium-sized NSX Edge and vCenter Server appliances. Large-sized appliances are recommended for deployments with more than 30 hosts or 3000 VMs or in any other situation where management cluster resources might be oversubscribed. Large-sized appliances are also required if you want to [Configure a Multi-Edge SDDC With Traffic Groups](https://docs.vmware.com/en/VMware-Cloud-services/services/GUID-B57490E3-1916-4214-B193-9D9E7AF3B10A.html).

You can use a control on the SDDC **Settings** tab to upsize a medium-sized SDDC to a large-sized one. This change is permanent and cannot be undone. The operation incurs about an hour of SDDC downtime, and requires a vCenter re-start and an NSX failover. If there aren't enough free resources available, the operation adds a host to the SDDC.

**Note** This operation cannot be performed while SDDC maintenance, including the addition or removal of hosts, is underway.
Prerequisites

You must be logged in to the VMC Console at https://vmc.vmware.com. as a user with a VMC service role of Administrator or Administrator (Delete Restricted).

Procedure

2. On the card for your SDDC, click View Details and then click the Settings tab. The Settings page displays information about SDDC settings, pre-defined user accounts, and SDDC access via the API and PowerCLI.
3. Expand the Management Appliances item under the SDDC section of the Settings tab to view or change the appliance size in this SDDC. If the appliance size is NSX_MEDIUM, you can click UPSIZE to open the Upsize management appliances dialog. To upsize the appliance to NSX_LARGE, select the checkboxes to confirm that you understand the consequences of your action, then click UPSIZE.

The system displays a message to confirm that the requested operation has started and track its progress.

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 configure objects that are supported and managed by VMware, such as hosts, clusters, and management virtual machines. For detailed information about the privileges assigned to this role, see CloudAdmin Privileges.

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.

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

Understanding Authorization in vSphere in the vSphere Documentation 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.

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

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
- Add a Cluster
- Remove a Cluster
- Add Hosts
- Remove Hosts
- About Elastic DRS
- Using Policies and Profiles
- Microsoft Product Licenses in VMware Cloud on AWS
- Converting Clusters from i3 to i3en Hosts

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.
The I3 host type is the default host type. I3 hosts have 36 cores, 512GiB RAM, and 10.37TiB raw storage capacity 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.

I3en

The I3en host type is optimized for data-intensive workloads. I3en hosts have 96 logical cores, 768GiB RAM, and approximately 45.84 TiB raw storage capacity per host. Single-host or two-host SDDCs cannot contain the I3en host type. I3en hosts are currently available only in version 1.10v4 SDDCs, and in a limited number of regions.

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 that has the same permissions as the one created in the initial SDDC cluster.
- Each cluster contains a workloadDatastore that has the same permissions as the one created in the initial SDDC cluster.

Note The first cluster created in the SDDC is reserved for management workloads, and contains the Mgmt-ResourcePool and vsanDatastore. Additional clusters are created as needed for the workloadDatastore.

Procedure

2. On the card for the SDDC you want to add a cluster to, select Actions > Add Cluster.
3 Select the host type.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>i3 (Local SSD)</td>
<td>Provision hosts with a fixed amount of local SSD storage per host.</td>
</tr>
<tr>
<td>I3en (Local SSD)</td>
<td>Provision hosts with a larger amount of local SSD storage per host. I3en hosts are currently only available with version 1.10v4 of the SDDC software, and are only available in some regions.</td>
</tr>
</tbody>
</table>

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

For i3 hosts, 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.

For i3en hosts, all CPU cores are hyperthreaded and offered as logical cores 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 is offered as physical cores and 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 Click **Add Cluster**.

**Results**

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.

Note If you add one or more hosts to a two-host SDDC, the minimum size of that SDDC will be permanently increased to three hosts. You will not be able to reduce the number of hosts below three later.

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.

**Results**

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.

**Note** Although you can create an SDDC containing two hosts, you cannot reduce the number of hosts in an existing SDDC below three.
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

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.

   This action initiates the host removal process. If you are removing a single host, billing for that host stops immediately. Multiple hosts are removed one at a time to avoid violating vSAN storage policies. A host slated for removal transitions to the READY state while its data is being moved. It can take up to several hours to move large volumes of data. When the data move is complete, the host transitions out of the READY state and billing for that host stops.

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:

- Single host starter SDDCs

Special considerations apply to two-host SDDCs. Only the Default Storage Scale-Out policy is available for two-host SDDCs. EDRS cannot scale-in an SDDC to fewer than three hosts. Therefore, when a two-host SDDC is scaled-out to three hosts, it cannot be scaled back to two hosts.

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 your workloads' needs.

In a new SDDC, elastic DRS uses the Default Storage Scale-Out policy, adding hosts only when storage utilization exceeds the threshold of 75%. You can select a different policy if it provides better support for your workload VMs. For any policy, 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.

Note  For two-host SDDCs, only the Default Storage Scale-Out policy is available.

The following policies are available:

Optimize for Best Performance

This policy adds hosts more quickly and removes hosts more slowly in order to avoid performance slowdowns as demand spikes. It has the following thresholds:

<table>
<thead>
<tr>
<th>Resource</th>
<th>High Threshold</th>
<th>Low Threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>90% utilization</td>
<td>50% utilization</td>
</tr>
<tr>
<td>Memory</td>
<td>80% utilization</td>
<td>50% utilization</td>
</tr>
<tr>
<td>Storage</td>
<td>70% utilization</td>
<td>20% utilization</td>
</tr>
</tbody>
</table>

Optimize for Lowest Cost

This policy adds hosts more slowly and removes hosts more quickly in order to provide baseline performance while keeping host counts to a practical minimum. It has the following thresholds:
### Optimize for Rapid Scale-Out

This policy adds four hosts at a time when needed for memory or CPU, and adds hosts one at a time when needed for storage. You must manually remove these hosts when they are no longer needed. It has the following thresholds:

<table>
<thead>
<tr>
<th>Resource</th>
<th>High Threshold</th>
<th>Low Threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>90% utilization</td>
<td>60% utilization</td>
</tr>
<tr>
<td>Memory</td>
<td>80% utilization</td>
<td>60% utilization</td>
</tr>
<tr>
<td>Storage</td>
<td>70% utilization</td>
<td>20% utilization</td>
</tr>
</tbody>
</table>

#### Procedure

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

   The **Default Storage Scale-Out** policy has no parameters. For other policies, specify a **Minimum cluster size** of 3 or more and a **Maximum cluster size** consistent with your expected workload resource consumption. The **Maximum cluster size** applies to CPU and Memory. To maintain storage capacity and ensure data durability, the service can add more hosts than what you specified in **Maximum cluster size**.

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.
   - In your SDDC, click OPEN VCENTER.
   - From the vSphere Client Home, click Policies and Profiles > Compute Policies.
   - Click Add to open the New Compute Policy Wizard.
   - 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.
   - 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.
   - 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.

**Microsoft Product Licenses in VMware Cloud on AWS**

You have a variety of options for licensing Microsoft products running as workloads on VMware Cloud on AWS. You can use your existing licenses or purchase new licenses through VMware to use with VMware Cloud on AWS.
Bring Existing Windows Licenses to VMware Cloud on AWS

If you've already purchased Microsoft software, and the licenses are eligible, bring your own licenses (BYOL) to VMware Cloud on AWS. Bringing your own licenses allows you to:

- Take advantage of the efficiencies of the cloud while using already-purchased perpetual licenses.
- Extend the lifecycle of your software without additional hardware costs.
- Expedite your migration to the cloud by using existing VM images.

The requirements for bringing your own licenses to VMware Cloud on AWS depend on whether you have Microsoft Software Assurance and license mobility benefits associated with those licenses and when those licenses were acquired.

- If you do not have Software Assurance: You may migrate licenses for products purchased before October 1, 2019, or which were added as a true-up as part of an Enterprise Enrollment that was effective before October 1, 2019. These licenses can only be upgraded to versions that were available before October 1, 2019. See The Amazon Web Services and Microsoft FAQ for more information.

  **Note**  This scenario particularly applies to Windows Server licenses. Windows Server is not eligible for license mobility benefits, and therefore you cannot migrate any Windows Server licenses purchased after October 1, 2019.

- If you have Software Assurance: Microsoft License Mobility through Software Assurance allows many Microsoft licenses to be migrated to VMware Cloud on AWS. For more information on License Mobility, see License Mobility.

Subscribe to Windows Server and SQL Server Licenses from VMware

You can subscribe to Windows Server and SQL Server licenses for your use on VMware Cloud on AWS. The licenses are:

- Offered per host for all hosts in the cluster. All hosts in a cluster must be licensed.
- Billed on a calendar month basis based on the maximum number of hosts that were deployed in that cluster during the month. You are not billed for maintenance or remediation hosts.
- Billing begins when you select the license. If you choose to remove the license, you are billed for the entire calendar month.
- After you have selected the licenses, you may deploy an unlimited number of the applicable VMs on the licensed hosts.

License Mobility

Eligible Microsoft server applications such as Microsoft SQL Server, may, in certain cases, be deployed on VMware Cloud on AWS using existing licenses.
This allows you to more easily move your workloads to a VMware Cloud on AWS SDDC, without any additional Microsoft software licensing fees. Microsoft Volume Licensing customers with eligible server applications covered by active Microsoft Software Assurance (SA) contracts may migrate licenses acquired after October 1, 2019. Not only will License Mobility make the transition easier for existing SA customers, it provides customers who prefer to purchase perpetual licenses the ability to continue doing so while still taking advantage of the efficiencies of the cloud.

**Note** Licenses acquired before October 1, 2019 may be migrated with or without Software Assurance (SA) or any additional steps.

### How to Sign Up

All customers using License Mobility through Software Assurance must complete a license verification process with Microsoft, and Microsoft will ensure that you have eligible licenses with active Software Assurance. To start the verification process and review additional details, go to: [https://www.microsoft.com/en-us/licensing/licensing-programs/software-assurance-license-mobility.aspx](https://www.microsoft.com/en-us/licensing/licensing-programs/software-assurance-license-mobility.aspx).

Within 10 days of deployment, complete the License Verification Form available on the Volume Licensing Document Search website and provide it to your Microsoft representative or preferred resell partner, so he or she can submit your form to Microsoft. Once submitted, Microsoft will confirm your eligibility and communicate your verification status to you and your chosen Authorized Mobility Partner.

### Eligibility for License Mobility

To be eligible for license mobility, the following conditions must be met:

- All Microsoft server products migrated to VMware Cloud on AWS must be eligible via the Microsoft License Mobility through Software Assurance program as set forth by Microsoft at [http://www.microsoft.com/licensing/about-licensing/product-licensing.aspx](http://www.microsoft.com/licensing/about-licensing/product-licensing.aspx)

  - Exchange Server
  - SharePoint Server
  - SQL Server Standard Edition
  - SQL Server Enterprise Edition
  - SQL Server Business Intelligence Edition
  - Skype for Business Server
  - System Center Server
  - Dynamics CRM Server
  - Dynamics AX Server
- Project Server
- Visual Studio Team Foundation Server
- BizTalk Server
- Forefront Identity Manager
- Forefront Unified Access Gateway
- Remote Desktop Services

**Note** The following products are not eligible for License Mobility through Software Assurance:
- Microsoft Server Windows operating system products
- Microsoft Windows client operating system products
- Desktop application products (for example, Microsoft Office)

### Select License Options from the VMC Console

You can enable Windows Server and SQL Server licenses from the VMC Console.

**Note** If you have purchased VMware Cloud on AWS services through a Managed Service Provider (MSP), your MSP must have signed a Software Services Reseller Addendum in order to enable these license options.

#### Procedure

2. Edit Microsoft Server Licenses.
   - If your SDDC has a single cluster, click **Edit Microsoft Server Licenses** at the bottom of the SDDC card.
   - If your SDDC has multiple clusters, click **Actions > Edit Microsoft Server Licenses** at the bottom of the
3. Select the licenses you want to purchase.
4. Select the checkboxes to confirm that you understand the license pricing and billing terms.
5. Click **Save**.

### Deploying Microsoft Server Instances

After you have properly licensed your SDDC clusters, you have the option to deploy your server instances from pre-packaged VMware VMs, from a VMware-managed content library, or by importing your own existing instances for deployment on VMware Cloud on AWS.

#### Deploy Microsoft Server Instances from Pre-packaged VMs

VMware provides a set of pre-packaged VMs that are ready to deploy.
VMware provides a curated Microsoft software repository with the following OVF packages for your use:

- Windows Server 2019 Datacenter
- Windows Server 2016 Datacenter
- Windows Server Datacenter (provides Microsoft Semi-Annual Channel Release)
- Windows Server 2019 Datacenter with SQL Server 2019 Enterprise

The following SQL Server features are pre-configured in the OVA:

- Database Engine services
- Client tools connectivity
- Client tools backwards compatibility

SQL Server services are configured as follows:

- SQL Service Agent: Automatic
- SQL Server Database Engine: Automatic
- SQL Server Browser: Manual

The following configuration was applied to the default SQL Server instance:

- "Grant perform Volume Management Tool" is enabled
- Min Server Memory: 0 MB
- Max Server Memory: 5940 MB
- Authentication mode: "Windows Authentication"
- SQL Server Administrator Role: "BUILTIN\Administrators (Administrators)"

**Note** If you need to add features to the installed instance, use the SQL Server ISO image provided in the same Content Library. See [Create a VM Using a Microsoft ISO](#) for more information on using the ISO images.

**Note** Windows Firewall is enabled in all VMware-provided OVAs.

The OVF packages have the following configuration:

- Hardware compatibility: ESXi 7.0 and later (Hardware Version 17).
- 4 CPUs
- 8 GB memory
- Network adapter: VMXNET3
- single 90GB VMDK attached to VMware Paravirtual vSCSI (PVSCSI) controller

**Note** Access to the VMware-curated Microsoft software repository should be used only for deploying Microsoft binaries for use on VMware Cloud on AWS.

**Procedure**

1. Subscribe to the VMware-curated Microsoft software repository by creating a subscribed Content Library using the following URL: [https://vmc-microsoft-templates.s3-us-west-2.amazonaws.com/Images/lib.json](https://vmc-microsoft-templates.s3-us-west-2.amazonaws.com/Images/lib.json)
   

2. Deploy the desired OVF into your environment.

   For more information on deploying OVFs from Content Libraries, see [https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.vm_admin.doc/GUID-3C02B3FC-5DE6-48AA-9AD3-7F0D1C7EC4B6.html](https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.vm_admin.doc/GUID-3C02B3FC-5DE6-48AA-9AD3-7F0D1C7EC4B6.html).

3. Make any necessary modifications to the VM, such as adding vCPUs, adding disks, or changing network settings.

   For more information on configuring VMs, see [https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.vm_admin.doc/GUID-4AB8C63C-61EA-4202-8158-D9903E04A0ED.html](https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.vm_admin.doc/GUID-4AB8C63C-61EA-4202-8158-D9903E04A0ED.html).

4. Configure the compute gateway firewall using the VMC Console to allow outbound HTTP and HTTPS access to the internet.


5. Power on the VM.

6. Configure a Windows Server password to secure the VM according to your corporate security policy.

7. (Optional) Convert the VM into a template for re-use.

   You might need to reactivate VMs cloned from the template.

**What to do next**

- Update your VM with the latest patches and security updates. Although VMware supplies current versions of Microsoft products, it is your responsibility to apply the latest maintenance updates and security patches to ensure that the products run in a secure environment. Follow your enterprise recommendations on updating any binaries that you import into your SDDC.
- Update firewall rules. The activation and patch update process requires that the VM have internet access. Follow your enterprise guidelines on whether these firewall rules should be modified after activation.

Create a VM Using a Microsoft ISO

VMware also provides access to ISO images that you can use to deploy Windows Server machines.

VMware provides a curated Microsoft software repository with the following ISOs for your use:

- Windows Server 2019 Datacenter
- Windows Server 2019 Language Pack
- Windows Server 2016 Datacenter
- Windows Server Datacenter (provides Microsoft Semi-Annual Channel Release)
- SQL Server 2019 Enterprise. Use this ISO if you need to add features to the SQL Server instance.

**Note** Access to the VMware-curated Microsoft software repository should be used only for deploying Microsoft binaries for use on VMware Cloud on AWS.

**Procedure**

1. **Subscribe to the VMware-curated Microsoft software repository by creating a subscribed Content Library using the following URL:** [https://vmc-microsoft-templates.s3-us-west-2.amazonaws.com/Images/lib.json](https://vmc-microsoft-templates.s3-us-west-2.amazonaws.com/Images/lib.json)


2. **Create the VM.**

   For more information on creating VMs, see [https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.vm_admin.doc/GUID-AE8AFBF1-75D1-4172-988C-378C35C9FAF2.html](https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.vm_admin.doc/GUID-AE8AFBF1-75D1-4172-988C-378C35C9FAF2.html).

3. **Install the guest operating system and any other software from the ISO images.**

   For more information on installing software from ISO images, see [https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.vm_admin.doc/GUID-55FC02D4-F5B3-4357-BB6B-78240B7F16BA.html](https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.vm_admin.doc/GUID-55FC02D4-F5B3-4357-BB6B-78240B7F16BA.html).

4. **Install VMware Tools on the VM.**
5 Copy the activation script to the VM.

An ISO image containing the activation script is located in the subscribed Content Library.

a In the vSphere Client, navigate to the subscribed Content Library and click Other Types.

b Attach the VM's CD/DVD drive to the Windows_Activation_Script ISO in the Content Library.

For more information on connecting a Content Library ISO file to a VM, see https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.vm_admin.doc/GUID-BE1C18D2-8FF0-4F41-AA35-A4BA71D62EB4.html.

c Copy the Activation.ps1 script file to the VM's local disk.

6 Make any necessary modifications to the VM, such as adding vCPUs, adding disks, or changing network settings.

For more information on configuring VMs, see https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.vm_admin.doc/GUID-4AB8C63C-61EA-4202-8158-D9903E04A0ED.html.

7 Configure the compute gateway firewall using the VMC Console to allow outbound HTTP and HTTPS access to the internet.


8 Power on the VM.

9 Run the activation script.

a In the guest operating system, open a command window and change to the directory where you copied the Activation.ps1 script.

b Type powershell Activation.ps1 and press Enter.

10 Configure a Windows Server password to secure the VM according to your corporate security policy.

What to do next

- Update your VM with the latest patches and security updates. Although VMware supplies current versions of Microsoft products, it is your responsibility to apply the latest maintenance updates and security patches to ensure that the products run in a secure environment. Follow your enterprise recommendations on updating any binaries that you import into your SDDC.

- Update firewall rules. The activation and patch update process requires that the VM have internet access. Follow your enterprise guidelines on whether these firewall rules should be modified after activation.
Import Your Windows Server VM into VMware Cloud on AWS

You can import an existing VM running Windows Server into VMware Cloud on AWS.

When you import virtual machines, you are responsible for ensuring that a license is available for the Microsoft workload either using BYOL or using VMware-supplied licenses.

Procedure

1. Import your Windows VM to VMware Cloud on AWS.
   
   You can use a variety of methods to do this including cold migration, migration with vMotion, migration with HCX, or cloning from a Content Library template you have created.

2. Do one of the following in order to maintain the activation status of the Windows Server instance.
   
   - Use the VMware-supplied activation script as described in Activate or Reactivate a Windows Server VM.
   - Maintain network connectivity to your enterprise's managed KMS server or another solution to update and maintain the activation status of your workloads.
   - Install and maintain a KMS in your VMware Cloud on AWS SDDC.

Activate or Reactivate a Windows Server VM

You can use a VMware-provided activation script to activate or reactivate a Windows Server VM that is licensed for your VMware Cloud on AWS SDDC with VMware-supplied licenses.

Operations that change the BIOS UUID or Disk ID of the Windows Server VM will result in the VM requiring activation. These operations include:

- Cloning a VM
- Converting a VM to a template

Procedure

1. Subscribe to the VMware-curated Microsoft software repository by creating a subscribed Content Library using the following URL: https://vmc-microsoft-templates.s3-us-west-2.amazonaws.com/images/lib.json

2 Copy the activation script to the VM.

An ISO image containing the activation script is located in the subscribed Content Library.

a In the vSphere Client, navigate to the subscribed Content Library and click Other Types.

b Attach the VM’s CD/DVD drive to the Windows Activation Script ISO in the Content Library.

For more information on connecting a Content Library ISO file to a VM, see https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.vm_admin.doc/GUID-BE1C18D2-8FF0-4F41-AA35-A4BA71D62EB4.html.

c Copy the Activation.ps1 script file to the VM's local disk.

3 Configure the compute gateway firewall using the VMC Console to allow outbound HTTP and HTTPS access to the internet.


4 Run the activation script.

a In the guest operating system, open a command window and change to the directory where you copied the Activation.ps1 script.

b Type powershell Activation.ps1 and press Enter.

What to do next

- Update your VM with the latest patches and security updates. Although VMware supplies current versions of Microsoft products, it is your responsibility to apply the latest maintenance updates and security patches to ensure that the products run in a secure environment. Follow your enterprise recommendations on updating any binaries that you import into your SDDC.

- Update firewall rules. The activation and patch update process requires that the VM have internet access. Follow your enterprise guidelines on whether these firewall rules should be modified after activation.

Converting Clusters from i3 to i3en Hosts

You have the option of converting an existing i3 host cluster to i3en hosts, to take advantage of the greater storage capacity and other benefits of i3en hosts.

Contact your VMware representative to schedule a cluster conversion. A conversion window is scheduled and you will have the opportunity to approve the conversion window.

Cluster conversion is currently available in SDDCs running SDDC 1.10 bundle versions.
You receive notifications when a cluster conversion is scheduled, about to start, and completed. To ensure that you receive these notifications, ensure that donotreply@vmware.com is added to your email allow list.

**Cluster Conversion Process**

3 days before the cluster conversion is scheduled, VMware will run pre-checks on the cluster to ensure that it is ready for conversion.

During the conversion, EDRS scale-in is turned off so that it does not interfere with the process. Two i3en hosts are added to the cluster. The NSX Edge VMs are migrated to these two new hosts. Then workload VMs are migrated off of one of the i3 hosts and it is removed from the cluster. The removal of i3 hosts and the addition of i3en hosts is repeated until all i3 hosts have been removed and the cluster is fully converted. Then EDRS scale-in is re-enabled. Based on cluster utilization, the number of i3en hosts might differ from the number of i3 hosts you started with.

The estimated number of i3en hosts in the target cluster is based on the following factors:

- The current used capacity in the starting VSAN cluster.
- The number of hosts present in the starting cluster.
- The space-savings efficiency ratio of the starting cluster.
- The available capacity in the capacity tier of storage for the target i3en instances.
- An extra 30% headroom for VSAN operations and overhead.
- The estimated fault domains required in the target cluster. Currently, the estimate does not take into account the VM storage policies and estimates the required fault domains based only on the cluster size. This means that for all clusters containing 7 hosts or fewer, the target cluster will contain the same number of hosts as the source cluster.

The estimate is a best guess only. The final result might differ based on the state of the cluster. After conversion, EDRS might scale in or scale out the cluster based on the resource usage and the EDRS policy applied to the cluster. You can also manually resize the cluster after conversion is complete.

Cluster conversion might take hours to days to complete. VMware recommends taking a backup before the cluster conversion takes place.

**Impact of Cluster Conversion on Operation**

There is no downtime to workload VMs or management appliances during the conversion process. You are unable to perform the following operations during cluster conversion:

- Removing hosts
- Editing EDRS policy settings
During cluster conversion, do not perform the following actions on the cluster which is being converted:

- Do not perform hot or cold workload migrations to or from the cluster being converted.
- Do not perform workload provisioning (New/Clone VM).
- Do not make changes to Storage-based Policy Management settings for workload VMs.
- Avoid starting HCX migrations that might overlap with the conversion window.
- Avoid the following DRaaS activity on the cluster being converted:
  - Create or destroy site pairings
  - Execute recovery plan
  - Planned migration
  - Test failover or test cleanup
  - Real failover
  - Reprotect
  - Replication management operations, such as configuring or stopping replication
- Do not add or remove hosts from the cluster being converted.

Compute policy tags are not copied over during cluster conversion. You will need to attach host policy tags after conversion is complete.

**Cluster Conversion and Billing**

During the cluster conversion process, your cluster contains a mixture of i3 and i3en hosts. Until the cluster conversion is complete, all hosts are billed at the i3 host rate. After the conversion is complete, billing switches to the i3en rate.

Converting the cluster from i3 to i3en hosts does not convert any term commitments that you have purchased. If you purchased an i3 term commitment, you can choose to purchase a new i3en term commitment or have your i3en hosts billed at the on-demand rate. In either case, you will continue to pay for your i3 term commitment.
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
- Using the vRealize Automation Cloud Add-On

**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)"

User-Driven Activity Events

log_type Contains Activity

VMC Notification Gateway Events

log_type Contains Notification

VMware Cloud Services Audit Events

log_type Contains csp-audit

Using the vRealize Automation Cloud Add-On

You can use the vRealize Automation Cloud add-on to activate the quick cloud automation setup for VMware Cloud on AWS to onboard and explore a populated VMware Cloud on AWS Cloud environment based on your source SDDC.

For information about how to use vRealize Automation with VMware Cloud on AWS, see Quick cloud automation setup for VMware Cloud on AWS in the VMware vRealize Automation Cloud Product Documentation.
## Getting Templates, ISOs, and Other Content into Your SDDC

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.

<table>
<thead>
<tr>
<th>Content Type</th>
<th>How to transfer it to your SDDC</th>
</tr>
</thead>
<tbody>
<tr>
<td>.vmtx template</td>
<td>- Use the Content Onboarding Assistant to transfer the template to your SDDC.</td>
</tr>
<tr>
<td></td>
<td>- Clone the templates to OVF template in an on-premises Content Library and subscribe to the Content Library from your SDDC.</td>
</tr>
<tr>
<td>OVF template</td>
<td>- Add the template to an on-premises Content Library and subscribe to the content library from your SDDC.</td>
</tr>
<tr>
<td></td>
<td>- Create a local Content Library in your SDDC, and upload the OVF template to it.</td>
</tr>
<tr>
<td></td>
<td>- 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.</td>
</tr>
<tr>
<td>OVA template</td>
<td>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.</td>
</tr>
<tr>
<td>ISO image</td>
<td>- Upload the ISO image to the workloadDatastore.</td>
</tr>
<tr>
<td></td>
<td>- Import the ISO image into an on-premises Content Library and subscribe to the Content Library from your SDDC.</td>
</tr>
<tr>
<td></td>
<td>- Create a local Content Library in your SDDC, and upload the ISO image to it.</td>
</tr>
<tr>
<td></td>
<td>- Use the Content Onboarding Assistant to transfer the ISO image to your SDDC.</td>
</tr>
<tr>
<td>scripts or text files</td>
<td>- Import the file into an on-premises Content Library and subscribe to the Content Library from your SDDC.</td>
</tr>
<tr>
<td></td>
<td>- Create a local Content Library in your SDDC and upload the file to it.</td>
</tr>
<tr>
<td></td>
<td>- Use the Content Onboarding Assistant to transfer the file to your SDDC.</td>
</tr>
</tbody>
</table>
This chapter includes the following topics:

- Use the Content Onboarding Assistant to Transfer Content to Your SDDC
- Use a Content Library to Import Content into Your SDDC
- Upload Files or Folders to your SDDC

**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](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.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>onpremServer server</td>
<td>The host name of the vCenter Server for your on-premises data center.</td>
</tr>
<tr>
<td>onpremInfraServer psc-server</td>
<td>The host name of the on-premises Platform Services Controller. This is optional for embedded configurations.</td>
</tr>
<tr>
<td>onpremUsername username</td>
<td>The user name used to log in to the on-premises vCenter Server.</td>
</tr>
<tr>
<td>location foldername</td>
<td>The location of files such as scripts or ISO images on the on-premises datastore. Use the format datastore-name:folder/.</td>
</tr>
<tr>
<td>cloudServer server</td>
<td>The host name of the cloud SDDC vCenter Server.</td>
</tr>
<tr>
<td>cloudInfraServer infra-server</td>
<td>The host name of the cloud SDDC vCenter Server. This is optional.</td>
</tr>
<tr>
<td>cloudFolderName foldername</td>
<td>The name of the vCenter Server folder on the cloud SDDC where .vmtx templates will be stored.</td>
</tr>
<tr>
<td>cloudRpName resource-pool-name</td>
<td>The resource pool on the cloud SDDC for the .vmtx templates.</td>
</tr>
<tr>
<td>cloudNetworkName network-name</td>
<td>The distributed virtual port group on the cloud SDDC for the .vmtx templates.</td>
</tr>
<tr>
<td>sessionUpdate value</td>
<td>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.</td>
</tr>
</tbody>
</table>
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.

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.

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

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.

Results

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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>To create a new folder</td>
<td>a  Select the WorkloadDatastore or an existing folder.</td>
</tr>
<tr>
<td></td>
<td>b  Select New Folder.</td>
</tr>
<tr>
<td>To upload a file</td>
<td>a  Select a folder.</td>
</tr>
<tr>
<td></td>
<td>b  Click Upload Files.</td>
</tr>
<tr>
<td></td>
<td>c  Select a file and click OK.</td>
</tr>
<tr>
<td>To upload a folder</td>
<td>a  Select a folder.</td>
</tr>
<tr>
<td></td>
<td>b  Select Upload Folder.</td>
</tr>
<tr>
<td></td>
<td>c  Select a folder and click OK.</td>
</tr>
</tbody>
</table>
Migrating Virtual Machines

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.

It’s important to note that any constraints that apply to on-premises migrations are likely to apply to hybrid migrations as well. For example, issues described in Enable Virtual CPU Performance Counters can prevent migration of VMs that enable performance counters when the source or destination cluster enables Enhanced vMotion Compatibility.

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](https://vmc.vmware.com/solutions) and the VMware Cloud Migration solution at [https://vmc.vmware.com/solutions](https://vmc.vmware.com/solutions).

**Hybrid Migration with VMware HCX Checklist**

Follow this checklist to be sure your on-premises and SDDC configurations are appropriate for hybrid migration using VMware HCX.

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Networking speed</td>
<td>Migration with vMotion using HCX requires a minimum of 100 Mbps throughput between source and destination.</td>
</tr>
<tr>
<td>On-premises vSphere version</td>
<td></td>
</tr>
</tbody>
</table>
- For vMotion: vSphere 6.0, 6.5, 6.7, 7.0  
- For bulk migration: vSphere 6.0, 6.5, 6.7, 7.0  
- For cold migration: vSphere 6.0, 6.5, 6.7, 7.0 |
| On-premises virtual switch configuration | vSphere Distributed Switch  
NSX-T Distributed Virtual Switch (N-VDS)  
vSphere standard switch |
<p>| Installation of VMware HCX Manager in the on-premises data center | See the <a href="https://vmc.vmware.com/solutions">VMware HCX Product Documentation</a>. HCX Connector Environment Requirements are described in <a href="https://vmc.vmware.com/solutions">Software Version Requirements for the HCX Installations</a> in the VMware HCX Product Documentation. |
| Establish the HCX Interconnect with your SDDC | Pair the VMware HCX Manager with your VMware Cloud on AWS SDDC as a remote site as described in Configuring and Managing the HCX Interconnect and Configuring and Managing the HCX Interconnect with the Multi-Site Service Mesh. |
| 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. |
| VMware Cloud on AWS firewall rules | Create firewall rules to open the ports used by HCX as described in Network Port and Protocol Requirements. |</p>
<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>On-premises firewall rules</td>
<td>Create firewall rules to open the ports used by HCX as described in <a href="#">Network Port and Protocol Requirements</a>.</td>
</tr>
</tbody>
</table>
| Virtual machine hardware and settings           | Ensure that these requirements are met for virtual machine hardware.  
  - Virtual machine hardware version and virtual disk size as specified in [VMware Configuration Maximums](#).  
  - 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 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 Table 5-1, **vMotion Compatibility Effects of Spectre patch**. To find the correct patch for your on-premises hosts, see [https://kb.vmware.com/s/article/52245](https://kb.vmware.com/s/article/52245). All hosts in VMware Cloud on AWS SDDCs have been patched.

<table>
<thead>
<tr>
<th>On-premises Host Processor Family and Patch Status</th>
<th>Virtual Machine Hardware Version</th>
<th>Has the VM been power-cycled in VMware Cloud on AWS SDDC?</th>
<th>vMotion from On-premises to VMware Cloud on AWS</th>
<th>vMotion from VMware Cloud on AWS to On-premises</th>
</tr>
</thead>
<tbody>
<tr>
<td>Broadwell (SPECTRE patched)</td>
<td>&lt; 9</td>
<td>No</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Yes</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td>9-13</td>
<td>No</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Yes</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Broadwell (Not SPECTRE patched)</td>
<td>&lt; 9</td>
<td>No</td>
<td>Supported</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Yes</td>
<td>Supported</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>9-13</td>
<td>No</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Yes</td>
<td>Supported</td>
<td>Not supported</td>
</tr>
<tr>
<td>Non-Broadwell</td>
<td>&lt; 9</td>
<td>No</td>
<td>Not supported</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Yes</td>
<td>Not supported</td>
<td>Not supported</td>
</tr>
<tr>
<td></td>
<td>9-13</td>
<td>No</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Yes</td>
<td>Supported</td>
<td>Not supported</td>
</tr>
</tbody>
</table>

**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](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 VMware HCX Checklist**.
<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Networking speed and latency</td>
<td>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.</td>
</tr>
</tbody>
</table>
| 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)

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>On-premises firewall rules</td>
<td>Ensure that you have created the necessary firewall rules as described in Required Firewall Rules for vMotion.</td>
</tr>
<tr>
<td>Virtual machine hardware and settings</td>
<td>Ensure that these requirements are met for virtual machine hardware.</td>
</tr>
<tr>
<td></td>
<td>- Virtual machine hardware version 9 or later is required for migration with vMotion from the on-premises data center to the cloud SDDC.</td>
</tr>
<tr>
<td></td>
<td>- EVC is not supported in the VMware Cloud on AWS SDDC.</td>
</tr>
<tr>
<td></td>
<td>- 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.</td>
</tr>
<tr>
<td></td>
<td>- Migration of VMs with DRS or HA VM overrides is not supported. For more information on VM overrides, see Customize an Individual Virtual Machine.</td>
</tr>
</tbody>
</table>

**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.

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

<table>
<thead>
<tr>
<th>Use Cases</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESXi NFC traffic</td>
<td>remote (on-premises)</td>
<td>ESXi</td>
<td>Provisioning (TCP 902)</td>
</tr>
<tr>
<td></td>
<td>ESXi VMkernel networks used</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>for NFC.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Allow outbound ESXi</td>
<td>ESXi</td>
<td>remote (on-premises)</td>
<td>Any (All Traffic)</td>
</tr>
<tr>
<td>access to on-premises</td>
<td></td>
<td>ESXi</td>
<td></td>
</tr>
<tr>
<td>vMotion traffic.</td>
<td>remote (on-premises)</td>
<td>ESXi</td>
<td>vMotion (TCP 8000)</td>
</tr>
<tr>
<td></td>
<td>ESXi vMotion VMkernel</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>networks</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

On-Premises Firewall Rules for vMotion

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

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

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

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

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

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

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.

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>On-premises vSphere version</td>
<td>vSphere 6.5 patch d and later</td>
</tr>
<tr>
<td></td>
<td>vSphere 6.0 update 3 and later</td>
</tr>
<tr>
<td>On-premises virtual switch configuration</td>
<td>Standard switches, vSphere Distributed Switch 6.0, or vSphere Distributed Switch 6.5</td>
</tr>
</tbody>
</table>
### Requirement Description

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IPsec VPN</strong></td>
<td>Configure an IPsec VPN for the management gateway. See &quot;Configuring VPNs and Gateways&quot; in <em>Getting Started With VMware Cloud on AWS</em>.</td>
</tr>
<tr>
<td><strong>Hybrid Linked Mode</strong></td>
<td>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 &quot;Hybrid Linked Mode&quot; in <em>Managing the VMware Cloud on AWS Data Center</em>.</td>
</tr>
<tr>
<td><strong>VMware Cloud on AWS and on-premises firewall rules</strong></td>
<td>Ensure that you have created the necessary firewall rules as described in <em>Required Firewall Rules for Cold Migration</em>.</td>
</tr>
<tr>
<td><strong>On-premises DNS configuration</strong></td>
<td>Ensure that your on-premises DNS server can correctly resolve the address for the cloud vCenter Server.</td>
</tr>
</tbody>
</table>

### 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*.

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

#### On-Premises Firewall Rules for Cold Migration

Ensure that the following rules are configured in your on-premises firewall.
<table>
<thead>
<tr>
<th>Rule</th>
<th>Action</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>On-premises to vCenter Server</td>
<td>Allow</td>
<td>remote (on-premises) vSphere Client subnet</td>
<td>VMware Cloud on AWS vCenter Server IP address</td>
<td>HTTPS</td>
<td>443</td>
</tr>
<tr>
<td>Remote to ESXi provisioning</td>
<td>Allow</td>
<td>remote (on-premises) subnet</td>
<td>SDDC management subnet</td>
<td>TCP</td>
<td>902</td>
</tr>
<tr>
<td>Cloud SDDC to on-premises vCenter Server</td>
<td>Allow</td>
<td>CIDR block for cloud SDDC management network</td>
<td>On-premises vCenter Server</td>
<td>HTTPS</td>
<td>443</td>
</tr>
<tr>
<td>Cloud SDDC to ESXi Remote Console</td>
<td>Allow</td>
<td>CIDR block for cloud SDDC management network</td>
<td>VMware Cloud on AWS vCenter Server IP address</td>
<td>TCP</td>
<td>902</td>
</tr>
<tr>
<td>Cloud SDDC to Remote LDAP (Required for HLM only)</td>
<td>Allow</td>
<td>CIDR block for cloud SDDC management network</td>
<td>Remote LDAP Server</td>
<td>TCP</td>
<td>389, 636</td>
</tr>
</tbody>
</table>
Accessing AWS Services

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
- Access an S3 Bucket Using an S3 Endpoint
- Access an S3 Bucket Using the Internet Gateway
- Use AWS CloudFormation to Create an SDDC

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 be configured to allow the intended traffic or the connection can't 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.
VMware Knowledge Base article 76577 has additional information that applies to cases where the default AWS Security Group has a missing or altered allow-all rule for outbound traffic.

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.
   - Select the instance that you deployed in Step 1.
   - In the instance description, click the instance’s Security Group and click the Inbound tab.
   - Click Edit.
   - Click Add Rule.
In the **Type** dropdown menu, select the type of traffic that you want to allow.

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.

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

Click **Save**.

**(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.

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

Click **Edit**.

Click **Add Rule**.

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

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.

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

Click **Save**.

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 \texttt{com.amazonaws.region-AZ.s3} service of type Gateway where region-AZ matches the region and AZ your SDDC is in. For example, \texttt{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 \texttt{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 HTTPS.

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.

   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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>The CIDR block for the logical network that the VM in your SDDC is connected to.</td>
</tr>
<tr>
<td>Destination</td>
<td>Select S3 Prefixes.</td>
</tr>
<tr>
<td>Service</td>
<td>Select HTTPS.</td>
</tr>
<tr>
<td>Applied to</td>
<td>Clear All Uplinks and select VPC Interface.</td>
</tr>
</tbody>
</table>

Results

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.

   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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>The CIDR block for the logical network that the VM in your SDDC is connected to.</td>
</tr>
<tr>
<td>Destination</td>
<td>Any</td>
</tr>
<tr>
<td>Service</td>
<td>Select HTTPS.</td>
</tr>
</tbody>
</table>

**Results**

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](https://github.com/vmwaresamples/vmware-cloud-on-aws-integration-examples/blob/master/CloudFormation/README.md) on the VMware blog.

**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](https://github.com/vmwaresamples/vmware-cloud-on-aws-integration-examples/blob/master/CloudFormation/README.md) 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>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>connected_account_id</td>
<td>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.</td>
</tr>
<tr>
<td>customer_subnet_ids</td>
<td>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.</td>
</tr>
<tr>
<td>email</td>
<td>currently unimplemented</td>
</tr>
<tr>
<td>vpc_cidr</td>
<td>Subnet CIDR block for management traffic. Default is 10.2.0.0/16</td>
</tr>
<tr>
<td>name</td>
<td>The name of the SDDC to be created</td>
</tr>
<tr>
<td>numOfHosts</td>
<td>The number of hosts initially added to the SDDC</td>
</tr>
<tr>
<td>orgId</td>
<td>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</td>
</tr>
<tr>
<td>region</td>
<td>Must be US_WEST_2</td>
</tr>
<tr>
<td>user_refresh_token</td>
<td>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.</td>
</tr>
</tbody>
</table>

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.

Results

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.

```json
{
    "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"
        ],
        "Resource": [
            "*"
        ]
    }
}
```

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeRouteTables",
                "ec2:CreateRoute",
                "ec2:DeleteRoute",
                "ec2:ReplaceRoute"
            ],
            "Resource": ["*"
        ]
    }
}
```
"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

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

See the VMware Product Interoperability Matrices for the list of vRealize Automation versions that you can use with VMware Cloud on AWS.

This chapter includes the following topics:

- Prepare Your SDDC to Work with vRealize Products
- Connect vRealize Automation 8.x to Your SDDC

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 7-1. Management Gateway Firewall Rules Required by vRealize Automation

<table>
<thead>
<tr>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCenter</td>
<td>CIDR block of on-premises data center</td>
<td>vCenter</td>
<td>Any (All Traffic)</td>
</tr>
<tr>
<td>vCenter Ping</td>
<td>Any</td>
<td>vCenter</td>
<td>ICMP (All ICMP)</td>
</tr>
</tbody>
</table>
Table 7-1. Management Gateway Firewall Rules Required by vRealize Automation (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>On Premises to ESXi Ping</td>
<td>CIDR block of on-premises data center</td>
<td>ESXi Management Only</td>
<td>ICMP (All ICMP)</td>
</tr>
<tr>
<td>On Premises to ESXi Remote Console and Provisioning</td>
<td>CIDR block of on-premises data center</td>
<td>ESXi Management Only</td>
<td>TCP 902</td>
</tr>
<tr>
<td>On-Premises to SDDC VM</td>
<td>CIDR block of on-premises data center</td>
<td>CIDR block of SDDC logical network</td>
<td>Any (All Traffic)</td>
</tr>
<tr>
<td>SDDC VM to On-Premises</td>
<td>CIDR block of SDDC logical network</td>
<td>CIDR block of on-premises data center</td>
<td>Any (All Traffic)</td>
</tr>
</tbody>
</table>

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

Connect vRealize Automation 8.x to Your SDDC

When you connect your on-premises installation of vRealize Automation 8.x to your VMware Cloud on AWS SDDC, you use vRealize Automation Cloud Assembly to deploy VMs, applications, and services as SDDC workloads.

**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**

- If you are using vRealize Automation 8.x, follow the example workflows in Create a VMware Cloud on AWS cloud account in vRealize Automation Cloud Assembly within a sample workflow to configure your on-premises installation of vRealize Automation 8.x to work with VMware Cloud on AWS.

  If you are using an earlier version of vRealize Automation, see Connect vRealize Automation 7.x to Your SDDC.

Connect vRealize Automation 7.x to Your SDDC

You can connect your on-premises installation of vRealize Automation 7.x to your cloud SDDC to create blueprints allowing users to deploy VMs.

**Prerequisites**

- See the VMware Product Interoperability Matrices for the list of vRealize Automation 7.x releases that you can use with VMware Cloud on AWS.
- 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)**.
4. Specify the cloud admin credentials.
5. 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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource Pool</td>
<td>Compute-ResourcePool</td>
</tr>
<tr>
<td>Datastore</td>
<td>WorkloadDatastore</td>
</tr>
<tr>
<td>VM &amp; Template Folder</td>
<td>Workloads</td>
</tr>
<tr>
<td>Network</td>
<td>Use the logical network that you created as part of the prerequisites</td>
</tr>
</tbody>
</table>

**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](#).
Service Notifications and Activity Log

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

The notification gateway provides a central integration point for all customer-facing notifications from VMware Cloud on AWS. The notification gateway is designed to keep you up-to-date on Day 2 operations events and service updates, including maintenance notifications, Elastic DRS Add Host events, subscription expiration reminders, and VMware Site Recovery notifications. You can find a list of all notifications in Notifications Available from VMware Cloud on AWS.

The notification channels that are available include email, VMC Console, vSphere Client, the Activity Log UI, and VMware Log Insight Cloud.

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, add donotreply@vmware.com to your email allow list.

This chapter includes the following topics:

- View the Activity Log
- View and Subscribe to the Service Status Page
- Notifications Available from VMware Cloud on AWS

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

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](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.

---

### Notifications Available from VMware Cloud on AWS

The following lists provide all the notification events and activity events currently available from the VMware Cloud on AWS Activity Log and vRealize Log Insight Cloud.

For more information on identifying the notification and activity events in vRealize Log Insight Cloud, see [Using the vRealize Log Insight Cloud Add-On](#).

#### Table 8-1. Notifications Available from Notifications Gateway

<table>
<thead>
<tr>
<th>Display Name</th>
<th>Template ID</th>
<th>Description</th>
<th>Email Channel</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maintenance Related Notifications</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maintenance Change Window Complete</td>
<td>MaintenanceChangeWindowComplete</td>
<td>vCenter Server upgrade is complete. (Used only in version 1.8 and earlier.)</td>
<td>Yes</td>
</tr>
<tr>
<td>Maintenance Change Canceled</td>
<td>MaintenanceChangeCanceled</td>
<td>A scheduled upgrade of an SDDC has been canceled.</td>
<td>Yes</td>
</tr>
<tr>
<td>Host Patching Complete</td>
<td>HostPatchingComplete</td>
<td>SDDC Upgrade has completed. (Used only in version 1.8 and earlier.)</td>
<td>Yes</td>
</tr>
<tr>
<td>DFC Deduplication Scheduled</td>
<td>DFC-DedupeScheduled</td>
<td>A DFC change to an SDDC has been scheduled.</td>
<td>Yes</td>
</tr>
<tr>
<td>DFC Deduplication Start</td>
<td>DFC-DedupeStart</td>
<td>A DFC change to an SDDC has begun.</td>
<td>Yes</td>
</tr>
<tr>
<td>DFC Deduplication Complete</td>
<td>DFC-DedupeComplete</td>
<td>A DFC change to an SDDC has completed.</td>
<td>Yes</td>
</tr>
<tr>
<td>DFC Deduplication Canceled</td>
<td>DFC-DedupeCanceled</td>
<td>A DFC change to an SDDC has been canceled.</td>
<td>Yes</td>
</tr>
<tr>
<td>Display Name</td>
<td>Template ID</td>
<td>Description</td>
<td>Email Channel</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>Initial Rollout Scheduled</td>
<td>NSX-T-InitialRolloutScheduling</td>
<td>An upgrade of an SDDC has been scheduled. (Used only in version 1.8 and earlier when using NSX-T.)</td>
<td>Yes</td>
</tr>
<tr>
<td>Control Plane Window Started</td>
<td>NSX-T-ControlPlaneWindowStarted</td>
<td>vCenter Server upgrade has begun. (Used only in version 1.8 and earlier.)</td>
<td>Yes</td>
</tr>
<tr>
<td>Host Networking Started</td>
<td>NSX-T-HostNetworkingStarted</td>
<td>NSX-T upgrade has begun. (Used only in version 1.8 and earlier.)</td>
<td>Yes</td>
</tr>
<tr>
<td>Host Networking Complete</td>
<td>NSX-T-HostNetworkingComplete</td>
<td>NSX-T upgrade has completed. (Used only in version 1.8 and earlier.)</td>
<td>Yes</td>
</tr>
<tr>
<td>Reschedule Notification</td>
<td>NSX-T-RescheduleNotification</td>
<td>A scheduled upgrade of an SDDC has been rescheduled. (Used only in version 1.8 and prior when using NSX-T.)</td>
<td>Yes</td>
</tr>
<tr>
<td>V2-RolloutScheduled</td>
<td>V2-RolloutScheduled</td>
<td>An upgrade of an SDDC has been scheduled. (Used in version 1.9 and later.)</td>
<td>Yes</td>
</tr>
<tr>
<td>V2-RolloutRescheduled</td>
<td>V2-RolloutRescheduled</td>
<td>An upgrade of an SDDC has been rescheduled (Used in version 1.9 and later.)</td>
<td>Yes</td>
</tr>
<tr>
<td>V2-RolloutCancelled</td>
<td>V2-RolloutCancelled</td>
<td>An upgrade of an SDDC has been canceled (Used in version 1.9 and later.)</td>
<td>Yes</td>
</tr>
<tr>
<td>V2-Phase1Started</td>
<td>V2-Phase1Started</td>
<td>Upgrade of the SDDC Control Plane has begun. (Used in version 1.9 and later.)</td>
<td>Yes</td>
</tr>
<tr>
<td>V2-Phase1Completed</td>
<td>V2-Phase1Completed</td>
<td>Upgrade of the SDDC Control Plane has completed. (Used in version 1.9 and later.)</td>
<td>Yes</td>
</tr>
<tr>
<td>V2-Phase2Started</td>
<td>V2-Phase2Started</td>
<td>Upgrade of the ESXi hosts in an SDDC has begun. (Used in version 1.9 and later.)</td>
<td>Yes</td>
</tr>
<tr>
<td>V2-Phase2Completed</td>
<td>V2-Phase2Completed</td>
<td>Upgrade of the ESXi hosts in an SDDC has completed. (Used in version 1.9 and later.)</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Table 8-1. Notifications Available from Notifications Gateway (continued)

<table>
<thead>
<tr>
<th>Display Name</th>
<th>Template ID</th>
<th>Description</th>
<th>Email Channel</th>
</tr>
</thead>
<tbody>
<tr>
<td>V2-Phase3Started</td>
<td>V2-Phase3Started</td>
<td>Upgrade of NSX Manager has begun. (Used in version 1.9 and later.)</td>
<td>Yes</td>
</tr>
<tr>
<td>V2-Phase3Completed</td>
<td>V2-Phase3Completed</td>
<td>Upgrade of NSX Manager has completed. (Used in version 1.9 and later.)</td>
<td>Yes</td>
</tr>
<tr>
<td>V2-MaintenanceDelayed</td>
<td>V2-MaintenanceDelayed</td>
<td>Upgrade of an SDDC has been delayed. (Used in version 1.9 and later.)</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>SDDC Upgrade Notifications</strong></td>
<td></td>
</tr>
<tr>
<td>Add temporary ESX hosts</td>
<td>VRTAddHostCompleted</td>
<td>Successfully added temporary host to each cluster.</td>
<td>No</td>
</tr>
<tr>
<td>Backup of management VMs</td>
<td>VRTBackupCompleted</td>
<td>Successfully completed backup of management VMs.</td>
<td>No</td>
</tr>
<tr>
<td>Control plane upgrade</td>
<td>VRTControlPlaneUpgradeCompleted</td>
<td>Control plane upgrade completed successfully.</td>
<td>No</td>
</tr>
<tr>
<td>Data plane health check</td>
<td>VRTDataPlaneHealthCompleted</td>
<td>Data plane health check completed successfully.</td>
<td>No</td>
</tr>
<tr>
<td>Data plane upgrade</td>
<td>VRTDataPlaneUpgradeCompleted</td>
<td>Data plane upgrade completed successfully.</td>
<td>No</td>
</tr>
<tr>
<td>SDDC upgrade health check</td>
<td>VRTHealthCheckCompleted</td>
<td>SDDC upgrade health check completed successfully.</td>
<td>No</td>
</tr>
<tr>
<td>Host network upgrade</td>
<td>VRTNetworkingUpgradeCompleted</td>
<td>Network upgrade of hosts in all clusters completed successfully.</td>
<td>No</td>
</tr>
<tr>
<td>NSX controller upgrade</td>
<td>VRTNSXControllersUpgradeCompleted</td>
<td>Upgrade of NSX Controllers completed successfully.</td>
<td>No</td>
</tr>
<tr>
<td>NSX edge upgrade</td>
<td>VRTNSXEdgesUpgradeCompleted</td>
<td>Upgrade of NSX Edges completed successfully.</td>
<td>No</td>
</tr>
<tr>
<td>NSX manager upgrade</td>
<td>VRTNSXManagerUpgradeCompleted</td>
<td>Upgrade of NSX Manager completed successfully.</td>
<td>No</td>
</tr>
<tr>
<td>POP upgrade</td>
<td>VRTPopUpgradeCompleted</td>
<td>POP upgrade completed successfully.</td>
<td>No</td>
</tr>
<tr>
<td>Remove temporary ESX hosts</td>
<td>VRTRemoveHostCompleted</td>
<td>Successfully removed the temporary host from clusters.</td>
<td>No</td>
</tr>
<tr>
<td>Stage upgrade bundles</td>
<td>VRTStagingCompleted</td>
<td>Successfully staged the upgrade bundles.</td>
<td>No</td>
</tr>
<tr>
<td>UC Upgrade</td>
<td>VRTUCUpgradeCompleted</td>
<td>Successfully upgraded the NSX Upgrade Co-ordinator.</td>
<td>No</td>
</tr>
<tr>
<td>Display Name</td>
<td>Template ID</td>
<td>Description</td>
<td>Email Channel</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>----------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>Upgrade Issue</td>
<td>VRTUpgradeFailed</td>
<td>Issue encountered during upgrade. VMware is working to resolve the issue</td>
<td>No</td>
</tr>
<tr>
<td>SDDC upgrade maintenance</td>
<td>VRTUpgradeMaintenanceCompleted</td>
<td>SDDC is out of maintenance.</td>
<td>No</td>
</tr>
<tr>
<td>vCenter upgrade</td>
<td>VRTvCenterUpgradeCompleted</td>
<td>vCenter upgrade completed successfully.</td>
<td>No</td>
</tr>
<tr>
<td>vCenter upgrade started</td>
<td>VRTvCenterUpgradeStarted</td>
<td>vCenter upgrade started.</td>
<td>No</td>
</tr>
<tr>
<td>NSX Edge downtime</td>
<td>VRTNSXEdgeUpgradeDowntime</td>
<td>Change of active Edge due to upgrade at {timestamp}.</td>
<td>No</td>
</tr>
<tr>
<td>NSX Edge upgrade downtime</td>
<td>VRTNSXEdgeDowntime</td>
<td>Active Edge was migrated to a different host at {timestamp}.</td>
<td>No</td>
</tr>
<tr>
<td>NSX Edge upgrade</td>
<td>VRTNSXEdgesUpgradeCompleted</td>
<td>Upgrade of NSX Edges completed successfully.</td>
<td>No</td>
</tr>
<tr>
<td>Upgrade of all hosts in a cluster</td>
<td>VRTClusterUpgradeCompleted</td>
<td>Upgrade of all hosts in {cluster_name} completed successfully.</td>
<td>No</td>
</tr>
<tr>
<td>Upgrade of hosts</td>
<td>VRTClusterUpgradeProgress</td>
<td>Upgrade of hosts in {completed}/{total} clusters completed successfully.</td>
<td>No</td>
</tr>
<tr>
<td>Network upgrade of host</td>
<td>VRTClusterNetworkingUpgradeProgress</td>
<td>Network upgrade of all hosts in {cluster_name} completed successfully.</td>
<td>No</td>
</tr>
<tr>
<td>Network upgrade of cluster</td>
<td>VRTClusterNetworkingUpgradeCompleted</td>
<td>Network upgrade of hosts in {completed}/{total} clusters completed successfully.</td>
<td>No</td>
</tr>
<tr>
<td>Autoscaler/EDRS notifications</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>eDRS: Host Add (Storage)</td>
<td>StorageScaleOut</td>
<td>eDRS successfully added a host after storage capacity reached 70% or 75%.</td>
<td>Yes</td>
</tr>
<tr>
<td>One Node Planned Maintenance</td>
<td>OneNodePlannedMaintenance</td>
<td>One node SDDC planned maintenance will result in the SDDC being deleted. Add hosts to avoid losing the SDDC.</td>
<td>Yes</td>
</tr>
<tr>
<td>eDRS: Host Add (CPU)</td>
<td>CpuScaleOut</td>
<td>eDRS successfully added a host after CPU utilization reached 90%.</td>
<td>Yes</td>
</tr>
<tr>
<td>Display Name</td>
<td>Template ID</td>
<td>Description</td>
<td>Email Channel</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>eDRS: Host Add (Memory)</td>
<td>MemoryScaleOut</td>
<td>eDRS successfully added a host after memory utilization reached 80%.</td>
<td>Yes</td>
</tr>
<tr>
<td>eDRS: Host Maximum Reached</td>
<td>EdrsReachedMaximumHostLimit</td>
<td>eDRS reached maximum host limit.</td>
<td>Yes</td>
</tr>
<tr>
<td>eDRS: Host Maximum Exceeded</td>
<td>EdrsExceededMaximumHostLimit</td>
<td>eDRS exceeded maximum host limit.</td>
<td>Yes</td>
</tr>
<tr>
<td>Host Issue Detected</td>
<td>HostIssueDetected</td>
<td>Autoscaler has detected an issue with an ESXi host.</td>
<td>No</td>
</tr>
<tr>
<td>Host Successfully Replaced</td>
<td>ReplaceHostSuccessful</td>
<td>An ESXi host that was experiencing an issue was replaced.</td>
<td>No</td>
</tr>
<tr>
<td>Host Successfully Remediated</td>
<td>RemEDIATEHostSUCCESSFUL</td>
<td>An ESXi host that was experiencing an issue was remediated.</td>
<td>No</td>
</tr>
<tr>
<td>Planned Maintenance: Started</td>
<td>PlannedMaintenanceStarted</td>
<td>Planned maintenance activity has started.</td>
<td>No</td>
</tr>
<tr>
<td>General Org Notifications</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Expiring subscription in 30 days</td>
<td>expiringSubscription30Days</td>
<td>Reminder to take action for the expiring subscription.</td>
<td>Yes</td>
</tr>
<tr>
<td>Expiring subscription in 60 days</td>
<td>expiringSubscription60Days</td>
<td>Reminder to take action for the expiring subscription.</td>
<td>Yes</td>
</tr>
<tr>
<td>Reminder for expiring subscription today</td>
<td>expiringSubscriptionToday</td>
<td>Reminder to take action for the expiring subscription.</td>
<td>No</td>
</tr>
<tr>
<td>Reminder for AWS account linking on day 4</td>
<td>starshot-awsAccountLinkingDay4</td>
<td>Reminder for Single Host SDDC user to complete account linking.</td>
<td>Yes</td>
</tr>
<tr>
<td>Reminder for AWS account linking on day 13</td>
<td>starshot-awsAccountLinkingDay13</td>
<td>Reminder for Single Host SDDC user to complete account linking.</td>
<td>Yes</td>
</tr>
<tr>
<td>Reminder for AWS account linking on day 28</td>
<td>starshot-awsAccountLinkingDay28</td>
<td>Reminder for Single Host SDDC user to complete account linking.</td>
<td>Yes</td>
</tr>
<tr>
<td>Expiring Single Host Today</td>
<td>ExpiringSingleHost_0Day</td>
<td>Reminder that a Single Host SDDC is expiring and will be removed from the environment today.</td>
<td>Yes</td>
</tr>
<tr>
<td>Expiring Single Host in 2 Days</td>
<td>ExpiringSingleHost_2Days</td>
<td>Reminder that a Single Host SDDC is expiring and will be removed from the environment in 2 days.</td>
<td>Yes</td>
</tr>
<tr>
<td>Display Name</td>
<td>Template ID</td>
<td>Description</td>
<td>Email Channel</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>--------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>Expiring Single Host in 7 Days</td>
<td>ExpiringSingleHost_7Days</td>
<td>Reminder that a Single Host SDDC is expiring and will be removed from the environment in 7 days.</td>
<td>Yes</td>
</tr>
<tr>
<td>Expiring SPP Fund in 7 Days</td>
<td>ExpiringSPPfund_7Days_with_other_funds</td>
<td>Reminder that an SPP fund is expiring and you may lose the remaining credits in 7 days.</td>
<td>Yes</td>
</tr>
<tr>
<td>Expiring SPP Fund in 7 Days</td>
<td>ExpiringSPPfund_7Days_without_other_funds</td>
<td>Reminder that an SPP fund is expiring and you may lose the remaining credits in 7 days.</td>
<td>Yes</td>
</tr>
<tr>
<td>Expiring SPP Fund in 30 Days</td>
<td>ExpiringSPPfund_30Days_with_other_funds</td>
<td>Reminder that an SPP fund is expiring and you may lose the remaining credits in 30 days.</td>
<td>Yes</td>
</tr>
<tr>
<td>Expiring SPP Fund in 30 Days</td>
<td>ExpiringSPPfund_30Days_without_other_funds</td>
<td>Reminder that an SPP fund is expiring and you may lose the remaining credits in 30 days.</td>
<td>Yes</td>
</tr>
<tr>
<td>Expiring SPP Fund in 60 Days</td>
<td>ExpiringSPPfund_60Days_with_other_funds</td>
<td>Reminder that an SPP fund is expiring and you may lose the remaining credits in 60 days.</td>
<td>Yes</td>
</tr>
<tr>
<td>Expiring SPP Fund in 60 Days</td>
<td>ExpiringSPPfund_60Days_without_other_funds</td>
<td>Reminder that an SPP fund is expiring and you may lose the remaining credits in 60 days.</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**VMware Site Recovery Notifications**

<table>
<thead>
<tr>
<th>Display Name</th>
<th>Template ID</th>
<th>Description</th>
<th>Email Channel</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site Recovery - SSL certificates replacement started</td>
<td>Draas-SSLCertificateRenew-started</td>
<td>VMware Site Recovery has started replacement of SSL certificates of SRM and VR appliances in the SDDC.</td>
<td>Yes</td>
</tr>
<tr>
<td>Site Recovery - SSL certificates replacement started</td>
<td>Draas-SSLCertificateRenew-started-vmc-only</td>
<td>VMware Site Recovery has started replacement of SSL certificates of SRM and VR appliances in the SDDC.</td>
<td>Yes</td>
</tr>
<tr>
<td>Site Recovery - SSL certificates replacement completed</td>
<td>Draas-SSLCertificateRenew-completed</td>
<td>VMware Site Recovery has completed replacement of SSL certificates of SRM and VR appliances. Customer action is required on the remote (on-premises) DR site to recover the normal state of the VR pairing.</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Table 8-1. Notifications Available from Notifications Gateway (continued)

<table>
<thead>
<tr>
<th>Display Name</th>
<th>Template ID</th>
<th>Description</th>
<th>Email Channel</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site Recovery - SSL certificates replacement</td>
<td>Draas-SSLCertificateRenew-completed-vmc-only</td>
<td>VMware Site Recovery has completed replacement of SSL certificates of SRM and VR appliances. Customer action is required on the remote (on-premises) DR site to recover the normal state of the VR pairing.</td>
<td>Yes</td>
</tr>
<tr>
<td>Site Recovery - Scheduled SSL certificates replacement</td>
<td>Draas-SSLCertificateRenew canceled</td>
<td>This is a heads up notification for VSR maintenance activity - replacement of SRM and VR appliances SSL certificates. It is sent at least 7 days before the start of the maintenance. Usually such maintenance takes less than 30min, and the visible impact is the SRM and VR processes are restarted (usually less than 2mins). After the maintenance, user action is required on the remote (on-premises) DR site to recover the normal state of the VR pairing. (Existing replications are not affected, so the customer workloads remain protected.) If for some reason the maintenance can't be executed at the scheduled time, Draas-SSLCertificateRenew-canceled notification is sent, which is normally followed up and new maintenance is scheduled. SSL certificates of SRM and VR appliances are due to expire and VMware Site Recovery has scheduled replacement of these certificates.</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Table 8-1. Notifications Available from Notifications Gateway (continued)

<table>
<thead>
<tr>
<th>Display Name</th>
<th>Template ID</th>
<th>Description</th>
<th>Email Channel</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site Recovery - Scheduled SSL certificates replacement</td>
<td>Draas-SSLCertificateRenew-vmc-only</td>
<td>This is a heads up notification for VSR maintenance activity - replacement of SRM and VR appliances SSL certificates. It is sent at least 7 days before the start of the maintenance. Usually such maintenance takes less than 30min, and the visible impact is the SRM and VR processes are restarted (usually less than 2mins). After the maintenance, user action is required on the remote (on-premises) DR site to recover the normal state of the VR pairing. (Existing replications are not affected, so the customer workloads remain protected.) If for some reason the maintenance can't be executed at the scheduled time, Draas-SSLCertificateRenew-canceled notification is sent, which is normally followed up and new maintenance is scheduled. SSL certificates of SRM and VR appliances are due to expire and VMware Site Recovery has scheduled replacement of these certificates.</td>
<td>Yes</td>
</tr>
<tr>
<td>Site Recovery - SSL certificates replacement canceled</td>
<td>Draas-SSLCertificateRenew-canceled</td>
<td>VMware Site Recovery has canceled the scheduled replacement of SSL certificates of SRM and VR appliances</td>
<td>Yes</td>
</tr>
<tr>
<td>Site Recovery - Scheduled Upgrade Started</td>
<td>Draas-upgrade-start</td>
<td>VMware Site Recovery has started its scheduled upgrade</td>
<td>Yes</td>
</tr>
<tr>
<td>Display Name</td>
<td>Template ID</td>
<td>Description</td>
<td>Email Channel</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>Site Recovery - Scheduled Upgrade</td>
<td>Draas-upgrade-planned</td>
<td>VMware Site Recovery has scheduled its upgrade in 7 days. Customer should ensure that SRM recovery plans are in a state which allows upgrade to avoid re-schedule or cancelation of the upgrade. This heads up notification for VSR maintenance activity - upgrade of SRM and VR appliances. It is send at least 7 days before the actual start of the maintenance. Normally the upgrade completes for ~30min, but the maintenance windows is booked for 4h to allow time for troubleshooting / fixing if there are issues. The VSR upgrade should not overlap with the SDDC upgrade window, and it doesn’t impact non VSR related functionality in the SDDC. Actual visible impact for the user is due to restart of SRM and VR which is in less than 2mins. Customer action is required prior maintenance - customer needs to ensure that their SRM recovery plans are in a state which allows upgrade. If this is not true at the time of the maintenance, the maintenance is re-scheduled or cancelled. Customer also needs to make sure that their on-prem SRM/VR version is upgraded to compatible one with the cloud SRM/VR version to be deployed.</td>
<td>Yes</td>
</tr>
<tr>
<td>Display Name</td>
<td>Template ID</td>
<td>Description</td>
<td>Email Channel</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>Site Recovery - Scheduled Upgrade - 8.2 port change</td>
<td>Draas-upgrade-planned-82portchange</td>
<td>VMware Site Recovery has scheduled its upgrade in 7 days. Customer should ensure that SRM recovery plans are in a state which allows upgrade to avoid re-schedule or cancelation of the upgrade. This is received only when you upgrading VMware Site Recovery from 8.1 to 8.3.</td>
<td>Yes</td>
</tr>
<tr>
<td>Site Recovery - Re-Scheduled Upgrade</td>
<td>Draas-upgrade-replanned</td>
<td>VMware Site Recovery has re-scheduled its upgrade for another date.</td>
<td>Yes</td>
</tr>
<tr>
<td>Site Recovery - Scheduled Upgrade Completed</td>
<td>Draas-upgrade-finish</td>
<td>VMware Site Recovery has completed its scheduled upgrade.</td>
<td>Yes</td>
</tr>
<tr>
<td>Site Recovery - Scheduled Upgrade Canceled</td>
<td>Draas-upgrade-cancel</td>
<td>VMware Site Recovery has canceled its scheduled upgrade.</td>
<td>Yes</td>
</tr>
<tr>
<td>Site Recovery - On-prem Upgrade</td>
<td>Draas-upgrade-paired-on-prem</td>
<td>Heads-up for upgrade of VMware Site Recovery to 8.3 for SDDCs paired to on-prem site with SRM 8.1 or later.</td>
<td>Yes</td>
</tr>
<tr>
<td>Site Recovery - vmc(820) Upgrade</td>
<td>Draas-upgrade-paired-vmc-820</td>
<td>Heads-up for upgrade of VMware Site Recovery to 8.3 for SDDCs paired to another VMC on AWS SDDC.</td>
<td>Yes</td>
</tr>
<tr>
<td>Site Recovery - On-prem(820) Upgrade</td>
<td>Draas-upgrade-paired-on-prem-820</td>
<td>Heads-up for upgrade of VMware Site Recovery to 8.3 for SDDCs paired to on-prem site with SRM 8.2.</td>
<td>Yes</td>
</tr>
<tr>
<td>Site Recovery - vCenter certificate renew completed</td>
<td>Draas-VC-cert-replaced-vr-pairing-needs-reconfigure</td>
<td>Renew of PSC/vCenter Certificate in VMC on AWS SDDC was performed.</td>
<td>Yes</td>
</tr>
<tr>
<td>VMC Operator Notifications</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SDDC SSL Certification Replacement</td>
<td>SddcSSLCertificationReplacement</td>
<td>A vCenter and NSX SSL certificate update window has been scheduled for your SDDC.</td>
<td>Yes</td>
</tr>
<tr>
<td>Single Host SDDC Failure</td>
<td>Single_Host_SDDC_Failure</td>
<td>Host failure notification for a single host SDDC.</td>
<td>Yes</td>
</tr>
<tr>
<td>Display Name</td>
<td>Template ID</td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>--------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cluster addition</td>
<td>CLUSTER-CREATE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deployment of SDDC</td>
<td>SDDC-PROVISION</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cluster deletion</td>
<td>CLUSTER-DESTROY</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Removal of ESX host</td>
<td>ESX-DELETE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Removal of SDDC</td>
<td>SDDC-DELETE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Provision of ESX host</td>
<td>ESX-PROVISION</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Provision of Multi-AZ SDDC</td>
<td>MULTI-AZ-SDDC-PROVISION</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Scale up SDDC from Single Host</td>
<td>SDDC-CONVERT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Multi-AZ Cluster addition</td>
<td>MULTIAZ_CLUSTER-CREATE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Creation of subscription</td>
<td>CREATE-OFFER-SUBSCRIPTION</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Linking of AWS account</td>
<td>ACCOUNT-LINK</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deletion of POP ssh access</td>
<td>DELETE_POP_SSH_ACCESS_TASK_TYPE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Update of POP ssh access</td>
<td>UPDATE_SSH_ACCESS_TASK_TYPE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Update of vCenter delegated user</td>
<td>UPDATE_VCENTER_DELEGATED_USER_TASK</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Updating Management VM</td>
<td>MANAGEMENT-VM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deletion of vCenter delegated user</td>
<td>DELETE_VCENTER_DELEGATED_USER_TASK</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Addition of POP ssh access</td>
<td>ADD_POP_SSH_ACCESS_TASK_TYPE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Creation of delegated vCenter user</td>
<td>CREATE_DELEGATED_VCENTER_USER_TASK</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Creation of an SDDC group</td>
<td>SDDC_GROUP_CREATE_TASK_TYPE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Update of an SDDC group</td>
<td>SDDC_GROUP_UPDATE_TASK_TYPE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deletion of an SDDC group</td>
<td>SDDC_GROUP_DELETE_TASK_TYPE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SDDC member added to group</td>
<td>SDDC_GROUP_MEMBER_ADDITION_TASK_TYPE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SDDC member deleted from group</td>
<td>SDDC_GROUP_MEMBERS_DELETION_TASK_TYPE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Addition of a Direct Connect Gateway to a group</td>
<td>SDDC_GROUP_ON_PREM_CONNECTIVITY_PROPOSAL_TASK_TYPE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deletion of a Direct Connect Gateway from a group</td>
<td>SDDC_GROUP_ON_PREM_CONNECTIVITY_DELETE_TASK_TYPE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Addition of an external AWS account</td>
<td>SDDC_SHARE_CONNECTOR_TASK_TYPE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Removal of an external AWS account</td>
<td>SDDC_SHARE_CONNECTOR_DELETE_TASK_TYPE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Update to external attachments</td>
<td>EXTERNAL_L3_CONNECTION_TASK_TYPE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Troubleshooting

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
- Unable to Connect to VMware Cloud on AWS
- Unable to Connect to vCenter Server
- Unable to Select Subnet When Creating SDDC
- Unable to Copy Changed Password Into vCenter Login Page
- Compute Workloads Are Unable to Reach an On-Premises DNS Servers Over a Policy-Based VPN

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.
   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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Delete cookies</strong></td>
<td>Follow the instructions for your browser. If you want to delete only specific cookies, delete ones with &quot;vmware&quot; and &quot;vidm&quot; in the name.</td>
</tr>
<tr>
<td>Google Chrome:</td>
<td>See <a href="https://support.google.com/chrome/answer/95647">https://support.google.com/chrome/answer/95647</a></td>
</tr>
<tr>
<td><strong>Open an incognito or private browsing window</strong></td>
<td>Follow the instructions for your browser:</td>
</tr>
<tr>
<td>Google Chrome:</td>
<td>Click the menu button and select <strong>New incognito window</strong>.</td>
</tr>
<tr>
<td>Mozilla Firefox:</td>
<td>Click the menu button and select <strong>New Private Window</strong>.</td>
</tr>
<tr>
<td>Microsoft Internet Explorer:</td>
<td>Click the tools button and select <strong>Safety &gt; InPrivate Browsing</strong>.</td>
</tr>
<tr>
<td>Microsoft Edge:</td>
<td>Click the More icon, and select <strong>New InPrivate window</strong>.</td>
</tr>
<tr>
<td>Safari:</td>
<td>Select <strong>File &gt; New Private Window</strong>.</td>
</tr>
</tbody>
</table>

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>
<thead>
<tr>
<th>Use Cases</th>
<th>Service</th>
<th>Source</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provide access to vCenter Server from the internet.</td>
<td>HTTPS</td>
<td>public IP address</td>
<td>vCenter</td>
</tr>
<tr>
<td>Use for general vSphere Client access as well as for monitoring vCenter Server</td>
<td>HTTPS</td>
<td>IP address or CIDR block from on-premises data center</td>
<td>vCenter</td>
</tr>
<tr>
<td>Provide access to vCenter Server over VPN tunnel.</td>
<td>HTTPS</td>
<td>IP address or CIDR block from on-premises data center</td>
<td>vCenter</td>
</tr>
<tr>
<td>Required for Management Gateway VPN, Hybrid Linked Mode, Content Library.</td>
<td>Any</td>
<td>vCenter</td>
<td>IP address or CIDR block from on-premises data center</td>
</tr>
</tbody>
</table>

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 Servers Over a Policy-Based VPN

Workload VMs in an SDDC that uses a policy-based VPN for its on-premises connection are unable to reach an on-premises DNS server.

Problem
You connect to your VMware Cloud on AWS SDDC to your on-premises SDDC over a policy-based VPN and can ping IP addresses in the on-premises network from VMs in the SDDC network but workload VMs cannot reach your on-premises DNS servers.

Cause
The problem occurs if the policy-based VPN connection to your on-premises SDDC has not been configured to allow DNS requests.

Solution
1 If you can configure your on-premises connection over a route-based VPN or Direct Connect, you can skip the rest of these steps.

2 If you must use a policy-based VPN as your on-premises connection, configure the SDDC side of the VPN tunnel to allow DNS requests over the VPN.
   b Select Networking & Security > VPN > Policy Based.
   c Click the vertical ellipsis icon for the VPN and select Edit VPN.
d  Under the **Local Network** drop-down, select **cgw-dns-network**.

e  Click **SAVE**.

3  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.