Getting Started With VMware Cloud on AWS

07 August 2024
SDDC Version 1.24
VMware Cloud on AWS

vmware by Broadcom

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

https://docs.vmware.com/

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

Contents

Getting Started With VMware Cloud on AWS

This guide provides all the information you'll need to create your first VMware Cloud™ on AWS software-defined data center (SDDC).

We've structured it as a workflow of recommended steps that should get you up and running quickly. You can use this checklist to track your progress:

Table 1-1. VMware Cloud on AWS Onboarding Checklist

[ ] Chapter 1 Learn	Start with this collection of references that introduce you to the features of VMware Cloud on AWS.
[ ] Chapter 2 Plan	Gather information about the workloads you want to run in VMware Cloud on AWS and the network connections You'll need that information when you deploy and configure your first SDDC.
[ ] Chapter 3 Prepare	Before you can use VMware Cloud on AWS, you'll need to verify your credentials in the Broadcom Support Porta about the roles that you and your colleagues will have in configuring and operating the new SDDC.
[ ] Chapter 4 Operate	Use your Broadcom credentials to log in to the VMware Cloud Console and get started.

After you have deployed and configured your SDDC, see the VMware Cloud on AWS Networking and Security Guide and 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 purchase VMware Cloud on AWS and use it 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. It was written for readers who have used vSphere in an on-premises environment and are familiar with virtualization concepts and IPv4 networks. In-depth knowledge of vSphere or Amazon Web Services is not required.

Learn

1

VMware provides a broad array of learning resources tailored to the needs of anyone who wants to know more about VMware Cloud on AWS and how you can use it to meet your business needs.

Use the VMware Cloud Launchpad

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.

Familiarize Yourself With the VMware Cloud Tech Zone

The VMware Cloud Tech Zone provides a broad range of technical materials for all technical levels designed to help you understand how VMware Cloud on AWS can help you achieve your business objectives. This material focusses on "why" rather then "how to," and includes introductions to new features, design guides, Designlets, and references to VMware hands-on labs.

View the VMware Cloud on AWS Release Notes

Check the VMware Cloud on AWS Release Notes page frequently to review the available features and when they were released, as well as links to additional information or requirements to use them.

Review the VMware Cloud on AWS Service Level Agreement and Support Policy

The Service Level Agreement (SLA) defines those VMware Cloud on AWS service components that have an availability commitment and provides details of that commitment. I includes a legal definition of the scope of our responsibilities in providing you with a cloud service, and outlines the division of responsibilities between you and VMware.

The Support Policy defines our weekday global support for cloud deployments.

An understanding of these document can be helpful when you need to Get Support.

Plan

2

Creating your first VMware Cloud on AWS SDDC requires only a few steps, but before you start, take a few minutes to think about how you'll use the SDDC, and how to configure it to meet your needs.

Many of the choices you have to make when you deploy your first SDDC can be revisited later if you need to, but some of them can't be changed without deleting the SDDC, including all its workloads and configuration settings, and deploying a new one.

Procedure

1 Resource Planning

A VMware Cloud on AWS SDDC virtualizes networking, storage, and compute resources. Understanding the needs of your SDDC workloads can help you design and deploy an SDDC that meets those needs in a scalable, cost-effective way.

2 Network Planning

A VMware Cloud on AWS SDDC network is carved out of a subnet in an AWS VPC that you own. Before you can deploy your first SDDC, you need to create that VPC and subnet using AWS tools.

3 Identity and Access Management

In addition to the rights associated with their roles as members of a VMware Cloud on AWS Organization, users also have rights associated with an identity established in a corporate directory that supports protocols like LDAP and SAML.

Resource Planning

A VMware Cloud on AWS SDDC virtualizes networking, storage, and compute resources. Understanding the needs of your SDDC workloads can help you design and deploy an SDDC that meets those needs in a scalable, cost-effective way.

Matching SDDC Resources to Workload Needs

SDDC compute (CPU), memory, and storage resources are provided by the host and storage types you choose when you create the SDDC There are two separate systems that run in an SDDC to manage resources and ensure workloads have sufficient capacity available to support their operation:

vSphere Distributed Resource Scheduler (DRS)

DRS can migrate workloads between hosts in a cluster to help ensure that all available host resources are being used to meet workload requirements. DRS also makes use of vSphere HA Admission Control to ensure that sufficient capacity is reserved so that in case of a host failure, all resource reservations applied to powered-on VMs are met. It acts as a gatekeeper and will prevent a VM from powering on if the cluster does not have sufficient resources to satisfy those reservations in such a scenario.

VMware Cloud on AWS Elastic DRS

Elastic DRS is a feature, unique to VMware Cloud on AWS, that monitors total cluster utilization and, using customer-defined policies, can add or remove hosts to optimize the cluster performance/cost equation. VMware Cloud on AWS allows hosts to be added or removed on demand. Any hosts that get added by EDRS are be billed at on-demand rates until they are removed unless a matching subscription is available.

One of the best places to start figuring out the SDDC resources needed by your workloads is the VMware Cloud Sizer. This complimentary VMware Cloud service estimates the resources required to run various predefined workloads given a specified number of virtual CPUs (cores). Read the VMware Cloud Sizer Feature Brief to learn more.

Storage

An SDDC can use vSAN or external NFS storage. The host and storage types you choose when you create the SDDC apply to SDDC Cluster-1, which supports SDDC management appliances. When you add clusters to the SDDC, you can use other host types if you want. For more information, see VMC on AWS Host Types. The VMware Cloud Tech Zone article VMware Cloud on AWS: Storage Architectureexplains our storage architecture and available storage types. And the VMware Cloud Tech Zone Designlets VMware Cloud on AWS Management Cluster Planning and VMware Cloud on AWS: Stretched Clusters provide an in-depth discussion of SDDC host and cluster configuration options.

Compute and Memory

SDDC compute and memory capacity is determined by host count and host type. VMware Cloud on AWS provides host types suited to various resource consumption profiles: storage-optimized, compute-optimized, and a balance of the two. In addition to the list in VMC on AWS Host Types, there's also a Host Types Feature Brief that provides a more detailed look at host types and their

capabilities. An understanding of the compute (CPU) and memory requirements of your workload VMs can help you choose the host type for your initial cluster, and for any additional clusters you add to your SDDC. You can find CPU, memory, and storage details for all supported VMware Cloud on AWS host types in VMware Configuration Maximums.

Network Planning

A VMware Cloud on AWS SDDC network is carved out of a subnet in an AWS VPC that you own. Before you can deploy your first SDDC, you need to create that VPC and subnet using AWS tools.

Before you deploy an SDDC, you'll need to understand how it will be used, who will use it, and how the management appliances and workloads in it will connect to other networks. You'll also need:

- Administrator access to an AWS account so you can create and configure the VPC.
- Information about Choosing a Region so you can understand how the available AWS regions and availability zones affect your plans for SDDC deployment.
- IP address space details for other networks, including your on-premises network and networks used by services such as storage providers and disaster recovery solutions, to which the SDDC network will connect. Your SDDC management network address space cannot overlap with any of those address spaces.
- A network addressing plan including:
  - any routes into the SDDC you plan to advertise externally, and a list of the addresses to which they will be advertised
  - SDDC network gateways from which where you want traffic to egress the network
- Any public IP addresses, assigned to you by IANA or another regional internet registry. where your customers expect your applications to be accessible.

It would also be a good idea for you to review the VMware Cloud Tech Zone article VMware Cloud on AWS: Network Architecture, which provides a detailed discussion of the components of an SDDC network.

Many of the decisions you have to make when creating the AWS VPC and subnet you'll use for VMware Cloud on AWS can't be changed without deleting the SDDC and starting over, so lets begin with a summary of the AWS objects and operations you'll need to understand before making those decisions.

AWS Accounts and Account Linking

Every VMware Cloud on AWS SDDC runs in an AWS account owned and managed by VMware and dedicated to your VMware Cloud on AWS Organization. This gives VMware complete responsibility for the operational integrity of the VPC and the SDDC services that run in it. We use AWS cross-account access to link this VPC to your own VPC during SDDC deployment. We give you a couple of options when it's time to link the accounts, including delayed linking for

single-host trial SDDCs and re-using an AWS account that had been previously linked to an SDDC that you abandoned, but for most new SDDC deployments, it's a good idea to start by creating a VPC owned by an AWS account that you own and have Administrator access to. Before you do that, you need to understand the basics of AWS regions and availability zones

AWS Regions and Availability Zones

VMware Cloud on AWS services are available in many AWS regions. Service availability in each region is documented here. You have to choose a region before you can deploy an SDDC, and that choice, once made, cannot be changed. Consider the following when choosing a regions for your SDDC:

- A region that's geographically close to the majority of your users helps reduce network latency for them.
- A region that's geographically close to any on-premises data centers you'll be connecting with helps reduce network latency for those connections.
- If you plan to use the SDDC for Disaster Recovery (DR), pick a region that's geographically distant from the data you're protecting, but close enough to your users and on-premises data centers to keep latency to a minimum.

Every AWS region includes multiple availability zones (AZs), each of which constitutes a separate fault domain. 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.

Note The AZ names you see in the VMware Cloud Console are unique to your AWS account. The same AZ could have a different name when viewed from another account

The VMware Cloud Tech Zone article VMware Cloud on AWS: Stretched Clusters has more information about how stretched clusters work in VMware Cloud on AWS. We discuss stretched clusters in more detail in our topic on Resource Planning.

VPC Subnets

When you deploy an SDDC, you have to choose at least one AZ for it to occupy. If you want the SDDC to have stretched clusters, you'll need to choose two. And because the SDDC will be deployed in the AZ containing the subnet you select, it's best to start by creating a VPC and subnet in every region of that AZ. Doing this makes it easier to identify all AZs where your SDDC can be deployed and select the one that best meets your SDDC placement needs. The VPC you connect to when deploying the SDDC becomes the Connected Amazon VPC in the VMware Cloud Console. The VPC subnet is used only for communication between workloads running in your SDDC and native AWS services in the connected VPC.

The VPC subnet CIDR must be unique within your enterprise network and cannot overlap with any other SDDC networks, including the Management subnet discussed in the next section. The minimum size for the VPC subnet the SDDC is linked to is /27, but to support the maximum capacity of the SDDC's management cluster, we recommend using a /26 subnet. There is no advantage to using a subnet larger than /26. Once the SDDC has been created, you cannot moify or delete or change this subnet.

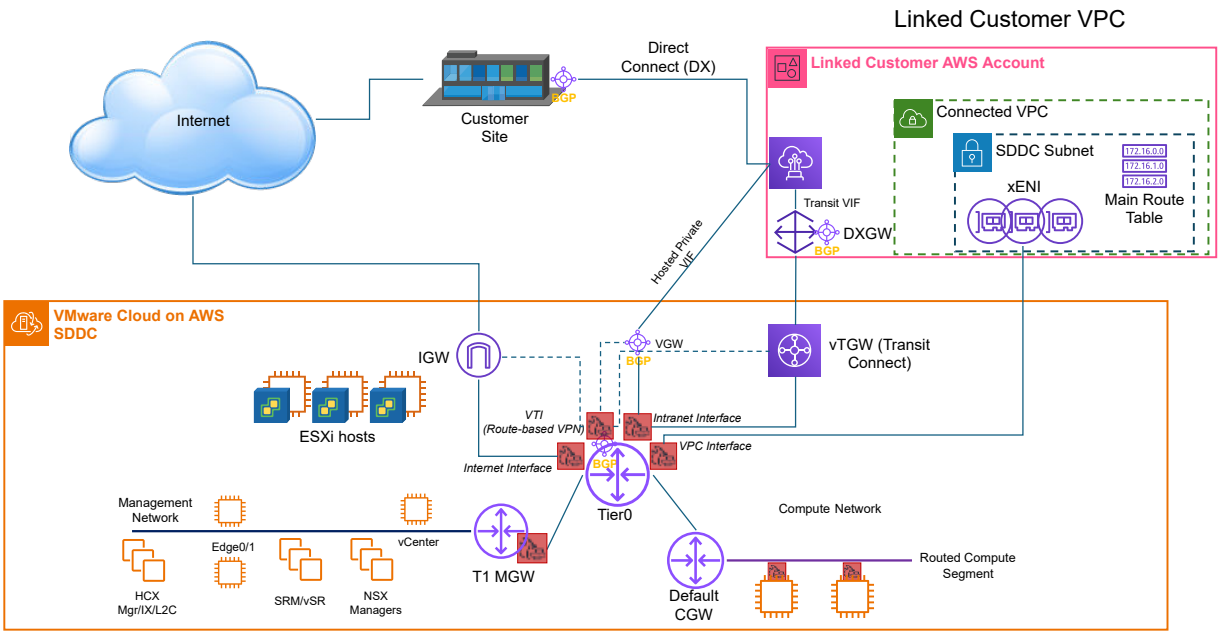
See Creating a Subnet in Your VPC in the AWS documentation for information about how to use the Amazon VPC console to create a subnet in your VPC.

SDDC Subnets

As you can see in this simplified diagram, a VMware Cloud on AWS SDDC contains two subnets;

- A single Management subnet, used by SDDC management components such as the ESXi hosts (management, vMotion, and other interfaces), vCenter, NSX Manager, and managed services such as HCX and Site Recovery appliances.
- A Compute network with one or more Compute subnets for use by SDDC workloads.

Figure 2-1. SDDC Network Topology



The Management Subnet

When you create the SDDC, you have to specify a CIDR block for the Management Subnet. CIDR blocks of size 16, 20, or 23 are supported, with a couple of restrictions:

- It cannot overlap with the VPC subnet CIDR.
- It cannot overlap with the CIDR of any on-premises network.

- It 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. You can't change the Management CIDR block size after the SDDC has been deployed, so you need to think about how many hosts your SDDC will need. For example, a /23 management subnet might not support enough hosts for a long-lived SDDC that you expect to put into production use. If you expect to grow your SDDC beyond a handful of hosts or think you might want to deploy additional clusters, /20 is a better choice for the management subnet CIDR. Onboarding and Managing VMware Cloud on AWS: Part 1- Preparing to deploy an SDDC has more information about the relationship of Management CIDR block size to SDDC host capacity. And our Resource Planning page has more information about matching SDDC capacity to workload needs.

Compute Subnets

Unlike the Management subnet, which you must specify before you deploy the SDDC, compute subnets can be created only after the SDDC is up and running. Each compute subnet is a virtual network (an NSX network segment) that is typically routed so that workloads connected to it are accessible from other networks, but also be configured as an isolated network with no external connectivity, or an extended network that you can use with an L2VPN. Selecting IP Subnets and Connectivity for your SDDC has more information about SDDC subnets and how they connect to each other and the outside world.

See Also

- Onboarding and Managing VMware Cloud on AWS: Part 1- Preparing to deploy an SDDC
- Onboarding and Managing VMware Cloud on AWS – Part 2: Deploying an SDDC and Connecting your AWS account.
- Selecting IP Subnets and Connectivity for your SDDC
- Deploying and Managing a Software-Defined Data Center

Identity and Access Management

In addition to the rights associated with their roles as members of a VMware Cloud on AWS Organization, users also have rights associated with an identity established in a corporate directory that supports protocols like LDAP and SAML.

Identity and access management for VMware Cloud on AWS is based on your identity in your Broadcom account. See Create or Update Your Broadcom Account for details.

Prepare

3

Anyone who creates or manages a VMware Cloud on AWS SDDC must have an account in the Broadcom Support Portal and be a member of a VMware Cloud services organization. Start by creating or updating your Broadcom account, then create a VMware Cloud services organization and invite others to join.

Each a VMware Cloud services 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 join the Organization. By default, these users are assigned the role of Organization Member and can use VMware Cloud on AWS and other cloud services belonging to the Organization, but cannot invite new users.

Procedure

1. Create or Update Your Broadcom Account

   Your Broadcom account connects you to the Broadcom Support Portal, which is your gateway to VMware Cloud on AWS services.

2. Create and Manage a VMware Cloud on AWS Organization

   Anyone who needs to access the VMware Cloud Console must be a member of a VMware Cloud on AWS Organization.

3. Purchase Options for VMware Cloud on AWS

   You can purchase VMware Cloud on AWS directly from Broadcom or from an authorized reseller.

4. View VMware Cloud on AWS Subscriptions

   VMware Cloud on AWS is available by subscription only.

Create or Update Your Broadcom Account

Your Broadcom account connects you to the Broadcom Support Portal, which is your gateway to VMware Cloud on AWS services.

You use the Broadcom Support Portal to purchase VMware Cloud on AWS, access support, search the Knowledge Base, and join Broadcom Product Communities.

Procedure

1 Create or update your Broadcom account.

   All VMware Customer Connect accounts have been migrated to the Broadcom Support Portal. If you had a VMware Customer Connect account, you do not need to create a new one, but you do need to activate your Broadcom account and update your profile information before you can use your VMware ID to log in to the VMware Cloud Console.

   If you did not have a VMware Customer Connect account, you'll need to register as a new user of the Broadcom Support Portal. Open the User Registration page and provide your corporate email address. See Broadcom Knowledge Base article 145581 for more information about creating and using this account.

   If you had been using Multi-Factor Identification (MFA) with your VMware Customer Connect account, you will be prompted to reconfigure it when you update your Broadcom account. See Broadcom Knowledge Base article 216428 for more information.

2 Click **My Entitlements** to view the products you have licensed.

3 Click **My Downloads** to view available downloads for your products.

Create and Manage a VMware Cloud on AWS Organization

Anyone who needs to access the VMware Cloud Console must be a member of a VMware Cloud on AWS Organization.

When you create one of these Organizations, you become the Organization owner, and can populate the Organization with new members and assign them roles appropriate to their responsibilities.

As a VMware Cloud on AWS Organization owner, you can invite others to become members of the Organization. Organization members have both Organization roles and service roles. 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. Organization members do not have any service roles until an Organization owner assigns them.

Prerequisites

You must have a valid account in the Broadcom Support Portal to create or join a VMware Cloud on AWS Organization. See Create or Update Your Broadcom Account to learn more.

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 who are currently members of your Organization.

3 Click **Add Users**.

4 Enter an email address for each user you want to add. Separate multiple addresses with a comma, space, or newline.

   Users who you invite to your Organization must have a valid account in the Broadcom Support Portal to join. Users who do not have a Broadcom account are prompted to create one during the sign-up process.

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**.

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

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

   See Assign Organization and Service Roles for information about available roles and their rights.

Purchase Options for VMware Cloud on AWS

You can purchase VMware Cloud on AWS directly from Broadcom or from an authorized reseller.

On-demand host purchases are no longer available. You must purchase subscriptions in advance of SDDC deployment, host addition, or cluster creation.

Billing for VMware Cloud on AWS consists of upfront subscription purchases and ancillary charges billed monthly in arrears.

- VMware Cloud on AWS is available only through subscriptions purchased either through Broadcom direct sales or an authorized reseller. Self-service subscription purchase is no longer supported, and subscriptions must be purchased in advance of SDDC deployment and host scaling. For contact information for Broadcom sales in different geographies, see Contact Sales.
- In addition to upfront subscription purchases, ancillary charges such as AWS EC2 network charges, Elastic IP addresses, Microsoft SPLA, and other charges resulting from VMware Cloud on AWS usage are billed to customers with the Net 30 payment option. These ancillary charges cannot be paid for upfront or with subscriptions, and will be itemized on the customer bill in arrears. Ancillary charges accrue as soon as an SDDC is deployed.

After subscription purchase and onboarding, you deploy and manage your VMC on AWS infrastructure through the VMware Cloud Console.

The VMware Cloud on AWS service includes the Elastic DRS (EDRS) feature that protects the SDDC from host failures and storage overflows. EDRS protects the health of the SDDC by adding hosts whenever a scaling event is triggered, and cannot be turned off. You must purchase additional 1 year subscriptions in advance to account for potential scaling events. You will receive notifications when a scaling event is approaching for one of your SDDCs.

To simplify planning for potential scale-up events, we recommend purchasing an additional 1 subscription for every 26 hosts for a single availability zone SDDC, and an additional 2 subscriptions for every stretched cluster SDDC. If you anticipate larger scaling events due to migrations or other activities, we encourage you to purchase additional subscriptions to account for future anticipated usage.

If you have hosts in excess of your purchased subscriptions, whether through EDRS storage scale-outs or due to expired subscriptions, your access to the VMware Cloud on AWS service and your SDDCs may be paused until the overconsumption is resolved. After 48 hours of excess usage, you will lose access to your SDDC(s) and workloads until you purchase sufficient subscriptions, and soon after that, your SDDC(s) will be irrevocably deleted.

VMware Cloud on AWS Packaging

VMware Cloud on AWS is packaged with several other VMware offerings to provide a range of capabilities for your SDDC.

VMware Cloud on AWS includes vSphere, vSAN, and NSX.

View VMware Cloud on AWS Subscriptions

VMware Cloud on AWS is available by subscription only.

Note Subscriptions purchased after April 30th, 2024 are currently not visible on the subscriptions tab. To view recently purchased subscriptions, log into the Broadcom Support Portal, select **VMware Cloud Foundation** from the top-level navigation menu, and click **My Entitlements**. For more information on using the Broadcom Support portal, see the Broadcom Support Portal Getting Started Guide.

Procedure

- To view your subscriptions, click the **Subscriptions** tab in the VMware Cloud Console.

Operate

4

Now that you have a plan and an organization in place, it's time to deploy, configure, and operate your first VMware Cloud on AWS SDDC.

Procedure

1 Log In to the VMware Cloud Console

Use the VMware Cloud Console to create and manage your VMware Cloud on AWS Organization and SDDCs.

2 Deploy an SDDC

A VMware Cloud on AWS Software-Defined Data Center (SDDC) is a collection of bare-metal AWS instances (hosts) running a standard set of VMware software components, including vCenter and NSX software-defined networking.

3 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.

4 Get Support

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

Log In to the VMware Cloud Console

Use the VMware Cloud Console to create and manage your VMware Cloud on AWS Organization and SDDCs.

Use your Broadcom credentials to log in to the VMware Cloud Console, which is the starting point for creating and updating your Organization and its SDDCs. The console has a navigation pane on the left side of the browser window. Use it to navigate to any of these console functions:

Launchpad

The Launchpad provides technical details on how you can use VMware products and solutions to achieve business outcomes.

Inventory

Lists all of your SDDCs and any SDDC Groups you have created. Pick an SDDC card and click **VIEW DETAILS**.

Subscriptions

Lists your subscriptions to VMware Cloud Services.

Activity Log

The Activity Log lists SDDC events for the past six months.

Tools

Provides access to a variety of VMware tools and utilities that you can download to help with SDDC workflows.

Developer Center

Provides access to VMware Cloud on AWS APIs and related tooling that you can use to automate SDDC workflows.

Maintenance

Lists any SDDC Upgrade and Maintenance events that have been scheduled, and allows you to request maintenance.

Notification Preferences

Enables you to select the Service Notifications that you want to receives about SDDC events

Browser Support in VMware Cloud on AWS

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.

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**.

Deploy an SDDC

A VMware Cloud on AWS Software-Defined Data Center (SDDC) is a collection of bare-metal AWS instances (hosts) running a standard set of VMware software components, including vCenter and NSX software-defined networking.

Each SDDC runs in an Amazon Virtual Private Cloud (VPC) and provides a full VMware stack, including vCenter, NSX software-defined networking, and storage, and one or more ESXi hosts that provide compute and storage resources to your workloads. When you create an SDDC, you can choose between vSAN Original Storage Architecture (vSAN), vSAN Express Storage Architecture (vSAN ESA), and external storage such as NFS.

When you're done with your Network Planning and Resource Planning, take a look at the VMware Cloud Tech Zone Quick Start guide, then follow up with the Deploy an SDDC section of the *VMware Cloud on AWS Operations Guide*.

To ensure control and security, an SDDC provides separate networks for management and compute components. Management components such as vCenter, ESXi, and NSX manager connect to the SDDC management network. You can create an IPsec VPN to provide secure access to the management network through the SDDC Management Gateway, an NSX Edge dedicated to this function. You access compute components (workload VMs on a compute

network) through a Compute Gateway. The compute network is typically implemented as an L2VPN that provides a single IP address space that spans your on-premises and SDDC environments. The Compute Gateway, a separate NSX Edge instance and Distributed Logical Router, control network access to workload VMs.

For more information about SDDC networking, see VMware Cloud on AWS Networking and Security

Configure SDDC Networking and Security

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

To learn more about the options for setting up that connection, use the Networking and Security Dashboard. If you just want to quickly set up a route-based VPN connecting your on-premises data center to your SDDC over the Internet, follow these steps.

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 lifebytes rekeying.

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

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.

Connect to vCenter Server

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

By default, the SDDC Management Gateway blocks traffic to all management network destinations, including vCenter, 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:

- 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 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 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 information about how to create a firewall rule that allows secure access the SDDC vCenter.
3. (Optional) Open the **Settings** tab and select another method for connecting to vCenter.

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.

Deploy Workload VMs

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. 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 Managing Virtual Machines in VMware Cloud on AWS for more ways to provision your SDDC with VM templates and ISO images that you can use to create workload VMs.

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.

Get Support

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 the **Support** tab to view the support information.
2. See How Do I Get Support for more information about using VMware Cloud Services in-product support.