

# VMware Cloud on AWS Operations Guide

20 September 2022

SDDC Version 1.20

VMware Cloud on AWS

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

<https://docs.vmware.com/>

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

Copyright © 2017-2022 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

# Contents

## About VMware Cloud on AWS Operations 6

### 1 About Software-Defined Data Centers 7

Supported SDDC Versions 7

Configuration Maximums for VMware Cloud on AWS 8

Correlating VMware Cloud on AWS with Component Releases 8

VMware Cloud on AWS Developer Resources 10

Deploying and Managing a Software-Defined Data Center 11

Deploy an SDDC from the VMC Console 14

Rename an SDDC 22

Delete an SDDC 22

Creating and Managing SDDC Deployment Groups with VMware Transit Connect™ 23

Create or Modify an SDDC Group 30

Add Compute Gateway Firewall Rules to Enable SDDC Group Member Workload Connectivity 40

Attach a Direct Connect Gateway to an SDDC Group 42

Use vCenter Linking in an SDDC Group 44

Configure SDDC Compliance Hardening 46

Disable Networking & Security Tab Access 46

Disable Add-On Services 49

Using VMware Tanzu™ Kubernetes Grid™ with VMware Cloud on AWS 51

Activate Tanzu Kubernetes Grid in an SDDC Cluster 53

Allow Internal Access to a Tanzu Kubernetes Grid Namespace 56

Enable Internet Access to a Kubernetes Service 57

Deactivate Tanzu Kubernetes Grid Services in a Cluster 58

SDDC Upgrades and Maintenance 59

View an SDDC Maintenance Schedule Reservation 63

Submit an Upgrade Schedule Request 63

View Maintenance Progress 66

Convert UTC Time to Local Time 67

Estimating the Duration of SDDC Maintenance 67

Actions Taken by VMware to Ensure SDDC Health 68

View Billing Information 70

Upsize SDDC Management Appliances 71

Roles and Permissions in the SDDC 72

### 2 Managing SDDC Hosts and Clusters 74

VMware Cloud on AWS Host Types 74

|   |            |
|---|------------|
| Add a Cluster   | 75         |
| Remove a Cluster  | 76         |
| Add Hosts   | 77         |
| Remove Hosts  | 78         |
| About External Storage  | 80         |
| Add External Storage to a Cluster                                     | 80         |
| Remove External Storage From a Cluster                                | 81         |
| About Elastic DRS   | 81         |
| How the Elastic DRS Algorithm Works                                   | 82         |
| Select Elastic DRS Policy   | 84         |
| Understanding Auto-Remediation  | 86         |
| Using Policies and Profiles   | 89         |
| Create or Delete a VM-Host Affinity Policy                            | 90         |
| Create or Delete a VM-Host Anti-Affinity Policy                       | 91         |
| Create or Delete a VM-VM Affinity Policy                              | 93         |
| Create or Delete a VM-VM Anti-Affinity Policy                         | 94         |
| Create or Delete a Disable DRS vMotion Policy                         | 95         |
| Microsoft Product Licenses in VMware Cloud on AWS                     | 96         |
| License Mobility  | 97         |
| Select License Options from the VMC Console                           | 98         |
| Deploying Microsoft Server Instances                                  | 99         |
| Activate or Reactivate a Windows Server VM                            | 104        |
| Converting Host Types in Clusters                                     | 105        |
| <b>3 Working With SDDC Add-On Services</b>                            | <b>108</b> |
| Using the vRealize Log Insight Cloud Add-On                           | 108        |
| Using the vRealize Automation Cloud Add-On                            | 109        |
| Using VMware Carbon Black Workload                                    | 109        |
| Using the NSX Advanced Firewall Add-On                                | 110        |
| <b>4 Getting Templates, ISOs, and Other Content into Your SDDC</b>    | <b>111</b> |
| Use the Content Onboarding Assistant to Transfer Content to Your SDDC | 112        |
| Use a Content Library to Import Content into Your SDDC                | 114        |
| Upload Files or Folders to your SDDC                                  | 115        |
| <b>5 Migrating Virtual Machines</b>                                   | <b>116</b> |
| Hybrid Migration With VMware HCX                                      | 117        |
| Hybrid Migration with VMware HCX Checklist                            | 117        |
| Hybrid Migration with vMotion   | 118        |
| Hybrid Migration with vMotion Checklist                               | 120        |
| Required Firewall Rules for vMotion                                   | 121        |

|          |  |            |
|----------|--|------------|
|          | Bulk Migration with vMotion  | 123        |
|          | Hybrid Cold Migration  | 123        |
|          | Hybrid Cold Migration Checklist  | 124        |
|          | Required Firewall Rules for Cold Migration   | 124        |
| <b>6</b> | <b>Accessing AWS Services</b>  | <b>126</b> |
|          | Configure Amazon FSx for NetApp ONTAP as External Storage                                | 126        |
|          | Connecting EC2 With SDDC Workloads   | 129        |
|          | Access an S3 Bucket Using an S3 Endpoint   | 131        |
|          | Access an S3 Bucket Using the Internet Gateway   | 133        |
| <b>7</b> | <b>Using On-Premises vRealize Automation with Your Cloud SDDC</b>                        | <b>135</b> |
|          | Prepare Your SDDC to Work with vRealize Products   | 135        |
|          | Connect vRealize Automation 8.x to Your SDDC   | 136        |
|          | Connect vRealize Automation 7.x to Your SDDC   | 136        |
| <b>8</b> | <b>Service Notifications and Activity Log</b>  | <b>138</b> |
|          | View the Activity Log  | 138        |
|          | View and Subscribe to the Service Status Page  | 139        |
|          | Notifications Available from VMware Cloud on AWS   | 139        |
|          | Set Notification Preferences   | 151        |
| <b>9</b> | <b>Troubleshooting</b>   | <b>152</b> |
|          | Get Support  | 152        |
|          | Unable to Connect to VMware Cloud on AWS   | 152        |
|          | Unable to Connect to vCenter Server  | 153        |
|          | Unable to Select Subnet When Creating SDDC   | 154        |
|          | Unable to Copy Changed Password Into vCenter Login Page                                  | 155        |
|          | Compute Workloads Are Unable to Reach an On-Premises DNS Servers Over a Policy-Based VPN | 155        |

# About VMware Cloud on AWS Operations

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

## Intended Audience

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

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

# About Software-Defined Data Centers

# 1

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

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

This chapter includes the following topics:

- [Supported SDDC Versions](#)
- [Configuration Maximums for VMware Cloud on AWS](#)
- [Correlating VMware Cloud on AWS with Component Releases](#)
- [VMware Cloud on AWS Developer Resources](#)
- [Deploying and Managing a Software-Defined Data Center](#)
- [Creating and Managing SDDC Deployment Groups with VMware Transit Connect™](#)
- [Configure SDDC Compliance Hardening](#)
- [Using VMware Tanzu™ Kubernetes Grid™ with VMware Cloud on AWS](#)
- [SDDC Upgrades and Maintenance](#)
- [View Billing Information](#)
- [Upsize SDDC Management Appliances](#)
- [Roles and Permissions in the SDDC](#)

## Supported SDDC Versions

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

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

To find the version of your SDDC software, see [Get Support](#).

**Table 1-1. Lifecycle Support for SDDC Software Versions**

| SDDC Version | Expiration Date    |
|--------------|--------------------|
| 1.20         | TBD                |
| 1.19         | TBD                |
| 1.18         | TBD                |
| 1.17         | March 31, 2023     |
| 1.16         | February 28, 2023  |
| 1.15         | October 31, 2022   |
| 1.14         | September 30, 2022 |
| 1.13         | February 28, 2022  |
| 1.12         | January 31, 2022   |
| 1.11         | July 31, 2021      |
| 1.10         | June 30, 2021      |

## Configuration Maximums for VMware Cloud on AWS

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

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

For the latest maximums, see [VMware Configuration Maximums](#)

## Correlating VMware Cloud on AWS with Component Releases

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

| SDDC version | ESXi version           | VSAN version           | vCenter Server version | NSX version            | Virtual Machine Hardware version |
|--------------|------------------------|------------------------|------------------------|------------------------|----------------------------------|
| 1.20         | 8.0.0 (Build 20430035) | 8.0.0 (Build 20430035) | 8.0.0 (Build 20432146) | 4.0.1 (Build 20417290) | 19 (version 14 is the default)   |
| 1.19         | 8.0.0 (Build 20011649) | 8.0.0 (Build 20011649) | 8.0.0 (Build 20011647) | 4.0.0 (Build 20002995) | 19 (version 14 is the default)   |



| SDDC version | ESXi version           | VSAN version           | vCenter Server version  | NSX version            | Virtual Machine Hardware version |
|--------------|------------------------|------------------------|-------------------------|------------------------|----------------------------------|
| 1.18v6       | 7.0.3 (Build 20278438) | 7.0.3 (Build 20278438) | 7.0.3 (Build 20277315)  | 3.1.5 (Build 20266905) | 19 (version 14 is the default)   |
| 1.18v5       | 7.0.3 (Build 20067464) | 7.0.3 (Build 20067464) | 7.0.3 (Build 20073839)  | 3.1.5 (Build 20020624) | 19 (version 14 is the default)   |
| 1.18v4       | 7.0.3 (Build 19888012) | 7.0.3 (Build 19888012) | 7.0.3 (Build 19888010)  | 3.1.5 (Build 19852944) | 19 (version 14 is the default)   |
| 1.18v3       | 7.0.3 (Build 19774523) | 7.0.3 (Build 19774523) | 7.0.3 (Build 19774521)  | 3.1.5 (Build 19540791) | 19 (version 14 is the default)   |
| 1.18v2       | 7.0.3 (Build 1966653)  | 7.0.3 (Build 19666536) | 7.0.3 (Build 19666520)  | 3.1.5 (Build 19540791) | 19 (version 14 is the default)   |
| 1.18         | 7.0.3 (Build 19585512) | 7.0.3 (Build 19585512) | 7.0.3 (Build 19584923)  | 3.1.5 (Build 19540791) | 19 (version 14 is the default)   |
| 1.17         | 7.0.3 (Build 18877114) | 7.0.3 (Build 18877114) | 7.0.3 (Build 18944372)  | 3.1.4 (Build 18898460) | 19 (version 14 is the default)   |
| 1.16v12      | 7.0.3 (Build 20239070) | 7.0.3 (Build 20239070) | 7.0.3 (Build 20225869)  | 3.1.3 (Build 20217630) | 19 (version 14 is the default)   |
| 1.16v11      | 7.0.3 (Build 20028060) | 7.0.3 (Build 20028060) | 7.0.3 (Build 20029357)  | 3.1.3 (Build 20006856) | 19 (version 14 is the default)   |
| 1.16v10      | 7.0.3 (Build 19924251) | 7.0.3 (Build 19924251) | 7.0.3 (Build 19924211)  | 3.1.3 (Build 19891738) | 19 (version 14 is the default)   |
| 1.16v9       | 7.0.3 (Build 19760096) | 7.0.3 (Build 19760096) | 7.0.3 (Build 19760094 ) | 3.1.3 (Build 19762317) | 19 (version 14 is the default)   |
| 1.16v8       | 7.0.3 (Build 19588084) | 7.0.3 (Build 19588084) | 7.03 (Build 19504857)   | 3.1.3 (Build 19724625) | 19 (version 14 is the default)   |
| 1.16v7       | 7.0.3 (Build 19588084) | 7.0.3 (Build 19588084) | 7.0.3 (Build 19504857 ) | 3.1.3 (Build 19572985) | 19 (version 14 is the default)   |
| 1.16v6       | 7.0.3 (Build 19230660) | 7.0.3 (Build 19230660) | 7.0.3 (Build 19388229)  | 3.1.3 (Build 19536855) | 19 (version 14 is the default)   |
| 1.16v5       | 7.0.3 (Build 19230660) | 7.0.3 (Build 19230660) | 7.0.3 (Build 19388229)  | 3.1.3 (Build 19187344) | 19 (version 14 is the default)   |
| 1.16v4       | 7.0.3 (Build 19230660) | 7.0.3 (Build 19230660) | 7.0.3 (Build 19230656)  | 3.1.3 (Build 19187344) | 19 (version 14 is the default)   |
| 1.16v3       | 7.0.3 (Build 18895054) | 7.0.3 (Build 18895054) | 7.0.3 (Build 18923793)  | 3.1.3 (Build 18883348) | 19 (version 14 is the default)   |
| 1.16v2       | 7.0.3 (Build 18809690) | 7.0.3 (Build 18809690) | 7.0.3 (Build 18725380)  | 3.1.3 (Build 18707895) | 19 (version 14 is the default)   |
| 1.16         | 7.0.3 (Build 18710037) | 7.0.3 (Build 18710037) | 7.0.3 (Build 18725380)  | 3.1.3 (Build 18707895) | 19 (version 14 is the default)   |
| 1.15v2       | 7.0.2 (Build 18186873) | 7.0.2 (Build 18186873) | 7.0.2 (Build 18241532)  | 3.1.2 (Build 18196142) | 17                               |

| SDDC version                       | ESXi version           | VSAN version           | vCenter Server version  | NSX version            | Virtual Machine Hardware version |
|------------------------------------|------------------------|------------------------|-------------------------|------------------------|----------------------------------|
| 1.15                               | 7.0.2 (Build 18110030) | 7.0.2 (Build 18110030) | 7.0.2 (Build 18137590)  | 3.1.2 (Build 18112709) | 17                               |
| 1.14v7                             | 7.0.2 (Build 18893290) | 7.0.2 (Build 18893290) | 7.0.2 (Build 18900449)  | 3.0.3 (Build 18790718) | 17                               |
| 1.14v6                             | 7.0.2 (Build 18596908) | 7.0.2 (Build 18596908) | 7.0.2 (Build 18596906)  | 3.0.3 (Build 18574048) | 17                               |
| 1.14v5                             | 7.0.2 (Build 18370790) | 7.0.2 (Build 18370790) | 7.0.2 (Build 18370788 ) | 3.0.3 (Build 18358881) | 17                               |
| 1.14v4                             | 7.0.2 (Build 18226209) | 7.0.2 (Build 18226209) | 7.0.2 (Build 18231847)  | 3.0.3 (Build 18084735) | 17                               |
| 1.14v3                             | 7.0.2 (Build 18118720) | 7.0.2 (Build 18118720) | 7.0.2 (Build 18119277)  | 3.0.3 (Build 18084735) | 17                               |
| 1.14v2                             | 7.0.2 (Build 17867587) | 7.0.2 (Build 17867587) | 7.0.2 (Build 17933601)  | 3.0.3 (Build 17818935) | 17                               |
| 1.14                               | 7.0.2 (Build 17776467) | 7.0.2 (Build 17776467) | 7.0.2 (Build 17803906)  | 3.0.3 (Build 17723245) | 17                               |
| VMware Cloud on AWS GovCloud (1.9) | 7.0.0 (Build 15423985) | 7.0.0 (Build 15423985) | 7.0.0 (Build 15424599)  | 2.5.1 (Build 15419370) | 17                               |

**Note** See VMware Knowledge Base Article [88920](#) for information about steps you can take to increase the efficiency of applications running on i3en metal.

To find compatible versions of solutions, see the [VMware Product Interoperability Matrix](#).

- [VMware Site Recovery Manager Interoperability](#)
- [VMware HCX](#)

## VMware Cloud on AWS Developer Resources

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

Visit the [VMware Cloud on AWS Dev Center](#) to find out more about the available APIs, SDKs, CLIs, and other resources. You can also use many of the native vSphere tools that apply to your on-premises vSphere installation to automate vSphere operations in the SDDC. See [Working with the Developer Center](#) in the *vSphere Documentation*.

# Deploying and Managing a Software-Defined Data Center

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

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

## Connected AWS Account

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

You can deploy one, two or multiple hosts on VMware Cloud on AWS.

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

## AWS VPC Configuration and Availability Requirements

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

- The subnet must be in an AWS Availability Zone (AZ) where VMware Cloud on AWS is available. Start by creating a subnet in every AZ in the AWS Region where the SDDC will be created. It helps you identify all AZs where an SDDC can be deployed and select the one that best meets your SDDC placement needs, whether you want to keep your VMC workloads close to or isolated from your AWS workloads running in a particular AZ. See [Creating a Subnet in Your VPC](#) in the AWS documentation for information about how to use the Amazon VPC console to create a subnet in your VPC.
- The subnet must exist in the connected AWS account. It cannot be one owned by and shared from another account.
- The AWS account being linked must have sufficient capacity to create a minimum of 17 ENIs per SDDC in each region where an SDDC is deployed. Although you cannot provision more than 16 hosts in a cluster, SDDC operations including planned maintenance and Elastic DRS can require us to temporarily add as many as 16 more hosts, so we recommend using an AWS that has sufficient capacity for 32 ENIs per SDDC per region.
- We recommend dedicating a /26 CIDR block to each SDDC and not using that subnet for any other AWS services or EC2 instances. Because some of the IP addresses in this block are reserved for internal use, a /26 CIDR block is the smallest subnet that can accommodate SDDC IP address requirements.

- Any VPC subnets on which AWS services or instances communicate with the SDDC must be associated with the main route table of the connected VPC. Use of a custom route table or replacement of the main route table is not supported. By default, AWS limits the size of the main route table to 50 routes. Because the main route table must accommodate an entry for each routed SDDC network segment as well as the management network CIDR and any additional routes you create directly in your AWS account, the default limit might not be adequate for your SDDC networks, especially if you connect more than one SDDC to the VPC. You can request a route table size increase as described in [Amazon VPC quotas](#).
- If necessary, you can link multiple SDDCs to a VPC if the VPC subnet used for ENI connectivity has a large enough CIDR block to accommodate them. Because all SDDCs in a VPC use the same main route table, make sure that network segments in those SDDCs do not overlap with each other or the VPC's primary CIDR block. Workload VMs on routed SDDC networks can communicate with all subnets in the VPC's primary CIDR block, but are unaware of other CIDR blocks that might exist in the VPC.

## AWS Elastic IP Requirements

Every SDDC consumes at least 4 AWS Elastic IP (EIP) addresses that are not displayed on the VMC Console. These EIPs are required for core SDDC operations. Charges for them are listed in the VMware on AWS [Pricing](#) document under *Additional charges not included*. EIPs are billed per-hour. EIP address remaps, typically initiated by vMotion or a failover event on the edge gateway, are free of charge for the first 100 events. Here's a summary of how these core EIPs are used in a new SDDC:

**Table 1-2. Core EIP Usage**

| Usage                         | Description  |
|-------------------------------|--|
| Management                    | Provides VMware support with access to your SDDC.  |
| Management Gateway (MGW) SNAT | Provides the SNAT address for traffic egressing the MGW to the Internet.   |
| Compute Gateway (CGW) SNAT    | Provides the default SNAT address for traffic egressing the CGW to the Internet.   |
| vCenter Server Public IP      | Provides the IP address used for vCenter Server when the <b>vCenter FQDN</b> is set to <b>Public IP</b> . See <a href="#">Set vCenter Server FQDN Resolution Address</a> . This EIP is always consumed, even if you set the <b>vCenter FQDN</b> to <b>Private IP</b> . |

## Single Host SDDC starter Configuration for VMware Cloud on AWS

You can jump start your VMware Cloud on AWS experience with a Single Host SDDC starter configuration. This is a time-limited offering designed for you to prove the value of VMware Cloud on AWS in your environment. The service life of a Single Host environment is limited to 60 days. At any point during the service life of a Single Host SDDC, you can scale it up to a production configuration with two or more hosts with no loss of data. If you do not scale up the Single Host SDDC before the end of the service life, the SDDC is deleted along with all the workloads and data it contains.

## Stretched Clusters for VMware Cloud on AWS

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

The following restrictions apply to stretched clusters:

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

For limitations that affect all stretched clusters, see [VMware Configuration Maximums](#).

Additionally, large-sized SDDC appliances are not supported with two-host stretched clusters.

## Connecting to the SDDC and Configuring SDDC Networks

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

## Custom Core Counts

When you deploy your initial SDDC, all host CPUs in the initial SDDC cluster are enabled. You cannot deactivate any host CPUs in the initial SDDC cluster. However, if you deploy additional clusters, you can choose to deactivate some of the host CPUs in the cluster, which can help save on licensing costs for software that is licensed on a per-CPU basis. If you want to take advantage of this feature, plan the size of your initial cluster and subsequent clusters accordingly.

## Credit Card Payments

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

The implementation of the upfront \$2000 pre-charge is part of VMware's fraud-prevention policy. This pre-charge is waived at VMware's discretion based on the your current level of engagement with VMware. You will learn of the waiver when you are about to deploy your first SDDC.

By default, credit cards can't be used as the payment method for purchasing subscriptions. If you need to use a credit card to purchase a subscription, open a support ticket, and VMware will assist you with the purchase.

## Deploy an SDDC from the VMC Console

Deploy an SDDC to host your workloads in the cloud.

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

### Procedure

- 1 Log in to the VMC Console at <https://vmc.vmware.com>.
- 2 Create the SDDC.

#### To start from the Launchpad:

From the **Launchpad**, click **VMware Cloud on AWS** in the **Infrastructure** column, then click **Learn More** and **Get Started** to open the **Create Software-Defined Data Center (SDDC)** page.

#### To start from the Inventory view:

From the **Inventory** page, click **ADD DEPLOYMENT** and select **VMware Cloud on AWS** from the drop-down menu.

- 3 Choose a seller.

See [Purchase Options for VMware Cloud on AWS](#). You cannot change the seller after the SDDC is created.

#### 4 Configure SDDC properties.

a Choose a **Cloud**.

For a **VMware Cloud on AWS** deployment, select **AWS**.

b Select an **AWS Region** in which to deploy the SDDC.

See [Choosing a Region](#) for a list of available regions and the features they support.

c Select a **Deployment type**.

| Option                   | Description  |
|--------------------------|--|
| <b>Single Host</b>       | Select this option to create Single Host Starter Configuration SDDC. Single Host Starter Configuration SDDCs expire after 60 days. For more information, see <a href="#">Deploying a Single Host SDDC Starter Configuration</a> .  |
| <b>Multi-Host</b>        | Select this option to create an SDDC with two or more hosts.   |
| <b>Stretched Cluster</b> | If you create a multiple-host SDDC, you also have the option to create a stretched cluster that spans two availability zones (AZs). This configuration provides data redundancy in the event that there is a problem with one of the AZs. The system deploys management VMs in the first AZ you select. Both AZs can be used by your workloads. Either can be used for failover. You need a minimum of two hosts (one in each AZ) to create a stretched cluster. Hosts must be added in pairs. |

d Select the host type.

Currently available host types are i3 and i3en. For more information on host types, see [VMC on AWS Host Types](#).

e Make up an **SDDC Name**.

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

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

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

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

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

#### 5 (Optional) Click **Show Advanced Configuration** to select the size of the SDDC appliances.

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

To deploy the SDDC with large appliances, select **Large** from the **SDDC Appliance Size** drop-down control.

**Note** Large-sized appliances are not supported for SDDCs with a two-host stretched cluster as the primary cluster.

If you create the SDDC with a medium appliance configuration and find that you need additional management cluster resources, you can change the **SDDC Appliance Size** to large. See [Upsize SDDC Management Appliances](#).

**6** Click **Next** to connect to an AWS account.

See [AWS VPC Configuration and Availability Requirements](#) and [Account Linking and the VMware Cloud on AWS CloudFormation Template](#) for important information about requirements for the AWS account and subnets.

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

**7** Select a **VPC** and **Subnet** from the drop-down menu and click **Next**.

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

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

- Choose a range of IP addresses that does not overlap with the AWS subnet you are connecting to. If you plan to connect your SDDC to an on-premises data center, the IP address range of the subnet must be unique within your enterprise network infrastructure. It cannot overlap the IP address range of any of your on-premises networks. For a complete list of IPv4 addresses reserved by VMware Cloud on AWS, see [Reserved Network Addresses](#) in the *VMware Cloud on AWS Networking and Security* guide.
- If you are deploying a single-host SDDC, the IP address range 192.168.1.0/24 is reserved for the default compute network of the SDDC. If you specify a management network address range that overlaps that address, single-host SDDC creation fails. If you are deploying a multi-host SDDC, no compute gateway logical network is created during deployment, so you'll need to create one after the SDDC is deployed.



- CIDR blocks of size 16, 20, or 23 are supported, and must be in one of the "private address space" blocks defined by [RFC 1918](#) (10.0.0.0/8, 172.16.0.0/12, or 192.168.0.0/16). The primary factor in choosing a Management CIDR block size is the anticipated scalability requirements of the SDDC. The management CIDR block cannot be changed after the SDDC has been deployed, so a /23 block is appropriate only for SDDCs that will not require much growth in capacity.

| CIDR block size | Number of hosts (Single AZ)                         | Number of hosts (Multi AZ) |
|-----------------|---|----------------------------|
| 23              | 27  | 22                         |
| 20              | 251   | 246                        |
| 16              | See <a href="#">VMware Configuration Maximums</a> . |                            |

**Note** Because VMware Cloud on AWS reserves the capacity to add hosts (and their IP addresses) to every SDDC to meet SLA requirements during maintenance operations or in case of host failure, the number of usable hosts is reduced from what's shown here by two per SDDC, plus one more per cluster. This means that, for example, an SDDC with two clusters and a /23 management CIDR has enough IP addresses to deploy up to 23 hosts. The remaining addresses are reserved to be used when needed by hosts deployed to meet SLA requirements.

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

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

### What to do next

After your SDDC is created, do the following:

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

## Choosing a Region

VMware Cloud on AWS is available in many AWS regions. Some AWS regions do not support all VMware Cloud on AWS features.

AWS regions are named geographic locations where Amazon has sited their data centers. Every region includes multiple availability zones (AZs), each of which constitutes a separate fault domain. Failures in one availability zone do not affect the other AZs in its region. Events such as natural disasters and power grid failures do not typically affect more than one AWS region. Configuring your VMware Cloud on AWS SDDC to use stretched clusters (in multiple AZs) provides additional fault tolerance for SDDC operations. Configuring your VMware Cloud on AWS organization to have SDDCs in multiple regions can improve your organization's ability to tolerate large-scale events that can compromise an entire region. See the VMware Tech Zone article [VMware Cloud on AWS: Stretched Clusters](#) for more information about AWS regions and AZs, and how to configure and use VMware Cloud on AWS stretched clusters.

See [AWS Region and Availability Zone Support](#) for a list of AWS regions and AZs that support VMware Cloud on AWS.

## Account Linking and the VMware Cloud on AWS CloudFormation Template

AWS account linking is part of the SDDC deployment process. For new customers or those who plan to create only a few SDDCs, the process is straightforward and typically requires little or no involvement with the underlying AWS objects and protocols. Administrators who deploy multiple SDDCs might require a better understanding of the details of this process, along with the AWS roles and permissions involved.

### About AWS Account Linking

The VMware Cloud on AWS CloudFormation template (CFT) runs in the AWS US West (Oregon) region. This doesn't affect where the resulting SDDCs are created, since the required permissions are valid in all regions, but the AWS account that runs the CFT must not be restricted by AWS Service Control Policies (SCP) from accessing the Oregon region. Once the CFT is loaded, you can edit it to change the region if you need to. You can run the CFT in any region, but you should keep an internal document noting where it was run. If your organization has no members who can access the Oregon region, you can download the CFT from the link provided when you click **OPEN AWS CONSOLE WITH COUDFORMATION TEMPLATE** or just send that link to an AWS Administrator to run, since linking an AWS account to a VMC organization happens only once.

As part of account linking, and periodically during ongoing SDDC operations, the linked AWS account takes an inventory of the organization's VPCs and subnets in all regions so that it can have an up-to-date list of AWS regions and AZs available to the organization. This operation can fail if the account is restricted by SCP from accessing those regions or VPCs. This sort of failure is acceptable as long as the restricted regions and VPCs won't be used by VMware Cloud on AWS.

We recommend creating a subnet in every AZ prior to account linking. Any AZ that does not have a subnet when the account is linked will be unavailable for future use by VMware Cloud on AWS even if you create a subnet later until a system-initiated rescan is performed. You can initiate a rescan by running the CFT again, but we don't recommend this for an organization that is already linked and has SDDCs deployed.

There's more information about account linking in the VMware Cloud Tech Zone designlet [VMware Cloud on AWS Connected VPC to Native AWS](#). For information about how to unlink an account, see VMware Knowledge Base article [83400](#).

### AWS Roles Used by Account Linking

Every time you run the VMware Cloud on AWS CFT, a new set of AWS roles is defined and your VMware Cloud on AWS organization is updated to use those roles for future SDDC deployments. The CFT grants one or more VMware-owned AWS accounts access to these roles in your AWS account:

- AWS account IDs of the form 909\*\*\*\*\*262 or 347\*\*\*\*\*669: VMware Cloud on AWS uses these accounts to query AWS resources such as subnets and VPCs, and for ENI creation and association during SDDC deployment or host additions.
- A 12-digit AWS account ID that is unique for each organization and is used for ongoing operations such as updating route tables when segments are added or removed or an NSX Edge migration or failover occurs.

Existing SDDCs continue to use the roles defined when the SDDC was created, which can create a scenario where multiple sets of roles (and CFTs) are active in the your AWS account, and deleting any of them will impact the SDDCs using it. The IAM roles and CFT being used by an SDDC are shown on the **Connected VPC** page under the **Networking & Security** tab of an SDDC.

The IAM roles created by the CFT grant AWS AssumeRole privileges to the VMware AWS accounts used by the VMware Cloud on AWS service for a specific AWS Policy. This policy is defined and managed by AWS, and for security reasons, VMware does not have rights to change it. If you modify or delete these roles, the account link is broken, communication with the connected VPC fails, and you can no longer deploy new SDDCs or add new hosts to existing SDDCs linked to that account. Contact VMware support to request remediation.

### Permissions Statement

To run the CloudFormation template that links a VMware Cloud on AWS organization to an AWS VPC, VMware must add several required AWS roles and permissions to your AWS account. Initial permissions required for account linking appear in the first half of the statement are shown here in a normal font. The account that runs this template must have these permissions. After account linking completes, only the permissions granted by the IAM roles (shown here in *italics*) are needed,

---

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

---

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeRouteTables",
```

```

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

```

```

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

```

Because VMware Cloud on AWS requires AWS rights for SDDC deployment and ongoing operations such as routing updates and host replacements, you need to ensure that these roles can use the AWS AssumeRole function as needed and not be blocked by AWS features such as Control Tower Guardrails or Service Control Policies (SCP). The IAM roles require only a minimal set of permissions, which are managed by AWS in the policy: AmazonVPCCrossAccountNetworkInterfaceOperations, which is the only access granted by the IAM roles created by the template.

To see the associated Policy Permissions document, log into the AWS

Console and open [https://console.aws.amazon.com/iam/home?region=us-east-1#/policies/arn:aws:iam::aws:policy/AmazonVPCCrossAccountNetworkInterfaceOperations\\$jsonEditor](https://console.aws.amazon.com/iam/home?region=us-east-1#/policies/arn:aws:iam::aws:policy/AmazonVPCCrossAccountNetworkInterfaceOperations$jsonEditor).

Here's the summary description of that policy.

```

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

```

```

        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets"
    ],
    "Resource": [
        "*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses"
    ],
    "Resource": [
        "*"
    ]
}
]
}

```

## Rename an SDDC

You can rename an existing SDDC.

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

### Procedure

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

## Delete an SDDC

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

When you delete an SDDC, all ENIs created for it in the connected VPC are deleted and their IP addresses released. Routes added to the main route table remain, but in most cases will have a status of “Blackhole” because they point to a deleted ENI.

### Procedure

- 1 Log in to the VMC Console at <https://vmc.vmware.com>.
- 2 On the card for the SDDC you want to remove, click **Actions > Delete SDDC**.

### 3 Confirm that you understand the consequences of deleting an SDDC.

Select all of the following:

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

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

### 4 Click **DELETE SDDC**.

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

An SDDC deployment group uses VMware Transit Connect to provide high-bandwidth, low-latency connections between SDDCs in the group. An SDDC group can include VPCs you own. You can also add an AWS Direct Connect Gateway (DXGW) to provide connectivity between group members and your on-premises SDDCs.

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

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

### Group Membership

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

- It must be at SDDC version 1.11 or later. Members of a multi-region group must be at SDDC version 1.15 or later.
- Its management network CIDR block cannot overlap the management CIDR block of any other group member.
- It cannot be a member of another SDDC Group.

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

---

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

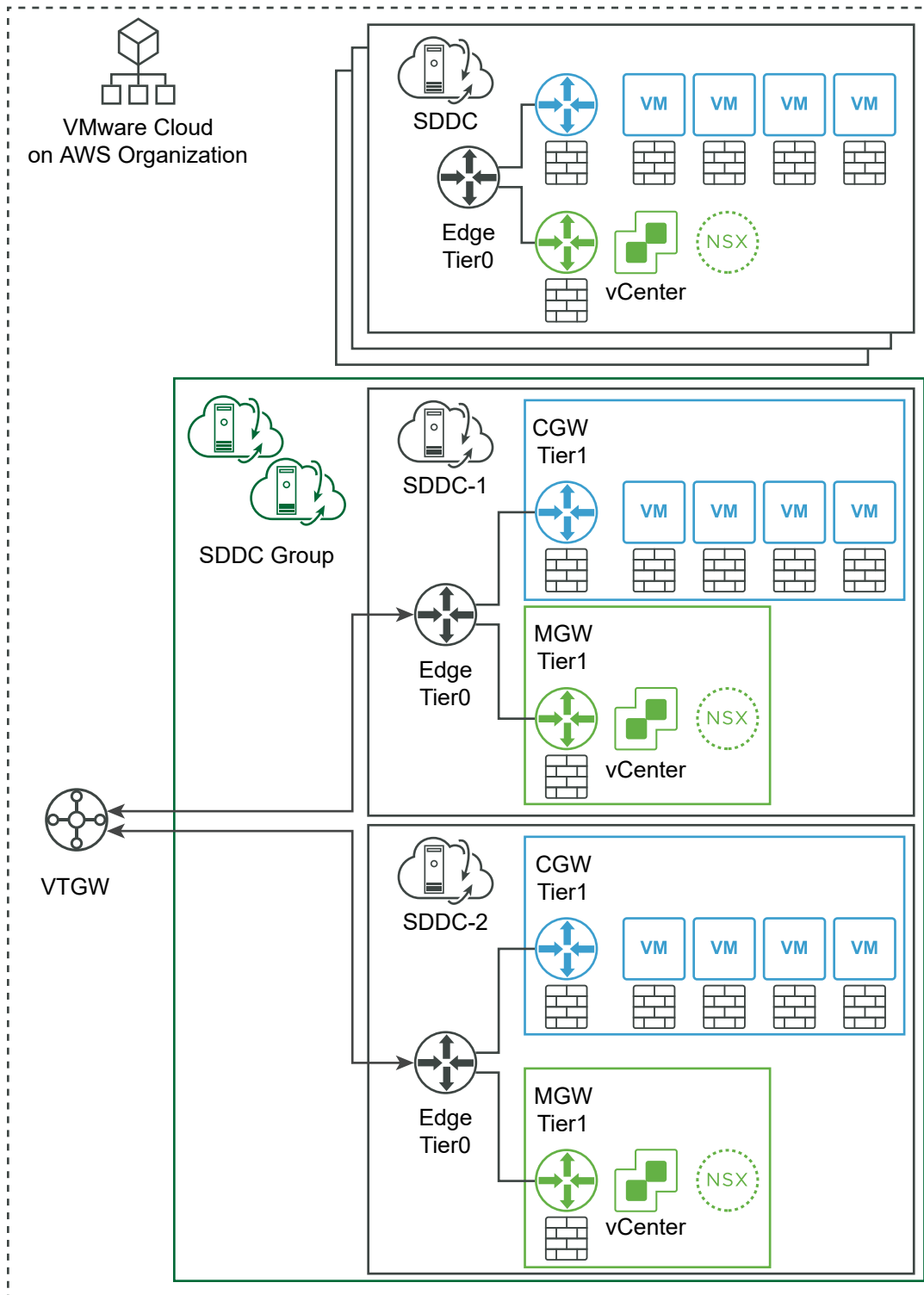
---

## Internal Group Connectivity Using VMware Transit Connect

Peer connectivity among SDDC group members requires a VMware Managed Transit Gateway (VTGW). This is an AWS resource owned and managed by VMware. Adding the first member to an SDDC Group creates one of these resources and assigns it to the group. Creation and operation of a VTGW incurs additional charges on your VMware Cloud on AWS bill. When a group has members in more than one region, a VTGW is created in each of those regions.



Figure 1-1. VMware Transit Connect Connects SDDCs in the Group With Each Other

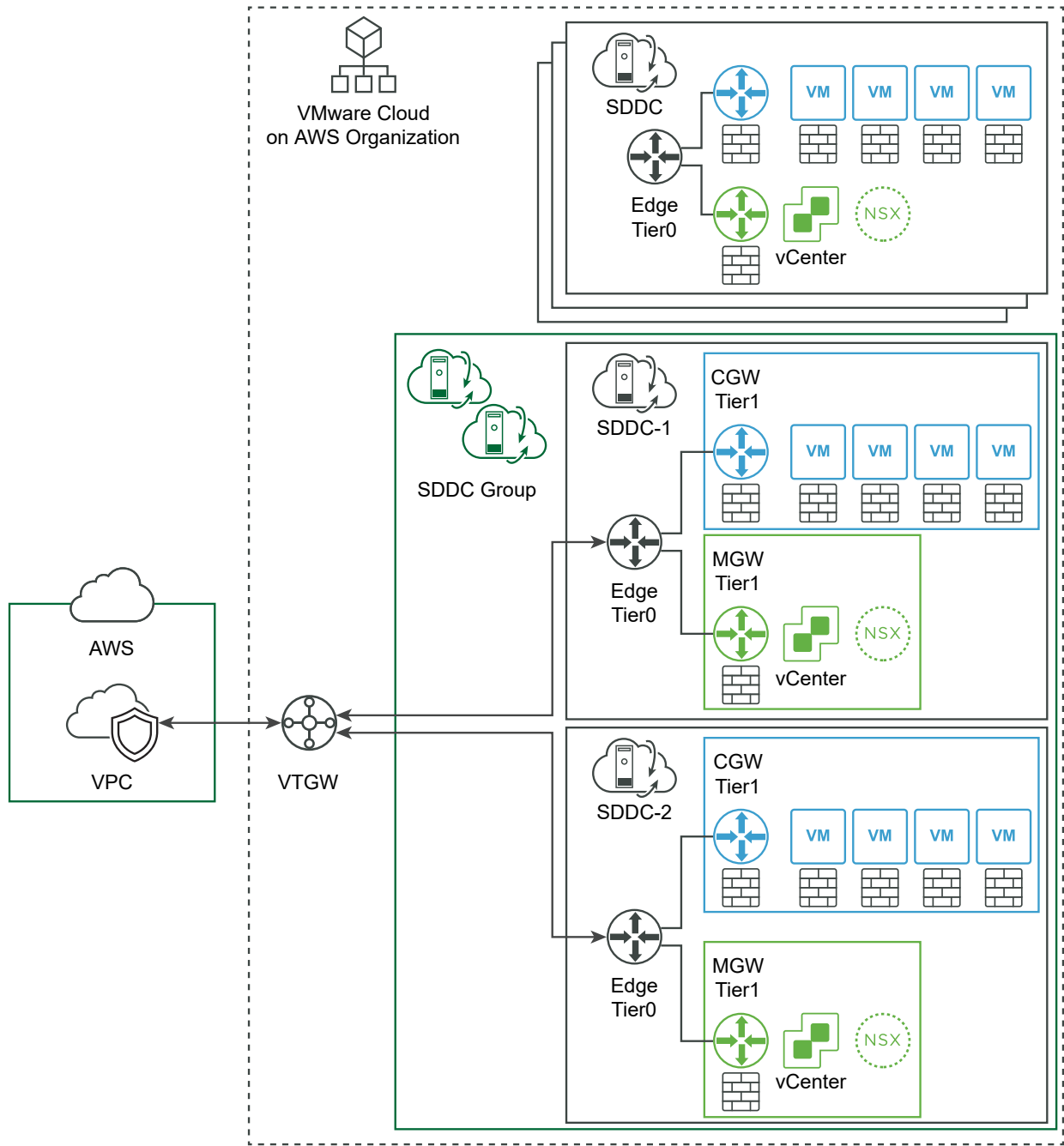


Members can be added to and removed from a group as needed. You cannot remove a group until all members have been removed. Removing the group also destroys the group's VMware Managed Transit Gateway.

## Attaching a VPC to an SDDC Group

Attaching a VPC to an SDDC group simplifies network connections between SDDCs in the group and AWS services that run in that VPC. You use the VMC Console to make the VTGW (an AWS resource) available for sharing, then use the AWS console to accept the shared resource and associate it with the VPCs you'd like to attach to the SDDC Group. VTGW connections to attached VPCs do not span regions in a multi-region group.

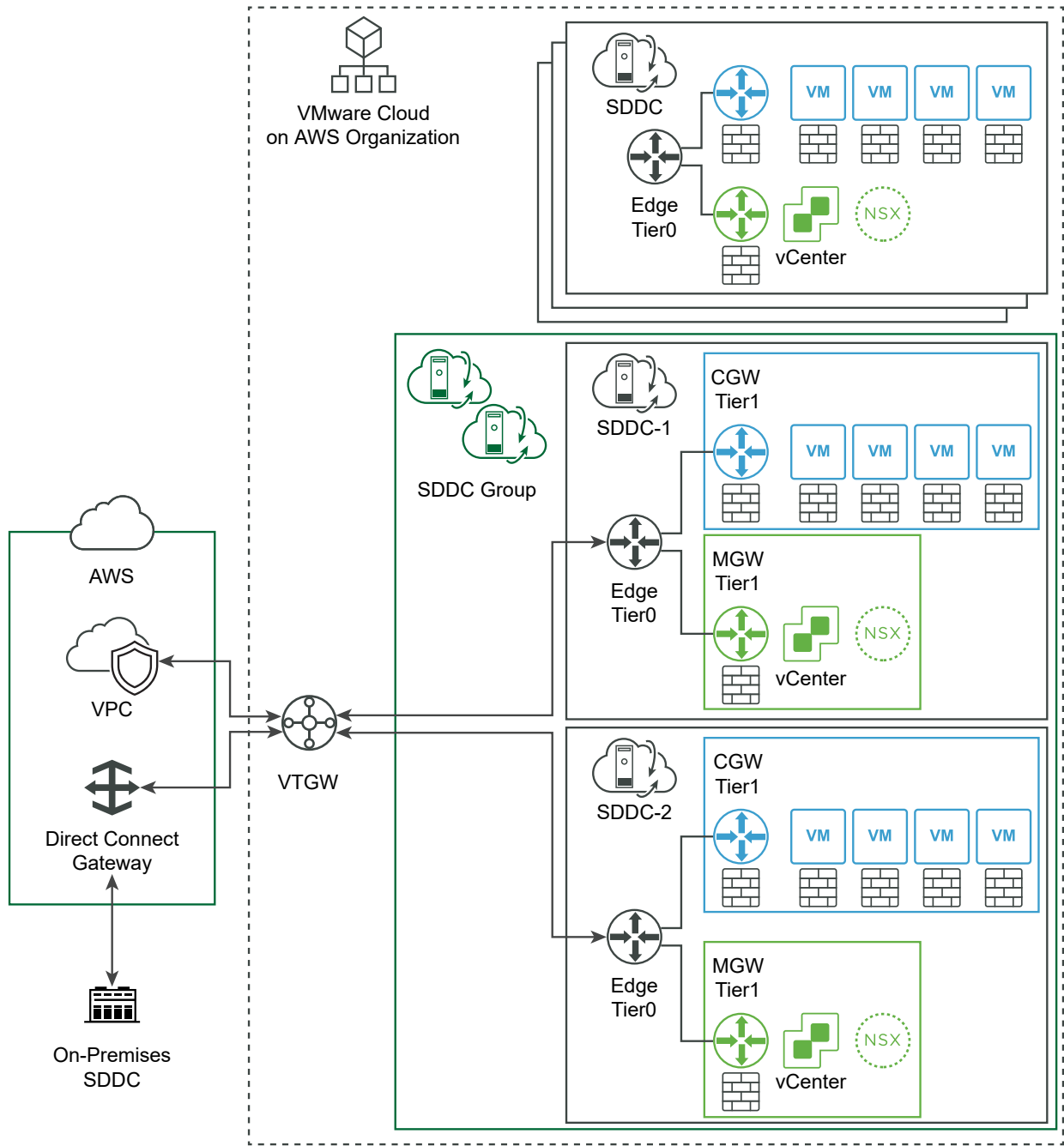
Figure 1-2. Using VMware Transit Connect to Attach a VPC to an SDDC Group



## External Group Connectivity Using AWS Direct Connect Gateway

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

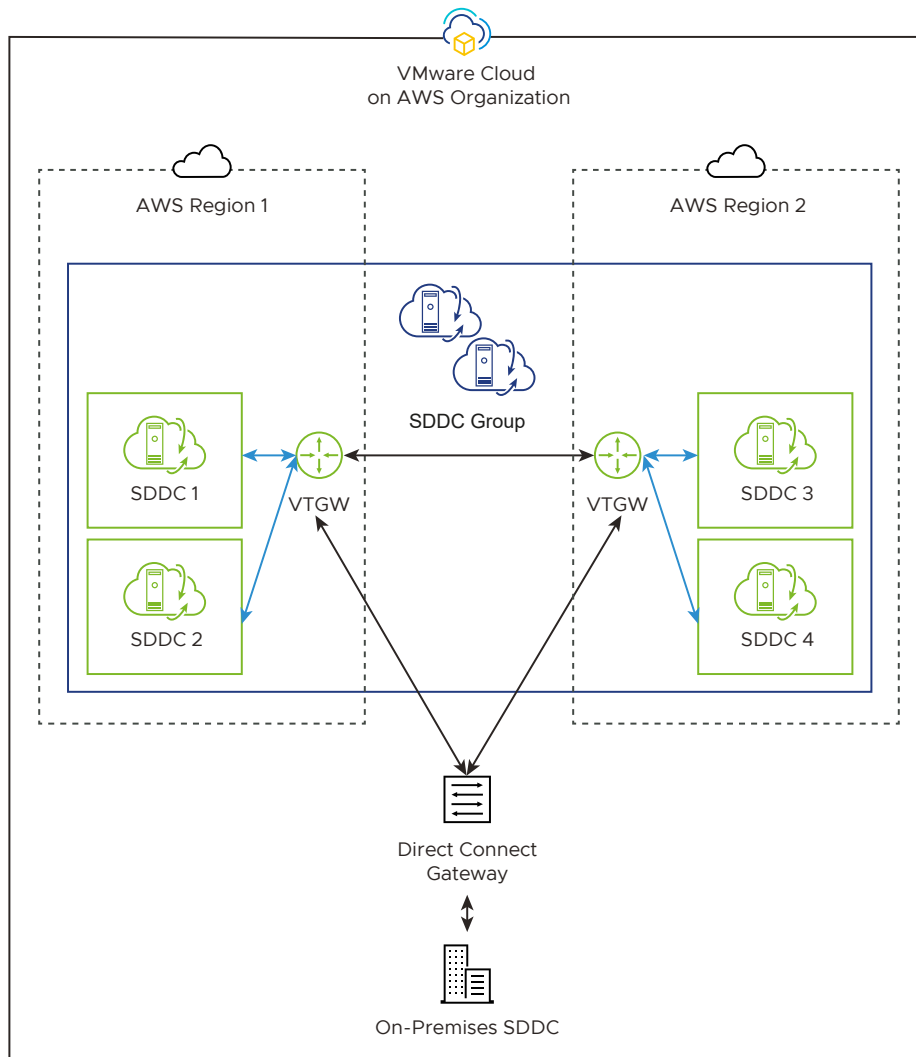
Figure 1-3. An AWS Direct Connect Gateway Connects the SDDC Group to On-Premises SDDCs



## Group SDDCs from Multiple Regions

A multi-region SDDC group provides the same kinds of connectivity as a single-region SDDC group, including connections to VPCs and on-premises data centers, although connections to VPCs do not span regions. When a group has members in more than one region, group creation provisions a VTGW in each of those regions and connects it to the group members in that region. This VTGW is peered with the other VTGWs in the group to provide a single IP address space that includes all group members. To be included in a multi-region SDDC group, an SDDC must be at version 1.15 or later. VPC associations to a group are valid only within the region occupied by the VPC. SDDC group members in other regions cannot access the VPC over the VTGW.

Figure 1-4. Multi-Region SDDC Group



## Routing and Peering

SDDC group members advertise their local network segments, which are added to the route tables of the SDDC's Tier-0 router and the group's VTGW. To view or download a list of VMware Transit Connect routes learned and advertised by a member SDDC, open the SDDC's **Networking & Security** tab and click **Transit Connect**. See [View Routes Learned and Advertised over VMware Transit Connect](#) in the *VMware Cloud on AWS Networking and Security* guide. Peering between VTGW instances is supported within the same region or across different regions.

To view the routes learned and advertised by all SDDCs in the group, click the **Routing** tab. You can use the drop-down control. Select **External** to view routes between members or **Members** to view routes between members and external endpoints like VPCs or Direct Connect Gateways. **External** routes carry traffic originating from an external endpoint like a VPC or DXGW to an SDDC group member. **Members** routes carry traffic originating in a member SDDC and include SDDC group members and external endpoints.

SDDCs in the group learn routes to the networks advertised by other SDDCs in the group and those advertised over the group's DXGW. They also learn the CIDRs for any VPCs attached to the group. Because AWS imposes a limit of 20 prefixes that can be advertised by a DXGW to an external endpoint like an on-premises SDDC, the CIDR block prefixes of all SDDC group members must fall within a range that can be summarized without exceeding that limit.

VMware Transit Connect enforces several routing policies:

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

---

**Note** When an SDDC becomes a member of an SDDC group, several aspects of existing SDDC networking change:

- Routes advertised by a route-based VPN are preferred over routes advertised by VMware Transit Connect or a DXGW. However, all outbound traffic from hosts to destinations outside the SDDC network is routed to the VTGW or private VIF regardless of other routing configurations in the SDDC. This includes vMotion and vSphere replication traffic. You must ensure that inbound traffic to ESXi hosts is also routed over the DXGW interface so that the inbound and outbound traffic paths are symmetrical.
  - If the same route is advertised over the VTGW and DX, the VTGW path is preferred. This includes routes from a DXGW connected to the VTGW.
  - The maximum MTU for intranet traffic among group members is limited to 8500 bytes. An MTU of up to 8900 bytes can still be used for traffic internal to the SDDC, or over DX. See [Create a Private Virtual Interface for SDDC Management and Compute Network Traffic](#) in the *VMware Cloud on AWS Networking and Security* guide.
- 

## Create or Modify an SDDC Group

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

## Prerequisites

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

## Procedure

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

2 On the **Inventory** page, click **SDDC Groups**.

3 On the **SDDC Groups** tab, click **ACTIONS** and select **Create SDDC Group**.

Give the group a **Name** and optional **Description**, then click **NEXT**. You can edit the group later to change these values.

4 On the **Membership** grid, select the SDDCs to include as group members.

The grid displays a list of all SDDCs in your organization. To qualify for membership in the group, an SDDC must meet several criteria:

- It must be at SDDC version 1.11 or later. Members of a multi-region group must be at SDDC version 1.15 or later.
- Its management network CIDR block cannot overlap the management CIDR block of any other group member.
- It cannot be a member of another SDDC Group.

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

5 Acknowledge that you understand and take responsibility for the costs you incur when you create an SDDC group, then click **CREATE GROUP** to create the SDDC Group and its VMware Transit Connect network.

Charges begin when you click **CREATE GROUP**. You cannot pause or cancel the process after it starts. Group members won't be able to use the group's VMware Transit Connect network until deployment is complete. Deployment typically takes about fifteen minutes. When deployment is complete, the group's **Connectivity Status** changes from **PENDING** to **CONNECTED**.

6 (Optional) To modify the group name and description or to add or remove group members, click **ACTIONS** and select **Edit Group**.

You cannot edit the group while its **Connectivity Status** is **PENDING**.

## What to do next

To view the routes learned and advertised by SDDCs, VPCs, and TGW/DGW instances in the group, click the **Routing** tab. Select **External** in the drop-down control to view routes used by external endpoints like VPCs or Direct Connect Gateways. Select **Members** to view routes used by member SDDCs.

To enable network traffic between workloads in member SDDCs, you'll need to create a set of compute gateway firewall rules in each member. See [Add Compute Gateway Firewall Rules to Enable SDDC Group Member Workload Connectivity](#) for details. You'll need to do this for each new member you add to the group.

## Attach a VPC to an SDDC Group

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

Although VMware Transit Connect handles all compute and management network traffic among SDDC group members, it does not automatically configure AWS route tables to send traffic originating from an external VPC or other AWS object to the SDDC group's VTGW. Network topologies that require this sort of connectivity include creation of a "security VPC" through which all traffic between the SDDC group and the Internet is routed for inspection, and any similar requirement to enable communication between AWS objects and SDDC Group members. This sort of network topology requires you to define the destination routes for traffic from the SDDC group's VTGW to the VPC, as we show in [Step 8](#)

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

### Procedure

- 1 On the **Inventory** page of the VMC Console, click **SDDC Groups**, then click the **Name** of the group to which you want to attach the VPC.
- 2 On the **External VPC** tab for the group, click **ADD ACCOUNT** and specify the AWS account that owns the VPC you want to attach to the group.  
  
This enables AWS resource sharing in that account for the VTGW.
- 3 In the AWS console, open **Resource Access Manager > Shared with me** to accept the shared VTGW resource.  
  
The resource **Name** has the form `VMC-Group-UUID` and a **Status** of **Pending**. Click the resource name to open the resource **Summary** card, then click **Accept resource share** and confirm acceptance,
- 4 In the VMC Console, return to the **VPC Connectivity** tab for the group and wait for **Status** of the resource share you accepted in [Step 3](#) to change from **ASSOCIATING** to **ASSOCIATED**.  
  
VPC resource association can take up to ten minutes. Once the VPC association is complete, you can attach the VTGW.
- 5 Return to the AWS console **Resource Access Manager** to find the resource ID of the shared VTGW resource.

It will be listed under **Shared with me: Shared resources** with a **Resource ID** of the form `TGW-UUID` and a **Resource type** of `ec2:TransitGateway`.



## 6 Create the Transit Gateway attachment.

- a Select the **Transit Gateway ID** identified in [Step 5](#) and specify an **Attachment type** of VPC, and select the **VPC ID** you would like to connect to the SDDC group.
- b Select a **Subnet ID** in each Availability Zone (AZ) that requires connectivity to the group.  
You can select only one subnet per AZ, but SDDC group members can communicate with all VPC subnets in that AZ.
- c If the VPC is an FSx VPC as described in [Configure Amazon FSx for NetApp ONTAP as External Storage](#), you must also select **DNS support**.
- d Click **Create Transit Gateway Attachment** to create the attachment.

## 7 In the VMC Console, return to the **External VPC** tab for the group and **ACCEPT** the shared VPC attachment.

When the VPC status changes to **PENDING\_ACCEPTANCE**, click **ACCEPT** to accept it. The status changes to **AVAILABLE** after the acceptance process completes. Acceptance can take up to ten minutes.

## 8 Configure additional routes to the VPC.


In the AWS console, identify the route tables associated with any subnets in the VPC connected to the shared VTGW and need to communicate with the SDDC Group. On the **Routes** tab of the route table, click **Edit Routes** and add any CIDRs in the SDDC group as the destination with the target set to the VTGW ID you identified in [Step 5](#). The list of CIDRs for the SDDC group can be found in the VMC Console for the SDDC group on the **Routing** tab, by selecting **External** in the **Route Table** drop-down.

As an alternative to manually editing the routes, consider creating a managed prefix list and adding it to the main route table associated with the VPC. See [Use a Managed Prefix List to Simplify Routing For External VPC and TGW Objects](#).

## 9 (Optional) Configure additional destination routes to the VPC.

When you create an SDDC group, the system creates routes for the VPC's primary CIDR and any secondary CIDRs. If you need to have destinations beyond the VPC routed through it (something you might need for a Security VPC or Transit VPC), you can define additional CIDR blocks to route to the attached VPC.

To create or modify routing from the group's VTGW to the external VPC, open the **External VPC** tab and select the **AWS Account ID** that owns the VPC and expand the row. If no routes have been specified, click **ADD ROUTES** in the **Routes** column to open the **Edit Routes** page and add one or more routes that use this VPC as a **Target**. Otherwise the **Routes** column

shows the first route and the number of additional routes. Click the pencil icon () to open the **Edit Routes** page so you can edit this list. Each prefix defines a route from the group's VTGW to the VPC listed in the **VPC ID** column. Each prefix also appears as a **Target** on the group's **Routing** tab. You can specify up to 100 routes to each attached VPC.

## What to do next

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

## Attach an AWS Transit Gateway to an SDDC Group

Attach an AWS Transit Gateway to an SDDC Group to enable SDDC Group members to facilitate network connections between SDDCs in the group and AWS services that run in any VPC in any region.

Attaching an AWS Transit Gateway (TGW) to an SDDC group is a multi-step process that requires you to use both the VMC Console and the AWS console. You use the VMC Console to request access to an existing TGW, then you use the AWS console to attach it to the SDDC Group's VTGW. Unlike a VTGW, which is an AWS resource managed by VMware, a TGW is a pure AWS resource that you can consume and manage on your own. See [Getting started with transit gateways](#) in the AWS documentation.

### Procedure

- 1 On the **Inventory** page of the VMC Console, click **SDDC Groups**, then click the **Name** of the group to which you want to attach the AWS TGW.
- 2 On the **External TGW** tab for the group, click **ADD TGW** and provide the required parameter and value information.

| Parameter                | Value  |
|--------------------------|--|
| <b>AWS account ID</b>    | The AWS account that owns the TGW.   |
| <b>TGW ID</b>            | The AWS ID of the TGW. You can use an existing TGW owned by the specified AWS account or create a new one in that account. |
| <b>TGW Location</b>      | The AWS region where the TGW resides.  |
| <b>VMC on AWS Region</b> | The AWS region where the SDDC group resides.   |
| <b>Routes</b>            | AWS resource destination prefixes reachable via this peering connection  |

Click **ADD** to add the TGW as a peer to the group's VTGW. When **Status** column changes to **PENDING\_ACCEPTANCE**, proceed to [Step 3](#)

- 3 Log in to the AWS console with administrator credentials for the AWS Account ID you specified in [Step 2](#).

In the AWS console navigate to **Transit Gateway Attachments**, select the TGW whose TGW ID matches the one you specified in [Step 2](#) and click **Accept Transit Gateway Attachment**.

- 4 In the VMC Console, return to the **External TGW** tab for the group and verify that the TGW **State** has changed to **ASSOCIATED**.

## 5 (Optional) Associate an AWS route table with the attached TGW.


Peering sessions for the new TGW require the TGW attachment to be associated with an AWS route table. In some environments, a route table won't be associated with the attachment by default, so you'll need use the AWS console and associate a routing table with the attachment. See "Add routes between the transit gateway and your VPCs" in [Getting started with transit gateways](#).

## 6 Create CGW firewall rules to enable workload traffic through the TGW.

See [Add Compute Gateway Firewall Rules to Enable SDDC Group Member Workload Connectivity](#).

## 7 Configure additional source and destination routes in the SDDC or AWS routing tables.

To create or modify routing from the group's VTGW to the external TGW, open the **External TGW** tab. Select the **AWS Account ID** that owns the TGW and expand the row. If no routes have been specified, click **ADD ROUTES** in the **Routes** column to open the **Edit Routes** page and add one or more routes that use this TGW as a **Target**. Otherwise the **Routes** column

shows the first route and the number of additional routes. Click the pencil icon (  ) to open the **Edit Routes** page so you can edit this list. Each prefix defines a route from the group's VTGW to the TGW listed in the **TGW Peering Attachment ID** column. Each prefix also appears as a **Target** on the group's **Routing** tab. You can specify up to 100 routes to each attached TGW.

As an alternative to manually editing the routes, consider creating a managed prefix list and adding it to the main route table associated with the TGW. See [Use a Managed Prefix List to Simplify Routing For External VPC and TGW Objects](#).

See [Getting Started with VMware Transit Connect Intra-Region Peering for VMware Cloud on AWS](#) for examples and suggestions.

## Use a Managed Prefix List to Simplify Routing For External VPC and TGW Objects

When you extend SDDC Group connectivity to include native AWS objects such as VPCs, Transit Gateways (TGWs), and Direct Connect Gateways (DXGWs) that you own and manage, you must also edit VPC route tables or a VMware Cloud on AWS managed prefix list to establish and maintain connectivity between the group's VTGW and these objects.

Route management for connections between VMware Cloud on AWS networks and native AWS objects depends on your network topology. For all topologies that include native AWS objects such as TGWs and VPCs, you must define return paths from those objects to the SDDC group, as shown in [Attach a VPC to an SDDC Group](#) and [Attach an AWS Transit Gateway to an SDDC Group](#). Topologies that send traffic from the SDDC group to a native AWS object (such as a "security VPC" through which all traffic between the SDDC group and the Internet is routed for inspection) require you to configure those outbound routes manually, either by editing native route tables as described in the AWS [Virtual Private Cloud User Guide](#), or by using a VMware Cloud on AWS managed prefix list.

A managed prefix list (a list of subnet CIDRs that VMware manages and shares with your AWS account) is the best option for most SDDC groups, since it updates external VPC and TGW route tables automatically during NSX Edge migration or failover, and whenever SDDC group members are added and removed.

#### Procedure

- 1 On the **Inventory** page of the VMC Console, click **SDDC Groups**, then click the **Name** of the group that has the VPC attached.

- 2 To create a managed prefix list that you can use to simplify manual maintenance of routes to and from the group members' subnets and external AWS objects, open the **Routing** tab for the group and click **CREATE PREFIX LIST**.

You can skip this step if you want to manually update the external VPC's route tables.

- a On the **Create Prefix List** card, fill in the required values, then click **CREATE PREFIX LIST**.

|                                  |   |
|----------------------------------|---|
| <b>Prefix List Name</b>          | Make up a name.   |
| <b>VMC on AWS Region</b>         | Select a region from the list of AWS regions occupied by SDDC group members.  |
| <b>AWS Region</b>                | The region where you want the prefix list to be created. Initially the same as the <b>VMC on AWS Region</b> value, but you can change it to have the prefix list created in a different region. |
| <b>AWS Accounts to associate</b> | This list is prepopulated with the 12-digit AWS account IDs associated with the SDDC group. You can add or remove account IDs as needed.  |

When you click **CREATE PREFIX LIST**, the **Status** of the prefix list changes to **Creation in Progress**.

- b When the **Status** of the prefix list changes to **Created**, use an AWS identity that has permission to accept a resource share and log into the AWS console using one of the **Associated AWS Accounts**.

Click **Resource Access Manager > Shared with me** to see a list of AWS resources shares the account can access. The resource **Name** has the form `VMC-SHARED-PREFIX-LIST-ID` and a **Status** of **Pending**. Click the resource **Name** to open the resource share details card, then click **Accept resource share** and confirm acceptance.

- c In the AWS console, open **Your VPCs**, select a VPC, and add one or more prefixes to the VPC's main route table.

Click **Add route**, enter the prefix list ID as a **Destination** and specify the SDDC group's VTGW as the **Target**.

**Note** Each prefix list counts as a single **Route** when added to a route table but can contain many entries, each of which counts toward the route table's quota. See [AWS VPC route table quotas](#) and be sure that the route table has sufficient capacity to accommodate all the routes in the prefix list.

After you add a prefix list to a VPC route table, all routes from SDDC group members to target TGW or VPC objects are updated automatically.

- 3 To modify or remove a managed prefix list, open the **Routing** tab for the group.

- To modify a **Prefix List Name** or its **Associated AWS Accounts** click the pencil icon (✎) to open the **Edit Prefix List Name** or **Associate AWS Accounts** card.

- To remove a prefix list, select it and click **DELETE PREFIX LIST**. You must remove any resources (such as route tables) associated with the list before you delete it.
- 4 To view the current set of routes programmed (either manually or from a managed prefix list) for this SDDC group, open the **Routing** tab for the group.

You can view routes to **Members** (SDDCs in the group along with the group's VTGW and any connected VPCs), or to **External** endpoints (SDDCs in other groups). You can filter each list by object Type (SDDC, VPC, or TGW).

## Aggregate and Filter Routes to Uplinks

Use route aggregation and filtering to control the set of routes advertised to SDDC network uplinks like Direct Connect, VMware Transit Connect and the Connected VPC. You'll need this in cases where you have to reduce the number of entries in a VPC route table or limit the set of routes that are advertised to external connections.

In SDDCs at version 1.17 and later, you can use the NSX Manager Web Interface to aggregate routes to the INTRANET and SERVICES uplinks. And beginning at SDDC version 1.20, you can also use NSX Manager to filter the set of routes advertised to those uplinks. Route aggregation and filtering are not exposed in the legacy VMC Console **Networking & Security** tab.

In the default configuration, all segments in the SDDC Compute Network are advertised to the Connected Amazon VPC and external connections such as AWS Direct Connect and VMware Transit Connect. You can manage the list of CIDRs that get advertised this way by aggregating and optionally filtering these routes. Filtered routes are not advertised to the selected uplinks. Management subnets are always advertised. When both aggregation and filtering are applied, aggregated subnets are advertised even though they may include CIDRS that would normally be filtered out. To view or download the current set of routes advertised to the Connected VPC open the NSX Manager **Networking** tab and click **Connected VPC > Advertised**. To view or download the current set of routes advertised to **Transit Connect**, see [View Routes Learned and Advertised over VMware Transit Connect](#).

### Procedure

- 1 Log in to VMware Cloud Services at <https://vmc.vmware.com>.
- 2 Click **Inventory > SDDCs**, then pick an SDDC card and click **VIEW DETAILS**.
- 3 Click **OPEN NSX MANAGER**.
- 4 Aggregate CGW subnet CIDRs.
  - a On the NSX Manager **Networking** tab, click **Global Configuration > Route Aggregation**.
  - b Create a prefix list of CIDR blocks to aggregate.

Under **Aggregation Prefix Lists**, click **ADD AGGREGATION PREFIX LIST** and give the list a **Name**, then click **Set** to open the **Set Prefixes** editor. Add prefix CIDRS as needed. The system normalizes any CIDRS that contain an inaccurate subnet (one in the middle of larger range).

- c Add a route configuration that includes the new prefix list.

Under **Route Configurations**, click **ADD ROUTE CONFIGURATION** and give the new configuration a **Name**. Select the **Aggregation Prefix List** you created and choose a **Connectivity Endpoint**:

- Select **INTRANET** to apply this routing configuration to Direct Connect and VMware Transit Connect.
- Select **SERVICES** to apply this routing configuration to the connected VPC. See [Enable AWS Managed Prefix List Mode for the Connected Amazon VPC](#) for information about how AWS Managed Prefix Lists affect aggregation of routes to the Connected VPC.

- d Click **SAVE** to create the new configuration.

**Aggregated** routes are flagged in the **Advertised Routes** table of the **Transit Connect** page and on the **Advertised** page of the **Connected Amazon VPC** tab.

- 5 (Optional) Apply route filtering to uplinks.

On the NSX Manager **Networking** tab, click **Global Configuration > Route Filtering**. Toggle **Egress Filtering** for one or both of the listed **Connectivity Endpoints** to prevent CGW subnets from being advertised to that endpoint.

- Select **INTRANET** to apply this routing configuration to Direct Connect and VMware Transit Connect.
- Select **SERVICES** to apply this routing configuration to the connected VPC.

---

**Note** Before you can apply route filtering to the SERVICES uplink, you must [Enable AWS Managed Prefix List Mode for the Connected Amazon VPC](#).

---

Non-default CGW segments are not advertised to the selected uplinks. These segments remain reachable when they are within an aggregation. Segments that are filtered out (not advertised) have a **Status** of **Filtered** on the **Advertised** page of the **Connected Amazon VPC** tab. Segments that are not filtered out (advertised) have a **Status** of **Success** on that page. Filtered routes that include an aggregation are flagged as **Aggregated** here and on the **Transit Connect** page (see [View Routes Learned and Advertised over VMware Transit Connect](#)).

## View SDDC Group Support Information

Support Information for an SDDC group includes its creation date, group ID, and VTGW IDs.

You can find SDDC group support Information on the **Support** tab for the SDDC Group. You can also use the vRealize Log Insight Cloud add-on to view events logged by an SDDC group. A vRealize Log Insight Cloud regex of the form `type\[SDDC_GROUP | SDDC_SHARE | EXTERNAL\]` returns SDDC group log entries in a stream.

### Prerequisites

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

**Procedure**

- 1 Log in to the VMC Console at <https://vmc.vmware.com>.
- 2 On the **Inventory** page, click **SDDC Groups**.
- 3 Click **VIEW DETAILS** on the card for a group to open the group **Summary** screen.
- 4 Click the **Support** tab to view **Support Information** for the group.

**Remove an SDDC Group**

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

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

**Prerequisites**

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

**Procedure**

- 1 Log in to the VMC Console at <https://vmc.vmware.com>.
- 2 On the **Inventory** page, click **SDDC Groups** and click the group you want to remove.
- 3 Click the **Name** checkbox to select all SDDCs in the group, then click **REMOVE SDDCS**.  
Confirm that you understand the implications of removing the SDDCs, then click **CONTINUE** to proceed with the removal. Removal can take several minutes per SDDC.
- 4 After all the SDDCs have been removed, click **ACTIONS > Delete Group** to remove the group and its associated AWS resources.  
Confirm that you understand the effects of removing the group, then click **DELETE GROUP** to proceed with the removal.

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

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

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



VMware Cloud on AWS defines a set of inventory groups intended for use in Compute Gateway firewall rules that provide high-level control over traffic among group members. These groups contain the prefixes (CIDR blocks) for routes learned over VMware Transit Connect and any AWS Transit Gateways owned by the SDDC's AWS account owner.

### Transit Connect Customer TGW Prefixes

Routes learned from customer-owned AWS Transit Gateways.

### Transit Connect DGW Prefixes

Routes learned from the group's Direct Connect Gateway.

### Transit Connect Native VPCs Prefixes

Routes learned from the group's attached VPCs.

### Transit Connect other SDDCs Prefixes

Routes learned from other SDDCs in the group.

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

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

### Procedure

- 1 On the **Networking & Security** tab, click **Gateway Firewall**.
- 2 Define inventory groups as needed to provide sources and destinations for workload traffic.

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

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

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

| Name                     | Sources                                     | Destinations | Services | Applied To               | Action |
|--------------------------|---|--------------|----------|--------------------------|--------|
| Inbound from other SDDCs | <b>Transit Connect other SDDCs Prefixes</b> | Any          | Any      | Direct Connect Interface | Allow  |

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

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

### Create the Groups

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

- A group named **Local Workloads** that includes segment prefixes for the SDDC's own workload segments.
- A group named **Peer Workloads** that includes segment prefixes for workload segments of other SDDCs in the group.
- A group named **Peer SDDC vCenters** that includes the private IP address of the vCenter in each SDDC in the group.

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

### Create the Rules

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

| Name                            | Sources                | Destinations           | Services  |
|---------------------------------|------------------------|------------------------|---|
| Local workload to peer workload | <b>Local Workloads</b> | <b>Peer Workloads</b>  | As needed for outbound traffic from local workloads to workloads in other group members |
| Peer workload to local workload | <b>Peer Workloads</b>  | <b>Local Workloads</b> | As needed for in traffic to local workloads from workloads in other group members       |

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

## Attach a Direct Connect Gateway to an SDDC Group

After you create an SDDC Group, you can connect an on-premises SDDC to that group's Direct Connect Gateway to give it DX connectivity to all members of the SDDC group.

VMware Transit Connect handles all compute and management network traffic among SDDC group members. Many SDDC group members will also need to make network connections to your on-premises data center. To enable these connections, associate an AWS Direct Connect Gateway with the group's VMware Managed Transit Gateway.

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

### Prerequisites

You must create an AWS Direct Connect Gateway. See [Creating a Direct Connect gateway](#) in the AWS documentation.

### Procedure

- 1 On the **Inventory** page of the VMC Console, click **SDDC Groups**, then click the **Name** of the group to which you want to attach the Direct Connect Gateway.
- 2 On the **Direct Connect** tab for the group, click **ADD ACCOUNT** and specify the AWS account that owns the Direct Connect Gateway you want to add to the group.

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

| Option                                      | Description  |
|---|--|
| <b>Direct Connect Gateway Attachment ID</b> | The ID value, displayed on the AWS console <b>Direct Connect Gateways</b> page for the gateway object.   |
| <b>Location</b>                             | Specifies additional regional VTGW attachments for this gateway. A single Direct Connect gateway attachment in any region can handle traffic among all members of a multi-region group, but transitive routing is not supported. If a group has members in two different regions but only a single DXGW connection, only traffic from the SDDC in the region connected to the DXGW is routed to the on-premises data center. Use the <b>VTGW Location</b> control to associate the DXGW with a VTGW in another region. |
| <b>Allowed Prefixes</b>                     | A comma-separated list of compute network CIDR blocks of SDDC group members for the specified <b>VTGW Location</b> .   |

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

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

Acceptance can take up to 20 minutes. When it completes:

- In the AWS console, the gateway will have a **State** of **associated** on the AWS **Direct Connect Gateways** page for the gateway object.
- In the VMC Console, the gateway will have a **State** of **Connected** in the **Direct Connect** tab for the group.

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

See [Transit gateway attachments to a Direct Connect gateway](#) in the AWS VPC documentation.

- 5 (Optional) Add a Direct Connect Gateway location.

In a multi-region SDDC group, you can attach a group VTGW in any region to a Direct Connect Gateway. On the **Direct Connect Gateway** tab for the group, click **ADD LOCATION** to open the **Add Direct Connect Gateway Location** card, then specify an AWS region to attach to the gateway and one or more **Allowed Prefixes**.

### What to do next

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

## Use vCenter Linking in an SDDC Group

An organization that includes an SDDC deployment group can link the vCenter Server systems in those SDDCs to enable an administrator to manage their combined inventories in the same vSphere Client view.

When you enable vCenter linking in an SDDC group, a cloud administrator can log in as `cloudadmin@vmc.local` and use the vSphere Client to manage all the vCenter Server systems in the group. If the `cloudadmin@vmc.local` account configures these systems to use single sign-on, then users with accounts in that single sign-on domain can access all the linked systems in the group.

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

### Prerequisites

### Networking

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

Migration with vMotion of a VM across the vCenter Server instances in a linked SDDC group does not work because VMware Transit Connect creates only L3 connectivity between the group members. Migration with vMotion requires L2 connectivity.

### SDDC Version

vCenter Linking requires SDDC version 1.12 or higher.

## Service Role

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

## vCenter Name Resolution

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

## Hybrid Linked Mode

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

## VMware Cloud Disaster Recovery

vCenter Linking is not supported for SDDCs that are protected by VMware Cloud Disaster Recovery.

### Procedure

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

- 2 On the **Inventory** page, click **SDDC Groups**.

This page lists all the SDDC groups in your organization. To create an SDDC group, see [Create or Modify an SDDC Group](#).

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

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

- 4 To link all the vCenter Server systems in the list, click **LINK ALL VCENTERS**.

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

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

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

## 6 To unlink all the vCenter Server systems in the list, click **UNLINK ALL VCENTERS**.

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

# Configure SDDC Compliance Hardening

To prepare an SDDC to run workloads that must be periodically audited to verify compliance with standards such as the Payment Card Industry Data Security Standard (PCI DSS) and Information Security Registered Assessors Program (IRAP), you must disable access to the VMC Console **Networking & Security** tab and also disable certain SDDC add-on services.

Compliance hardening of a VMware Cloud on AWS SDDC helps you provide a runtime environment suitable for compliance-audited workloads. VMware Cloud on AWS SDDC compliance hardening uses a shared accountability model that distributes security and compliance responsibilities among AWS, VMware, and the customer. Read the Technical White Paper [Migrating PCI Workloads to VMware Cloud on AWS](#) for supplemental guidance covering the responsibilities and ownership of compliance hardening functions in VMware Cloud on AWS.

---

**Note** VMware Cloud on AWS does not enable compliance hardening by default. Contact your account team for more information.

Compliance hardening can be configured in new SDDCs at version 1.14 and later created in an AWS region that provides the appropriate support, as shown in [Choosing a Region](#).

---

Because certain SDDC features and add-on services are not compatible with compliance hardening requirements, you must disable them before migrating PCI workloads to your SDDC.

## Disable Networking & Security Tab Access

To prepare a new SDDC to run compliance-audited workloads, you must create a firewall rule that allows you to connect directly to the SDDC's local NSX Manager, then disable the VMC Console **Networking & Security** tab and use the local NSX Manager to manage your SDDC networks.

Access controls on the VMC Console **Networking & Security** tab are not appropriate for a compliance-hardened SDDC. Any access to an SDDC using the **Networking & Security** tab renders the SDDC non-compliant. To maintain compliance, you must manage your SDDC networks using only the local NSX Manager, which has an authentication framework that meets compliance hardening requirements. Access to the **Networking & Security** tab must be disabled before you begin a compliance audit, and must remain disabled the duration of the audited period.

Before you disable access to the **Networking & Security** tab, you'll use it to create a VPN connection to your on-premises data center and a management gateway firewall rule that allows you to access the local NSX Manager over that VPN. After you verify that you can access NSX Manager, you can proceed to prepare the SDDC for compliance hardening by disabling access to the **Networking & Security** tab. If you need to re-enable access to the **Networking & Security** tab, contact VMware Support.

### Prerequisites

- You must be logged into the VMC console as a user with a VMC service role of **Administrator** or **Administrator (Delete Restricted)**.
- You must have a VPN connection to the SDDC. See [Configure a VPN Connection Between Your SDDC and On-Premises Data Center](#) in the *VMware Cloud on AWS Networking and Security* guide. After you have disabled Networking & Security tab access, a connection to the local NSX Manager over a VPN is the only way to manage your SDDC network. To ensure that you can reach the local NSX Manager in the event of a network failure, we recommend configuring a redundant connection such as AWS Direct Connect to with a route-based VPN as the backup, as described in [Configure Direct Connect to a Private Virtual Interface for SDDC Management and Compute Network Traffic](#) in the *VMware Cloud on AWS Networking and Security* guide.
- Compliance hardening must be enabled in the SDDC. VMware Cloud on AWS does not enable compliance hardening by default. Contact your account team for more information. Compliance hardening can be configured in SDDCs at version 1.14 and later created in an AWS region that provides the appropriate support, as shown in [Choosing a Region](#).

### Procedure

- 1 Log in to the VMC Console at <https://vmc.vmware.com>.
- 2 Create a Management Gateway firewall rule that allows you to open an HTTPS connection to the local NSX Manager for this SDDC.

See [Add or Modify Management Gateway Firewall Rules](#) in the *VMware Cloud on AWS Networking and Security* guide for more information about how to create a Management Gateway firewall rule. The rule must have the following parameters:

| MGW Firewall Rule Property | Value  |
|----------------------------|--|
| Sources                    | <b>Any</b> , or a specific IP address in your on-premises network. |
| Destinations               | The <b>NSX Manager</b> system-defined group.                       |

| MGW Firewall Rule Property | Value           |
|----------------------------|-----------------|
| Services                   | HTTPS (TCP 443) |
| Action                     | Allow           |

### 3 (Required) Test the firewall rule.

You cannot gain access to the local NSX manager until you have disabled access to the **Networking & Security** tab, so it's important to verify that your firewall rule works before you proceed with the next step. To test the rule, verify that you can view the local NSX manager's `index.html` page. Use a Web browser to open a connection to `https://NSX-Manager-IP/nsx/index.html` where *NSX-Manager-IP* is the **Private IP** shown under **Access NSX Manager via internal network** in **NSX Manager Information** on the **Settings** tab of your SDDC. If your firewall rule is correct, this request returns the local NSX Manager's `index.html` page, which displays several JSON key/value pairs, including `error_code: 403`. You cannot take any actions on this page.

### 4 After you have verified that your firewall rule is correct, you can proceed to disable access to the **Networking & Security** tab.

- Navigate to the **Settings** tab of your SDDC.
- On the **Compliance Hardening** section of the **Settings** tab, expand the **Networking & Security tab access** line to display the **Disable Networking & Security tab access** card.
- Confirm your understanding of the workflow.

After you have verified that you can access the local NSX Manager's `index.html` page, select the checkbox to confirm that you have created and tested the necessary firewall rule and are ready to proceed. Select the checkbox to confirm that you understand that you'll need to file a VMware support request if you want to re-enable access to the **Networking & Security** tab for this SDDC.

- Click **DISABLE** to disable Networking & Security access.

### 5 Open NSX Manager.

Log in to the VMC Console and open the **Networking & Security** tab. Click the **OPEN NSX MANAGER** button on this tab and log in with the **Default NSX Manager Credentials**. See [NSX Manager](#) in the *NSX-T Data Center Administration Guide* for information about how to use NSX Manager.

---

**Note** If you want to view (but not modify) the networking configuration for this SDDC, you can log in with the credentials of the **NSX Manager Audit User Account**, which are available under **NSX Manager Information** on the **Settings** tab.

---



## What to do next

After you have disabled Networking & Security tab access, you must use the local NSX Manager to manage your SDDC network. You can navigate the NSX Manager UI in much the same way as you navigate the **Networking & Security** tab. See [NSX Manager](#) in the *NSX-T Data Center Administration Guide* for information about how to use NSX Manager.

---

**Important** To conform with PCI compliance requirement 8.2.4 (Change user passwords/passphrases at least once every 90 days), you must use the NSX manager REST API, as documented in VMware Knowledge Base article [83551](#).

---

If you need to re-enable access to the **Networking & Security** tab, contact VMware Support.

## Disable Add-On Services

To prepare an existing SDDC to run compliance-audited workloads, you must disable certain add-on services.

Because certain SDDC add-on services are not compatible with compliance hardening, you must disable them before migrating compliance-audited workloads to your SDDC. If you disable SDDC add-on services, you'll need to contact VMware Support to have them re-enabled.

---

**Note** Add-on services are not enabled in a new SDDC. This procedure is only required when reconfiguring an existing SDDC to disable its add-on services.

---

### Prerequisites

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

### Procedure

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

The **Compliance Hardening** area of this tab displays the status of the VMware HCX and VMware Site Recovery add-ons.

- 3 Disable the VMware HCX Add-On. (You can install and enable HCX in a new SDDC and use it to migrate compliance-audited workloads, but after that migration is complete, you must disable it. )

On the **Compliance Hardening** section of the **Settings** tab, expand the **HCX Add-on** control to display the **Disable VMware HCX add-on** card.

- a Uninstall HCX from the SDDC vCenter.

If you have created any custom firewall rules that reference HCX inventory groups, remove them before you begin to uninstall HCX, then follow the procedures documented in [Uninstalling HCX in VMware Cloud on AWS Deployments](#) to clean up SDDC resources created or used by VMware HCX. After HCX has been uninstalled, select the checkbox to confirm that the clean-up is complete and you are ready to proceed.

- b Click **DISABLE** to open the **Disable VMware HCX add-on** page.

- c Confirm that you understand the workflow:

- Select the checkbox to confirm that you have uninstalled HCX and cleaned up any remaining HCX resources (see [3.a](#)).
- Select the checkbox to confirm that you understand that you'll need to contact VMware support if you want to re-enable the VMware HXC add-on for this SDDC.

- d Click **DISABLE** to disable the VMware HCX add-on.

- 4 Disable VMware Site Recovery 8.4 Compatibility.

VMware Site Recovery meets compliance audit requirements at version 8.5 and later.

You must disable compatibility with Site Recovery 8.4 add-on to prepare an SDDC to run compliance-audited workloads.

Use the vSphere Client to verify the version of VMware Site Recovery that is active in your SDDC. If VMware Site Recovery is not active in your SDDC, after Activate on SDDC at version 1.14 and later, version 8.5 or later will be provisioned. If VMware Site Recovery is active in your SDDC with version 8.4 you can contact support to have the Site Recovery add-on upgraded to 8.5 or later or deactivate Site Recovery.

On the Compliance Hardening section of the Settings tab, expand the Site Recovery Add-on v8.4 compatibility control to display the Disable VMware Site Recovery 8.4 add-on compatibility control.

- a (Optional) (If using 8.4 and no longer need it) Follow the procedures documented in [Deactivate VMware Site Recovery](#) to clean up SDDC resources created or used by VMware Site Recovery.
- b (Optional) (If using 8.4 and no longer need it) Uninstall Site Recovery Manager from the on-premises site. See [Uninstall Site Recovery Manager on the on-premises site](#) in the VMware Site Recovery Product Documentation.

- c (Optional) (If using 8.4 and still need Site Recovery) Contact support to have the Site Recovery add-on upgraded to 8.5. Proceed with the remaining steps only after the upgrade to 8.5 or later has been completed.
- d Click **DISABLE** to open the **Disable Site Recovery Add-On v8.4 Compatibility** page.
- e Confirm that you understand the workflow: Select the checkbox to confirm that you have checked VSR add-on version and if active with 8.4 - have either deactivated it and uninstalled Site Recovery Manager or requested its upgrade and it has been upgraded to 8.5 or later. (see 4.a, 4.b and 4.c). Select the checkbox to confirm that you understand that you'll need to contact VMware support if you want to re-enable Site Recovery 8.4 Compatibility for this SDDC.
- f Click **DISABLE** to disable compatibility with the VMware Site Recovery add-on.

## Using VMware Tanzu™ Kubernetes Grid™ with VMware Cloud on AWS

Tanzu Kubernetes Grid is a managed service offered by VMware Cloud on AWS. Activate Tanzu Kubernetes Grid in one or more SDDC clusters to configure Tanzu support in the SDDC vCenter Server.

### Tanzu Services in the Cloud

Like vSphere, Tanzu services in your VMware Cloud on AWS SDDC work very much like they do in an on-premises data center. Because some vSphere and Tanzu components are managed by VMware, a few of the on-premises administrative workflows that you're familiar with aren't needed when you use Tanzu Kubernetes Grid with VMware Cloud on AWS.

For information about Tanzu Kubernetes Grid administration in VMware Cloud on AWS, you can refer to the [VMware Tanzu 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.
- In VMware Cloud on AWS, the Tanzu workload control plane can be activated only through the VMC Console.

In addition to the high-level differences we've noted, many topics in the [VMware Tanzu Documentation](#) are written specifically for on-premises users, and don't include some of the information you need when using Tanzu services in VMware Cloud on AWS.

Table 1-3. Topic Content Differences Between On-Premises and SDDC Tanzu

| Topic   | Content Highlights   |
|---|--|
| <ul style="list-style-type: none"> <li>■ <a href="#">Creating and Managing Content Libraries for Tanzu Kubernetes releases</a></li> <li>■ <a href="#">Migrate Tanzu Kubernetes Clusters to a New Content Library</a></li> </ul> | Tanzu Kubernetes Grid for VMware Cloud on AWS is pre-provisioned with a VMC-specific content library that you cannot modify.   |
| <a href="#">vSphere with Tanzu User Roles and Workflows</a>   | The vCenter Server in your SDDC includes a predefined <b>CloudAdmin</b> role that is not present in your on-premises vCenter. This role has privileges required to create and manage workloads on your SDDC, but does not allow access to SDDC management components that are supported and managed by VMware, such as hosts, clusters, and management virtual machines. |
| <a href="#">Deploying Workloads to vSphere Pods</a>   | Tanzu Kubernetes Grid for VMware Cloud on AWS does not support vSphere Pods.   |
| <a href="#">Provision a Self-Service Namespace Template</a>   | Creation of TanzuSupervisor Namespace templates is not supported by VMware Cloud on AWS.   |
| <ul style="list-style-type: none"> <li>■ <a href="#">Configure a vSphere Namespace for Tanzu Kubernetes releases</a></li> <li>■ <a href="#">Create and Configure a vSphere Namespace</a></li> </ul>                             | vSphere namespaces for Kubernetes releases are configured automatically during Tanzu Kubernetes Grid activation.   |
| <a href="#">Workflow for Provisioning Tanzu Kubernetes Clusters</a>   | Step 10 of this procedure, "Monitor the deployment of cluster nodes using the vSphere Client", does not apply to Tanzu Kubernetes Grid.  |
| <a href="#">Virtual Machine Classes for Tanzu Kubernetes Clusters</a>   | In Tanzu Kubernetes Grid, the VM Service allows probe definitions only for port 6443.  |

## The Workload Control Plane, Namespace Segments, and Tier-1 Gateways

Each vSphere namespace requires an SDDC network segment. To preserve network isolation between namespaces, the workload control plane creates a Tier-1 router in your SDDC network for each namespace you create. These routers, which are listed in the **Tier-1 Gateways** page of the SDDC **Networking & Security** tab handle east-west traffic between containers connected to the namespace segment, and route north-south traffic through namespace egress and ingress points. They function much like the Compute Gateway (CGW) in your SDDC, but unlike the CGW, which is created as part of the SDDC and persists for the life of the SDDC, these per-namespace Tier-1 gateways are created and destroyed along with the Tanzu namespaces they support.

For more about SDDC network architecture, see [NSX Networking Concepts](#) in the *VMware Cloud on AWS Networking and Security* guide, and read the VMware Tech Zone article [TKG Managed Service Networking](#).

## How Tanzu Activation Affects an SDDC Network

When you activate Tanzu Kubernetes Grid in a VMware Cloud on AWS SDDC, the system creates several additional Tier-1 routers for use by the Workload Control Plane. After activation, vSphere creates additional Tier 1 routers for each namespace you create. Read-only details about these routers are listed in the **Tier-1 Gateways** page of the SDDC.

In an SDDC that uses AWS Direct Connect, ingress and egress CIDRs are advertised to the DX connection. In an SDDC that is a member of an SDDC group, these CIDRs are advertised to the VTGW.

## Activate Tanzu Kubernetes Grid in an SDDC Cluster

Activating Tanzu Kubernetes Grid in a cluster in your SDDC configures cluster storage and compute resources and SDDC networking for use with Tanzu services.

You can start from the **Inventory** view or the **Launchpad**, or from any cluster card in the details view of an SDDC.

### Prerequisites

You must be logged in to the VMC Console at <https://vmc.vmware.com/> as a user with a VMware Cloud Services Service Role of **Administrator** or **Administrator (Delete Restricted)**.

You can activate Tanzu Kubernetes Grid in any SDDC at version 1.16 and later. Activation is a per-cluster workflow that you can initiate in any conventional cluster that was created at SDDC version 1.16 or later, has at least 112 GB of available memory, and has sufficient free resources to support 16 vCPUs. In a medium SDDC configuration, a cluster requires a minimum of three hosts to qualify for activation. In a large configuration, this minimum rises to four hosts. Stretched clusters are not supported.

If you want to enable Tanzu Kubernetes Grid on additional clusters, remember that three-host clusters must have the default core count (16) to ensure adequate failover capacity. Clusters with four or more hosts can have a reduced core count. See [Add a Cluster](#).

---

**Note** Transient activities that affect cluster resource consumption can cause the cluster eligibility test to fail. The best practice is to avoid activating Tanzu Kubernetes Grid on any cluster that is the source or destination of a VMware HCX migration.

---

Before you can use Tanzu Kubernetes Grid in your SDDC, you must be able to open the SDDC vCenter (see [Connect to vCenter Server](#) in the *VMware Cloud on AWS Getting Started* guide. Many common Tanzu Kubernetes Grid workflows require connectivity between your on-premises data center and your SDDC, as detailed in [Configure SDDC Networking and Security](#).

To activate Tanzu Kubernetes Grid, you must define several CIDR blocks for the Tanzu workload control plane. Those CIDR blocks cannot overlap existing ones assigned to the SDDC Management or Compute networks or your on-premises networks, and cannot be changed after activation, so you'll need to have a list of those CIDR blocks handy during this procedure.

## Procedure

- 1 Log in to the VMC Console at <https://vmc.vmware.com>.
- 2 Select one or more SDDCs for Tanzu Kubernetes Grid activation.

### To start from the Launchpad:

From the **Launchpad**, click **Kubernetes** in the **Solutions** column, then click **Learn More** and **Get Started** to open the **Get started with Tanzu Kubernetes Grid** view displaying a list of all SDDCs in your organization that are eligible for Tanzu Kubernetes Grid activation. Select one or more SDDCs in this list and click **NEXT**.

### To start from the Inventory view:

From the **Inventory** page, click **SDDCs**, then select an SDDC and click **VIEW DETAILS**.

- 3 Activate Tanzu Kubernetes Grid for a cluster.

On the cluster card, click **ACTIONS** and select **Activate Tanzu Kubernetes Grid**. VMware Cloud on AWS checks cluster resources to be sure that they meet requirements for activating Tanzu Kubernetes Grid, then prompts you to configure workload management networking.

#### 4 Configure the Workload Management Network.

See [The Workload Control Plane, Namespace Segments, and Tier-1 Gateways](#) for more about how Tanzu Kubernetes Grid configures and uses SDDC networks.

##### a Specify workload network CIDR blocks for this cluster.

CIDR blocks of size 16, 20, 23, or 26 are supported, and must be in one of the "private address space" blocks defined by [RFC 1918](#) (10.0.0.0/8, 172.16.0.0/12, or 192.168.0.0/16). For each CIDR block, specify a range of IP addresses that does not overlap with:

- the SDDC Management or Compute networks
- your on-premises network
- any CIDR block you specify in this cluster
- any CIDR block you specify in another cluster in this SDDC

For a complete list of IPv4 addresses reserved by VMware Cloud on AWS, see [Reserved Network Addresses](#) in the *VMware Cloud on AWS Networking and Security* guide. These CIDR blocks cannot be changed after you activate Tanzu Kubernetes Grid.

##### Service CIDR

This block of addresses is allocated to Tanzu supervisor services for the cluster. You can use the default CIDR block (10.96.0.0/24) or pick another one, but a span of at least /24 is required.

##### Namespace Network CIDR

This block of addresses is allocated to namespace segments. It should have a span of at least /23 to provide adequate capacity for Tanzu Kubernetes Grid workloads in the cluster. Consider a span of /16 or /12.

##### Ingress CIDR

This block of addresses is allocated to receive inbound traffic through load-balancers to containers. The system allocates a destination NAT (DNAT) address from this pool for each namespace in the cluster, so a span of /23 or /26 should be adequate.

##### Egress CIDR

This block of addresses is allocated to outbound traffic from containers and guest clusters. The system allocates a source NAT (SNAT) IP address from this pool for each namespace in the cluster, so a span of /23 or /26 should be adequate.

##### b Click **VALIDATE AND PROCEED** to validate the CIDR blocks you have specified.

You can't change workload network CIDR blocks after activation is complete for a cluster, so the system must validate the ranges you've specified before activation can proceed. Network range validation can take up to 15 seconds.

## 5 Review and activate.

Upon successful Network range validation, the system displays cluster and workload management network details. Click **ACTIVATE TANZU KUBERNETES GRID** to create these clusters and allocate the CIDR blocks. The SDDC **Summary** page shows that Tanzu Kubernetes Grid is **Activating**. The system displays a status message showing the cluster names and the time that activation started. When activation completes, the SDDC Summary page shows that Tanzu Kubernetes Grid is **Activated**.

### What to do next

After activation completes, open the **Workload Management** page of the vSphere Client. The new Tanzu Kubernetes Grid cluster is listed in the **Clusters** tab. The **Namespaces** tab lists the next steps you can take. One of the first steps you should consider is to [register this cluster with Tanzu Mission Control](#). For help configuring and using a newly-activated Tanzu Kubernetes Grid cluster, start with these pages from *vSphere with Tanzu Configuration and Management*:

- [Configuring and Managing vSphere Namespaces](#) (Self-service namespace Tanzu Kubernetes Grid templates are not supported by VMware Cloud on AWS.)
- [Connecting to vSphere with Tanzu Clusters](#)
- [Provisioning and Operating TKGS Clusters](#)

## Allow Internal Access to a Tanzu Kubernetes Grid Namespace

To provide access to workloads in a Tanzu Kubernetes Grid namespace from your internal network, create a Distributed Firewall rule that allows network access from a jump host to a namespace segment.

When using Tanzu Kubernetes Grid in a VMware Cloud on AWS SDDC, procedures like the one in [SSH to Tanzu Kubernetes Cluster Nodes as the System User Using a Password](#) require you to add a VMware Cloud on AWS distributed firewall rule to allow access to a namespace network. In this topic, we describe the firewall rule you'll need if you want to enable SSH access to a Tanzu Kubernetes Grid namespace in your SDDC from a jump host in a different Tanzu Kubernetes Grid namespace.

### Procedure

- 1 Log in to VMware Cloud Services at <https://vmc.vmware.com>.
- 2 Get the IP address of the jump host VM.

See [Create a Linux Jump Host VM](#). The IP address is shown vCenter UI under the **Summary** tab for the jump host VM.

- 3 Find the segment identifier for the namespace segment.

This is shown as **Network** under **Related Objects** on the **Summary** tab for any of the cluster nodes.



- 4 Create a Distributed Firewall rule allowing access from the jump host to nodes in the namespace network.

Follow the procedure in [Add or Modify Distributed Firewall Rules](#) in the *VMware Cloud on AWS Networking and Security* guide. Create a new policy if you need one, then create a rule that uses the following values:

| Option       | Description  |
|--------------|--|
| Sources      | Enter the IP address of the jump host.   |
| Destinations | Enter the CIDR block of the namespace segment.   |
| Services     | Typically <b>SSH TCP port 22</b> or <b>RDP TCP port 3389</b> but can be set to whatever services the jump host needs to use. |
| Action       | <b>Allow</b>   |

#### What to do next

After you publish the firewall rule, you can use the jump host to access nodes in the Tanzu Kubernetes Grid cluster over SSH or another service.

## Enable Internet Access to a Kubernetes Service

To enable access from the public Internet to a Kubernetes service running in a Tanzu Kubernetes Grid cluster, publish the service internally, then give it a public IP address and create a DNAT rule that exposes the published service at an IP address in the ingress CIDR.

Internet access to cluster services is managed by a load balancer through a DNATted public IP address in the Ingress CIDR block you specified when you activated Tanzu Kubernetes Grid. In VMware Cloud on AWS, the load balancer service is implemented by the NSX Container Plug-in, which is automatically configured for each SDDC cluster on which you activate Tanzu Kubernetes Grid. See [Overview of NSX Container Plug-in](#) for more information.

The following steps outline a typical workflow that you can use to make a Kubernetes service accessible from the public Internet. The VMware Cloud Tech Zone article [Set Up Public Access to Tanzu Kubernetes Clusters in VMware Cloud on AWS](#) explains this workflow in more detail.

#### Procedure

- 1 Log in to VMware Cloud Services at <https://vmc.vmware.com>.
- 2 Use the VMware Cloud on AWS API to publish the service internally.

Deploy it as a service of type LoadBalancer, specifying the namespace and node ports, as shown here.

```
apiVersion: v1
kind: service
metadata:
  name: example-svc
  namespace: ns1
  labels:
```

```

    app: hardtop-example
spec:
  ports:
    port: 80
    targetPort: 8080
  type: LoadBalancer
  selector:
    app: example-app

```

Deploying a Kubernetes service of `type: LoadBalancer` publishes it and makes it accessible within the cluster at the specified port (`port: 80` in this example) and maps a node port for the service to a random port above 30000.

- 3 Create a VMware Cloud on AWS Compute Gateway firewall rule allowing access to the VM on the its external IP and mapped node port (we're using 31552 in this example).

Use a `kubectl` command like this one to return the service properties you need for the firewall rule.

```

kubectl get service example-svc -n ns1

```

| NAME        | TYPE         | CLUSTER-IP   | EXTERNAL-IP | PORT(S)      |
|-------------|--------------|--------------|-------------|--------------|
| example-svc | LoadBalancer | 10.96.249.36 | 10.130.1.9  | 80:31552/TCP |

Follow the procedure in [Add or Modify Management Gateway Firewall Rules](#) in the *VMware Cloud on AWS Networking and Security* guide to create a rule with parameters like these:

| Option       | Description   |
|--------------|---|
| Sources      | Any   |
| Destinations | The EXTERNAL-IP of the service (10.130.1.9 in this example) |
| Services     | HTTP  |
| Action       | Allow   |

- 4 Request a public IP address for the VM providing the service.

Follow the procedure in [Request or Release a Public IP Address](#) in the *VMware Cloud on AWS Networking and Security* guide:

- 5 Create a DNAT rule for this public IP.

Follow the procedure in [Create or Modify NAT Rules](#) in the *VMware Cloud on AWS Networking and Security* guide to create a DNAT rule matching the public IP to the internal IP. If your rule specifies **Match Internal Address**, you'll also need to create a firewall rule allowing access to the **Public IP** address on the Internet interface.

## Deactivate Tanzu Kubernetes Grid Services in a Cluster

Deactivate Tanzu Kubernetes Grid in an SDDC cluster if you no longer need Tanzu workload management features in the cluster.

## Prerequisites

You must be logged in to the VMC Console at <https://vmc.vmware.com/> as a user with a VMware Cloud Services Service Role of **Administrator** or **Administrator (Delete Restricted)**.

---

**Important** Deactivating Tanzu Kubernetes Grid on an SDDC cluster deletes its Tanzu supervisor cluster along with all namespaces, workloads, and persistent volumes. Before you deactivate Tanzu Kubernetes Grid, back up or relocate any critical workloads, workload data, or application data.

---

## Procedure

- 1 Log in to the VMC Console at <https://vmc.vmware.com/>.
- 2 On the **Inventory** page, click **SDDCs** and select the SDDC where you want to deactivate Tanzu Kubernetes Grid .
- 3 Remove any firewall rules that reference segments in a Tanzu workspace.

This includes the Distributed Firewall Rule described in [Allow Internal Access to a Tanzu Kubernetes Grid Namespace](#).

- 4 Click **ACTIONS** and select **Deactivate Tanzu Kubernetes Grid**.

Deactivating Tanzu causes these events in the SDDC vCenter Server.

- All Tanzu workloads in the cluster are stopped.
- The Tanzu supervisor cluster is deleted.
- All namespaces in the supervisor cluster are deleted.
- All persistent volumes (VMDKs) associated with supervisor namespaces or Tanzu Kubernetes Grid clusters are deleted.

Select all the checkboxes to confirm that you understand the consequences of this action, then click **Deactivate Tanzu Kubernetes Grid**.

## SDDC Upgrades and Maintenance

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

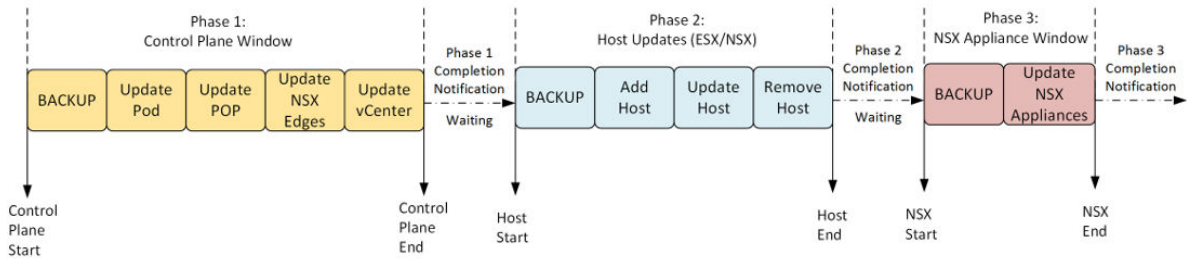
Upgrades to even-numbered releases of the SDDC software, such as VMC Version 1.10 or 1.12, will be provided to all SDDCs and are mandatory. Odd-numbered releases, such as 1.11 or 1.13, are available only for new SDDC deployments. These optional releases are not available for upgrades.

When an SDDC update is upcoming, VMware sends a notification email to you. Typically, this occurs 7 days before a regular update and 1-2 days before an emergency update. Delays to upgrades could result in your SDDC running an unsupported software version. See [Supported SDDC Versions](#).

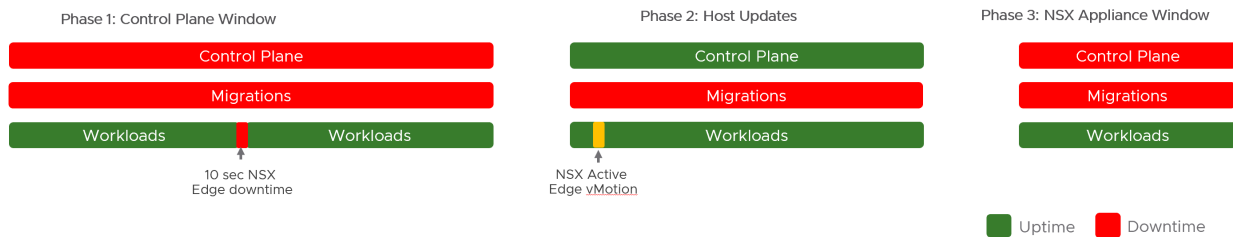
You also receive notifications by email when each phase of the update process starts, completes, is rescheduled, or is canceled. To ensure that you receive these notifications, ensure that donotreply@vmware.com is added to your email allow list.

## Upgrade Process for SDDCs Using NSX

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



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



### Important During upgrades:

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

Maintenance is performed in three phases.

**Phase 1: Control Plane Updates.** These are the updates to vCenter Server and NSX Edge. A backup of the management appliances is taken during this phase. If a problem occurs, there is a restore point for the SDDC. A management gateway firewall rule is added during this phase. There is an NSX Edge failover during this upgrade phase, resulting in a brief downtime. You do not have access to NSX Manager and vCenter Server during this phase. During this time, your workloads and other resources function as usual subject to the constraints outlined above.

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

---

**Note** VMware Site Recovery certificates in the SRM and VR appliances are also replaced if the vCenter Server certificate was replaced. VMware HCX has its own certificates that are not replaced as part of the SDDC Upgrade process.

---

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

- AppVolumes: <https://kb.vmware.com/s/article/2150281>
- Horizon Enterprise: <https://kb.vmware.com/s/article/74599>
- VMware Site Recovery: <https://kb.vmware.com/s/article/78499>

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

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

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

Phase 3: These are the updates to the NSX appliances. A backup of the management appliances is taken during this phase. If a problem occurs, there is a restore point for the SDDC. A management gateway firewall rule is added during this phase. You do not have access to NSX Manager and vCenter Server during this phase. During this time, your workloads and other resources function as usual subject to the constraints outlined above.

When Phase 3 is complete, you receive a notification.

For more information on estimating the duration of each phase, see [Estimating the Duration of SDDC Maintenance](#).

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

## On-Premises NSX Edge Compatibility for L2VPN

If your SDDC includes a Layer 2 VPN (L2VPN), the NSX upgrade might introduce an incompatibility between the server (SDDC) and client (on-premises) ends of the L2VPN. Take these steps to minimize L2VPN downtime after an SDDC upgrade:

- 1 See [Correlating VMware Cloud on AWS with Component Releases](#) for the NSX version that the upgrade will apply.
- 2 See the L2VPN Interoperability table in [Install and Configure the On-Premises NSX Edge](#) in the *VMware Cloud on AWS Networking and Security* for the set of supported L2VPN client and server versions.
- 3 If the version of NSX that the SDDC upgrade will apply is compatible with your existing on-premises NSX Edge, no action is needed. Otherwise, follow the procedure in [Install and Configure the On-Premises NSX Edge](#) to replace your existing on-premises NSX Edge with a compatible version. If there is an NSX Edge version that is compatible with your SDDC pre- and post-upgrade, upgrade the on-premises Edge before the SDDC upgrade begins. If there is no NSX Edge version that meets this criterion, you must wait until the SDDC upgrade is complete before you upgrade the on-premises Edge. This scenario will result in L2VPN downtime for the duration of the on-premises upgrade.

## Updates for VMware Hybrid Cloud Extension (HCX)

For customers using HCX:

- The VMware Hybrid Cloud Extension (HCX) for the SDDC managers will not be upgraded as part of this release.
- Avoid starting HCX migrations that might overlap with the SDDC upgrade window. HCX bulk migration processes might be halted, and HCX vMotion migrations might fail.
- For more details, see the *VMware HCX User Guide* at <https://docs.vmware.com/en/VMware-NSX-Hybrid-Connect/index.html>.

## Updates for the VMware vCenter Cloud Gateway

For customers using the VMware vCenter Cloud Gateway:

- The VMware vCenter Cloud Gateway will be updated to the latest release.
- The user interface for the VMware vCenter Cloud Gateway might be inaccessible during the upgrade of the appliance.
- For more information, see the documentation for the vCenter Cloud Gateway Appliance at <https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vsphere.vmc-aws-manage-data-center.doc/GUID-58C1AC46-3F99-4F93-BB1F-FD1878B49374.html>.

## Updates for Horizon Enterprise

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

## Impact of Updates on VMware Site Recovery

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

- You cannot open the Site Recovery UI for the SDDC under maintenance. From the remote SDDC Site Recovery UI, this site will appear as disconnected.
- Recovery plan failover operations towards the SDDC under maintenance cannot be initiated. Failover operations in progress might fail when maintenance starts.
- Incoming replications are interrupted. Depending on RPO settings and the maintenance duration, RPO violations notification for these replications might appear in the remote Site Recovery UI. RPO violations should disappear automatically sometime after the maintenance is completed, depending on when vSphere Replication manages to sync the accumulated delta. Replications outgoing from the SDDC under maintenance are not affected.
- For more information, see the documentation for VMware Site Recovery at <https://docs.vmware.com/en/VMware-Site-Recovery/index.html>.

## View an SDDC Maintenance Schedule Reservation

You can view the times scheduled for upcoming SDDC maintenance.

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

### Prerequisites

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

### Procedure

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

If maintenance is scheduled for this SDDC, you'll see an **Upcoming maintenance** card showing a date and time range for the maintenance.

## Submit an Upgrade Schedule Request

To request scheduling for upgrades to your SDDC, you can use the VMC Console .


Upgrades for VMware Cloud on AWS SDDCs are deployed in a rollout across the service. When an upgrade rollout is available for your organization, you receive an email notification and a notification in the VMC Console. Typically, you receive this notification 30 to 60 days before upgrades begin for a rollout. After you receive the notification, you can submit a scheduling request for any of your SDDCs.

A VMware rollout admin evaluates your scheduling request and attempts to accommodate it, based on available upgrade capacity and other factors. Based on your schedule request inputs (if any) and other upgrade process constraints, the rollout admin places the upgrade for your SDDC into a proposed schedule at least 3 weeks ahead of a proposed start date. You can view the placement and submit or edit an upgrade request to provide feedback and request any changes to the proposed schedule prior to final scheduling. Final scheduling will occur within 1-2 weeks prior to the start date for Phase 1 of the upgrade.

### Procedure

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



- 2 Click the Maintenance (  ) tab.
- 3 Click the **Rollouts** tab.
- 4 Select the rollout that you want to schedule.  
Each rollout represents an SDDC bundle release that is available for upgrade.
- 5 Select the SDDCs to include in your schedule request, and click **Schedule Request**.
- 6 In the **Pick preferred weeks** section, select your first preference for the week in which upgrades for the selected SDDCs to occur.
- 7 (Optional) Click **Add Preference** and select an additional week. You can specify up to three preferences total.
- 8 In the **Dates to exclude from upgrade scheduling** text box, enter any dates on which you do not want upgrades to occur.
- 9 In the **Preferred maintenance hours** text box, specify the times of the day when you prefer upgrades to be scheduled.
- 10 In the final text box, enter any other information required to help VMware schedule your upgrade.
- 11 Click **Submit Request**.

### Results

Your request is submitted to VMware. The **Requests** tab is displayed, which shows your scheduling requests and their status.

A VMware rollout admin will review your request. If the rollout admin adds questions or comments to your request, you receive a notification in email and in the VMC Console.

### View and Edit Upgrade Schedule Requests

After you have submitted an upgrade scheduling request, you can use the VMC Console to view the status of your requests and edit them.



**Procedure**

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



- 2 Click the Maintenance (  ) tab.

- 3 Click the **Requests** tab.

A list of all your schedule requests is displayed. Requests that the rollout admin has not yet reviewed are in the **Submitted** status. Requests that the rollout admin has reviewed are in the **Reviewed** status.

- 4 (Optional) To expand the details for a request, click the >> icon.

- 5 (Optional) Click **Edit Request** to edit or delete the request.

- Edit any of the request parameters and click **Update Request**.
- To delete the request, click **Delete Request**.

**View Upgrade Scheduling and Status**

You can view the schedule and status for your SDDC upgrades on the **Maintenance** tab of the VMC Console.

**Procedure**

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



- 2 Click the Maintenance (  ) tab.

- 3 Click the **Rollouts** tab.

- 4 Select the rollout that you want to view.

**Results**

The SDDCs for which this rollout is applicable are displayed.

| <input type="checkbox"/>            |                            | Version | Phase 1                          | Phase 2                           | Phase 3                           | Request ID | Status   |
|-------------------------------------|----------------------------|---------|----------------------------------|-----------------------------------|-----------------------------------|------------|----------|
| <input checked="" type="checkbox"/> | testing_do_not_delete      | 1.18v3  |                                  |                                   |                                   | 7133503123 | Planning |
| <input checked="" type="checkbox"/> | lev-integration-nsxt-tests | 1.16v9  |                                  |                                   |                                   | 5019262073 | Planning |
| <input type="checkbox"/>            | egration-tests             | 1.18v2  | June 7, 2022 at 1:00:00 PM GMT-5 | June 10, 2022 at 7:00:00 AM GMT-5 | June 12, 2022 at 7:00:00 AM GMT-5 |            | Placed   |
| <input type="checkbox"/>            | lev-restore-tests          | 1.14v7  |                                  |                                   |                                   |            | Planning |
| Items per page 20 4 items           |                            |         |                                  |                                   |                                   |            |          |

The following information is shown in this grid:

| Column     | Description  |
|------------|--|
| Version    | The current SDDC bundle version.   |
| Phase 1    | If the SDDC is in the <b>Placed</b> , <b>Scheduled</b> , or <b>In Progress</b> status, this shows the time allocated for Phase 1 of the upgrade.   |
| Phase 2    | If the SDDC is in the <b>Placed</b> , <b>Scheduled</b> , or <b>In Progress</b> status, this shows the time allocated for Phase 2 of the upgrade.   |
| Phase 3    | If the SDDC is in the <b>Placed</b> , <b>Scheduled</b> , or <b>In Progress</b> status, this shows the time allocated for Phase 3 of the upgrade.   |
| Request ID | If you have submitted a scheduling request for this SDDC, the request ID is shown in this column. Click the ID to see the request details.   |
| Status     | <p>This shows the status of the upgrade scheduling. The following statuses are available:</p> <p><b>Planning</b></p> <p>A rollout is available for this SDDC, but the rollout admin has not placed or scheduled the SDDC.</p> <p><b>Placed</b></p> <p>The rollout admin has selected the preferred week for the upgrade.</p> <p><b>Scheduled</b></p> <p>Either the rollout admin has accepted the customer requested schedule and the time for the upgrade has been blocked, or the default upgrade time selected by the rollout administrator is acceptable to the customer.</p> <p><b>In Progress</b></p> <p>The upgrade is in progress.</p> <p><b>Completed</b></p> <p>The upgrade is complete.</p> |

## Status

## View Maintenance Progress

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

### Procedure

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

## 2 Navigate to the **Maintenance** tab of your SDDC.

If maintenance is ongoing, the maintenance summary shows information about the current phase and step of maintenance.

## 3 Click **View Details** to see more details on the maintenance steps.

You can see details of the operations performed in each step, as well as start and end times for the steps.

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

# Convert UTC Time to Local Time

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

### Procedure

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

| Option                              | Description  |
|-------------------------------------|--|
| Use a time zone calculator          | Use the time zone calculator at <a href="https://www.timeanddate.com/worldclock/converter.html">https://www.timeanddate.com/worldclock/converter.html</a> to convert from UTC time to your time.   |
| Compute local time using UTC offset | <ul style="list-style-type: none"> <li>a Determine the time offset from UTC time for your local time zone. See <a href="https://en.wikipedia.org/wiki/List_of_UTC_time_offsets">https://en.wikipedia.org/wiki/List_of_UTC_time_offsets</a>.</li> <li>b Add the time offset to the UTC time (expressed in 24-hour time).</li> <li>c If daylight saving time is in effect in your local time zone, adjust for daylight saving time.</li> </ul> |

# Estimating the Duration of SDDC Maintenance

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

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

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

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

## Phase 1: Control Plane Updates

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

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

## Phase 2: Host Updates

This phase consists of updates to the hosts and host networking software in the SDDC.

Use the table below to estimate the duration of Phase 2.

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

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

## Phase 3: NSX Appliance Updates

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

## Actions Taken by VMware to Ensure SDDC Health

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

### VM Operations

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

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

## **vCenter Operations**

### **vCenter Sessions (Connections) Maxed Out**

If many sessions are created and not cleared, vCenter Server might become inaccessible. Typically this is caused by automation creating a large number of sessions. This generates an automated alert and VMware will restart vCenter Server. You will receive an email notification when this happens.

### **vCenter Server Reboot**

A number of different issues might require a reboot of vCenter Server. Some issues might require an immediate reboot for remediation, while others might allow for continued usage with a reboot required in the near future. In the latter case, you will receive an email notification alerting you that a restart will occur in the next 24 hours. After a reboot, ongoing tasks and application connections might need to restart.

### **Expired vCenter CA Certificate Removal**

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

## **NSX Operations**

### **Management Plane (NSX Manager) Restart**

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

### **NSX Edge Failover**

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

## **SDDC Operations**

### **Single Host SDDC Failure**

The Single Host SDDC starter configuration has no SLA and is appropriate for proof-of-concept or test and development use cases. VMware does not perform any remediation in

the event of a Single Host SDDC failure. You will receive an email notification if a Single Host SDDC failure occurs.

## SDDC Backups

We back up every SDDC daily at 0900Z as well as prior to any planned maintenance activity.

- What we back up: vCenter Server, vSAN configuration, and NSX. We do not back up customer data and workload VMs.
- Backup retention: Maximum age of 28 days and maximum of 56 backups. Backups are stored: encrypted in S3 within the SDDC's region and deleted when the SDDC is deleted. You cannot recover a deleted SDDC from backup.
- Recovery of management components is governed by your SLA. VMware will decide whether to recover from backup or repair.

## NFS Datastores

### Datastore availability

If vSphere hosts lose access to an NFS datastore (all paths down) for more than 320 seconds, vSphere HA will power-off all VMs on that host that had data stored on the impacted datastore. HA will attempt to restart the VM on a host that has a healthy connection to the datastore.

### SDDC Health

If a host is blocked from entering maintenance mode because a running VM cannot be relocated due to partial NFS Datastore availability, VMware operations will power off the offending VM. VMware will attempt to recover any impacted workload, but the VMs remain powered off until storage access is restored and you power them back on.

## View Billing Information

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

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

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

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

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

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

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

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

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

---

**Note** If you purchased through AWS, pricing and payment details are not shown in the VMware Cloud Services Console. Pricing is determined by your agreement with AWS. For more information, see [Purchase Options for VMware Cloud on AWS](#).

---

#### Procedure

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

## Upsize SDDC Management Appliances

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

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

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

---

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

---

#### Prerequisites

You must be logged in to the VMC Console at <https://vmc.vmware.com/> as a user with a VMware Cloud Services Service Role of **Administrator** or **Administrator (Delete Restricted)**.

#### Procedure

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

- 2 On the card for your SDDC, click **View Details** and then click the **Settings** tab.

The **Settings** page displays information about SDDC settings, pre-defined user accounts, and SDDC access via the API and PowerCLI.

- 3 Expand the **Management Appliances** item under the **SDDC** section of the **Settings** tab to view or change the appliance size in this SDDC.

If the appliance size is **NSX\_MEDIUM**, you can click **UPSIZE** to open the **Upsize management appliances** dialog. To upsize the appliance to **NSX\_LARGE**, select the checkboxes to confirm that you understand the consequences of your action, then click **UPSIZE**.

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

## Roles and Permissions in the SDDC

VMware Cloud on AWS limits your access to vSphere resources that must remain under the control of the service provider. It also prevents you from modifying default roles created in a new SDDC.

The service provider (VMware) is granted super-user rights over all users, groups, rights, roles, and inventory objects in your organization. See [Understanding Authorization in vSphere](#) in the *VMware vSphere Documentation* for more information about roles and rights in the system.

### SDDC vCenter Roles

#### CloudAdmin

The CloudAdmin role has the privileges necessary to create and manage SDDC workloads and related objects such as storage policies, content libraries, vSphere tags, and resource pools. This role cannot access or configure objects that are supported and managed by VMware, such as hosts, clusters, and management virtual machines. The CloudAdmin role can create, clone, or modify non-default roles. For detailed information about the privileges assigned to this role, see [CloudAdmin Privileges](#).

#### CloudGlobalAdmin

The CloudGlobalAdmin role is an internal role that must exist during SDDC deployment but can be removed by a CloudAdmin after deployment is complete.

### SDDC vCenter Users and Groups

A new SDDC is populated with a single organization user account, cloudadmin@vmc.local. This user is a member of the vCenter CloudAdminGroup and has the vCenter role of CloudAdmin. Although this role does not have rights to create local vCenter users or groups in the SDDC, it has rights to configure vCenter Single Sign-On and Hybrid Linked Mode, which allow access to the SDDC vCenter by single sign-on users. See [Configuring Hybrid Linked Mode](#) in *Managing the VMware Cloud on AWS Data Center*.



## AWS Roles

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

---

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

---

For more information, see [Account Linking and the VMware Cloud on AWS CloudFormation Template](#)

# Managing SDDC Hosts and Clusters

## 2

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

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

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

This chapter includes the following topics:

- [VMware Cloud on AWS Host Types](#)
- [Add a Cluster](#)
- [Remove a Cluster](#)
- [Add Hosts](#)
- [Remove Hosts](#)
- [About External Storage](#)
- [About Elastic DRS](#)
- [Understanding Auto-Remediation](#)
- [Using Policies and Profiles](#)
- [Microsoft Product Licenses in VMware Cloud on AWS](#)
- [Converting Host Types in Clusters](#)

## VMware Cloud on AWS Host Types

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

A given cluster in your SDDC must contain hosts of the same type. Some host types might not be available within a particular region or availability zone. For more about host types available in VMware Cloud on AWS, see the VMware Cloud Tech Zone article [SDDC Host Types](#)

i3

The i3 host type is the default host type. I3 hosts have 36 cores, 512GiB RAM, and 10.37TiB raw storage capacity per host.

### i3en

The i3en host type is optimized for data-intensive workloads. I3en hosts have 96 logical cores, 768GiB RAM, and approximately 45.84 TiB raw storage capacity per host. Single-host SDDCs cannot contain the i3en host type.

### i4i

The i4i host type has 128 logical cores, 1024GiB RAM, and 20.46TiB raw storage capacity per host.

## Add a Cluster

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

Additional clusters are created in the same availability zones as the initial SDDC cluster. When you deploy an additional cluster, all hosts in the cluster must be of the same type, but they don't have to be the type used in the cluster initially created for the SDDC. Logical networks you have created for your SDDC are automatically shared across all clusters. Compute and storage resources are configured similarly for all clusters. For example:

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

---

**Note** The initial cluster contains the Mgmt-ResourcePool and vsanDatastore, and all management workloads run in this cluster. All clusters contain a workloadDatastore and run virtual machine workloads.

Custom core counts can be selected only during cluster creation and only for secondary clusters. Custom core counts are not supported in Cluster-0 because all cores are required for management VMs.

---

For configuration and capacity details covering conventional 2-host clusters and stretched 4-host clusters, see the VMware TechZone article [Entry-level Clusters on VMware Cloud on AWS](#)

### Procedure

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

For more information on available host types, see [VMware Cloud on AWS Host Types](#).

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

2-host clusters with only 8 CPUs enabled are not supported. .

For i3 hosts, all CPU cores are enabled by default on each host in the cluster. If you'd like to disable some of the cores to save on licensing costs for applications that are licensed on a per-core basis, you can enable a subset of the available cores. This subset applies to all hosts in the cluster. Other cores on each host are disabled and remain disabled for the lifetime of the host.

For i3en hosts, all CPU cores are hyperthreaded and offered as logical cores by default on each host in the cluster. If you'd like to disable some of the cores to save on licensing costs for applications that are licensed on a per-core basis, you can enable a subset of the available cores. This subset is offered as physical cores and applies to all hosts in the cluster. Other cores on each host are disabled and remain disabled for the lifetime of the host.

---

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

---

- 5 Select the number of hosts in the cluster.

- 6 click **Add Cluster**.

#### Results

A progress bar shows the progress of cluster creation.

## Remove a Cluster

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

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

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

#### Prerequisites

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

#### Procedure

- 1 Log in to the VMC Console at <https://vmc.vmware.com>.
- 2 Click on the SDDC and then click **Summary**.

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

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

## Add Hosts

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

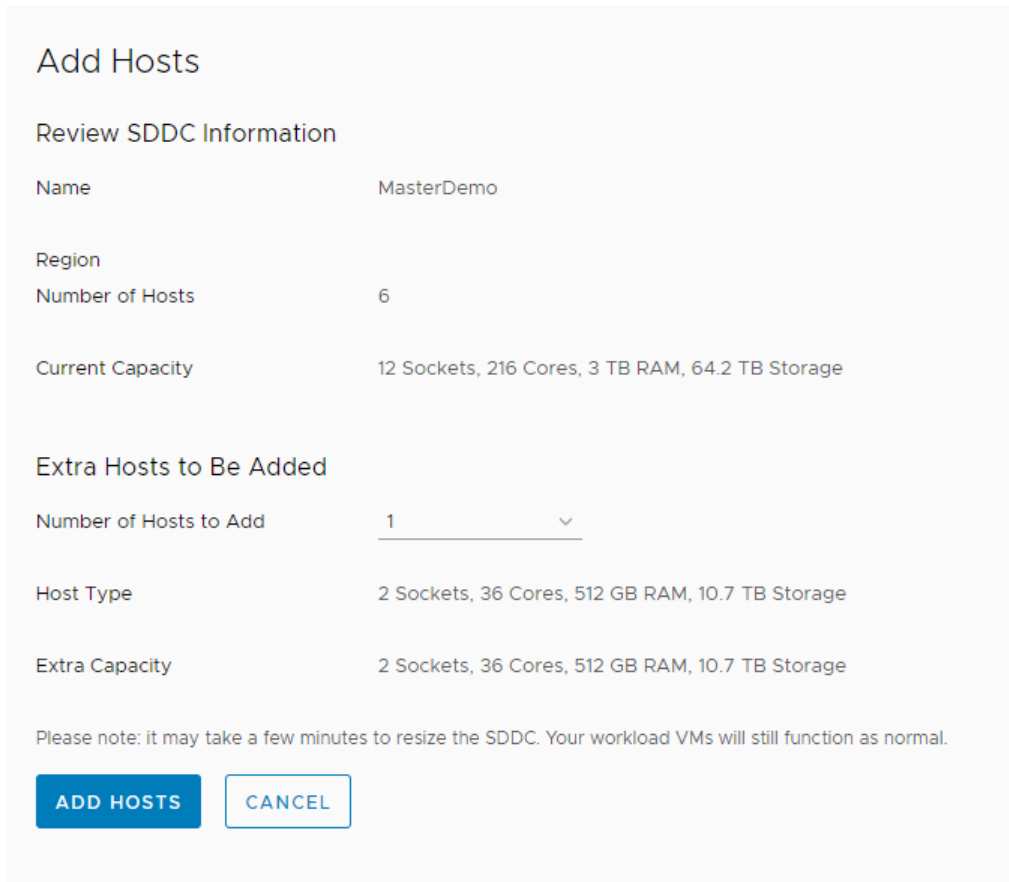
You can add hosts to your SDDC as long as you do not exceed the maximum number of hosts allotted to your account.

### Procedure

- 1 Log in to the VMC Console at <https://vmc.vmware.com>.
- 2 Click on the SDDC and then click **Summary**.
- 3 Select where to add the hosts.
  - If the SDDC has only one cluster, select **Actions > Add Hosts** from the SDDC card.

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

The Add Hosts page is



**Add Hosts**

**Review SDDC Information**

|                  |  |
|------------------|--|
| Name             | MasterDemo                                       |
| Region           |  |
| Number of Hosts  | 6  |
| Current Capacity | 12 Sockets, 216 Cores, 3 TB RAM, 64.2 TB Storage |

**Extra Hosts to Be Added**

|                        |  |
|------------------------|--|
| Number of Hosts to Add | 1 <span>▼</span>                                 |
| Host Type              | 2 Sockets, 36 Cores, 512 GB RAM, 10.7 TB Storage |
| Extra Capacity         | 2 Sockets, 36 Cores, 512 GB RAM, 10.7 TB Storage |

Please note: it may take a few minutes to resize the SDDC. Your workload VMs will still function as normal.

**ADD HOSTS** **CANCEL**

displayed.

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

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

### Results

One or more hosts are added to your SDDC cluster.

## Remove Hosts

You can remove hosts from your SDDC as long as the number of hosts in your SDDC cluster remains above the minimum required by vSAN storage policies.

Both conventional (single-AZ) and stretched clusters require at least two hosts. A stretched cluster that has been scaled out to four or six hosts cannot be scaled in. Stretched clusters with more than six hosts can be scaled both out and in.

Whenever you reduce cluster size, storage latency increases due to process overhead introduced by host removal. The duration of this overhead varies with the amount of data involved. It can take as little as an hour, though an extreme case could require more than 48 hours. While cluster-size reduction (scale-in) is underway, workload VMs supported by the affected clusters can experience significant increases in storage latency.

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

### Prerequisites

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

### Procedure

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

- 4 Select the number of hosts you want to remove.

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

---

**Note** All vSAN storage policies have requirements for a minimum number of hosts. If you attempt to reduce the number of hosts below this minimum, the operation fails. See [vSAN Policies](#) in *Managing the VMware Cloud on AWS Data Center*.

---

- 5 Select the **I understand that this action cannot be undone** check box.
- 6 Click **Remove**.

This action initiates the host removal process. A host slated for removal transitions to the DELETING state while its data is being moved and billing for the host stops. It can take several hours to move large volumes of data. When the data move is complete, the host is removed from vCenter inventory.

- If you are removing a single host, billing for that host stops immediately.
- If you are removing multiple hosts, they are queued and removed one at a time to avoid violating vSAN storage policies. Billing for a host continues while it is queued for removal. After each queued host is removed, VMware Cloud on AWS verifies that removing the next host in the queue won't violate vSAN storage policies. If that check fails, the host is not removed and billing continues. Otherwise, the host is removed.

## About External Storage

Use the **Storage** tab of the VMC Console to add customer-managed storage to an SDDC cluster.

The **Storage** tab of the VMC Console gives you the tools you need to add, remove, and reconfigure mountable storage (filesystems) like NFS.

---

**Note** VMware Cloud on AWS supports external storage starting with SDDC version 1.20. For information about upgrading an SDDC, see [Submit an Upgrade Schedule Request](#).

---

### NFS Datastores

NFS datastore support within VMware Cloud on AWS provides independent customer-managed scaling of compute and storage within an SDDC. This data storage may store Virtual Machines, Virtual Disks, Content Libraries, ISO, and similar objects. Customers may attach any of the following VMware Cloud on AWS Certified NFS Storage targets from the SDDC management console.

- Amazon FSx for NetApp ONTAP

Datastores are associated with and attached to vSphere Clusters.

#### Restrictions

SOIC (storage I/O control) is not supported for use in VMware Cloud on AWS datastores and will be automatically disabled.

#### Integrated services that do not support NFS Datastores

- VMware Cloud Disaster Recovery
- VMware Site Recovery
- Tanzu Services

## Add External Storage to a Cluster

Use the **Storage** tab of your SDDC to add external storage to a cluster.

VMware Cloud on AWS supports external storage starting with SDDC version 1.20. To request an upgrade to an existing SDDC, please contact VMware support or notify your Customer Success Manager.

---

**Note** External storage cannot be attached to stretched clusters.

---

#### Procedure

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



- 2 In the VMC Console, open the **Storage** tab of your SDDC. Click **ATTACH DATASTORE** and fill in the required values.

The **External Storage** card displays a table with a row for each cluster in the SDDC. Expand the row for a cluster to view its attached datastores, or to attach a new one.

|  |  |
|--|--|
| Cluster  | Select a cluster. Cluster-1 is preselected if there are no other clusters.                         |
| Datastore  | Choose <b>Attach a new datastore</b>   |
| <ul style="list-style-type: none"> <li>■ NFS server address</li> <li>■ Export</li> <li>■ Storage Vendor</li> </ul> | NFS datastores only. See <a href="#">Configure Amazon FSx for NetApp ONTAP as External Storage</a> |
| Datastore Name   | Give the datastore a name. Datastore names must be unique within an SDDC.                          |

Click **ATTACH DATASTORE** to attach the datastore to the cluster.

## Remove External Storage From a Cluster

Use the **Storage** tab of your SDDC to remove external storage from a cluster.

### Procedure

- 1 Log in to the VMC Console at <https://vmc.vmware.com>.
- 2 Select a datastore from which to remove external storage.

On the card for the SDDC from which you want to remove external storage, open the **Storage** tab and select a datastore. Click the vertical ellipsis button to the left of the cluster name and select **Detach Datastore**.

- 3 On the **Detach Datastore** page, select the datastore to detach, then click **DETACH DATASTORE**.

The system requires a few minutes to detach the datastore, and displays a success message when the remove is complete.

## About Elastic DRS

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

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

---

**Note** You cannot disable Elastic DRS in VMware Cloud on AWS. VMware has pre-configured Elastic DRS thresholds across all available policies to ensure SDDC availability. One of the Elastic DRS policies listed in [Select Elastic DRS Policy](#) is always active.

---

Elastic DRS is not supported for single host starter SDDCS. Elastic DRS requires at least three hosts in a single-AZ SDDC and six hosts in a multi-AZ SDDC.

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

## How the Elastic DRS Algorithm Works

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

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

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

### Scale-out Recommendation

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

### Scale-in Recommendation

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

---

**Note** Whenever you reduce cluster size, storage latency increases due to process overhead introduced by host removal. The duration of this overhead varies with the amount of data involved. It can take as little as an hour, though an extreme case could require more than 48 hours. While cluster-size reduction (scale-in) is underway, workload VMs supported by the affected clusters can experience significant increases in storage latency.

---

## Scaling Multiple Availability Zone Clusters

When Elastic DRS generates a scale-in or scale-out event for a multiple availability zone cluster, hosts are removed or added in both availability zones.

If a host fails in a multiple availability zone cluster, Auto-Scaler attempts to replace it in its original availability zone. If it is unable to do this because of a full or partial availability zone failure, Elastic DRS scales out the cluster in the remaining availability zone. It adds non-billable hosts in the remaining availability zone until the cluster reaches its original host count. This scale out is dependent on available capacity and is not guaranteed. When the failed availability zone is restored, Elastic DRS scales in the cluster to remove the extra hosts.

## Time Delays Between Two Recommendations

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

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

## Interactions of Recommendations with Other Operations

The following operations might interact with Elastic DRS recommendations:

- User-initiated addition or removal of hosts.

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

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

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

- Planned Maintenance Operation

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

- Auto-remediation

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

- SDDC maintenance window

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

## Select Elastic DRS Policy

Set the Elastic DRS policy on a cluster to optimize for your workloads' needs.

In a new SDDC, Elastic DRS uses the **Elastic DRS Baseline** policy, adding hosts after storage utilization reaches 80% or if an AWS Availability Zone failure occurs. You can select a different policy if it provides better support for your workload VMs. For any policy, scale-out is triggered when a cluster reaches the high threshold for any resource. Scale-in is triggered only after all of the low thresholds have been reached. See [How the Elastic DRS Algorithm Works](#) for more information about EDRS scale-out and scale-in logic.

---

**Note** In two-host SDDCs and stretched clusters with fewer than six hosts, only the **Elastic DRS Baseline** policy is available.

---

The following policies are available:

### Optimize for Best Performance

When scaling in, this policy removes hosts gradually in order to avoid performance slowdowns as demand spikes. It has the following thresholds:

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

### Optimize for Lowest Cost

When scaling in, this policy removes hosts quickly in order to maintain baseline performance while keeping host counts to a practical minimum. It has the following thresholds:

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

### Optimize for Rapid Scale-Out

This policy adds multiple hosts at a time when needed for memory or CPU, and adds hosts incrementally when needed for storage. By default, hosts are added two at a time, but beginning with SDDC version 1.14 you can specify a larger increment if you need faster scaling for disaster recovery and similar use cases. When using this policy, scale-out time increases with the number of hosts added and, when the increment is large (12 hosts), can take up to 40 minutes in some configurations. You must manually remove these hosts when they are no longer needed. This policy has the following thresholds:

| Resource | High Threshold  | Low Threshold                |
|----------|-----------------|------------------------------|
| CPU      | 80% utilization | 0% utilization (no scale-in) |
| Memory   | 80% utilization | 0% utilization (no scale-in) |
| Storage  | 80% utilization | 0% utilization (no scale-in) |

Elastic DRS policies are based on two variables:

#### Minimum cluster size

The minimum host count that permits EDRS scaling. Once minimum cluster size is reached, EDRS cannot perform a scale-in operation, but you can still remove hosts manually until your organization's minimum host count is reached.

#### Maximum cluster size

The maximum host count that permits EDRS scaling. Once maximum cluster size is reached, EDRS cannot perform a scale-out operation, but you can still add hosts manually until your organization's maximum host count is reached.

#### Procedure

- 1 Log in to the VMC Console at <https://vmc.vmware.com>.
- 2 Click **Inventory** > **SDDCs**, then pick an SDDC card and click **VIEW DETAILS**.
- 3 On the card for the SDDC or cluster, click **ACTIONS** and choose **Edit EDRS Settings**.

- 4 Select the Elastic DRS policy you want to use.

The **Elastic DRS Baseline** policy has no parameters. For other policies, specify a **Minimum cluster size** of 2 or more and a **Maximum cluster size** consistent with your expected workload resource consumption. The **Maximum cluster size** applies to CPU and Memory. To maintain storage capacity and ensure data durability, the service can add more hosts than what you specified in **Maximum cluster size**.

- 5 Click **Save**.

## Understanding Auto-Remediation

The VMware Cloud on AWS autoscaler service monitors the health of your SDDC infrastructure, detects incipient and actual failures, and automatically remediates the infrastructure by replacing hosts before or after a failure occurs.

AWS Infrastructure is reliable, but failures are inevitable in even the most reliable infrastructure. The [AWS Architecture framework reliability](#) pillar discusses their design principles for reliability in the cloud. VMware Cloud on AWS extends these principles by abstracting the underlying infrastructure and leveraging the predictive failure analysis capabilities of vCenter Server and ESXi to provide reactive remediation when failures occur and predictive remediation that can prevent failures from affecting workloads.

Most of the auto-remediation process happens in the background and is carried out without affecting existing workloads. Auto-remediation monitors the health of the system and can quickly add hardware to an SDDC when necessary, inserting a new host into your cluster when a fault occurs or a health issue is detected and evacuating workload VMs from failed or failing hardware. In addition, because all VMware Cloud on AWS SDDCs use VMware vSAN and vSphere HA, workloads affected by host failures are automatically relocated and restarted.

---

**Note** You are never billed for extra hosts used for auto-remediation or planned maintenance.

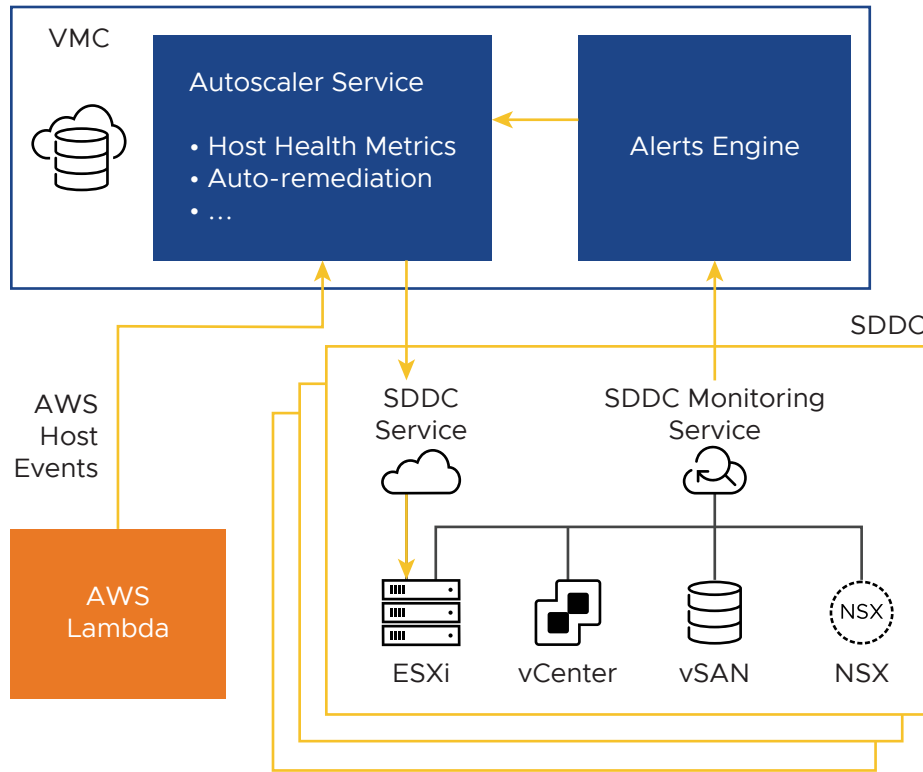
---

## Auto-Remediation High-Level Architecture

Auto-remediation architecture includes components supplied by both AWS and VMware.

- AWS sends VMware host-level information, notably AWS Planned Maintenance events. The autoscaler service receives these notifications and automatically remediates any issues within the SDDC.
- A monitoring service at the SDDC level receives notifications from the underlying VMware Cloud on AWS components.

See the VMware Cloud Tech Zone article [Feature Brief: Auto Remediation](#) for more.



## Reactive Remediation

Reactive auto-remediation monitors hardware and software faults and attempts to remediate problems in several ways. Auto-Remediation is an internal process and is constantly evolving. VMware Cloud on AWS users have no access to the workflow or its configuration, but to help you understand it better, here's a high-level overview of the steps currently involved.

### 1: Monitor

VMware Cloud on AWS continuously monitors the health of every host in your SDDC. When a failure is detected, an event is sent to auto-remediation.

### 2: Wait for transient events

Some of the detected failures can be temporary. For example, when the monitoring system cannot reach a host due to a temporary connectivity issue. Auto-remediation waits for five minutes to determine whether the problem is temporary. If it is, auto-remediation returns without taking any action.

### 3: Add a host

If the error does not resolve after five minutes, auto-remediation begins adding a host to the SDDC. Pre-emptively adding a host in this way ensures that the host is available if required. Note that you are not billed for this host until it replaces a faulty host in your SDDC.

### 4: Determine failure type and take action

Hosts can fail for different reasons, and require different action. For example, a vSAN disk failure on a host that is still connected to a vCenter Server can be remediated through a soft reboot, whereas a PSOD host requires a hard reboot.

## 5: Check host health

The next step is to check if the remediation action has fixed the host. If the failed host is now healthy after a soft or hard reboot, auto-remediation avoids further disruption to the SDDC. It collects and takes any other necessary actions and removing the new host that was added pre-emptively in Step 3.

## 6: Replace host

If the failed host cannot be revived then the autoscaler removes the failed host, and replaces it with the host that was added in Step 3. vSphere HA and vSAN are triggered and compute policy tags are attached to the new host.

## Pre-emptive Remediation

In addition to reactive remediation, the autoscaler monitors several independent feeds in an attempt to spot failures before they manifest. If the service determines a host is likely to encounter a hardware failure, a non-disruptive preemptive planned maintenance event is triggered. It is still possible that the host will fail before the planned maintenance is completed, but by preemptively initiating host replacement, the impact is minimized. During planned maintenance:

- 1 A new host is added to the cluster.
- 2 The faulty host is placed into maintenance mode with a full data evacuation. This non-disruptively moves any VMs and or vSAN data to other hosts within the cluster.
- 3 The faulty host is removed from the cluster

## Autoscaler Events

When the autoscaler service receives a failure event, it determines the failure type and then takes appropriate action. The SDDC activity log includes any autoscaler activities, but does not show the failure event that triggered the activity.

### vCenter Server events.

- An event is triggered to check the host connection state
- An event is triggered when the ESXi host is disconnected or not responding.

### DAS events

- vSphere HA events: An event is created when there is no communication with master node, or HA is down. (FDM)
- When a host goes down, HA system reports a host failure.



**vSAN events**

- When there is a disk failure on the hosts.
- When the vSAN host is disconnected.

**EDRS events (non-failure)**

Upgrade: Disable EDRS. Maintenance activities frequently require an extra host, this host(s) is added as part of the maintenance event. EDRS is disabled for the duration of any planned maintenance to prevent these activities from triggering Scale-in/out events.

**AWS events**

- Planned maintenance events. Notification from AWS that an instance health issue has been detected and the instance should be evacuated.
- Personal Health Dashboard (PHD). An event stream that provides insight into various hardware components and allows VMware to spot hardware failures preemptively.
- System status check. Monitors the health of the AWS systems the Instance relies upon. This check reports issues that only AWS can fix. In many cases, these issues are transient, and no action is required.
- Instance status check. Monitors the software and network configuration for each instance. This check monitors the availability of the instance by issuing periodic ARP requests to the NIC. In addition to reporting on instance availability at the EC2 layer. Instance status checks monitor the underlying hardware utilization and will report Networking issues, Memory Exhaustion, Corrupt file system, kernel errors, etc. Unlike System Status Checks, Instance status checks require VMware interaction to resolve.

**SDDC events**

vCenter Server host health.

## Using Policies and Profiles

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

### Creating and Managing Compute Policies

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

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

---

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

---

## Monitoring Compliance

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

## Create or Delete a VM-Host Affinity Policy

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

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

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

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

- A policy cannot prevent a host from entering maintenance mode. If the host needs to be put into maintenance mode, VMs with an affinity for the host are automatically migrated to another host in the cluster, then migrated back when the maintenance completes and the host becomes available.
- A policy cannot prevent a host configured for HA from executing a failover. VMs with an affinity for the failed host can be migrated to any available host in the cluster.
- A policy cannot prevent a VM from powering-on. If a VM subject to a host affinity policy specifies a resource reservation that no host can meet, it is powered on on any available host.

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

### Prerequisites

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

## Procedure

- 1 Create a category and tag for VMs that you want to include in a VM-Host affinity policy.  
Pick a category name that describes common characteristics, such as license requirements, of VMs you plan to tag as members of that category.
- 2 Create a category and tag for hosts that you want to include in a VM-Host affinity policy.  
You can use existing tags and categories or create new ones specific to your needs. See [vSphere Tags and Attributes](#) for more about creating and using tags.
- 3 Tag the VMs and hosts that you want to include in a VM-Host affinity policy.
- 4 Create a VM-Host affinity policy.

- a In your SDDC, click **OPEN VCENTER**.
- b From the vSphere Client Home, click **Policies and Profiles > Compute Policies**.
- c Click **Add** to open the **New Compute Policy** Wizard.
- d Fill in the policy **Name** and choose **VM-Host affinity** from the **Policy type** drop-down control.

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

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

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

---

**Note** In a stretched cluster, each host is automatically tagged with an **Availability zones** tag. All hosts in an availability zone (AZ) are assigned the same tag, so you can use these tags to establish an affinity between a VM and any host in the cluster that has a specific availability zone tag.

Compute policy does not affect the location of VM storage, so be sure that VM storage policies locate a copy of VM storage in the AZ where VM is deployed. Compute policy does not affect network paths to and from the VM, which might transit a different AZ than the one where the VM is deployed.

---

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

## Create or Delete a VM-Host Anti-Affinity Policy

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

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

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

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

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

### Prerequisites

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

### Procedure

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

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

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

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

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

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

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

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

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

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

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

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

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

---

**Note** In a stretched cluster, each host is automatically tagged with an **Availability zones** tag. All hosts in an availability zone are assigned the same tag, so you can use these tags to establish anti-affinity between a VM and any host in the cluster that has a specific availability zone tag.

---

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

## Create or Delete a VM-VM Affinity Policy

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

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

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

### Prerequisites

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

### Procedure

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

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

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

- 3 Create a VM-VM affinity policy.

- a In your SDDC, click **OPEN VCENTER**.
- b From the vSphere Client, click **Policies and Profiles > Compute Policies**.
- c Click **Add** to open the **New Compute Policy Wizard**
- d Fill in the policy **Name** and choose **VM-VM affinity** from the **Policy type** drop-down control.

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

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

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

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

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

## Create or Delete a VM-VM Anti-Affinity Policy

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

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

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

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

### Prerequisites

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

### Procedure

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

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

- 2 Tag the VMs that you want to include in each group.
- 3 Create a VM-VM anti-affinity policy.
  - a In your SDDC, click **OPEN VCENTER**.
  - b From the vSphere Client, click **Policies and Profiles > Compute Policies**.
  - c Click **Add** to open the **New Compute Policy** Wizard.

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

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

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

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

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

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

## Create or Delete a Disable DRS vMotion Policy

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

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

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

### Prerequisites

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

### Procedure

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

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

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

- 3 Create a Disable DRS vMotion policy.

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

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

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

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

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

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

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

## Microsoft Product Licenses in VMware Cloud on AWS

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

### Bring Existing Windows Licenses to VMware Cloud on AWS

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

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

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

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

---

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

---

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



## Subscribe to Windows Server and SQL Server Licenses from VMware

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

- Offered for all hosts in the cluster. All hosts in a cluster must be licensed. You cannot mix licenses purchased from VMware with BYOL licenses in the same cluster.
- Billed based on the maximum number of hosts that were deployed in that cluster during your billing cycle. You are not billed for maintenance or remediation hosts.
- Billing begins when you select the license. If you choose to remove the license, you are billed for the entire billing period.
- After you have selected the licenses, you may deploy an unlimited number of the applicable VMs on the licensed hosts.

### License Mobility

Eligible Microsoft server applications such as Microsoft SQL Server, may, in certain cases, be deployed on VMware Cloud on AWS using existing licenses.

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

---

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

---

### How to Sign Up

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

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

## Eligibility for License Mobility

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

- All Microsoft server products migrated to VMware Cloud on AWS must be eligible via the Microsoft License Mobility through Software Assurance program as set forth by Microsoft at <http://www.microsoft.com/licensing/about-licensing/product-licensing.aspx>
- The server applications must be on the list of eligible products published by Microsoft at <http://www.microsoft.com/licensing/about-licensing/product-licensing.aspx>. The list includes:
  - Exchange Server
  - SharePoint Server
  - SQL Server Standard Edition
  - SQL Server Enterprise Edition
  - SQL Server Business Intelligence Edition
  - Skype for Business Server
  - System Center Server
  - Dynamics CRM Server
  - Dynamics AX Server
  - Project Server
  - Visual Studio Team Foundation Server
  - BizTalk Server
  - Forefront Identity Manager
  - Forefront Unified Access Gateway
  - Remote Desktop Services

---

**Note** The following products are not eligible for License Mobility through Software Assurance:

- Microsoft Server Windows operating system products
  - Microsoft Windows client operating system products
  - Desktop application products (for example, Microsoft Office)
- 

## Select License Options from the VMC Console

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

Licenses are enabled and billed for all hosts in the cluster. Mixing VMware-provided Microsoft licenses with BYOL licenses in the same cluster is not supported.

If you have purchased VMware Cloud on AWS services through a reseller, your reseller must have signed a Software Services Reseller Addendum in order to enable these license options.

For details on Microsoft Server license pricing, contact your sales representative or reseller.

#### Procedure

- 1 Log in to the VMC Console at <https://vmc.vmware.com>.
- 2 Edit Microsoft Server Licenses.
  - If your SDDC has a single cluster, click **Edit Microsoft Server Licenses** at the bottom of the SDDC card.
  - If your SDDC has multiple clusters, click **Actions > Edit Microsoft Server Licenses** at the bottom of the cluster card.
- 3 Select the licenses you want to purchase.

Billing begins as soon as you select the licenses. See [Subscribe to Windows Server and SQL Server Licenses from VMware](#) for more information on billing.
- 4 If you are part of an academic institution recognized by Microsoft as eligible for associated licensing rights and terms, select **Academic institution recognized by Microsoft**.

For more information on academic licensing for Microsoft products, see [Programs for Educational Institutions](#) or speak with your Microsoft license representative. After you have enabled academic licenses for a cluster, you cannot revert to regular licensing terms.
- 5 Select the checkboxes to confirm that you understand the license pricing and billing terms.
- 6 Click **Save**.

## Deploying Microsoft Server Instances

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

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

VMware provides a set of pre-packaged VMs that are ready to deploy.

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

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

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

- Database Engine services
- Client tools connectivity

- Client tools backwards compatibility

SQL Server services are configured as follows:

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

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

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

---

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

---



---

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

---

The OVF packages have the following configuration:

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

---

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

---

#### Procedure

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

For more information on creating

Content Libraries, see <https://docs.vmware.com/en/VMware-vSphere/7.0/>

[com.vmware.vsphere.vm\\_admin.doc/GUID-2A0F1C13-7336-45CE-B211-610D39A6E1F4.html](https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.vm_admin.doc/GUID-2A0F1C13-7336-45CE-B211-610D39A6E1F4.html).

- 2 Deploy the desired OVF into your environment.

For more information on deploying OVFs from Content Libraries, see

[https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.vm\\_admin.doc/GUID-3C02B3FC-5DE6-48AA-9AD3-7F0D1C7EC4B6.html](https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.vm_admin.doc/GUID-3C02B3FC-5DE6-48AA-9AD3-7F0D1C7EC4B6.html).

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

For more information on configuring VMs, see

[https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.vm\\_admin.doc/GUID-4AB8C63C-61EA-4202-8158-D9903E04A0ED.html](https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.vm_admin.doc/GUID-4AB8C63C-61EA-4202-8158-D9903E04A0ED.html).

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

This is required for initial activation of the Windows

server image. For more information about firewall configuration,

see <https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vmc-aws-networking-security/GUID-A5114A98-C885-4244-809B-151068D6A7D7.html>.

- 5 Power on the VM.
- 6 Configure a Windows Server password to secure the VM according to your corporate security policy.
- 7 (Optional) Convert the VM into a template for re-use.

You might need to reactivate VMs cloned from the template.

#### What to do next

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

## Create a VM Using a Microsoft ISO

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

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

- Windows Server 2019 Datacenter
- Windows Server 2019 Language Pack
- Windows Server 2016 Datacenter
- Windows Server Datacenter (provides Microsoft Semi-Annual Channel Release)

- SQL Server 2019 Enterprise. Use this ISO if you need to add features to the SQL Server instance.

---

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

---

## Procedure

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

For more information on creating

Content Libraries, see [https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.vm\\_admin.doc/GUID-2A0F1C13-7336-45CE-B211-610D39A6E1F4.html](https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.vm_admin.doc/GUID-2A0F1C13-7336-45CE-B211-610D39A6E1F4.html).

- 2 Create the VM.

For more information on creating VMs, see

[https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.vm\\_admin.doc/GUID-AE8AFBF1-75D1-4172-988C-378C35C9FAF2.html](https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.vm_admin.doc/GUID-AE8AFBF1-75D1-4172-988C-378C35C9FAF2.html).

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

Three different language ISO images are available in addition to the English language ISO:

- Chinese: [https://vmc-microsoft-templates.s3.us-west-2.amazonaws.com/Images\\_NonEnglish/chinese/lib.json](https://vmc-microsoft-templates.s3.us-west-2.amazonaws.com/Images_NonEnglish/chinese/lib.json)
- Japanese: [https://vmc-microsoft-templates.s3.us-west-2.amazonaws.com/Images\\_NonEnglish/japanese/lib.json](https://vmc-microsoft-templates.s3.us-west-2.amazonaws.com/Images_NonEnglish/japanese/lib.json)
- French: [https://vmc-microsoft-templates.s3.us-west-2.amazonaws.com/Images\\_NonEnglish/french/lib.json](https://vmc-microsoft-templates.s3.us-west-2.amazonaws.com/Images_NonEnglish/french/lib.json)

The content library is updated with the following versions of the software for the relevant language:

- Windows Server 2019 Datacenter
- Windows Server 2019 Language Pack
- Windows Server 2016 Datacenter
- Windows Server 2016 Language Pack
- SQL Server 2019 Enterprise. Use this ISO if you need to add features to the SQL Server instance.

For more information on installing software from ISO images, see

[https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.vm\\_admin.doc/GUID-55FC02D4-F5B3-4357-BB6B-78240B7F16BA.html](https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.vm_admin.doc/GUID-55FC02D4-F5B3-4357-BB6B-78240B7F16BA.html).

- 4 Install VMware Tools on the VM.

## 5 Copy the activation script to the VM.

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

- a In the vSphere Client, navigate to the subscribed Content Library and click **Other Types**.
- b Attach the VM's CD/DVD drive to the `Windows_Activation_Script` ISO in the Content Library.

For more information on connecting a Content

Library ISO file to a VM, see [https://docs.vmware.com/en/](https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.vm_admin.doc/GUID-BE1C18D2-8FF0-4F41-AA35-A4BA71D62EB4.html)

[VMware-vSphere/7.0/com.vmware.vsphere.vm\\_admin.doc/GUID-BE1C18D2-8FF0-4F41-AA35-A4BA71D62EB4.html](https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.vm_admin.doc/GUID-BE1C18D2-8FF0-4F41-AA35-A4BA71D62EB4.html).

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

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

For more information on configuring VMs, see

[https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.vm\\_admin.doc/GUID-4AB8C63C-61EA-4202-8158-D9903E04A0ED.html](https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.vm_admin.doc/GUID-4AB8C63C-61EA-4202-8158-D9903E04A0ED.html).

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

This is required for initial activation of the Windows

server image. For more information about firewall configuration,

see <https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vmc-aws-networking-security/GUID-A5114A98-C885-4244-809B-151068D6A7D7.html>.

## 8 Power on the VM.

## 9 Run the activation script.

- a In the guest operating system, open a command window and change to the directory where you copied the `Activation.ps1` script.
- b Type `powershell Activation.ps1` and press Enter.

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

### What to do next

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

## Import Your Windows Server VM into VMware Cloud on AWS

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

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

### Procedure

- 1 Import your Windows VM to VMware Cloud on AWS.

You can use a variety of methods to do this including cold migration, migration with vMotion, migration with HCX, or cloning from a Content Library template you have created.

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

## Activate or Reactivate a Windows Server VM

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

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

- Cloning a VM
- Converting a VM to a template

### Procedure

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

For more information on creating

Content Libraries, see <https://docs.vmware.com/en/VMware-vSphere/7.0/>

[com.vmware.vsphere.vm\\_admin.doc/GUID-2A0F1C13-7336-45CE-B211-610D39A6E1F4.html](https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.vm_admin.doc/GUID-2A0F1C13-7336-45CE-B211-610D39A6E1F4.html).



## 2 Copy the activation script to the VM.

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

- a In the vSphere Client, navigate to the subscribed Content Library and click **Other Types**.
- b Attach the VM's CD/DVD drive to the `Windows_Activation_Script` ISO in the Content Library.

For more information on connecting a Content

Library ISO file to a VM, see [https://docs.vmware.com/en/](https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.vm_admin.doc/GUID-BE1C18D2-8FF0-4F41-AA35-A4BA71D62EB4.html)

[VMware-vSphere/7.0/com.vmware.vsphere.vm\\_admin.doc/GUID-BE1C18D2-8FF0-4F41-AA35-A4BA71D62EB4.html](https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.vm_admin.doc/GUID-BE1C18D2-8FF0-4F41-AA35-A4BA71D62EB4.html).

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

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

This is required for initial activation of the Windows

server image. For more information about firewall configuration,

see <https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vmc-aws-networking-security/GUID-A5114A98-C885-4244-809B-151068D6A7D7.html>.

## 4 Run the activation script.

- a In the guest operating system, open a command window and change to the directory where you copied the `Activation.ps1` script.
- b Type `powershell Activation.ps1` and press Enter.

### What to do next

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

## Converting Host Types in Clusters

You have the option of converting clusters to use a new host type, if the original host type you selected no longer meets your needs.

Currently, the following conversions are available:

- You can convert clusters containing i3 hosts to i3en or i4i hosts.
- You can convert clusters containing i3en hosts to i4i hosts.

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

You receive notifications when a cluster conversion is scheduled, about to start, and completed. To ensure that you receive these notifications, ensure that `donotreply@vmware.com` is added to your email allow list.

## Cluster Conversion Process

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

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

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

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

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

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

## Impact of Cluster Conversion on Operation

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

- Removing hosts
- Editing EDRS policy settings

During cluster conversion, do not perform the following actions on the cluster which is being converted:

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

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

## Cluster Conversion and Billing

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

Converting the cluster host types does not convert any term commitments that you have purchased. For example, if you purchased an i3 term commitment, and later converted that cluster to use i3en hosts, you can choose to purchase a new i3en term commitment or have your i3en hosts billed at the on-demand rate. In either case, you will continue to pay for your i3 term commitment.

# Working With SDDC Add-On Services

## 3

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

This chapter includes the following topics:

- [Using the vRealize Log Insight Cloud Add-On](#)
- [Using the vRealize Automation Cloud Add-On](#)
- [Using VMware Carbon Black Workload](#)
- [Using the NSX Advanced Firewall Add-On](#)

## Using the vRealize Log Insight Cloud Add-On

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

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

## SDDC Audit Log Events

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

### ESXi Audit Events

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

### vCenter Audit Events

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

## NSX Audit Events

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

## NSX Firewall and Packet Log Events

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

## User-Driven Activity Events

```
log_type Contains Activity
```

## VMC Notification Gateway Events

```
log_type Contains Notification
```

## VMware Site Recovery Events

```
text contains vmware-dr
AND
text doesnot contain vmware-dr-audit
```

## VMware Cloud Services Audit Events

```
log_type Contains csp-audit
```

# Using the vRealize Automation Cloud Add-On

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

For information about how to use vRealize Automation with VMware Cloud on AWS, see [Quick cloud automation setup for VMware Cloud on AWS](#) in the *VMware vRealize Automation Cloud Product Documentation*.

# Using VMware Carbon Black Workload

VMware Carbon Black Workload helps security and infrastructure teams identify workload vulnerabilities and prevent, detect, and respond to attacks.

VMware Carbon Black Workload™ delivers advanced protection purpose-built for securing workloads running in VMware Cloud to reduce the attack surface and strengthen security posture, while simplifying operations for IT and Security teams.

For more information, see [VMware Carbon Black Workload for VMware Cloud on AWS](#)

## Using the NSX Advanced Firewall Add-On

The NSX Advanced Firewall add-on enables your SDDC to use advanced NSX security features.

NSX Advanced Firewall for VMware Cloud on AWS gives your SDDC access to advanced NSX application security features, including:

- NSX [Layer 7 Context Profile](#)
- NSX [Distributed IDS/IPS](#)
- NSX [Identity Firewall](#)

To activate the NSX Advanced Firewall Add-On in your SDDC, open the **Add-Ons** tab and click **ACTIVATE** on the **NSX Advanced Firewall** add-on card. After the add-on is activated, NSX advanced security features become available on the **Networking & Security** tab of your SDDC. See [About NSX Advanced Firewall Features](#) in the *VMware Cloud on AWS Networking and Security* guide for details about how to use the new features, and for step-by-step instructions for deactivating the add-on if you no longer need it.

# Getting Templates, ISOs, and Other Content into Your SDDC

## 4

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

| Content Type          | How to transfer it to your SDDC   |
|-----------------------|---|
| .vmtx template        | <ul style="list-style-type: none"><li>■ Use the Content Onboarding Assistant to transfer the template to your SDDC.</li><li>■ Clone the templates to OVF template in an on-premises Content Library and subscribe to the Content Library from your SDDC.</li></ul>  |
| OVF template          | <ul style="list-style-type: none"><li>■ Add the template to an on-premises Content Library and subscribe to the content library from your SDDC.</li><li>■ Create a local Content Library in your SDDC, and upload the OVF template to it.</li><li>■ Deploy the OVF template directly from a client machine to your SDDC in the vSphere Client. Right-click the <b>Compute-ResourcePool</b> resource pool and select <b>Deploy OVF template</b>.</li></ul> |
| OVA template          | Deploy the OVA template directly from a client machine to your SDDC using the vSphere Client. Right-click the <b>Compute-ResourcePool</b> resource pool and select <b>Deploy OVF template</b>   |
| ISO image             | <ul style="list-style-type: none"><li>■ Upload the ISO image to the workloadDatastore.</li><li>■ Import the ISO image into an on-premises Content Library and subscribe to the Content Library from your SDDC.</li><li>■ Create a local Content Library in your SDDC, and upload the ISO image to it.</li><li>■ Use the Content Onboarding Assistant to transfer the ISO image to your SDDC.</li></ul>  |
| scripts or text files | <ul style="list-style-type: none"><li>■ Import the file into an on-premises Content Library and subscribe to the Content Library from your SDDC.</li><li>■ Create a local Content Library in your SDDC and upload the file to it.</li><li>■ Use the Content Onboarding Assistant to transfer the file to your SDDC.</li></ul>   |

This chapter includes the following topics:

- [Use the Content Onboarding Assistant to Transfer Content to Your SDDC](#)
- [Use a Content Library to Import Content into Your SDDC](#)
- [Upload Files or Folders to your SDDC](#)

## Use the Content Onboarding Assistant to Transfer Content to Your SDDC

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

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

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

---

**Note** The Content Onboarding Assistant adds scripts and ISO images to a Content Library that is published from your on-premises data center and subscribed from your SDDC. It does not add existing OVF or OVA templates to the Content Library. For other ways of transferring OVF or OVA templates to your SDDC, see [Getting Templates, ISOs, and Other Content into Your SDDC](#) in the *VMware Cloud on AWS Operations Guide*.

---

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

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

### Prerequisites

Before you run Content Onboarding Assistant, do the following:

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



## Procedure

- 1 Prepare scripts and ISO images for addition to the Content Library by moving them into a single folder in your on-premises data center.  
     .vmtx templates need no special preparation.
- 2 Download the Content Onboarding Assistant from the download location.
  - a Click **Tools** in left-hand column of the VMC Console.
  - b On the Content Onboarding Assistant card, click **DOWNLOAD** to download `Content-Onboarding-Assistant-version.jar`, where *version* is **1.5** or a newer version of the file.
- 3 In the terminal or command line, switch to the directory where you placed the `Content-Onboarding-Assistant.jar` file and enter the command `java -jar jar_file_name --cfg full_path_to_config_file`.

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

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

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

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

| Parameter   | Description  |
|---|--|
| <code>cloudNetworkName</code> <i>network-name</i> | The distributed virtual port group on the cloud SDDC for the <code>.vmtx</code> templates.   |
| <code>sessionUpdate</code> <i>value</i>           | The time in milliseconds between session update calls. The default value is 60000 ms (10 minutes). If you experience issues with sessions timing out while the Content Onboarding Assistant is running, decrease this value. |

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

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

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

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

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

- 7 Select how to transfer your `.vmtx` templates.

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

## Results

The Content Onboarding Assistant does the following:

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

## What to do next

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

# Use a Content Library to Import Content into Your SDDC

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

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

### Prerequisites

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

### Procedure

- 1 Add your templates, ISO images, and scripts to the on-premises Content Library.  
All `.vmtx` templates are converted to OVF templates.
- 2 Publish your on-premises Content Library.
- 3 In your SDDC, create a Content Library that subscribes to the one you published in [Step 2](#). Content is synchronized from your on-premises data center to your SDDC in VMware Cloud on AWS.

## Upload Files or Folders to your SDDC

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

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

### Prerequisites

You must have the CloudAdmin role on the datastore.

### Procedure

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

| Option                 | Description  |
|------------------------|--|
| To create a new folder | <ol style="list-style-type: none"> <li>a Select the WorkloadDatastore or an existing folder.</li> <li>b Select <b>New Folder</b>.</li> </ol>                 |
| To upload a file       | <ol style="list-style-type: none"> <li>a Select a folder.</li> <li>b Click <b>Upload Files</b>.</li> <li>c Select a file and click <b>OK</b>.</li> </ol>     |
| To upload a folder     | <ol style="list-style-type: none"> <li>a Select a folder.</li> <li>b Select <b>Upload Folder</b>.</li> <li>c Select a folder and click <b>OK</b>.</li> </ol> |

# Migrating Virtual Machines

# 5

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

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

## Migration within the SDDC

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

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

## Hybrid Migration

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

- [Hybrid Migration With VMware HCX](#)

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

### ■ Hybrid Migration with vMotion

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

### ■ Hybrid Cold Migration

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

## Hybrid Migration With VMware HCX

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

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

**Note** Deployment of VMware HCX in 2-Host Stretched Clusters has limited support for production environments or for proof-of-concept purposes only. See VMware Knowledge Base article [87043](#) for details.

## Hybrid Migration with VMware HCX Checklist

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

| Requirement   | Description  |
|---|--|
| Networking speed  | Migration with vMotion using HCX requires a minimum of 100 Mbps throughput between source and destination.   |
| On-premises vSphere version                                       | <ul style="list-style-type: none"> <li>■ For vMotion: vSphere 6.0, 6.5, 6.7, 7.0</li> <li>■ For bulk migration: vSphere 6.0, 6.5, 6.7, 7.0</li> <li>■ For cold migration: vSphere 6.0, 6.5, 6.7, 7.0</li> </ul>  |
| On-premises virtual switch configuration                          | vSphere Distributed Switch<br>NSX Distributed Virtual Switch (N-VDS)<br>vSphere standard switch  |
| Installation of VMware HCX Manager in the on-premises data center | See the <i>VMware HCX Product Documentation</i> . HCX Connector Environment Requirements are described in <a href="#">Software Version Requirements for the HCX Installations</a> in the <i>VMware HCX Product Documentation</i> .                                 |
| Establish the HCX Interconnect with your SDDC                     | Pair the VMware HCX Manager with your VMware Cloud on AWS SDDC as a remote site as described in <a href="#">Configuring and Managing the HCX Interconnect</a> and <a href="#">Configuring and Managing the HCX Interconnect with the Multi-Site Service Mesh</a> . |

| Requirement                           | Description  |
|---------------------------------------|--|
| L2 VPN                                | Extend a network from your on-premises datacenter to your VMware Cloud on AWS SDDC as described in <a href="#">Extending Networks with VMware HCX</a> .  |
| VMware Cloud on AWS firewall rules    | Create firewall rules to open the ports used by HCX as described in <a href="#">Network Port and Protocol Requirements</a> .   |
| On-premises firewall rules            | Create firewall rules to open the ports used by HCX as described in <a href="#">Network Port and Protocol Requirements</a> .   |
| Virtual machine hardware and settings | <p>Ensure that these requirements are met for virtual machine hardware.</p> <ul style="list-style-type: none"> <li>Virtual machine hardware version and virtual disk size as specified in <a href="#">VMware Configuration Maximums</a>.</li> <li>EVC is not supported in the VMware Cloud on AWS SDDC.</li> <li>VMs that are created in the cloud SDDC or that have been power-cycled after migration to the cloud SDDC can't be migrated back to the on-premises data center with vMotion unless the on-premises EVC baseline is Broadwell. You can relocate these VMs after powering them off, as long as their virtual machine hardware version is compatible with the on-premises data center.</li> </ul> <p>The following virtual machines are not supported:</p> <ul style="list-style-type: none"> <li>VMs with shared .vmdk files.</li> <li>VMs with virtual media or ISOs attached.</li> </ul> |

## Hybrid Migration with vMotion

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

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

## Summary of Supported Configurations

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

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

See VMware Knowledge Base article [56991](#) for more information.

## Restrictions on VMs Migrated with vMotion

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

- VMs that use standard virtual switches for networking cannot be migrated back to an on-premises data center after being migrated to the cloud SDDC.
- Any VM that has been power-cycled in the cloud SDDC can only be migrated back to an on-premises host or cluster with the Broadwell chipset or EVC mode.
- If your on-premises hosts haven't been patched to address vulnerability to side channel analysis due to speculative execution (also referred to as the Spectre Variant 2 vulnerability), this may affect vMotion compatibility as shown in [Table 5-1. vMotion Compatibility Effects of Spectre patch](#). To find the correct patch for your on-premises hosts, see <https://kb.vmware.com/s/article/52245>. All hosts in VMware Cloud on AWS SDDCs have been patched.

**Table 5-1. vMotion Compatibility Effects of Spectre patch**

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

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

These restrictions don't apply to cold migration.

## Hybrid Migration with vMotion Checklist

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

**Note** HCX-based vMotion has a different set of requirements. See [Hybrid Migration with VMware HCX Checklist](#).

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

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



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

| Requirement                           | Description  |
|---------------------------------------|--|
| On-premises firewall rules            | Ensure that you have created the necessary firewall rules as described in <a href="#">Required Firewall Rules for vMotion</a> .  |
| Virtual machine hardware and settings | <p>Ensure that these requirements are met for virtual machine hardware.</p> <ul style="list-style-type: none"> <li>■ Virtual machine hardware version 9 or later is required for migration with vMotion from the on-premises data center to the cloud SDDC.</li> <li>■ EVC is not supported in the VMware Cloud on AWS SDDC.</li> <li>■ VMs that are created in the cloud SDDC or that have been power-cycled after migration to the cloud SDDC can't be migrated back to the on-premises data center with vMotion unless the on-premises EVC baseline is Broadwell. You can relocate these VMs after powering them off, as long as their virtual machine hardware version is compatible with the on-premises data center.</li> <li>■ Migration of VMs with DRS or HA VM overrides is not supported. For more information on VM overrides, see <a href="#">Customize an Individual Virtual Machine</a>.</li> </ul> |

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

## Required Firewall Rules for vMotion

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

### VMC on AWS Firewall Rules for vMotion

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

| Use Cases  | Source   | Destination                                    | Service           |
|--|--|--|-------------------|
| Provide access to vCenter Server from the on-premises.<br>Use for general vSphere Client access as well as for monitoring vCenter Server | remote (on-premises) vSphere Client IP address | vCenter  | HTTPS             |
| Allow outbound vCenter Server access to on-premises vCenter Server.  | vCenter  | remote (on-premises) vCenter Server IP address | Any (All Traffic) |

| Use Cases                                      | Source   | Destination  | Service                |
|--|--|--|------------------------|
| Allow SSO vCenter Server                       | remote (on-premises)<br>Platform Services<br>Controller IP address | vCenter  | SSO (TCP 7444)         |
| ESXi NFC traffic                               | remote (on-premises)<br>ESXi VMkernel networks<br>used for NFC.    | ESXi   | Provisioning (TCP 902) |
| Allow outbound ESXi<br>access to on-premises . | ESXi   | remote (on-premises)<br>ESXi management<br>VMkernel networks | Any (All Traffic)      |
| Allow vMotion traffic.                         | remote (on-premises)<br>ESXi vMotion VMkernel<br>networks          | ESXi   | vMotion (TCP 8000)     |

## On-Premises Firewall Rules for vMotion

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

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

## Bulk Migration with vMotion

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

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

### Summary of Supported Configurations

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

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

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

## Hybrid Cold Migration

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

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

### Summary of Supported Configurations

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

**Table 5-4. Supported Configurations for Hybrid Cold Migration**

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

## Hybrid Cold Migration Checklist

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

| Requirement  | Description   |
|--|---|
| On-premises vSphere version                        | vSphere 6.5 patch d and later<br>vSphere 6.0 update 3 and later   |
| On-premises virtual switch configuration           | Standard switches, vSphere Distributed Switch 6.0, or vSphere Distributed Switch 6.5  |
| IPsec VPN  | Configure an IPsec VPN for the management gateway. See "Configuring VPNs and Gateways" in <i>Getting Started With VMware Cloud on AWS</i> .   |
| Hybrid Linked Mode                                 | Hybrid Linked Mode is required to initiate migration from the vSphere Client. It is not required to initiate migration using the API or PowerCLI. See "Hybrid Linked Mode" in <i>Managing the VMware Cloud on AWS Data Center</i> . |
| VMware Cloud on AWS and on-premises firewall rules | Ensure that you have created the necessary firewall rules as described in <a href="#">Required Firewall Rules for Cold Migration</a> .  |
| On-premises DNS configuration                      | Ensure that your on-premises DNS server can correctly resolve the address for the cloud vCenter Server.   |

## Required Firewall Rules for Cold Migration

### SDDC Management Gateway Firewall Rules for Cold Migration

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

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

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

## On-Premises Firewall Rules for Cold Migration

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

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

# Accessing AWS Services

# 6

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

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

This chapter includes the following topics:

- [Configure Amazon FSx for NetApp ONTAP as External Storage](#)
- [Connecting EC2 With SDDC Workloads](#)
- [Access an S3 Bucket Using an S3 Endpoint](#)
- [Access an S3 Bucket Using the Internet Gateway](#)

## Configure Amazon FSx for NetApp ONTAP as External Storage

Amazon FSx for NetApp ONTAP integration with VMware Cloud on AWS is an AWS-managed external NFS datastore built on NetApp's ONTAP file system that can be attached to a cluster in your SDDC. It provides customers with flexible, high-performance virtualized storage infrastructure that scales independently of compute resources.

For more information and a reference architecture, see the VMware Cloud Tech Zone article [VMware Cloud on AWS integration with Amazon FSx for NetApp ONTAP](#).

---

**Note** VMware Cloud on AWS supports external storage starting with SDDC version 1.20. For information about upgrading an SDDC, see [Submit an Upgrade Schedule Request](#).

---

Each mountpoint exported by an FSx for ONTAP service is treated as a separate datastore when added as external storage. See [Actions Taken by VMware to Ensure SDDC Health](#) for details about the impact of NFS storage failures on SDDC operations.

You cannot deploy FSx for ONTAP in the Connected VPC. Instead, you must deploy it in another VPC that you own, then connect the VPC to a VMware Managed Transit Gateway (VTGW).

## Prerequisites


- Log in to the AWS console and create a VPC in the same region as the SDDC. It can be owned by any of your AWS accounts, but it must be a new VPC created for this use. In this document, we refer to this VPC as the FSx for ONTAP VPC.
- Follow the procedure in [Create an Amazon FSx for NetApp ONTAP file system](#) to create an FSx for ONTAP Multi-AZ deployment in the FSx for ONTAP VPC. The Storage Virtual Machine (SVM) floating IP address shown in the **Endpoints** section of the **Storage Virtual Machine** tab must be accessible from the SDDC Management Gateway. Make a note of this address. You'll need it when you attach the FSx for ONTAP storage to an SDDC cluster.
- To use FSx for ONTAP as an external datastore, an SDDC must be a member of an SDDC group so that it can use the group's VTGW. If you need to create a new SDDC group that includes this SDDC, or attach the SDDC to an existing SDDC group, follow the procedures in [Create or Modify an SDDC Group](#). To learn more about SDDC groups, see [Creating and Managing SDDC Deployment Groups with VMware Transit Connect™](#)

## Procedure

- 1 Open the VMC Console and follow the procedure in [Attach a VPC to an SDDC Group](#) to attach the FSx for ONTAP VPC to the SDDC group.
  - a Click **Add Account** and provide the AWS account ID that you used to create the FSx for ONTAP VPC. (Step 2 of [Attach a VPC to an SDDC Group](#).)
  - b In the AWS console navigate to **Transit Gateway Attachments** and use the dropdown control in the **Details** section to select the **Transit gateway ID** of the VTGW. Select the **DNS support** checkbox under **VPC attachment**, and click **Create Transit Gateway Attachment**. (Step 6 of [Attach a VPC to an SDDC Group](#).)

## 2 Add routes between the FSx for ONTAP VPC and the SDDC group VTGW.

- a Add a route from the SDDC group's VTGW to the FSx for ONTAP VPC floating IP range.

Open the **External VPC** tab for the SDDC group and select the **AWS Account ID** that owns the VPC and expand the row. If no routes have been specified, click **ADD ROUTES** in the **Routes** column to open the **Edit Routes** page and add one or more routes that use this VPC as a **Target**. Otherwise the **Routes** column shows the first route and the number of additional routes. Click the pencil icon () to open the **Edit Routes** page so you can edit this list to add the FSx for ONTAP VPC floating IP range.

- b Add the SDDC management prefixes to the route table(s) used for the FSx ONTAP deployment.

In the AWS console, navigate to the **Amazon FSx** page and select **File systems**, then click your file system to see the route table and other details. Click the route table ID under **Route tables**, then edit the route table to add a route with these parameters:

| Destination                  | Target                   |
|------------------------------|--------------------------|
| SDDC Management Gateway CIDR | VTGW transit gateway ID. |

See [Add and remove routes from a route table](#) in the AWS documentation for more information about editing the main route table of a VPC.

## 3 Add an inbound rule to the VPC's default security group.

In the AWS console, select the default Security Group for the FSx for ONTAP VPC and click the **Inbound** tab. Add a rule with the following parameters.

| Type        | Source   |
|-------------|--|
| All traffic | <b>Custom.</b> Enter the SDDC Management Gateway CIDR. |

Click **Save**.

## 4 Attach a mountpoint from the FSx datastore to the SDDC.

See [Add External Storage to a Cluster](#). In the VMC Console, open the **Storage** tab of your SDDC. Click **ATTACH DATASTORE** and fill in the required values.

|                           |  |
|---------------------------|--|
| <b>Cluster</b>            | Select a cluster. Cluster-1 is preselected if there are no other clusters. Stretched clusters are not supported.   |
| <b>Datastore</b>          | Choose <b>Attach a new datastore</b>   |
| <b>NFS server address</b> | The <b>NFS IP address</b> shown in the <b>Endpoints</b> section of the FSx <b>Storage Virtual Machine</b> tab. Click <b>VALIDATE</b> to validate the address and retrieve the list of mountpoints (NFS exports) from the server. |
| <b>Export</b>             | Pick one from the list of mountpoints exported by the server at the <b>NFS server address</b> . Each mountpoint must be added as a separate datastore.   |



|                |   |
|----------------|---|
| Storage Vendor | AWS FSx ONTAP   |
| Datastore Name | Give the datastore a name. Datastore names must be unique within an SDDC. |

Click **ATTACH DATASTORE** to add the FSx datastore.

## Connecting EC2 With SDDC Workloads

You can deploy an EC2 instance in your connected Amazon VPC and configure AWS security policies and compute gateway firewall rules to allow it to connect with your workload VMs.

Although this topic focusses on enabling traffic between your SDDC workloads and an EC2 instance in the Connected VPC, the modifications detailed in steps 2 and 3 also enable traffic between the EC2 instance and the SDDC management network, and similar AWS Security Group modifications should enable SDDC connectivity to any native AWS service that is reachable at an IP address in the Connected VPC's primary CIDR.

The default AWS Security Group in the connected VPC controls traffic from EC2 instances in the VPC to VMs in the SDDC. This traffic must also pass through the Compute Gateway firewall (and the Distributed Firewall if you're using that). All of these controls must be configured to allow the intended traffic or the connection can't be established.

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

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

VMware Knowledge Base article [76577](#) has additional information that applies to cases where the default AWS Security Group has a missing or altered allow-all rule for outbound traffic.

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

### Prerequisites

To complete this task, you need the following information:

- The CIDR blocks of the network segments the VMs in your SDDC are connected to. Click **Segments** on the **Networking & Security** tab to list all segments.

- The connected Amazon VPC and subnet. Click **Connected VPC** in the **System** category on the **Networking & Security** tab to open the **Connected Amazon VPC** page, which provides this information under **VPC ID** and **VPC Subnet**.

#### Procedure

- 1 Deploy the EC2 instance in your AWS account.

Keep in mind the following when creating the EC2 instance:

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

- 2 Add inbound rules to the Security Group applied to the instance. Select the EC2 instance that you deployed in [Step 1](#) and configure its Security Group to allow inbound traffic from the logical network or IP address associated with the VM in your SDDC.
  - a Select the instance that you deployed in [Step 1](#).
  - b In the instance description, click the instance's Security Group and click the **Inbound** tab.
  - c Click **Edit**.
  - d Click **Add Rule**.
  - e In the **Type** dropdown menu, select the type of traffic that you want to allow.
  - f In the **Source** text box, select **Custom** and enter the IP addresses or CIDR block of VMs in the SDDC that need to communicate with the instance.
  - g (Optional) Add rules as needed for additional CIDR blocks or traffic type you want to connect to the instance from VMs in your SDDC.
  - h Click **Save**.

- 3 (Optional) If you need to allow traffic initiated by the instance that you deployed in [Step 1](#) to a VM in your SDDC, edit the default Security Group for the connected Amazon VPC to add inbound rules that identify the instances by CIDR block or Security Group.
  - a In the AWS console, select the default Security Group for the Connected Amazon VPC and click the **Inbound** tab.
  - b Click **Edit**.
  - c Click **Add Rule**.
  - d In the **Type** dropdown menu, select the type of traffic that you want to allow.
  - e In the **Source** text box, select **Custom** and enter the IP addresses or CIDR block of VMs in the SDDC that need to communicate with the instance.  
  
If all the VMs are associated with the same SDDC Inventory Group, you can specify that Group as the **Source** rather than using an IP address or CIDR block.
  - f (Optional) Add rules as needed for additional CIDR blocks or traffic type you want to connect to the instance from VMs in your SDDC.
  - g Click **Save**.
- 4 Configure the necessary compute gateway firewall rules.

See [Add or Modify Compute Gateway Firewall Rules](#) in *VMware Cloud on AWS Networking and Security*.

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

---

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

---

- 5 (Optional) Configure distributed firewall rules.

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

## Access an S3 Bucket Using an S3 Endpoint

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

## Procedure

### 1 Create an S3 endpoint.

See [Gateway VPC Endpoints](#) and [Endpoints for Amazon S3](#) in the *Amazon Virtual Private Cloud User Guide*.

- a For **Service category**, select AWS services.
- b Under **Service Name**, select a `com.amazonaws.region-AZ.s3` service of type **Gateway** where *region-AZ* matches the region and AZ your SDDC is in. For example, `com.amazonaws.us-west-2.s3`.
- c In the **VPC** drop down, select the VPC that is connected to your SDDC.
- d Under **Configure route tables**, select the **Route Table ID** where the value in the **Main** column is **Yes**. This Route Table is used by the SDDC and should also be associated with the VPC subnet the SDDC is connected to.
- e Under **Policy** select the default Full Access policy or create a more restrictive one. See [Endpoints for Amazon S3](#) in the *Amazon Virtual Private Cloud User Guide*. Traffic to S3 from the SDDC will have its source IP NATted to an IP from the subnet selected at SDDC deployment, so any policy must allow traffic from that subnet.
- f Click **Create Endpoint** to create the endpoint and add routes for the S3 public IP ranges in the region to the main route table.

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

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

- a In the AWS console, select the default Security Group for the Connected Amazon VPC and click the **Outbound** tab.
- b Click **Edit**.
- c Click **Add Rule**.
- d In the **Type** dropdown menu, select **HTTPS**.
- e In the **Destination** text box, select the prefix list associated with the S3 endpoint.  
  
You can find this prefix list in the VPC's **Managed prefix lists** card. If you see multiple prefix lists here, choose one that is specific to the region that contains the S3 service you're interested in.
- f Click **Save**.

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

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

- a Log in to the VMC Console at <https://vmc.vmware.com>.
  - b Click > **Connected VPC**
  - c Under **Service Access**, click **Enable** next to **S3 Endpoint**.
- 4 From the VMC Console, create a compute gateway firewall rule to allow HTTPS access to the connected Amazon VPC.
    - a On the **Networking & Security** tab, click **Gateway Firewall**.
    - b On the **GATEWAY FIREWALL** page, click **Compute Gateway**.
    - c Click **ADD RULE** and add a rule with the following parameters, where *Workload-CIDR* is the CIDR block for the segment that the workload VMs that need to access S3.

| Sources              | Destinations | Services | Applied To    | Action |
|----------------------|--------------|----------|---------------|--------|
| <i>Workload-CIDR</i> | S3 Prefixes  | HTTPS    | VPC Interface | Allow  |

## Results

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

## Access an S3 Bucket Using the Internet Gateway

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

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

## Prerequisites

Ensure that the access permissions for the S3 bucket permit access from your cloud SDDC from the Internet. See [Managing Access Permissions to Your Amazon S3 Resources](#) for more information.

## Procedure

- 1 Log in to VMware Cloud Services at <https://vmc.vmware.com>.
- 2 Click **Inventory > SDDCs**, then pick an SDDC card and click **VIEW DETAILS**.
- 3 Click **OPEN NSX MANAGER** and log in with the **NSX Manager Admin User Account** shown on the SDDC **Settings** page.

You can also use the VMC Console **Networking & Security** tab for this workflow. See [SDDC Network Administration with NSX Manager](#).

- 4 Disable access to S3 from the Connected Amazon VPC.

Click **Cloud Services > Connected VPC** to open the **Connected Amazon VPC** page, then toggle the S3 **Enabled** setting.

- 5 From the VMC Console, create a compute gateway firewall rule to allow https access to the internet.
  - a On the **GATEWAY FIREWALL** page, click **Compute Gateway**.
  - b Click **ADD RULE** and add a rule with the following parameters, where *Workload-CIDR* is the CIDR block for the segment that the workload VMs that need to access S3.

| Sources              | Destinations | Services | Applied To         | Action |
|----------------------|--------------|----------|--------------------|--------|
| <i>Workload-CIDR</i> | Any          | HTTPS    | Internet Interface | Allow  |

## Results

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

# Using On-Premises vRealize Automation with Your Cloud SDDC

## 7

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

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

This chapter includes the following topics:

- [Prepare Your SDDC to Work with vRealize Products](#)
- [Connect vRealize Automation 8.x to Your SDDC](#)

## Prepare Your SDDC to Work with vRealize Products

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

### Procedure

- 1 Configure a VPN connection over the public Internet or AWS Direct connect.  
See [Configure VPN Connectivity to the On-Premises Data Center](#) and [Configure AWS Direct Connect for VMware Cloud on AWS](#) in *VMware Cloud on AWS Networking and Security*.
- 2 Verify that the vCenter Server FQDN is resolvable at a private IP address on the management network.  
See [Set vCenter Server FQDN Resolution Address](#) in *VMware Cloud on AWS Networking and Security*.

- 3 Configure additional firewall rules if necessary.

vRealize Automation requires the following Management Gateway firewall rules.

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

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

**Table 7-1. Management Gateway Firewall Rules Required by vRealize Automation (continued)**

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

See [Add or Modify Management Gateway Firewall Rules](#) in *VMware Cloud on AWS Networking and Security*.

## Connect vRealize Automation 8.x to Your SDDC

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

### Prerequisites

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

### Procedure

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

If you are using an earlier version of vRealize Automation, see [Connect vRealize Automation 7.x to Your SDDC](#).

## Connect vRealize Automation 7.x to Your SDDC

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

### Prerequisites

- See the [VMware Product Interoperability Matrices](#) for the list of vRealize Automation 7.x releases that you can use with VMware Cloud on AWS.



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

#### Procedure

- 1 In vRealize Automation, select **Infrastructure > Endpoints**.
- 2 Select **New > Virtual > vSphere (vCenter)**.
- 3 Specify the vCenter Server URL in the format **https://fqdn/sdk**.
- 4 Specify the cloud admin credentials.
- 5 Click **Test Connection** and **Accept Certificate**.
- 6 Create a Fabric Group.
  - a Add the cloud admin as the fabric administrator.
  - b Add the default SDDC cluster Cluster-1 to the Compute Resources.
 For more information on creating a Fabric Group, see [Create a Fabric Group](#).
- 7 Create reservations for the components that the cloud admin has access to.

| Option               | Description   |
|----------------------|---|
| Resource Pool        | Compute-ResourcePool  |
| Datastore            | WorkloadDatastore   |
| VM & Template Folder | Workloads   |
| Network              | Use the logical network that you created as part of the prerequisites |

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

- 8 Create a Network Profile for the logical network you created as part of the prerequisites.  
For more information on creating a network profile, see [Create a Network Profile](#).
- 9 Create a Blueprint.  
For more information on Blueprints, see [Providing Service Blueprints to Users](#).

# Service Notifications and Activity Log



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

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

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

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

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

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

This chapter includes the following topics:

- [View the Activity Log](#)
- [View and Subscribe to the Service Status Page](#)
- [Notifications Available from VMware Cloud on AWS](#)
- [Set Notification Preferences](#)

## View the Activity Log

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

### Procedure

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

## 2 Click **Activity Log**.

Entries are displayed in reverse chronological order, with the newest entries at the top.

- 3 (Optional) If an entry indicates that a task failed, click to expand the task to show the error message.

## View and Subscribe to the Service Status Page

VMware publishes service operational status and maintenance schedules at [status.vmware-services.io](https://status.vmware-services.io).

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

### Procedure

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

## Notifications Available from VMware Cloud on AWS

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

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

### Maintenance Related Notifications

| Display Name                       | Template ID                     | Description   | Email Channel |
|------------------------------------|---------------------------------|---|---------------|
| Maintenance Change Window Complete | MaintenanceChangeWindowComplete | vCenter Server upgrade is complete. (Used only in version 1.8 and earlier.) | Yes           |
| Maintenance Change Canceled        | MaintenanceChangeCanceled       | A scheduled upgrade of an SDDC has been canceled.                           | Yes           |
| Host Patching Complete             | HostPatchingComplete            | SDDC Upgrade has completed. (Used only in version 1.8 and earlier.)         | Yes           |
| DFC Deduplication Scheduled        | DFC-DedupeScheduled             | A DFC change to an SDDC has been scheduled.                                 | Yes           |
| DFC Deduplication Start            | DFC-DedupeStart                 | A DFC change to an SDDC has begun.  | Yes           |
| DFC Deduplication Complete         | DFC-DedupeComplete              | A DFC change to an SDDC has completed.                                      | Yes           |
| DFC Deduplication Canceled         | DFC-DedupeCanceled              | A DFC change to an SDDC has been canceled.                                  | Yes           |

| Display Name                 | Template ID                     | Description   | Email Channel |
|------------------------------|---------------------------------|---|---------------|
| Initial Rollout Scheduled    | NSX-T-InitialRolloutScheduling  | An upgrade of an SDDC has been scheduled. (Used only in version 1.8 and earlier when using NSX.)          | Yes           |
| Control Plane Window Started | NSX-T-ControlPlaneWindowStarted | vCenter Server upgrade has begun. (Used only in version 1.8 and earlier.)                                 | Yes           |
| Host Networking Started      | NSX-T-HostNetworkingStarted     | NSX upgrade has begun. (Used only in version 1.8 and earlier.)  | Yes           |
| Host Networking Complete     | NSX-T-HostNetworkingComplete    | NSX upgrade has completed. (Used only in version 1.8 and earlier.)  | Yes           |
| Reschedule Notification      | NSX-T-RescheduleNotification    | A scheduled upgrade of an SDDC has been rescheduled. (Used only in version 1.8 and prior when using NSX.) | Yes           |
| V2-RolloutScheduled          | V2-RolloutScheduled             | An upgrade of an SDDC has been scheduled. (Used in version 1.9 and later.)                                | Yes           |
| V2-RolloutRescheduled        | V2-RolloutRescheduled           | An upgrade of an SDDC has been rescheduled (Used in version 1.9 and later.)                               | Yes           |
| V2-RolloutCancelled          | V2-RolloutCancelled             | An upgrade of an SDDC has been canceled (Used in version 1.9 and later.)                                  | Yes           |
| V2-Phase1Started             | V2-Phase1Started                | Upgrade of the SDDC Control Plane has begun. (Used in version 1.9 and later.)                             | Yes           |
| V2-Phase1Completed           | V2-Phase1Completed              | Upgrade of the SDDC Control Plane has completed. (Used in version 1.9 and later.)                         | Yes           |
| V2-Phase2Started             | V2-Phase2Started                | Upgrade of the ESXi hosts in an SDDC has begun. (Used in version 1.9 and later.)                          | Yes           |
| V2-Phase2Completed           | V2-Phase2Completed              | Upgrade of the ESXi hosts in an SDDC has completed. (Used in version 1.9 and later.)                      | Yes           |
| V2-Phase3Started             | V2-Phase3Started                | Upgrade of NSX Manager has begun. (Used in version 1.9 and later.)  | Yes           |

| Display Name                                     | Template ID                                       | Description   | Email Channel              |
|--|---|---|----------------------------|
| V2-Phase3Completed                               | V2-Phase3Completed                                | Upgrade of NSX Manager has completed. (Used in version 1.9 and later).  | Yes                        |
| V2-MaintenanceDelayed                            | V2-MaintenanceDelayed                             | Upgrade of an SDDC has been delayed. (Used in version 1.9 and later.)   | Yes                        |
| AZ failure simulation has started                | AZfailuresimulationtestinghasstarted              | Simulation of an AZ failure has started for a stretched cluster.  | Yes                        |
| AZ failure simulation has completed successfully | AZfailuresimulationtestingcomplete                | Simulation of an AZ failure has completed successfully for a stretched cluster.   | Yes                        |
| AZ failure simulation completed with exceptions  | AZfailuresimulationtestingcompletedwithexceptions | Simulation of an AZ failure has completed for a stretched cluster. During the simulation, some VMs could not be recovered. Verify that these VMs have correct storage policies applied and sufficient resources available for recovery. | Yes                        |
| Host Issue Detected                              | HostIssueDetected                                 | Autoscaler has detected an issue with an ESXi host.   | Contact support to opt-in. |
| Host Successfully Replaced                       | ReplaceHostSuccessful                             | An ESXi host that was experiencing an issue was replaced.   | Contact support to opt-in. |
| Host Successfully Remediated                     | RemediateHostSuccessful                           | An ESXi host that was experiencing an issue was remediated.   | Contact support to opt-in. |
| Planned Maintenance: Started                     | PlannedMaintenanceStarted                         | Planned maintenance activity has started.   | Contact support to opt-in. |

## SDDC Upgrade Notifications

| Display Name             | Template ID                     | Description  | Email Channel |
|--------------------------|---------------------------------|--|---------------|
| Add temporary ESX hosts  | VRTAddHostCompleted             | Successfully added temporary host to each cluster. | No            |
| Backup of management VMs | VRTBackupCompleted              | Successfully completed backup of management VMs.   | No            |
| Control plane upgrade    | VRTControlPlaneUpgradeCompleted | Control plane upgrade completed successfully.      | No            |

| Display Name               | Template ID                       | Description  | Email Channel |
|----------------------------|-----------------------------------|--|---------------|
| Data plane health check    | VRTDataPlaneHealthCompleted       | Data plane health check completed successfully.                          | No            |
| Data plane upgrade         | VRTDataPlaneUpgradeCompleted      | Data plane upgrade completed successfully.                               | No            |
| SDDC upgrade health check  | VRTHealthCheckCompleted           | SDDC upgrade health check completed successfully.                        | No            |
| Host network upgrade       | VRTNetworkingUpgradeCompleted     | Network upgrade of hosts in all clusters completed successfully.         | No            |
| NSX controller upgrade     | VRTNSXControllersUpgradeCompleted | Upgrade of NSX Controllers completed successfully.                       | No            |
| NSX edge upgrade           | VRTNSXEdgesUpgradeCompleted       | Upgrade of NSX Edges completed successfully.                             | No            |
| NSX manager upgrade        | VRTNSXManagerUpgradeCompleted     | Upgrade of NSX Manager completed successfully.                           | No            |
| POP upgrade                | VRTPopUpgradeCompleted            | POP upgrade completed successfully.                                      | No            |
| Remove temporary ESX hosts | VRTRemoveHostCompleted            | Successfully removed the temporary host from clusters.                   | No            |
| Stage upgrade bundles      | VRTStagingCompleted               | Successfully staged the upgrade bundles.                                 | No            |
| UC Upgrade                 | VRTUCUpgradeCompleted             | Successfully upgraded the NSX Upgrade Co-ordinator.                      | No            |
| Upgrade Issue              | VRTUpgradeFailed                  | Issue encountered during upgrade. VMware is working to resolve the issue | No            |
| SDDC upgrade maintenance   | VRTUpgradeMaintenanceCompleted    | SDDC is out of maintenance.  | No            |
| vCenter upgrade            | VRTvCenterUpgradeCompleted        | vCenter upgrade completed successfully.                                  | No            |
| vCenter upgrade started    | VRTvCenterUpgradeStarted          | vCenter upgrade started.   | No            |
| NSX Edge downtime          | VRTNSXEdgeUpgradeDowntime         | Change of active Edge due to upgrade at {timestamp}.                     | No            |
| NSX Edge upgrade downtime  | VRTNSXEdgeDowntime                | Active Edge was migrated to a different host at {timestamp}.             | No            |
| NSX Edge upgrade           | VRTNSXEdgesUpgradeCompleted       | Upgrade of NSX Edges completed successfully.                             | No            |

| Display Name                      | Template ID                          | Description  | Email Channel |
|-----------------------------------|--------------------------------------|--|---------------|
| Upgrade of all hosts in a cluster | VRTClusterUpgradeCompleted           | Upgrade of all hosts in {cluster_name} completed successfully.                   | No            |
| Upgrade of hosts                  | VRTClusterUpgradeProgress            | Upgrade of hosts in {completed}/{total} clusters completed successfully.         | No            |
| Network upgrade of host           | VRTClusterNetworkingUpgradeProgress  | Network upgrade of all hosts in {cluster_name} completed successfully.           | No            |
| Network upgrade of cluster        | VRTClusterNetworkingUpgradeCompleted | Network upgrade of hosts in {completed}/{total} clusters completed successfully. | No            |

## Autoscaler/EDRS Notifications

| Display Name                     | Template ID                    | Description  | Email Channel |
|----------------------------------|--------------------------------|--|---------------|
| High Storage Consumption Warning | HighStorageConsumptionInternal | A vSAN cluster has exceeded 70% storage capacity but has not yet reached the scale out threshold.            | Yes           |
| eDRS: Host Add (Storage)         | StorageScaleOut                | eDRS successfully added a host after storage capacity reached 80%.   | Yes           |
| One Node Planned Maintenance     | OneNodePlannedMaintenance      | One node SDDC planned maintenance will result in the SDDC being deleted. Add hosts to avoid losing the SDDC. | Yes           |
| eDRS: Host Add (CPU)             | CpuScaleOut                    | eDRS successfully added a host after CPU utilization reached 90%.  | Yes           |
| eDRS: Host Add (Memory)          | MemoryScaleOut                 | eDRS successfully added a host after memory utilization reached 80%.   | Yes           |
| eDRS: Host Maximum Reached       | EdrsReachedMaximumHostLimit    | eDRS reached maximum host limit.   | Yes           |
| eDRS: Host Maximum Exceeded      | EdrsExceededMaximumHostLimit   | eDRS exceeded maximum host limit.  | Yes           |
| Host Issue Detected              | HostIssueDetected              | Autoscaler has detected an issue with an ESXi host.  | No            |
| Host Successfully Replaced       | ReplaceHostSuccessful          | An ESXi host that was experiencing an issue was replaced.  | No            |

| Display Name                 | Template ID               | Description   | Email Channel |
|------------------------------|---------------------------|---|---------------|
| Host Successfully Remediated | RemediateHostSuccessful   | An ESXi host that was experiencing an issue was remediated. | No            |
| Planned Maintenance: Started | PlannedMaintenanceStarted | Planned maintenance activity has started.                   | No            |

## General Org Notifications

| Display Name                               | Template ID                               | Description  | Email Channel |
|--|---|--|---------------|
| Expiring subscription in 30 days           | expiringSubscription30Days                | Reminder to take action for the expiring subscription.   | Yes           |
| Expiring subscription in 60 days           | expiringSubscription60Days                | Reminder to take action for the expiring subscription.   | Yes           |
| Reminder for expiring subscription today   | expiringSubscriptionToday                 | Reminder to take action for the expiring subscription.   | No            |
| Reminder for AWS account linking on day 4  | starshot-awsAccountLinkingDay4            | Reminder for Single Host SDDC user to complete account linking.                                  | Yes           |
| Reminder for AWS account linking on day 13 | starshot-awsAccountLinkingDay13           | Reminder for Single Host SDDC user to complete account linking.                                  | Yes           |
| Reminder for AWS account linking on day 28 | starshot-awsAccountLinkingDay28           | Reminder for Single Host SDDC user to complete account linking.                                  | Yes           |
| Expiring Single Host Today                 | ExpiringSingleHost_0Day                   | Reminder that a Single Host SDDC is expiring and will be removed from the environment today.     | Yes           |
| Expiring Single Host in 2 Days             | ExpiringSingleHost_2Days                  | Reminder that a Single Host SDDC is expiring and will be removed from the environment in 2 days. | Yes           |
| Expiring Single Host in 7 Days             | ExpiringSingleHost_7Days                  | Reminder that a Single Host SDDC is expiring and will be removed from the environment in 7 days. | Yes           |
| Expiring SPP Fund in 7 Days                | ExpiringSPPfund_7Days_with_other_funds    | Reminder that an SPP fund is expiring and you may lose the remaining credits in 7 days.          | Yes           |
| Expiring SPP Fund in 7 Days                | ExpiringSPPfund_7Days_without_other_funds | Reminder that an SPP fund is expiring and you may lose the remaining credits in 7 days.          | Yes           |



| Display Name                 | Template ID                                | Description  | Email Channel |
|------------------------------|--|--|---------------|
| Expiring SPP Fund in 30 Days | ExpiringSPPfund_30Days_with_other_funds    | Reminder that an SPP fund is expiring and you may lose the remaining credits in 30 days. | Yes           |
| Expiring SPP Fund in 30 Days | ExpiringSPPfund_30Days_without_other_funds | Reminder that an SPP fund is expiring and you may lose the remaining credits in 30 days. | Yes           |
| Expiring SPP Fund in 60 Days | ExpiringSPPfund_60Days_with_other_funds    | Reminder that an SPP fund is expiring and you may lose the remaining credits in 60 days. | Yes           |
| Expiring SPP Fund in 60 Days | ExpiringSPPfund_60Days_without_other_funds | Reminder that an SPP fund is expiring and you may lose the remaining credits in 60 days. | Yes           |

## Site Recovery Notifications

| Display Name   | Template ID                                  | Description   | Email Channel |
|--|--|---|---------------|
| Site Recovery - SSL certificates replacement started   | Draas-SSLCertificateRenew-started            | VMware Site Recovery has started replacement of SSL certificates of SRM and VR appliances in the SDDC.  | Yes           |
| Site Recovery - SSL certificates replacement started   | Draas-SSLCertificateRenew-started-vmc-only   | VMware Site Recovery has started replacement of SSL certificates of SRM and VR appliances in the SDDC.  | Yes           |
| Site Recovery - SSL certificates replacement completed | Draas-SSLCertificateRenew-completed          | VMware Site Recovery has completed replacement of SSL certificates of SRM and VR appliances. Customer action is required on the remote (on-premises) DR site to recover the normal state of the VR pairing. | Yes           |
| Site Recovery - SSL certificates replacement completed | Draas-SSLCertificateRenew-completed-vmc-only | VMware Site Recovery has completed replacement of SSL certificates of SRM and VR appliances. Customer action is required on the remote (on-premises) DR site to recover the normal state of the VR pairing. | Yes           |

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

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

| Display Name                      | Template ID           | Description  | Email Channel |
|-----------------------------------|-----------------------|--|---------------|
| Site Recovery - Scheduled Upgrade | Draas-upgrade-planned | <p>VMware Site Recovery has scheduled its upgrade in 7 days. Customer should ensure that SRM recovery plans are in a state which allows upgrade to avoid re-schedule or cancelation of the upgrade.</p> <p>This heads up notification for VSR maintenance activity - upgrade of SRM and VR appliances. It is send at least 7 days before the actual start of the maintenance. Normally the upgrade completes for ~ 30min, but the maintenance windows is booked for 4h to allow time for troubleshooting / fixing if there are issues.</p> <p>The VSR upgrade should not overlap with the SDDC upgrade window, and it doesn't impact non VSR related functionality in the SDDC. Actual visible impact for the user is due to restart of SRM and VR which is in less than 2mins. Customer action is required prior maintenance - customer needs to ensure that their SRM recovery plans are in a state which allows upgrade. If this is not true at the time of the maintenance, the maintenance is re-scheduled or cancelled. Customer also needs to make sure that their on-prem SRM/VR version is upgraded to compatible one with the cloud SRM/VR version to be deployed.</p> | Yes           |

| Display Name  | Template ID   | Description   | Email Channel |
|---|---|---|---------------|
| Site Recovery - Scheduled Upgrade - 8.2 port change | Draas-upgrade-planned-82portchange                  | VMware Site Recovery has scheduled its upgrade in 7 days. Customer should ensure that SRM recovery plans are in a state which allows upgrade to avoid re-schedule or cancelation of the upgrade. This is received only when you upgrading VMware Site Recovery from 8.1 to 8.3. | Yes           |
| Site Recovery - Re-Scheduled Upgrade                | Draas-upgrade-replanned                             | VMware Site Recovery has re-scheduled its upgrade for another date.   | Yes           |
| Site Recovery - Scheduled Upgrade Completed         | Draas-upgrade-finish                                | VMware Site Recovery has completed its scheduled upgrade.   | Yes           |
| Site Recovery - Scheduled Upgrade Canceled          | Draas-upgrade-cancel                                | VMware Site Recovery has canceled its scheduled upgrade.  | Yes           |
| Site Recovery - On-prem Upgrade                     | Draas-upgrade-paired-on-prem                        | Heads-up for upgrade of VMware Site Recovery to 8.3 for SDDCs paired to on-prem site with SRM 8.1 or later.   | Yes           |
| Site Recovery - vmc(820) Upgrade                    | Draas-upgrade-paired-vmc-820                        | Heads-up for upgrade of VMware Site Recovery to 8.3 for SDDCs paired to another VMC on AWS SDDC.  | Yes           |
| Site Recovery - On-prem(820) Upgrade                | Draas-upgrade-paired-on-prem-820                    | Heads-up for upgrade of VMware Site Recovery to 8.3 for SDDCs paired to on-prem site with SRM 8.2.  | Yes           |
| Site Recovery - vCenter certificate renew completed | Draas-VC-cert-replaced-vr-pairing-needs-reconfigure | Renew of PSC/vCenter Certificate in VMC on AWS SDDC was performed.  | Yes           |

## VMC Operator Notifications

| Display Name                       | Template ID                     | Description   | Email Channel |
|------------------------------------|---------------------------------|---|---------------|
| SDDC SSL Certification Replacement | SddcSSLCertificationReplacement | A vCenter and NSX SSL certificate update window has been scheduled for your SDDC. | Yes           |
| Single Host SDDC Failure           | Single_Host_SDDC_Failure        | Host failure notification for a single host SDDC.                                 | Yes           |

## Activity Events

| Display Name                       | Template ID                        |
|------------------------------------|------------------------------------|
| Cluster addition                   | CLUSTER-CREATE                     |
| Deployment of SDDC                 | SDDC-PROVISION                     |
| Cluster deletion                   | CLUSTER-DESTROY                    |
| Removal of ESX host                | ESX-DELETE                         |
| Removal of SDDC                    | SDDC-DELETE                        |
| Provision of ESX host              | ESX-PROVISION                      |
| Provision of Multi-AZ SDDC         | MULTI-AZ-SDDC-PROVISION            |
| Scale up SDDC from Single Host     | SDDC-CONVERT                       |
| Multi-AZ Cluster addition          | MULTIAZ_CLUSTER-CREATE             |
| Creation of subscription           | CREATE-OFFER-SUBSCRIPTION          |
| Linking of AWS account             | ACCOUNT-LINK                       |
| Deletion of POP ssh access         | DELETE_POP_SSH_ACCESS_TASK_TYPE    |
| Update of POP ssh access           | UPDATE_SSH_ACCESS_TASK_TYPE        |
| Update of vCenter delegated user   | UPDATE_VCENTER_DELEGATED_USER_TASK |
| Updating Management VM             | MANAGEMENT-VM                      |
| Deletion of vCenter delegated user | DELETE_VCENTER_DELEGATED_USER_TASK |
| Addition of POP ssh access         | ADD_POP_SSH_ACCESS_TASK_TYPE       |
| Creation of delegated vCenter user | CREATE_DELEGATED_VCENTER_USER_TASK |
| Creation of an SDDC group          | SDDC_GROUP_CREATE_TASK_TYPE        |
| Update of an SDDC group            | SDDC_GROUP_UPDATE_TASK_TYPE        |
| Deletion of an SDDC group          | SDDC_GROUP_DELETE_TASK_TYPE        |

| Display Name                                      | Template ID  |
|---|--|
| SDDC member added to group                        | SDDC_GROUP_MEMBER_ADDITION_TASK_TYPE               |
| SDDC member deleted from group                    | SDDC_GROUP_MEMBERS_DELETION_TASK_TYPE              |
| Addition of a Direct Connect Gateway to a group   | SDDC_GROUP_ON_PREM_CONNECTIVITY_PROPOSAL_TASK_TYPE |
| Deletion of a Direct Connect Gateway from a group | SDDC_GROUP_ON_PREM_CONNECTIVITY_DELETE_TASK_TYPE   |
| Addition of an external AWS account               | SDDC_SHARE_CONNECTOR_TASK_TYPE                     |
| Removal of an external AWS account                | SDDC_SHARE_CONNECTOR_DELETE_TASK_TYPE              |
| Update to external attachments                    | EXTERNAL_L3_CONNECTION_TASK_TYPE                   |

## Set Notification Preferences

All notification appear in the Activity Log in the console. You can set preferences to choose which notifications you receive through email.

### Procedure

- 1 Log in to the VMC Console at <https://vmc.vmware.com>.
- 2 Click the preferences icon in the left navigation.
- 3 Select which notifications you want to receive through email.
  - Select the check box next to a notification category to receive email notifications for all events in that category.
  - Expand a category and select individual check boxes to receive notifications for individual events.
- 4 Click **Save Changes** to save the your changes.

# Troubleshooting

# 9

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

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

This chapter includes the following topics:

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

## Get Support

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

### Procedure

- 1 Before you contact VMware for support, have the support information for your SDDC ready.
  - a Log in to the VMC Console at <https://vmc.vmware.com>.
  - b Click **Inventory > SDDCs**, then pick an SDDC card and click **VIEW DETAILS**.
  - c Click **Support** to view the support information.
- 2 See [How Do I Get Support](#) for more information about using VMware Cloud Services in-product support.

## Unable to Connect to VMware Cloud on AWS



### Problem

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

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

### Cause

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

### Solution

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

| Option  | Description  |
|---|--|
| <b>Delete cookies</b>                               | <p>Follow the instructions for your browser. If you want to delete only specific cookies, delete ones with "vmware" and "vidm" in the name.</p> <ul style="list-style-type: none"> <li>■ Google Chrome: See <a href="https://support.google.com/chrome/answer/95647">https://support.google.com/chrome/answer/95647</a></li> <li>■ Mozilla Firefox: See <a href="https://support.mozilla.org/en-US/kb/delete-cookies-remove-info-websites-stored">https://support.mozilla.org/en-US/kb/delete-cookies-remove-info-websites-stored</a></li> <li>■ Microsoft Internet Explorer: <a href="https://support.microsoft.com/en-us/help/17442/windows-internet-explorer-delete-manage-cookies">https://support.microsoft.com/en-us/help/17442/windows-internet-explorer-delete-manage-cookies</a></li> <li>■ Microsoft Edge: <a href="https://support.microsoft.com/en-us/help/10607/microsoft-edge-view-delete-browser-history">https://support.microsoft.com/en-us/help/10607/microsoft-edge-view-delete-browser-history</a></li> <li>■ Safari: <a href="https://support.apple.com/kb/PH21411?locale=en_US">https://support.apple.com/kb/PH21411?locale=en_US</a></li> </ul> |
| <b>Open an incognito or private browsing window</b> | <p>Follow the instructions for your browser:</p> <ul style="list-style-type: none"> <li>■ Google Chrome: Click the menu button and select <b>New incognito window</b>.</li> <li>■ Mozilla Firefox: Click the menu button and select <b>New Private Window</b>.</li> <li>■ Microsoft Internet Explorer: Click the tools button and select <b>Safety &gt; InPrivate Browsing</b>.</li> <li>■ Microsoft Edge: Click the More icon, and select <b>New InPrivate window</b>.</li> <li>■ Safari: Select <b>File &gt; New Private Window</b>.</li> </ul>  |

## Unable to Connect to vCenter Server

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

### Problem

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

### Cause

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

### Solution

- ◆ Create the following firewall rules.

**Table 9-1. Firewall Rules Required for vCenter Access**

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

## Unable to Select Subnet When Creating SDDC

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

### Problem

While deploying an SDDC, there is a step in which you select a VPC and subnet in your AWS account to connect to your SDDC. You might be unable to select a subnet during this step. A message in the UI indicates that there are no eligible subnets in the AWS availability zone (AZ) and region where the SDDC will be created.

### Cause

You must select a subnet created in the availability zone (AZ) where you plan to deploy your SDDC. If you have created only a single subnet and it's not in an AZ that supports VMware Cloud on AWS, you'll see this message.

**Solution**

- 1 Follow the recommendation in [Deploying and Managing a Software-Defined Data Center](#) to create a subnet in every AZ in the AWS Region where the SDDC will be created.
- 2 Re-try the subnet selection step in [Deploy an SDDC from the VMC Console](#).

## Unable to Copy Changed Password Into vCenter Login Page

**Problem**

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

**Cause**

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

**Solution**

Contact Technical Support and request a password change. See [Get Support](#).

## Compute Workloads Are Unable to Reach an On-Premises DNS Servers Over a Policy-Based VPN

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

**Problem**

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

**Cause**

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

**Solution**

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

- 2 If you must use a policy-based VPN as your on-premises connection, configure the SDDC side of the VPN tunnel to allow DNS requests over the VPN.
  - a Log in to the VMC Console at <https://vmc.vmware.com>.
  - b Select **Networking & Security > VPN > Policy Based**.
  - c Click the vertical ellipsis icon for the VPN and select **Edit VPN**.
  - d Under the **Local Network** drop-down, select **cgw-dns-network**.
  - e Click **SAVE**.
- 3 Configure the on-premises side of the tunnel of connect to *local\_gateway\_ip/32* in addition to the Local Gateway IP address. This allows DNS requests to be routed over the VPN.