VMware Cloud on AWS Getting Started

9 OCT 2017

VMware Cloud on AWS services

vmware®

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

https://docs.vmware.com/

The VMware Web site also provides the latest product updates.

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 Getting Started

The *VMware Cloud on AWS Getting Started* documentation provides information about creating cloud software-defined data centers (SDDCs) using VMware Cloud™ on AWS, configuring networking and other parameters for your SDDC, and connecting an SDDC to your on-premises data center.

To help you get started with VMware Cloud™ on AWS, this information describes how to set up your VMware Cloud™ on AWS account, create an SDDC, and configure it. In addition, this information includes a number of examples and scenarios to help you get the most out of your SDDC.

Intended Audience

This information is intended for anyone who wants to use VMware Cloud™ on AWS to create, configure, and manage an SDDC. The information is written for administrators who have a basic understanding of configuring and managing vSphere in an on-premises environment and are familiar with virtualization concepts. In-depth knowledge of Amazon Web Services is not required.

Updated Information

This *VMware Cloud™ on AWS Getting Started Guide* is updated with each release of the product or when necessary.

This table provides the update history of the *VMware Cloud™ on AWS Getting Started Guide*.

Revision	Description
9 OCT 2017	The topic "Example Management Gateway Firewall Rules," on page 19 has been updated with additional rules. The topic "Hybrid Linked Mode Prerequisites," on page 37 has been added.
3 OCT 2017	The topic "Access an S3 Bucket Using an S3 Endpoint," on page 59 has been updated to correct the instructions for updating the security group policy.
5 SEP 2017	■ The topic "Create a Logical Network," on page 25 has been updated to reflect additional VPN configuration that must be done to allow a logical networking using DHCP to communicate with an on-premises DNS server. ■ The topic "Create a Compute VPN," on page 28 has been updated to reflect additional VPN configuration that must be done to allow a logical networking using DHCP to communicate with an on-premises DNS server. ■ The topic "Set Compute Gateway DNS," on page 32 has been updated to reflect additional VPN configuration that must be done to allow a logical networking using DHCP to communicate with an on-premises DNS server. ■ A new topic, "Compute Workloads Are Unable to Reach an On-Premises DNS Server," on page 74, has been created with information on troubleshooting connections to on-premises DNS servers.
30 AUG 2017	■ The topic "Hybrid Linked Mode Prerequisites," on page 37 has been updated to indicate that UPN format is required for the user name when configuring Active Directory over LDAP
28 AUG 2017	Initial release.

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.

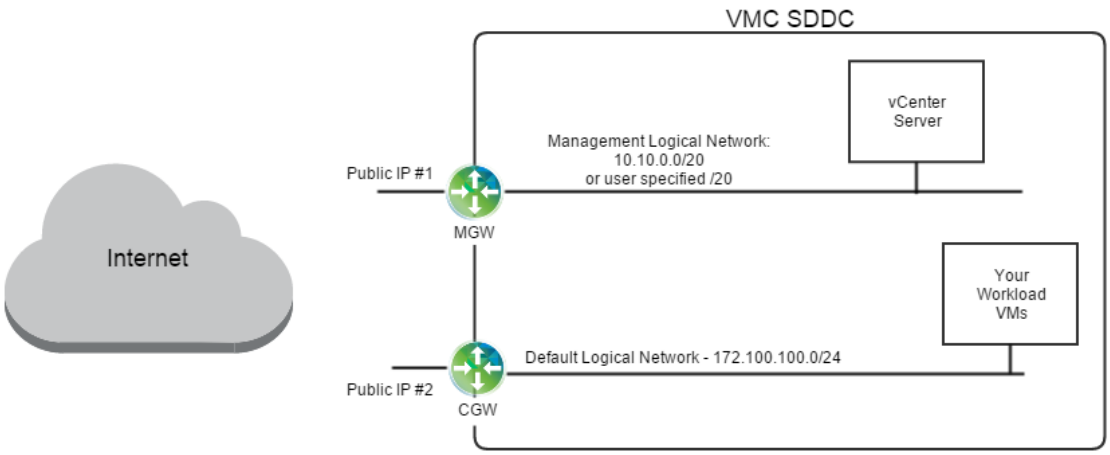
Deploying and Managing a Software-Defined Data Center 2

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.

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.

The default topology deployed is shown below.

Figure 2-1. 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.

This chapter includes the following topics:

Deploy an SDDC from the VMC Console

Deploy an SDDC to host your workloads in the cloud.

During the SDDC creation, you connect your SDDC to an AWS account, and select a VPC and subnet within that account. Using a CloudFormation template, VMware Cloud™ on AWS creates an Elastic Network Interface (ENI), allowing your SDDC and services in the Amazon VPC and subnet in your AWS account to communicate without needing to route traffic through the internet gateway. You can only connect an SDDC to a single Amazon VPC.

Currently, you can deploy an SDDC with a minimum of 4 hosts.

Prerequisites

- Ensure that you have an AWS account before you create an SDDC. The subnet you intend to connect should be in the same region that you plan to use for your SDDC.
- Create an appropriate subnet with at least 64 IP addresses (a /27 CIDR block) in each availability zone (AZ) in your VPC.

Procedure

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

2 Click **Create SDDC**.

3 Connect to your AWS account.

VMware has defined a CloudFormation template to connect your AWS account. This template creates the IAM roles necessary to allow communication between your SDDC and your AWS account.

a Click **Open AWS Console with CloudFormation Template.**

The AWS console opens in a separate browser tab.

b Log in to your AWS account.

c On the **Create Stack** page, click **I acknowledge that AWS CloudFormation might create IAM resources** and click **Create**.

The VMC Console shows the progress of the connection.

4 Configure SDDC properties.

a Enter a name for your SDDC.

b Select the number of hosts in the SDDC.

c Select the AWS region in which to deploy the SDDC.

5 Select a VPC and a subnet in your AWS account to connect to.

Choose a subnet with at least 64 IP addresses in it (a /27 CIDR block). If you don't have a VPC or a subnet that meets the requirements, log in to your AWS account and create them.

6 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 10.0.0.0/16.

You can't change the values specified for the management network after the SDDC has been created. Consider the following when you choose these values:

- Only CIDR blocks of size /16, /20, or /23 are supported.

- 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.
- The maximum number of hosts your SDDC can contain depends on the size of the CIDR block you specify. If the CIDR block is in the form XXX.XXX.XXX.XXX/YY, then the maximum number of hosts the SDDC can contain is (2 ^(27 - YY)) - 3. The table shows the number of hosts based on the value of YY.

YY (Number of bits in the CIDR block prefix)	Number of hosts
23	13
20	125
16	2045

7 Click **Deploy 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 "Get Help and Support," on page 71 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 3, "Configuring Management Gateway Networking," on page 17 and Chapter 4, "Configuring Compute Gateway Networking," on page 25.
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.

Configuring Management Gateway Networking 3

In the VMC Console, you can configure firewall rules, configure an IPsec VPN, and configure DNS for the management gateway.

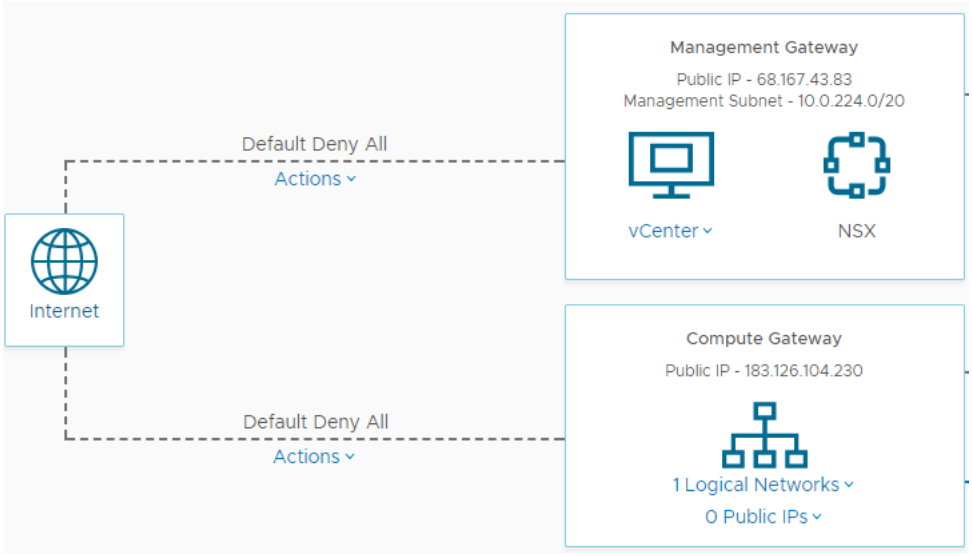
This chapter includes the following topics:

Set Management Gateway Firewall Rules

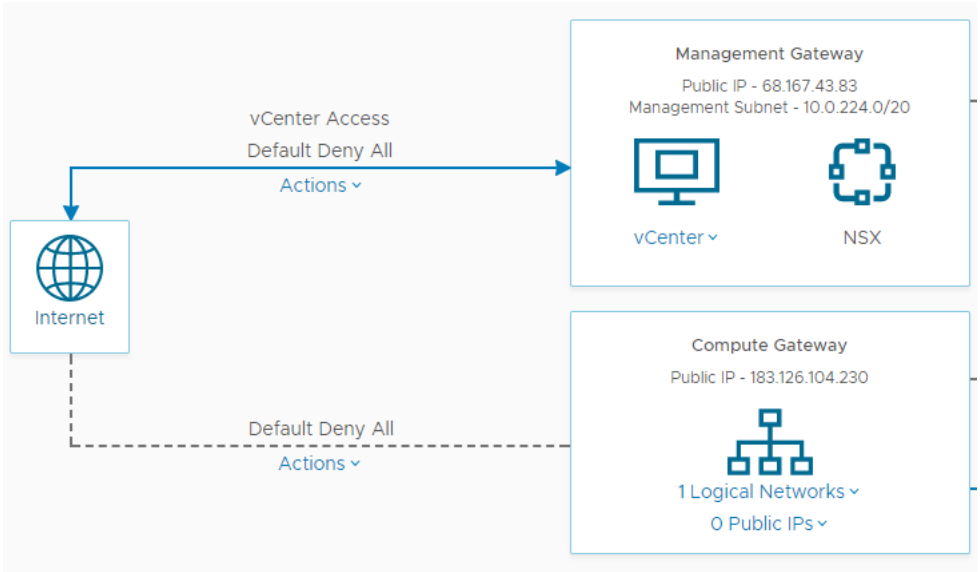
By default, the firewall for the management gateway is set to deny all inbound and outbound traffic. Add additional firewall rules to allow traffic as needed.

NOTE In order to access vCenter Server in your SDDC, you must set a firewall rule to allow traffic to the vCenter Server.

When access to vCenter Server is blocked, the topology diagram on the Network tab shows a dotted line between the internet and the management gateway.



After you have added a firewall rule to allow access to vCenter Server, the diagram shows a solid line between the internet and the management gateway.



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

5 Click **Add Rule**.

6 Enter the rule parameters.

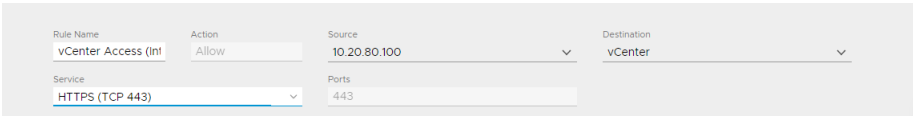
Option	Description
Rule Name	Enter a descriptive name for the rule.
Action	The only action available for management gateway firewall rules is **Allow**.

Option	Description
Source	Enter or select one of the following options for the source: ■ An IP address, IP address range, or **any** to allow traffic from that address or address range ■ **vCenter** to allow traffic from your SDDC's vCenter Server. ■ **ESXi Management Only** to allow traffic from your SDDC's ESXi management.
Destination	Enter or select one of the following options for the destination: ■ An IP address, IP address range, or **any** to allow traffic from that address or address range ■ **vCenter** to allow traffic to your SDDC's vCenter Server. ■ **ESXi Management Only** to allow traffic to your SDDC's ESXi management.
Service	Select one of the following to apply the rule to: ■ Any (All Traffic) ■ ICMP (All ICMP) ■ HTTPS (TCP 443) - applies only to vCenter Server as a destination. ■ SSO (TCP 7444) - applies only to vCenter Server as a destination. ■ Provisioning (TCP 902) - applies only to ESXi Management Only as a destination. ■ Remote Console (TCP 903) applies only to ESXi Management Only as a destination.
Ports	The port that the selected service uses for communication.

7 Use the up and down arrow icons to change the order of the firewall rules.

Firewall rules are applied in order from top to bottom.

The following graphic shows an example firewall rule that allows all traffic to reach vCenter Server from a particular IP address.



See "Example Management Gateway Firewall Rules," on page 19 for more examples of firewall rules for specific use cases.

Example Management Gateway Firewall Rules

Some common firewall rule configurations include opening access to the vSphere Client from the internet, allowing access to vCenter Server through the management VPN tunnel, and allowing remote console access.

The following table shows the Service, Source, and Destination settings for commonly-used firewall rules.

Table 3-1. Commonly-used Firewall Rules

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.
Provisioning operations involving network file copy traffic, such as cold migration, cloning from on-premises VMs, snapshot migration, replication, and so on.	Provisioning	IP address or CIDR block, either public or from an on-premises data center connected by a VPN tunnel	ESXi Management
VMRC remote console access Required for vRealize Automation	Remote Console	IP address or CIDR block, either public or from an on-premises data center connected by a VPN tunnel	ESXi Management
vMotion traffic over VPN	Any	ESXi Management	IP address or CIDR block from on-premises data center
Ping traffic to vCenter Server for network troubleshooting.	ICMP (All ICMP)	IP address or CIDR block, either public or from an on-premises data center connected by a VPN tunnel	vCenter
Ping traffic to ESXi management network for network troubleshooting	ICMP (All ICMP)	IP address or CIDR block, either public or from an on-premises data center connected by a VPN tunnel	ESXi Management

Set Management Gateway DNS

Set a DNS server to allow the management gateway, ESXi hosts, and management VMs behind the DNS to resolve fully-qualified domain names (FQDNs) to IP addresses.

Note In order to use Hybrid Linked Mode and Content Library, configure a DNS server in your on-premises network to ensure that your cloud SDDC can resolve FQDNs within your on-premises infrastructure.

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 Under **Management Gateway**, click **DNS.**

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

Note Both DNS servers must be able to resolve all intended FQDNs. Do not add one public DNS server and one private DNS server. If you do, FQDN resolution becomes unpredictable and Hybrid Linked Mode and other features no longer work.

Recommended On-Premises VPN Settings

You need to use specific settings with your on-premises router to ensure that your VPN connection is created successfully.

Phase 1 Internet Key Exchange (IKE) Settings

Settings marked with an * can't be changed in the VMC Console interface and are required for proper operation of the VPN tunnel. Settings not marked can be edited in the VMC Console. The values in the table are the recommended values. If you choose other values, please ensure that your on-premises gateway is set to match what you have set in the VMC Console.

Attribute	Value
Protocol*	IKEv1
ISAKMP mode*	Main mode (Disable aggressive mode)
ISAKMP/IKE SA lifetime*	28800 seconds
Encryption Algorithm	AES-256
Hashing Algorithm*	SHA-1
Diffie Hellman	DH Group 2
IPsec Mode*	Tunnel
IKE Authentication*	Pre-Shared Key

Phase 2 Settings

Attribute	Value
Encryption Algorithm	AES-256
Hashing Algorithm*	SHA-1
Tunnel Mode*	Encapsulating Security Payload (ESP)
Diffie Hellman	DH Group 2
SA lifetime *	3600 seconds (one hour)
Perfect forward secrecy (PFS)*	Enabled

Mapping NSX Parameters to VMC Console VPN Parameters

The table below matches terms for VPN parameters used in NSX Edge configuration to the terms used in the VMC Console.

NSX Property Name	VMC Console Property Name
Name	VPN Name
Peer ID	On-prem Gateway IP
Peer Endpoint	On-prem Gateway IP
Peer Subnets	On-prem Network
Local ID	Uplink SNAT (not a user-entered value)
Local Endpoint	Uplink IP (not a user-entered value)
Local Subnets	Local Network
Encryption Algorithm	Encryption
Perfect Forward Secrecy	Perfect Forward Secrecy
Authentication	PSK (not a user-entered value)
Diffie Hellman Group	Diffie Hellman
Pre-Shared Key	Pre-Shared Key
Enabled	True (not a user-entered value)

Create a Management VPN

Configure an IPsec VPN between your on-premises data center and cloud SDDC to allow easier and more secure communication between the two.

Creating a management VPN allows you to securely access the vCenter Server system and Content Library deployed in your SDDC. You don't have to set up a VPN connection, but transferring virtual machine templates and disk images into your SDDC in the cloud is easier if you do.

Prerequisites

Configuring a management 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.
- The router or firewall should be configured with cryptography settings as described in "Recommended On-Premises VPN Settings," on page 21.
- If your on-premises gateway is behind another firewall, allow IPsec VPN traffic to pass through the firewall to reach your device by doing the following:
  - 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 Configure the Management Gateway side of the tunnel.

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

b Navigate to the Networking tab of your SDDC.

c Under **Management Gateway**, click **VPN** and then **Add VPN**.

d 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 **DH2**
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.

2 Configure the on-premises side of the tunnel.

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 settings VPN settings you've configured.

When the VPN tunnel is configured, you should be able to verify connectivity in both the VMC Console and by accessing the vCenter Server deployed in your environment with a Web browser.

Change the Management Gateway FQDN Resolution

You can change how the Management Gateway performs FQDN resolution. You can use a private IP, resolvable from the VPN you set up, or to use a public IP from the Internet.

Prerequisites

Set up the VPN for the Management Gateway. See "Create a Management VPN," on page 22.

Procedure

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

2 Navigate to the Networking tab of your SDDC.

3 Under **Management Gateway**, click **DNS** and then **Edit**.

4 Select **Private IP resolvable from VPN** or **Public IP resolvable from Internet** and click **Save**.

Configuring Compute Gateway Networking

4

The compute gateway handles network traffic for your workload VMs.

You can configure firewall rules, inbound NAT, VPN connections, DNS, and public IP addresses for your compute gateway.

This chapter includes the following topics:

Create a Logical Network

Create logical networks to provide network access to workload VMs.

Your SDDC starts with a single default logical network, sddc-cgw-network-1. You can use the HTML5 vSphere Client to create additional logical networks.

Procedure

1 Log in to the vSphere Client for your SDDC.

You cannot create logical networks using the vSphere Web Client.

2 Select **Menu > Global Inventory Lists**.

3 Select **Logical Networks**.

4 Click **Add**.

5 In the **Name** text field, enter a name for the logical network.

6 In the **CIDR Block** text field, enter a CIDR block in xxx.xxx.xxx.0/YY format.

Prefix length should be between 22 and 30, because your logical network must have no more than 1000 ports.

7 (Optional) Select **Enabled** to enable DHCP.

If you enable DHCP on a logical network and you have configured an on-premises DNS server, you must edit your compute gateway VPN to enable DNS queries to be correctly forwarded over the VPN. Select **cgw-dns-network** as one of the local networks for the VPN.

8 (Optional) If you enabled DHCP, enter the domain name to use with VMs attached to this logical network in the **DNS Domain Name** text box.

9 Click **OK**.

What to do next

After you have created the logical network, you can attach VMs to it. See "Attach a VM to or Detach a VM from a Logical Network," on page 26.

Optionally, you can use this logical network as part of a VPN connection to your on-premises data center or to an Amazon VPC. See

- "Create a Compute VPN," on page 28
- "Create a VPN Connection Between the Compute Gateway and an Amazon VPC," on page 29

Attach a VM to or Detach a VM from a Logical Network

You can connect and disconnect a single or multiple VMs from a logical network.

Procedure

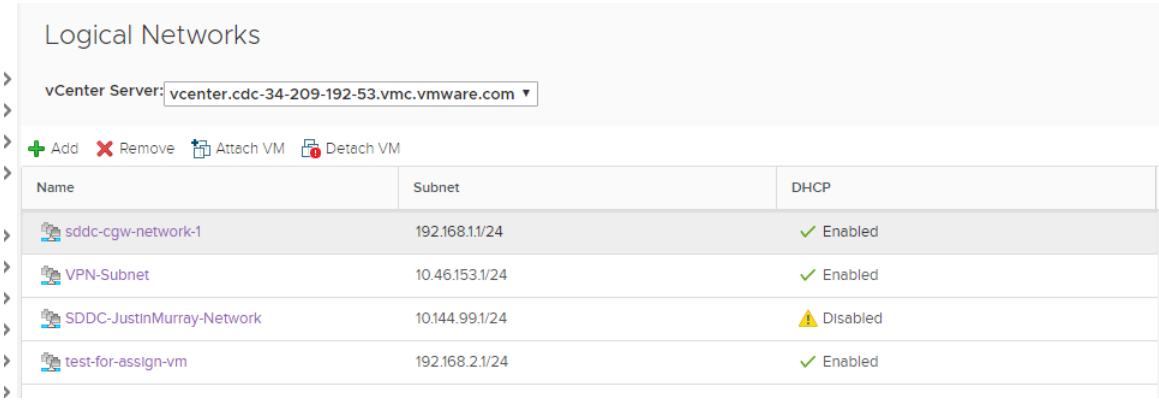
1 Log in to the vSphere Client for your SDDC.

2 Select **Menu > Global Inventory Lists**.

3 Select **Logical Networks**.

4 In the **vCenter Server** drop down menu, select the vCenter Server that manages the logical network you want to use.

5 Click next to the logical network name to select it.



6 Select whether to attach or detach VMs.

- Click **Attach VM** to attach VMs to the selected network.
- Click **Detach VM** to detach VMs from the selected network.

7 Select the virtual machine(s) you want to attach or detach, click **>>** to move them to the **Selected Objects** column, and click **Next**.

8 For each VM, select the virtual NIC you want to attach and click **Next**.

9 Click **Finish**.

Set Compute Gateway Firewall Rules

By default, the firewall for the compute gateway is set to deny all inbound and outbound traffic. Add additional firewall rules to allow traffic as needed.

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

5 Click **Add Rule**.

6 Enter the rule parameters.

Option	Description
Rule Name	Give the rule a descriptive name.
Action	Select **Allow** or **Deny**.
Source	Select the source for the network traffic. ■ Enter an IP address, an IP address range, or **Any** if you want the rule to apply to all traffic. ■ Select **All Internet and VPN** if you want the rule to apply to all traffic from the internet and the compute gateway VPN. ■ Select **All Connected AWS VPC** if you want the rule to apply to traffic from the connected Amazon VPC.
Destination	Select the destination for the network traffic. ■ Enter an IP address, an IP address range, or **Any** if you want the rule to apply to all traffic. ■ Select **All Internet and VPN** if you want the rule to apply to all traffic to the internet and the compute gateway VPN. ■ Select **All Connected AWS VPC** if you want the rule to apply to traffic to the connected Amazon VPC.
Service	Select one of the following: ■ Select **Any** to create a rule that applies to all traffic, regardless of protocol or port used. ■ Select a specific service to create a rule that applies to that protocol and port. ■ Select **Custom TCP**, **Custom UDP**, or **Custom ICMP** to create a rule that applies to a service and/or port that is not available in the dropdown menu.
Ports	If you selected a custom TCP, UDP, or ICMP service, enter the port number used by this service.

7 Use the up and down arrow icons to adjust the ordering of the firewall rules.

Firewall rules are applied in order from top to bottom.

Create a Compute VPN

Configure a compute VPN to allow VMs in your SDDC to communicate securely with VMs in an on-premises data center or within an Amazon VPC.

Create a compute gateway VPN allows you to deploy hybrid application architectures in which some VMs in the application are in your on-premises data center or on Amazon EC2, while others are in your cloud SDDC.

Prerequisites

Configuring a compute 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.
- The router or firewall should be configured with cryptography settings as described in "Recommended On-Premises VPN Settings," on page 21.
- If your on-premises gateway is behind another firewall, allow IPsec VPN traffic to pass through the firewall to reach your device by doing the following:
  - 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 Configure the Compute Gateway side of the tunnel.

   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**, click **VPN** and then **Add VPN**.

d Complete the Compute Gateway VPN configuration.

Parameter	Description
VPN Name	Enter a name for the VPN.
Remote Gateway Public IP	Enter the public IP address of your on-premises gateway.
Remote Gateway Private IP	If your gateway device is behind NAT, enter the private IP address of your on-premises gateway.
Remote Networks	Enter the address of your on-premises compute network.
Local Gateway IP	Displays the IP address of the SDDC compute gateway. This is not an editable field.
Local Network	Select the logical network to connect to using this VPN. If the logical network uses DHCP and you have configured an on-premises DNS server, also select the **cgw-dns-network** to allow DNS requests to travel over the VPN.
Encryption	Select **AES-256**.
Perfect Forward Secrecy	Select **Enabled**
Diffie Hellman	Select **DH2**
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.

2 Configure the on-premises side of the tunnel.

a Consult the documentation for your gateway or firewall device to learn how to configure it to match the settings VPN settings you've configured.

Configuration of the gateway device in your on-premises data center might need to be performed by a member of your networking team.

b If you selected as **Local Network** a non-default logical network that uses DHCP, 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.

When the VPN tunnel is configured, you should be able to verify connectivity in the VMC Console.

Create a VPN Connection Between the Compute Gateway and an Amazon VPC

If you need to connect VMs in your SDDC with resources in an Amazon VPC that isn't connected to your account using a cross-VPC ENI, you can create a VPN connection between your compute gateway and that VPC.

If the Amazon VPC is connected to your VMware Cloud™ on AWS, you don't need to create this VPN connection to access it.

Prerequisites

To create this VPN connection , you need:

- A working SDDC in VMware Cloud™ on AWS
- An AWS account

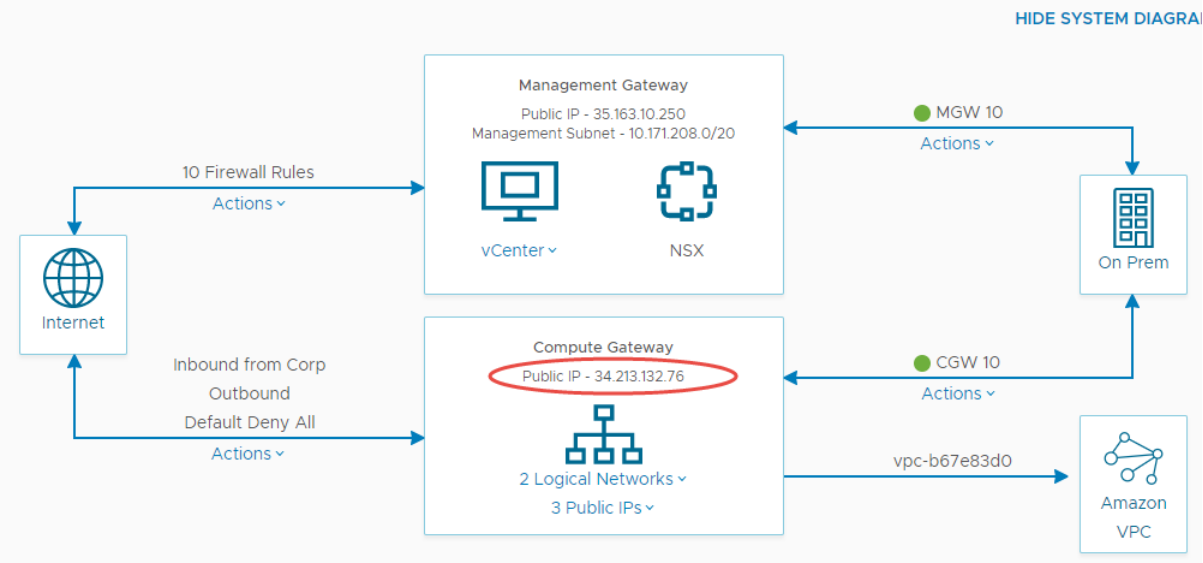
Procedure

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

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

3 Click **Network**.

4 Note the public IP address of the compute gateway as shown in the network system diagram.



5 Note the CIDR block for the logical network you want to connect to the VPN.

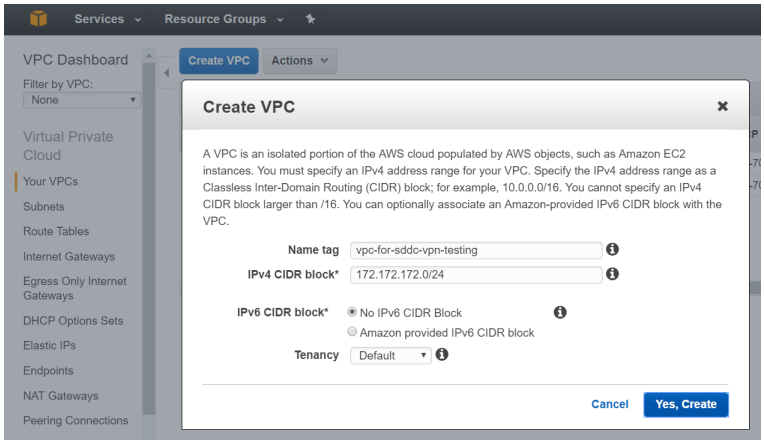
6 In another browser tab, log in to your AWS account.

7 If you don't already have a VPC and subnet you want to use, create them.

a Go to https://console.aws.amazon.com/vpc/ and select **Your VPCs**.

b Click **Create VPC**.

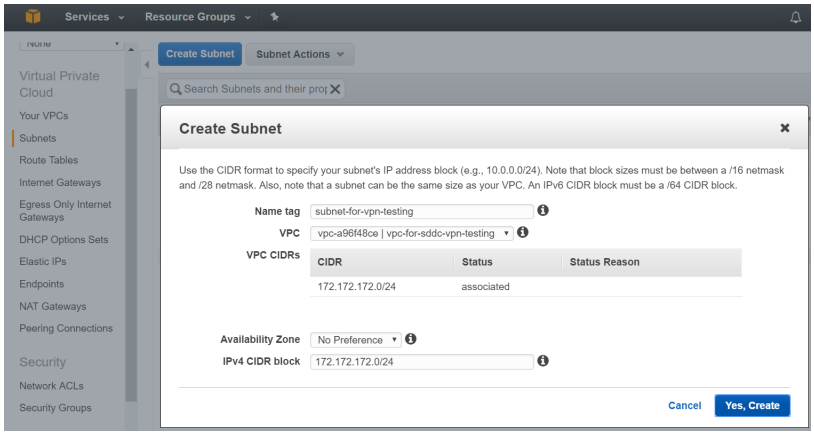
c Enter a name and an IPv4 CIDR block for the VPC and click **Yes, Create**.



d Click **Subnets** and click **Create Subnet**.

e Enter a name for the subnet.

f Select the VPC for the subnet and click **Yes, Create**.



8 Create a Customer Gateway.

a Under **VPN Connections**, select **Customer Gateways**.

b Click **Create Customer Gateway**.

c Enter a name for the gateway.

d For the **IP address**, enter the IP address of your SDDC compute gateway that you noted in Step 4.

9 Create a Virtual Private Gateway and attach it to your VPC .

a Click **Virtual Private Gateways** and click **Create Virtual Private Gateway**.

b Enter a name for the Virtual Private Gateway, and click **Yes, Create**.

c Make sure that the Virtual Private Gateway is selected and click **Attach to VPC**.

d Select the VPC to attach the gateway to.

10 Create the VPN tunnel.

Option	Description
Name tag	Enter a name for the VPN connection.
Virtual Private Gateway	Select the Virtual Private Gateway you created in Step 9.
Customer Gateway	Select **Existing** and then select the Customer Gateway you created in Step 8
Routing Options	Select **Static**.
Static IP Prefixes	Enter the CIDR block for the SDDC logical network that you noted in Step 5.

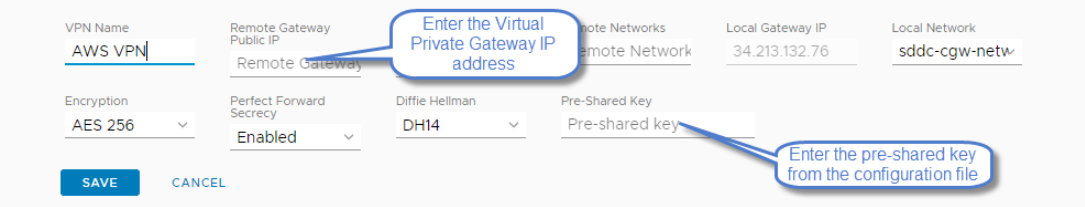
11 Click **Yes, Create** and then click **Download Configuration**.

Option	Description
Vendor	Select **Generic**.
Platform	Select **Generic**.
Software	Select **Vendor Agnostic**.

12 Open the configuration file and copy the Pre-Shared Key and the Virtual Private Gateway IP address.

13 In the VMC Console, create a VPN connection to the AWS Virtual Private Gateway as described in "Create a Compute VPN," on page 28.

Include the Virtual Private Gateway IP and Pre-Shared Key as indicated in the screenshot below.



14 Verify that the tunnel comes up on the SDDC side by looking for the **Connected** status.

15 Verify that the tunnel comes up on the AWS side.

a Go to https://console.aws.amazon.com/vpc/ and select **VPN Connections**.

b Select the VPN.

c Click **Tunnel Details** and check that the status is **UP**.

16 Add a route to your SDDC from the AWS console.

a Log in to the AWS console and select **VPC**.

b Select the route table for your VPC and click the **Routes** tab.

c Click **Edit**.

d Click **Add another route**.

e In the **Destination** text box, enter the CIDR block range for the logical network in your SDDC.

f In the **Target** field, select the Virtual Private Gateway you created.

Set Compute Gateway DNS

Set a DNS server to allow the compute gateway and workload VMs to resolve fully-qualified domain names (FQDNs) to IP addresses.

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 Under **Compute Gateway**, click **DNS.**

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

Note Both DNS servers must be able to resolve all intended FQDNs. Do not add one public DNS server and one private DNS server. If you do, FQDN resolution becomes unpredictable.

Request Public IP Address

You can request public IP addresses to assign to workload VMs to allow access to these VMs from the internet. VMware Cloud on AWS will provision the IP address from AWS.

Prerequisites

Before you create a public IP address, you should assign your VM a static IP address from its logical network.

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 Under **Compute Gateway**, click **Public IPs**.

5 Click **Request Public IP**.

6 Enter any notes that you want to make about the IP address.

7 Click **Save**.

After a few moments, the Public IP address is provisioned.

What to do next

After the Public IP address is provisioned, you must configure NAT to direct traffic from the public IP address to the internal IP address of a VM in your SDDC. See "Configure NAT Settings," on page 33.

Configure NAT Settings

Inbound Network Address Translation (NAT) allows you to map internet traffic to a public-facing IP address and port to a private IP address and port inside your SDDC's compute network.

When configuring NAT rules, you have the option of configuring either one-to-one NAT or one-to-many NAT. Use one-to-one NAT when you want to map a single public IP address and port to a single internal IP address and port. For example, a public IP of 198.51.100.5 and port 443 is mapped to 172.100.100.20 and port 443. In some cases, you might choose to map a source port to a different destination port. For example, 198.51.100.5 and port 80 might be mapped to 172.100.100.20 and port 8080.

Use one-to-many NAT when a single public IP address and port is mapped to one internal IP address and multiple ports, or to multiple internal IP addresses and ports.

Prerequisites

Before you can assign a public IP address to a virtual machine, you must assign the virtual machine to a logical network and give it a static IP address.

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 Under **Compute Gateway**, click **NAT**.

5 Click **Add NAT Rule**.

6 Enter the NAT parameters.

Option	Description
Description	Enter a description for the NAT rule.
Public IP	Select the Public IP address you have provisioned for the VM.

Option	Description
Service	Select one of the following. ■ Select **Any** for a rule that applies to all inbound traffic. ■ Select a particular service to create a rule that applies only to traffic using that protocol and port. ■ Select **Custom TCP**, **Custom UDP**, or **ICMP (All ICMP)** to create a rule that applies to a service and/or port that is not available in the dropdown menu.
Public Ports	If you selected a custom TCP or UDP, enter the port to use for that service.
Internal IP	Enter the internal (private) IP address to direct the traffic from the public address to.
Internal Ports	If you selected a custom TCP or UDP, enter the port to use for that service.

7 Click **Save**.

Connect to vCenter Server 5

The **Connection** tab for your SDDC assists you in connecting to vCenter Server in a number of ways.

Procedure

- Select a method for connecting to your SDDC's vCenter Server.

Option	Description
Connect using the vSphere Client	Click the link under **vSphere Client (HTML5)**. The credentials for log in are shown under **Authentication**. Click to copy an item to the clipboard.
Connect to the API Explorer	Click the link under **vCenter Server API Expolorer**. The credentials for log in are shown under **Authentication**. Click to copy an item to the clipboard.
Connect using PowerCLI	The cmdlet for connecting is shown under **PowerCLI Connect**. Click to copy the cmdlet to the clipboard. The credentials for log in are shown under **Authentication**. Click to copy an item to the clipboard.

About Hybrid Linked Mode 6

Hybrid Linked Mode allows you to link your VMware Cloud™ on AWS vCenter Server instance with an on-premises vCenter Server instance.

Using Hybrid Linked Mode, you can:

- Log in to the vCenter Server instance in your SDDC using your on-premises credentials.
- View and manage the inventories of both your on-premises and VMware Cloud™ on AWS data centers from a single vSphere Client interface.
- Cold migrate workloads between your on-premises data center and cloud SDDC.

Requirements and Limitations for Hybrid Linked Mode

Currently, the following requirements and limitations apply for Hybrid Linked Mode.

- You can link a cloud SDDC to an on-premises data center running vSphere 6.5 patch d and later.
- You can link a cloud SDDC to only one on-premises data center.
- Only an embedded Platform Services Controller configuration is supported for the on-premises data center.

This chapter includes the following topics:

Hybrid Linked Mode Prerequisites

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

- Ensure that your on-premises data center meets the following requirements.
  - Your on-premises vCenter Server system is running vSphere 6.5 patch d and later.
  - You can link only one on-premises vCenter Server system.
  - Your on-premises vCenter Server system is an embedded Platform Services Controller configuration.
- Configure a management gateway IPsec VPN connection between your on-premises data center and cloud SDDC.

- Ensure that you have network connectivity between your VMware Cloud™ on AWS management gateway and your on-premises ID source and SSO domain. If necessary, create firewall rules in the VMC Console as shown below.

Use Cases	Service	Source	Destination
SDDC vCenter Server access	HTTPS	IP address or CIDR block from on-premises data center	vCenter
vCenter Single Sign-On access	SSO	IP address or CIDR block, either public or from an on-premises data center connected by a VPN tunnel	vCenter

- Ensure that an on-premises DNS server is configured for your management gateway so that it can resolve the FQDN for the identity source.
- Ensure that your on-premises gateway or firewall allows access to the necessary ports from your SDDC for the following services.

Service	Ports
On-premises vCenter Server	443
On-premises Platform Services Controller	389, 636
On-premises Active Directory server	389, 636, 3268, 3269
On-premises DNS	53

- Decide which of your on-premises users you want to grant Cloud Administrator permissions to. Add these users to a group within your identity source.
- Ensure that you have login credentials for a user who has a minimum of read-only access to the Base DN for users and groups in your on-premises environment.
- Ensure that you have the login credentials for your on-premises vSphere SSO domain.

Add a Cloud Administrator Group

After you have added an identity source, you can select a group of users to grant Cloud Administrator permissions to in your SDDC.

The group of users you select in this process have full Cloud Administrator permissions in your VMware Cloud™ on AWS SDDC.

If you want to add more than one group, you can repeat this process.

Procedure

1 If you haven't already, log in to the vSphere Client for your SDDC and browse to the Linked Domains page.

   a Select **Menu > Administration** to display the Administration page.

   b Under **Hybrid Cloud**, select **Linked Domains**.

2 Under **Add Cloud Administrators Group**, click **Add**.

3 Select the identity source you want to use.

4 Click the search icon and search for the user group.

5 Click **OK**.

At this point, the users in the group you selected can log into your SDDC with their on-premises credentials and have full Cloud Administrator permissions. If you want to assign more restrictive permissions to other users, do this through the permissions management interface in the vSphere Client.

Link to an On-Premises SSO Domain

After you have linked an identity source and added a group with Cloud Administrator permissions, you can link an on-premises vCenter Single Sign-On (SSO) domain to complete the configuration of Hybrid Linked Mode.

Prerequisites

If you haven't already, add a Cloud Administrator user group: "Add a Cloud Administrator Group," on page 38

Procedure

1 If you haven't already, log in to the vSphere Client for your SDDC and browse to the Linked Domains page.

   a Select **Menu > Administration** to display the Administration page.

   b Under **Hybrid Cloud**, select **Linked Domains**.

2 Under **Link to On-Prem Domain**, click **Link**.

3 Configure the on-premises domain settings.

Option	Description
Platform Service Controller	The FQDN or IP Address of the Platform Services Controller
HTTPS Port	The HTTPS port used by the Platform Services Controller. By default, this is 443.
SSO Domain Name	The SSO domain name.
SSO User Name	The SSO user name.
SSO Password	The password for the SSO user.

4 Click **Link**.

   Linking might take a few minutes to complete. During the linking process, lookup services, tags and categories, the trust-signing certificate, and on-premises trusted root chain are synchronized from the on-premises domain to the cloud SDDC. When the linking process is complete, a dialog box is displayed that prompts you to log out.

5 Click **OK** to log out.

   In order to see the inventory of your on-premises vCenter Server together with that of your SDDC, you must log out and log back in as an on-premises user with Cloud Administrator permissions.

Unlink an SSO Domain

You can unlink a vCenter Single Sign-On (SSO) domain when you no longer want to use Hybrid Linked Mode with that on-premises server.

For example, you might want to link an on-premises data center to your SDDC in order to migrate virtual machines to the SDDC, and then unlink the on-premises data center. If you plan to decomission a linked on-premises data center, unlink it before doing so.

Note Unlinking an SSO domain does not remove the associated identity source or permissions that you added before linking the domain. Users can still use their on-premises credentials to authenticate to your SDDC, and retain the permissions granted to them. However, they are not able to view the on-premises inventory after unlinking the domain.

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

Prerequisites

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

Procedure

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

   A dialog box appears asking you to confirm the unlinking. Note that all currently active sessions are logged out when you unlink a domain.
3. Click **OK**.

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

The SSO domain is unlinked. You can now log back in with your cloud or on-premises credentials and view the resources in your SDDC. If you want to continue using Hybrid Linked Mode, you can link to another SSO domain or relink to the same domain.

Managing SDDC Hosts 7

You can add hosts to your SDDC cluster or remove hosts from your SDDC cluster as long as the number of hosts does not fall below the minimum or above the maximum for your SDDC.

The minimum number of hosts in an SDDC cluster is 4. The maximum number hosts depends on various factors, including what kind of account you signed up for.

When you add a host to the SDDC, it is added to the existing cluster in the SDDC, and its storage becomes part of the vSAN storage for the cluster.

This chapter includes the following topics:

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.

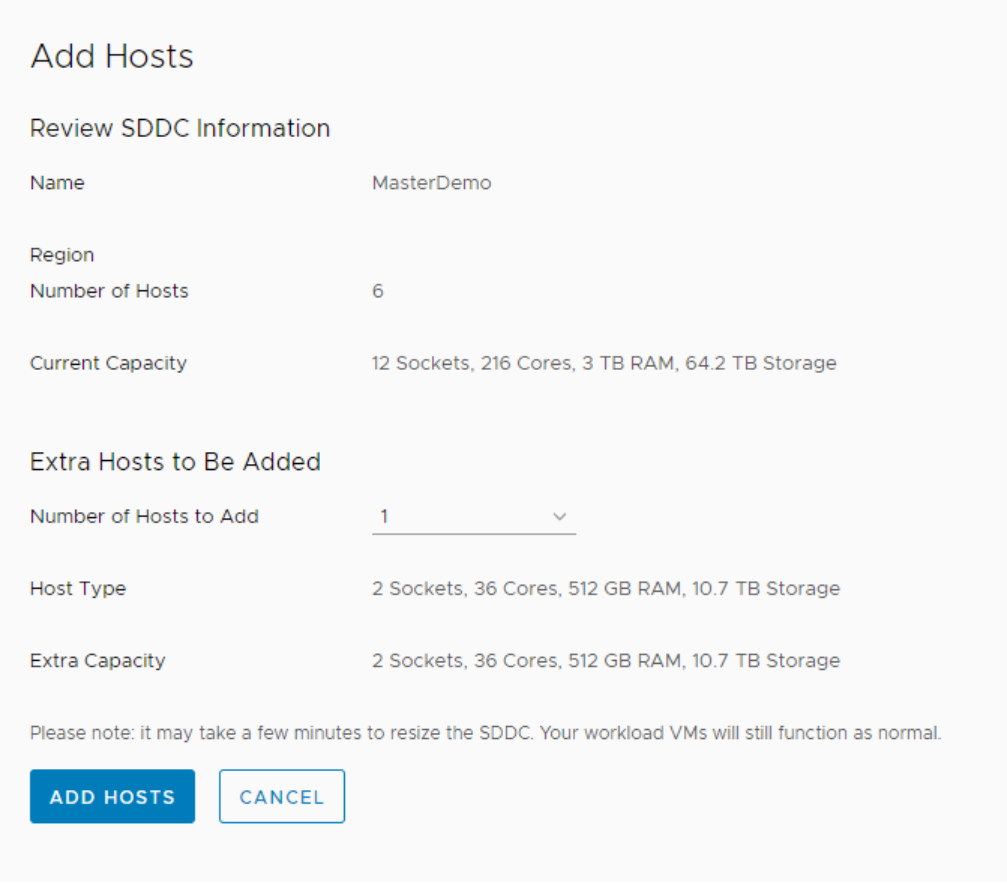
Procedure

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

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

3 Select **Actions > Add Hosts**.

The Add Hosts page is displayed.



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

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 at 4 or more.

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.

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**

4 Select the number of hosts you want to remove.

5 Select the **I understand that this action cannot be undone** check box.

6 Click **Remove**.

VMware Cloud™ on AWS Storage 8

VMware Cloud™ on AWS provides storage in the form of two vSAN datastore available to the hosts in the SDDC cluster: workloadDatastore, managed by the Cloud Administrator, and vsanDatastore, managed by VMware.

Workload Datastore

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

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

Note Currently, an issue causes the Storage Compatibility page of the Create VM Storage Policy wizard to report double the actual storage capacity that is available. The vsanDatastore and workloadDatastore are backed by the same storage, but the capacity for each is reported separately, making it appear as though there is twice as much storage.

vsanDatastore

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

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

Getting Templates, ISOs, and Other Content into Your SDDC

9

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.

The Content Onboarding Assistant adds scripts, ISO images to a Content Library that is published from your on-premises data center and subscribed from your SDDC. It does not add existing OVF or OVA templates to the Content Library. For ways of transferring OVF or OVA templates to your SDDC, see Chapter 9, "Getting Templates, ISOs, and Other Content into Your SDDC," on page 45.

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 as described in "Create a Management VPN," on page 22.
- Configure your SDDC to use an internal DNS server that works with your on-premises hosts. See "Set Management Gateway DNS," on page 20.

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 don't want to use the Content Onboarding Assistant, or if you already have a Content Library in your on-premises data center, you can use the Content Library to import content into your SDDC.

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

For more information on creating content libraries, see Create a Library.

Prerequisites

Before you import content, do the following:

- Set up a VPN connection between your on-premises data center and your SDDC as described in "Create a Management VPN," on page 22.
- Configure your SDDC to use an internal DNS server that works with your on-premises hosts. See "Set Management Gateway DNS," on page 20.

Procedure

1. If you don't already have one, create a Content Library in your on-premises data center.
2. Add your templates, ISO images, and scripts to the Content Library.

   All `.vmtx` templates are converted to OVF templates.
3. Publish your content library.
4. In your SDDC, create a content library that is subscribed to the content library you published from your on-premises data center. 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**.

Creating Virtual Machines 10

Currently, you are limited in the ways you can create virtual machines because of permissions restrictions in your SDDC.

You can create a VM by:

- Upload an ISO image, `.vmtx` template, OVA template, or OVF template directly to the workloadDatastore in your SDDC.
- Using an ISO image from a Content Library.
- Using an OVF template from a Content Library.
- Deploying an OVF or OVA template from your client machine or from a URL.
- Using a `.vmtx` template imported into your SDDC using the Content Onboarding Assistant

At the moment, you can't:

- Attach a client-side ISO image to a VM to install the operating system.

This chapter includes the following topics:

Create a VM using an ISO in a Content Library

You can create a VM and use an ISO image in a Content Library to install the operating system.

Prerequisites

Have a Content Library containing the ISO image you want to use.

- For more information on creating a subscribed Content Library, see "Use a Content Library to Import Content into Your SDDC," on page 48
- For more information on creating a Content Library using the Content Onboarding Assistant, see "Use the Content Onboarding Assistant to Transfer Content to Your SDDC," on page 46.
- For more information on creating local Content Library, see Create a Library.
- For more information on importing content in to a Content Library, see Import Items to a Library from a Local File on Your System.

Procedure

1 From the vSphere Client VMs and Templates view, right click the **Workloads** folder and select **New virtual machine**.

2 Select **Create a new virtual machine** and click **Next**.

3 Proceed through the New Virtual Machine wizard, using the following settings.

   a For the VM folder, select **Workloads**, **Templates**, or another folder that you have write permissions on.

   b For the compute resource, select **Compute-ResourcePool**.

   c For the datastore, select **workloadDatastore**.

4 On the Customize Hardware page, connect the ISO image to the VM.

   a Next to **New CD/DVD Drive**, select **Content Library ISO file.**

   b Select the ISO image and click **OK**.

   c Select **Connect at Power On** and click **Next**.

5 Review the VM settings and click **Finish**.

6 Power on the VM and complete the guest operating system installation.

Deploy a Virtual Machine from a .vmtx Template

You can deploy a VM from a `.vmtx` template that you imported using the Content Onboarding Assistant.

Prerequisites

Import the template using the Content Onboarding Assistant. For more information, see "Use the Content Onboarding Assistant to Transfer Content to Your SDDC," on page 46.

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**.

Deploy a VM from an OVF Template in a Content Library

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

Prerequisites

Have a Content Library containing the OVF template you want to use.

- For more information on creating a subscribed Content Library, see "Use a Content Library to Import Content into Your SDDC," on page 48
- For more information on creating a Content Library using the Content Onboarding Assistant, see "Use the Content Onboarding Assistant to Transfer Content to Your SDDC," on page 46.
- For more information on creating local Content Library, see Create a Library.

- For more information on importing content in to a Content Library, see Import Items to a Library from a Local File on Your System.

Procedure

1. From the vSphere Client VMs and Templates view, right click the **Workloads** folder and select **New virtual machine**.
2. Select **Deploy from template** and click **Next**.
3. Select the template to deploy.
4. Proceed through the New Virtual Machine wizard, using the following settings.
   a. For the VM folder, select **Workloads**, **Templates**, or another folder that you have write permissions on.
   b. For the compute resource, select **Compute-ResourcePool**.
   c. For the datastore, select **workloadDatastore**.
5. On the Select networks page, enter an IP address in the **IP address** field.

   The **IP Allocation Settings** on this page show only the Static IP option, even if the logical network you have selected uses DHCP. You must enter something into the **IP address** field to proceed in the wizard. If DHCP is enabled, the VM deploys with DHCP.
6. Review the VM settings and click **Finish**.

Deploy a VM from a Client OVF or OVA Template

You can deploy a VM from an OVF or OVA template on your client machine.

For more information on deploying OVF or OVA templates, see Deploying OVF and OVA Templates.

Prerequisites

Have an OVF or OVA template on your client machine.

Procedure

1. From the vSphere Client VMs and Templates view, right click the **Workloads** folder and select **Deploy OVF Template**.
2. Select **Local file**, click **Choose files**, and browse to the OVF or OVA template.
3. Proceed through the Deploy OVF 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**.
4. On the Select networks page, enter an IP address in the **IP address** field.

   The **IP Allocation Settings** field is populated based on your OVF descriptor file. If the imported OVF only specifies DHCP, the **IP Allocation Settings** show only DHCP. If the OVF specifies both static IP and DHCP, **IP Allocation Settings** shows both.

11 Configuring Virtual Machines

After you create a virtual machine, you can perform configuration tasks such as setting a public IP address or enabling access to a Remote Console.

Many of the configuration tasks are the same in an on-premises data center and in a cloud SDDC. See the *Virtual Machine Administration* documentation.

This chapter includes the following topics:

Enable Access to the Virtual Machine Remote Console

To access the Virtual Machine Remote Console (VMRC) for VMs in your cloud SDDC, ensure that you have correctly configured firewall access to ESXi the VPN settings for On-Premises routers. You must also update the `hosts` file on any machines from which you want to access the VMRC.

Prerequisites

- Complete firewall and VPN configuration. See Chapter 3, "Configuring Management Gateway Networking," on page 17.
- On Windows, you need administrator privileges to edit the `hosts` file.

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. Under **Management Gateway**, click **Firewall Rules**.
5. 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

6 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.

7 On the machine from which you want to access the VM's remote console, edit the `/etc/hosts` file (on Linux or MacOS) or `C:\Windows\System32\drivers\etc\hosts` (on Windows) and add the following line for each host.

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

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

12 Accessing AWS Services

During SDDC deployment, you connected your SDDC to an Amazon VPC in your AWS account, creating a high-bandwidth, low-latency interface between your SDDC and services in the Amazon VPC.

Using this connection, you can enable access between VMs in your SDDC and services in your AWS account, such as EC2 and S3.

This chapter includes the following topics:

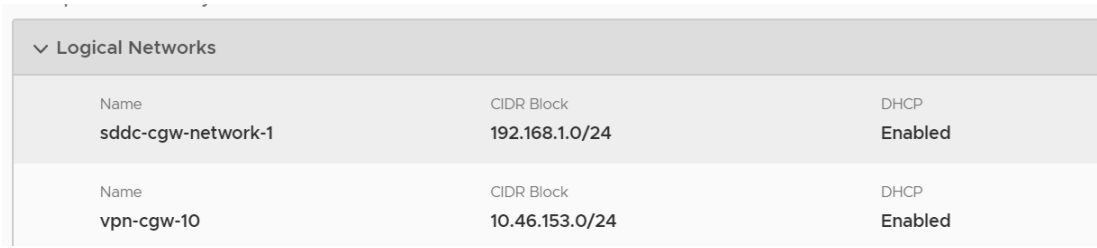
Access an EC2 Instance

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.

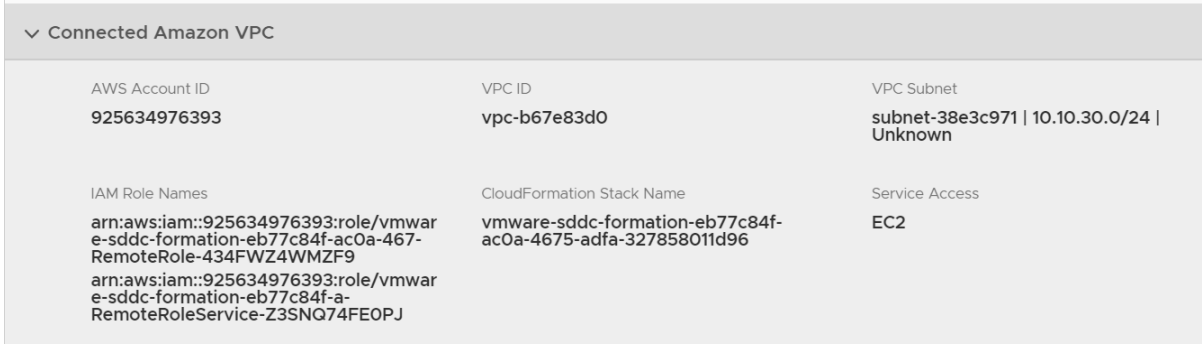
Prerequisites

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 subnet 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.

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 Create a compute gateway firewall rule to allow https access to the connected Amazon VPC.

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

b **View Details**

c **Network**

d 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.

Using On-Premises vRealize Automation with Your Cloud SDDC

13

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

Currently vRealize Automation 7.2 or 7.3 is supported 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 the VPN for the management gateway as described in "Create a Management VPN," on page 22.
3. Configure a management gateway firewall rule to allow traffic to vCenter Server as described in "Set Management Gateway Firewall Rules," on page 17.
4. Create a logical network as described in "Create a Logical Network," on page 25and note its CIDR.
5. Configure a VPN for the compute gateway as described in "Create a Compute VPN," on page 28.

   Specify the CIDR of the logical network you created in the previous step.
6. Configure additional management gateway firewall rules.

Name	Source	Destination	Service
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)

7 Configure 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

8 Modify DNS settings so that the vCenter Server FQDN resolves to a private IP as described in "Set Management Gateway DNS," on page 20.

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," on page 61.
- Ensure that all vRealize Automation VMs are configured to use TLS 1.2.

Procedure

1 In vRealize Automation, select **Infrastucture > 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, 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

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

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.

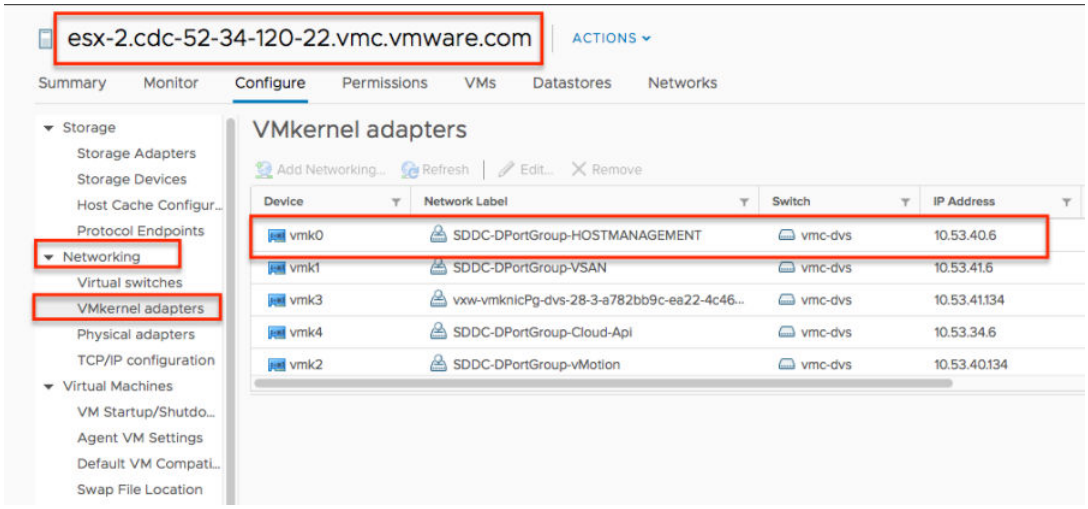
   a Log in to the vSphere Client for your SDDC.

   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
```

Roles and Permissions in the SDDC 14

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.

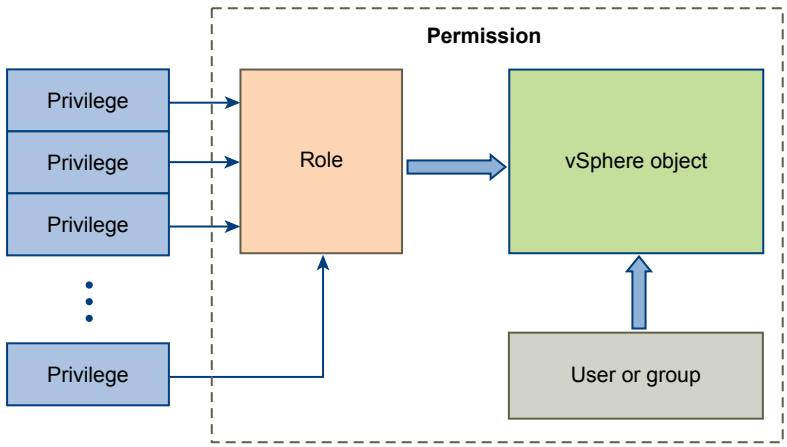
CloudGlobalAdmin The CloudGlobalAdmin role is associated with global privileges and allows you to create and manage content library objects and perform some other global tasks.

This chapter includes the following topics:

Understanding the Permission Model

Users of VMware Cloud™ on AWS have different permissions on different objects in the object hierarchy. Each permission gives one user or group a set of privileges, that is, a role for that object.

Figure 14-1. Permissions



Permissions in VMware Cloud™ on AWS

Permissions are initially set by VMware. For example, when you log in as cloudadministrator, you might have the CloudAdmin role on a ComputeResourcePool object and the CloudGlobalAdmin role on a ManagementResourcePool object. If have the privileges associated with CloudAdmin on ComputeResourcePool, then you can create and manage virtual machines there. If you have the privileges associated with CloudGlobalAdmin on ManagementResourcePool, then you cannot create and manage virtual machines, but you can perform some other global tasks, for example content library management.

Permissions Background Information

The permission model of VMware Cloud™ on AWS is simpler than the model for an on-premises vSphere environment. If you're interested in some background information, here are the basic concepts.

Privileges	Privileges are fine-grained access controls.
Roles	Roles are sets of privileges. Roles allow you to assign permissions on an object based on a typical set of tasks that users perform. Default roles are predefined and cannot be changed. VMware Cloud™ on AWS does not support custom roles.
Permissions	Each object in the object hierarchy has associated permissions. Each permission specifies for one group or user which privileges that group or user has on the object.
Users and Groups	The Hybrid Linked Mode feature allows a CloudAdmin to limit permissions for some users or groups on parts of the object hierarchy.

View Permissions and Privileges

For each object in the object hierarchy, you can check whether you have CloudAdmin or CloudGlobalAdmin permissions on that object. You can view the privileges that are associated with the CloudAdmin and with the CloudGlobal role from the vSphere Client.

Procedure

1 Select and object in the object hierarchy, for example a resource pool or virtual machine, and click **Permissions**.

  You see the CloudAdmin or the CloudGlobalAdmin role is assigned to users in the CloudAdminGroup.

2 You can then view the privileges associated with each group.

  a On the vSphere Client Home page, click **Administration**.

  b Under **Access Control**, click **Roles**.

  c Click the **CloudAdmin** role or click the **CloudGlobalAdmin** role.

  d Click the **Privileges** tab on the right.

You can scroll through the list of privileges to see the privileges that the Cloud Administrator has. See https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.vsphere.security.doc/GUID-ED56F3C4-77D0-49E3-88B6-B99B8B437B62.html for a detailed list of all vSphere privileges.

Privileges Reference

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

VMware assigns a different role on different objects to a cloud administrator: either the CloudAdmin role or the CloudGlobalAdmin role. As a result, you can either perform global tasks on that object, or you can perform specific tasks such as creating virtual machines or folders.

Table 14-1. Privileges in the Cloud SDDC

Privilege Set	CloudAdmin	CloudGlobalAdmin	Comment
Alarms	All **Alarms** privileges.	--	
Auto Deploy	--	--	VMware performs host management.
Content Library	--	All **Content Library** privileges	
Cryptographer--	--	--	Not supported in this version of the product.
Datacenter	--	--	VMware performs data center creation, deletion, and other data center operations.
Datastore	A CloudAdmin user has the following **Datastore** privileges: ■ **Datastore.Allocate space** ■ **Datastore.Browse datastore** ■ **Datastore.Configure datastore** ■ **Datastore.Low level file operations** ■ **Datastore.Remove file** ■ **Datastore.Update virtual machine metadata**	--	
dvPort Group	--	--	VMware performs data center network operations.
Distributed Switch	--	--	VMware performs data center network operations.
ESX Agent Manager	--	--	VMware performs host management.
Extension	--	--	Not supported in the cloud SDDC
Folder	All **Folder** privileges.	--	
Global	A CloudAdmin user has the following **Global** privileges: ■ **Global.Cancel Task** ■ **Global.Global Tag** ■ **Global.Health** ■ **Global.Log Event** ■ **Global.Set custom attribute** ■ **Global.System Tag**	A CloudGlobalAdmin user has the following **Global** privileges: ■ **Global. Manage custom attributes** ■ **Global.Service manager**	

Table 14-1. Privileges in the Cloud SDDC (Continued)

Privilege Set	CloudAdmin	CloudGlobalAdmin	Comment
Host	A CloudAdmin user has the following **Host** privilege: ■ **Host. vSphere Replication. Manage replication**	--	VMware performs all other host management.
Hybrid Linked Mode	--	A CloudGlobalAdmin user has the following **Hybrid Linked Mode** privilege: ■ **Hybrid Linked Mode. Manage**	Not currently documented for the on-premises version of vSphere.
Inventory Service	--	All **Inventory Service** privileges.	Not currently documented for the on-premises version of vSphere.
Network	A CloudAdmin user has the following **Network** privilege: ■ **Network. Assign network**	--	VMware performs other network management tasks.
Performance	--	--	
Permissions	--	**Permissions.ModifyPermissions**	
Profile-driven Storage	--	All **Profile-driven Storage** privileges.	
Resource	All **Resource** privileges.		
Scheduled Task	A CloudAdmin user has the following **Scheduled Task** privilege: ■ **Scheduled Task. Create** ■ **Scheduled Task. Delete** ■ **Scheduled Task. Edit** ■ **Scheduled Task. Run**	A CloudGlobalAdmin user has the following **Scheduled Task** privilege: ■ **Scheduled Task. Global Message**	
Sessions	--	A CloudGlobalAdmin user has the following **Session** privileges: ■ **Sessions. Message** ■ **Sessions. Validate Session**	
Storage Views	A CloudAdmin user has the following **Storage Views** privilege: ■ **Storage Views. View**	--	
System	All **System** privileges.	--	
Task	--	--	**Task** privileges control the ability of extensions to manage tasks. VMware manages extensions for you.
vApp	All **vApp** privileges.	--	

Table 14-1. Privileges in the Cloud SDDC (Continued)

Privilege Set	CloudAdmin	CloudGlobalAdmin	Comment
Virtual Machine	A CloudAdmin user has most **Virtual Machine** privileges. The following privileges are NOT available: ■ **Virtual Machine. Interaction. Create Secondary** ■ **Virtual Machine. Interaction. Disable Secondary** ■ **Virtual Machine. Interaction.Enable Secondary** ■ **Virtual Machine. Interaction. Make Primary** ■ **Virtual Machine. Interaction. Record** ■ **Virtual Machine. Interaction. Replay**	--	
vService	All **vService** privileges.	--	

Troubleshooting 15

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 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.
Access documentation and other learning resources	 Click the help icon and click **Early Access Home Page**. Here you can find the most up-to-date version of this guide, as well as videos, blog posts, and other resources to help you use VMware Cloud™ on AWS.
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.

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. You must create a firewall rule to allow traffic to the vCenter Server.

Solution

- Create a firewall rule as described in "Set Management Gateway Firewall Rules," on page 17

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," on page 71.

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.

Index