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

https://docs.vmware.com/
## Contents

About Managing the VMware Cloud™ on AWS Data Center 5

### 1 vSphere Administration in VMware Cloud on AWS 6
- vSphere Components and Interfaces 8
- View Permissions and Privileges 10
- CloudAdmin Privileges 11

### 2 Installing and Configuring the vCenter Cloud Gateway Appliance 16
- Install the vCenter Cloud Gateway Appliance from the Graphical Installer 16
- Install the vCenter Cloud Gateway Appliance Using the Command-Line Installer 20
- Backing Up the Cloud Gateway Appliance 22
- Updates to the Gateway Appliance and Component Features 22
- Replace the Certificate for the Cloud Gateway Appliance 22

### 3 Configuring Hybrid Linked Mode 24
- Hybrid Linked Mode Prerequisites 25
- Configuring Hybrid Linked Mode using the vCenter Cloud Gateway Appliance 28
  - Link the vCenter Cloud Gateway Appliance to Your Cloud SDDC 28
  - Replace the Certificate for the vSphere Cloud Gateway Appliance 30
- Configuring Hybrid Linked Mode from the Cloud SDDC 31
  - Validate Network Connectivity for Hybrid Linked Mode 31
  - Link to an On-Premises Data Center 32
  - Add an Identity Source to the SDDC LDAP Domain 32
- Troubleshooting Networking for Hybrid Linked Mode 33
  - Connectivity Validator: DNS Server Can't Be Reached 33
  - Connectivity Validator: DNS Lookup Failure for a Given FQDN 34
  - Connectivity Validator: Ping Failure for a Given FQDN 35
  - Connectivity Validator: Port Reachability Failure for a given FQDN 36
  - Connectivity Validator: Traceroute Failure for a given FQDN 37
  - Connectivity Validator: Test Failure Due to Internal Error 38
- Unlink a Cloud SDDC 38

### 4 Clusters and Resource Pools in VMware Cloud on AWS 41
- Predefined Clusters and Resource Pools 42
- Examine VMs and Hosts in the Cluster 43
- Examine and Monitor vSphere DRS 44
- Examine and Monitor vSphere HA 44
- Examine Cluster Configuration 45
Create and Manage Child Resource Pools  46

5  vsAN Storage in VMware Cloud on AWS  49
  Storage Capacity and Data Redundancy  50
  vsAN Deduplication and Compression  50
  Enabling TRIM/UNMAP Commands for VMware Cloud on AWS Clusters  51
  vsAN Encryption in VMware Cloud on AWS  51
    Generate New Encryption Keys in VMware Cloud on AWS  51
  vsAN Policies  52
    Define a Virtual Machine Storage Policy for vsAN  57
    Assign Storage Policies to Virtual Machines  58
  Shared Storage Clusters on vsAN  59

Managing Virtual Machines in VMware Cloud on AWS  61
  VM Configurations With Limited or No Support in the SDDC  62
    Virtual Hardware Support in the VMware Cloud on AWS SDDC  64
  Using PowerCLI and the Guest Operations API  64
  Deploy a VM from an OVF Template in a Content Library  65
About Managing the VMware Cloud™ on AWS Data Center

The Managing the VMware Cloud on AWS Data Center documentation explains how to configure and manage your VMware Cloud on AWS software-defined data center (SDDC) and the virtual machines that run in it.

Intended Audience

This information was written for administrators who have a basic understanding of configuring and managing vSphere in an on-premises environment and are familiar with VMware virtualization concepts. In-depth knowledge of Amazon Web Services is not required.

vSphere Management in VMware Cloud on AWS

After you complete the initial configuration of your VMware Cloud on AWS SDDC and its networks, you can create resource pools and folders, add a vCenter Single Sign-On identity source, and perform other operations that you might already be familiar with from an on-premises environment. You can also use hybrid linked mode to view and manage your on-premises vCenter Server and the one in your VMware Cloud on AWS SDDC with a common set of user identities.
vSphere Administration in VMware Cloud on AWS

vSphere in a software-defined data center like your VMware Cloud on AWS SDDC works in the same way that your on-premises vSphere does. In the SDDC, some vSphere components are owned and managed by VMware, so some of the on-premises administrative workflows that you're familiar with aren't needed in VMC.

For information about vSphere administration in VMware Cloud on AWS, you should refer to the vSphere Documentation, but you'll need to keep a few high-level differences in mind when reading those topics:

- VMware Cloud on AWS users don't have physical access to access ESXi host hardware and cannot log in to the ESXi host operating system. Procedures that require this kind of access are performed by VMware staff.
- Global Permissions are not replicated from your on-premises vCenter Server and the vCenter Server in your SDDC. Global permissions do not apply to objects that VMware manages for you, like SDDC hosts and datastores.

Specific Differences to be Aware Of

In addition to the high-level differences we've noted, many topics in the vSphere Documentation are written specifically for on-premises users, and don't include some of the information you need when using vSphere in the SDDC.
### Table 1-1. Topic Content Differences Between On-Premises and SDDC vSphere

<table>
<thead>
<tr>
<th>Topic</th>
<th>Highlights</th>
</tr>
</thead>
<tbody>
<tr>
<td>vSphere Managed Inventory Objects</td>
<td>Each VMware Cloud on AWS SDDC has a single data center named SDDC-Datacenter. The data center defines the namespace for networks and datastores. The names for these objects must be unique within a data center. You cannot have two datastores with the same name within a single data center. Virtual machines, templates, and clusters need not be unique within the data center, but must be unique within their folder.</td>
</tr>
<tr>
<td>vCenter Server System Roles</td>
<td>The vCenter Server in your SDDC includes two predefined roles that are not present in your on-premises vCenter.</td>
</tr>
<tr>
<td><strong>CloudAdmin Role</strong></td>
<td>The CloudAdmin role has the necessary privileges for you to create and manage workloads on your SDDC. However, you cannot access or configure certain management components that are supported and managed by VMware, such as hosts, clusters, and management virtual machines.</td>
</tr>
<tr>
<td><strong>CloudGlobalAdmin Role</strong></td>
<td>The CloudGlobalAdmin role, which has a subset of the privileges granted to the CloudAdmin role, is deprecated as of SDDC version 1.7.</td>
</tr>
<tr>
<td>Host Management with the VMware Host Client</td>
<td>VMware Cloud on AWS users don’t have physical access to access ESXi host hardware and cannot log in to the ESXi host operating system. Procedures that require this kind of access are performed by VMware staff.</td>
</tr>
<tr>
<td>Securing ESXi Hosts</td>
<td></td>
</tr>
</tbody>
</table>
Table 1-1. Topic Content Differences Between On-Premises and SDDC vSphere (continued)

<table>
<thead>
<tr>
<th>Topic</th>
<th>Highlights</th>
</tr>
</thead>
<tbody>
<tr>
<td>Securing vCenter Server Systems</td>
<td>In an on-premises SDDC, you are responsible for ensuring the security of your vCenter Server system. In VMware Cloud on AWS, VMware performs most of these tasks for you. You are responsible for following security best practices, especially for the VMs in your environment, and might want to be aware of some other aspects of vCenter Server and vCenter Single Sign-On such as password and lockout policies.</td>
</tr>
<tr>
<td>vSphere Authentication with vCenter Single Sign-On</td>
<td>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. Contact Technical Support and request a password change. After installation, <a href="mailto:cloudadmin@vmc.local">cloudadmin@vmc.local</a> has administrator access to both vCenter Single Sign-On and vCenter Server. That user can also add identity sources, set the default identity source, and set policies in the vmc.local domain. Certain management operations in the vmc.local domain are restricted to VMware Cloud on AWS operations staff.</td>
</tr>
</tbody>
</table>

This chapter includes the following topics:

- vSphere Components and Interfaces
- View Permissions and Privileges
- CloudAdmin Privileges

vSphere Components and Interfaces

VMware vSphere is a suite of software components for virtualization. These include ESXi, vCenter Server, and other software components that fulfill a number of different functions in the vSphere environment. VMware manages many parts of your VMware Cloud on AWS SDDC for you, but you can examine all components, and change certain parts of the configuration.

vSphere Components

vSphere includes the following software components:

ESXi
The hypervisor on which you run virtual machines as a set of configuration and disk files that together perform all the functions of a physical machine.

**Note** No VMware Cloud on AWS user can have physical access to access ESXi host hardware or root access to the ESXi operating system. Procedures that require this kind of access must be performed by VMware staff. This means that you can't add, remove, or manage ESXi users, or undertake any other aspects of [Host Management with the VMware Host Client](#).

### vCenter Server

A service that acts as a central administrator for VMware ESXi hosts.

vCenter Server runs continuously in the background. It performs its monitoring and managing activities even when no clients are connected.

VMware Cloud on AWS includes a single vCenter Server that can be connected to an on-premises vCenter Server using Hybrid Linked Mode.

### vCenter Single Sign-On

A service that is part of the vCenter Server management infrastructure. The vCenter Single Sign-On authentication service makes the VMware cloud infrastructure platform more secure by allowing the various vSphere software components to communicate with each other through a secure token exchange mechanism, instead of requiring each component to authenticate a user separately with a directory service like Active Directory.

### vSphere Interfaces

The vSphere interface you use depends on the task you want to perform and on the component you want to manage.

**vSphere Client**

The vSphere Client is an HTML5-based client for managing VMware Cloud on AWS. vSphere Client also performs most configuration tasks for on-premises vSphere SDDCs.

**vSphere Command-Line Interfaces**

vSphere supports multiple command-line interfaces for configuring virtual machines and other vSphere components.

**vSphere SDKs**

vSphere supports several SDKs for managing different aspects of your vSphere environment.

**Virtual Machine Console**

Just as a physical machine, each virtual machine has a console that supports certain management tasks, depending on the operating system.
vCenter Server Features

Many vCenter Server features that required special licensing in earlier versions of the product are available as part of the vSphere Standard license in vSphere 6.x and are also supported for VMware Cloud on AWS.

vCenter Server features include:

vSphere vMotion

Enables you to move running virtual machines from one ESXi host to another ESXi host without service interruption.

Storage vMotion

Allows you to move the disks and configuration file of a running virtual machine from one datastore to another without service interruption.

vSphere High Availability

vSphere High Availability ensures that if a host fails in an SDDC cluster, all virtual machines on the host are restarted on another host in the same cluster. vSphere High Availability settings are preconfigured in VMware Cloud on AWS and cannot be changed by customers.

vSphere DRS

Helps improve resource allocation and power consumption across all hosts and resource pools. vSphere DRS collects resource use information for all hosts and virtual machines in the cluster and or migrates virtual machines in the following situations:

- Initial placement – When you power on a virtual machine in the cluster for the first time, DRS either places the virtual machine or makes a recommendation.
- Load balancing – DRS attempts to improve resource use across the cluster by performing automatic migrations of virtual machines (vMotion) or by providing a recommendation for virtual machine migrations.

See Using Policies and Profiles for more detail on the storage policies that govern DRS operation in the SDDC.

View Permissions and Privileges

For each object in the hierarchy, you can use the vSphere Client view the privileges granted to users in the CloudAdmin role as well as other predefined or custom roles.

Procedure

1. Select an object in the object hierarchy, for example a resource pool or virtual machine, and click Permissions.
2 You can then view the privileges associated with each group.
   a On the vSphere Client Home page, click **Administration**.
   b Under **Access Control**, click **Roles**.
   c Click a role name (**CloudAdmin**, for example).
   d Click the **Privileges** tab on the right.

**Results**

You can scroll through the list to see the privileges granted to the selected role. See **Defined Privileges** for a detailed list of all vSphere privileges.

**CloudAdmin Privileges**

Because VMware performs host administration and other tasks for you, a Cloud Administrator requires fewer privileges than an Administrator user on an on-premises data center.

The CloudAdmin role has a set of privileges that is dynamically generated for your SDDC. They include most of the available privileges in all categories. To view the privileges granted to the CloudAdmin role, log into the SDDC vSphere Client, click **Administration > Roles**, select CloudAdmin from the list of roles, then click **PRIVILEGES**.

You can also use a PowerShell snippet like this one to retrieve the list of privileges for the CloudAdmin role in your SDDC.

```powershell
$vmcUserName = "CloudAdmin"
($authMgr.RoleList | where {$_.Name -eq $vmcUserName}).Privilege
```

The CloudAdmin role has the following privileges in SDDC Version 1.9. This list might not be correct for other SDDC versions.

- Alarm.Acknowledge
- Alarm.Create
- Alarm.Delete
- Alarm.DisableActions
- Alarm.Edit
- Alarm.SetStatus
- Authorization.ModifyPermissions
- Authorization.ModifyRoles
- CertificateManagement.Manage
- Cns.Searchable
- ComputePolicy.Manage
- ContentLibrary.AddLibraryItem
- ContentLibrary.CheckInTemplate
Managing the VMware Cloud on AWS Data Center

InventoryService.Tagging.ObjectAttachable
Network.Assign
Resource.ApplyRecommendation
Resource.AssignVAppToPool
Resource.AssignVMToPool
Resource.ColdMigrate
Resource.DeletePool
Resource.EditPool
Resource.HotMigrate
Resource.MovePool
Resource.QueryVMotion
Resource.RenamePool
ScheduledTask.Create
ScheduledTask.Delete
ScheduledTask.Edit
ScheduledTask.Run
Sessions.GlobalMessage
Sessions.ValidateSession
StorageProfile.Update
StorageProfile.View
StorageViews.View
System.Anonymous
System.Read
System.View
Trust.Manage
VApp.ApplicationConfig
VApp.AssignResourcePool
VApp.AssignVApp
VApp.AssignVM
VApp.Clone
VApp.Create
VApp.Delete
VApp.Export
VApp.ExtractOvfEnvironment
VApp.Import
VApp.InstanceConfig
VApp.ManagedByConfig
VApp.Move
VApp.PowerOff
VApp.PowerOn
VApp.Rename
VApp.ResourceConfig
VApp.Suspend
VApp.Unregister
VirtualMachine.Config.AddExistingDisk
VirtualMachine.Config.AddNewDisk
VirtualMachine.Config.AddRemoveDevice
VirtualMachine.Config.AdvancedConfig
VirtualMachine.Config.Annotation
VirtualMachine.Config.CPUCount
VirtualMachine.Config.ChangeTracking
VirtualMachine.Config.DiskExtend
VirtualMachine.Config.DiskLease
VirtualMachine.Config.EditDevice
VirtualMachine.Config.HostUSBDevice
VirtualMachine.Config.ManagedBy
VirtualMachine.Config.Memory
VirtualMachine.Config.MksControl
VirtualMachine.Config.QueryFTCompatibility
VirtualMachine.Config.QueryUnownedFiles
VirtualMachine.Config.RawDevice
VirtualMachine.Config.ReloadFromPath
VirtualMachine.Config.RemoveDisk
VirtualMachine.Config.Rename
VirtualMachine.Config.ResetGuestInfo
VirtualMachine.Config.Resource
VirtualMachine.Config.Settings
VirtualMachine.Config.SwapPlacement
VirtualMachine.Config.UpgradeVirtualHardware
VirtualMachine.GuestOperations.Execute
VirtualMachine.GuestOperations.Modify
VirtualMachine.GuestOperations.ModifyAliases
VirtualMachine.GuestOperations.Query
VirtualMachine.GuestOperations.QueryAliases
VirtualMachine.Hbr.ConfigureReplication
VirtualMachine.Hbr.MonitorReplication
VirtualMachine.Hbr.ReplicaManagement
VirtualMachine.Interact.AnswerQuestion
VirtualMachine.Interact.Backup
VirtualMachine.Interact.ConsoleInteract
VirtualMachine.Interact.CreateScreenshot
VirtualMachine.Interact.DefragmentAllDisks
VirtualMachine.Interact.DeviceConnection
VirtualMachine.Interact.DnD
VirtualMachine.Interact.GuestControl
VirtualMachine.Interact.PowerOff
VirtualMachine.Interact.PowerOn
VirtualMachine.Interact.PutUsbScanCodes
VirtualMachine.Interact.Reset
VirtualMachine.Interact.SESparseMaintenance
VirtualMachine.Interact.SetCDMedia
VirtualMachine.Interact.SetFloppyMedia
VirtualMachine.Interact.Suspend
VirtualMachine.Interact.ToolsInstall
VirtualMachine.Inventory.Create
VirtualMachine.Inventory.CreateFromExisting
VirtualMachine.Inventory.Delete
VirtualMachine.Inventory.Move
VirtualMachine.Inventory.Register
VirtualMachine.Inventory.Unregister
VirtualMachine.Namespace.Event
VirtualMachine.Namespace.EventNotify
VirtualMachine.Namespace.ModifyContent
VirtualMachine.Namespace.Query
VirtualMachine.Namespace.ReadContent
VirtualMachine.Provisioning.Clone
VirtualMachine.Provisioning.CloneTemplate
For more information on the permissions granted by each privilege, see the vSphere Defined Privileges reference.
The Cloud Gateway Appliance is an appliance installed in your on-premises data center. It provides a number of features for hybrid management, that is, cases where an on-premises data center is connected to your cloud SDDC.

Features available from the Cloud Gateway Appliance include:

- Hybrid Linked Mode. Hybrid Linked Mode allows you to view and manage your on-premises data center and your cloud SDDC from a single view. See Chapter 3 Configuring Hybrid Linked Mode.

This chapter includes the following topics:

- Install the vCenter Cloud Gateway Appliance from the Graphical Installer
- Install the vCenter Cloud Gateway Appliance Using the Command-Line Installer
- Backing Up the Cloud Gateway Appliance
- Updates to the Gateway Appliance and Component Features
- Replace the Certificate for the Cloud Gateway Appliance

Install the vCenter Cloud Gateway Appliance from the Graphical Installer

Download and install the Cloud Gateway Appliance if you want to enable Hybrid Linked Mode from your on-premises SDDC or access other solutions available from the Cloud Gateway Appliance.

**Note** The instructions in this section apply to version 1.11 and later of the SDDC software.

**Prerequisites**

Verify that the host on which you intend to install the Cloud Gateway Appliance appliance meets the following hardware requirements.
## Hardware

<table>
<thead>
<tr>
<th>Minimum required</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPUs</td>
</tr>
<tr>
<td>Memory</td>
</tr>
<tr>
<td>Storage</td>
</tr>
</tbody>
</table>

- Ensure that the Cloud Gateway Appliance and your vCenter Server instances can reach each other over your network. Ensure that the following firewall ports are open.

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>User's web browser</td>
<td>Cloud Gateway Appliance</td>
<td>5480</td>
<td>Gathering support bundle</td>
</tr>
<tr>
<td>Cloud Gateway Appliance</td>
<td>On-premises vCenter Server</td>
<td>443</td>
<td>Hybrid Linked Mode</td>
</tr>
<tr>
<td>Cloud Gateway Appliance</td>
<td>On-premises Platform Services Controller</td>
<td>443, 389</td>
<td>Hybrid Linked Mode</td>
</tr>
<tr>
<td>Cloud Gateway Appliance</td>
<td>Cloud SDDC vCenter Server</td>
<td>443</td>
<td>Hybrid Linked Mode</td>
</tr>
<tr>
<td>Cloud Gateway Appliance</td>
<td>Cloud ESXi host</td>
<td>902</td>
<td>Virtual Machine Console</td>
</tr>
<tr>
<td>Cloud Gateway Appliance</td>
<td>On-premises Active Directory server (ports dependent on your usage)</td>
<td>389, 636, 3268, 3269</td>
<td>Identity source</td>
</tr>
</tbody>
</table>

The following figure shows the ports required to be open for linking with the Cloud Gateway Appliance.

---

### Procedure

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

2. Click the **Tools ( )** tab.
3 Click **Download** on the Gateway Appliance card.

You are directed to My VMware, where you can complete the download of the appliance installer ISO image.

4 In the installer ISO image, browse to the `ui-installer` folder and open the folder for the operating system from which you want to install the appliance.
   - For Windows OS, go to the `win32` subdirectory and run the `installer.exe` file.
   - For Linux OS, go to the `lin64` subdirectory, and run the `installer` file.
   - For Mac OS, go to the `mac` subdirectory and run the `Installer.app` file.

5 Click **Get Started**.

6 Accept the End User License agreement and click **Next**.

7 Specify the Gateway deployment parameters and click **Next**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Steps</th>
</tr>
</thead>
</table>
| You can connect to an ESXi host on which to deploy the appliance. | 1 Enter the FQDN or IP address of the ESXi host.  
2 Enter the HTTPS port of the ESXi host.  
3 Enter the user name and password of a user with administrative privileges on the ESXi host, for example, the root user.  
4 Click **Next**.  
5 Verify that the certificate warning displays the SHA1 thumbprint of the SSL certificate that is installed on the target ESXi host, and click **Yes** to accept the certificate thumbprint. |
| You can connect to a vCenter Server instance and browse the inventory to select an ESXi host or DRS cluster on which to deploy the appliance. | 1 Enter the FQDN or IP address of the vCenter Server instance.  
2 Enter the HTTPS port of the vCenter Server instance.  
3 Enter the user name and password of user with vCenter Single Sign-On administrative privileges on the vCenter Server instance, for example, the administrator@your_domain_name user.  
4 Click **Next**.  
5 Verify that the certificate warning displays the SHA1 thumbprint of the SSL certificate that is installed on the target vCenter Server instance, and click **Yes** to accept the certificate thumbprint.  
6 Select the data center or data center folder that contains the ESXi host or DRS cluster on which you want to deploy the appliance, and click **Next**.  
**Note** You must select a data center or data center folder that contains at least one ESXi host that is not in lockdown or maintenance mode.  
7 Select the ESXi host or DRS cluster on which you want to deploy the appliance, and click **Next**. |
8 Set up the target appliance VM and click **Next**.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM name</td>
<td>Enter a name for the Cloud Gateway Appliance VM. The appliance name must not contain a percent sign (%), backslash (), or forward slash (/) and must be no more than 80 characters in length.</td>
</tr>
<tr>
<td>Set root password</td>
<td>Set a root password for the Cloud Gateway Appliance VM. The password must contain only lower ASCII characters without spaces, at least eight characters, a number, uppercase and lowercase letters, and a special character, for example, an exclamation mark (!), hash key (#), at sign (@), or brackets (()).</td>
</tr>
<tr>
<td>Confirm root password</td>
<td>Confirm the password you set above.</td>
</tr>
</tbody>
</table>

9 Select the datastore location for the Cloud Gateway Appliance and click **Next**.

   a Select the datastore where you want to place the Cloud Gateway Appliance.
   
   b Select **Enable Thin Disk Mode** to conserve disk space by deploying the appliance using a thin disk.

10 Configure the network settings for the appliance and click **Next**.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>Select the network. The networks displayed in the drop-down menu depend on the network settings of the target server. If you are deploying the appliance directly on an ESXi host, non-ephemeral distributed virtual port groups are not supported and are not displayed in the drop-down menu.</td>
</tr>
<tr>
<td>IP version</td>
<td>Select the version for the appliance IP address. You can select either IPv4 or IPv6.</td>
</tr>
</tbody>
</table>
| IP assignment   | Select how to allocate the IP address of the appliance.  
   - **static**  
     The wizard prompts you to enter the IP address and network settings.  
     **Note** Avoid using an IP address as a system name. If you use an IP address as a system name, you cannot change the IP address and update the DNS settings after deployment.  
   - **DHCP**  
     A DHCP server is used to allocate the IP address. Select this option only if a DHCP server is available in your environment. |
<p>| FQDN            | If you have an enabled DDNS in your environment, you can enter a fully qualified domain name (FQDN) for the appliance. If you enter a FQDN that already exists, the installer warns you that this will cause an error in deployment unless you isolate the network that the appliance is on. For example, you can deploy the appliance on a different port group from the existing FQDN. |</p>
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>If you selected a static IP address, enter the IP address for the appliance. If you enter an IP address that already exists, the installer warns you that this will cause an error in deployment unless you isolate the network that the appliance is on. For example, you can deploy the appliance on a different port group from the existing IP address.</td>
</tr>
<tr>
<td>Subnet mask or prefix length</td>
<td>Enter the subnet mask or prefix length for the IP address.</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>Enter the default gateway to be used by the appliance.</td>
</tr>
<tr>
<td>DNS Servers</td>
<td>Enter the addresses of the DNS servers used by the appliance.</td>
</tr>
</tbody>
</table>

11 Configure appliance Settings and click **Next**.

- Select **Synchronize Time with NTP servers** and enter the address of one or more NTP servers in the text box to use NTP servers for time synchronization.
- Select **Synchronize Time with ESXi host** to synchronize time to the host you're deploying to.

12 Click **Finish** to deploy the appliance.

**Results**

The Cloud Gateway Appliance is deployed to your on-premises environment. A progress bar shows the progress of deployment.

**What to do next**

To configure services, open the Cloud Gateway Appliance UI at `https://gw-address:5480/gw-platform/` where `gw-address` is the IP address or FQDN of the appliance.

**Note** After you have installed the appliance, consider configuring appliance log collection following the guidelines in [VMware Knowledge Base article 67158](https://kb.vmware.com/s/article/67158). Appliance logs are useful when requesting support.

**Install the vCenter Cloud Gateway Appliance Using the Command-Line Installer**

Use the command-line installer to script or automate your Cloud Gateway Appliance installation.

**Note** The instructions in this section apply to version 1.11 and later of the SDDC software.

Use the command `vcgw-deploy` to install the Cloud Gateway Appliance from the command line. In addition to installing the appliance, you can use `vcgw-deploy` to validate your installation templates and run pre-checks on your installation. For a full list of `vcgw-deploy` options, run `vcgw-deploy install --help`. 
Prerequisites

Verify that the host on which you intend to install the Cloud Gateway Appliance meets the following hardware requirements.

<table>
<thead>
<tr>
<th>Hardware</th>
<th>Minimum required</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPUs</td>
<td>8</td>
</tr>
<tr>
<td>Memory</td>
<td>24 GB</td>
</tr>
<tr>
<td>Storage</td>
<td>190 GB</td>
</tr>
</tbody>
</table>

Procedure


2. Click the **Tools** tab.

3. Click **Download** on the Gateway Appliance card.

   You are directed to My VMware, where you can complete the download of the appliance installer ISO image.

4. Prepare a JSON template for the installation.
   a. In the installer ISO image, browse to the `cli-installer/templates` directory.
      
      This directory contains sample JSON templates for installing the Cloud Gateway Appliance either directly on an ESXi host or through a vCenter Server system.
   b. Copy a template to a working directory and edit it to include the necessary parameters.
      
      For more information about available template parameters, invoke the installer with the option `--template-help`. For example, on Windows, enter `vcgw-deploy.exe install --template-help`.

5. From the command line, change directory to the `cli-installer` directory and run the installation prechecks.
   a. For Windows OS, enter `vcgw-deploy.exe install path-to-template --precheck-only`.
   b. For Linux OS, enter `vcgw-deploy install path-to-template --precheck-only`.
   c. For Mac OS, enter `vcgw-deploy install path-to-template --precheck-only`.

   The prechecks identify problems with the template and parameters provided, so that you can fix any errors before launching the installation.

6. Launch the installer.
   a. For Windows OS, enter `vcgw-deploy.exe install path-to-template --accept-eula`.
   b. For Linux OS, enter `vcgw-deploy install path-to-template --accept-eula`.
   c. For Mac OS, enter `vcgw-deploy install path-to-template --accept-eula`.
What to do next

**Note**  After you have installed the appliance, consider configuring appliance log collection following the guidelines in [VMware Knowledge Base article 67158](https://kb.vmware.com/s/article/67158). Appliance logs are useful when requesting support.

## Backing Up the Cloud Gateway Appliance

Back up the Cloud Gateway Appliance is not necessary, because it is stateless and can be redeployed if needed.

File-based backup and restore solutions are not supported for the Cloud Gateway Appliance.

## Updates to the Gateway Appliance and Component Features

VMware periodically releases updates for the Cloud Gateway Appliance as well as for the individual solutions available through the appliance.

The Cloud Gateway Appliance regularly checks for updates every five minutes and applies them when they are available. Individual solutions, such as Hybrid Linked Mode, are updated separately from the core appliance.

To view the current version for the Cloud Gateway Appliance, log in to the VAMI UI at `https://gw-address:5480/ui` and select **Help > About**.

To view the current version for Hybrid Linked Mode, log into the vSphere Client UI for the Cloud Gateway Appliance, click the Help icon, and select **About VMware vSphere**.

## Replace the Certificate for the Cloud Gateway Appliance

You can replace the certificate for the Cloud Gateway Appliance when the certificate expires or when you want to use a certificate from another certificate provider.

**Important**  If you have configured Hybrid Linked Mode on the Cloud Gateway Appliance, do not use this procedure to replace the certificate. Use the process in [Replace the Certificate for the vSphere Cloud Gateway Appliance](#) instead.

### Procedure

1. Connect to the Cloud Gateway Appliance using SSH.
Choose whether to use a self-signed certificate or one signed by a Certificate Authority (CA).

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generate a self-signed certificate</td>
<td>At the command line, type <code>openssl req -x509 -newkey rsa:4096 -keyout server.pem -out cert.pem -days 365 -nodes</code> to generate the certificate.</td>
</tr>
</tbody>
</table>
| Use a CA-signed certificate           | a. Generate a Certificate Signing Request (CSR) by typing `openssl req -new -newkey rsa:2048 -nodes -out server.csr - keyout server.pem` at the command line.  
   b. Provide the CSR to your CA according to their request process.  
   c. When you receive the certificate from your CA, place it in a location you can access from the Cloud Gateway Appliance. |

3 Append the `cert.pem` file that you generated or received from your CA to the `server.pem` file by typing `cat cert.pem >> server.pem`.

4 Backup the old certificate by typing `cp /etc/applmgmt/appliance/server.pem /etc/applmgmt/appliance/server.pem.bk`.

5 Replace the old certificate with the `server.pem` file that you created in Step 3 by typing `mv server.pem /etc/applmgmt/appliance/`.

6 Type `systemctl restart gps_envoy.service` to restart the envoy service.

7 If Cloud Foundation registration is enabled, type `systemctl restart aap_envoy.service` to restart the Atlas Agent Platform envoy service.
Configuring Hybrid Linked Mode

Hybrid Linked Mode allows you to link your cloud vCenter Server instance with an on-premises vCenter Single Sign-On domain.

**Important** Before you can use Hybrid Linked Mode, you must configure your on-premises vCenter to enable single sign-on. See [vSphere Authentication with vCenter Single Sign-On](#) for details.

If you link your cloud vCenter Server to a domain that contains multiple vCenter Server instances linked using Enhanced Linked Mode, all of those instances are linked to your cloud SDDC.

Using Hybrid Linked Mode, you can:

- View and manage the inventories of both your on-premises and cloud data centers from a single vSphere Client interface, accessed using your on-premises credentials.
- Migrate workloads between your on-premises data center and cloud SDDC.
- Share tags and tag categories from your vCenter Server instance to your cloud SDDC.

Hybrid Linked Mode supports on-premises vCenter Server systems with either embedded or external Platform Services Controller (both Windows and vCenter Server Appliance). vCenter Server systems with external Platform Services Controller instances linked in Enhanced Linked Mode are also supported, up to the scale limits documented in [vSphere Configuration Maximums](#).

You have two options for configuring Hybrid Linked Mode. You can use only one of these options at a time.

- You can install the Cloud Gateway Appliance and use it to link from your on-premises data center to your cloud SDDC. In this case, SSO users and groups are mapped from your on-premises environment to the SDDC and you do not need to add an identity source to the SDDC LDAP domain.
- You can link your cloud SDDC to your on-premises vCenter Server. In this case, you must add an identity source to the SDDC LDAP domain.

This chapter includes the following topics:

- Hybrid Linked Mode Prerequisites
- Configuring Hybrid Linked Mode using the vCenter Cloud Gateway Appliance
Hybrid Linked Mode Prerequisites

Ensure that you have met the following prerequisites before configuring Hybrid Linked Mode.

Common Prerequisites

The following prerequisites are common to both linking from the Cloud Gateway Appliance and from the cloud SDDC.

- Configure a connection between your on-premises data center and the SDDC. You can use Direct Connect, a VPN, or both. See Configure AWS Direct Connect for VMware Cloud on AWS and Configure a VPN Connection Between Your SDDC and On-Premises Data Center in the VMware Cloud on AWS Networking and Security guide.
- Regardless of the type of connection you choose, the vCenter FQDN must resolve to a private IP address. This is not the default configuration. See Set vCenter Server FQDN Resolution Address for more information.
- Ensure that your on-premises data center and your cloud SDDC are synchronized to an NTP service or other authoritative time source. Hybrid Linked Mode can tolerate a time skew of up to ten minutes between the on-premises data center and the cloud SDDC.
- The maximum latency between your cloud SDDC and on-premises data center cannot exceed 100 msec roundtrip.
- Decide which of your on-premises users will have Cloud Administrator permissions. Add these users to a group within your identity source. Ensure that this group has access to your on-premises environment.

Prerequisites for Linking with Cloud Gateway Appliance

The following prerequisites apply when linking with the Cloud Gateway Appliance.

- Install the Cloud Gateway Appliance as described in Install the vCenter Cloud Gateway Appliance from the Graphical Installer.
- Your on-premises environment is running vSphere 6.5 patch d or later.
- Ensure that the Cloud Gateway Appliance and your vCenter Server instances can reach each other over your network. Ensure that the following firewall ports are open.

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>User's web browser</td>
<td>Cloud Gateway Appliance</td>
<td>5480</td>
<td>Gathering support bundle</td>
</tr>
<tr>
<td>Cloud Gateway Appliance</td>
<td>On-premises vCenter Server</td>
<td>443</td>
<td>Hybrid Linked Mode</td>
</tr>
<tr>
<td>Source</td>
<td>Destination</td>
<td>Port</td>
<td>Purpose</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>------</td>
<td>---------</td>
</tr>
<tr>
<td>Cloud Gateway Appliance</td>
<td>On-premises Platform Services Controller</td>
<td>443, 389</td>
<td>Hybrid Linked Mode</td>
</tr>
<tr>
<td>Cloud Gateway Appliance</td>
<td>Cloud SDDC vCenter Server</td>
<td>443</td>
<td>Hybrid Linked Mode</td>
</tr>
<tr>
<td>Cloud Gateway Appliance</td>
<td>Cloud ESXi host</td>
<td>902</td>
<td>Virtual Machine Console</td>
</tr>
<tr>
<td>Cloud Gateway Appliance</td>
<td>On-premises Active Directory server (ports dependent on your usage)</td>
<td>389, 636, 3268, 3269</td>
<td>Identity source</td>
</tr>
</tbody>
</table>

The following figure shows the ports required to be open for linking with the Cloud Gateway Appliance.

---

**Prerequisites for Linking from the Cloud SDDC**

The following prerequisites apply when linking from the cloud SDDC.

- Your on-premises vCenter Server system is running one of the following:
  - vSphere 6.0 Update 3 patch c and later.
  - vSphere 6.5 patch d and later.
- Ensure that you have the login credentials for your on-premises vSphere SSO domain.
Ensure that you have login credentials for a user who has a minimum of read-only access to the Base DN for users and groups in your on-premises environment. This is used when adding an identity source.

Ensure that an on-premises DNS server is configured for your management gateway so that it can resolve the FQDN for the identity source and on-premises systems.

Ensure that your on-premises gateway or firewall allows access to the necessary ports from your SDDC for the following services.

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Ports</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud SDDC</td>
<td>On-premises vCenter Server</td>
<td>443</td>
<td>Hybrid Linked Mode</td>
</tr>
<tr>
<td>Cloud SDDC</td>
<td>On-premises Platform Services Controller</td>
<td>389, 443</td>
<td>Hybrid Linked Mode</td>
</tr>
<tr>
<td>Cloud SDDC</td>
<td>On-premises Active Directory server (ports dependent on your usage)</td>
<td>389, 636, 3268, 3269</td>
<td>Identity Source</td>
</tr>
<tr>
<td>Cloud SDDC</td>
<td>On-premises DNS</td>
<td>53</td>
<td>Resolving FQDN of on-premises vCenter Server and Active Directory Server</td>
</tr>
<tr>
<td>Cloud SDDC</td>
<td>On-premises ESXi host</td>
<td>902</td>
<td>Virtual Machine Console</td>
</tr>
</tbody>
</table>

The following figure shows the ports that are required to be open for linking from the cloud SDDC.

Run the Connectivity Validator tests to check that network connectivity is correctly established for Hybrid Linked Mode. See Validate Network Connectivity for Hybrid Linked Mode.
Configuring Hybrid Linked Mode using the vCenter Cloud Gateway Appliance

Configure the Cloud Gateway Appliance to enable Hybrid Linked Mode from your on-premises environment.

In this case, you log into the Cloud Gateway Appliance to view and manage your on-premises and cloud environments together.

**Note**  The instructions in this section apply to version 1.11 and later of the SDDC software.

- **Link the vCenter Cloud Gateway Appliance to Your Cloud SDDC**
  Use this procedure to link the Cloud Gateway Appliance to your cloud SDDC using Hybrid Linked Mode.

- **Replace the Certificate for the vSphere Cloud Gateway Appliance**
  You can replace the certificate for the Cloud Gateway Appliance when the certificate expires or when you want to use a certificate from another certificate provider.

**Link the vCenter Cloud Gateway Appliance to Your Cloud SDDC**

Use this procedure to link the Cloud Gateway Appliance to your cloud SDDC using Hybrid Linked Mode.

**Note**  The instructions in this section apply to version 1.11 and later of the SDDC software.

**Prerequisites**

- You must have Administrator privileges in your on-premises environment in order to perform this task.

**Procedure**

1. In a web browser, go to https://gw-address:5480/gw-platform/ where gw-address is the IP address or FQDN of the appliance.

2. On the Multi-vCenter Connect card, click **Get Started**.

3. Log in with your Cloud Gateway Appliance credentials.

4. Enter the credentials for the cloud vCenter Server.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCenter Server</td>
<td>Enter the FQDN of the vCenter Server instance in your cloud SDDC.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter the username for the Cloud Administrator.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password for the Cloud Administrator.</td>
</tr>
</tbody>
</table>
5 Enter your on-premises SSO settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platform Services Controller</td>
<td>Enter the IP address or fully qualified domain name of the Platform Services controller in your on-premises environment.</td>
</tr>
<tr>
<td>HTTPS Port</td>
<td>Enter the HTTPS port used by the Platform Services Controller.</td>
</tr>
<tr>
<td>Single Sign-On User Name</td>
<td>Enter the Single Sign-On administrator user name in the form user@sso-domain.</td>
</tr>
</tbody>
</table>

Configuring SSO takes approximately 2-3 minutes.

6 Select whether to join the Cloud Gateway Appliance to your Active Directory domain.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Skip</td>
<td>If you are using Active Directory with LDAP, and your Active Directory server is already joined to the on-premises vCenter Server, select Skip to skip this step of the process. If your Active Directory server is not joined to the on-premises vCenter Server or if your Active Directory server uses IWA (regardless of whether or not it is joined to the on-premises vCenter Server, select Join.</td>
</tr>
<tr>
<td>Join</td>
<td>Enter the following parameters:</td>
</tr>
<tr>
<td></td>
<td>a In the Domain text box, enter an Active Directory domain name. For example, mydomain.com.</td>
</tr>
<tr>
<td></td>
<td>b Optionally, in the Organizational Unit text box, provide the full OU LDAP FQDN. For example, OU=Engineering,DC=mydomain,DC=com.</td>
</tr>
<tr>
<td></td>
<td>c In the Username text box, enter the user name for the Active Directory administrator in User Principal Name (UPN) format. For example, <a href="mailto:example@mydomain.com">example@mydomain.com</a>.</td>
</tr>
<tr>
<td></td>
<td>d In the Password field, enter the password for the Active Directory administrator.</td>
</tr>
<tr>
<td></td>
<td>If your Active Directory server uses IWA, click Restart Gateway. After the appliance restarts, click Get Started on the Multi-vCenter Connect card and log in again before proceeding.</td>
</tr>
</tbody>
</table>

7 Add the groups you have defined in your on premises environment to serve as cloud administrator groups.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a Select the on-premises identity source.</td>
<td></td>
</tr>
<tr>
<td>b Enter the name of the administrator group in the search box and select the group.</td>
<td></td>
</tr>
</tbody>
</table>

8 Click Configure.

The linking process requires a few minutes to complete.

What to do next

When the linking process is complete, choose one of the following:

- Click Launch vSphere Client to view and manage your on-premises and cloud SDDCs.
Click **Go Back to Cloud Gateway** to return to the Cloud Gateway management UI.

**Note**  Linking from the Cloud Gateway Appliance grants the selected AD group or groups cloud administrator access to the SDDC. If you want to configure a user or group with a lesser level of access, you must add the identity source directly to your SDDC as described in Add an Identity Source to the SDDC LDAP Domain.

After you have added the identity source to the SDDC, you must assign the permissions you want to grant to the users and/or groups as described in https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-A0F6D9C2-CE72-4FE5-BAFC-309CFC519EC8.html. After you have configured the identity source in the SDDC, users' permissions are based solely on what is configured in the SDDC. If you don't configure permissions for these users in the SDDC, they will experience issues when viewing the SDDC inventory from the vSphere Client UI on the Cloud Gateway Appliance.

**Replace the Certificate for the vSphere Cloud Gateway Appliance**

You can replace the certificate for the Cloud Gateway Appliance when the certificate expires or when you want to use a certificate from another certificate provider.

**Prerequisites**

You can replace the certificate only after Hybrid Linked Mode is enabled.

Generate certificate signing requests (CSRs) for each certificate you want to replace. Provide the CSR to your Certificate Authority. When the Certificate Authority returns the certificate, place it in a location that you can access from the Cloud Gateway Appliance.

**Procedure**

1. In a web browser, go to http://cga-address/ui where cga-address is the IP address or FQDN of the Cloud Gateway Appliance.
2. Log in with your on-premises credentials.
3. Navigate to the Certificate Management UI.
   a. From the **Home** menu, select **Administration**.
   b. Under **Certificates**, click **Certificate Management**.
4. Enter your credentials and click **Login and Manage Certificates**.
5. On the Machine SSL Certificate, select **Actions > Replace**.
6. Click the browse button on the Certificate Chain and provide the path of the certificate chain file.
   This file should contain the machine SSL certificate, the Root CA certificate, and the entire chain of trust.
7. Click the browse button on the private key and provide the private key for the certificate.
8 Click Replace.

What to do next

When the certificate is successfully replaced, restart all services on the Cloud Gateway Appliance. See https://kb.vmware.com/s/article/2109887.

Configuring Hybrid Linked Mode from the Cloud SDDC

As an alternative to using the Cloud Gateway Appliance, you can configure Hybrid Linked Mode from the cloud SDDC.

In this case, you use your cloud SDDC's vSphere Client to view and manage your complete inventory. When you link from the cloud SDDC, you can link only one on-premises domain.

Validate Network Connectivity for Hybrid Linked Mode

Use the VMC Console Connectivity Validator to check that all required network connectivity is in place for Hybrid Linked Mode.

When you provide the required inputs to the Connectivity Validator, it can verify the network connections required for Hybrid Linked Mode.

Procedure

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

2 Click View Details for your SDDC.

3 Click the Troubleshooting tab.

4 From the Use Case drop down menu, select Hybrid Linked Mode.

   The Hybrid Linked Mode connectivity tests are shown. Tests are organized into groups according to the input needed for each group.

5 In the Input column, enter the required input for each test you want to run.

6 Run one or more tests.
   - To run all tests, click Run All.
   - To run a particular test group, click Run Group to the right of the group listing.
   - To run an individual test, expand the test group and click Run next to the individual test.

Results

The status of each test is displayed as it runs. When a test has finished, you can expand the test to see details of the test results.

What to do next

When all tests pass, continue to set up Hybrid Linked Mode. See Add an Identity Source to the SDDC LDAP Domain.
Link to an On-Premises Data Center

To complete the configuration of Hybrid Linked Mode from the cloud SDDC, link your on-premises data center from your cloud vCenter Server.

Procedure

1. If you haven't already, log in to the vSphere Client for your SDDC and browse to the Linked Domains page.
   a. Select Menu > Administration to display the Administration page.
   b. Under Hybrid Cloud, select Linked Domains.

2. Connect to the on-premises vCenter Server.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platform Services Controller</td>
<td>Enter the IP address or FQDN of the Platform Services Controller instance in your on-premise data center.</td>
</tr>
<tr>
<td>HTTPS Port</td>
<td>Enter the HTTPS port used by the Platform Services Controller.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter the username for the on-premises SSO administrator.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password for the on-premises SSO administrator.</td>
</tr>
</tbody>
</table>

3. Add the groups you have defined in your on-premises environment to serve as cloud administrator groups.
   a. Select the on-premises identity source.
      - If you haven't already added the on-premises identity source, do so as described in Add an Identity Source to the SDDC LDAP Domain.
   b. Enter the name of the administrator group in the search box and select the group.

4. Click Link.

Add an Identity Source to the SDDC LDAP Domain

The first step toward configuring Hybrid Linked Mode from your SDDC is to add your on-premises LDAP domain as an identity source for the SDDC vCenter Server.

You can configure Hybrid Linked Mode from your SDDC if your on-premises LDAP service is provided by a native Active Directory (Integrated Windows Authentication) domain or an OpenLDAP directory service.

**Important** If you are using OpenLDAP as the identity source, see the VMware knowledge base article at [http://kb.vmware.com/kb/2064977](http://kb.vmware.com/kb/2064977) for additional requirements.
Prerequisites

Ensure that you meet the Common Prerequisites in Hybrid Linked Mode Prerequisites. You should also take a look at Identity Sources for vCenter Server with vCenter Single Sign-On in the VMware vSphere Product Documentation for additional information about configuring and using identity sources and certificates.

Procedure

1. Log in to the vSphere Client for your SDDC.
   
   To add an identity source, you must be logged in as cloudadmin@vmc.local or another member of the Cloud Administrators group.

2. Configure single sign-on to add an identity provider.
   
   Follow the steps in Add or Edit a vCenter Single Sign-On Identity Source in the VMware vSphere Product Documentation.

3. Configure the identity source settings.
   
   See Active Directory over LDAP and OpenLDAP Server Identity Source Settings for detailed information about the configuration parameters.

Results

When the identity source is added, on-premises users can authenticate to the SDDC, but have the No access role. Add permissions for a group of users to give them the Cloud Administrator role.

Troubleshooting Networking for Hybrid Linked Mode

You can use the network troubleshooting functionality in the VMC Console or as part of the Hybrid Linked Mode functionality in the Cloud Gateway Appliance to troubleshoot network connectivity for Hybrid Linked Mode.

Connectivity Validator: DNS Server Can't Be Reached

On-prem Primary DNS Server or On-prem Secondary DNS Server tests fail in the Connectivity Validator.

Problem

The tests Connectivity to On-prem Primary DNS Server on Port 53 and/or Connectivity to On-prem Secondary DNS Server on Port 53 in the Connectivity Validator fail with a message that says Port 53 Connection timed out.
Figure 3-1. Image of failed DNS Server connectivity test

Cause

Potential causes of this failure could be:

- The IPsec VPN connection from the cloud SDDC to the on-premises data center might be down.
- The DNS server port 53 is blocked by a firewall rule on the cloud SDDC or on-premises data center.
- You have entered an incorrect IP address for the DNS server.
- The DNS server is down.

Solution

1. Verify that the VPN tunnel from the cloud SDDC to on-premises is up. See View VPN Tunnel Status and Statistics.

2. Inspect the firewall rules in the VMC Console to ensure that access to port 53 on the on-premises DNS server is not blocked.

3. Inspect the firewall rules in your on-premises environment to ensure that access to port 53 on the on-premises DNS server is not blocked.

4. Verify that you entered the correct IP address for your on-premises DNS servers. See Specify Management Gateway DNS Servers.

5. Verify that your DNS server is running, and bring it back up if it is down.

Connectivity Validator: DNS Lookup Failure for a Given FQDN

The DNS lookup test for an on-premises vCenter Server, Platform Services Controller, Active Directory, or ESXi fails.

Problem

One or more DNS lookup tests fails. The Resolved Address field in the test results shows no result.
Figure 3-2. Example of DNS lookup test failure

Cause

If the DNS server reachability test succeeded, but the DNS lookup for a given FQDN fails, this could be caused by one of the following:

- The on-premises DNS server does not have an entry for the given FQDN.
- You entered an incorrect FQDN for the test.

Solution

1. Ensure that you entered the correct FQDN.
2. Check that the on-premises DNS server has an entry for the FQDN.

Connectivity Validator: Ping Failure for a Given FQDN

The test that pings an on-premises vCenter Server, Platform Services Controller, Active Directory, or ESXi fails.

Problem

A ping test for a given FQDN fails. Test details show that no responses to ICMP packets were received.

Figure 3-3. Example of a ping test failure
Cause

Potential causes of this failure could be:

- A firewall rule in the cloud SDDC or the on-premises data center might be blocking ICMP traffic.
- The remote system with the given FQDN is powered-off.

Solution

1. Check your firewall rules set in the VMC Console to ensure that they are not blocking ICMP traffic to the given FQDN.
2. Check your on-premises firewall rules to ensure that they are not blocking ICMP traffic to the given FQDN.
3. Check that the remote system being pinged is powered-on and functioning, and power on or restart if necessary.

Connectivity Validator: Port Reachability Failure for a Given FQDN

A test to reach a specific port on

Problem

A test for connectivity to a particular port at a given FQDN fails with the message Port *port-number* Connection timed out.

Figure 3-4. Example of a port reachability test failure

<table>
<thead>
<tr>
<th>Source</th>
<th>Test Group</th>
<th>Input</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>On-prem Primary DNS Server</td>
<td>9.8.7.6</td>
<td>Run Group</td>
</tr>
<tr>
<td>Source</td>
<td>On-prem Secondary DNS Server</td>
<td>9.8.7.6</td>
<td>Run Group</td>
</tr>
<tr>
<td>Source</td>
<td>On-prem Helper</td>
<td>9.8.7.6</td>
<td>Run Group</td>
</tr>
<tr>
<td>Source</td>
<td>Network</td>
<td>9.8.7.6</td>
<td>Run Group</td>
</tr>
</tbody>
</table>

Test Result

- **Success**
  1. PING group for 9.8.7.6
- **Failed**
  2. Ping to On-prem Helper (9.8.7.6) failed (9.8.7.6)
  3. Transient to On-prem Helper (9.8.7.6) failed (9.8.7.6)
  4. Connectivity to On-prem Helper (9.8.7.6) failed (9.8.7.6)

Test Result

- **Failed**
  1. Failed to connect

Cause

Potential causes of this failure could be:

- A firewall rule in the cloud SDDC or the on-premises data center might be blocking access to the port.
- The remote system with the given FQDN is powered-off.
Solution

1. Check your firewall rules set in the VMC Console to ensure that they are not blocking access to the specified port.

2. Check your on-premises firewall rules to ensure that they are not blocking access to the specific port.

3. Check that the remote system being pinged is powered-on and functioning, and power on or restart if necessary.

Connectivity Validator: Traceroute Failure for a given FQDN

A traceroute test to a given FQDN fails.

Problem

A traceroute test to an FQDN fails. In the test results, you can see hops to the destination listed without accompanying IP addresses.

Figure 3-5. Example of traceroute test failure

<table>
<thead>
<tr>
<th>Hybrid Link Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Traceroute Test Result" /></td>
</tr>
</tbody>
</table>

Causes

Potential causes of this failure could be:

- If the ping test to the FQDN itself is successful, a firewall rule in the cloud SDDC or the on-premises data center might be blocking ICMP traffic to one of the hops along the traffic path.

- The remote system with the given FQDN is powered-off.

Solution

1. Check your firewall rules set in the VMC Console to ensure that they are not blocking ICMP traffic to one of the hops along the traffic path.
Check your on-premises firewall rules to ensure that they are not blocking ICMP traffic to the one of the hops on the traffic path.

Check that the remote system is powered-on and functioning, and power on or restart if necessary.

**Connectivity Validator: Test Failure Due to Internal Error**

A test fails due to an internal error.

**Problem**

Any of the Connectivity Validator tests might fail with an error message beginning with *Internal Error:*

**Figure 3-6. Example of test failure due to internal error**

**Cause**

This error most commonly occurs when the Connectivity Validator experiences an internal connectivity problem.

**Solution**

Most of these failures are intermittent and resolve without you needing to do anything. However, if the error persists, contact VMware customer support.

**Unlink a Cloud SDDC**

You can unlink a cloud SDDC from Hybrid Linked Mode when you no longer want linking between your cloud SDDC and a particular on-premises data center.
For example, you might want to link an on-premises data center to your SDDC in order to migrate virtual machines to the SDDC, and then unlink the on-premises data center. If you plan to decommission a linked on-premises data center, unlink it before doing so.

**Note** Unlinking an on-premises data center from the cloud SDDC does not remove the associated identity source or permissions that you added before linking the domain. Users can still use their on-premises credentials to authenticate to your SDDC, and retain the permissions granted to them. However, they are not able to view the on-premises inventory after unlinking the domain. When you unlink a cloud SDDC from the Cloud Gateway Appliance, users can't use their on-premises credentials to log into the cloud SDDC any longer.

Unlinking also leaves tags and categories in place, because VMs in your cloud SDDC might still be using those tags.

**Prerequisites**

Ensure that you have network connectivity between your SDDC management gateway and your SSO Domain.

**Procedure**

1. Log into the appropriate system.
   - If you linked your cloud SDDC and your on-premises data center from the Cloud Gateway Appliance, log into the Cloud Gateway Appliance UI.
   - If you linked your cloud SDDC and your on-premises data center from the cloud vCenter Server, log in to the vSphere Client for your SDDC.

2. Browse to the Linked Domains page.
   - Select **Menu > Administration** to display the Administration page.
   - Under **Hybrid Cloud**, select **Linked Domains**.

3. Under the name of the linked domain, click **Unlink**.
   - A dialog box appears asking you to confirm the unlinking. Note that all currently active sessions are logged out when you unlink a domain.

4. Click **OK**.
   - When the unlinking is complete, you are prompted to log out.

5. Click **OK** to log out.
Results

The SSO domain is unlinked. If you want to continue using Hybrid Linked Mode, you can link to another SSO domain or relink to the same domain.

**Note** After you unlink from the cloud SDDC, new connections to the cloud SDDC vSphere Client cannot view or interact with previously-linked on-premises resources. Currently active sessions in the cloud SDDC vSphere Client continue to be able to view and interact with resources in the previously linked on-premises vCenter Server instances until the users of those sessions log out of the cloud SDDC vSphere Client or the sessions expire. If necessary, log in to each of the previously-linked on-premises vCenter Server instances, and forcibly terminate these sessions.

After you unlink from the Cloud Gateway Appliance, new connections to the Cloud Gateway Appliance cannot view or interact with previously-linked cloud resources. Currently active sessions in the Cloud Gateway Appliance continue to be able to view and interact with resources in the cloud SDDC until the users of those sessions log out or the sessions expire. If necessary, log in to the Cloud Gateway Appliance and forcibly terminate these sessions.
In an on-premises vSphere environment, you configure clusters to group ESXi hosts and to set vSphere HA, vSphere DRS, and other cluster features. You use resource pools group resources. In a VMware Cloud on AWS environment, VMware creates a single cluster with a preset configuration. VMware creates a resource pool for compute VMs and a second resource pool for management VMs. You can view cluster and resource pool settings and create and configure child resource pools.

What you can do in VMware Cloud on AWS depend on what you select.
Table 4-1. Supported Tasks on Clusters and Resource Pools in VMware Cloud on AWS

<table>
<thead>
<tr>
<th>Object</th>
<th>Supported Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster</td>
<td>A VMware Cloud on AWS environment has one cluster that includes all ESXi hosts that are part of your SDDC.</td>
</tr>
<tr>
<td></td>
<td>- View the cluster configuration, including vSphere DRS and vSphere HA. The clouadmin user cannot change the cluster configuration.</td>
</tr>
<tr>
<td></td>
<td>- Examine all hosts and all resource pools that are associated with the cluster. You can see the consumed memory and CPU, HA state, and uptime.</td>
</tr>
<tr>
<td></td>
<td>- Examine VMs, datastores, and networks that are associated with the cluster.</td>
</tr>
<tr>
<td></td>
<td>- Set tags and attributes. See vSphere Tags and Attributes.</td>
</tr>
<tr>
<td>Resource pool</td>
<td>A VMware Cloud on AWS environment has two predefined resource pools. You can perform the following tasks:</td>
</tr>
<tr>
<td></td>
<td>- Create new virtual machines and child resource pools.</td>
</tr>
<tr>
<td></td>
<td>- Change resource allocation settings on child resource pools</td>
</tr>
<tr>
<td></td>
<td>- Rename the resource pools to better match company policy.</td>
</tr>
<tr>
<td></td>
<td>- Monitor the resource pool, its VMs, and its child resource pools, and examine resource pool utilization.</td>
</tr>
<tr>
<td></td>
<td>- Set tags and attributes. See vSphere Tags and Attributes.</td>
</tr>
</tbody>
</table>

Note  Some menu options, such as Delete, are available on top-level resource pools but have no effect. As clouadmin@vmc.local, you do not have permissions to perform those tasks. A warning appears in the Alarms window.

This chapter includes the following topics:
- Predefined Clusters and Resource Pools
- Examine VMs and Hosts in the Cluster
- Examine and Monitor vSphere DRS
- Examine and Monitor vSphere HA
- Examine Cluster Configuration
- Create and Manage Child Resource Pools

Predefined Clusters and Resource Pools

Your VMware Cloud on AWS SDDC initially includes a single cluster, named Cluster-1, that contains two resource pools. Additional clusters that you create are numbered sequentially, Cluster-2, Cluster-3, and so on.
A vSphere cluster organizes and manages all CPU, memory, and storage resources of a set of hosts. Each cluster supports multiple resource pools. A resource pool is logical abstraction for flexible management of resources. Resource pools can be grouped into hierarchies and used to hierarchically partition available CPU and memory resources. See Managing Resource Pools in the vSphere Product Documentation more information.

On creation, Cluster-1 has two predefined resource pools. They share the same physical hardware but are dedicated to different uses.

**Mgmt-ResourcePool**

This resource pool is always created in Cluster-1, and never consumes resources from other clusters. Resources in this pool are reserved for management VMs so that they can operate without consuming resources from the Compute-ResourcePool. For a summary of resources consumed by management VMs, see the SDDC vCPUs and SDDC RAM values in VMware Configuration Maximums.

**Compute-ResourcePool**

This resource pool is initially created in Cluster-1. By default, all workload virtual machines are created in the top-level (root) Compute-ResourcePool. Each additional cluster that you create starts with its own top-level Compute-ResourcePool. You can create child resource pools of any Compute-ResourcePool to give you more control over fine-grained allocation of compute resources.

### Examine VMs and Hosts in the Cluster

In an VMware Cloud on AWS environment, you can examine the VMs and hosts in a cluster.

**Procedure**

1. In the vSphere Client, click **Menu** and select **Hosts and Clusters**.
2. Select **Cluster-1**.
   
   In VMware Cloud on AWS, **Cluster-1** holds configuration settings for all SDDC clusters.
3. Click **VMs** to examine virtual machines and vApps.
   
   a. Check how much CPU and memory that each VM is consuming, and check the allocated and used storage.
   b. Right-click a down arrow in the title bar to show or hide columns in this display.
   c. If you want to make changes to a VM or vApp, select it, right-click the VM in the object hierarchy, click **Settings**, and make the change.

   See the Virtual Machine Management documentation for VMware Cloud on AWS for details.
4 Click **Hosts** to see the resource that the hosts in the cluster are consuming.

You can request additional hosts if current resource usage shows that you’ll need them soon.

**Examine and Monitor vSphere DRS**

vSphere DRS ensures optimal resource allocation across the VMs in your SDDC. In an on-premises environment, you can configure several options, for example, you can use fully automated DRS or decide to receive recommendations. In a VMware Cloud on AWS SDDC, VMware has preconfigured the vSphere DRS options for the cluster of hosts.

VMware has selected settings that ensure optimal resource distribution while minimizing the number of migrations that occur. You don’t have to - and you can’t - change those selections. You might find it interesting to look at the preconfigured values.

**Note** For a seamless user experience, the screens for configuring, monitoring, and examining clusters and resource pools are the same in an on-premises SDDC and in a VMware Cloud on AWS SDDC. However, the **Edit** button is grayed out for VMware Cloud on AWS.

**Procedure**

1. In the vSphere Client, click **Menu** and select **Hosts and Clusters**.

2. Select **Cluster-1**.

   In VMware Cloud on AWS, **Cluster-1** holds configuration settings for all SDDC clusters.

3. Examine the DRS settings, which fully automate resource allocation across the cluster.

   The UI explains the background information. For detailed information, see the vSphere Resource Management documentation.

**Examine and Monitor vSphere HA**

vSphere High Availability (HA) ensures availability of the virtual machines in your SDDC. If a host fails, vSphere HA restarts its VMs on a different host. In a VMware Cloud on AWS SDDC, vSphere HA is enabled by default on all clusters, and cannot be disabled.

To ensure availability of all workload and management VMs in your SDDC, VMware Cloud on AWS must maintain sufficient capacity to power them on in the event of host failure. HA admission control is the primary mechanism for capacity maintenance. Admission control imposes constraints on resource usage, and can prevent any action that consumes more resources than the cluster can support during a failover. These constraints apply to actions like powering on or migrating a VM, or reserving additional CPU or memory resources for a VM, and effectively limit the availability of host resources as shown here:

- In a two-host SDDC cluster, admission control prevents you from powering-on more than 36 VMs or assigning more than 1152 MHz CPU reservation to a single VM.
In SDDC clusters with three to five hosts, admission control reserves one host for failover.

In SDDC clusters of six or more hosts, two hosts are reserved for failover.

For additional details about system limits, see VMware Configuration Maximums.

For a detailed discussion of vSphere HA and other features that ensure availability in an on-prem vSphere environment, see How vSphere HA Works in the VMware vSphere Product Documentation. Although most HA settings in VMware Cloud on AWS are managed for you by VMware and cannot be changed in your SDDC's vCenter Server, it's important to understand the fundamental concepts of vSphere HA and how they apply to workload deployment in your SDDC.

Procedure

1. In the vSphere Client, click Menu and select Hosts and Clusters.

2. Select Cluster-1.

   In VMware Cloud on AWS, Cluster-1 holds configuration settings for all SDDC clusters.

3. (Optional) Examine the vSphere HA settings, which are optimized for VMware Cloud on AWS.

   Although you cannot modify these settings, familiarity with them makes it easier for you to understand how VMs are deployed across the clusters in your SDDC.

4. Click the vSphere HA Monitoring link for more information on vSphere HA events.

Examine Cluster Configuration

In your VMware Cloud on AWS SDDC, you can examine all cluster configuration details that you can view and change in an on-premises deployment.

**Note**  For a seamless user experience, the screens for configuring, monitoring, and examining clusters and resource pools are the same in an on-premises SDDC and in a VMware Cloud on AWS SDDC. However, the Edit button is grayed out for VMware Cloud on AWS.

Procedure

1. In the vSphere Client, click Menu and select Hosts and Clusters.

2. Select Cluster-1.

   In VMware Cloud on AWS, Cluster-1 holds configuration settings for all SDDC clusters.
3  Examine the following settings.

<table>
<thead>
<tr>
<th>Configuration Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>Displays the predefined swap file location and VM Compatibility settings.</td>
</tr>
<tr>
<td>VMware EVC</td>
<td>VMware Enhanced vMotion Compatibility is disabled. The hosts are uniform, so vMotion Compatibility problems do not occur.</td>
</tr>
<tr>
<td>VM/Host Groups</td>
<td>The administrators of your VMware Cloud on AWS environment create rules to ensure that certain virtual machines never run on the same rules. You can view those rules, but you cannot create rules.</td>
</tr>
<tr>
<td>VM/Host Rules</td>
<td>VM Overrides change the behavior of certain VMs. For example, the vCenter VM has the highest vSphere HA Restart Priority. You can view the overrides that the VMware Cloud on AWS administrator set for some system VMs. You cannot specify overrides for your own VMs.</td>
</tr>
<tr>
<td>VM Overrides</td>
<td>VM Overrides change the behavior of certain VMs. For example, the vCenter VM has the highest vSphere HA Restart Priority. You can view the overrides that the VMware Cloud on AWS administrator set for some system VMs. You cannot specify overrides for your own VMs.</td>
</tr>
<tr>
<td>Host Options</td>
<td>Displays host options, including some information about the host.</td>
</tr>
<tr>
<td>Host Profile</td>
<td>All ESXi hosts are managed by VMware and are set up in a uniform fashion. Host profiles are not required.</td>
</tr>
</tbody>
</table>

Create and Manage Child Resource Pools

Resource pools allow you perform resource allocation depending on the needs of different groups. You can create a hierarchy of child resource pools for the top-level compute resource pool, called Compute-ResourcePool by default. You can specify resource settings when you create a resource pool, and you can change those settings later.

For example, assume a host has a number of virtual machines. The marketing department uses three of the virtual machines and the QA department uses two virtual machines. Because the QA department needs larger amounts of CPU and memory, the administrator creates one resource pool for each group. The administrator sets CPU Shares to High for the QA department pool and to Normal for the Marketing department pool so that the QA department users can run automated tests. The second resource pool with fewer CPU and memory resources is sufficient for the lighter load of the marketing staff. Whenever the QA department is not fully using its allocation, the marketing department can use the available resources.

The numbers in the following figure show the effective allocations to the resource pools.
Figure 4-1. Parent Resource Pools and Child Resource Pools

Compute Resource-Pool
6GHz, 30GB

RP-QA
4GHz, 20GB

VM
QA 1

VM
QA 2

RP-Marketing
2GHz, 10GB

VM
Marketing 1

VM
Marketing 2

VM
Marketing 3
Procedure

1 Start the task.

<table>
<thead>
<tr>
<th>Task</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a resource pool</td>
<td>Right-click the parent resource pool and select <strong>New Resource Pool</strong>.</td>
</tr>
<tr>
<td>Edit resource pool settings</td>
<td>Right-click a resource pool and select <strong>Edit Resource Settings</strong>.</td>
</tr>
</tbody>
</table>

**Note**: If you edit the settings of a system-defined resource pools, the changes do not take effect.

2 Specify how to allocate CPU and memory resources.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name for this resource pool.</td>
</tr>
</tbody>
</table>
| Shares | Specify shares for this resource pool with respect to the parent’s total resources. Sibling resource pools share resources according to their relative share values bounded by the reservation and limit.  
  - Select **Low**, **Normal**, or **High** to specify share values respectively in a 1:2:4 ratio.  
  - Select **Custom** to give each virtual machine a specific number of shares, which expresses a proportional weight. |
| Reservation | Specify a guaranteed CPU or memory allocation for this resource pool. "Defaults to 0.  
  A nonzero reservation is subtracted from the unreserved resources of the parent (host or resource pool). The resources are considered reserved, regardless of whether virtual machines are associated with the resource pool. |
| Expandable Reservation | When the check box is selected (default), expandable reservations are considered during admission control.  
  If you power on a virtual machine in this resource pool, and the combined reservations of the virtual machines are larger than the reservation of the resource pool, the resource pool can use resources from its parent or ancestors. |
| Limit | Specify the upper limit for this resource pool’s CPU or memory allocation.  
  You can usually accept the default (**Unlimited**).  
  To specify a limit, deselect the **Unlimited** check box. |

3 Click **OK**.
vSAN Storage in VMware Cloud on AWS

VMware Cloud on AWS provides two vSAN datastores in each SDDC cluster: WorkloadDatastore, managed by the Cloud Administrator, and vsanDatastore, managed by VMware.

These datastores are logical entities that share a common capacity pool. Each datastore reports the total available free space in the cluster as its **Capacity**. Capacity consumed in either datastore updates the **Free** value for both.

**vsanDatastore**

This datastore provides storage for the management VMs in your SDDC, such as vCenter Server, NSX controllers, and so on.

The management and troubleshooting of the vSAN storage in your SDDC is handled by VMware. For this reason, you can't edit the vSAN cluster settings or monitor the vSAN cluster. You also do not have permission to browse this datastore, upload files to it, or delete files from it.

**WorkloadDatastore**

This datastore provides storage for your workload VMs, templates, ISO images, and any other files you choose to upload to your SDDC. You have full permission to browse this datastore, create folders, upload files, delete files, and perform all other operations needed to consume this storage.

The datastores in your SDDC are assigned the default VM storage policy by default. You can define additional storage policies and assign them to either datastore. For more information on vSAN storage policies, see **Using vSAN Policies**.

This chapter includes the following topics:

- Storage Capacity and Data Redundancy
- vSAN Deduplication and Compression
- Enabling TRIM/UNMAP Commands for VMware Cloud on AWS Clusters
- vSAN Encryption in VMware Cloud on AWS
vSAN Policies

Shared Storage Clusters on vSAN

Storage Capacity and Data Redundancy

SDDC storage capacity and data redundancy scale with the number of nodes in the SDDC.

Single node SDDCs provide no data redundancy. SDDCs with more nodes support data redundancy through various RAID configurations. All SDDC storage provides data deduplication, data compression, or both. Data redundancy in SDDCs that have more than one host is expressed as a number of failures to tolerate (FTT), where a failure can be the loss of a single host in a cluster or a single storage device in an array.

All RAID configurations consume data to support redundancy. You can calculate the projected capacity needs for your workloads based on the host instance type, cluster configuration, and failure tolerance settings using the VMware Cloud on AWS Sizer and TCO tool found at https://vmc.vmware.com/sizer/workload-profiles.

vSAN Deduplication and Compression

vSAN performs block-level deduplication and compression to save storage space. This allows you to make more efficient and cost-effective use of storage in your VMware Cloud on AWS SDDC.

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

Deduplication and compression are automatically enabled for VMware Cloud on AWS clusters containing i3 hosts and cannot be turned off. In clusters that use Elastic vSAN, deduplication is restricted to the removal of zero blocks. Redundant blocks that contain data are not deduplicated. Clusters containing i3en hosts are automatically enabled for compression only. Enabling compression without deduplication improves performance. It also allows for increased availability, because the fault domain can be restricted to a single disk rather than a disk group.

Deduplication occurs inline when data is written back from the cache tier to the capacity tier. The deduplication algorithm uses a fixed block size and is applied within each disk group. Redundant copies of a block within the same disk group are deduplicated.

Storage savings resulting from deduplication and compression are highly dependent on the workload data. On average, storage space savings are in the range of 1.5X to 2X.
Enabling TRIM/UNMAP Commands for VMware Cloud on AWS Clusters

Support for TRIM and UNMAP commands allows vSAN clusters to reclaim space when files are deleted in a VM or when space is allocated for multiple writes to the same file.

Provisioning virtual machines with thin-provisioned disks allows you to conserve storage space. The disk starts small, and expands to accommodate the storage space needed by the guest operating system, up to the maximum disk size allocated.

Even with thin provisioning, there are obstacles to a fully efficient use of storage space in VM disks. By default, the VM disk does not shrink when files are deleted in the guest operating system. In addition, many guest operating systems always direct new writes to free disk blocks. This can cause a small file that is frequently written to, such as a log file, to grow to consume a large amount of disk space.

The guest operating system can send TRIM/UNMAP commands to allow the virtual machine disk to reclaim previously used space as free disk space.

By default, support for these commands is not enabled. To request that this feature be enabled for your SDDC, contact your VMware account team. The feature is enabled on a per-cluster basis. You must reboot the workload VMs in the cluster to allow them to take advantage of this feature after enablement.

When deleting large files or performing a scheduled space reclamation job to reclaim a large block of capacity, the space reclamation process can affect production workloads. This most often manifests as increased latencies. If possible, schedule large space reclamation jobs during off-peak hours to reduce any potential impact. After it has caught up, the system can process in-line deletes without incurring significant penalties.

vSAN Encryption in VMware Cloud on AWS

vSAN encrypts all user data at rest in VMware Cloud on AWS.

Encryption is enabled by default on each cluster deployed in your SDDC, and can't be turned off. When you deploy a cluster, vSAN uses the AWS Key Management Service (AWS KMS) to generate a Customer Master Key (CMK), which is stored by AWS KMS. vSAN then generates a Key Encryption Key (KEK) and encrypts it using the CMK. The KEK is in turn used to encrypt Disk Encryption Keys (DEKs) generated for each vSAN disk.

You can change KEKs by using either the vSAN API or the vSphere Client UI. This process is known as performing a shallow rekey. Changing the CMK or DEKs is not supported. If you must change the CMK or DEKs, create a new cluster and migrate your VMs and data to it.

Generate New Encryption Keys in VMware Cloud on AWS

You can generate new Key Encryption Keys (KEKs) for your VMware Cloud on AWS cluster if needed.
This process is known as performing a shallow rekey. Changing the CMK or DEKs is not supported. If you must change the CMK or DEKs, create a new cluster and migrate your VMs and data to it.

**Procedure**

1. Log in to the vSphere Client for your cloud SDDC.
2. Navigate to the vSAN cluster.
3. Click the **Configure** tab.
4. Under vSAN, select **Services**.
5. Click **Generate New Encryption Keys**.
6. Click **Apply** to generate a new KEKs.

The Disk Encryption Keys (DEKs) are re-encrypted with the new KEKs.

**Example: Using VMware PowerCLI for this Task**

If you know the cloudadmin password, you can use a PowerCLI command like this one to do a shallow re-key for the vSAN service. This example, based the Vsan-EncryptionRekey.psl code sample you can download from [https://code.vmware.com/samples/2200#code](https://code.vmware.com/samples/2200#code), re-keys the vSAN service running on Cluster-1 of SDDC vCenter vcenter.sddc-54-200-165-35.vmwarevmc.com:

```
PS > ./Vsan-EncryptionRekey.psl -vCenter vcenter.sddc-54-200-165-35.vmwarevmc.com -User cloudadmin@vmc.local -Password cloudadmin-password -ReKey shallow -ClusterName Cluster-1
```

**vSAN Policies**

vSAN storage policies define storage requirements for your virtual machines. These policies guarantee the required level of service for your VMs because they determine how storage is allocated to the VM.

VMware Cloud on AWS includes two vSAN datastores, one for the management VMs (vsanDatastore) and one for the workload VMs (WorkloadDatastore). Both datastores share the same underlying storage devices and consume from the same pool of free space.

Each virtual machine deployed to a vSAN datastore is assigned at least one virtual machine storage policy. You can assign storage policies when you create or reconfigure virtual machines.

Storage policies have availability attributes and advanced attributes.

**Availability Attributes for vSAN VM Storage Policies**

**Site disaster tolerance**

Defines the data redundancy method used by stretched clusters to handle a site failure. This attribute applies to stretched clusters. If you have a standard vSAN cluster, choose None (standard cluster).
The options are:

- None (standard cluster)
- Dual-site mirroring (stretched cluster)
- None - Keep data on primary (stretched cluster)
- None - Keep data on secondary (stretched cluster)

**Failures to tolerate**

Defines the number of host and device failures that a virtual machine can tolerate. You can choose to have no data redundancy, or select a RAID configuration optimized for either performance (Mirroring) or capacity (Erasure Coding).

- RAID-1 uses more disk space to place the components of objects but provides better performance for accessing the objects.
- RAID-5/6 (Erasure Coding) uses less disk space, but the performance is reduced.

**Table 5-1. RAID Configurations, FTT, and Host Requirements**

<table>
<thead>
<tr>
<th>RAID Configuration</th>
<th>Failures to Tolerate (FTT)</th>
<th>Minimum Hosts Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAID-1 (Mirroring)</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>RAID-5 (Erasure Coding)</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>RAID-1 (Mirroring)</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>RAID-6 (Erasure Coding)</td>
<td>2</td>
<td>6</td>
</tr>
<tr>
<td>RAID-1 (Mirroring)</td>
<td>3</td>
<td>7</td>
</tr>
</tbody>
</table>

**Note** VMs with FTT = 0 (No Data Redundancy) might experience data loss if there is a failure or if the VM becomes unresponsive.

The Managed Storage Policy Profile determines the initial RAID configuration of a cluster. When a Managed Storage Policy Profile is applied to the cluster, the RAID configuration is updated automatically as the cluster size changes. See [VMware Cloud on AWS Managed Storage Policy Profiles](#) for details.

**Advanced Attributes for vSAN VM Storage Policies**

**Number of disk stripes per object**

Minimum number of capacity devices across which each replica of a virtual machine object is striped. A value higher than 1 might result in better performance, but also results in higher use of system resources. Default value is 1. Maximum value is 12. Change the default value only when recommended by VMware support.

**IOPS limit for object**
Defines the IOPS limit for an object, such as a VMDK. IOPS is calculated as the number of I/O operations, using a weighted size. If the system uses the default base size of 32 KB, a 64-KB I/O represents two I/O operations.

When calculating IOPS, read and write are considered equivalent, but cache hit ratio and sequentiality are not considered. If a disk’s IOPS exceeds the limit, I/O operations are throttled. If the IOPS limit for object is set to 0, IOPS limits are not enforced.

vSAN allows the object to double the rate of the IOPS limit during the first second of operation or after a period of inactivity.

Object space reservation

This setting defines the percentage of the logical size of the virtual machine disk (vmdk) object that must be reserved (provisioned) when deploying virtual machines. The default reservation value in VMware Cloud on AWS is 0% (Thin provisioning). You can specify Thick provisioning to reserve capacity for larger-than-expected vSAN writes, but the underlying vmdk structure remains the same as it is in the Thin provisioning configuration, and is not the same as the Thick provision eager zeroed provisioning model available on-premises.

Flash read cache reservation

This setting is ignored in VMware Cloud on AWS. In Hybrid vSan deployments, it designates how much flash capacity is reserved as read cache.

Disable object checksum

If the option is set to No, the object calculates checksum information to ensure the integrity of its data. If this option is set to Yes, the object does not calculate checksum information.

vSAN uses end-to-end checksum to ensure the integrity of data by confirming that each copy of a file is exactly the same as the source file. The system checks the validity of the data during read/write operations, and if an error is detected, vSAN repairs the data or reports the error.

If a checksum mismatch is detected, vSAN automatically repairs the data by overwriting the incorrect data with the correct data. Checksum calculation and error-correction are performed as background operations.

The default setting for all objects in the cluster is No, which means that checksum is enabled.

Force provisioning

If the option is set to Yes, the object is provisioned even if the Primary level of failures to tolerate, Number of disk stripes per object, and Flash read cache reservation policies specified in the storage policy cannot be satisfied by the datastore. Use this parameter in bootstrapping scenarios and during an outage when standard provisioning is no longer possible.

The default No is acceptable for most production environments. vSAN fails to provision a virtual machine when the policy requirements are not met, but it successfully creates the user-defined storage policy.
VMware Cloud on AWS Managed Storage Policy Profiles

When you create a cluster in your SDDC, VMware Cloud on AWS creates a managed storage policy profile that is applied by default to VMs that you create in the cluster. This storage policy profile is named "VMC Workload Storage Policy - cluster name". The policy settings ensure that the cluster meets the requirements outlined in the Service Level Agreement for VMware Cloud on AWS (the SLA). When you migrate a VM to a different cluster in the same SDDC, you must also change the VM storage policy. See Assign Storage Policies to Virtual Machines

Managed storage policy settings are based on the cluster configuration:

- Single host SDDCs are not covered by the SLA. They use a No data redundancy policy.
- Single-AZ clusters use thin provisioning and set a failure tolerance value based on cluster size and the host instance type:
  - Clusters using Elastic VSAN storage use 1 failure - RAID-1 (Mirroring) policy, regardless of cluster size.
  - Clusters using non-Elastic VSAN storage containing 3 to 5 hosts use 1 failure - RAID-1 (Mirroring).
  - Clusters using non-Elastic VSAN storage containing 6 or more hosts use 2 failures - RAID-6 (Erasure Coding).
- Stretched clusters use 1 failure - RAID-1 (Mirroring), but also have Site Disaster Tolerance set to Dual Site Mirroring.

Because the managed storage policy for non-Elastic VSAN clusters varies based on cluster size, adding or removing hosts will trigger a storage policy reconfiguration if it changes the size of the cluster so that it requires a different policy. For example, if you add an additional host to a cluster containing five i3.metal hosts, the storage policy for that cluster is reconfigured from using 1 failure - RAID-1 (Mirroring) to 2 failures - RAID-6 (Erasure Coding). The reverse happens if the extra host is removed and the number of hosts is reduced from six to five.

**Note** When you make a change to a cluster that triggers a managed storage policy reconfiguration, the reconfiguration temporarily requires additional storage. If the cluster is close to 75% storage capacity, this might trigger an EDRS scale out event, adding a host to the cluster. After the reconfiguration is completed, EDRS might not remove the additional host. Check your clusters after storage reconfiguration, and remove the additional host if necessary.

For a non-Elastic VSAN cluster with 6 or more hosts, you cannot remove a host if the cluster storage utilization is greater than 40% of the total storage capacity. For all other types of cluster, VMware strongly recommends that you do not remove a host if the cluster storage utilization is greater than 40% of the total storage capacity.
If you remove one or more hosts from a cluster, and that triggers a managed storage policy reconfiguration, the reconfiguration must complete before the host or hosts are removed. If your workloads use a large amount of storage, this reconfiguration could take anywhere from hours to days to complete. During this time, any hosts you have designated to be removed remain usable and you are still billed for host usage. After the storage policy reconfiguration completes, the host or hosts are removed and you are no longer billed for the host usage.

**Note** Do not edit the managed storage policies that VMware Cloud on AWS creates for your clusters. If you rename the policy, it is no longer managed by VMware Cloud on AWS. If you edit the settings of the managed storage policy, your changes are overwritten at the next storage policy reconfiguration.

If you do not want to use the managed storage policy, you can define your own storage policy and assign it as the default for the workload datastore. See https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.vsphere.vsan.doc/GUID-F52F0AE9-FB31-4236-B566-D9610B14C670.html.

**VM Templates and Managed Storage Policies**

If a VM template is associated with a VMware Cloud on AWS managed storage policy, the template's policy is not automatically updated if the cluster's policy is reconfigured. After the cluster's storage policy is reconfigured, the VM template compliance status is "Out of Date". To make the template policy status "Compliant", you must convert the template to a VM, reapply the VM storage policy, and then convert the VM back to a template.

When you deploy a VM from a template, VMware recommends that you select **Datastore Default** for the VM Storage Policy in order to ensure that the VM is deployed with the current cluster managed storage policy.

**Storage Policies and SLA Requirements**

When working with virtual machine storage policies, it's important to understand how they affect the consumption of storage capacity in the vSAN cluster and whether they meet the requirements defined in the Service Level Agreement for VMware Cloud on AWS (the SLA).

The managed storage policy is initially configured based on the number of hosts in the cluster. For example, a three-host cluster defaults to FTT=1 using the RAID-1 Mirroring policy. Clusters with more than six i3.metal hosts in a single AZ default to **2 failures - RAID-6 (Erasure Coding)**. You can create custom policies that align data availability with the needs of your underlying data,
but workload VMs with storage policies that do not meet the requirements set forth in the Service Level Agreement may not qualify for SLA Credits. The VM Storage Policy must be configured with the appropriate level of protection. Ephemeral workloads may use the No Data Redundancy policy to save capacity, foregoing any SLA guarantees of availability.

**Important** When scaling an i3.metal cluster up from five to six hosts, the failure tolerance for the underlying policy must be updated to **2 failures - RAID-6 (Erasure Coding)** or **2 failures - RAID-6 (Mirroring)** to compensate for the larger failure pool. Clusters using the managed storage policy will be reconfigured automatically, but you must manually update any clusters that use custom policies. Continued use of a failure toleration of 1 for this host configuration means that VMware cannot guarantee availability per the service definition guidance. R5.metal clusters using Elastic vSAN are able to sustain the SLA with failure toleration of 1 for any cluster size of three hosts or more.

For more information about designing and sizing considerations of storage policies, see the *Administering VMware vSAN* documentation.

**Define a Virtual Machine Storage Policy for vSAN**

You can create a storage policy that defines storage requirements for a VM and its virtual disks. In this policy, you reference storage capabilities supported by the vSAN datastore.

**Procedure**

1. In the vSphere Client, click **Menu > Policies and Profiles**, then click **VM Storage Policies**.
2. Click **Create VM storage policy**.
3. On the Name and description page:
   a. Leave the vCenter Server selected.
   b. Type a name and a description for the storage policy, and click **Next**.
4. On the vSAN page, specify the **Availability** and **Advanced** attributes and click **Next**.
   The defaults are appropriate for many situations. See *vSAN Policies* for details on each attribute.
5. On the Storage compatibility page, review the list of datastores that match this policy and click **Next**.
   To be eligible, a datastore does not need to satisfy all rule sets within the policy. The datastore must satisfy at least one rule set and all rules within this set. Verify that the vSAN datastore meets the requirements set in the storage policy and that it appears on the list of compatible datastores.
6. On the Ready to complete page, review the policy settings, and click **Finish**.
What to do next

Assign this policy to a virtual machine and its virtual disks. vSAN places the virtual machine objects according to the requirements specified in the policy. For information about applying the storage policies to virtual machine objects, see the vSphere Storage documentation.

Assign Storage Policies to Virtual Machines

You can assign a VM storage policy in an initial deployment of a virtual machine or when you perform other virtual machine operations, such as cloning or migrating.

This topic describes how to assign the VM storage policy when you create a virtual machine. For information about other deployment methods that include cloning, deployment from a template, and so on, see the vSphere Virtual Machine Administration documentation.

You can apply the same storage policy to the virtual machine configuration file and all its virtual disks. If storage requirements for your virtual disks and the configuration file are different, you can associate different storage policies with the VM configuration file and the selected virtual disks.

**Important** When migrating VM's between clusters in the same SDDC, you must also change the VM storage policy to the destination cluster's managed policy. The default option of Keep existing VM Storage Policies is only appropriate if using a custom policy; otherwise, select the policy assigned to the destination cluster.

Procedure

1. In the vSphere Client, start the virtual machine provisioning process and follow the appropriate steps.
2. Assign the same storage policy to all virtual machine files and disks.
   a. On the Select storage page, select a storage policy from the VM Storage Policy drop-down menu.
      Based on its configuration, the storage policy separates all datastores into compatible and incompatible sets. If the policy references data services offered by a specific storage entity, for example, Virtual Volumes, the compatible list includes datastores that represent only that type of storage.
   b. Select an appropriate datastore from the list of compatible datastores.
      The datastore becomes the destination storage resource for the virtual machine configuration file and all virtual disks.
3. Change the VM storage policy for the virtual disk.

   Use this option if requirements for storage placement are different for virtual disks. You can also use this option to enable I/O filter services, such as caching and replication, for your virtual disks.

   a. On the Customize hardware page, expand the New hard disk pane.

   b. From the VM storage policy drop-down menu, select the storage policy to assign to the virtual disk.

4. Complete the virtual machine provisioning process.

Results

After you create the virtual machine, the Summary tab displays the assigned storage policies and their compliance status.

What to do next

If storage placement requirements for the configuration file or the virtual disks change, you can later modify the virtual machine policy assignment.

Shared Storage Clusters on vSAN

VMware Cloud on AWS supports SCSI-3 Persistent Reservations for workload VMs. You need to use this capability when configuring a Windows Server Failover Cluster (WSFC) in your SDDC.

Most of what you need to know to configure workload VMs to support WSFC is explained in About Setup for Windows Server Failover Clustering on VMware vSphere in the vSphere Product Documentation. This topic adds a few steps that you'll need to follow if you want to configure WSFC to use the vSAN storage in your SDDC.

A Windows Server Failover Cluster uses SCSI-3 Persistent Reservations to arbitrate shared access to clustered disk resources. To make this work, VMs in the cluster must meet several configuration requirements:

- To enable use of SCSI-3 Persistent Reservations, shared disks must be accessed through a SCSI controller with SCSI Bus Sharing set to Physical.

- To prevent unsupported snapshots operations on the shared disks, the Disk Mode of all disks in the cluster must be set to Independent – Persistent.

In a VMware Cloud on AWS SDDC, vSAN supports SCSI-3 Persistent Reservations on up to six application nodes per guest cluster with up to 64 shared disks.

Note: When a VMDK is shared using SCSI-3 Persistent Reservations, VM operations such as snapshots, storage vMotion to or from a vSAN datastore, cloning, hot extension of a hard disk, and replication through vSphere Replication are not supported. See VMware Knowledge Base article 79616 for a detailed discussion of supported configurations.

You must not enable VMDK multi-writer on WSFC disk resources.
For a thorough discussion architectural guidelines and detailed stepwise procedures for configuring and migrating WSFC workloads on VMware Cloud on AWS, see the VMware Technical Article Microsoft SQL Server Workloads and VMware Cloud on AWS: Design, Migration, and Configuration and the VMware blog post Native SQL Server Cluster support on vSAN.

Procedure

1. Configure the first node in the cluster.
   
   Follow the steps in Add Hard Disks to the First Node for Cluster Across Physical Hosts with Clustered VMDKs on VMFS Datastores with these additions:
   
   a. After Step 12, set the Disk Mode to Independent – Persistent.
   
   b. (Optional) Assign the disk a custom VM storage policy.
      
      While not a requirement, it's likely that any data that you need to protect with WSFC would benefit from having a dedicated storage policy.

2. Configure additional nodes.
   
   Follow the steps in Add Hard Disks to Additional Nodes for Clusters Across Physical Hosts with these additions:
   
   a. After Step 11, set the Disk Mode to Independent – Persistent.
   
   b. (Optional) Assign the disk a custom VM storage policy.

3. Use the Microsoft Create Cluster Wizard to validate the cluster.

   Note During validation, the wizard displays a warning in the category Storage and subcategory Validate Storage Spaces Persistent Reservation. This warning is not applicable when configuring a Windows Server Failover Cluster in your SDDC and can be safely ignored.
Managing Virtual Machines in VMware Cloud on AWS

Your VMware Cloud on AWS SDDC provides all the tools you need to, you deploy, configure, and customize VMware virtual machines (VMs).

Because it is a service, VMware Cloud on AWS imposes a few constraints on VM operations, especially those that require you to have physical access to the host hardware or root access to the host operating system. But with a few exceptions (which we point out in this document), on-premises operations described in vSphere Virtual Machine Administration work the same way in your VMware Cloud on AWS SDDC.

Table 6-1. vSphere Virtual Machine Administration Highlights

<table>
<thead>
<tr>
<th>Topics</th>
<th>Content Highlights</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction to vSphere VMs</td>
<td>■ Overview of VM lifecycle and components.</td>
</tr>
<tr>
<td></td>
<td>■ List of VM files and what they’re used for.</td>
</tr>
<tr>
<td></td>
<td>■ Overview of VM hardware and other options.</td>
</tr>
<tr>
<td>Deploying Virtual Machines</td>
<td>Step-by-step instructions for creating VMs. You have many options, including:</td>
</tr>
<tr>
<td></td>
<td>■ Deploying a VM from scratch.</td>
</tr>
<tr>
<td></td>
<td>■ Cloning existing VMs or templates</td>
</tr>
<tr>
<td></td>
<td>■ Deploying an OVF or OVA template</td>
</tr>
<tr>
<td></td>
<td>■ Deploying a VM from an uploaded OVF or OVA file</td>
</tr>
<tr>
<td>Using Content Libraries</td>
<td>Content libraries are container objects for VM and vApp templates and other types of files, such as ISO images, text files, and so on. You can use the templates in the library to deploy virtual machines and vApps in the vSphere inventory. You can also use content libraries to share content between your on-premises infrastructure and your SDDC.</td>
</tr>
<tr>
<td>Configuring Virtual Machine Hardware</td>
<td>Detailed information about the options for configuring different hardware options, such as CPU, memory, and devices. You can modify existing virtual devices or add new devices, though as we’ve noted some constraints may apply in VMware Cloud on AWS compared to what you can do in your on-premises vCenter environment.</td>
</tr>
</tbody>
</table>
### Table 6-1. vSphere Virtual Machine Administration Highlights (continued)

<table>
<thead>
<tr>
<th>Topics</th>
<th>Content Highlights</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Configuring Virtual Machine Options</strong></td>
<td>Explains VM options and how to change them.</td>
</tr>
<tr>
<td></td>
<td>- Power Management settings</td>
</tr>
<tr>
<td></td>
<td>- UEFI secure boot for virtual machines</td>
</tr>
<tr>
<td></td>
<td>- VM Boot options</td>
</tr>
<tr>
<td></td>
<td>- Advance options such as logging, debugging, and latency sensitivity</td>
</tr>
<tr>
<td><strong>Customizing Virtual Machines</strong></td>
<td>Instructions for performing post-deployment customization tasks, including:</td>
</tr>
<tr>
<td></td>
<td>- Options for installing a guest OS</td>
</tr>
<tr>
<td></td>
<td>- Customizing the guest OS with a customization spec</td>
</tr>
<tr>
<td></td>
<td>- Using a virtual machine console</td>
</tr>
<tr>
<td></td>
<td>- Using snapshots</td>
</tr>
<tr>
<td></td>
<td>- Upgrading VMware Tools or the Hardware Compatibility setting.</td>
</tr>
<tr>
<td><strong>Managing the VMware Remote Console Proxy Configuration</strong></td>
<td>VMware Remote Console proxy for vSphere (VMRC proxy) is a service in the SDDC vCenter Server system that simplifies the establishment of VMRC connections to workload VMs.</td>
</tr>
</tbody>
</table>

### VM Configurations With Limited or No Support in the SDDC

Some virtual machine configurations that you may be using in your on-premises data center are not supported in the SDDC. Others are supported with limitations.

Use [vSphere Virtual Machine Administration](https://www.vmware.com) in the [VMware vSphere Documentation](https://www.vmware.com) as your guide to creating, configuring, and managing workload VMs in VMware Cloud on AWS. Because VMware Cloud on AWS is a service, some VM configuration options documented in [vSphere Virtual Machine Administration](https://www.vmware.com) aren't available for use in an SDDC even though they may be mentioned in a help topic or listed in the vSphere Client when you right-click a workload VM and choose **Edit Settings**. But with a few exceptions, which we document here, you can use the guidance provided in that document when you configure, deploy, and manage workload VMs in the SDDC.

For other limits imposed by VMware Cloud on AWS, see [VMware Configuration Maximums](https://www.vmware.com).

### Table 6-2. On-Premises VM Configuration Options That Are Unavailable in an SDDC

<table>
<thead>
<tr>
<th>Configuration Option</th>
<th>References</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use the vSphere Client and the vSphere Web Client.</td>
<td>The vSphere Client and other topics.</td>
<td>Only the vSphere Client is supported for access to the SDDC vCenter.</td>
</tr>
<tr>
<td>Enable hyperthreading in a virtual CPU.</td>
<td>Virtual CPU Configuration and other topics.</td>
<td>To mitigate security vulnerabilities, including the ones discussed in <a href="https://kb.vmware.com">VMware Knowledge Base article 55806</a> and <a href="https://kb.vmware.com">VMware Knowledge Base article 55808</a>, VMware Cloud on AWS manages CPU hyperthreading on all hosts.</td>
</tr>
<tr>
<td>Configuration Option</td>
<td>References</td>
<td>Comments</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Change CPU identification masks.</td>
<td>Change CPU Identification Mask Settings</td>
<td>You cannot change CPU ID mask of a VM in your SDDC.</td>
</tr>
<tr>
<td>Change virtual disk type.</td>
<td>Change the Virtual Disk Configuration</td>
<td>You cannot change storage type for virtual disks on a VM in your SDDC.</td>
</tr>
<tr>
<td>Configure virtual hardware.</td>
<td>Virtual Machine Hardware Available to vSphere Virtual Machines</td>
<td>You cannot create a VM that includes any virtual hardware device that requires a physical change to the host. This includes things like serial ports, USB drives, and floppy drives.</td>
</tr>
<tr>
<td>Add a SCSI controller.</td>
<td>Add a SCSI Controller to a Virtual Machine</td>
<td>You can add a SCSI controller but cannot use virtual SCSI bus sharing.</td>
</tr>
<tr>
<td>Map a raw LUN or logical disk.</td>
<td>Raw Device Mapping</td>
<td>VMware Cloud on AWS does not support external block storage. You cannot deploy a VM that uses an RDM disk in an SDDC.</td>
</tr>
<tr>
<td>Add a hard disk.</td>
<td>Large Capacity Virtual Disk Conditions and Limitations</td>
<td>VMware Cloud on AWS does not support external block storage. You cannot deploy a VM that uses VMFS5 or NFS in an SDDC.</td>
</tr>
<tr>
<td>Add a network adapter</td>
<td>Network Adapter Basics</td>
<td>VMware Cloud on AWS supports only E1000E, VMXNET3, and SR-IOV adapters.</td>
</tr>
<tr>
<td>Add virtual CPUs</td>
<td>Virtual CPU Limitations</td>
<td>Because hyperthreading is disabled in VMware Cloud on AWS hosts, a virtual machine in the SDDC cannot have more virtual CPUs than the number of physical cores on the host.</td>
</tr>
<tr>
<td>Configure a PCI passthrough device</td>
<td>Configure a PCI Device on a Virtual Machine</td>
<td>This feature is not supported in VMware Cloud on AWS</td>
</tr>
</tbody>
</table>

**On-Premises VM Configurations that are Blocked or Limited in an SDDC**

Certain VM configuration options can prevent the host from entering maintenance mode, interfere with vMotion, or otherwise prevent VMware from performing service upgrades. These configurations, which are permitted on premises, have limited support or no support the SDDC. If you upload a template with an unsupported configuration from your on-premises content library to your SDDC, VMs created from the template will not power on in the SDDC.
Table 6-3. VM Configurations With Limited or No Support in the SDDC

<table>
<thead>
<tr>
<th>Configuration Option</th>
<th>Support</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM includes a serial port with network output</td>
<td>None</td>
<td>This configuration is blocked in the SDDC</td>
</tr>
<tr>
<td>VM disk enables both multi-writer and Changed Block Tracking (CBT)</td>
<td>None</td>
<td>This configuration is blocked in the SDDC</td>
</tr>
<tr>
<td>VM includes a parallel port</td>
<td>None</td>
<td>Parallel ports are not supported for physical device or file output.</td>
</tr>
<tr>
<td>VM uses virtual or physical bus sharing</td>
<td>Limited</td>
<td>Physical bus sharing configurations are supported on hardware version 11 and later.</td>
</tr>
<tr>
<td>VM mounts a VMware Tools ISO and initiates a tools installation or upgrade.</td>
<td>Limited</td>
<td>vMotion is not allowed during VMware tools installation or upgrade. If vMotion required by SDDC maintenance is blocked by VM in this state, the system allows a few minutes for the operation to complete. If the operation does not complete, the system terminates the upgrade or installation and unmounts the ISO image to unblock the maintenance event. You'll need to manually re-start the installation or upgrade process after the maintenance is complete.</td>
</tr>
</tbody>
</table>

Virtual Hardware Support in the VMware Cloud on AWS SDDC

Virtual machine compatibility in VMware Cloud on AWS closely tracks what is supported by the ESXi and vCenter Server versions associated with your SDDC.

For a list of virtual hardware versions and related features supported by ESXi and vCenter Server versions, see Hardware Features Available with Virtual Machine Compatibility Settings in the VMware vSphere Product Documentation. To see what versions of ESXi and vCenter Server are running in your SDDC, see Correlating VMware Cloud on AWS with Component Releases.

See VM Configurations With Limited or No Support in the SDDC for a summary of virtual machine configurations that are not supported, or are supported with limitations, in the SDDC.

Using PowerCLI and the Guest Operations API

You can use the vSphere Guest Operations API or the PowerCLI Invoke-VMScript and Copy-VMGuestFile cmdlet in your customization workflows for SDDC VMs.

Prerequisites

- Configure either or both of these connections between your on-premises environment and your SDDC.
  - Management VPN
  - Direct Connect through a Private Virtual Interface (VIF)
See Getting Started With VMware Cloud on AWS and VMware Cloud on AWS Networking and Security.

- Create a management network firewall rule that allows access from your on-premises network to port 443 of your SDDC hosts. See Add or Modify Management Gateway Firewall Rules.

Procedure

1. Verify that the VM is running the latest version of VMware Tools.

2. Verify that you can access the Guest Operations API, either directly or via a simple PowerCLI cmdlet.

   You could use a cmdlet like this one to test your ability to reach port 443 on the ESXi host with IP address 10.100.1.1.

   ```powershell
   PS C:\Users\admin> Test-NetConnection -Port 443 -ComputerName 10.100.1.1
   ```

   A response of True or TcpTestSucceeded indicates a successful test.

**Example: Using the PowerCLI Invoke-VMScript Cmdlet**

After you establish a network connection that allows traffic to port 443 on your hosts, you can use the Guest Operations API directly, or via PowerCLI as shown here. API and cmdlet requests go to port 443 on the host where the subject VM (Win10-Example here) is running. VMware Tools running on the VM handles the requested guest operations.

```powershell
PS C:\Users\admin> $vm = Get-VM Win10-Example
PS C:\Users\admin>
Invoke-VMScript –ScriptText "dir C:" –VM $vm –GuestUser admin –GuestPassword $passwd"

ScriptOutput
------------------------------------------------------
| Directory: C:\
| ...
```

**Deploy a VM from an OVF Template in a Content Library**

You can deploy a virtual machine from an OVF template in a local or subscribed content library.

**Prerequisites**

You must have a Content Library containing the OVF template you want to use.

- For more information on creating content libraries, see Create a Library.
- For more information on importing content into a content library, see Populating Libraries with Content.
Procedure

1. From the vSphere Client VMs and Templates view, right click a valid parent object of a VM, such as the Workloads folder, and select New virtual machine.

2. Select Deploy from template and click Next.

3. Select the template to deploy.

4. Proceed through the New Virtual Machine wizard, using the following settings.
   a. For the VM folder, select Workloads, Templates, or another folder that you have write permissions on.
   b. For the compute resource, select Compute-ResourcePool.
   c. For the datastore, select workloadDatastore.

5. On the Select networks page, enter an IP address in the IP address field.
   The IP Allocation Settings on this page show only the Static IP option, even if the logical network you have selected uses DHCP. You must enter something into the IP address field to proceed in the wizard. If DHCP is enabled, the VM deploys with DHCP.

6. Review the VM settings and click Finish.