AWS Whitepaper

SDDC Deployment and Best Practices Guide on AWS

SDDC Deployment and Best Practices Guide on AWS: AWS Whitepaper

Table of Contents

SDDC Deployment and Best Practices Guide on AWS

Publication date: **May 20, 2021** (*Document revisions*)

This guide is intended for IT infrastructure architects, administrators, and IT professionals who are planning to implement a VMware Cloud Software Defined Data Center (SDDC). It contains the steps and considerations required to stand up an SDDC as well as leveraging best practices and recommendations.

The information is written for readers who have used vSphere in an on-premises environment and are familiar with virtualization concepts.

A moderate knowledge of Amazon Web Services (AWS) is useful, but is not required.

The AWS Well-Architected Framework helps you understand the pros and cons of the decisions you make when building systems in the cloud. The six pillars of the Framework allow you to learn architectural best practices for designing and operating reliable, secure, efficient, cost-effective, and sustainable systems. Using the AWS Well-Architected Tool, available at no charge in the AWS Management Console, you can review your workloads against these best practices by answering a set of questions for each pillar.

For more expert guidance and best practices for your cloud architecture—reference architecture deployments, diagrams, and whitepapers—refer to the AWS Architecture Center.

To prepare for deployment, you should understand design decisions and gather necessary information. This deployment guide provides planning considerations and step-by-step instructions.

This guide covers the following planning considerations:

- Architecture
- Personnel
- Account requirements
- AWS infrastructure
- Network planning

Additionally, the guide provides you with step-by-step instructions to activate VMware Cloud on AWS and create your first SDDC.

Introduction

To prepare for deployment, you should understand design decisions and gather necessary information. This deployment guide provides planning considerations and step-by-step instructions.

This guide covers the following planning considerations:

- Architecture
- Personnel
- Account requirements
- AWS infrastructure
- Network planning

Additionally, the guide provides you with step-by-step instructions to activate VMware Cloud on AWS and create your first SDDC.

Are you Well-Architected?

The AWS Well-Architected Framework helps you understand the pros and cons of the decisions you make when building systems in the cloud. The six pillars of the Framework allow you to learn architectural best practices for designing and operating reliable, secure, efficient, cost-effective, and sustainable systems. Using the AWS Well-Architected Tool, available at no charge in the AWS Management Console, you can review your workloads against these best practices by answering a set of questions for each pillar.

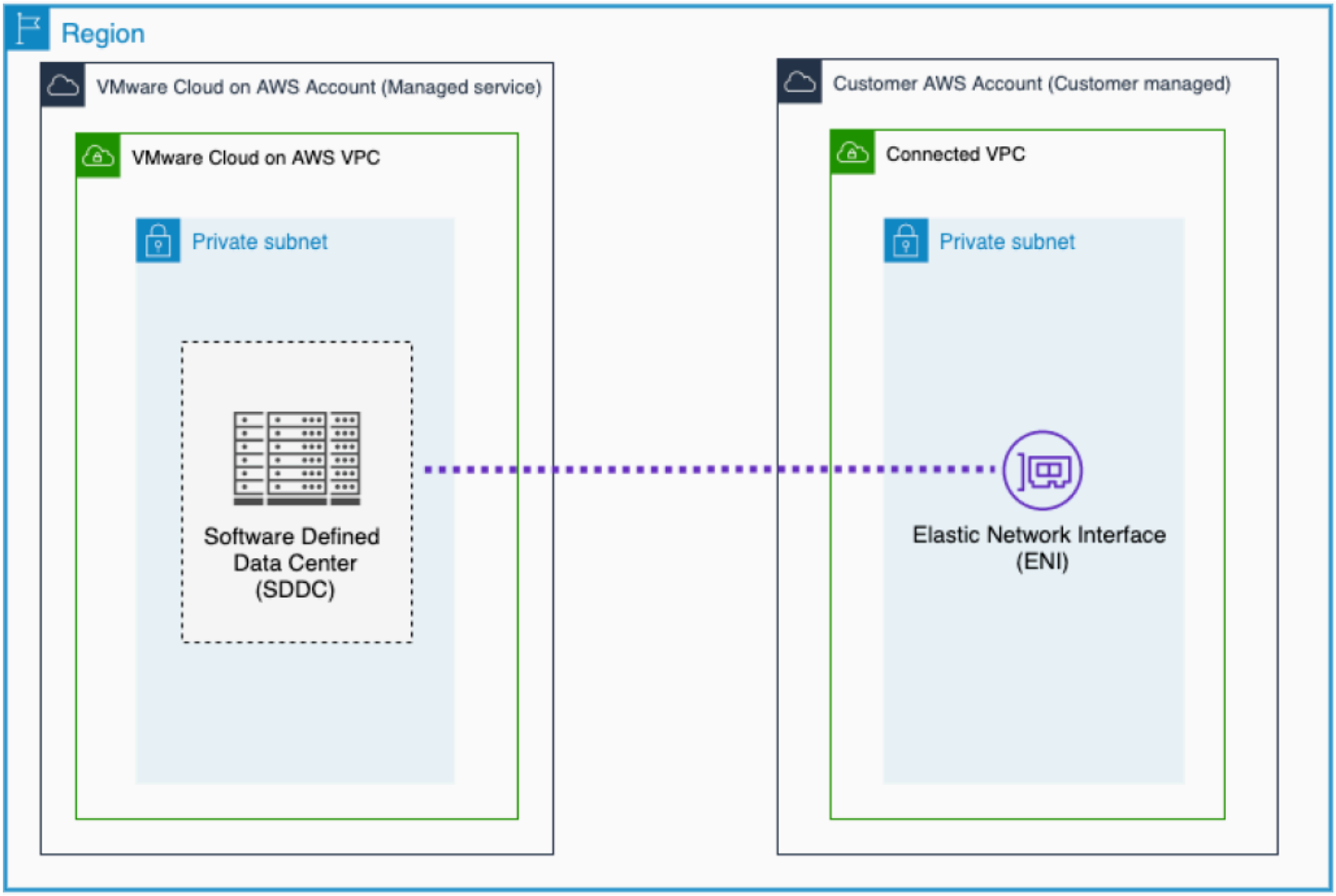
For more expert guidance and best practices for your cloud architecture—reference architecture deployments, diagrams, and whitepapers—refer to the AWS Architecture Center.

Before you begin

Planning a VMware Cloud on AWS deployment requires a moderate level of familiarity with AWS. If you're new to AWS, visit the AWS Identity and Access Management (IAM) site and the Amazon Virtual Private Cloud (VPC) site. These will help provide you with the foundational constructs you need. These sites provide materials for learning how to design, deploy, and operate your infrastructure and applications on the AWS Cloud.

Architecture

This is a high-level overview architecture.



High-level architecture of the VMware Cloud on an AWS managed account connected to a customer owned AWS account

This paper covers key preparation steps, associated resources, and deployment instructions to guide you through deployment of your first SDDC environment within your chosen Region and Availability Zone. This includes the following:

- Creating a single Virtual Private Cloud (VPC) within your AWS account
- Planning and provisioning a private subnet network within your chosen Availability Zone (AZ) for SDDC integration
- Activating the VMware Cloud on the AWS service

- Deployment of a non-stretched SDDC within a single AZ

Personnel planning

A critical first step in the planning process is to identify personnel that will be involved in the initial account onboarding process, and technical personnel involved in the deployment of the SDDC. The following is a list of common “roles” required to activate the service and deploy an SDDC.

> **Note**
>
> Depending on the organizational structure, a single person may encompass more than one role.

- **AWS administrator** — Required to ensure that at least one user is created with the permissions necessary to link the VMware Cloud on the AWS service with a new or existing AWS account.
- **Cloud administrator** — Performs all planning for the deployment of the SDDC. Performs the deployment of the SDDC. Performs the initial account link to the AWS account.
- **Network administrator** — Allocates IP ranges needed for the deployment of the SDDC and AWS environment. The network administrator will work with the cloud administrator to ensure that the correct network classless inter-domain routing (CIDR) ranges are set during deployment. The network administrator plans and implements connectivity from the on-premises environment to the SDDC.
- **Security administrator** — Reviews and approves security policy for the SDDC.

Account requirements

Topics

AWS account

One of the requirements of VMware Cloud on AWS is that all deployed SDDCs must be linked to your AWS account. If you have a pre-existing account, you can use it for this purpose. If you don't have an AWS account, see How do I create and activate a new AWS account? for instructions.

> **Important**
>
> After an AWS account has been associated with a VMware Organization as the seller of record, the AWS account number cannot be updated. There can be only one AWS seller of record per VMware Organization.

Once you have an AWS account, ensure that all technical personnel have been added to the account and that they have been configured with the permissions necessary to properly manage the account. At minimum, there must be one user within the AWS account who has sufficient permissions to run the AWS CloudFormation template, which performs account linking to the SDDC.

When creating a stack, AWS CloudFormation makes underlying service calls to AWS to provision and configure your resources. You can use AWS Identity and Access Management (IAM) to manage permissions.

AWS account management: explore AWS Organizations

AWS accounts that host the Connected VPC can belong to AWS Organizations. This enables you to centrally govern your AWS Cloud resources.

If you are using AWS Organizations, you should determine which accounts you want to associate with VMware Cloud on AWS in advance. You can then create an organization unit (OU) and associate those accounts with the account identified for VMware Cloud on AWS.

The Connected VPC or AWS customer account is owned, operated, and paid for directly by the you, if you choose to utilize any AWS services within that account. To successfully attach the AWS customer-owned account to the SDDC, the AWS account should have at least one VPC within that account. This attachment enables you to use native AWS services to compliment whatever service you use to run on VMware Cloud on AWS.

Multi-account governance: AWS Control Tower and Landing Zones

You may want to utilize AWS Control Tower to manage the AWS Organization to enforce governance across multi-account environments. In this scenario, create a separate OU for the account to use with VMware Cloud on AWS. On the OU, ensure the guardrail rules you put into place do not restrict CloudFormation from creating the necessary resources in the connected VPC.

The CloudFormation template used by VMware has the prefix `vmware-sddc-formation`. The CloudFormation stack does the following in the connected VPC within the connected account:

- It creates immutable IAM roles in the VPC; namely `RemoteRole`, `RemoteRolePlayer`, `RemoveRoleService`, and `BasicLambdaRole`.
- It creates an IAM policy called `AmazonVPCCrossAccountNetworkOperations` for the above roles.
- It creates AWS Lambda functions for event notifications.

whether you use AWS Organizations or AWS Control Tower with landing zones, you need to configure your policies to allow the account that will be associated with VMware Cloud on AWS to complete these operations in the VPC.

Standalone accounts

Standalone accounts can be added to an AWS Organizations or AWS Control Tower landing zone later. When using standalone accounts, ensure you have set your governance policies to allow you to run any native AWS service you may require in your connected VPC.

VMware Customer Connect account

You will require a VMware Customer Connect (formerly MyVMware) profile to access the VMware Cloud on AWS service. If you do not have a profile, you can create one at VMware Customer Connect.

Once created, ensure that your 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.

VMware Cloud on AWS account

During the deal process, your Cloud Sales Specialist or Client Executive requests that you identify a Fund Owner and a Fund User. After your deal is processed, a service welcome email is sent to the Fund Owner and Fund User. This email contains the link you must use to sign up for a VMware Cloud on AWS account. This link can be used only once. The link will redirect you to the VMware Cloud Services Portal (CSP) website where you can log in into the VMware Cloud on AWS service using your VMware Customer Connect credentials.

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. Your VMware Customer Connect account is used to create the Organization and will make you an Organization Owner. Organizational Owners are assigned the Organization Owner's role and have complete administrative access to their Organization. They grant roles to access the Organization and its services, manage billing and subscription, and file support requests. New users can be assigned the Organization Owner role or the Organization Member role. Both types of users can manage the SDDC cloud, but only those with the Organizational Owner role can invite more users.

VMware Cloud on AWS has its own set of roles within IAM that need to be enabled manually:

- Administrator
- Administrator (delete restricted)
- NSX Cloud Administrator
- NSX Cloud Auditor

The major tasks performed by Organization users include, but are not limited to:

- Adding hosts to the SDDC

- Removing hosts from the SDDC
- Configuring the management network for vCenter access / administration: VPN, DNS, Firewall rules
- Configuring and maintaining the compute network for workloads: logical networks, firewall rules, NAT, VPN, DNS, Public IP addresses

Infrastructure preparation and planning

Before you begin, examine the deployment requirements as specified in the following table.

Table 1 — Design considerations

Area	Description
Region	VMware Cloud on AWS isn't currently supported in all AWS Regions. For a current list of supported Regions for VMware Cloud on AWS, see Available AWS Regions.
Availability Zone (AZ)	It is good practice to deploy the SDDC to the same Region and AZ as your current or planned native AWS workloads. Traffic between the SDDC and the AWS resources in the same AZ as your customer-owned VPC will not incur cross-AZ traffic charges. Traffic between different AZs in the same Region is billable to the customer-owned AWS account. This is according to the standard pricing of AWS.
VPC and subnet	Within a Region, a VPC and subnet are required to facilitate cross-account linking to the SDDC. Here are some things to consider when selecting these resources: • A new or existing VPC can be leveraged as the Connected VPC. This provides the SDDC

with high bandwidth and low latency access to native AWS services.

- When creating new VPC, consider a unique IPv4 CIDR block which is non-overlapping with the SDDC. This is particularly important if you will be connecting your AWS VPC via a VPN or Direct Connect to your on-premises environment.
- The subnet must be in an AWS 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. This helps you identify all AZs where an SDDC can be deployed, and select the one that best meets your SDDC placement needs. You may want to keep your VMC workloads close to or isolated from your AWS workloads running in a particular AZ, depending on your organizat ion's security requirements,

  See Creating a subnet in Your VPC to learn how to use the Amazon VPC console to create a subnet in your VPC.
- As part of the SDDC deployment, a series of Elastic network interfaces (ENIs) are created for use by the hosts of the SDDC. An ENI is a high bandwidth, private, and dedicated connection which resides inside the customer VPC. An AWS subnet is required to facilitate the account linking.
- The linked AWS account must have sufficien t capacity to create a minimum of 17 ENIs per SDDC cluster 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 AWS to temporarily add as many as 16 more hosts, so AWS recommends using an AWS account that has sufficient capacity for 34 ENIs per SDDC per Region. • AWS recommends dedicating a /26-CIDR block for each SDDC. Do not use that subnet for any other AWS services or Amazon Elastic Compute Cloud (Amazon 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 the addresses required for an SDDC. • The subnet must exist in the AWS account and not be shared from another account.
VPC route table	When VMware Cloud on AWS is connected to your VPC, it always uses the main route table in the VPC. The main route table should be dedicated to VMware Cloud on AWS. Where applicable, the route table is updated by VMware with new networks created within the SDDC. There are scenarios where customers create separate route tables within a VPC for different reasons. In these instances, remember that the custom route table will **not** be automatically updated when the main route table is updated based on any network changes within the SDDC. You'll have to manually update the custom route table in the connected VPC.

<table>
<tr><td>Security groups</td><td>The Cross-account ENIs exist within the customer-owned AWS account, and you have full access to apply security groups to the ENIs, which should otherwise not be touched. These actions can permanently undermine connectivity between the AWS environment and the SDDC. These can be identified in the AWS console with the description VMware VMC Interface DO NOT USE.</td></tr>
<tr><td>Resources</td><td>If necessary, request service quota increases for the following resources. You might need to do this if an existing deployment uses these resources, and you might exceed the default quotas with this deployment. The Service Quotas console displays your usage and quotas. For more information, see AWS service quotas. The deployment requires the following:

<table><tr><th>Resource</th><th>This deployment uses</th></tr><tr><td>VPCs</td><td>1</td></tr><tr><td>Subnet</td><td>1</td></tr><tr><td>ENIs</td><td>17</td></tr><tr><td>Route Table</td><td>1</td></tr></table></td></tr>
</table>

IAM permissions	For a summary of the permissions required to run the CloudFormation template, see AWS Roles and Permissions. Some of the initial permissions required to create the SDDC are removed from the role after the SDDC is has created. These can be seen in the Appendix of this document.

SDDC management IP planning	When you create an SDDC, you are required to specify an IP range for your managemen t network. This IP address range cannot be changed after the SDDC is created. As a result, it is critical to carefully plan out this IP range. In single-AZ deployment, a /23 CIDR can support 27 ESXi hosts, while a /20 can support up to 251, and a /16 up to 4091, but the number of hosts is currently limited to the SDDC maximum of 300. When deploying a multi-AZ (or stretched cluster) SDDC, the limits are 22 hosts, 246 hosts, and the SDDC maximum hosts for /23, /20 and /16 CIDRs, respectively. • **Size** — The range needs to be large enough to facilitate all hosts which will be deployed on day one, but also must account for future growth. • **Uniqueness** — You should provision an IP range which is unique within your organizat ion. This is particularly important if you will be connecting to your SDDC via a VPN or AWS Direct Connect, or if you are cross-lin king to a production VPC or other SDDCs. • **Ability to summarize** — Ideally this block should be a subnet of some larger space which is allocated to the SDDC as a whole. By subnetting a larger dedicated supernet, you will gain the ability to simplify routing between your on-premises environment and the SDDC, and you will potentially simplify network security policies used to secure the SDDC.

SDDC compute IP planning	To provision compute workloads within the SDDC, you must create at least one compute network segment. Although it is not required to provision an SDDC, VMware recommends allocating at least one IP address range for the SDDC compute network. After the SDDC has been provisioned, you can create a network segment using this address range. Compute networks are used for all VM traffic within the SDDC and are defined as individua l segments in NSX. VMware Cloud on AWS supports three types of logical network segments: routed, extended, and disconnec ted. • **Routed** — Has connectivity to other logical networks in the SDDC and, through the SDDC firewall, to external networks. This is the only segment type that supports DHCP. • **Extended** — Extends an existing Layer 2 MPLS VPN (L2VPN) tunnel, providing a single IP address space that spans the SDDC and an on-premises network. • **Disconnected** — has no uplink and provides an isolated network accessible only to VMs connected to it. Disconnected segments are created when needed by VMware HCX.

Prepare DNS strategy	VMware Cloud on AWS customers have many options to implement hybrid DNS solutions , ranging from self-hosted to fully managed native services from AWS. **Considerations**: Google DNS servers are set up initially when the SDDC is first deployed. NSX-T Tier 1 gateways, the management gateway (MGW) and the compute gateway (CGW) in VMware Cloud on AWS, act only as forwarders, relaying the queries from VMs to the actual DNS servers specified. The devices also cache the responses, improving performance. DNS servers configured under the MGW DNS Forwarder are used by the management components such as vCenter to resolve the on-premises fully qualified domain names (FQDNs). Features such as Hybrid Linked Mode (HLM) or Site Recovery may not work until the customer-managed DNS servers are configured here, as the management VMs using Google DNS cannot resolve the on-premises resources by default. **On-premises DNS servers** This is an option for customers who have on-premises DNS servers they wish to leverage. The benefit of this setup is that you can quickly get started, but because the SDDC VMs send DNS queries back to these servers over a IPSEC VPN or Direct Connect (Private VIF), you should be aware that a potential latency can be introduced.

The subnets containing these DNS servers must be permitted or advertised over VPN or Direct Connect. This makes them dependent on the network connectivity. In addition to the network connectivity, both firewalls (VMware Cloud on AWS and the on-premises firewall) must allow DNS traffic UDP/53 and TCP/53). Both the primary and secondary DNS servers should be reachable and provide consistent results.

Local DNS servers

In this configuration, DNS servers reside in one or more logical networks of the VMware Cloud on AWS SDDC. To avoid single points of failure and to prevent traffic going back to the on-premises data center, ensure that additional DNS servers are available in the cloud SDDC. Placing local AD/DNS servers in the SDDC could be a preferred method for increased availability and performance because workloads are catered locally.

If you are syncing with on-premises AD/DNS, both primary and secondary DNS servers should be reachable and provide consistent results. Subnets containing these DNS servers must be permitted or advertised over VPN or Direct Connect along with the firewalls configured to allow DNS traffic (UDP/53 & TCP/53) on the MGW of the SDDC.

DNS server in AWS

In this configuration, customers can leverage DNS servers that reside in AWS. Examples of this are Amazon EC2 instances with DNS

	configured, or making use of Amazon DNS services. This is useful for customers who already use DNS in their AWS environment. The benefit of this is you can take advantage of cross-VPC connectivity. Take into considera tions the DNS design with VMC and the following DNS options, as described in this blog.

Summary of IP Planning

The following table is an example of how to plan your IP addresses and subnets.

For customers planning to deploy multiple SDDCs, it is important to ensure the CIDRs do not overlap.

When deploying SDDCs into different AZs and subnets, ensure that you plan properly using unique subnets on each site.

Component	Value	
AWS Region	Frankfurt	
VPC Name	VMC-VPC	
VPC CIDR Block	172.31.0.0/16	
SDDC Name	VMC-SDDC01	
SDDC Management CIDR block	10.3.0.0/16	
Subnet Purpose	Availability Zone A	Availability Zone B
Connected SDDC	172.31.1.0/24	172.31.2.0/24

NTP planning

Ensure that your on-premises data center and your cloud SDDC are synchronized to an NTP service or other authoritative time source.

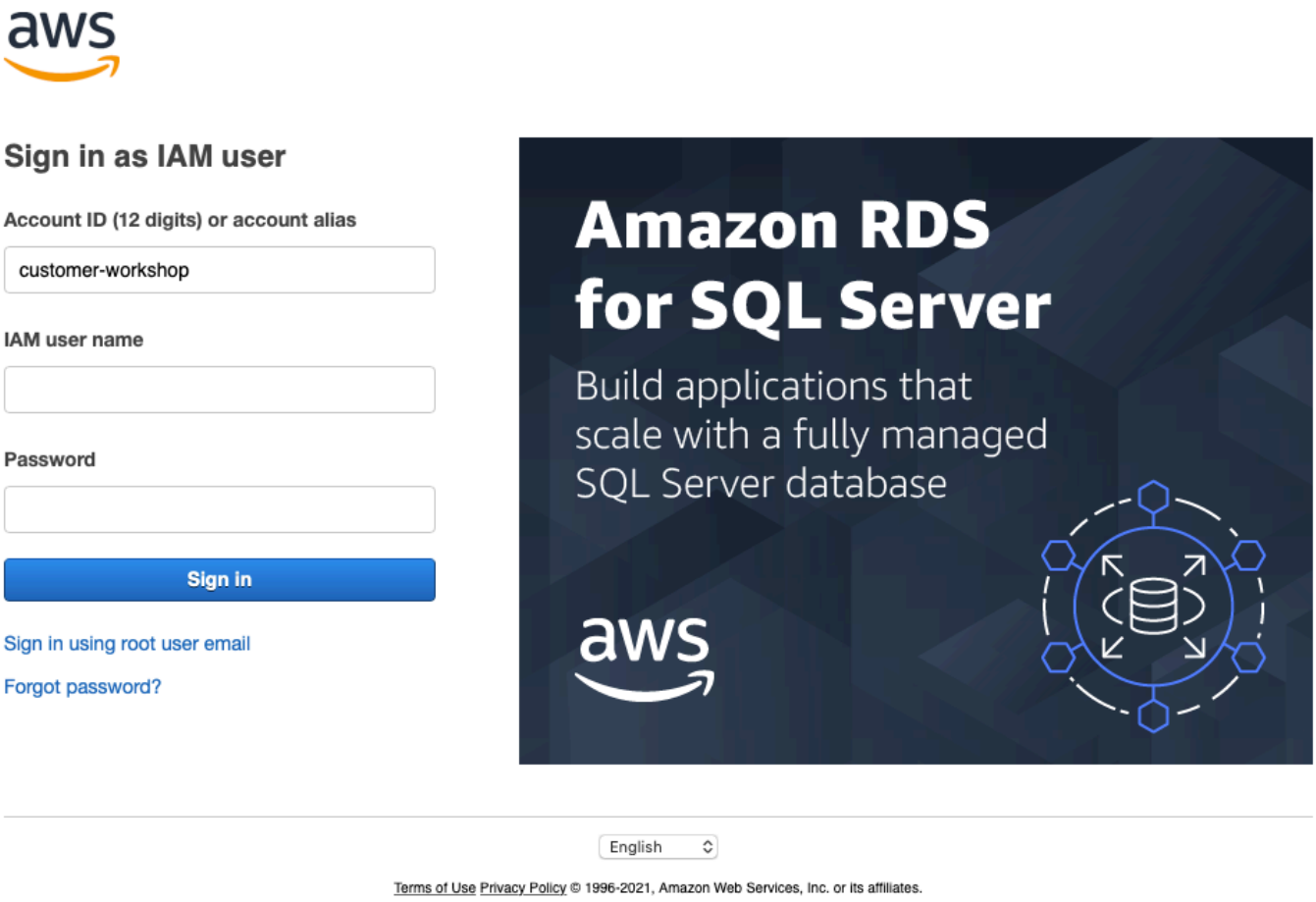
Security audit	Because VMware Cloud requires certain permissions within the customer-owned AWS account, you may be required to perform a security audit prior to onboarding. Most typically, security auditors want to review the CloudFormation template used by VMware Cloud.
Release notes	VMware Cloud on AWS is able to release new features at a faster pace than 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.
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. (Optional) Subscribe to receive real time alerts and updates.

Service Level Agreement (SLA)	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 is dependent on the monthly uptime percentage for the affected availability component. Read and bookmark the Service Level Agreement for VMware Cloud on AWS.

Deployment steps

Step 1. Sign in to your AWS account

1. Sign in to your AWS account at https://aws.amazon.com with an IAM user that has the necessary permissions. For details, see Infrastructure preparation and planning.
2. Ensure that your AWS account is configured correctly, as discussed in Infrastructure preparation and planning.

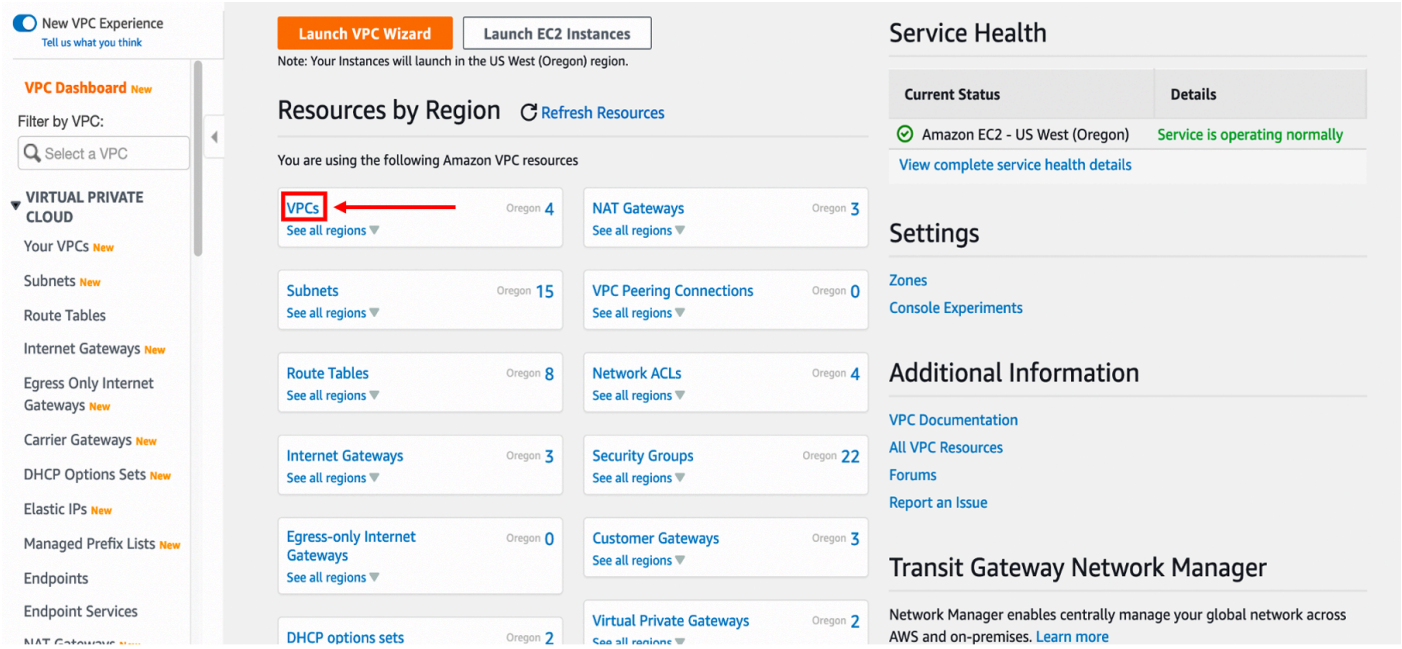


Sign in to Amazon RDS for SQL Server

3. At this stage you need to define the Amazon VPC which will be linked to the SDDC during the onboarding phase. If you intend to use an existing VPC, skip Step 2 and continue from Step 3 to create a private subnet for ENI connectivity.

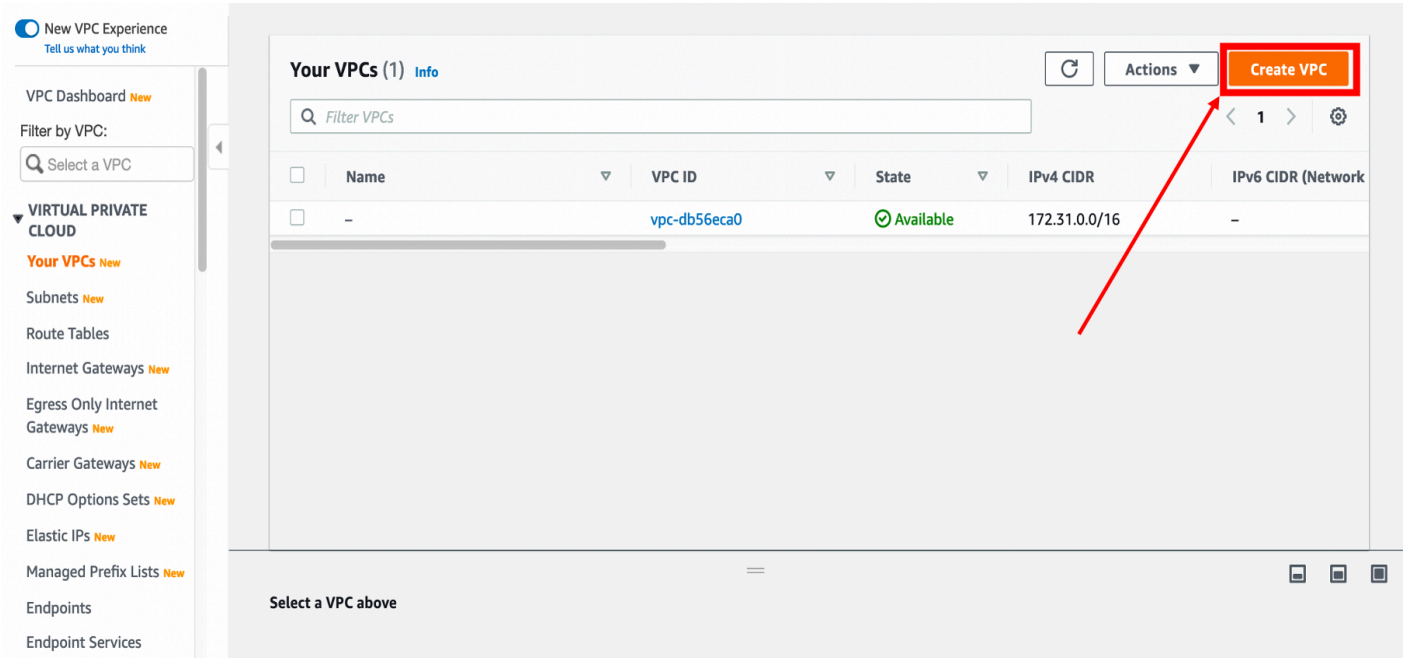
Step 2. Create a new VPC

1. Ensure the AWS Region displayed in the upper-right corner of the navigation bar is the correct Region in which you intend to deploy your VMware Cloud on AWS SDDC.
2. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
3. In the navigation pane, choose **Your VPCs** > **VPCs.**



*From the Amazon VPC Console, choose **Your VPCs** > **VPCs***

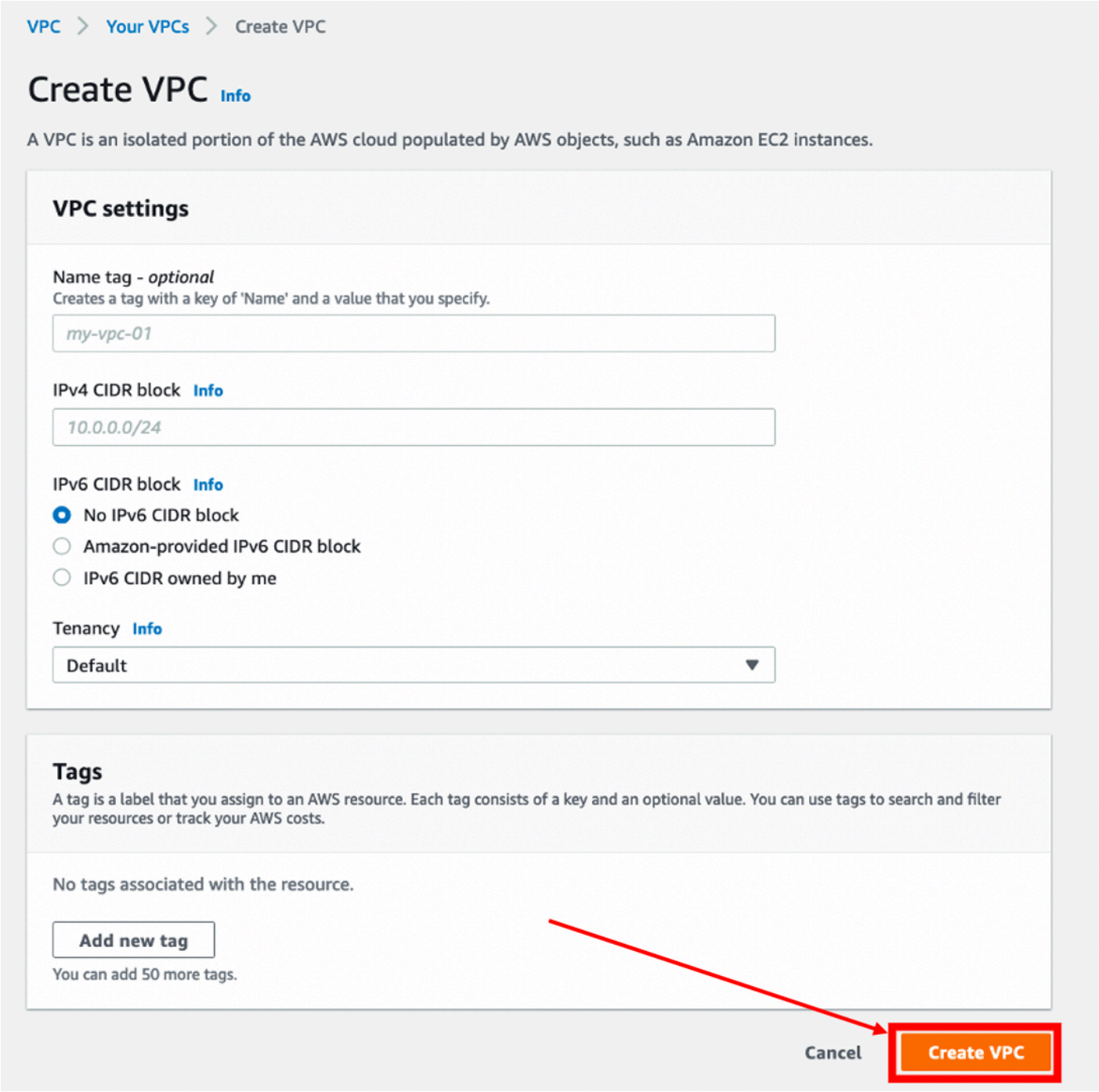
4. Choose **Create VPC.**



*Choose **Create VPC***

5. Enter the VPC details:

   - **Name tag** — Optionally provide a name for your VPC. This creates a tag with a key of Name and the value that you specify.
   - **IPv4 CIDR block** — Specify an IPv4 CIDR block for the VPC. The smallest CIDR block you can specify is /26, and the largest is /16. AWS recommends that you specify a CIDR block from the private (non-publicly routable) IP address ranges as specified in RFC 1918. For example, `10.0.0.0/16`, or `192.168.0.0/16`.
   - **Tenancy** — Default.



*Enter the VPC details and choose **Create VPC***

6. Choose **Create VPC**.
7. Choose **Close**.

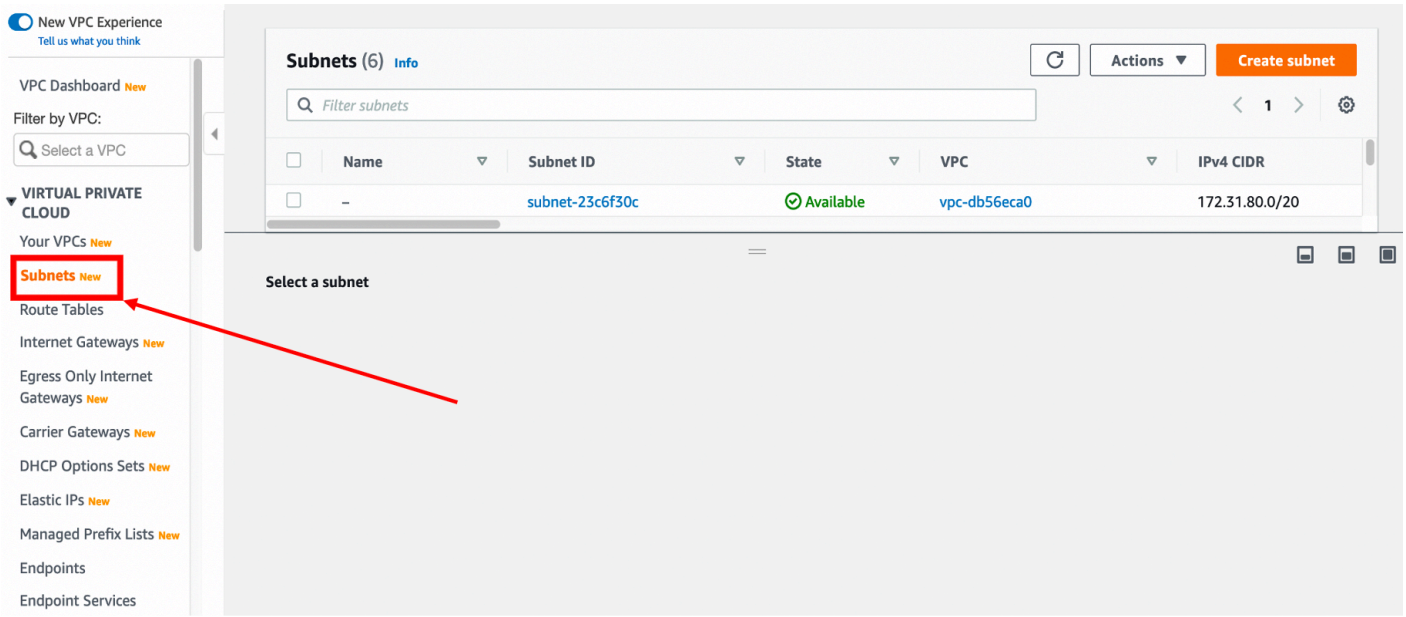
Step 3. Create a private subnet for the ENI

In this step, you will create a private subnet for each Availability Zone where you want to deploy VMware Cloud on AWS.

> **Note**
>
> A subnet with no internet gateway attached is recommended unless there is valid reason to do otherwise.

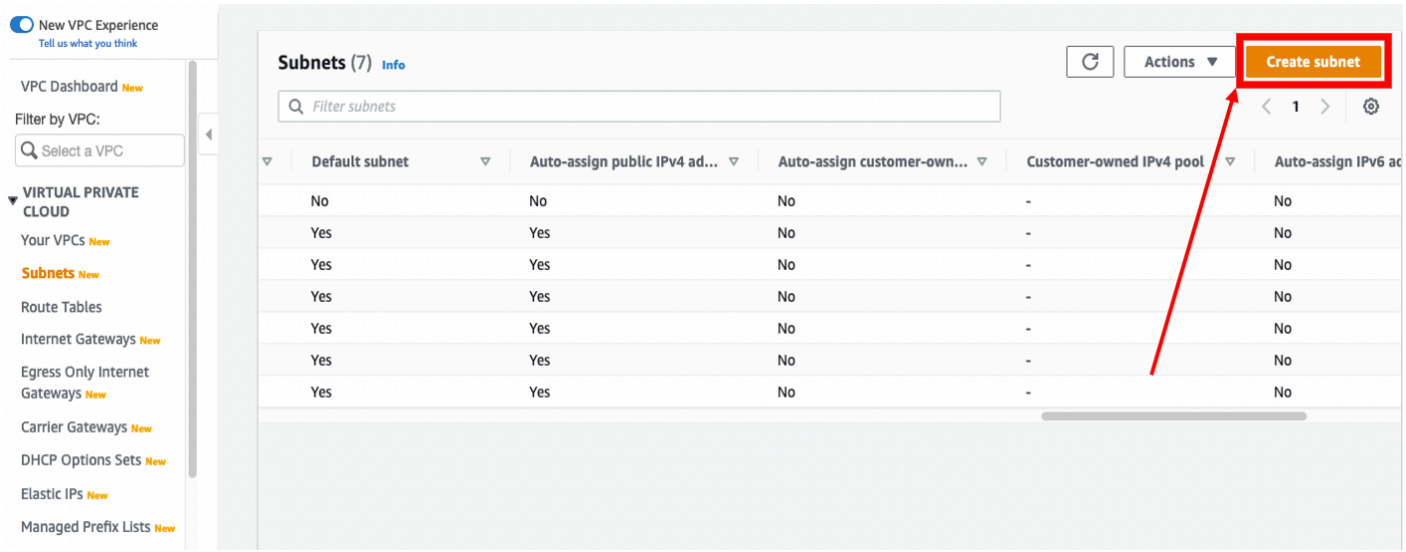
Add subnets to the VPC. You will add three subnets in different Availability Zones.

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose **Subnets**.



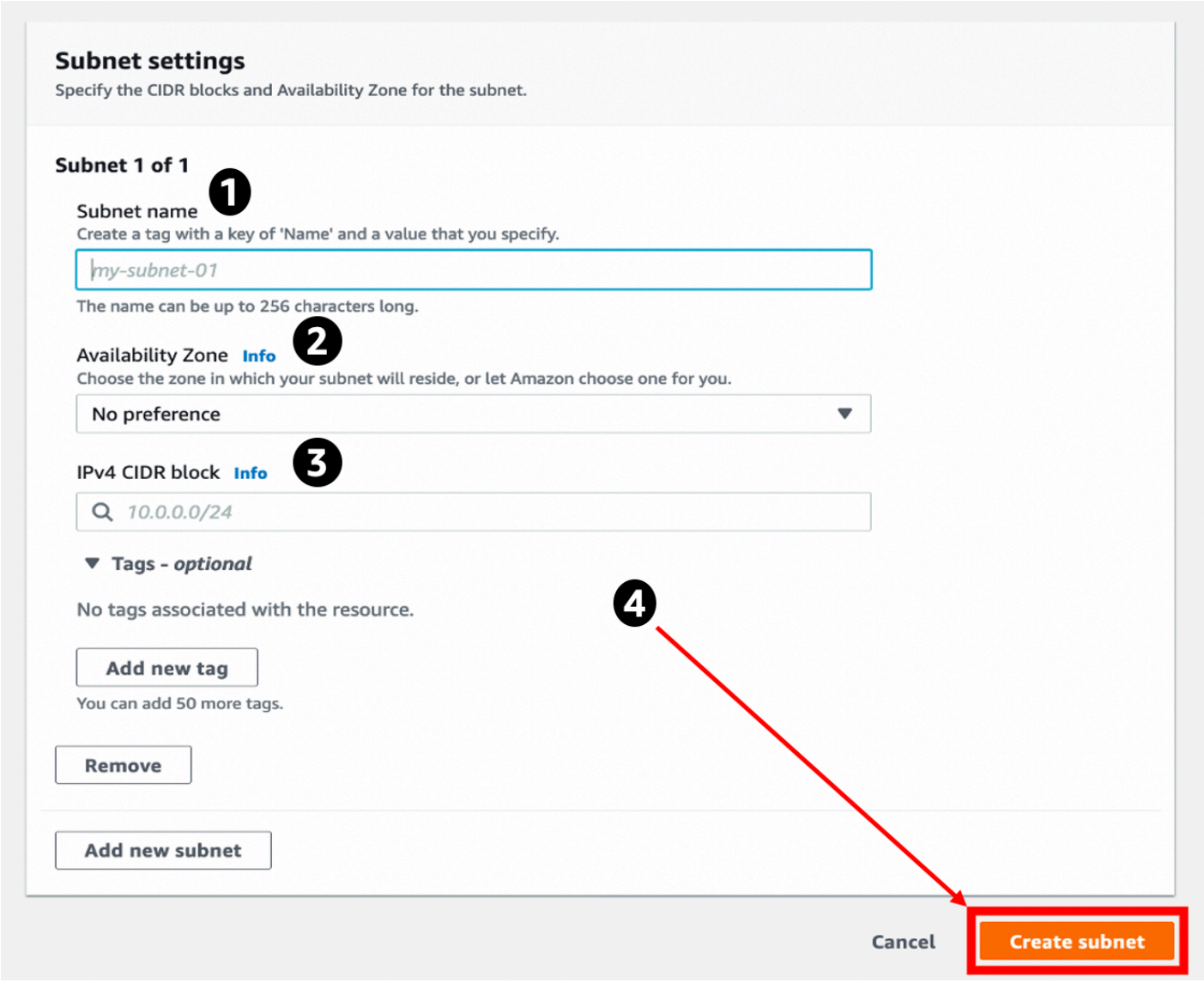
*Choose **Subnets***

3. Choose **Create Subnet**.



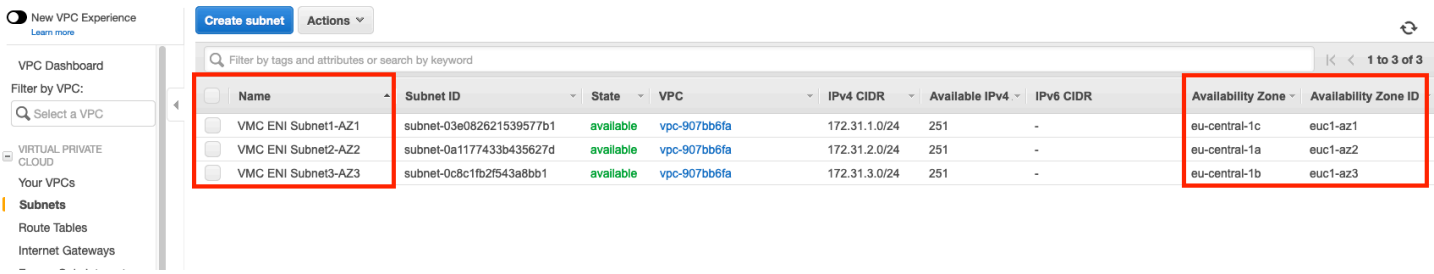
*Choose **Create subnet***

4. In the **Create Subnet**dialog box, do the following:
   - For **Name tag**, type an identifiable name such as “SDDC ENI private subnet”.
   - For **Availability Zone**, choose the first Availability Zone in the list.
   - For **CIDR block**, type the CIDR block to use for the subnet.
   - Choose **Create**.



*Enter subnet settings and choose **Create subnet***

5. Repeat steps 2 and 3 to create subnets for each remaining Availability Zone in the Region.
6. In this example, you have three subnets attached to the VPC.



The three subnets attached to the VPC

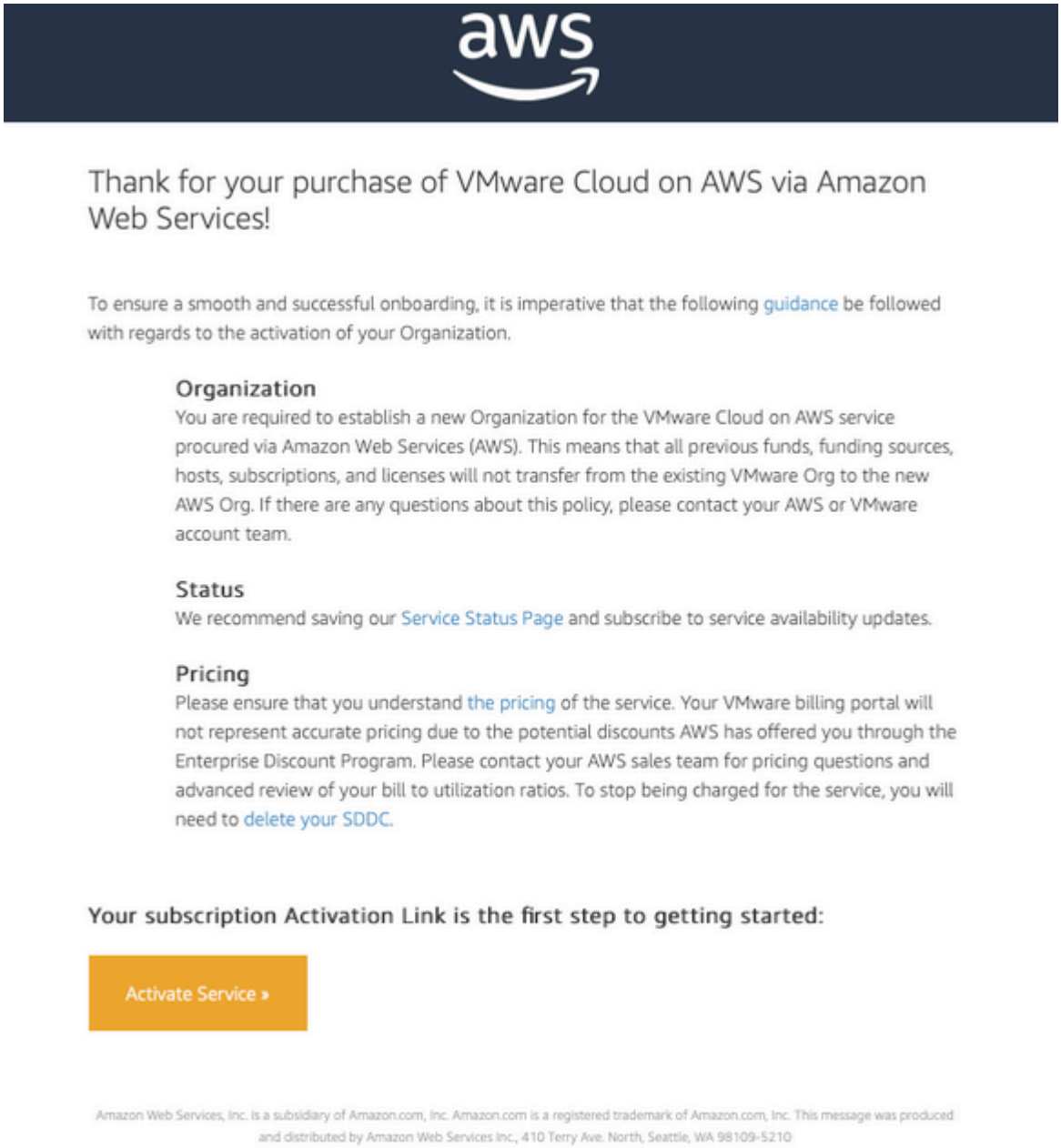
You are now ready to activate your VMware Cloud on AWS service.

Step 4. Activate VMware Cloud on AWS

The following steps require activation to the VMware Cloud on AWS. This step can be skipped if already completed.

During the process of purchasing VMware Cloud on AWS, you specify an email contact 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.

1. After receiving the Welcome letter from AWS, choose the **Activate Service** link to be redirected to the VMware Cloud on AWS portal.



Thank for your purchase of VMware Cloud on AWS via Amazon Web Services!

To ensure a smooth and successful onboarding, it is imperative that the following guidance be followed with regards to the activation of your Organization.

Organization
You are required to establish a new Organization for the VMware Cloud on AWS service procured via Amazon Web Services (AWS). This means that all previous funds, funding sources, hosts, subscriptions, and licenses will not transfer from the existing VMware Org to the new AWS Org. If there are any questions about this policy, please contact your AWS or VMware account team.

Status
We recommend saving our Service Status Page and subscribe to service availability updates.

Pricing
Please ensure that you understand the pricing of the service. Your VMware billing portal will not represent accurate pricing due to the potential discounts AWS has offered you through the Enterprise Discount Program. Please contact your AWS sales team for pricing questions and advanced review of your bill to utilization ratios. To stop being charged for the service, you will need to delete your SDDC.

Your subscription Activation Link is the first step to getting started:

Activate Service »

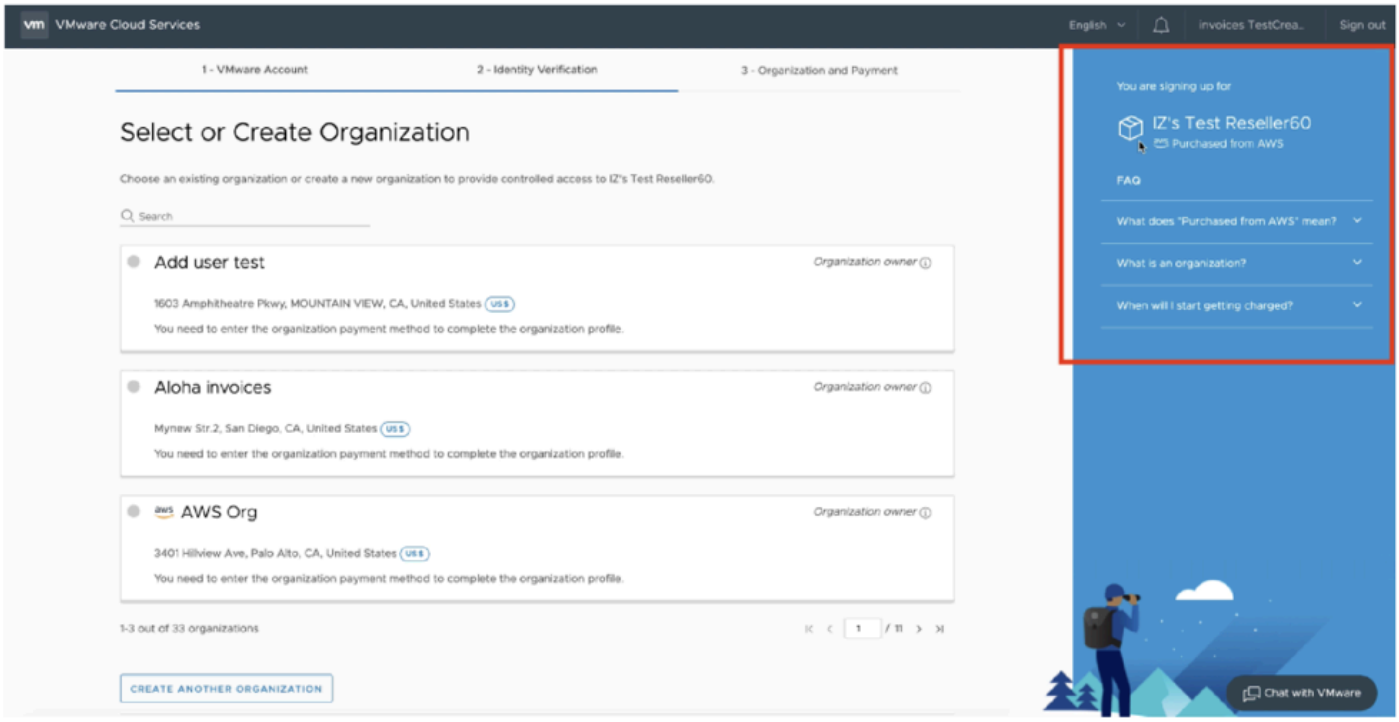
Amazon Web Services, Inc. is a subsidiary of Amazon.com, Inc. Amazon.com is a registered trademark of Amazon.com, Inc. This message was produced and distributed by Amazon Web Services Inc., 410 Terry Ave. North, Seattle, WA 98109-5210

*Choose **Activate Service***

> **Important**
>
> The welcome email is sent from no-reply-vmware-cloud-on-aws@amazon.com. Ensure the email wasn't processed by corporate spam filter.
> VMware Cloud on AWS accounts are based on an Organization name and ID. The very first user will need a valid VMware Customer Connect account. This account is used

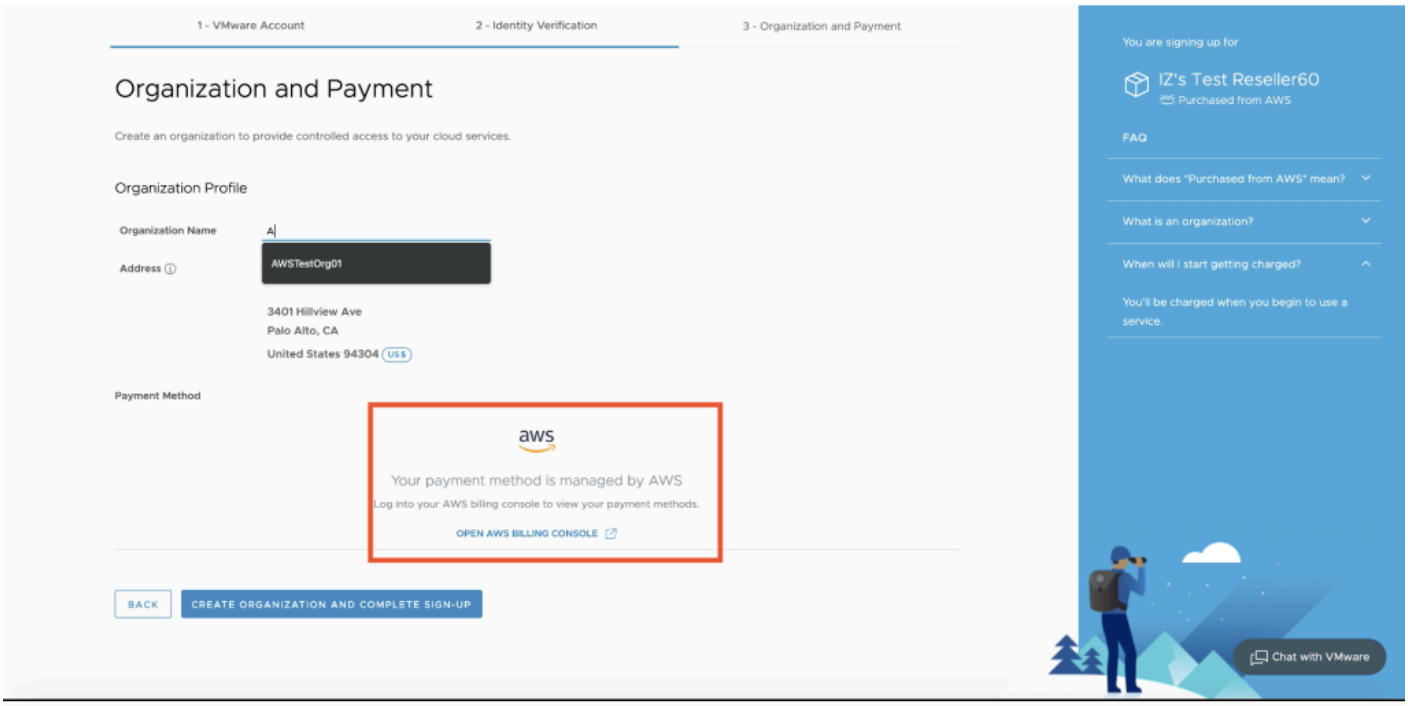
to create an Organization (Name and ID), and the initial user used is set up as the Organization Owner.

2. Log in using the VMware Customer Connect credentials previously supplied to AWS.
3. Review the terms and conditions for service usage, then select the check box to accept.
4. Choose **Next** to successfully complete the account activation. You will be redirected to the VMware Cloud on AWS console via https://vmc.vmware.com.
5. Create an Organization linked to the VMware Customer Connect account. Each Organization corresponds to a group or line of business subscribed to VMware Cloud on AWS.



Create an Organization linked to the VMware Customer Connect account

6. Enter the Organization name and address to provide a logical distinction for the organization. In the example below, `AWSTestOrg01` is used for the organization name.



Enter the Organization name

7. Choose **Create Organization** and complete sign-up to successfully complete the process.

> **Note**
>
> This organization has no relationship to AWS Organizations. Each organization has one or more Organization Owners, who have access to all the resources and services of the Organization and can invite users to the account.

Step 5. Identity and Access Management

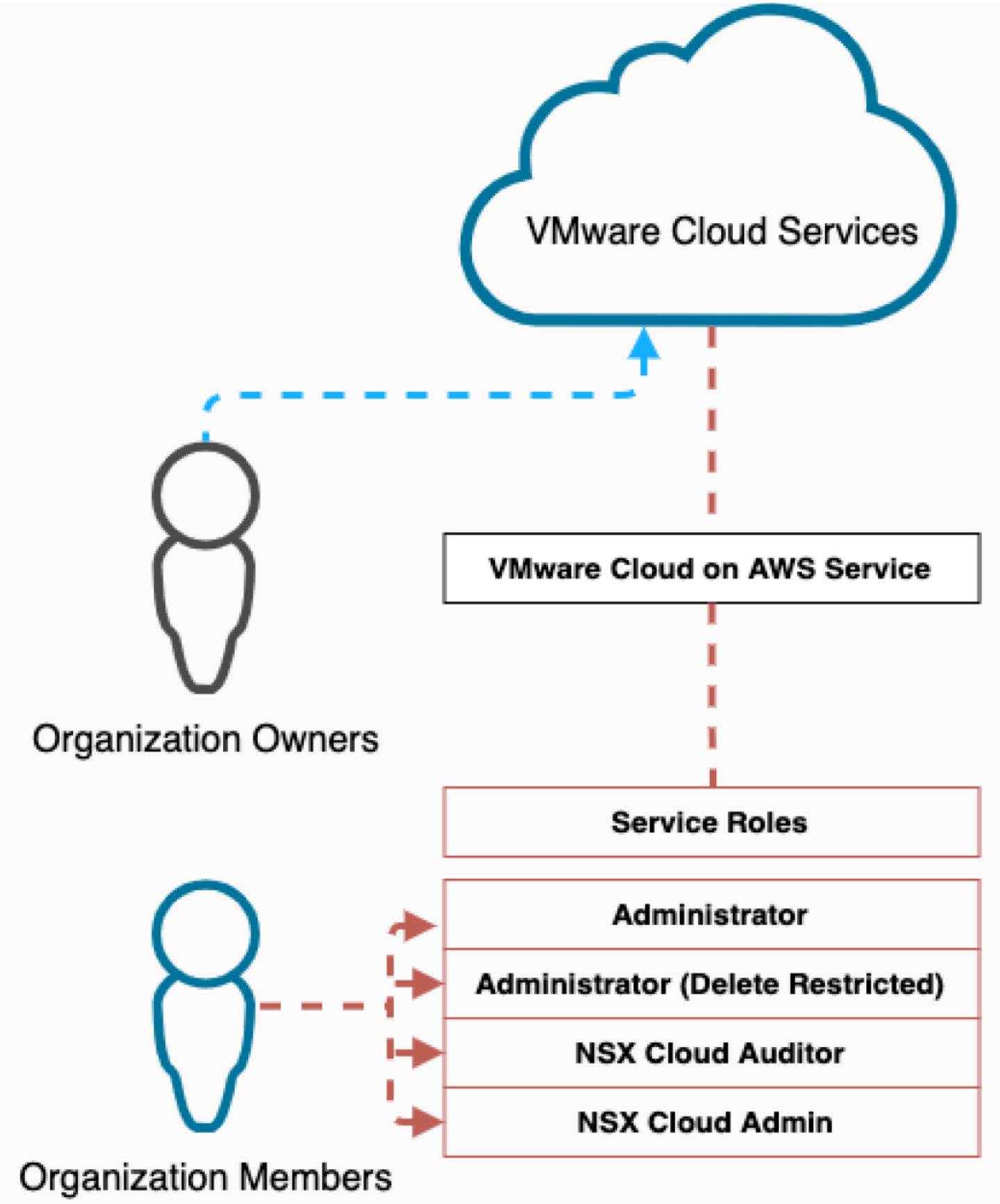
Just as it is a best practice to limit access to the vSphere Client, it is also a best practice to limit access to the Cloud Services and SDDC console. Users requiring access to the vSphere Client do not necessarily require access to the Cloud Services and SDDC console. Only users who are responsible for the entire SDDC or NSX components (such as VPN or firewall) should have access.

Within the newly created organization, there are two types of Organization Roles – Organization Owner and Organization Member. As the creator of the Organization, the initial user used is setup as the Organization Owner. This means you can add, remove, and modify users as well as access

to VMware Cloud Services. There can be multiple owners. Organization Members can access Cloud Services, but cannot add, remove, or modify users.

Within the Cloud Services Console, you can assign specific service roles to Organization members.

For example, the VMware Cloud on AWS service enables you to assign Administrator, Administrator (Delete Restricted), NSX Cloud Auditor, and NSX Cloud Administrator roles.


VMware Cloud Services
VMware Cloud on AWS Service
Organization Owners
Service Roles
Administrator
Administrator (Delete Restricted)
NSX Cloud Auditor
NSX Cloud Admin
Organization Members

Two types of role-based access roles

Federation

An enterprise using VMware Cloud Services can set up federation with a corporate domain. This enables you to use your Organization's single sign-on and identity source to sign in to VMware Cloud Services. You can then set up multi-factor authentication as part of federation access policy settings.

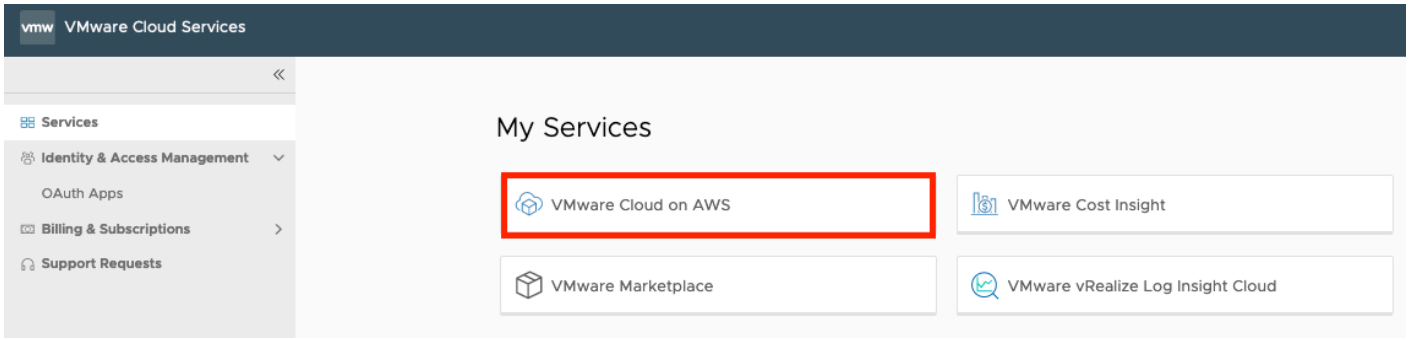
Using federated identity management enables you to control authentication to your Organization and services by assigning Organization and service roles to your enterprise groups.

To set up a federated identity with the VMware Identity Manager service you will need the VMware Identity Manager connector, which is provided at no additional cost.

Deploying VMware Cloud on AWS SDDC

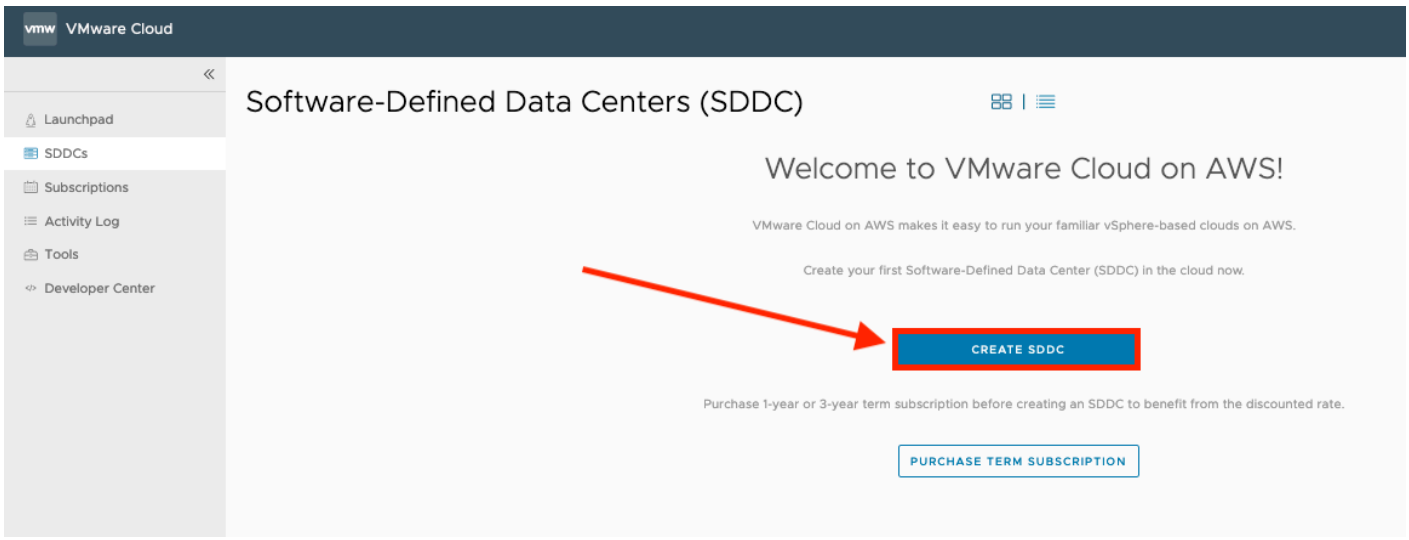
To start the deployment process, sign in to Cloud Services Portal (CSP).

1. Log in to the VMC Console at https://vmc.vmware.com.
2. Choose **VMware Cloud on AWS Service** from the services listed.



*Choose **VMware Cloud on AWS Service***

3. Choose **Create SDDC**.



*Choose **Create SDDC***

4. Enter the SDDC properties:
   - **AWS Region** — Choose the Region where you want to deploy the SDDC. This will be the same Region as the previously created VPC.

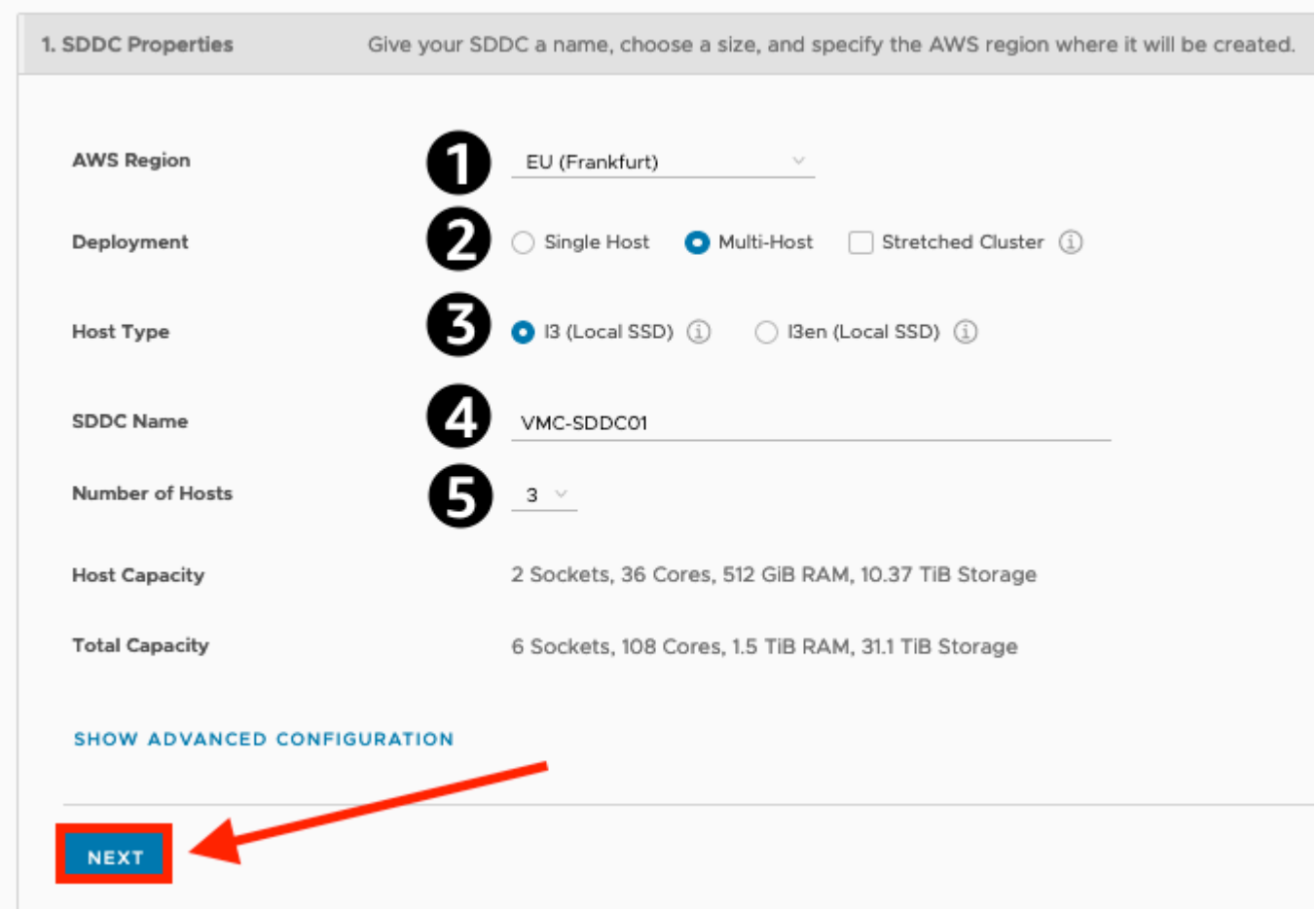
- **Deployment** — Choose **Multi-Host** or **Single-Host**. Single-Host configuration is limited to a 30-day lifespan. You can scale up to the minimum of 2-host without disruption before the 30-day period ends.
- **Host Type** — Select the host type: `i3` or `i3en`.
- **SDDC Name** — Enter the name of SDDC. This is a display name and doesn't reflect the cluster or vCenter name.
- **Number of Hosts** — if you are deploying a multi-host cluster, specify the initial number of hosts in the SDDC. You can add or remove hosts later if needed.
- **Host Capacity and Total Capacity** — This will update to reflect the number of hosts selected.
- **Show Advanced Configuration** — (Optional) 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.

  The Large SDDC type is also required for the "Edge Scale Out" feature; should be noted that if a customer plans to leverage Traffic Groups (to scale out source-based routes via distinct Edges) that this is required at deployment time. It should also be noted that this setting cannot be changed after the SDDC has been deployed.

  If you create the SDDC with a medium appliance configuration and find that you need additional management cluster resources, you can upsize the configuration to large sized appliances.

5. When you have finished, choose **Next**.



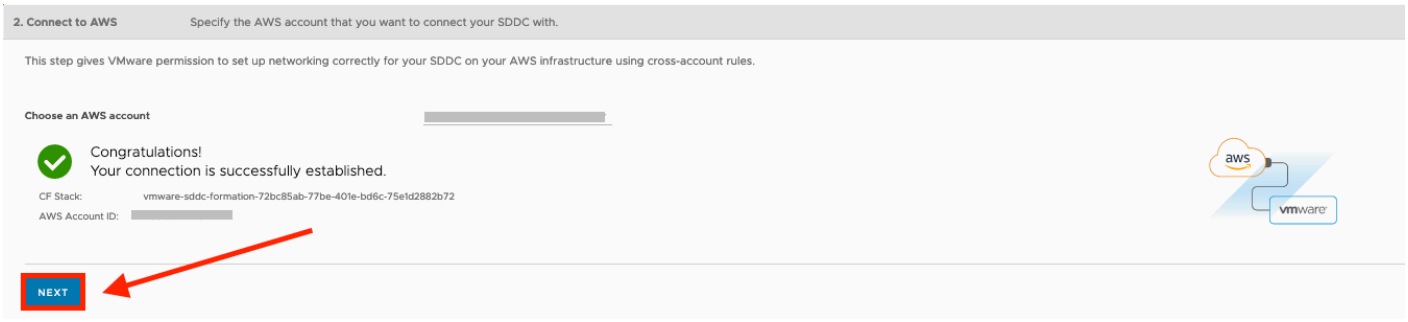
*Enter the SDDC properties and choose **NEXT***

6. Connect to your AWS account.

> **Important**
>
> After an AWS account has been associated with a VMware Organization as the seller of record, the AWS account number cannot be updated. There can be only one AWS seller of record per VMware Organization.

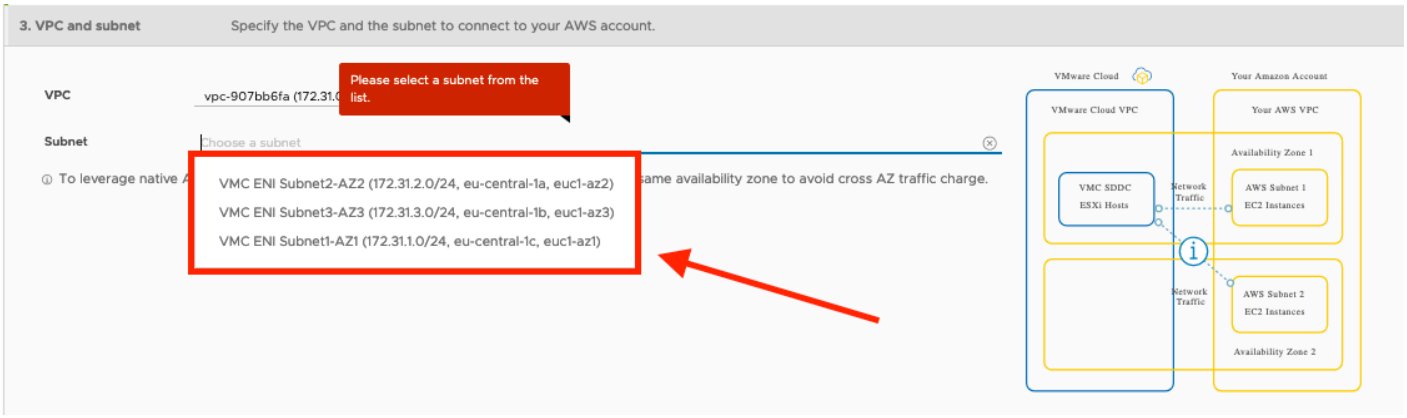
- **Connect to a new AWS account** — Select this option and follow the instructions on the page. The VMC Console shows the progress of the connection. Once completed, you can progress to the next step. The account needs to have sufficient permissions to run a CloudFormation Template in the customer account.

7. Choose **NEXT**.



*After you connect to your AWS account, choose **NEXT***

8. Select your previously-configured VPC and subnet.

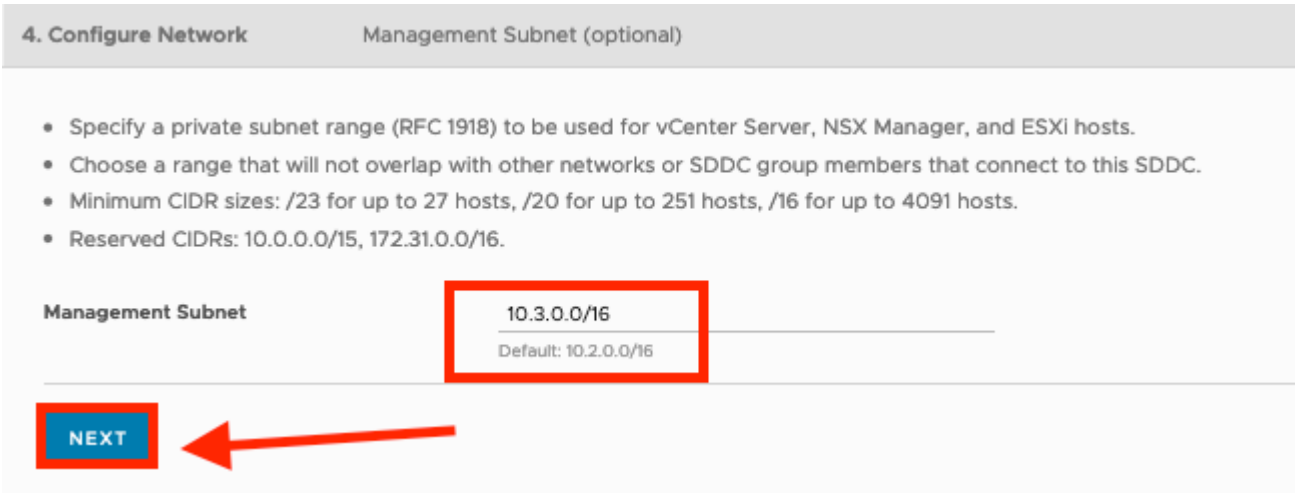


Select your previously-configured VPC and subnet.

9. Choose **NEXT**.

10. Enter the Management Subnet CIDR block for the SDDC.

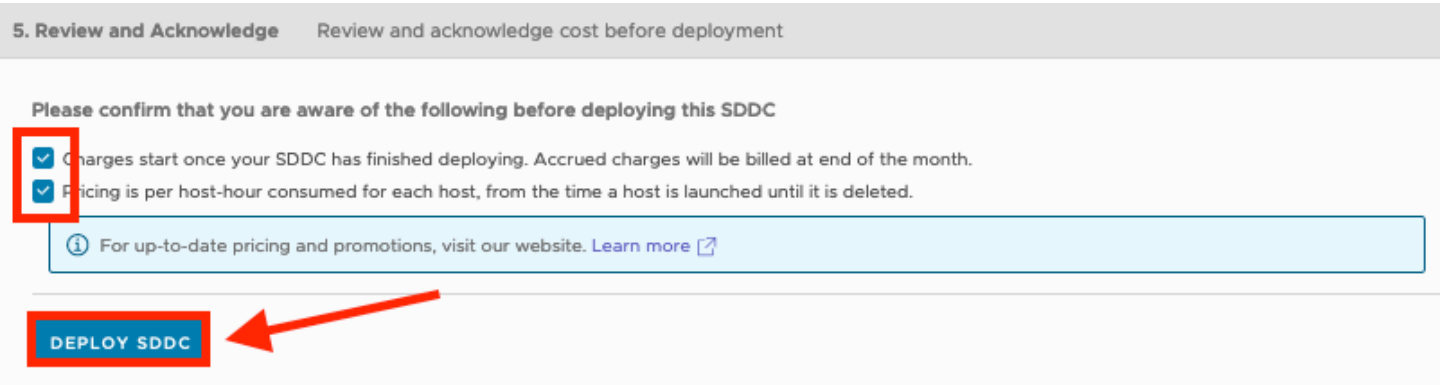
11. Choose **NEXT**.



Enter the Management Subnet CIDR block for the SDDC and choose **NEXT**

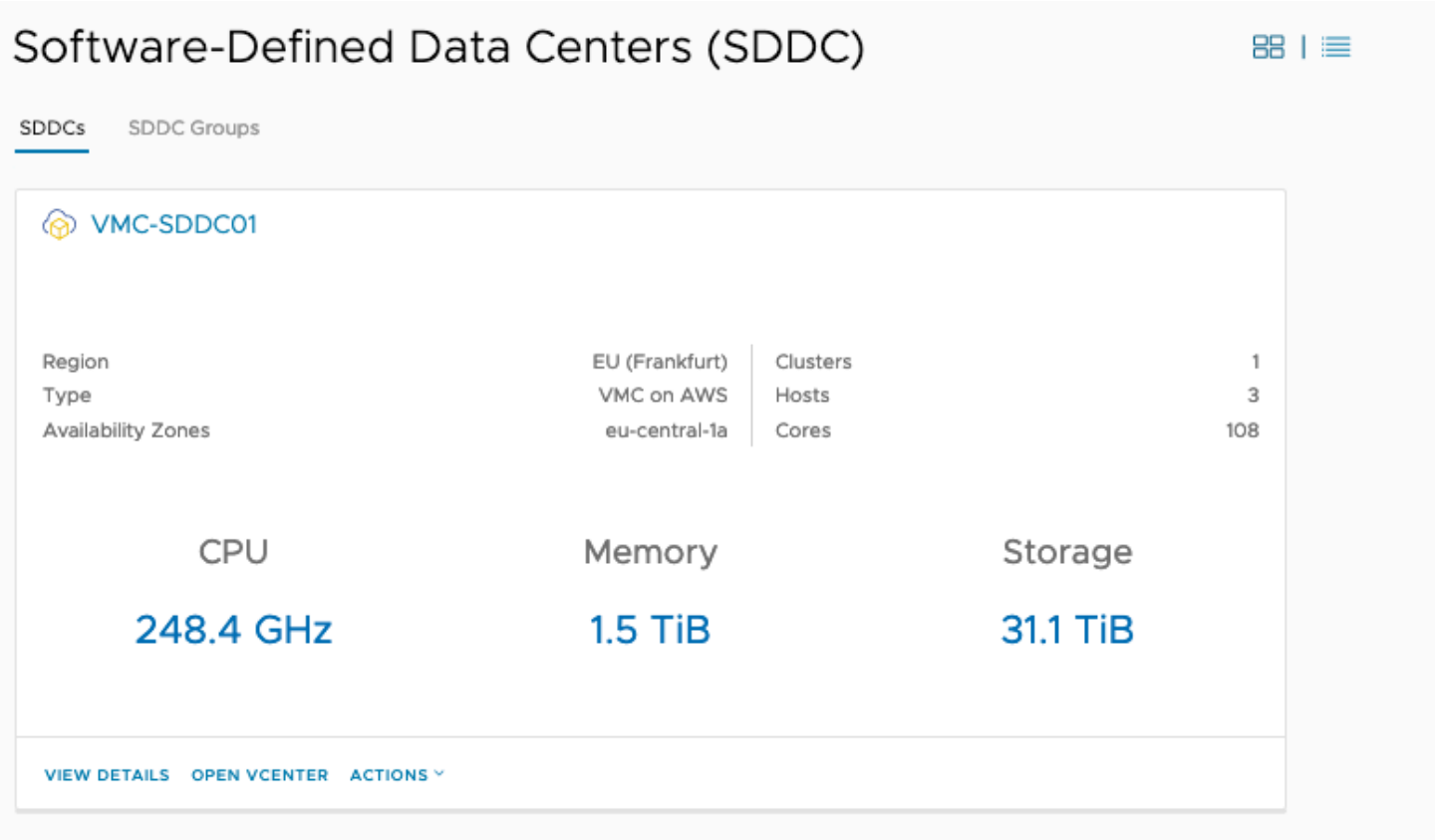
> **Important**
>
> This must be a RFC1918 private address space (`10.0.0.0/8`, `172.16.0.0/12`, or `192.168.0.0/16`) with CIDR block sizes of /16, /20, or /23. The management CIDR block cannot be changed after the SDDC is deployed. Choose a range of IP addresses that does not overlap with the AWS subnet you are connecting to. If you plan to connect the SDDC to an on-premises DC or another environment, the IP subnet must be unique within your enterprise network infrastructure. Choose a CIDR that will give you future scalability.
> Refer to the *SDDC management IP planning* entry in the *Design considerations* table, located in the the section called "Infrastructure preparation and planning" section of this document.

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



*Select **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.



A successfully deployed SDDC

Conclusion

This guide is intended for IT infrastructure architects, administrators, and IT professionals who are planning to implement a VMware Cloud Software Defined Data Center (SDDC).

You can experiment with the features and capabilities of VMware Cloud on AWS with a low-cost single host SDDC starter configuration for test and development or proof of concept use cases. You can easily scale the number of hosts within the 30-day time period to a 2+ host SDDC and retain all your data.

Contributors

Contributors to this document include:

- Kiran Reid, Partner Specialist Solutions Architect
- Osama Masfary, Specialist Solutions Architect

Appendix

IAM roles

```
"Effect": "Allow",
"Action": [
"cloudformation:CreateStack",
"cloudformation:DescribeStacks",
"cloudformation:DescribeStackEvents",
"cloudformation:DescribeStackResource",
"cloudformation:DescribeStackResources",
"cloudformation:GetTemplateSummary",
"cloudformation:ListStackResources",
"cloudformation:GetTemplate",
"cloudformation:ListChangeSets",
"cloudformation:GetStackPolicy"
],
},
{
"Effect": "Allow",
"Action": [
"iam:CreateRole",
"iam:CreatePolicy",
```

```
    "iam:AttachRolePolicy",

    "iam:GetRole",

    "iam:PassRole",

    "iam:PutRolePolicy",

    "lambda:CreateFunction",

    "lambda:InvokeFunction",

    "lambda:GetFunctionConfiguration",

    "cloudformation:DescribeStackResource",

    "cloudformation:DescribeStackResources"

    ],
```

The other roles remain in your AWS account:

- arn:aws:iam::aws:policy/AmazonVPCCrossAccountNetworkInterfaceOperations
- arn:aws:iam::role/vmware-sddc-formation-4c517b6f-1e2-BasicLambdaRole-SD4OX7YN3MNU
- arn:aws:iam::role/vmware-sddc-formation-4c517b6f-1e2-RemoteRolePayer-169300WFK6EYA
- arn:aws:iam::aws:policy/AmazonVPCCrossAccountNetworkInterfaceOperations

Document revisions

To be notified about updates to this whitepaper, subscribe to the RSS feed.

Change	Description	Date
Minor update	MyVMware is now VMware Customer Connect.	July 13, 2023
Initial publication	Whitepaper published.	May 20, 2021

Note

To subscribe to RSS updates, you must have an RSS plug-in enabled for the browser you are using.

Notices

Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) represents current AWS product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from AWS and its affiliates, suppliers or licensors. AWS products or services are provided “as is” without warranties, representations, or conditions of any kind, whether express or implied. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

AWS Glossary

For the latest AWS terminology, see the AWS glossary in the *AWS Glossary Reference*.