

VMware Cloud on AWS Getting Started

19 October 2023

SDDC Version 1.22

VMware Cloud on AWS

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

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

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

Copyright © 2017-2023 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

Contents

Getting Started With VMware Cloud on AWS	5
1 Purchase Options for VMware Cloud on AWS	6
2 VMware Cloud on AWS: Advanced Edition	8
4 Onboarding Checklist for Purchasing Through VMware	12
Use the Launchpad	13
Read Your Service Welcome Email	14
Update Your VMware Customer Connect Account	14
View Your Subscription Purchase Program Fund	15
Log into the VMware Cloud Console	15
Add Organization Owners and Organization Users	16
Create a Subscription	16
View Your Billing Information	16
View the VMware Cloud on AWS Roadmap	17
View the VMware Cloud on AWS Release Notes	17
Sign Up to Receive Service Alerts	17
Review the Service Level Agreement for VMware Cloud on AWS	17
5 Onboarding Checklist for Purchasing through AWS	19
6 Account Creation and Management	22
Creating an Account	22
Create an Organization Owner Account with a Customer Connect Account	22
Create an Organization Owner Account Without a Customer Connect Account	23
Invite a New User	24
Accept an Account Invitation	24
Assign Roles to an Organization Member	25
7 Browser Support in VMware Cloud on AWS	27
8 Create a Subscription for VMware Cloud on AWS	28
Exchange a Subscription	30
9 Deploying and Managing a Software-Defined Data Center	31
Deploying a Single Host SDDC Starter Configuration	35
Request Access and Create an Account	36

Scale Up a Single Host SDDC Starter Configuration	36
Deploy an SDDC from the VMC Console	37
Choosing a Region	41
AWS Region and Availability Zone Support	41
View SDDC Information and Get Support	43
Set the Language and Regional Format for the VMware Cloud Console	44
10 Connect to vCenter Server	46
11 Configure SDDC Networking and Security	48
12 Deploy Workload VMs	50
Use the Content Onboarding Assistant to Transfer Content to Your SDDC	50
Deploy a Virtual Machine from a .vmtx Template	53
Assign a Public IP Address to a VM	53
Access the Virtual Machine Remote Console	54
13 Get Support	56

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* 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, take a look at the VMware Cloud on AWS [Launchpad](#) and the [VMware Cloud Tech Zone](#) for tips that can help you configure deploy your new SDDC environment quickly and correctly.

Purchase Options for VMware Cloud on AWS

1

You have multiple options for purchasing VMware Cloud on AWS.

Purchasing from different sources results in a different seller of record being associated with the resources you purchase. The seller of record is responsible for billing the resources purchased from them. The seller of record also determines attributes such as payment types, terms of service, catalogue, region, and currency. Multiple options allow you to select the best seller attributes for your organization.

You can have more than one seller of record in an Organization. For example, if you currently have an Organization containing SDDCs through VMware, and you want to purchase additional SDDCs through AWS, you can add AWS as a seller of record to allow you to add those SDDCs. You can do the reverse for an Organization containing SDDCs purchased from AWS to allow you purchase SDDCs and additional services sold by VMware. To add another seller of record, contact your Account Executive for assistance.

Purchase Through VMware

When you purchase VMware Cloud on AWS through VMware:

- VMware is the seller of record.
- Billing is done by VMware.
VMware terms of service, payment methods, currencies, regions, discounts, and pricing apply.
- You deploy and manage your VMware Cloud on AWS infrastructure through the VMware Cloud Console.

For more information on purchasing VMware Cloud on AWS through VMware, go to <https://cloud.vmware.com/vmc-aws>.

Purchase Through AWS

When you purchase VMware Cloud on AWS through AWS:

- AWS is the seller of record.

- Billing is done by AWS. Through this purchase model, the payment instruments, terms of service, region, currency, and so on, are determined by your relationship with AWS and the Enterprise Discount Program (EDP) credits that you purchased through them. Contact your AWS sales team for all questions related to pricing and billing.
- You deploy and manage your VMware Cloud on AWS infrastructure through the VMware Cloud Console.

Table 1-1. Service and Feature Support for Purchasing Through AWS

	Currently Supported
Services	<ul style="list-style-type: none"> ■ Core VMware Cloud on AWS ■ VMware Cloud on AWS: Advanced edition ■ NSX Advanced Firewall ■ VMware Aria Automation ■ VMware Aria Operations ■ VMware Aria Operations for Logs ■ VMware Aria Operations for Networks ■ VMware Site Recovery ■ VMware Cloud Disaster Recovery ■ VMware Cloud on AWS Outposts
Purchasing Features	<ul style="list-style-type: none"> ■ Purchases with 1 year and 3 year term paid upfront ■ Purchases using monthly recurring billing ■ Purchases using Flexible Subscriptions
Purchasing Methods	<ul style="list-style-type: none"> ■ Purchases of SDDCs in a new Organization directly through AWS ■ Purchases through AWS for MSPs

For more information on purchasing through AWS, go to <https://aws.amazon.com/vmware/>.

Purchase Through a Managed Service Provider

When you purchase through a managed service provider (MSP), the MSP handles billing, support, deployment, and management of your VMware Cloud on AWS infrastructure. Consult your MSP for more information.

VMware Cloud on AWS: Advanced Edition

2

VMware Cloud on AWS now offers VMware Cloud on AWS: Advanced. This edition offers additional capabilities compared to the original VMware Cloud on AWS offering.

Currently, VMware Cloud on AWS: Advanced is available when purchasing through VMware or through AWS as the seller of record.

VMware Cloud on AWS: Advanced

VMware Cloud on AWS: Advanced includes vSphere, vSAN, NSX, VMware Aria Automation , and VMware Aria Operations.

VMware Cloud on AWS: Advanced is available with all regions and host types.

VMware Cloud on AWS Trial

3

The free trial program is offered only to selected VMware customers who are ready to migrate to the public cloud.

The eligibility criteria for the trial are as follows:

- The trial is only available to net new VMware Cloud on AWS accounts.
- The trial is available through both VMware Sales and VMware channel partners.
- The trial is globally available for all geographical regions.

For more information, see the [program FAQ](#).

When you are invited to the trial, you receive a welcome email with a trial activation link. The terms of the trial are as follows:

- When you click the activation link, you are asked to sign up or log in to VMware Cloud services. You are also asked to provide a payment method during onboarding. You are not charged during the trial period unless you consume services not included in the VMware Cloud on AWS Trial program. After you complete the onboarding steps and access the VMware Cloud Console, your trial is activated.
- The activation link for the trial can only be redeemed once. The trial is not tied to your email address, and you can forward the link to a partner or colleague for activation if needed.
- During the trial, you receive full access to the service console and to SDDC resources with i3.metal or i4i hosts. Refer to your welcome email for the number of SDDCs and hosts you can create during your trial. You can manage your workloads through vCenter Server and manage your network settings through NSX Manager.
- You can convert to paid usage any time during or after the trial by clicking the [convert to paid usage](#) button in the VMware Cloud console. Once you convert to paid usage, you pay for the hosts at the on-demand rate by default, but you can purchase a 1 or 3 year host subscription to get a better rate.
- If you don't convert to paid usage during your trial, you lose admin access to the VMware Cloud Console and access to your workloads when the trial period ends. After your trial period ends, your SDDC is deactivated for a number of days. By default this period is 7 days. Refer to your welcome email for the exact time period of this deactivation. During these days, you can still convert to paid usage to regain access to your SDDC and workloads. If you don't convert by the end of this period, your SDDC is deleted and your data is lost.

- Before you convert to paid usage, the costs that you incur with your VMware Cloud on AWS Trial are free, including Elastic IP, data transfer, bandwidth cost between VMware Cloud and AWS, and NSX Advanced Firewall.
- The trial program only applies to the VMware Cloud on AWS service. You are charged for any other services you consume, such as VMware Cloud on Dell, Aria services, VMware Cloud Disaster Recovery, VMware Site Recovery, and so on. If you consume any AWS native services, you are charged separately through AWS.
- • If you leverage Direct Connect, SDDC Groups, or Transit Connect during the trial period, you may incur additional costs through your VPC account in AWS that will be billed by AWS to you directly. These include the cost for private VIF for Direct Connect or Transit VIF and any transfer costs for data sent from your environment to VMC through an SDDC group (through Direct Connect, VPC, or Transit Connect). In addition, any attachment charges for connections to an SDDC group are also charged directly from AWS to you. See the pricing pages for [Transit Connect](#) and [Direct Connect](#) on AWS for more information.
- The following features are not available as part of the trial:
 - Term commitment (1 or 3 year subscription) purchase
 - host types that are not available as part of the trial program
 - adding additional hosts beyond your trial host count
 - Elastic DRS
 - Microsoft SPLA licensing
 - free access to some VMware services, including Aria and Tanzu
- VMware reserves the right to change the trial offer, including changing the offering details and the duration of the program.

If you activate the trial through the activation link that was sent to you, you indicate that you agreed to all the preceding terms.

You can also choose to activate trials for Aria services on top of the VMware Cloud on AWS Trial.

- VMware Aria Operations: Enable the trial through the **Integrated Services** tab in your **SDDC Details** page. Note that the VMware Aria Operations instance will default to US. You can reach out to chat support in the VMware Cloud Console if you need to migrate the instance to another region of choice. For more information, see [Activation of VMware Aria Operations for VMware Cloud on AWS](#).
- VMware Aria Automation : Enable the trial through the **Integrated Services** tab in your **SDDC Details** page. Note that the VMware Aria Automation instance will default to US. You can reach out to chat support in the VMware Cloud Console if you need to migrate the instance to another region of choice.

- VMware Aria Operations for Logs: After you create your first SDDC, the service is accessible through Cloud Services Console. Click **Start Trial** to get started. Alternatively, you can click on the **Start Free Trial** button of the Cloud Management solution in the VMware Cloud Console Launchpad. Note that the VMware Aria Operations for Logs instance will default to US. Email help-vrlic@vmware.com if you need to migrate the instance to another region of choice. For more information, see [Getting Started Checklist for VMware Aria Operations for Logs \(SaaS\)](#)

If you would like to contact sales to discuss purchase options, [submit your request here](#). If you have questions anytime during your trial, reach out to chat support in the VMware Cloud Console to get real-time help. To log in to the VMware Cloud Console, click <https://vmc.vmware.com/home>.

Onboarding Checklist for Purchasing Through VMware

4

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).

The process in this checklist applies to purchases made through VMware. If you purchased VMware Cloud on AWS through AWS, see [Chapter 5 Onboarding Checklist for Purchasing through AWS](#).

Procedure

1 Use the Launchpad

The VMware Cloud Launchpad is a consolidated starting point designed to help you learn about the latest VMware Hybrid Cloud solutions and infrastructure providers.

2 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.

3 Update Your VMware Customer Connect Account

Prior to logging in to the VMware Cloud Console, ensure that your Customer Connect 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.

4 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.

5 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.

6 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.

7 [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.

8 [View Your Billing Information](#)

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

9 [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.

10 [View the VMware Cloud on AWS Release Notes](#)

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

11 [Sign Up to Receive Service Alerts](#)

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

12 [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.

Use the Launchpad

The VMware Cloud Launchpad is a consolidated starting point designed to help you learn about the latest VMware Hybrid Cloud solutions and infrastructure providers.

The Launchpad provides technical details on how you can use VMware products and solutions to achieve business outcomes. The Launchpad is available to anyone, whether or not you are logged in to VMware Cloud on AWS. It includes detailed technical information, relevant tools, and tested workflows for VMware Hybrid Cloud solutions and infrastructure. Launchpad content includes these categories:

Overview

The Overview typically consists of a short video or image that provides a technical overview of the offering followed by additional details and diagrams covering the architecture and technical capabilities.

Journey

The Journey page helps you envision your end-to-end journey with VMware for the offering. The Journey typically consists of three or more stages, structured to help you achieve these key objectives:

- 1 Learn about the offering and prepare your environment.
- 2 Deploy the offering.
- 3 Configure the offering to maximize its capabilities and value.

For some offerings, the Journey also enables you to track and monitor your progress.

Resources

The Resources page includes links to technical documents, including white papers, solution briefs, and reference architectures, along with videos, FAQs and other documents that can help you understand the technical details of the offering and its underlying technologies.

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 welcome 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 VMware Customer Connect Account

Prior to logging in to the VMware Cloud Console, ensure that your Customer Connect 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 Customer Connect profile. In addition, spell out the name of your state in full. For example, enter **California** rather than **CA**.

Procedure

- ◆ To log in to Customer Connect, go to <https://my.vmware.com>.
- ◆ For more information on updating your Customer Connect profile, see <https://kb.vmware.com/s/article/2086266>.
- ◆ For more information on resetting your Customer Connect password, see <https://kb.vmware.com/s/article/2013963>.

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 Customer Connect: <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/82431>.
- ◆ 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 Customer Connect 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 6 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 Roles 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 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](#).
- ◆ Create your subscription by following the instructions at [Chapter 8 Create a Subscription for VMware Cloud on AWS](#).

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 Customer Connect, 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://www.vmware.com/products/vmc-on-aws/features-and-roadmaps.html>.

View the VMware Cloud on AWS Release Notes

VMware Cloud on AWS is able to release new features at a much faster pace than 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/services/rn/vmware-cloud-on-aws-release-notes/index.html>.

Sign Up to Receive Service Alerts

The VMware Cloud 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**.

Onboarding Checklist for Purchasing through AWS

5

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).

The process in this checklist applies to purchases made through AWS. If you purchased VMware Cloud on AWS through VMware, see [Chapter 4 Onboarding Checklist for Purchasing Through VMware](#).

Read Your Welcome Email

During the process of purchasing VMware Cloud on AWS, you specified email contacts for your Organization on the order form submitted to AWS. After the purchase is processed, AWS sends a welcome email to the email addresses specified.

The welcome email is sent from no-reply-vmware-cloud-on-aws@amazon.com. 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.

- 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 do not already have a VMware Cloud services account, you are prompted to create one.

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.

- 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 VMware Cloud account to log in.

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.

- Read [Chapter 6 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 Roles 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.

Create your subscription by following the instructions at [Chapter 8 Create a Subscription for VMware Cloud on AWS](#). Note that the pricing presented in the VMware Cloud Console does not accurately present pricing when AWS is the seller of record. Consult the AWS Console for your billing information for VMware Cloud on AWS.

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.

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 than our traditional on-premises software products. Check the release notes page frequently to keep updated on the new features that have been released.

Bookmark the VMware Cloud on AWS release notes page at <https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/rn/vmware-cloud-on-aws-release-notes/index.html>.

Sign Up to Receive Service Alerts

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

- 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.

- 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

6

VMware Cloud accounts are based on an Organization, which corresponds to a group or line of business subscribed to VMware Cloud 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 Members, who can use and manage cloud services belonging to the Organization, but cannot invite new users.

Both types of accounts are linked to a Customer Connect account.

Read the following topics next:

- [Creating an Account](#)
- [Invite a New User](#)
- [Accept an Account Invitation](#)
- [Assign Roles 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 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 Customer Connect Account

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

If you don't have a Customer Connect 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 Customer Connect account, and click **Next**.
- 3 Enter the password associated with your Customer Connect 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 Customer Connect credentials.
- 6 If you are not automatically redirected to the VMware Cloud Console, go to <https://vmc.vmware.com> and log in.

Create an Organization Owner Account Without a Customer Connect Account

If you do not already have a valid Customer Connect 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 Customer Connect credentials.

- 8 If you are not automatically redirected to the VMware Cloud Console, go to <https://vmc.vmware.com> and log in.

Invite a New User

As an Organization Owner or Organization Administrator, you can invite additional users as Organization Members to 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.

See [Assign Roles to an Organization Member](#) for more information about VMware Cloud on AWS service roles.

Procedure

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



- 2 Click the services icon () at the top right of the window, and select **Identity & 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 Assign a VMware Cloud Services Organization role to the new user.

See [What Organization roles are available in VMware Cloud Services](#) for the list of VMware Cloud Services Organization roles and their privileges.

- 6 Click **Add**.

Results

Invitation emails are sent to the invited users. They can use the link in the email to activate their accounts.

Accept an Account Invitation

After an Organization Owner has invited you to their organization in VMware Cloud, 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 Customer Connect account associated with your email	Enter your email address and Customer Connect password, and click Log In .
If you do not already have a Customer Connect 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 VMware Cloud Console, go to <https://vmc.vmware.com> and log in.

Assign Roles 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 member, permissions are granted for the most permissive role. For example, when an organization member who has both the Administrator role and the Auditor role, the more permissive Administrator permissions apply.

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.

Every organization member must have at least one the **Mandatory Roles** and can have zero or more of these **Additional Roles**.

Table 6-1. Organization Roles

Role Name	Rights in this Role
Access Log Auditor	Access log auditors have read-only access to VMware Cloud Services audit records for this SDDC.
Billing Read-only	Billing Read-only users can view but not modify billing information such as invoices and subscriptions,for one Organization.
Developer	Developers can create and manage OAuth apps to authorize the third-party apps they build to access protected resources.

Table 6-1. Organization Roles (continued)

Role Name	Rights in this Role
Project Administrator	Project administrators have full administrative access to projects to which they have been assigned. They can edit and manage access to the project and its resources.
Software Installer	Software installers can access and download additional software binaries and packages available for services in the organization.
Support User	Support users can access and file support requests to VMware. See How do I get support.

For more information about organization roles, see [Managing Users and Permissions](#) in the *VMware Cloud Services* documentation.

4 Assign a VMware Cloud on AWS service role.

Select the **VMware Cloud on AWS** service name under **Assign Service Roles** and select one or more VMware Cloud on AWS service roles from the drop-down control. The following VMware Cloud on AWS service roles are available:

Table 6-2. VMware Cloud on AWS Service Roles

Role Name	Rights in this Role
Administrator	Full cloud administrator rights to all VMware Cloud on AWS service features.
NSX Cloud Admin	Perform all tasks related to deployment and administration of the NSX service.
Administrator (Delete Restricted)	Full cloud administrator rights to all VMware Cloud on AWS service features but cannot delete SDDCs or clusters.
NSX Cloud Auditor	View NSX service settings and events but cannot make any changes to the service.

5 (Optional) Assign an NSX service role.

Administrative access to the VMware Cloud Console legacy **Networking & Security** tab requires both a VMware Cloud on AWS service role and an NSX service role.

See [Assign NSX Service Roles to Organization Members](#) for more information about NSX service roles.

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

What to do next

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

Browser Support in VMware Cloud on AWS

7

Confirm that your browsers support the VMware Cloud Console.

You can access the VMware Cloud Console with the most recent release (or its predecessor release) of any of these browsers.

- Microsoft Edge
- Mozilla Firefox
- Google Chrome

Note Verify that the browser you use to access VMware Cloud on AWS allows the use of WebSockets.

Create a Subscription for VMware Cloud on AWS



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.

You cannot cancel, convert, or modify an ordinary subscription after you have ordered it. If you choose a flexible subscription, you can exchange the remaining value of that subscription for another subscription at a future date. Pricing for this option includes a flexibility surcharge. Flexible subscriptions are subject to the following limitations:

- Flexible subscriptions are available with upfront payment terms only, and cannot be paid on a monthly basis. They can also be exchanged only for other upfront subscriptions.
- Flexible subscriptions are currently available only when purchasing through VMware and AWS. They are not available when purchasing through MSPs.
- You can't exchange only part of a flexible subscription. The entire subscription must be exchanged.
- If the remaining value of your flexible subscription is greater than the value of the new subscription you are exchanging it for, you will not receive a refund on the difference.
- Flexible subscriptions are available for i3, i3en, and i4i hosts.

If you purchased through AWS, you do not see details of the subscription pricing in the VMware Cloud Console. Pricing is determined by your agreement with AWS. For more information, see [Chapter 1 Purchase Options for VMware Cloud on AWS](#).

Prerequisites

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

Procedure

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

2 Click **Subscriptions** (.

3 Click **Create Term Commitment** and select **VMware Cloud on AWS**.

- 4 Select whether you want to purchase capacity on the basis by specifying a number of hosts to purchase or a number of workloads to protect with site recovery.

Option	Description
Host Capacity	<p>Select Host Capacity to select a term commitment based on purchasing hosts for provisioning of SDDCs.</p> <ul style="list-style-type: none"> a Select the region in which the subscription applies. b Select the host type. c Select the number of hosts you want as part of the subscription. <p>The total number of subscribed hosts cannot be more than the maximum allowed for your organization.</p>
Site Recovery	<p>Select Site Recovery to select a term commitment based on protecting a specified number of on-prem workloads.</p> <ul style="list-style-type: none"> a Select the region in which the subscription applies. b Specify the number of VMs to protect under this subscription.

- 5 Select the software edition.

VMware Cloud on AWS: Advanced includes vSphere, VSAN, NSX, VMware Aria Automation , and VMware Aria Operations.

- 6 Click **NEXT** to choose subscription terms.

- 7 Select whether you want the flexibility to change your subscription.

Choosing flexibility gives you the option to exchange your term commitment for another full term commitment at a future date:

- You can exchange a flexible VMware Cloud Foundation term commitment for a VMware Cloud on AWS or VMware Cloud on Dell EMC term commitment.
- You can exchange a flexible VMware Cloud on AWS term commitment for another VMware Cloud on AWS term commitment that includes a different number of hosts, host types, a different region, or a different time period.

Pricing for this option includes a flexibility surcharge. To exchange your subscription, contact customer success or support.

8 Select a payment term and click **NEXT**.

Option	Description
On-Demand	Select this option to have your usage charged on an hourly basis based on consumption.
1 Year	<p>Select a 1 year subscription term. For VMware Cloud on AWS select one of the following options:</p> <ul style="list-style-type: none"> ■ Select Pay Upfront to pay for the entire term in a single payment upfront. ■ Select Pay Monthly to pay for the term in monthly installments. You will be charged the monthly fee regardless of host usage. This option is not available for flexible subscriptions.
3 Year	<p>Select a 3 year subscription term with one of the following options:</p> <ul style="list-style-type: none"> ■ Select Pay Monthly to pay for the term in monthly installments. You will be charged the monthly fee regardless of host usage. This option is not available for flexible subscriptions.

9 Review the summary and click **PLACE ORDER**.

Results

You receive a notification email indicating that your subscription order has been received. After the order has been processed, you 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.

Exchange a Subscription

If you purchased a flexible subscription, you can exchange that subscription to change the number or type of hosts, region, and term.

Procedure

- 1 Log in to the VMware Cloud Console at <https://vmc.vmware.com>.
- 2 Click the Subscriptions tab.
- 3 Select **Actions > Exchange Subscriptions**.
- 4 Click the link to download the Microsoft Excel file and fill out your subscription information.
- 5 Click **Open a Support Ticket** to open a support ticket and attach the spreadsheet you filled out.

Results

After the support ticket is processed, your original subscription will be canceled and your new subscription activated. Note that the subscription exchange impacts your financial commitment only and will not affect currently running workloads. You might be subject to on-demand charges if your new subscription does not cover your current workloads.

Deploying and Managing a Software-Defined Data Center

9

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

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

Connected AWS Account

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

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

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

AWS VPC Configuration and Availability Requirements

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

- The subnet must be in an AWS Availability Zone (AZ) where VMware Cloud on AWS is available. Start by creating a subnet in every AZ in the AWS Region where the SDDC will be created. It helps you identify all AZs where an SDDC can be deployed and select the one that best meets your SDDC placement needs, whether you want to keep your VMC workloads close to or isolated from your AWS workloads running in a particular AZ. See [Creating a Subnet in Your VPC](#) in the AWS documentation for information about how to use the Amazon VPC console to create a subnet in your VPC.
- The subnet must exist in the connected AWS account. It cannot be one owned by and shared from another account.

- The AWS account being linked must have sufficient capacity to create a minimum of 17 ENIs per SDDC in each region where an SDDC is deployed. Although you cannot provision more than 16 hosts in a cluster, SDDC operations including planned maintenance and Elastic DRS can require us to temporarily add as many as 16 more hosts, so we recommend using an AWS that has sufficient capacity for 32 ENIs per SDDC per region.
- We recommend dedicating a /26 CIDR block to each SDDC and not using that subnet for any other AWS services or EC2 instances. Because some of the IP addresses in this block are reserved for internal use, a /26 CIDR block is the smallest subnet that can accommodate SDDC IP address requirements.
- By default, AWS services or instances that communicate with the SDDC must be on VPC subnets associated with the main route table of the connected VPC. To use a custom route table, enable AWS Managed Prefix List Mode. See [Enable AWS Managed Prefix List Mode](#) for more information. By default, AWS limits the size of the main route table to 50 routes. Because the main route table must accommodate an entry for each routed SDDC network segment as well as the management network CIDR and any additional routes you create directly in your AWS account, the default limit might not be adequate for your SDDC networks, especially if you connect more than one SDDC to the VPC. You can request a route table size increase as described in [Amazon VPC quotas](#).
- If necessary, you can link multiple SDDCs to a VPC if the VPC subnet used for ENI connectivity has a large enough CIDR block to accommodate them. Because all SDDCs in a VPC use the same main route table, make sure that network segments in those SDDCs do not overlap with each other or the VPC's primary CIDR block. Workload VMs on routed SDDC networks can communicate with all subnets in the VPC's primary CIDR block, but are unaware of other CIDR blocks that might exist in the VPC.

AWS Elastic IP Requirements

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

Table 9-1. Core EIP Usage

Usage	Description
Management	Provides VMware support with access to your SDDC.
Management Gateway (MGW) SNAT	Provides the SNAT address for traffic egressing the MGW to the Internet.

Table 9-1. Core EIP Usage (continued)

Usage	Description
Compute Gateway (CGW) SNAT	Provides the default SNAT address for traffic egressing the CGW to the Internet.
vCenter Server Public IP	Provides the IP address used for vCenter Server when the vCenter FQDN is set to Public IP . See Set vCenter Server FQDN Resolution Address . This EIP is always consumed, even if you set the vCenter FQDN to Private IP .

Single Host SDDC starter Configuration for VMware Cloud on AWS

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

Stretched Clusters for VMware Cloud on AWS

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

The following restrictions apply to stretched clusters:

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

You can find more information about stretched clusters in the VMware Cloud Tech Zone article [VMware Cloud on AWS: Stretched Clusters](#). For limitations that affect all stretched clusters, see [VMware Configuration Maximums](#). Additionally, large-sized SDDC appliances are not supported with two-host stretched clusters.

Connecting to the SDDC and Configuring SDDC Networks

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

Custom Core Counts

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

Credit Card Payments

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

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

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

Read the following topics next:

- [Deploying a Single Host SDDC Starter Configuration](#)
- [Deploy an SDDC from the VMC Console](#)
- [View SDDC Information and Get Support](#)
- [Set the Language and Regional Format for the VMware Cloud Console](#)

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 60-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. Subscriptions cannot be used to cover the cost of a Single Host SDDC starter configuration.

The Single Host SDDC starter configuration is limited to a 60-day lifespan. You can scale up to the minimum 2-host purchase at any point before the 60-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.
- Single Host SDDCs are charged on an on-demand basis only. Subscriptions cannot be used to pay for a Single Host SDDC.

- A Single Host SDDC cannot use the i3en host type.

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 Customer Connect 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 Customer Connect account, follow the steps in [Create an Organization Owner Account with a Customer Connect Account](#).
 - If you don't have a Customer Connect account, follow the steps in [Create an Organization Owner Account Without a Customer Connect 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 9 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 two 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**.

Results

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 VMware Cloud Console at <https://vmc.vmware.com>.
- 2 Create the SDDC.

To start from the Launchpad:

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

To start from the Inventory view:

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

- 3 Choose a seller.

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

VMware Cloud on AWS: Advanced includes vSphere, vSAN, NSX, VMware Aria Automation , and VMware Aria Operations.
- 5 Configure SDDC properties.
 - a Choose a **Cloud**.

For a **VMware Cloud on AWS** deployment, select **AWS**.
 - b Select an **AWS Region** in which to deploy the SDDC.

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

- c Select a **Deployment** type.

Option	Description
Single Host	Select this option to create Single Host Starter Configuration SDDC. Single Host Starter Configuration SDDCs expire after 60 days. For more information, see Deploying a Single Host SDDC Starter Configuration .
Multi-Host	Select this option to create an SDDC with two 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 (AZs). This configuration provides data redundancy in the event that there is a problem with one of the AZs. The system deploys management VMs in the first AZ you select. Both AZs can be used by your workloads. Either can be used for failover. You need a minimum of two hosts (one in each AZ) to create a stretched cluster. Hosts must be added in pairs.

Read the VMware Cloud Tech Zone Designlets [VMware Cloud on AWS Management Cluster Planning](#) and [VMware Cloud on AWS: Stretched Clusters](#) for an in-depth discussion of SDDC host and cluster configuration options.

- d Select the host type.

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

- e Make up an **SDDC Name**.

The name must be between 1 and 128 characters and cannot include the no-break space (0xC2) or soft hyphen (0xAD) characters. All other ISO-8859-15 printable characters are allowed.

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

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

You can add or remove hosts later if you need to. An SDDC requires at least three hosts to be eligible for upsizing. See [Upsize SDDC Management Appliances](#)

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.

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

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

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

Note Large-sized appliances are not supported for two-host SDDCs with stretched or conventional clusters.

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

- 7 Click **Next** to connect to an AWS account.

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

Option	Description
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 .
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 VMware Cloud Console shows the progress of the connection.

- 8 Select a **VPC** and **Subnet** from the drop-down menu and click **Next**.
- 9 (Optional) Click **NEXT** to configure the Management Subnet in the SDDC.

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

- Choose a range of IP addresses that does not overlap with the AWS subnet you are connecting to. If you plan to connect your SDDC to an on-premises data center, the IP address range of the subnet must be unique within your enterprise network infrastructure. It cannot overlap the IP address range of any of your on-premises networks. For a complete list of IPv4 addresses reserved by VMware Cloud on AWS, see [Reserved Network Addresses](#) in the *VMware Cloud on AWS Networking and Security* guide.

- If you are deploying a single-host SDDC, the IP address range 192.168.1.0/24 is reserved for the default compute network of the SDDC. If you specify a management network address range that overlaps that address, single-host SDDC creation fails. If you are deploying a multi-host SDDC, no compute gateway logical network is created during deployment, so you'll need to create one after the SDDC is deployed.
- CIDR blocks of size 16, 20, or 23 are supported, and must be in one of the "private address space" blocks defined by [RFC 1918](#) (10.0.0.0/8, 172.16.0.0/12, or 192.168.0.0/16). The primary factor in choosing a Management CIDR block size is the anticipated scalability requirements of the SDDC. The management CIDR block cannot be changed after the SDDC has been deployed, so a /23 block is appropriate only for SDDCs that will not require much growth in capacity.

CIDR block size	Maximum Number of hosts (Single AZ)	Maximum Number of hosts (Multi AZ)
/23	23	18
/20	228	224
/16	See VMware Configuration Maximums .	

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

- Multi-Edge SDDC with Traffic Groups
- SDDC Groups
- Multi-Cluster SDDC
- VCDR recovery SDDC

Because use of these features reduces SDDC host capacity, a management CIDR block size of /23 might be insufficient for some SDDC requirements.

- 10 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 or Modify 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 or Modify a Network Segment](#).
- (Optional) Activate add-on services such as VMware Aria Operations or VMware Aria Automation . See [Working with Integrated Services](#) in the *VMware Cloud on AWS Operations Guide*.

Choosing a Region

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

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

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

AWS Region and Availability Zone Support

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

For information on supported regions for VMware Cloud on AWS, see [AWS Region and Availability Zone Support](#).

AWS Regions that Support VMware Cloud on AWS

Most of the AWS regions that support VMware Cloud on AWS also support stretched clusters. Many also support SDDCs configured to run workloads that require compliance hardening to meet Payment Card Industry (PCI) Data Security Standard or Information Security Registered Assessors Program (IRAP) requirements.

Regions introduced by AWS after March 20, 2019 require manual enablement in your AWS account. See [Managing AWS Regions](#) in the *AWS General Reference* for more about this process.

AWS Region Name	Stretched Cluster Support	Compliance Hardening Support	Enablement Required	Availability Zones
Africa (Cape Town)	Y	PCI	Y	afs1-az1, afs1-az2, afs1-az3
Asia Pacific (Hong Kong)	Y	PCI	Y	ape1-az1, ape1-az2, ape1-az3
Asia Pacific (Hyderabad)	Y	PCI	Y	aps2-az1, aps2-az2, aps2-az3
Asia Pacific (Melbourne)	Y	PCI	Y	apse4-az1, apse4-az2, apse4-az3
Asia Pacific (Mumbai)	Y	PCI	N	aps1-az1, aps1-az2, aps1-az3
Asia Pacific (Osaka)	Y	PCI	Y	apne3-az1, apne3-az2, apne3-az3
Asia Pacific (Seoul)	Y	PCI	N	apne2-az1, apne2-az3
Asia Pacific (Singapore)	Y	PCI	N	apse1-az1, apse1-az2, apse1-az3
Asia Pacific (Sydney)	Y	IRAP, PCI	N	apse2-az1, apse2-az2, apse2-az3
Asia Pacific (Tokyo)	Y	PCI	N	apne1-az1, apne1-az2, apne1-az4
Canada (Central)	Y	PCI	N	cac1-az1, cac1-az2
Europe (Frankfurt)	Y	PCI	N	euc1-az1, euc1-az2, euc1-az3
Europe (Ireland)	Y	PCI	N	euw1-az1, euw1-az2, euw1-az3
Europe (London)	Y	PCI	N	euw2-az1, euw2-az2, euw2-az3
Europe (Milan)	Y	PCI	N	eus1-az1, eus1-az2, eus1-az3
Europe (Paris)	Y	PCI	N	euw3-az1, euw3-az2, euw3-az3
Europe (Stockholm)	Y	PCI	N	eun1-az1, eun1-az2, eun1-az3
Europe (Zurich)	Y	PCI	Y	euc2-az1, euc2-az2, euc2-az3
Middle East (Bahrain)	Y	PCI	Y	mes1-az1, mes1-az2, mes1-az3
South America (São Paulo)	Y	PCI	N	sae1-az1, sae1-az3
US East (N. Virginia)	Y	PCI	N	use1-az1, use1-az2, use1-az4, use1-az5, use1-az6

AWS Region Name	Stretched Cluster Support	Compliance Hardening Support	Enablement Required	Availability Zones
US East (Ohio)	Y	PCI	N	use2-az1, use2-az2, use2-az3
US West (N. California)	N	PCI	N	usw1-az1, usw1-az3
US West (Oregon)	Y	PCI	N	usw2-az1, usw2-az2, usw2-az3, usw2-az4 (i3.metal only)

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 13 Get Support](#) for additional details on getting help and support.

Procedure

- 1 Log in to the VMware Cloud Console at <https://vmc.vmware.com>.
- 2 Click **Inventory > SDDCs**, then pick an SDDC card and click **VIEW DETAILS**.

SDDC information is available on the following tabs.

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 .
Integrated Services	Lists the integrated services that are available in this SDDC. See Working With SDDC Add-On Services in the <i>VMware Cloud on AWS Operations Guide</i> .
Maintenance	Lists any upcoming SDDC maintenance events.
Troubleshooting	Includes tests for connectivity and other use cases.


Tab	Description
Settings	<p>The Settings page displays information about SDDC settings, pre-defined user accounts, and SDDC access via the API and PowerCLI.</p> <p>SDDC Management Appliance Size</p> <p>Displays the size of management appliances in this SDDC. These sizes were specified when the SDDC was created.</p> <p>Default vCenter User Account</p> <p>Displays the credentials for this pre-defined user. The password is generated when the SDDC is created. If you change it in vCenter, it does not get not updated on this page.</p> <p>vSphere Client (HTML5)</p> <p>Click this link to open the SDDC vCenter with the vSphere client. Log in as the default vCenter user.</p> <p>vCenter Server API Explorer</p> <p>Click this link to open the API Explorer view of this SDDC and access the VMC REST API.</p> <p>PowerCLI Connect</p> <p>Copy this command string and paste it into a PowerCLI window. Replace the password with the one for the default vCenter user account. If that password includes special characters, enclose it in single quotes.</p> <p>vCenter FQDN</p> <p>Shows the fully-qualified domain name of the vCenter in this SDDC and enables you to specify the associated IP address. See Set vCenter Server FQDN Resolution Address in the <i>VMware Cloud on AWS Networking and Security Guide</i>.</p>
Support	<p>You use the information in this tab when working with VMware Technical Support.</p> <p>See Chapter 13 Get Support.</p>

Set the Language and Regional Format for the VMware Cloud Console

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

The VMware Cloud Console supports English, French, German, Japanese, Korean, Spanish, Simplified Chinese, and Traditional Chinese. To set the language used by the VMware Cloud Console, set your language preferences in your VMware Cloud Services account. For more information, see [How Do I Change My Language and Regional Format](#) in the *VMware Cloud Services Documentation*.

Procedure

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

Connect to vCenter Server

10

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

By default, the SDDC Management Gateway blocks traffic to all management network destinations, including vCenter Server, from all sources. You must add management gateway firewall rules that allow only secure traffic from trusted sources. You can use any of these connection types to connect to the SDDC vCenter Server:

- [Configure AWS Direct Connect Between Your SDDC and On-Premises Data Center](#)

This option provides dedicated connectivity between your enterprise and the SDDC and can be used in conjunction with an IPsec VPN to encrypt traffic.

- [Configure a VPN Connection Between Your SDDC and On-Premises Data Center](#)

This option provides encrypted connectivity between your enterprise and the SDDC.

- If you can't use Direct Connect or a VPN, you can access the SDDC management network over the public internet and rely on management gateway firewall rules to prevent access by untrusted sources. This option may be appropriate for some use cases but is inherently less secure than the others.


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

- 1 If you have created a VPN, click the **OPEN VCENTER** button on the SDDC card, then click **VPN**.
- 2 If you haven't yet created a VPN and want to connect to vCenter Server over the public Internet, click **OPEN VCENTER** button on the SDDC card., then click **FIREWALL RULE**.

See [Add or Modify Management Gateway Firewall Rules](#) for details on how to create a firewall rule that allows secure access the SDDC vCenter Server.

- 3 (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

11

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 & 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, follow these steps.

Prerequisites

You must have the NSX Admin service role to view and configure features on the **Networking & Security** tab. See [Assign NSX Service Roles to Organization Members](#) in the *VMware Cloud on AWS Networking and Security* guide.

Procedure

Procedure

- 1 Create a route based VPN in the SDDC.

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. See [Create a Route-Based VPN](#) in the *VMware Cloud on AWS Networking and Security* guide.

2 Configure an on-premises IPsec VPN.

You can use NSX or any other device that can terminate an IPsec VPN.

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

- a If your on-premises VPN gateway is behind a firewall, you must configure that firewall to forward IPsec 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.

- b Download the SDDC IPsec VPN configuration file.

See the [IPsec VPN Settings Reference](#) in the *VMware Cloud on AWS Networking and Security* guide for more about what's in this file and how to use it to help you configure your on-premises VPN endpoint.

3 (Optional) Create a network segment.

A Single Host Starter SDDC is created with a single routed network segment named sddc-cgw-network-1. Multi-host SDDCs are created without a default network segment, so you must create at least one for your workload VMs. See [Create a Network Segment](#) in the *VMware Cloud on AWS Networking and Security* guide.

4 Create some basic firewall rules on the management gateway.

By default, the management gateway blocks traffic to all destinations from all sources. Add Management Gateway firewall rules to allow traffic as needed. See [Add or Modify Management Gateway Firewall Rules](#) in the *VMware Cloud on AWS Networking and Security* guide.

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. To use features such as migration with vMotion, cold migration, or Hybrid Linked Mode, switch the vCenter Server resolution to a private IP address resolvable from the VPN. See [Set HCX FQDN Resolution Address](#) in the *VMware Cloud on AWS Networking and Security* guide.

Deploy Workload VMs

12

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.

Read the following topics next:

- [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](#)
- [Access 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.

Note The Content Onboarding Assistant adds scripts and ISO images to a Content Library that is published from your on-premises data center and subscribed from your SDDC. It does not add existing OVF or OVA templates to the Content Library. For other ways of transferring OVF or OVA templates to your SDDC, see [Getting Templates, ISOs, and Other Content into Your SDDC](#) in the *VMware Cloud on AWS Operations Guide*.

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

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

Prerequisites

Before you run Content Onboarding Assistant, do the following:

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

Procedure

- 1 Prepare scripts and ISO images for addition to the Content Library by moving them into a single folder in your on-premises data center.
`.vmtx` templates need no special preparation.
- 2 Download the Content Onboarding Assistant from the download location.
 - a Click **Tools** in left-hand column of the VMware Cloud Console.
 - b On the Content Onboarding Assistant card, click **DOWNLOAD** to download `Content-Onboarding-Assistant-version.jar`, where *version* is **1.5** or a newer version of the file.

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

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

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

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

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

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

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

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

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

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

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

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

Results

The Content Onboarding Assistant does the following:

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

What to do next

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

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 VMware Cloud Console at <https://vmc.vmware.com>.

- 2 Click **Inventory > SDDCs**, then pick an SDDC and click **VIEW DETAILS**.
- 3 Click **OPEN NSX MANAGER** and log in with the **NSX Manager Admin User Account** shown on the SDDC **Settings** page. See [SDDC Network Administration with NSX Manager](#).

You can also use the VMware Cloud Console **Networking & Security** tab for this workflow.

- 4 Click **Public IPs** to open the Public IPs page.

This page is in the Networking category in NSX Manager and in the **System** category in the **Networking & Security** tab.

- 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.

- 5 Use the vSphere Client to assign the public IP address to a VM.

See [Configuring Network Settings](#) for details.

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*.

Access the Virtual Machine Remote Console

You can use the Virtual Machine Remote Console (VMRC) to access VMs in your cloud SDDC as long as you can access the SDDC over VMware Transit Connect, AWS Direct Connect (DX), or a VPN.

When connecting to your cloud SDDC over VMware Transit Connect or DX to a Private VIF, you can use VMRC to access workload VM consoles without needing to create any additional firewall rules. Access to VMRC over a VPN might require a management gateway firewall rule to allow this traffic to flow. See [Configure Direct Connect to a Private Virtual Interface for SDDC Management and Compute Network Traffic](#).

Prerequisites

- Your workstation must be able to connect to SDDC ESXi hosts over TCP port 443.
- Your workstation must have the VMRC package installed. You can download [VMRC](#) from Customer Connect.

Procedure

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

-
- 2 (Optional) Create a management gateway firewall rule to enable access to ESXi on port 443.

This rule is required only when you access VMRC over a VPN. See [Add or Modify Management Gateway Firewall Rules](#).

Option	Description
Source	IP address or CIDR block from a connected on-premises data center.
Destination	Select ESXi under System Defined Groups .
Services	HTTPS (TCP 443)

-
-
- 3 Open the vSphere Client and select the VM you want to connect to with VMRC.
- 4 Click **LAUNCH REMOTE CONSOLE**.

Get Support

13

A VMware Cloud on AWS Support User can get support by opening the **VMware Cloud Services** console.

Prerequisites

You must have the VMware Cloud on AWS **Support User** Service Role to open a support request. Your organization owner can assign this role to any organization member.

Procedure

- 1 Before you contact VMware for support, have the support information for your SDDC ready.
 - a Log in to the VMware Cloud Console at <https://vmc.vmware.com>.
 - b Click **Inventory** > **SDDCs**, then pick an SDDC and click **VIEW DETAILS**.
 - c Click **Support** to view the support information.
- 2 See [How Do I Get Support](#) for more information about using VMware Cloud Services in-product support.