VMware Cloud on AWS Operations Guide

8 February 2019
VMware Cloud on AWS

vmware®

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

https://docs.vmware.com/

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

docfeedback@vmware.com

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

Contents

About VMware Cloud on AWS Operations

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

Intended Audience

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

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

About Software-Defined Data Centers

1

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

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

This chapter includes the following topics:

Deploying and Managing a Software-Defined Data Center

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

There are a number of factors that you should consider before deploying your SDDC.

The default topology deployed is shown below.

Connected AWS account

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

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

AWS VPC Subnet Configuration and Availability Requirements

The VPC and subnet you use to connect the SDDC to your AWS account must meet several requirements:

- It must be dedicated to the SDDC. No other AWS services or instances should connect to that subnet.
- You must never link more than one SDDC to a given VPC, even using different VPC subnets. There is a one-to-one relationship between an SDDC and a VPC.
- The subnet(s) used for the SDDC, as well as any subnets on which AWS services or instances communicate with the SDDC must all be associated with the VPC's main route table.
- 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.

Important Be sure that your connected Amazon VPC includes a subnet in each Availability Zone (AZ) in the AWS Region where the SDDC will be created. That way, you can identify all the AZs where an SDDC can be deployed and select the AZ that best meets your SDDC placement needs, whether you want to keep your VMC workloads close to or isolated from your existing 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.

Single Host SDDC starter configuration for VMware Cloud on AWS

You can kickstart your VMware Cloud on AWS experience with a Single Host SDDC starter configuration. This is a time-limited offering designed for you to prove the value of VMware Cloud on AWS in your environment. The service life of a Single Host environment is limited to 30 day intervals. At any point during the service life of the Single Host SDDC, you can choose to scale up to a production SDDC configuration with three or more hosts, without loss of data. If you don't scale up the Single Host SDDC before the end of the service life, the SDDC is deleted along with all the workloads and data it contains.

Stretched Clusters for VMware Cloud on AWS

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

The following restrictions apply to stretched clusters:

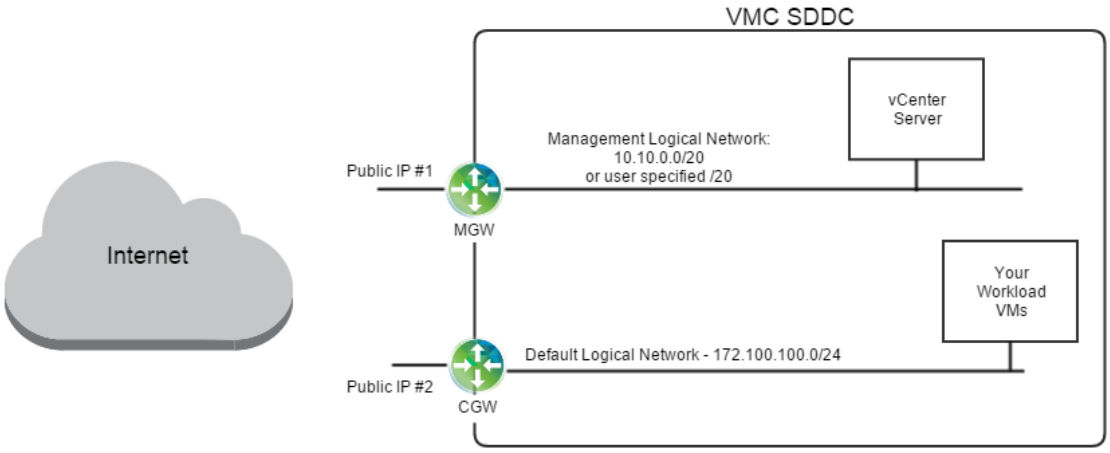
- You can't convert a stretched cluster to a single availability zone cluster, or vice versa.

- A given SDDC can contain either single availability zone clusters or stretched clusters, but not a mix of both.
- Currently, a given SDDC can contain only one stretched cluster.

Networking

The default networking topology deployed is shown below.

Figure 1-1. Default SDDC Topology



Management Gateway (MGW) The MGW is an NSX Edge Security gateway that provides north-south network connectivity for the vCenter Server and NSX Manager running in the SDDC. The Internet-facing IP address (Public IP #1) is automatically assigned from the pool of AWS public IP addresses when the SDDC is created. The management logical network internal to your SDDC is assigned the CIDR block 10.0.0.0/16 by default. When you create your SDDC, you can assign a different address block to prevent address conflicts with other environments that you connect to your SDDC.

Compute Gateway (CGW) The CGW provides north-south network connectivity for virtual machines running in the SDDC. VMware Cloud on AWS creates a default logical network to provide networking for these VMs. You can create additional logical networks using the vSphere Client.

You will need to configure IPsec VPNs, firewall rules, and other networking elements to allow full communication between your on-premises data center and your cloud SDDC.

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. There is a one-to-one relationship between SDDCs and customer AWS accounts. You can connect an SDDC to a single customer AWS account and Amazon VPC.

Procedure

1. Log in to the VMC Console at https://vmc.vmware.com.
2. Click **Create SDDC**.
3. Configure SDDC properties.
   a. Select the AWS region in which to deploy the SDDC.

      The following regions are available:

      - US West (Oregon)
      - US East (N. Virginia)
      - Europe (London)
      - Europe (Frankfurt)
      - Asia Pacific (Sydney)
      - Asia Pacific (Tokyo)
      - Europe (Ireland)
      - US West (N. California)
      - US East (Ohio)

   b. Select deployment options.

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

c Enter a name for your SDDC.

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

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

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

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

4 Connect to an AWS account.

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

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

5 Click **NEXT** to specify a range of IP addresses for the management subnet in the SDDC.

Enter an IP address range for the management network 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 the values specified for the management network after the SDDC has been created, so consider the following when you specify this address range:

- Choose a range of IP addresses that does not overlap with the AWS subnet you are connecting to. If you plan to connect your SDDC to an on-premises data center, the IP address range of the subnet must be unique within your enterprise network infrastructure. It cannot overlap the IP address range of any of your on-premises networks.
- The IP address range 192.168.1.0/24 is reserved for the default compute gateway logical network of the SDDC you are deploying. If you specify a management network address range that overlaps with 192.168.1.0/24, the default compute gateway logical network cannot be created during deployment, so you'll need to create one manually after the SDDC is deployed.

  In addition, CIDR blocks 10.0.0.0/15 and 172.31.0.0/16 are reserved for internal use. The management network CIDR block cannot overlap either of these ranges.

- CIDR blocks of size 16, 20, or 23 are supported. The primary factor in selecting a Management CIDR block size is the anticipated scalability requirements of the SDDC. If you intend to scale your SDDC beyond four hosts, consider using a /20 CIDR block. For CIDR blocks of size 20 or 16, the maximum number of hosts your SDDC can contain is limited to 160. Regardless of the number of AZs it occupies, an SDDC can have at most ten clusters with at most 16 hosts per cluster.

  A /23 CIDR block is appropriate for testing, or for SDDCs that you know will not require much growth in capacity. For CIDR blocks of size 23, the maximum number of hosts your SDDC can contain depends on the CIDR block size you specify and whether the SDDC occupies a single availability zone (AZ) or multiple AZs.

CIDR block size	Number of hosts (Single AZ)	Number of hosts (Multi AZ)
23	27	22
20, 16	160 (10 clusters with at most 16 hosts per cluster, regardless of the number of AZs.)	

What to do next

To connect to vCenter Server and manage your new SDDC, you must either configure a VPN connection to the management gateway or configure a firewall rule to allow access to vCenter Server.

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 remove, click **Actions > Rename SDDC**.
3. Type the new SDDC name and click **RENAME**.

Delete an SDDC

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

Procedure

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

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

Select all of the following:

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

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

4 Click **DELETE SDDC**.

View Billing Information

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

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

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

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

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

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

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

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

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

Procedure

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

Roles and Permissions in the SDDC

The CloudAdmin role and the CloudGlobalAdmin role are predefined in your cloud SDDC. When you log in VMware assigns you one of those roles on each object in the object hierarchy.

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

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

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:

Add a Cluster

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

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

Currently adding a cluster to an SDDC deployed in multiple availability zones is not supported.

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

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

Procedure

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

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

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

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

4 Select the number of hosts in the cluster.

5 click **Add Cluster**.

A progress bar shows the progress of cluster creation.

Remove a Cluster

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

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

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

Prerequisites

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

Procedure

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

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

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

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

Add Hosts

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

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

Procedure

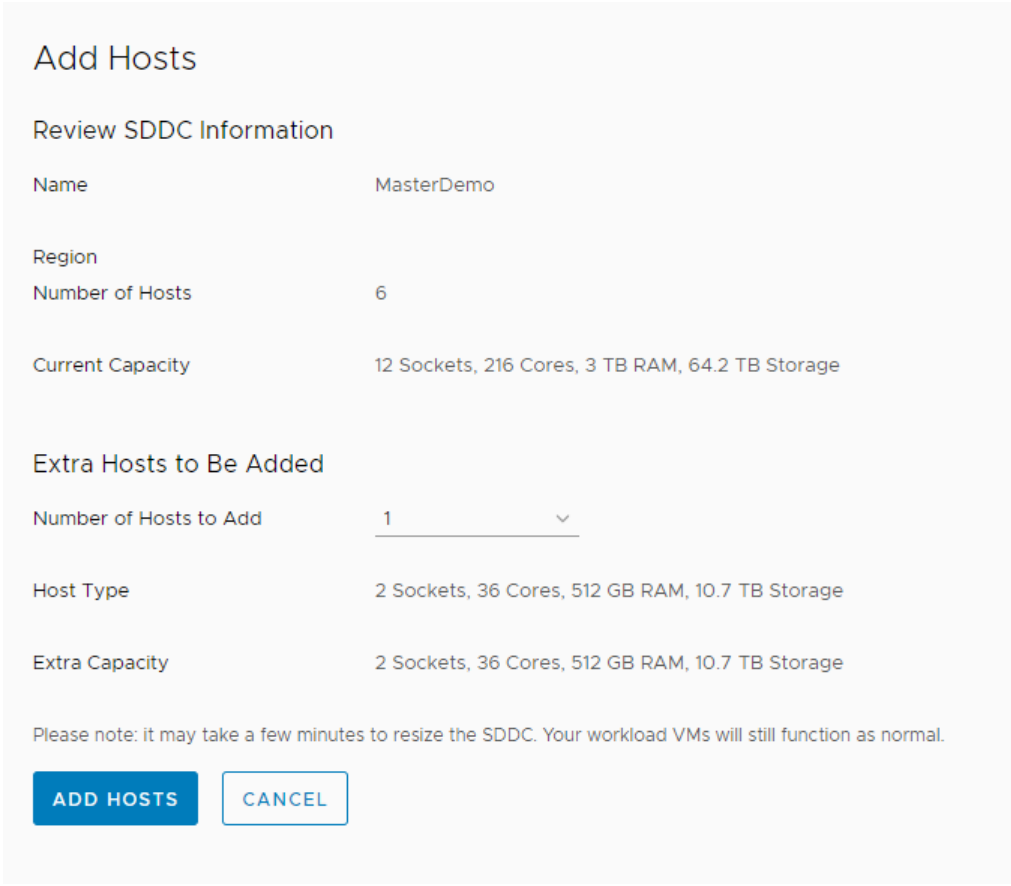
1 Log in to the VMC Console at https://vmc.vmware.com.

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

3 Select where to add the hosts.

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

The Add Hosts page is displayed.



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

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

One or more hosts are added to your SDDC cluster.

Remove Hosts

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

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

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

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

Prerequisites

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

Procedure

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

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

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

About Elastic DRS

Elastic DRS allows you to set policies to automatically scale your cloud SDDC by adding or removing hosts in response to demand.

To enable Elastic DRS, you apply a policy to a cluster in your SDDC. The policy has the following elements:

- Turn on or turn off Elastic DRS for the cluster.
- Specify the minimum and maximum number of hosts for the cluster.
- Specify whether the policy applied should optimize for cost or performance in applying recommendations.

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

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

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

How the Elastic DRS Algorithm Works

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

The algorithm 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 are predefined for each policy type and cannot be altered by user.

The algorithm runs every 5 minutes and monitors resource utilization over a period of time. Taking into consideration spikes and randomness in the utilization, the algorithm makes a determination to scale out or scale in a cluster by generating an alert. This alert is processed immediately by provisioning a new host or removing a host from the cluster.

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 75% but memory and CPU utilization remain below their respective thresholds, a scale-out recommendation is generated. The scale-out recommendation is not acted on if the number of hosts in the cluster is at the maximum specified value. A vCenter Server event is posted to indicate the start, completion, or failure of scaling out on the cluster.

Scale-in Recommendation

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

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

Time Delays Between Two Recommendations

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

- 30 minutes delay between two successive scale-out events.
- 3 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 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, fresh recommendations will be applied. If a planned maintenance event is received while an Elastic DRS recommendation is being applied for that cluster, the planned maintenance task will be queued. After the Elastic DRS recommendation task completes, the planned maintenance task starts.

- Auto-remediation

  As a result of auto-remediation, a failed host is replaced by a new host. While auto-remediation is in progress, the current recommendation by the Elastic DRS algorithm are ignored. After the auto-remediation operation completes, fresh recommendations will be applied. If an auto-remediation event is received while an Elastic DRS recommendation is being applied to that cluster, the auto-remediation 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 maintenance in the next 6 hours, EDRS recommendations are ignored.

Select Elastic DRS Policy

Set the Elastic DRS policy on a cluster to optimize for either cost or performance in scale-in and scale-out.

Elastic DRS is turned off by default.

Procedure

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

Option	Description
Optimize for Best Performance	Select the **Minimum cluster size** and **Maximum cluster size**. Elastic DRS adds hosts more quickly and removes hosts more slowly in order to provide best performance.
Optimize for Lowest Cost	Select the **Minimum cluster size** and **Maximum cluster size**. Elastic DRS adds hosts more slowly and removes hosts more quickly in order to provide the lowest cost.

5. Click **Save**.

Using Policies and Profiles

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

Creating and Managing Compute Policies

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

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

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

Monitoring Compliance

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

Create or Delete a VM-Host Affinity Policy

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

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

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

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

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

Prerequisites

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

Procedure

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

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

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

   Pick a category name that describes common characteristics, such as installed license types, of hosts you plan to tag as members of that category.

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

4. Create a VM-Host affinity policy.

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

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

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

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

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

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

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

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

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

Create or Delete a VM-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. 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.

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

- If the policy applies to more VMs that 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.
2. Tag the VMs that you want to include in each group.
3. Create a VM-VM anti-affinity policy.
   a. In your SDDC, click **OPEN VCENTER**.
   b. From the vSphere Client Home, click **Policies and Profiles > Compute Policies**.
   c. Click **Add** to open the **New Compute Policy** Wizard.
   d. Fill in the policy **Name** and choose **VM-VM anti affinity** from the **Policy type** drop-down control.

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

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

Create or Delete a Disable DRS vMotion Policy

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

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

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

Prerequisites

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

Procedure

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

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

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

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

Working With SDDC Add-On Services

3

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

Using The VMware Log Intelligence Service

The VMware Log Intelligence Service enables you to collect and analyze logs generated in your SDDC.

A trial version of the VMware Log Intelligence Service is enabled by default in a new SDDC. The trial period begins when a user in your organization accesses the Log Intelligence 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 VMware Log Intelligence, see the VMware Log Intelligence Documentation.

Getting Templates, ISOs, and Other Content into Your SDDC

4

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

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

This chapter includes the following topics:

Use the Content Onboarding Assistant to Transfer Content to Your SDDC

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

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

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

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

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

Prerequisites

Before you run Content Onboarding Assistant, do the following:

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

Procedure

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

   `.vmtx` templates need no special preparation.

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

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

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

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

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

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

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

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

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

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

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

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

The Content Onboarding Assistant does the following:

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

What to do next

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

Use a Content Library to Import Content into Your SDDC

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

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

Prerequisites

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

Procedure

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

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

2 Publish your on-premises Content Library.

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

Upload Files or Folders to your SDDC

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

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

Prerequisites

You must have the CloudAdmin role on the datastore.

Procedure

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

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

Migrating Virtual Machines 5

Migration refers to the process of moving virtual machines. VMware Cloud on AWS supports a number of different migration scenarios.

Types of Migration

There are three basic types of migration.

migration with vMotion	Migration with vMotion allows moving a powered on virtual machine from one host and/or datastore to another. Migration with vMotion is also referred to as "hot migration" or "live migration". Migration with vMotion is the best option for migrating small workloads without any downtime during migration.
bulk migration	You can perform bulk migration using the VMware Hybrid Cloud Extension (HCX). Bulk migration uses host-based replication to move large scale VMs between on-premises data centers and cloud SDDCs with low downtime. To reduce downtime, the source VM remains powered-on during the replication and then is powered off and booted on the destination immediately after migration or during a scheduled window.
cold migration	Cold migration is moving a powered-off virtual machine from one host and/or datastore to another. Cold migration is a good option when you can tolerate some virtual machine downtime during the migration process.

Migration within SDDC and Hybrid Migration Use Cases

Migration within SDDC refers to migrating virtual machines within your VMware Cloud on AWS SDDC. Cloud migration does not require additional configuration of your SDDC. The following cloud migration use cases are supported:

- cold migration and migration with vMotion between hosts within the same cluster within an SDDC
- cold migration and migration with vMotion between hosts in different clusters within the same SDDC

Hybrid migration refers to migrating virtual machines between an on-premises data center and a VMware Cloud on AWS SDDC. Hybrid migration use cases require additional prerequisites and configuration to ensure both compatibility of the virtual machines and appropriate network bandwidth and latency to support the migration. The following hybrid migration use cases are supported:

- Migration with vMotion from on-premises data center to cloud SDDC
- Migration with vMotion from cloud SDDC to on-premises data center (with some restrictions for VMs previously migrated from on-premises data centers)
- Cold migration from on-premises data center to cloud SDDC and from cloud SDDC to on-premises data center.
- Using HCX, bulk migration, migration with vMotion, and cold migration from the on-premises data center to the cloud SDDC and back. See the section "Migrating Virtual Machines" in https://hcx.vmware.com/content/docs/vmware-hcx-user-manual.pdf for more information on migration with HCX.

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. 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

Table 5-1. vMotion Compatibility Effects of Spectre patch (Continued)

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
		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.

Migration Options

You have different options for how you carry out migration depending on how many virtual machines you want to migrate and what type of interface you want to use.

Migration Type	Interface type	Use:
migration with vMotion	UI	■ For single VMs: vSphere Client (requires Hybrid Linked Mode configuration) ■ HCX
	command-line/automation	■ API ■ PowerCLI ■ HCX
bulk migration	UI or command-line/automation	HCX
cold migration	UI	■ For single VMs: vSphere Client (requires Hybrid Linked Mode configuration) ■ HCX
	command-line/automation	■ API ■ PowerCLI ■ HCX

Summary of Supported Configurations for Hybrid Migration

The following table summarizes the supported configurations for hybrid migration. For detailed requirements and configuration instructions, see Hybrid Cold Migration Checklist and Hybrid Migration with vMotion Checklist.

Migration Type	On-premises vSphere Version	Network Connectivity	VDS version on-premises
migration with vMotion	vSphere 6.0u3	AWS Direct Connect with private virtual interface and L2 VPN	VMware Distributed Switch version 6.0
	vSphere 6.5 patch d	AWS Direct Connect with private virtual interface and L2 VPN	VMware Distributed Switch version 6.0
			VMware Distributed Switch version 6.5 (requires upgrade of distributed switches in VMware Cloud on AWS SDDC)
	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 swithc, or Cisco Nexus 1000v
bulk migration	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
cold migration	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

This chapter includes the following topics:

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.

vMotion Requirements for SDDCs With NSX-T

Requirement	Description
Networking speed and latency	Migration with vMotion requires sustained minimum bandwidth of 250 Mbps between source and destination vMotion vMkernel interfaces, and a maximum latency of 100 ms round trip between source and destination.
On-premises vSphere version	One of: ■ vSphere 6.7u1 ■ vSphere 6.5P03 or higher.
On-premises DVS version	6.0 higher.
On-premises NSX version	any
IPsec VPN	Configure an IPsec VPN for the management gateway. See "Configuring VPNs and Gateways" in *Getting Started With VMware Cloud on AWS*.
Direct Connect	Direct Connect over a private virtual interface between your on-premise datacenter and your VMware Cloud on AWS SDDC is required for migration with vMotion. See Using AWS Direct Connect with VMware Cloud on AWS.
Hybrid Linked Mode	Hybrid Linked Mode is required to initiate migration from the vSphere Client. It is not required to initiate migration using the API or PowerCLI. See "Hybrid Linked Mode" in *Managing the VMware Cloud on AWS Data Center*.
L2 VPN	Configure a Layer 2 VPN to extend virtual machine networks between your on-premises data center and cloud SDDC. Routed networks are not supported. See *VMware Cloud on AWS Networking and Security*.
VMware Cloud on AWS firewall rules	Ensure that you have created the necessary firewall rules as described in Required Firewall Rules for vMotion.

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

Note 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.

vMotion Requirements for SDDCs with NSX for vSphere

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	vSphere 6.5 patch d and later
	vSphere 6.0 update 3 and later If your on-premises vCenter Server is part of an MxN Enhanced Linked Mode configuration, nodes in your on-premises data center must be within the same site to minimize latency.
	vSphere 5.1 or 5.5 vMotion from on-premises data centers running vSphere 5.1 or 5.5 can be supported only by using the VMware Hybrid Cloud Extension. See https://hcx.vmware.com/content/docs/vmware-hcx-enterprise-install-guide.pdf for more information.
On-premises virtual switch configuration	Standard switches If you use standard switches for virtual machine networking, you can migrate virtual machines to your cloud SDDC, but cannot migrate them back to your on-premises data center.

Requirement	Description
	vSphere Distributed Switch 6.0 By default, VMware Cloud on AWS SDDCs are deployed with vSphere Distributed Switch version 6.0. Use vSphere Distributed Switch version 6.0 in your on-premises data center for compatibility.
	vSphere Distributed Switch 6.5 If you must use vSphere Distributed Switch version 6.5 in your on-premises data center, you can request an upgrade of the distributed switches in your cloud SDDC. Contact VMware Support.
IPsec VPN	Configure an IPsec VPN for the management gateway. See "Configuring VPNs and Gateways" in *Getting Started With VMware Cloud on AWS*.
Direct Connect	Direct Connect over a private virtual interface between your on-premise datacenter and your VMware Cloud on AWS SDDC is required for migration with vMotion. See Using AWS Direct Connect with VMware Cloud on AWS.
Hybrid Linked Mode	Hybrid Linked Mode is required to initiate migration from the vSphere Client. It is not required to initiate migration using the API or PowerCLI. See "Hybrid Linked Mode" in *Managing the VMware Cloud on AWS Data Center*.
L2 VPN	Configure a Layer 2 VPN to extend virtual machine networks between your on-premises data center and cloud SDDC. Routed networks are not supported. See *VMware Cloud on AWS Networking and Security*.
VMware Cloud on AWS firewall rules	Ensure that you have created the necessary firewall rules as described in Required Firewall Rules for vMotion.
On-premises firewall rules	Ensure that you have created the necessary firewall rules as described in Required Firewall Rules for vMotion.
Virtual machine hardware and settings	Ensure that these requirements are met for virtual machine hardware. ■ Virtual machine hardware version 9 or later is required for migration with vMotion from the on-premises data center to the cloud SDDC. ■ EVC is not supported in the VMware Cloud on AWS SDDC. ■ VMs that are created in the cloud SDDC or that have been power-cycled after migration to the cloud SDDC can't be migrated back to the on-premises data center with vMotion unless the on-premises EVC baseline is Broadwell. You can relocate these VMs after powering them off, as long as their virtual machine hardware version is compatible with the on-premises data center. ■ Migration of VMs with DRS or HA VM overrides is not supported. For more information on VM overrides, see Customize an Individual Virtual Machine.

Required Firewall Rules for vMotion

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

VMC on AWS Firewall Rules for vMotion

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

Use Cases	Source	Destination	Service
Provide access to vCenter Server from the on premises. Use for general vSphere Client access as well as for monitoring vCenter Server	remote (on-premises) vSphere Client IP address	vCenter	HTTPS
Allow outbound vCenter Server access to on-premises vCenter Server.	vCenter	remote (on-premises) vCenter Server IP address	Any (All Traffic)
Allow SSO vCenter Server	remote (on-premises) Platform Services Controller IP address	vCenter	SSO (TCP 7444)
ESXi NFC traffic	remote (on-premises) ESXi VMkernel networks used for NFC.	ESXi	Provisioning (TCP 902)
Allow outbound ESXi access to on-premises .	ESXi	remote (on-premises) ESXi management VMkernel networks	Any (All Traffic)
Allow vMotion traffic.	remote (on-premises) ESXi vMotion VMkernel networks	ESXi	vMotion (TCP 8000)

On-Premises Firewall Rules for vMotion

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

Rule	Action	Source	Destination	Service	Ports
On-premises to vCenter Server	Allow	remote (on-premises) vSphere Client subnet	VMware Cloud on AWS vCenter Server IP address	HTTPS	443
Remote to ESXi provisioning	Allow	remote (on-premises) subnet		TCP 902	902

Rule	Action	Source	Destination	Service	Ports
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

Hybrid Migration with HCX Checklist

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

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

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

Hybrid Cold Migration Checklist

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

Requirement	Description
On-premises vSphere version	vSphere 6.5 patch d and later
	vSphere 6.0 update 3 and later
On-premises virtual switch configuration	Standard switches, vSphere Distributed Switch 6.0, or vSphere Distributed Switch 6.5
IPsec VPN	Configure an IPsec VPN for the management gateway. See "Configuring VPNs and Gateways" in *Getting Started With VMware Cloud on AWS*.
Hybrid Linked Mode	Hybrid Linked Mode is required to initiate migration from the vSphere Client. It is not required to initiate migration using the API or PowerCLI. See "Hybrid Linked Mode" in *Managing the VMware Cloud on AWS Data Center*.

Requirement	Description
VMware Cloud on AWS and on-premises firewall rules	Ensure that you have created the necessary firewall rules as described in Required Firewall Rules for Cold Migration.
On-premises DNS configuration	Ensure that your on-premises DNS server can correctly resolve the address for the cloud vCenter Server.

Required Firewall Rules for Cold Migration

VMC on AWS Firewall Rules for Cold Migration

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

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

On-Premises Firewall Rules for Cold Migration

Ensure that the following 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 (Required for HLM only)	Allow	CIDR block for cloud SDDC management network	Remote LDAP 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:

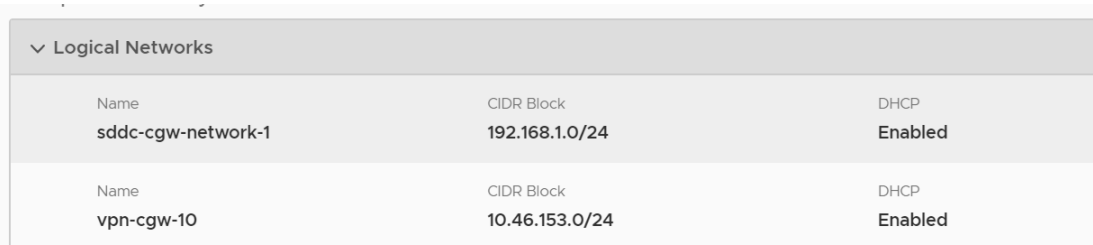
Access an EC2 Instance

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

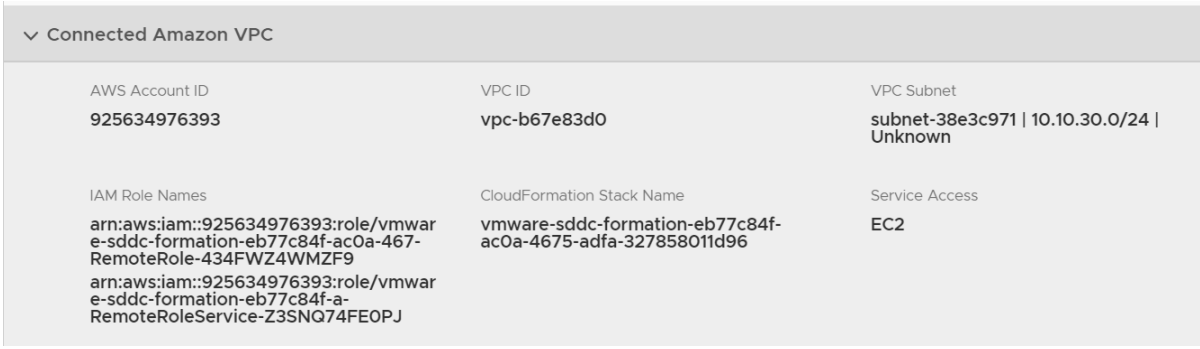
Prerequisites

To complete this task, you need the following information:

- The CIDR block for the logical network or networks that the VMs in your SDDC are using. You can find this in the Logical Networks section of the **Networking** tab in the VMC Console.



- The Amazon VPC and subnet that you connected to your SDDC during SDDC deployment. You can find this in the Connected Amazon VPC section of the **Networking** tab in the VMC Console.



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.
- 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.

2 Configure the security group for the EC2 instance to allow traffic to the logical network associated with the VM in your SDDC.

a Log into your AWS account.

b Select **EC2**.

c Select the EC2 instance that you want to be able to connect to.

d In the instance description, click the instance's security group and click the **Inbound** tab.

e Click **Edit**.

f Click **Add Rule**.

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

h In the **Source** text box, enter the CIDR block for the logical network that the VMs in your SDDC are attached to.

i Repeat steps Step 2f through Step 2h for each logical network that you want to be able to connect to.

j Click **Save**.

3 Configure compute gateway firewall rules to allow traffic to and from the connected Amazon VPC.

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

   b **View Details**

   c **Network**

   d Add two compute gateway firewall rules to allow traffic between the compute gateway and the Amazon VPC for the appropriate service.

   For the first firewall rule, use **All Linked AWS VPC** as the source, and the logical network for the VMs in your SDDC as the destination. For the second firewall rule, use the logical network for the VMs in your SDDC as the source, and **All Linked AWS VPC** as the destination.

Access an S3 Bucket Using an S3 Endpoint

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

Procedure

1 Create an S3 endpoint.

   a Log in to your AWS account.

   b Click **VPC** and then click **Endpoints**.

   c Click **Create Endpoint**.

   d In the **VPC** drop down, select the VPC that is connected to your VMware Cloud on AWS account.

   e In the **Service** drop down, select the S3 service.

   f Click **Next Step**.

   g Select the route table for the subnet you selected when you deployed your SDDC.

   h Click **Create Endpoint**.

2 Configure the security group for your connected Amazon VPC to allow traffic to the logical network associated with the VM in your SDDC.

   a Select **VPC**.

   b Click **Security Groups**

   c Click your connected Amazon VPC's security group and click the **Inbound** tab.

   d Click **Edit**.

   e Click **Add Rule**.

   f In the **Type** dropdown menu, select **HTTPS**.

   g In the **Source** text box, enter the CIDR block for the logical network that the VMs in your SDDC are attached to.

h Repeat steps Step 2f through Step 2h for each logical network that you want to be able to connect to.

i 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 **View Details**

c **Network**

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

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

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

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

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

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

Access an S3 Bucket Using the Internet Gateway

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

Procedure

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

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

2 Enable access to S3 through the internet gateway.

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

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

b **View Details**

c **Network**

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

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

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

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

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

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

Use AWS CloudFormation to Create an SDDC

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

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

Procedure

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

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

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

4 Upload the template you retrieved in Step 2.

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

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

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

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

Table 6-1. Environment Variables for Cloud Formation SDDC Stack

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

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

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

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

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.

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

This chapter includes the following topics:

Prepare Your SDDC to Work with vRealize Products

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

Procedure

1. If you haven't done so already, deploy your SDDC on VMware Cloud on AWS and make note of the management CIDR.
2. Configure an IPsec VPN for the management gateway.

   See "Configuring VPNs and Gateways" in *VMware Cloud on AWS Networking and Security*.

   Important To work with vRealize Products, the vCenter Server FQDN must resolve to a private IP address on the management network. Under **Management Gateway**, click **DNS.** and select **Private IP resolvable from VPN**.
3. Configure a logical network and compute VPN.

   See "Configuring Compute Gateway Networking" in *VMware Cloud on AWS Networking and Security*.
4. Configure additional firewall rules if necessary.

   The firewall rule accelerator creates all these rules for you. If you choose to create firewall rules manually, be sure to include the following rules on the Management Gateway and Compute Gateway firewalls.

Table 7-1. Additional Management Gateway Firewall Rules

Name	Source	Destination	Service
vCenter	CIDR block of on-premises data center	vCenter	Any (All Traffic)
vCenter Ping	Any	vCenter	ICMP (All ICMP)
On Premises to ESXi Ping	CIDR block of on-premises data center	ESXi Management Only	ICMP (All ICMP)
On Premises to ESXi Remote Console	CIDR block of on-premises data center	ESXi Management Only	Remote Console (TCP 903)
On Premises to ESXi Provisioning	CIDR block of on-premises data center	ESXi Management Only	Provisioning (TCP 902)

Note The MGW VPN Wizard creates these firewall rules for you. If you used the Wizard to create your management VPN and gateway, you don't need to add any more management gateway firewall rules to get VMware Cloud on AWS to work with vRealize Products.

Table 7-2. Additional Compute Gateway Firewall Rules

Name	Source	Destination	Service	Ports
On-Premises to SDDC VM	CIDR block of on-premises data center	CIDR block of SDDC logical network	Any (All Traffic)	Any
SDDC VM to On-Premises	CIDR block of SDDC logical network	CIDR block of on-premises data center	Any (All Traffic)	Any

Connect vRealize Automation to Your SDDC

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

Prerequisites

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

Procedure

1. In vRealize Automation, select **Infrastructure > Endpoints**.
2. Select **New > Virtual > vSphere (vCenter)**.
3. Specify the vCenter Server URL in the format **`https://fqdn/sdk`**.
4. Specify the cloud admin credentials.
5. (Optional) If you are using vRealize Automation 7.3 or 7.4, click **Test Connection** and **Accept Certificate**.

6 Create a Fabric Group.

   a Add the cloud admin as the fabric administrator.

   b Add the default SDDC cluster Cluster-1 to the Compute Resources.

   For more information on creating a Fabric Group, see Create a Fabric Group.

7 Create reservations for the components that the cloud admin has access to.

Option	Description
Resource Pool	Compute-ResourcePool
Datastore	WorkloadDatastore
VM & Template Folder	Workloads
Network	Use the logical network that you created as part of the prerequisites

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

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

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

9 Create a Blueprint.

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

What to do next

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

Enable vRealize Automation Access to the Remote Console

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

Procedure

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

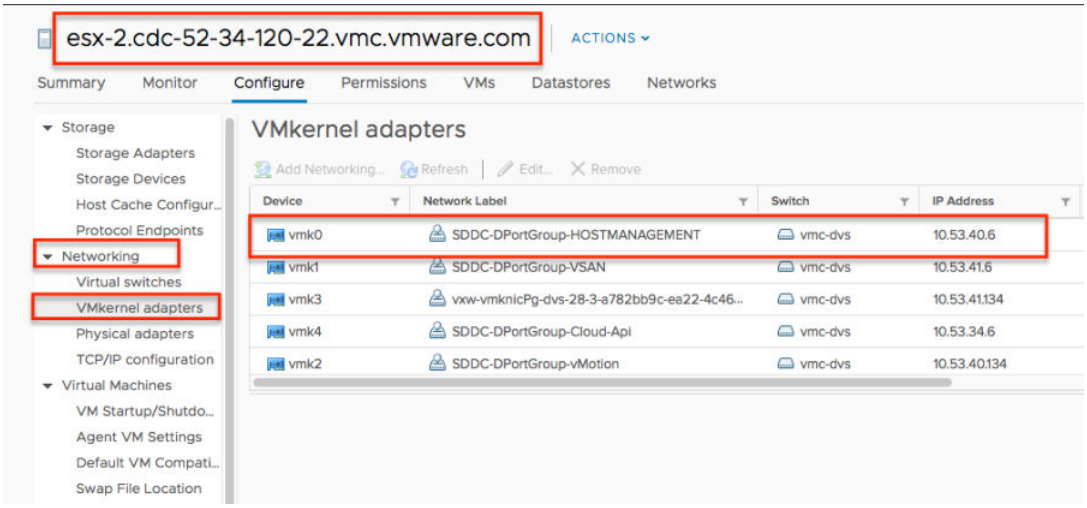
   a Log in to the vSphere Client for your SDDC.

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

   c Click the **Configure** tab.

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

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



2 Connect to the vRealize Automation appliance using ssh.

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

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

VMC Console Settings

8

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

Set Language for the VMC Console

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

The VMC Console UI supports English, German, and Japanese.

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

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

Procedure

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

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 Help and Support

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

Procedure

1. Before you contact VMware for support, have the support information for your SDDC ready.
   a. Log in to the VMC Console at https://vmc.vmware.com.
   b. Click **View Details** on the SDDC card.
   c. Click **Support** to view the support information.

2 Select a method for getting help or support.

Option	Description
Chat	Click the help icon  and click **Chat with VMware Support**. Type your message in the chat window. You can include images by dragging them into the chat window.
File a support request	Click the help icon  and click **Support Requests**. You are taken to the Cloud services console. Click **Support Center** to file a support request.
View contextual help	Click the help icon  . Browse the topics under the **Help Topics** heading, or type a question or keywords in the **Type your question here** field to search the available topics.
Ask a question in the forums	Click the help icon  and click **Ask the Community**. You can post questions and discuss the product with other users in these forums.

View and Subscribe to the Service Status Page

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

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

Procedure

1 Go to https://status.vmware-services.io to view the service status dashboard and incidents.

2 Click **Subscribe to Updates**.

3 Select the notification methods you prefer to subscribe to for the service.

Unable to Connect to VMware Cloud on AWS

Problem

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

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

Cause

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

Solution

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

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

Unable to Connect to vCenter Server

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

Problem

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

Cause

By default, the management gateway firewall is set to deny all traffic between the internet and vCenter Server. If you used the Firewall Rule Accelerator to create firewall rules for your Management Gateway, or used the MGW VPN wizard to create the management VPN and gateway, the required firewall rules should be created automatically. If you created your management network and gateway manually, be sure 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. Use for general vSphere Client access as well as for monitoring vCenter Server	HTTPS	public IP address	vCenter
Provide access to vCenter Server over VPN tunnel. Required for Management Gateway VPN, Hybrid Linked Mode, Content Library.	HTTPS	IP address or CIDR block from on-premises data center	vCenter
Provide access from cloud vCenter Server to on-premises services such as Active Directory, Platform Services Controller, and Content Library.	Any	vCenter	IP address or CIDR block from on-premises data center.

Unable to Select Subnet When Creating SDDC

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

Problem

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

Cause

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

Solution

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

Unable to Copy Changed Password Into vCenter Login Page

Problem

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

Cause

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

Solution

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

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

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

Problem

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

Cause

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

Solution

1 Configure the VMware Cloud on AWS side of the VPN tunnel to allow DNS requests over the VPN.

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

   b Navigate to the Networking tab of your SDDC.

   c Under **Compute Gateway** and click **VPN**.

   d Select **Actions > Edit**.

   e Under **Local Network**, select **cgw-dns-network**.

   f Click **Save**.

2 Configure the on-premises side of the tunnel of connect to *local_gateway_ip*/32 in addition to the Local Gateway IP address. This allows DNS requests to be routed over the VPN.