VMware Cloud on AWS Getting Started

14 June 2019

VMware Cloud on AWS

vmware®

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

https://docs.vmware.com/

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

docfeedback@vmware.com

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

Contents

Getting Started With VMware Cloud on AWS 5

1 Onboarding Checklist 6
- Read Your Service Welcome Email 7
- Update Your My VMware Account 7
- View Your Subscription Purchase Program Fund 8
- Log into the VMware Cloud Console 8
- Add Organization Owners and Organization Users 8
- Create a Subscription 9
- View Your Billing Information 9
- View the VMware Cloud on AWS Roadmap 10
- View the VMware Cloud on AWS Release Notes 10
- Sign Up to Receive Service Alerts 10
- Review the Service Level Agreement for VMware Cloud on AWS 10

2 Account Creation and Management 11
- Creating an Account 11
  - Create an Organization Owner Account with a My VMware Account 11
  - Create an Organization Owner Account Without a My VMware Account 12
- Invite a New User 13
- Accept an Account Invitation 13
- Assign a VMC Service Role to an Organization Member 14

3 Create a Subscription 16

4 Deploying and Managing a Software-Defined Data Center 17
- Deploying a Single Host SDDC Starter Configuration 21
  - Request Access and Create an Account 22
  - Scale Up a Single Host SDDC Starter Configuration 23
- Deploy an SDDC from the VMC Console 23
- View SDDC Information and Get Support 27

5 Connect to vCenter Server 28

6 Configure SDDC Networking and Security 29
- Create a Route-Based VPN 30
- Create an On-Premises IPsec VPN 32
- Create a Network Segment 34

Add or Modify Management Gateway Firewall Rules 36
Add a Management Group 37
Configure Management Network Private DNS 38

7 Deploy Workload VMs 39
Use the Content Onboarding Assistant to Transfer Content to Your SDDC 39
Deploy a Virtual Machine from a .vmtx Template 41
Assign a Public IP Address to a VM 42
Enable Access to the Virtual Machine Remote Console 42

8 Get Help and Support 44

Getting Started With VMware Cloud on AWS

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

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

Intended Audience

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

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

Onboarding Checklist

1

This onboarding checklist highlights the steps and resources that are available to you as you prepare to create your first VMware Cloud on AWS Software Defined Data Center (SDDC).

Procedure

1 Read Your Service Welcome Email

During the deal process, your Cloud Sales Specialist or Client Executive requested that you identify a Fund Owner and a Fund User. After your deal is processed, VMware sends a service welcome email to the Fund Owner and Fund User.

2 Update Your My VMware Account

Prior to logging in to the VMware Cloud Console, ensure that your My VMware account is up-to-date and all required fields are filled in. If required fields are missing, you will not be able to create your first SDDC.

3 View Your Subscription Purchase Program Fund

Many customers choose to purchase Subscription Purchase Program (SPP) credits, which can be redeemed against VMware Cloud on AWS in either an On-demand or Subscription consumption model. The Subscription model is similar to an AWS Regional Reserved Instance.

4 Log into the VMware Cloud Console

The service activation link provided to you in the service welcome email directs you to the VMware Cloud Console.

5 Add Organization Owners and Organization Users

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.

6 Create a Subscription

Subscriptions allow you to save money by committing to buy a certain amount of capacity for a defined period. A subscription is not required to use VMware Cloud on AWS. Any usage of the service not covered by a subscription is charged at the on-demand rate for the region selected.

7 View Your Billing Information

Fund owners can view billing information for the active method of payment in the organization.

8 View the VMware Cloud on AWS Roadmap

VMware Cloud on AWS has a public that roadmap intended to provide guidance to customers regarding features that are Available, in Preview, in Active Development and testing and Planning.

9 View the VMware Cloud on AWS Release Notes

VMware Cloud on AWS is able to release new features at a much faster pace that our traditional on premises software products. Check the release notes page frequently to keep updated on the new features that have been released.

10 Sign Up to Receive Service Alerts

The VMware Coud Operations team posts updates on planned maintenance events, maintenance start and end times, and service incidents on the VMware Cloud Services status page.

11 Review the Service Level Agreement for VMware Cloud on AWS

The Service Level Agreement (SLA) for VMware Cloud on AWS defines the service components that have an availability commitment as well as their associated targets.

Read Your Service Welcome Email

During the deal process, your Cloud Sales Specialist or Client Executive requested that you identify a Fund Owner and a Fund User. After your deal is processed, VMware sends a service welcome email to the Fund Owner and Fund User.

The wecome email is entitled, "Welcome to VMware Cloud on AWS." If you do not recall seeing it, check your spam message or corporate spam filter. This email contains a unique service activation link which directs you to the VMware Cloud Console. It is important to use this service activation link when you log into the VMware Cloud Console for the first time.

Procedure

- Find your "Welcome to VMware Cloud on AWS" welcome email which includes your unique service activation link.
- If the email is not in your inbox, check your corporate spam filter.
- If you still cannot find the email, ask your Cloud Sales Specialist or Customer Success Manager to resend the email or provide you with the service activation link.
- Complete the next step before clicking on the service activation link.

Update Your My VMware Account

Prior to logging in to the VMware Cloud Console, ensure that your My VMware account is up-to-date and all required fields are filled in. If required fields are missing, you will not be able to create your first SDDC.

You must provide a valid address as part of your My VMware profile. In addition, spell out the name of your state in full. For example, enter `California` rather than `CA`.

Procedure

- To log in to My VMware, go to https://my.vmware.com.
- For more information on updating your My VMware profile, see https://kb.vmware.com/s/article/2086266.

- For more information on resetting your My VMware password, see https://kb.vmware.com/s/article/2013961.

View Your Subscription Purchase Program Fund

Many customers choose to purchase Subscription Purchase Program (SPP) credits, which can be redeemed against VMware Cloud on AWS in either an On-demand or Subscription consumption model. The Subscription model is similar to an AWS Regional Reserved Instance.

It is your responsibility to be aware of your SPP fund balance and manage users who should have access to it. Only a Fund Owner can add additional Fund Users. Fund Owners and Fund Users can direct VMware Cloud on AWS to use the SPP fund as a payment method.

Procedure

- View your SPP fund balance on My VMware: https://kb.vmware.com/s/article/2143195.

  If you don't see an SPP fund listed under **Accounts > Hybrid & Subscription Purchasing Programs (HPP/SPP)**, then you should contact your Cloud Sales Specialist or Customer Success Manager.
- For more information on adding or removing fund users, see https://kb.vmware.com/s/article/2094497.
- To change a Fund Owner, do one of the following.
  - Select **Support > Product Licensing**.
  - Select **Account > VMware Cloud Services - User Management**.
  - Speak to your Customer Success Manager.

Log into the VMware Cloud Console

The service activation link provided to you in the service welcome email directs you to the VMware Cloud Console.

Procedure

1. Click the service activation link that was provided to you in the service welcome email.

   You will be directed to the VMware Cloud Console.
2. Use the email and password from your My VMware account to log in.

   This account should also be either the Fund Owner or Fund User and have access to the SPP fund.

Add Organization Owners and Organization Users

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.

Procedure

- Read Chapter 2 Account Creation and Management.
- For more information on inviting a new user, see Invite a New User.
- For more information on accepting an account invitation, see Accept an Account Invitation.
- For more information on assigning roles to organization member, see Assign a VMC Service Role to an Organization Member.

Create a Subscription

Subscriptions allow you to save money by committing to buy a certain amount of capacity for a defined period. A subscription is not required to use VMware Cloud on AWS. Any usage of the service not covered by a subscription is charged at the on-demand rate for the region selected.

You can use your SPP fund to purchase a subscription. You would have agreed to the number of hosts, type of hosts, and term (1 year or 3 year subscription) during the sales process to determine the amount of SPP credit purchased.

Sales promotions or Hybrid Loyalty Program discounts are applied to your fund after the first billing cycle.

Contact your Cloud Sales Specialist if you are uncertain of what your company committed to in terms of hosts under subscription.

Procedure

- Read "Working with Payment Methods and Billing" at https://docs.vmware.com/en/VMware-Cloud-services/services/Using-VMware-Cloud-Services/GUID-81C8F89A-669C-40BC-9211-50DB25C322C7.html.
- Create your subscription by following the instructions at Chapter 3 Create a Subscription.

View Your Billing Information

Fund owners can view billing information for the active method of payment in the organization.

You can only view billing information if you are the fund owner.

Procedure

- To display your billing information in My VMware, click **Billing** on the VMware Cloud Services Console page, or on the menu, click the **VMware Cloud Services** icon and click **Billing**.

View the VMware Cloud on AWS Roadmap

VMware Cloud on AWS has a public that roadmap intended to provide guidance to customers regarding features that are Available, in Preview, in Active Development and testing and Planning.

Procedure

- Bookmark the VMware Cloud on AWS roadmap at https://cloud.vmware.com/vmc-aws/roadmap.

View the VMware Cloud on AWS Release Notes

VMware Cloud on AWS is able to release new features at a much faster pace that our traditional on premises software products. Check the release notes page frequently to keep updated on the new features that have been released.

Procedure

- Bookmark the VMware Cloud on AWS release notes page at https://docs.vmware.com/en/VMware-Cloud-on-AWS/0/rn/vmc-on-aws-relnotes.html.

Sign Up to Receive Service Alerts

The VMware Coud Operations team posts updates on planned maintenance events, maintenance start and end times, and service incidents on the VMware Cloud Services status page.

Procedure

- Bookmark the VMware Cloud Services Status page: https://status.vmware-services.io/.
- (Optional) Subscribe to receive real time alerts and updates.

Review the Service Level Agreement for VMware Cloud on AWS

The Service Level Agreement (SLA) for VMware Cloud on AWS defines the service components that have an availability commitment as well as their associated targets.

You may be eligible for an SLA credit if one of the service components is unavailable and breaches the target SLA. The amount of the SLA credit you may be eligible for depends on the monthly uptime percentage for the affected availability component.

Procedure

- Read and bookmark the Service Level Agreement for VMware Cloud on AWS document at https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/support/vmw-cloud-aws-service-level-agreement.pdf.
- If you are eligible for an SLA credit, file a support ticket by selecting **Support > Product Licensing**.

Account Creation and Management

2

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
- Invite a New User
- Accept an Account Invitation
- Assign a VMC Service Role to an Organization Member

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.

Assign a VMC Service Role to an Organization Member

Organization members are assigned organization roles and service roles. As an organization owner, you can change both kinds of role assignments for members of your organization.

Organization roles specify the privileges that an organization member has over organization assets. Service roles specify the privileges that an organization member has when accessing VMware Cloud Services that the organization uses. All service roles can be assigned and changed by a user with organization owner privileges, so restrictive roles such as Administrator (Delete Restricted) or NSX Cloud Auditor should be assigned along with the role of organization member to prevent modification.

When multiple service roles are assigned to an organization user, permissions are granted for the most permissive role. For example, if the Administrator (Delete Restricted) role is selected along with the Administrator role, a user will be able to delete SDDCs and clusters. To ensure proper enforcement of the role, organization owners should select only Administrator (Delete Restricted) to ensure that an organization member cannot delete an SDDC or cluster.

Procedure

1 On the VMware Cloud Services toolbar, click **Identity & Access Management**.

2 Select a user and click **Edit Roles** to open the **Edit Roles** page.

3 To assign an organization role, select a role name from the **Assign Organization Roles** drop-down control.

For information about Organization Roles, see Managing Users and Permissions in the *VMware Cloud Services* documentation.

4 To assign a VMC service role, select the **VMware Cloud on AWS** service name under **Assign Service Roles** and select a VMware Cloud on AWS service role to assign.

The following roles are available:

Administrator	This role has full cloud administrator rights to all service features in the VMware Cloud on AWS console.
Administrator (Delete Restricted).	This role has full cloud administrator rights to all service features in the VMware Cloud on AWS console but cannot delete SDDCs or clusters.
NSX Cloud Auditor	This role can view NSX service settings and events but cannot make any changes to the service.
NSX Cloud Admin	This role can perform all tasks related to deployment and administration of the NSX service.

5 Click **SAVE** to save your changes.

What to do next

Ensure that any users whose roles were changed log out and log back in for the changes to take effect.

Create a Subscription

3

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

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

Prerequisites

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

Procedure

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

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

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

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

Deploying and Managing a Software-Defined Data Center

4

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

There are a number of factors to consider before deploying your SDDC.

Connected AWS account

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

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

AWS VPC Configuration and Availability Requirements

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

- It must be in an AWS Availability Zone (AZ) where VMC resources are available. Start by creating a subnet in every AZ in the AWS Region where the SDDC will be created. That way, you can identify all the AZs where an SDDC can be deployed and select the AZ that best meets your SDDC placement needs, whether you want to keep your VMC workloads close to or isolated from your existing AWS workloads running in a particular AZ. See Creating a Subnet in Your VPC in the AWS documentation for information about how to use the Amazon VPC console to create a subnet in your VPC.
- The AWS account being linked must have sufficient capacity to create a minimum of 17 ENIs per SDDC in the region, although we recommend sufficient capacity for 32 ENIs per SDDC to support maximum scalability.

- If necessary, you can link multiple SDDCs to a VPC as long as the VPC subnet used for ENI connectivity has big enough CIDR block to accommodate them. We recommend a /26 CIDR block (33 IP addresses) per SDDC. At a minim, you need a /27 CIDR block (17 IP addresses) . You can also allocate a separate VPC subnet for each SDDC connection. You must ensure in all cases that the CIDR blocks for the SDDC and the VPC do not overlap.
- The subnet(s) used for the SDDC, as well as any subnets on which AWS services or instances communicate with the SDDC must all be associated with the VPC's main route table.
- The IP address range of the subnet must be unique within your enterprise network infrastructure. It cannot overlap the IP address range of any of your on-premises networks.

Note Workload VMs in the SDDC can communicate over the ENI connection with all subnets in the primary CIDR block of the connected VPC. VMC is unaware of other CIDR blocks in the VPC.

Single Host SDDC starter configuration for VMware Cloud on AWS

You can jump start your VMware Cloud on AWS experience with a Single Host SDDC starter configuration. This is a time-limited offering designed for you to prove the value of VMware Cloud on AWS in your environment. The service life of a Single Host environment is limited to 30 days. At any point during the service life of a Single Host SDDC, you can scale it up to a production configuration with three or more hosts with no loss of data. If you don't scale up the Single Host SDDC before the end of the service life, the SDDC is deleted along with all the workloads and data it contains.

Stretched Clusters for VMware Cloud on AWS

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

The following restrictions apply to stretched clusters:

- The linked VPC must have two subnets, one in each AZ in the cluster.
- You can't convert a stretched cluster to a single availability zone cluster, or vice versa.
- A given SDDC can contain either single availability zone clusters or stretched clusters, but not a mix of both.
- Currently, a given SDDC can contain only one stretched cluster.
- You need a minimum of six hosts (three in each AZ) to create a stretched cluster. Hosts must be added in pairs.

SDDC Networking

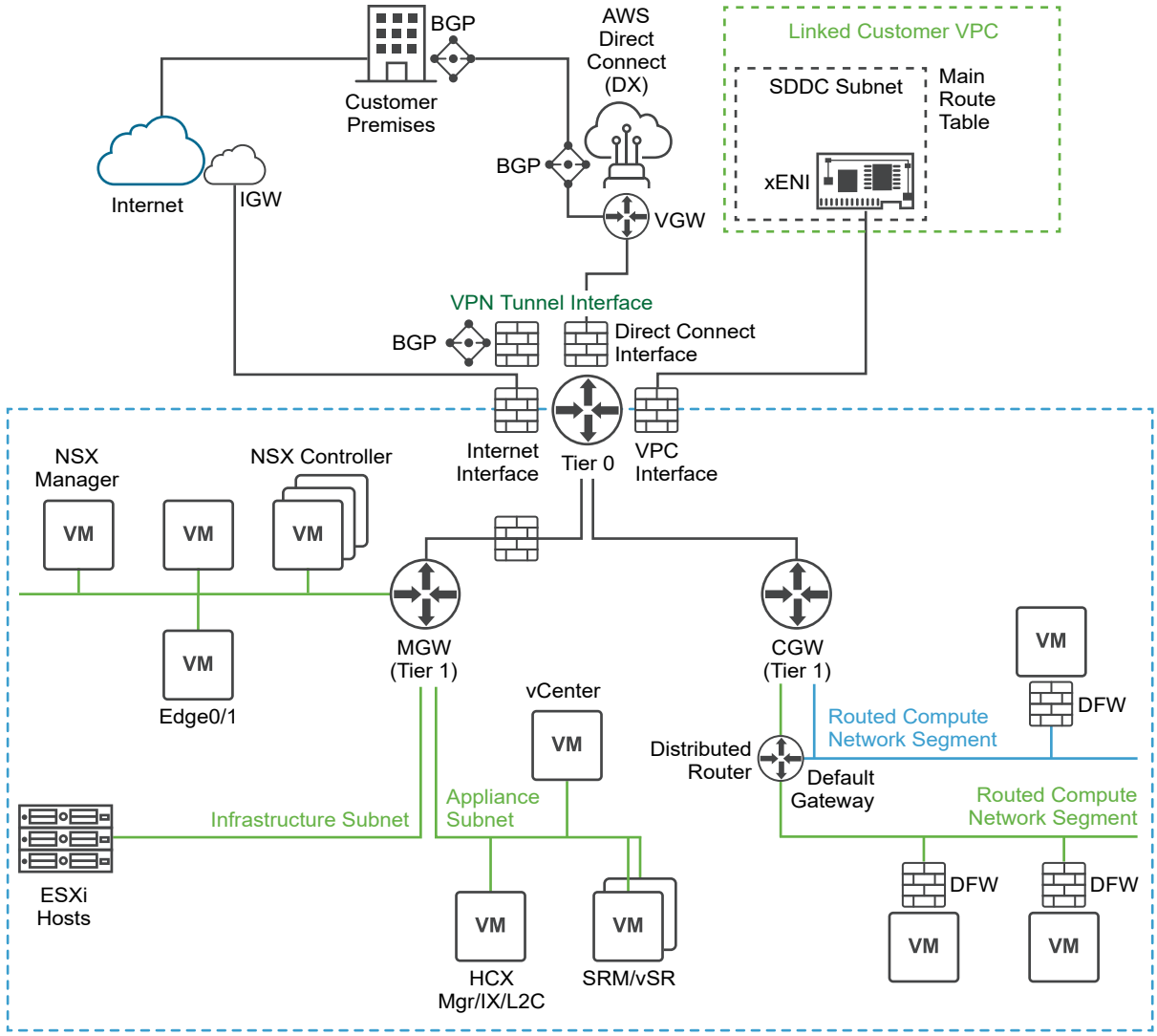
When you create an SDDC, it includes a Management Network and a Compute Network. The Management Network has two subnets:

Appliance Subnet	A subnet of the CIDR range you specified for the Management Subnet when you created the SDDC. This subnet is used by the vCenter, NSX, and HCX appliances in the SDDC. When you add appliance-based services such as SRM to the SDDC, they also connect to this subnet.
Infrastructure Subnet	A subnet of the CIDR range you specified for the Management Subnet when you created the SDDC. This subnet is used by the ESXi hosts in the SDDC.

The compute network can have up to 16 segments for your workload VMs. In a Single Host SDDC starter configuration, the compute network is created with one routed segment. In SDDC configurations that have more hosts, you'll have to create compute network segments to meet your needs.

A Tier 0 NSX Edge appliance sits between your on-premises networks and your SDDC networks, and routes traffic to either the management network or the compute network as appropriate.

Figure 4-1. SDDC Network Topology



Tier 0 Edge Appliance All traffic between your on-premises networks and the SDDC passes through this appliance. Compute Gateway firewall rules, which control access to workload VMs, are applied on its uplink interfaces.

Management Gateway (MGW) The MGW is an NSX Edge Security gateway that provides north-south network connectivity for the vCenter Server and other management appliances 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. Pick an address range (CIDR block) for the management subnet that can support the number of ESXi hosts in your

	SDDC. If you don't specify a range when you create the SDDC, the system uses a default of 10.2.0.0/16.
Compute Gateway (CGW)	The CGW provides north-south network connectivity for virtual machines running in the SDDC. In a single-node SDDC, VMware Cloud on AWS creates a default logical network segment (CIDR block 192.168.1.0/24) to provide networking for these VMs. You can create additional logical networks on the **Networking & Security** tab.

Before you can connect your on-premises network to your SDDC so you can migrate and run workload VMs in VMware Cloud on AWS, you'll need to configure, VPNs, firewall rules, AWS Direct Connect (optional) and other networking components. Chapter 6 Configure SDDC Networking and Security has more information about how to do that.

This chapter includes the following topics:

- Deploying a Single Host SDDC Starter Configuration
- Deploy an SDDC from the VMC Console
- View SDDC Information and Get Support

Deploying a Single Host SDDC Starter Configuration

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

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

The Single Host SDDC starter configuration is limited to a 30-day lifespan. You can scale up to the minimum 3-host purchase at any point before the 30-day period ends without losing any of your data. If you don't scale up the Single Host SDDC before the end of the service life, the SDDC is deleted along with all the workloads and data it contains.

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

- Accelerated on-boarding with expert support.
- Migration between on-premises and VMware Cloud on AWS using VMware Hybrid Cloud Extension for large-scale rapid migration, VMware vMotion for live migration, and cold migration.
- Disaster Recovery: Evaluate VMware Site Recovery, the cloud-based DR service optimized for VMware Cloud on AWS. VMware Site Recovery is purchased separately as an add-on service on a per-VM basis. Do not use the single host configuration for production disaster recovery, because this configuration has no SLA and data is lost in the event of a host failure.
- Hybrid Linked Mode support: Hybrid Linked Mode provides a single logical view of on-premises and VMware Cloud on AWS resources.

- All-Flash vSAN storage: An all-flash vSAN configuration, using flash for both caching and capacity, delivers maximum storage performance.
- Seamless, high-bandwidth, low-latency access to native AWS services such as EC2 and S3.

Single Host SDDCs have the following limitations.

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

Request Access and Create an Account

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

Procedure

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

   Important The email address you supply here must be a corporate email account. You cannot use an email address from a public email provider such as gmail.com, icloud.com, or others. For more information on how to update your My VMware profile, see https://kb.vmware.com/s/article/2086266.

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

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

What to do next

Ensure that you have met the prerequisites and then follow the steps in Chapter 4 Deploying and Managing a Software-Defined Data Center. Select **1** as the number of hosts in the SDDC.

Scale Up a Single Host SDDC Starter Configuration

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

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

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

Procedure

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

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

Deploy an SDDC from the VMC Console

Deploy an SDDC to host your workloads in the cloud.

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

Procedure

1. Log in to the VMC Console at https://vmc.vmware.com.
2. Click **Create SDDC**.

3 Configure SDDC properties.

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

The following regions are available:

- US West (Oregon)
- US East (N. Virginia)
- Europe (London)
- Europe (Frankfurt)
- Asia Pacific (Sydney)
- Asia Pacific (Tokyo)
- Europe (Ireland)
- US West (N. California)
- US East (Ohio)
- Asia Pacific (Singapore)
- Canada (Central)
- Europe (Paris)
- Asia Pacific (Mumbai)
- Asia Pacific (Seoul)
- South America (São Paulo)

b Select deployment options.

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

c Enter a name for your SDDC.

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

d Select the host type.

Option	Description
i3 (Local SSD)	Provision hosts with a fixed amount of local SSD storage per host.
R5 (EBS)	Provision hosts with EBS-based storage. When provisioning R5 hosts, you can select the storage capacity per host. This allows you to provision greater capacity for workloads requiring large storage capacities.

e If you selected R5 (EBS) hosts, select the storage capacity per host.

The value you select is used for all hosts in the cluster, including any hosts you add to the cluster after creation.

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

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

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

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

4 Connect to an AWS account.

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

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

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

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

- Choose a range of IP addresses that does not overlap with the AWS subnet you are connecting to. If you plan to connect your SDDC to an on-premises data center, the IP address range of the subnet must be unique within your enterprise network infrastructure. It cannot overlap the IP address range of any of your on-premises networks.
- If you are deploying a single host SDDC, the IP address range 192.168.1.0/24 is reserved for the default compute gateway logical network of the SDDC. If you specify a management network address range that overlaps with 192.168.1.0/24, the compute gateway logical network is created as 172.168.1.0/24. If you are deploying a full-scale SDDC, no compute gateway logical network is created during deployment, so you'll need to create one after the SDDC is deployed.

  In addition, CIDR blocks 10.0.0.0/15 and 172.31.0.0/16 are reserved for internal use. The management network CIDR block cannot overlap either of these ranges.
- CIDR blocks of size 16, 20, or 23 are supported. The primary factor in selecting a Management CIDR block size is the anticipated scalability requirements of the SDDC. If you intend to scale your SDDC beyond four hosts, consider using a /20 CIDR block. For CIDR blocks of size 20 or 16, the maximum number of hosts your SDDC can contain is limited to 160. Regardless of the number of AZs it occupies, an SDDC can have at most ten clusters with at most 16 hosts per cluster.

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

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

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

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

What to do next

After your SDDC is created, do the following:

- Configure a VPN connection to the management gateway.

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

View SDDC Information and Get Support

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

See Chapter 8 Get Help and Support for additional details on getting help and support.

Procedure

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

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

Tab	Description
Summary	Displays usage information. This tab does not always update immediately.
Networking & Security	Allows you to view and change networking for your SDDC. See VMware Cloud on AWS Networking and Security.
Settings	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.

Connect to vCenter Server

5

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

After your SDDC has been created, you can connect to the SDDC vCenter Server over the Internet or through a VPN. After adding a simple firewall rule to the Management Gateway, you can connect over the Internet as soon as your SDDC has been created. Later, after you have created a VPN, you can use it to connect to the SDDC vCenter Server instead of, or in addition to, connecting over the Internet.

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

Procedure

- To connect to vCenter Server over the Internet, click the **OPEN VCENTER** button on the SDDC card, then click **FIREWALL RULE** and add a rule like this one.

Source	**Any** or a public IP range you own.
Destination	vCenter (System-Defined Groups)
Services	HTTPS (TCP 443)

- If you have created a VPN and want to connect that way, click the **OPEN VCENTER** button on the SDDC card, then click **VPN**.
- (Optional) Open the **Settings** tab and select another method for connecting to vCenter Server.

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

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

Configure SDDC Networking and Security

6

To begin using VMware Cloud on AWS to run workloads in your SDDC, you'll need to set up a network connecting your on-premises data center to the SDDC. This network can include a dedicated connection over AWS Direct Connect, an IPSec VPN, or both.

While routing IPSec VPN traffic over Direct Connect can provide better performance at lower costs, you can start by setting up an IPSec VPN that connects to your SDDC over the Internet, then reconfigure that VPN to use Direct Connect later.

When you open the **Networking and Security** tab of a new SDDC, you can run the **Setup Networking and Security** wizard to guide you through the steps needed to configure Direct Connect and a VPN, access the vCenter in your SDDC, and change the default DNS server if you want to.

If you just want to set up a route-based VPN connecting your on-premises data center to your SDDC over the Internet, you can follow these steps.

Procedure

1 Create a Route-Based VPN

   A route-based VPN creates an IPsec tunnel interface and routes traffic through it as dictated by the SDDC routing table. A route-based VPN provides resilient, secure access to multiple subnets. When you use a route-based VPN, new routes are added automatically when new networks are created.

2 Create an On-Premises IPsec VPN

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

3 Create a Network Segment

   Network segments are logical networks for use by workload VMs in the SDDC.

4 Add or Modify Management Gateway Firewall Rules

   By default, the management gateway blocks traffic to all destinations from all sources. Add Management Gateway firewall rules to allow traffic as needed.

5 Configure Management Network Private DNS

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

Create a Route-Based VPN

A route-based VPN creates an IPsec tunnel interface and routes traffic through it as dictated by the SDDC routing table. A route-based VPN provides resilient, secure access to multiple subnets. When you use a route-based VPN, new routes are added automatically when new networks are created.

Route based VPNs in your VMware Cloud on AWS SDDC use an IPsec protocol to secure traffic and the Border Gateway Protocol (BGP) to discover and propagate routes as new networks are created. To create a route-based VPN, you configure BGP information for the local (SDDC) and remote (on-premises) endpoints, then specify tunnel security parameters for the SDDC end of the tunnel.

Procedure

1. Log in to the VMC Console at https://vmc.vmware.com.
2. Click **Networking & Security > VPN > Route Based**.
3. (Optional) Change the default local Autonomous System Number (ASN).

   All route-based VPNs in the SDDC use the same local ASN value in their implementation of BGP. It cannot be the same as the remote ASN for any configured VPN connections. The default value is 65000. To change this, click **EDIT LOCAL ASN**, enter a new value in the range 64521 to 65535, and click **APPLY**.
4. Click **ADD VPN** and give the new VPN a **Name**.
5. Select a **Local IP Address** from the drop-down menu.
   - If you have configured AWS Direct Connect for this SDDC and want the VPN to use it, select the private IP address.
   - Select the public IP address if you want the VPN to connect over Internet.
6. (Optional) If your on-premises gateway has a NAT address, enter that address as the **Remote Public IP**.

   This IP address must match the local identity (IKE ID) sent by the on-premises VPN gateway. If this field is empty, the **Remote Public IP** field is used to match the local identity of the on-premises VPN gateway.

7 For **BGP Local IP/Prefix Length**, enter the IP address, in CIDR format, of the local VPN tunnel.

Choose a network of size of /30 from the 169.254.0.0/16 subnet. The second and third IP addresses in this range are configured as the remote and local VTI (VPN Tunnel interfaces). For example, in the CIDR block 169.254.111.0/30 (address range 169.254.111.0-169.254.111.3), the local (SDDC) interface is 169.254.111.2/30 and the remote (on-premises) interface 169.254.111.1/30.

Note The following networks are reserved for internal use. The network you specify for **BGP Local IP/Prefix Length** must not overlap any of them.

- 169.254.0.2/28
- 169.254.10.1/24
- 169.254.11.1/24
- 169.254.12.1/24
- 169.254.13.1/24
- 169.254.101.253/30

8 For **BGP Remote IP**, enter the IP address of your on-premises VPN gateway.

9 For **BGP Remote ASN**, enter the ASN of your on-premises VPN gateway.

10 Configure **Advanced Tunnel Parameters**.

Option	Description
Tunnel Encryption	Select a Phase 2 security association (SA) cipher that is supported by your on-premises VPN gateway.
Tunnel Digest Algorithm	Select a Phase 2 digest algorithm that is supported by your on-premises VPN gateway. **Note** If you specify a GCM-based cipher for **Tunnel Encryption**, set **Tunnel Digest Algorithm** to **None**. The digest function is integral to the GCM cipher.
Perfect Forward Secrecy	Enable or Disable to match the setting of your on-premises VPN gateway. Enabling Perfect Forward Secrecy prevents recorded (past) sessions from being decrypted if the private key is ever compromised.
Preshared Key	Enter the preshared key string. The maximum key length is 128 characters. This key must be identical for both ends of the VPN tunnel.
IKE Encryption	Select a Phase 1 (IKE) cipher that is supported by your on-premises VPN gateway.
IKE Digest Algorithm	Select a Phase 1 digest algorithm that is supported by your on-premises VPN gateway. The best practice is to use the same algorithm for both the **IKE Digest Algorithm** and the **Tunnel Digest Algorithm**. **Note** If you specify a GCM-based cipher for **IKE Encryption**, set **IKE Digest Algorithm** to **None**. The digest function is integral to the GCM cipher. You must use IKE V2 if you use a GCM-based cipher .

Option	Description
IKE Type	■ Specify **IKE V1** to initiate and accept the IKEv1 protocol. ■ Specify **IKE V2** to initiate and accept the IKEv2 protocol. You must use IKEv2 if you have specified a GCM-based **IKE Digest Algorithm**. ■ Specify **IKE FLEX** to accept either IKEv1 or IKEv2 and then initiate using IKEv2. If IKEv2 initiation fails, IKE FLEX will not fall back to IKEv1.
Diffie Hellman	Select a Diffie Hellman group that is supported by your on-premises VPN gateway. This value must be identical for both ends of the VPN tunnel. Higher group numbers offer better protection. The best practice is to select group 14 or higher.

11 (Optional) Under **Advanced BGP Parameters**, enter a BGP **Secret** that matches the one used by the on-premises gateway.

12 Click **Save**.

The VPN creation process might take a few minutes. When the based VPN becomes available, the tunnel status and BGP session state are displayed. The following actions are available to help you with troubleshooting and configuring the on-premises end of the VPN:

- Click **DOWNLOAD CONFIG** to download a file that contains VPN configuration details. You can use these details to configure the on-premises end of this VPN.
- Click **VIEW STATISTICS** to view packet traffic statistics for this VPN.
- Click **VIEW ROUTES** to open a display of routes advertised and learned by this VPN.
- Click **DOWNLOAD ROUTES** to download a list of **Advertised Routes** or **Learned Routes** in CSV format.

What to do next

Create or update firewall rules as needed. To allow traffic through the route-based VPN, specify **VPN Tunnel Interface** in the **Applied to** field. The **All Uplinks** option does not include the routed VPN tunnel.

Create an On-Premises IPsec VPN

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

Prerequisites

Configuring an on-premises VPN requires the following:

- An on-premises router or firewall capable of terminating an IPsec VPN, such as Cisco ISR, Cisco ASA, CheckPoint Firewall, Juniper SRX, NSX Edge, or any other device capable of IPsec tunneling.

  Important The SDDC end of an IPSec VPN supports only time-based rekeying. Your on-premises device must disable lifebytes rekeying.

  Do not configure the on-premises side of the VPN to have an idle timeout (for example, the NSX **Session idle timeout** setting). On-premises idle timeouts can cause the VPN to become periodically disconnected.

- If your on-premises gateway is behind another firewall, you must configure that firewall to forward IPsec VPN protocol traffic:
  - Open UDP port 500 to allow Internet Security Association and Key Management Protocol (ISAKMP) traffic to be forwarded through the firewall.
  - Set IP protocol ID 50 to allow IPsec Encapsulating Security Protocol (ESP) traffic to be forwarded through the firewall.
  - Set IP protocol ID 51 to allow Authentication Header (AH) traffic to be forwarded through the firewall.

Procedure

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

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

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

Example: VPN Configuration File

```
# Configuration for IPsec VPN connection
#
# Peer NSX Edge and IPSec Site configuration details.
#
# IPsec site Id         : ipsecsite-17
# IPsec site name       : VPN1
# IPsec site description:
# IPsec site enabled    : true
# IPsec site vpn type   : Policy based VPN
# NSX Edge Id           : edge-1
# Feature version       : 45
```

```
# Time stamp            : 040618_182347GMT

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

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

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

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

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

What to do next

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

Create a Network Segment

Network segments are logical networks for use by workload VMs in the SDDC.

VMware Cloud on AWS supports three types of logical network segments: routed, extended and disconnected.

- A routed network segment (the default type) has connectivity to other logical networks in the SDDC and, through the SDDC firewall, to external networks.
- An extended network segment extends an existing L2VPN tunnel, providing a single IP address space that spans the SDDC and an on-premises network.
- A disconnected network segment has no uplink, and provides an isolated network accessible only to VMs connected to it. Disconnected segments are created when needed by HCX (see Getting started with VMware HCX). You can also create them yourself, and can convert them to other segment types.

A Single Host Starter SDDC is created with a single routed network segment named sddc-cgw-network-1. This network uses CIDR block 192.168.1.0/24, unless that conflicts with the CIDR block you chose for the SDDC management network. In that case, the default network uses CIDR block 172.10.1.0/24.

Multi-host SDDCs are not created with a default network segment, so you must create at least one for your workload VMs. You can use the VMC Console to create additional network segments or delete ones that are no longer in use.

When you create a network segment, ensure that it does not overlap your management network or any of the subnets in your connected Amazon VPC.

Procedure

1. Log in to the VMC Console at https://vmc.vmware.com.
2. Select **Networking & Security > Segments > Add Segments**.
3. Enter a **Name** for the segment.
4. Select a segment **Type** from the drop-down menu and configure the segment.

Type	Configuration
Routed	a Specify the CIDR block of the segment in the **Gateway/Prefix Length** field. b (Optional) Select **Enabled** to enable DHCP. Specify a DHCP IP Range and DNS Suffix such as example.com for the segment. VMs connecting to the segment get their IP addresses from the specified DHCP server and their FQDN has the specified suffix. 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.
Extended	Specify the ID of an existing L2VPN tunnel block of the segment in the **Tunnel ID** field.
Disconnected	Specify the CIDR block of the segment in the **Gateway/Prefix Length** field.

Note You cannot connect more than 1000 VMs to a network segment of any type.

5. Click **Save**.

   The system creates the requested segment. This operation can take up to 15 seconds to complete.

Add or Modify Management Gateway Firewall Rules

By default, the management gateway blocks traffic to all destinations from all sources. Add Management Gateway firewall rules to allow traffic as needed.

Prerequisites

Verify that management groups and services are configured. See Add a Management Group.

Procedure

1. Log in to the VMC Console at https://vmc.vmware.com.
2. On the **Networking & Security** tab, click **Gateway Firewall**.
3. On the **Gateway Firewall** card, click **Management Gateway**, then click **ADD NEW RULE**.
4. Enter the firewall rule parameters.

Option	Description
Rule Name	Enter a descriptive name for the rule.
Source	Click **Set Source** and enter or select one of the following options: Select **Any** to allow traffic from any source address or address range. Select **System Defined Groups** and select one of the following source options: ■ **ESXi** to allow traffic from your SDDC's ESXi hosts. ■ **NSX Manager** to allow traffic from your SDDC's NSX-T manager appliance. ■ **vCenter** to allow traffic from your SDDC's vCenter Server. Select **User Defined Groups** to use a management group that you have defined. See Add a Management Group.
Destination	Click **Set Destination** and enter or select one of the following options: Select **Any** to allow traffic to any destination address or address range. Select **System Defined Groups** and select one of the following destination options: ■ **ESXi** to allow traffic to your SDDC's ESXi management. ■ **NSX Manager** to allow traffic to your SDDC's NSX-T. ■ **vCenter** to allow traffic to your SDDC's vCenter Server.
Services	Select one of the following service types to apply the rule to: ■ Provisioning and Remote Console (TCP 902) applies only to the ESXi system-defined group as a **Destination**. ■ vMotion (TCP 8000). See Required Firewall Rules for vMotion. ■ HTTPS (TCP 443) applies only to vCenter Server system-defined group as a **Destination**. ■ ICMP (All ICMP) ■ SSO (TCP 7444) applies only to vCenter Serversystem-defined group as a **Destination**.

Option	Description
Action	The only action available for a management gateway firewall rule is **Allow**.
Logging	Enable or disable packet logging for this firewall rule. If enabled, the packet logs are forwarded to the Log Intelligence service. To access the logs, visit the Log Intelligence service console.

5 Click **PUBLISH** to create the rule.

Firewall rules are applied in order from top to bottom. Because there is always a default drop rule at the bottom, and the rules above are always **Allow** rules, rule order has no impact on traffic flow.

Example: Create a Firewall Rule

To create a firewall rule that enables vMotion traffic from the on-premises ESXi hosts to the ESXi hosts in the SDDC:

1 Create a management inventory group that contains the on-premises ESXi hosts that you want to enable for vMotion to the SDDC.

2 Create a management gateway rule with source ESXi and destination on-premises ESXi hosts.

3 Create another management gateway rule with source on-premises ESXi hosts group and destination ESXi with a vMotion service.

Add a Management Group

Management inventory groups contain managed SDDC infrastructure components and on-premises infrastructure components. You can use these groups in management gateway firewall policies.

Management inventory groups are created automatically for SDDC infrastructure components such as vCenter and NSX Manager. You can create additional management inventory groups by specifying the CIDR blocks to which group members are connected. For example, you could create an inventory group for ESXi hosts in the on-premises data center.

Procedure

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

2 Select **Networking & Security > Groups > Management Groups**.

3 Click **Add Group** and give the new group a **Name**.

4 In the **Members** column, enter one or more IP addresses in CIDR format specifying the subnets to which group members are connected.

Member Type must be an IP Address. Separate multiple addresses with commas.

5 Click **Save** to create the group.

Configure Management Network Private DNS

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

To use features such as migration with vMotion, cold migration, or Hybrid Linked Mode, swtich the vCenter Server resolution to a private IP address resolvable from the VPN.

Prerequisites

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

Procedure

1. Specify the DNS server addresses.

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

2. Choose a scope for DNS name resolution.

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

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

Deploy Workload VMs 7

Now that you've created a route-based VPN and a compute network segment, you're ready to deploy workload VMs in your VMware Cloud on AWS SDDC.

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

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

This chapter includes the following topics:

- Use the Content Onboarding Assistant to Transfer Content to Your SDDC
- Deploy a Virtual Machine from a .vmtx Template
- Assign a Public IP Address to a VM
- Enable Access to the Virtual Machine Remote Console

Use the Content Onboarding Assistant to Transfer Content to Your SDDC

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

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

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

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

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

Prerequisites

Before you run Content Onboarding Assistant, do the following:

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

Procedure

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

   `.vmtx` templates need no special preparation.

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

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

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

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

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

Parameter	Description
`onpremServer` *`server`*	The host name of the vCenter Server for your on-premises data center.
`onpremInfraServer` *`psc-server`*	The host name of the on-premises Platform Services Controller. This is optional for embedded configurations.
`onpremUsername` *`username`*	The user name used to log in to the on-premises vCenter Server.

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

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

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

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

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

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

7 Select how to transfer your `.vmtx` templates.

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

The Content Onboarding Assistant does the following:

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

What to do next

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

Deploy a Virtual Machine from a .vmtx Template

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

Procedure

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

Assign a Public IP Address to a VM

You can request a public IP address to a VM to make it available on the public Internet.

Procedure

1. Log in to the VMC Console at https://vmc.vmware.com.
2. Click **View Details** on the SDDC card.
3. Click **Networking & Security**.
4. Click **Public IPs** in the **System** category to open the Public IPs page.
   a. Click **REQUEST NEW 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.

What to do next

If you want the public address of the VM to be hidden by network address translation (NAT), see Configure NAT Settings in *VMware Cloud on AWS Networking and Security*. If you want to create firewall rules that manage network traffic to and from the VM, see Set NSX Edge Compute Gateway Firewall Rules , also in *VMware Cloud on AWS Networking and Security*.

Enable Access to the Virtual Machine Remote Console

To access the Virtual Machine Remote Console (VMRC) on VMs in your cloud SDDC, ensure that you have configured a management gateway firewall rule that allows access to ESXi on port 902.

Prerequisites

Your on-premises data center must have connectivity to the SDDC via Direct Connect or a VPN before you can use VMRC.

Procedure

1. Log in to the VMC Console at https://vmc.vmware.com.
2. Click **View Details** on the SDDC card.
3. Click **Networking & Security**.
4. Under **Gateway Firewall**, click **Add New Rule** and create a rule to enable access to ESXi on port 902.

Option	Description
Source	IP address or CIDR block, either public or from a connected on-premises data center.
Destination	Select ESXi under **System Defined Groups**.
Services	Provisioning and Remote Console (TCP 902)

Get Help and Support

8

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

Procedure

1 Before you contact VMware for support, have the support information for your SDDC ready.

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

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

   c Click **Support** to view the support information.

2 Select a method for getting help or support.

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