VMware Cloud on AWS Getting Started

16 November 2018
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

Getting Started With VMware Cloud on AWS

This guide provides information about creating cloud software-defined data centers (SDDCs) using VMware Cloud on AWS, configuring basic networking and other parameters for your SDDC, and connecting an SDDC to your on-premises data center.

After you have deployed and configured your SDDC, see the VMware Cloud on AWS *Networking and Security Guide* guide and the *Operations Guide* for information about advanced features that enable you to create a secure hybrid cloud with extended networking, single sign-on, and integration with other VMware and Amazon tools.

Intended Audience

This information is intended for anyone who wants to use VMware Cloud on AWS to create an SDDC that has the basic features required to run workloads in the cloud and can serve as a starting point for your exploration of additional features and capabilities. The information is written for readers who have used vSphere in an on-premises environment and are familiar with virtualization concepts. In-depth knowledge of vSphere or Amazon Web Services is not required.

Important Before you begin working through the procedures in this guide, download and read Preparing for VMware Cloud on AWS, a planning guide that covers critical preparation steps and associated resources that can help you configure deploy your new SDDC environment quickly and correctly.

Account Creation and Management

1

VMware Cloud on AWS accounts are based on an Organization, which corresponds to a group or line of business subscribed to VMware Cloud on AWS services.

Each Organization has one or more Organization Owners, who have access to all the resources and services of the Organization and can invite additional users to the account. By default, these additional users are Organization Users, who can create, manage, and access SDDCs belonging to the Organization, but cannot invite new users.

Note The VMware Cloud on AWS Organizations that you create or are a member of have no relationship to AWS Organizations.

Both types of accounts are linked to a My VMware account.

This chapter includes the following topics:

Creating an Account

You receive an email invitation containing a link that you can use to sign up for a VMware Cloud on AWS account. This link can be used only once.

When you sign up for the service, an Organization is created with an Organization ID and Organization Name. You are designated as the Organization Owner and can invite other users in your organization to use the service.

Create an Organization Owner Account with a My VMware Account

If you have a My VMware account, you can use it to create an Organization Owner account after you receive the invitation email.

If you don't have a My VMware account, you are prompted to create one during account creation.

Procedure

1. Click the activation link in your invitation email.

   You are taken to the sign up page.
2. Enter the email address associated with your My VMware account, and click **Next**.
3. Enter the password associated with your My VMware account, and click **Log In**.
4. Select the check box to accept the service terms and conditions and click **Next**

   You see a page acknowledging successful completion of your account creation. You are directed to a login page.
5. Log in with your My VMware credentials.
6. If you are not automatically redirected to the VMC Console, go to https://vmc.vmware.com and log in.

Create an Organization Owner Account Without a My VMware Account

If you do not already have a valid My VMware account, you can create one as part of the sign-up process.

Procedure

1. Click the activation link in your invitation email.

   You are taken to the sign up page.
2. Click **Create an Account**.
3. Fill in the required information and select the terms of service check boxes.

   Registration fails if:

   - You don't provide a valid address.
   - You don't enter the full name of your state. For example, if you enter **`CA`** instead of **`California`**, registration fails.
4. Click **Sign Up**.

   You receive an activation email within the next 10 minutes.
5. Open the email and click the activation link.

   The link is unique and can be used only once.
6. On the Welcome page, enter and confirm a password, and click **Save**.

   You are directed to a login page where you can sign in with your credentials.
7. Log in with your My VMware credentials.
8. If you are not automatically redirected to the VMC Console, go to https://vmc.vmware.com and log in.

Invite a New User

As an Organization Owner, you can invite additional users to your Organization.

Organization Members can't invite users to an organization.

Prerequisites

You must be an Organization Owner to invite additional users to your Organization.

Procedure

1. Log in to the VMC Console at https://vmc.vmware.com.
2. Click the services icon () at the top right of the window, and select **Identity and Access Management**.

   You see a list of all the users currently in your organization.
3. Click **Add Users**.
4. Enter an email address for each user you want to add, separated by a comma, space, or a new line.
5. Select the role to assign.
   - Organization Owner.
   - Organization Member.
6. Click **Add**.

Invitation emails are sent to each of the users you invited. They can use these emails to active their accounts.

Accept an Account Invitation

After an Organization Owner has invited you to their organization in VMware Cloud on AWS, you can accept the invitation to create your account and gain access to the service.

Procedure

1. In the invitation email you received, click **VIEW SERVICES**.

   The registration page opens in your Web browser.
2. Register your account.

Option	Description
If you already have a My VMware account associated with your email	Enter your email address and My VMware password, and click **Log In**.
If you do not already have a My VMware account associated with your email	a Enter your First Name, Last Name, and Password. b Select the check box to accept the VMware Terms of Use Agreement. c Click **Save**.

3 If you are not automatically redirected to the VMC Console, go to https://vmc.vmware.com and log in.

Create a Subscription 2

Subscriptions allow you to save money by committing to buy a certain amount of capacity for a defined period.

A subscription is not required to use VMware Cloud on AWS. Any usage of the service not covered by a subscription is charged the on-demand rate.

Prerequisites

You must have funds associated with your My VMware account that you can use to pay for the subscription.

Procedure

1. Log in to the VMC Console at https://vmc.vmware.com.
2. Click **Subscriptions**.
3. Click **Create Subscription**.
   a. Select the region in which the subscription applies.
   b. Select the number of hosts you want as part of the subscription.

      The total number of subscribed hosts cannot be more than the maximum allowed for your organization.
4. Click **NEXT** to choose subscription terms.

   The VMC Console retrieves and displays the currently available subscription terms. Select a term and click **NEXT** to confirm payment.
5. Review the summary and click **PLACE ORDER**.

You will receive a notification email indicating that your subscription order has been received. After the order has been processed, you will receive a second email notification letting you know either that your subscription is active, or that the subscription process failed. If the subscription failed, contact VMware support for assistance.

Deploying and Managing a Software-Defined Data Center 3

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.

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.

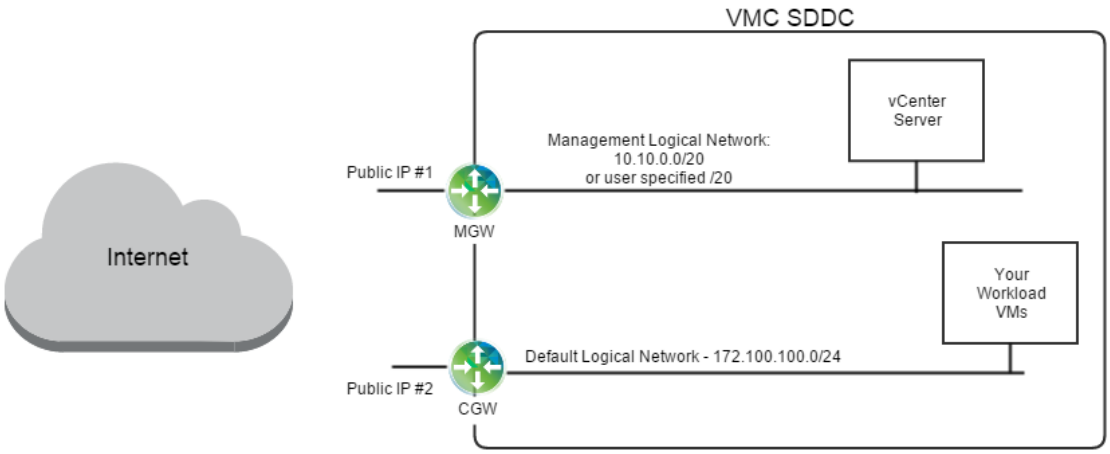
The following restrictions apply to stretched clusters:

- 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 3-1. 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.

This chapter includes the following topics:

Deploying a Single Host SDDC Starter Configuration

VMware Cloud on AWS allows you to deploy a starter configuration containing a single host.

The Single Host SDDC starter configuration allows you to kickstart your VMware Cloud on AWS hybrid cloud experience with a 30-day time-bound single host configuration. You can purchase this configuration on an hourly on-demand basis using a credit card or VMware credit funds.

The Single Host SDDC starter configuration is limited to a 30-day lifespan. You can scale up to the minimum 3-host purchase at any point before the 30-day period ends without losing any of your 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.

The Single Host SDDC starter configuration is appropriate for test and development or proof of concept use cases. Do not run production workloads on a single host SDDC. You can start to prove the value of VMware Cloud on AWS with the single host capabilities including:

- Accelerated on-boarding with expert support.
- Migration between on-premises and VMware Cloud on AWS using VMware Hybrid Cloud Extension for large-scale rapid migration, VMware vMotion for live migration, and cold migration.
- Disaster Recovery: Evaluate VMware Site Recovery, the cloud-based DR service optimized for VMware Cloud on AWS. VMware Site Recovery is purchased separately as an add-on service on a per-VM basis. Do not use the single host configuration for production disaster recovery, because this configuration has not SLA and data is lost in the event of a host failure.
- Hybrid Linked Mode support: Hybrid Linked Mode provides a single logical view of on-premises and VMware Cloud on AWS resources.
- All-Flash vSAN storage: An all-flash vSAN configuration, using flash for both caching and capacity, delivers maximum storage performance.
- Seamless, high-bandwidth, low-latency access to native AWS services such as EC2 and S3.

Single Host SDDCs have the following limitations.

- Features or operations that require more than 1 host running in VMware Cloud on AWS won't work with the Single Host SDDC. These include, but are not limited to, High Availability (HA), multiple clusters, stretched clusters across multiple availability zones, migration with vMotion between VMware Cloud on AWS environments, and Distributed Resource Scheduler (DRS).
- The Single Host SDDC has no SLA.
- If the single host fails, the data in your SDDC will be lost.

- Single Host SDDCs are not upgraded or patched.
- You can only provision one Single Host SDDC at a time.

Request Access and Create an Account

Start by requesting access to a Single Host Starter Configuration SDDC. When your access is approved, activate and create your account.

Prerequisites

Important Ensure that:

- If you plan to use an existing My VMware profile, it has a US-based address associated with it.
- The credit card you plan to use has a U.S. based address.
- The email address you plan to use to register is a corporate email account and not from a public email provider such as gmail.com, icloud.com, or others.

For more information on how to update your My VMware profile, see https://kb.vmware.com/s/article/2086266.

Procedure

1. Go to https://cloud.vmware.com/vmc-aws/single-host-access, fill in the required information, and click **Request**.

   If capacity is not currently available, you receive an email indicating that you are on the waiting list. This message includes links to resources that you can use to plan your deployment.

   When capacity is available, you receive an email notifying you that you can activate your subscription.
2. Create your organization owner account.
   - If you already have a My VMware account, follow the steps in Create an Organization Owner Account with a My VMware Account.
   - If you don't have a My VMware account, follow the steps in Create an Organization Owner Account Without a My VMware Account.
3. Name your organization and agree to the Terms of Service.
4. Enter credit card information for your default method of payment.

   Only US-based credit cards are accepted currently.
5. Click **Add Card**.

What to do next

Ensure that you have met the prerequisites and then follow the steps in Chapter 3 Deploying and Managing a Software-Defined Data Center. Select **1** as the number of hosts in the SDDC.

Scale Up a Single Host SDDC Starter Configuration

Single Host SDDC starter configurations have a limited lifespan before they expire. To keep your workloads and data beyond the expiration date, scale up your SDDC to a full production SDDC.

Scaling up a Single Host SDDC is not reversible. After you scale up to an SDDC with four or more hosts, you will not be able to remove hosts from the SDDC.

The card for a Single Host SDDC displays a banner showing the number of days left before expiration.

Procedure

1. On the SDDC banner, click **Scale Up**.
2. Review the settings for the scaled up SDDC and click **Scale Up Now**.

Your Single Host SDDC starter configuration is scaled up to a full production SDDC that no longer has an expiration date.

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 a multiple host SDDC.
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 6 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. **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.

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. Consider the following when you specify this address range:

- 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, no default compute gateway logical network is created during deployment and you will have to create one manually after the SDDC is deployed.
- 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 addresses you choose must be different from the ones in your on-premises data center, to avoid IP address conflicts.
- CIDR blocks of size 16, 20, or 23 are supported. For CIDR blocks of size 20 or 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. For CIDR blocks of size 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.

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

Note CIDR blocks 10.0.0.0/15, 172.17.0.0/16, 172.18.0.0/16, and 172.31.0.0/16 are reserved.

6 Click **DEPLOY SDDC** to create the SDDC.

The SDDC takes some time to deploy.

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.

View SDDC Information and Get Support

You can view SDDC information from the VMC Console, and you can get support. For fast resolution of your problem, it's important that you provide details about your environment.

See Chapter 7 Get Help and Support for additional details on getting help and support.

Procedure

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

2 Click **View Details** and select a tab.

Tab	Description
Summary	Displays usage information. This tab does not always update immediately.
Network	Allows you to view and change networking for your SDDC. See Chapter 4 Use the Configure MGW VPN Wizard to Configure a Management VPN and Gateway.
Connection Info	Use this tab as follows: ■ To go to the vSphere Client, click the corresponding link. ■ When you log in to vCenter Server, click the Copy icons next to Username and Password to copy that information to the clipboard and paste it into the login screen.
Support	You use the information in this tab when working with VMware Technical Support. a Click the chat icon  in the bottom right corner. b Give the VMware Cloud on AWS staff the Org ID, SDDC ID, or other information as needed.

Use the Configure MGW VPN Wizard to Configure a Management VPN and Gateway

4

A new SDDC includes a logical network (the management network) and an NSX Edge gateway that controls access to the network. To provide secure communications between this network and your on-premises management network, use the Configure MGW VPN wizard to create virtual private networks (VPNs) in each location, and configure the management gateway to connect them.

The wizard guides you through the steps to create a VPN in the SDDC, configure the management gateway with firewall rules, and specify DNS server addresses for the management network. Your networking team can configure the on-premises end of the management VPN using information you download from the SDDC, then connect it to the SDDC through the management gateway and test network connectivity

Note In addition to creating a management VPN, you can also create a compute VPN and an AWS Direct Connect connection between your on-premises data center and AWS services. For information about how to create these connections, see the *Networking and Security Guide*.

1 Create a Management VPN in your SDDC

   To create the management VPN, configure an IPsec VPN in the SDDC and another one in your on-premises datacenter. The management gateway connects these two VPNs and provides a common set of firewall rules and DNS services.

2 Create an On-Premises IPsec VPN

   Configuration of the gateway device in your on-premises data center might need to be performed by a member of your networking team. Consult the documentation for your gateway or firewall device to learn how to configure it to match the VPN settings you've configured.

3 Create Management Network Firewall Rules

   Firewall rules control the types of network traffic that can be sent and received through a network gateway. The Configure MGW VPN wizard includes a step that creates the firewall rules typically needed by the SDDC side of the management network. You must take an additional step to create matching firewall rules in your on-premises management gateway.

4 Configure Management Network Private DNS

   Specify the addresses of your private DNS servers so that the management gateway, ESXi hosts, and management VMs resolve fully-qualified domain names (FQDNs) to IP addresses on the management network.

5 Test Managment VPN Connectivity

After you have completed configuration of the management VPN, the Configure MGW VPN wizard runs a series of tests that validate management network connectivity for common use cases.

Create a Management VPN in your SDDC

To create the management VPN, configure an IPsec VPN in the SDDC and another one in your on-premises datacenter. The management gateway connects these two VPNs and provides a common set of firewall rules and DNS services.

Procedure

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

2 On Network tab of your SDDC, click **ACTIONS > Configure Management Gateway**.

3 Complete the Management Gateway VPN configuration.

Parameter	Description
VPN Name	Enter a name for the VPN.
Remote Gateway Public IP	Enter the IP address of your on-premises gateway.
Remote Gateway Private IP	If your on-premises gateway is behind NAT, provide the private IP address of the gateway.
Remote Networks	Enter the address of your on-premises management network.
Local Gateway IP	Displays the public IP address of the management gateway. This is not an editable field.
Local Network	Displays the CIDR block of the management subnet for the management gateway. This is not an editable field.
Encryption	Select **AES-256**.
Perfect Forward Secrecy	Select **Enabled**
Diffie Hellman	Select a Diffie Hellman group. Ensure that you use a group that your on-premises VPN gateway supports.
Pre-Shared Key	Enter a pre-shared key. The key is a string with a maximum length of 128 characters that is used by the two ends of the VPN tunnel to authenticate with each other.

Click **SAVE** to save this configuration and create the VPN.

After the system creates the VPN in the SDDC, you can click ACTIONS to Edit or Disable the VPN. When the VPN has a status of **Connected**, you can click **VPN Status Detail** to view VPN tunnel status and statistics.

4 Download the SDDC management VPN configuration details.

Under **Remote VPN Config File**, click **Download** to download a configuration file that you can use when you configure the on-premises side of this VPN.

What to do next

Configure the on-premises side of the management VPN.

Create an On-Premises IPsec VPN

Configuration of the gateway device in your on-premises data center might need to be performed by a member of your networking team. Consult the documentation for your gateway or firewall device to learn how to configure it to match the VPN settings you've configured.

Prerequisites

Configuring an on-premises VPN requires the following:

- An on-premises router or firewall capable of terminating an IPsec VPN, such as Cisco ISR, Cisco ASA, CheckPoint Firewall, Juniper SRX, NSX Edge, or any other device capable of IPsec tunneling.
- If your on-premises gateway is behind another firewall, you must configure that firewall to forward IPsec VPN protocol traffic:
  - Open UDP port 500 to allow Internet Security Association and Key Management Protocol (ISAKMP) traffic to be forwarded through the firewall.
  - Set IP protocol ID 50 to allow IPsec Encapsulating Security Protocol (ESP) traffic to be forwarded through the firewall.
  - Set IP protocol ID 51 to allow Authentication Header (AH) traffic to be forwarded through the firewall.

Procedure

1. Navigate to the Network tab of your SDDC.
2. Under **Management Gateway**, click **IPsec VPNs** and open the VPN that you created in Create a Management VPN in your SDDC.
3. Download the SDDC management VPN configuration details.

   Under **Remote VPN Config File**, click **Download** to download a configuration file listing the configuration parameters for the SDDC side of the management VPN.
4. Configure the on-premises management VPN.

   Use the information in the file you downloaded in Step 3. See Example: VPN Configuration File for an example of the information that this file contains.

Example: VPN Configuration File

```
# Configuration for IPsec VPN connection
#
# Peer NSX Edge and IPSec Site configuration details.
#
# IPsec site Id         : ipsecsite-17
# IPsec site name       : VPN1
# IPsec site description:
# IPsec site enabled    : true
# IPsec site vpn type   : Policy based VPN
# NSX Edge Id           : edge-1
```

```
# Feature version       : 45
# Time stamp            : 040618_182347GMT

#
# Internet Key Exchange Configuration
# Phase 1
# Configure the IKE SA as outlined below
IKE version                  : ikev1
Connection initiation mode   : initiator
Authentication method        : psk
Pre shared key               : 123456
Authentication algorithm     : sha1
Encryption algorithm         : aes256
SA life time                 : 28800 seconds
Phase 1 negotiation mode     : main
DH group                     : DH14

# IPsec_configuration
# Phase 2
# Configure the IPsec SA as outlined below
Protocol                        : ESP
Authentication algorithm        : sha1
Sa life time                    : 3600 seconds
Encryption algorithm            : aes256
Encapsulation mode              : Tunnel mode
Enable perfect forward secrecy  : true
Perfect forward secrecy DH group: DH14

# Peer configuration
Peer address    : 34.218.1.5 # Peer gateway public IP.
Peer id         : 34.218.1.5
Peer subnets    : [ 10.2.0.0/16 ]

# IPsec Dead Peer Detection (DPD) settings
DPD enabled     : true
DPD interval    : 30 seconds
DPD timeout     : 150 seconds

# Local configuration
Local address   : 66.70.190.7 # Local gateway public IP.
Local id        : 66.70.190.7
Local subnets   : [ 10.101.101.0/24 ]
```

What to do next

Configure firewall rules to manage traffic between the on-premises and SDDC ends of the management VPN. By default, your new management gateway firewall rules deny all traffic through the firewall. The firewall rules accelerator provides a set of predefined firewall rules that are likely to be appropriate for most new installations.

Create Management Network Firewall Rules

Firewall rules control the types of network traffic that can be sent and received through a network gateway. The Configure MGW VPN wizard includes a step that creates the firewall rules typically needed by the SDDC side of the management network. You must take an additional step to create matching firewall rules in your on-premises management gateway.

By default, the management gateway is created with firewall rules that block all traffic. After you set up both sides of the management VPN, run the **MGW Firewall Rules** step of the Configure MGW VPN wizard, then run the Firewall Rules Accelerator to quickly set up remote firewall rules in your on-premises gateway. Setting these rules is a prerequisite for using Hybrid Linked Mode, performing workload migrations, and many other tasks.

Procedure

1. In the Configure MGW VPN wizard, run **MGW Firewall Rules**.

   After the MGW firewall rules have been created, click **NEXT STEP** to configure remote firewall rules.
2. Navigate to the Network tab of your SDDC.
3. Under **Management Gateway**, click **IPsec VPNs**.
4. Click **Firewall Rule Accelerator**.

   The Firewall Rules Accelerator opens.
5. From the **VPN (Remote Network)** drop-down menu, select the remote (on-premises) network that you want to create firewall rules for.

   The Firewall Rules Accelerator displays the rules that will be created.
6. Click **Create Firewall Rules** to create these rules.

   Review the list of rules and select **I have created the necessary firewall rules** and click NEXT STEP.

Configure Management Network Private DNS

Specify the addresses of your private DNS servers so that the management gateway, ESXi hosts, and management VMs resolve fully-qualified domain names (FQDNs) to IP addresses on the management network.

Prerequisites

Use the Configure MGW VPN wizard to create the management network, gateways, and firewall rules.

Procedure

1. Specify the DNS server addresses.

   Click **Edit** and enter the IP addresses for **DNS Server 1** and, optionally, **DNS Server 2**.

2 Choose a scope for DNS name resolution.

   By default, the management gateway DNS is configured to resolve names to addresses on the public Internet (**Public IP resolvable from Internet**). To limit the scope to addresses on the management VPN. Select **Private IP resolvable from VPN**. This configuration change applies to both **DNS Server 1** and **DNS Server 2**.

3 Click **NEXT STEP** to save the management gateway DNS configuration and test management network connectivity.

Test Managment VPN Connectivity

After you have completed configuration of the management VPN, the Configure MGW VPN wizard runs a series of tests that validate management network connectivity for common use cases.

The management VPN connectivity validator includes a number of tests, each of which validates management network connectivity between your on-premises datacenter and your VMware Cloud on AWS SDDC.

Procedure

- Click **RUN ALL TESTS** to run all the tests.

  The wizard runs the tests in order and reports success or failure for each test. You can re-run individual tests or test groups if you need to.

What to do next

For more information about troubleshooting VPN connection issues, see Troubleshooting Virtual Private Networks in the *NSX for vSphere* documentation.

Connect to vCenter Server

5

Click the **OPEN VCENTER** button to open the vSphere client and log in to vCenter.

In addition to the **OPEN VCENTER** button, the **Connection Info** tab for your SDDC provides connection and authentication details for connecting to vCenter Server with the API Explorer and PowerCLI.

Procedure

- Open the **Connection Info** tab and select a method for connecting to vCenter Server.

Option	Description
Connect using the vSphere Client	Click the link under **vSphere Client (HTML5)**. This connection method is identical to the **OPEN VCENTER** button.
Connect to the API Explorer	Click the link under **vCenter Server API Explorer**. .
Connect using PowerCLI	The cmdlet for connecting is shown under **PowerCLI Connect**. Click to copy the cmdlet to the clipboard.

  Default credentials for all connection methods are displayed under **Authentication**. Click to copy a user name or password to the clipboard.

Create Virtual Machines

6

Now that you've created a management network and connected to vCenter Server, you can create virtual machines in your VMware Cloud on AWS SDDC.

VMware Cloud on AWS gives you several ways to create virtual machines in your SDDC. One of the simplest is to use the on-premises vSphere Content Onboarding Assistant to transfer virtual machine templates to your SDDC, then deploy the imported template as a VM. After you create a virtual machine, you can perform configuration tasks such as setting a public IP address or enabling access to a VM Remote Console.

See the *Operations Guide* for more ways to provision your SDDC with VM templates and ISO images that you can use to create workload VMs. See *Managing Virtual Machines in VMware Cloud on AWS* for information about configuring and managing workload VMs.

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.

Parameter	Description
`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.

Deploy a Virtual Machine from a .vmtx Template

You can deploy a VM from a `.vmtx` template.

Procedure

1. From the vSphere Client VMs and Templates view, right click the template and select **New VM from This Template**.
2. Proceed through the Deploy From Template wizard, using the following settings.
   a. For the VM folder, select **Workloads**, **Templates**, or another folder that you have write permissions on.
   b. For the compute resource, select **Compute-ResourcePool**.
   c. For the datastore, select **workloadDatastore**.

Assign a Public IP Address to a VM

You can assign a public IP address to a VM to make it available. This procedure includes requesting a public IP address, adding a NAT rule, and adding a firewall rule.

Procedure

1. Log in to the VMC Console at https://vmc.vmware.com.
2. Click **View Details** on the SDDC card.
3. Click **Network**.
4. Request a public IP address. Under **Compute Gateway**, click **Public IPs**.
   a. Click **Request Public IP**.
   b. Enter any notes that you want to make about the IP address.
   c. Click **Save**.

   After a few moments, the Public IP address is provisioned.
5. Add a NAT rule.
   a. Under **Compute Gateway**, click **NAT**.
   b. Click **Add NAT Rule**.
   c. Enter the NAT parameters.

Option	Description
Description	Enter a description for the NAT rule.
Public IP	Select the Public IP address you just provisioned for the VM.
Service	Select HTTPS (TCP 443)
Public Ports	443
Internal IP	Leave the default.
Internal Ports	Leave the default.

6 Set a firewall rule for the VM with the new public IP.

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

b Click **Add Rule**.

c Enter the rule parameters.

Option	Description
Rule Name	Give the rule a descriptive name.
Action	Select **Allow**.
Source	Select **Any**.
Destination	Enter the new public IP of your VM.
Service	Select HTTPS (TCP 443)
Ports	443

Enable Access to the Virtual Machine Remote Console

To access the Virtual Machine Remote Console (VMRC) on VMs in your cloud SDDC, ensure that you have configured a management gateway firewall rule that allows access to ESXi (port 903).

Prerequisites

You must create a management VPN before you can use VMRC.

Procedure

- Modify the management gateway firewall rules to allow access to port 903.

  Note Both the MGW VPN Wizard and the Firewall Rules Accelerator create this firewall rule. Skip this step if you have used either of these tools to create firewall rules for the management gateway. To add this rule manually, follow these steps.

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

  b Click **View Details** on the SDDC card.

  c Click **Network**.

  d Under **Management Gateway**, click **Firewall Rules**.

  e Click **Add Rule** and set a rule to enable access to port 903.

Option	Description
Source	IP address or CIDR block, either public or from an on-premises data center connected by a VPN tunnel
Destination	ESXi Management
Service	Remote Console

Get Help and Support

7

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 chat icon  and click **New Conversation**. Type your message in the chat window. You can include images by dragging them into the chat window. Currently, chat is monitored Monday through Friday, 6 a.m. to 6 p.m. PST.
File a support request on My VMware	Click the help icon  and click **My VMware**. You are taken directly to a form for filing 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 **VMware.com Community Forums**. You can post questions and discuss the product with other users in these forums.