

Cisco DNA Center on AWS Deployment Guide, Release 1.2.1

First Published: 2023-04-17

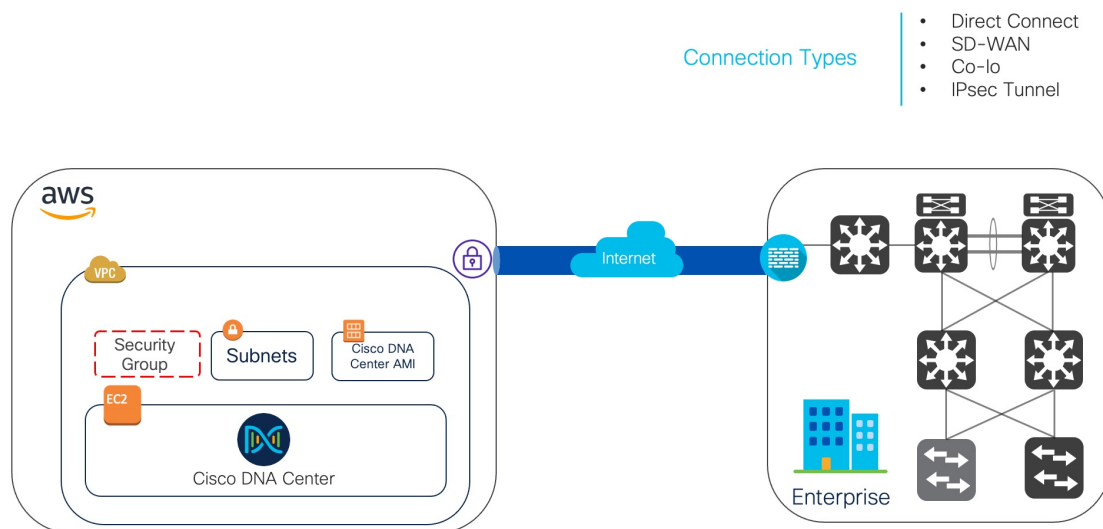
Last Modified: 2023-04-20

Cisco DNA Center on AWS Deployment Guide

Cisco DNA Center on AWS Overview

Cisco DNA Center offers centralized, intuitive management that makes it fast and easy to design, provision, and apply policies across your network environment. The Cisco DNA Center user interface provides end-to-end network visibility and uses network insights to optimize network performance and deliver the best user and application experience.

Cisco DNA Center on AWS provides the full functionality that a Cisco DNA Center appliance deployment offers. Cisco DNA Center on AWS runs in a customer's own AWS cloud environment and manages the customer's network from the cloud.



Deployment Overview

There are three ways to deploy Cisco DNA Center on AWS:

- **Automated Deployment:** Cisco DNA Center VA Launchpad configures Cisco DNA Center on AWS. It helps you create the services and components that are required for the cloud infrastructure. For example,

it helps create Virtual Private Clouds (VPCs), subnets, security groups, IPsec VPN tunnels, and gateways. Then the Cisco DNA Center Amazon Machine Image (AMI) deploys as an Amazon Elastic Compute Cloud (EC2) instance with the prescribed configuration in a new VPC along with subnets, transit gateways, and other essential resources like Amazon CloudWatch for monitoring, Amazon DynamoDB for state storage, and security groups.

Cisco provides two methods for you to use Cisco DNA Center VA Launchpad. You can download and install Cisco DNA Center VA Launchpad on a local machine, or you can access Cisco DNA Center VA Launchpad hosted by Cisco. Regardless of the method, Cisco DNA Center VA Launchpad provides the tools you need to install and manage your Cisco DNA Center Virtual Appliance (VA).

For the high-level procedure, see [Automated Deployment Workflow, on page 7](#).

- **Manual Deployment Using AWS CloudFormation:** You manually deploy the Cisco DNA Center AMI on your AWS account without Cisco DNA Center VA Launchpad. Instead, you use AWS CloudFormation, which is a deployment tool within AWS. Then you manually configure Cisco DNA Center by creating the AWS infrastructure, establishing a VPN tunnel, and deploying Cisco DNA Center. For the high-level procedure, see [Manual Deployment Using AWS CloudFormation Workflow, on page 42](#).
- **Manual Deployment Using AWS Marketplace:** You manually deploy the Cisco DNA Center AMI on your AWS account without Cisco DNA Center VA Launchpad. Instead, you use AWS Marketplace, which is an online software store within AWS. You launch the software through the Amazon Elastic Compute Cloud (Amazon EC2) launch console, and then you manually deploy Cisco DNA Center by creating the AWS infrastructure, establishing a VPN tunnel, and configuring your Cisco DNA Center VA. Note that for this deployment method, only Launch through EC2 is supported. The other two launch options (Launch from Website and Copy to Service Catalog) are not supported. For the procedure, see [Deploy Cisco DNA Center on AWS Manually Using AWS Marketplace, on page 52](#).

If you have minimal experience with the AWS administration, the automated method with Cisco DNA Center VA Launchpad offers the most streamlined, supportive installation process. If you are familiar with the AWS administration and have existing VPCs, the manual methods offer an alternative installation process.

Consider the benefits and drawbacks of each method with the following table:

Automated Deployment with Cisco DNA Center VA Launchpad	Manual Deployment Using AWS CloudFormation	Manual Deployment Using AWS Marketplace
<ul style="list-style-type: none"> • It helps create the AWS infrastructure, such as VPCs, subnets, security groups, IPsec VPN tunnels, and gateways, in your AWS account. • It automatically completes the installation of Cisco DNA Center. • It provides access to your VAs. • It provides manageability of your VAs. • Deployment time is approximately 1- 1½ hours. • Automated alerts are sent to your Amazon CloudWatch dashboard. • You can choose between an automated cloud or enterprise Network File System (NFS) backup. • Any manual alterations made to the automated configuration workflow of Cisco DNA Center on AWS can cause conflict with the automated deployment. 	<ul style="list-style-type: none"> • The AWS CloudFormation file is required to create a Cisco DNA Center VA on AWS. • You create the AWS infrastructure, such as VPCs, subnets, and security groups, in your AWS account. • You establish a VPN tunnel. • You deploy Cisco DNA Center. • Deployment time is approximately from a couple hours to a couple days. • You need to manually configure monitoring through the AWS console. • You can only configure an on-premises NFS for backups. 	<ul style="list-style-type: none"> • The AWS CloudFormation file is <i>not</i> required to create a Cisco DNA Center VA on AWS. • You create the AWS infrastructure, such as VPCs, subnets, and security groups, in your AWS account. • You establish a VPN tunnel. • You deploy Cisco DNA Center. • Deployment time is approximately from a couple hours to a couple days. • You need to manually configure monitoring through the AWS console. • You can only configure an on-premises NFS for backups.

Prepare for the Deployment

Before you deploy Cisco DNA Center on AWS, consider your network requirements and if you will need to implement supported Cisco DNA Center on AWS integrations and how you will access Cisco DNA Center on AWS.

In addition, Cisco strongly recommends you verify that the Cisco DNA Center VA TAR file you downloaded is a genuine Cisco TAR file. See [Verify the Cisco DNA Center VA TAR File, on page 6](#).

High Availability and Cisco DNA Center on AWS

The Cisco DNA Center on AWS high availability (HA) implementation is as follows:

- Single-node EC2 HA within an Availability Zone (AZ) is enabled by default.

- If a Cisco DNA Center EC2 instance crashes, AWS automatically brings up another instance in the same AZ.
- The experience and Recovery Time Objective (RTO) are similar to a power outage sequence in a bare-metal Cisco DNA Center appliance.

Guidelines for Integrating Cisco ISE on AWS with Cisco DNA Center on AWS

Cisco ISE on AWS can be integrated with Cisco DNA Center on AWS. To integrate them together in the cloud, consider the following guidelines:

- Cisco ISE on AWS should be deployed in a separate VPC from the one reserved for Cisco DNA Center VA Launchpad.
- The VPC for Cisco ISE on AWS can be in the same region as or a different region from the VPC for Cisco DNA Center on AWS.
- You can use VPC or Transit Gateway (TGW) peering, depending on your environment.
- To connect the Cisco DNA Center on AWS with Cisco ISE on AWS using a VPC or TGW peering, add the required routing entries to the VPC or TGW peering route tables and to the route table that is attached to the subnet associated with Cisco DNA Center on AWS or Cisco ISE on AWS.
- Cisco DNA Center VA Launchpad cannot detect any out-of-band changes to entities that were created by Cisco DNA Center VA Launchpad. These entities include VPCs, VPNs, TGWs, TGW attachments, subnets, routing, and so on. For example, it's possible to delete or change a VA pod that was created by Cisco DNA Center VA Launchpad from another application, and Cisco DNA Center VA Launchpad would not know about this change.

In addition to basic accessibility rules, you need to allow the following inbound ports for attaching a security group to the Cisco ISE instance in the cloud:

- For Cisco DNA Center on AWS and Cisco ISE on AWS integration, allow TCP ports 9060 and 8910.
- For radius authentication, allow UDP ports 1812, 1813, and any other enabled ports.
- For device administration via TACACS, allow TCP port 49.
- For additional settings, such as Datagram Transport Layer Security (DTLS) or RADIUS Change of Authorization (CoA) made on Cisco ISE on AWS, allow the corresponding ports.

Guidelines for Accessing Cisco DNA Center on AWS

After you create a virtual instance of Cisco DNA Center, you can access it through the Cisco DNA Center GUI and CLI.



Important

The Cisco DNA Center GUI and CLI are accessible only through the Enterprise network, not from the public network. With the automated deployment method, Cisco DNA Center VA Launchpad ensures that Cisco DNA Center is accessible only from the Enterprise intranet. With the manual deployment method, you need to ensure Cisco DNA Center is not accessible on the public intranet for security reasons.

Guidelines for Accessing the Cisco DNA Center GUI

To access the Cisco DNA Center GUI:

- Use a supported browser. For a current list of supported browsers, see the [Release Notes for Cisco DNA Center on AWS, Release 1.2.x](#).

- In a browser, enter the IP address of your Cisco DNA Center instance in the following format:

```
http://ip-address/dna/home
```

For example:

```
http://192.0.2.27/dna/home
```

- Use the following credentials for the initial login:

Username: **admin**

Password: **maglev1@3**



Note You are required to change this password when you log in to Cisco DNA Center for the first time.

Guidelines for Accessing the Cisco DNA Center CLI

To access the Cisco DNA Center CLI:

- Use the IP address and keys corresponding to the method you used to deploy Cisco DNA Center:
 - If you deployed Cisco DNA Center using Cisco DNA Center VA Launchpad, use the IP address and keys provided by Cisco DNA Center VA Launchpad.
 - If you deployed Cisco DNA Center manually using AWS, use your IP address and the keys provided by AWS.



Note The key must be a .pem file. If the key file is downloaded as key.cer file, you need to rename the file to key.pem.

- Manually change the access permissions on the key.pem file to 400. Use the Linux **chmod** command to change the access permissions. For example:

```
chmod 400 key.pem
```

- Use the following Linux command to access the Cisco DNA Center CLI:

```
ssh -i key.pem maglev@ip-address -p 2222
```

For example:

```
ssh -i key.pem maglev@192.0.2.27 -p 2222
```

Verify the Cisco DNA Center VA TAR File

Before deploying the Cisco DNA Center VA, we strongly recommend that you verify that the TAR file you downloaded is a genuine Cisco TAR file.

Before you begin

Ensure that you've downloaded Cisco DNA Center VA TAR file from the [Cisco Software Download](#) site.

Procedure

-
- Step 1** Download the Cisco public key (`cisco_image_verification_key.pub`) for signature verification from the location specified by Cisco.
 - Step 2** Download the secure hash algorithm (SHA512) checksum file for the TAR file from the location specified by Cisco.
 - Step 3** Obtain the TAR file's signature file (`.sig`) from Cisco support through email or by download from the secure Cisco website (if available).
 - Step 4** (Optional) Perform an SHA verification to determine whether the TAR file is corrupted due to a partial download.

Depending on your operating system, enter one of the following commands:

- On a Linux system: **sha512sum** <tar-file-filename>
- On a Mac system: **shasum -a 512** <tar-file-filename>

Microsoft Windows does not include a built-in checksum utility, but you can use the `certutil` tool:

```
certutil -hashfile <filename> sha256
```

For example:

```
certutil -hashfile D:\Customers\FINALIZE.BIN sha256
```

On Windows, you can also use the [Windows PowerShell](#) to generate the digest. For example:

```
PS C:\Users\Administrator> Get-FileHash -Path D:\Customers\FINALIZE.BIN
Algorithm Hash Path
SHA256 B84B6FFD898A370A605476AC7EC94429B445312A5EEDB96166370E99F2838CB5
D:\Customers\FINALIZE.BIN
```

Compare the command output to the SHA512 checksum file that you downloaded. If the command output does not match, download the TAR file again and run the appropriate command a second time. If the output still does not match, contact Cisco support.

- Step 5** Verify that the TAR file is genuine and from Cisco by verifying its signature:

```
openssl dgst -sha512 -verify cisco_image_verification_key.pub -signature <signature-filename>
<tar-file-filename>
```

Note This command works in both Mac and Linux environments. For Windows, you must download and install OpenSSL (available on the [OpenSSL Downloads](#) site) if you have not already done so.

If the TAR file is genuine, running this command displays a `verified OK` message. If this message fails to appear, do not install the TAR file and contact Cisco support.

Deploy Cisco DNA Center on AWS Using the Automated Deployment Method

You provide Cisco DNA Center VA Launchpad with the needed details to create the AWS infrastructure in your AWS account, which includes a VPC, IPsec VPN tunnel, gateways, subnets, and security groups. As a result, Cisco DNA Center VA Launchpad deploys the Cisco DNA Center AMIs as an Amazon EC2 instance with the prescribed configuration in a separate VPC. The configuration includes the subnets, transit gateways, and other essential resources like Amazon CloudWatch for monitoring, Amazon DynamoDB for state storage, and security groups.

Using Cisco DNA Center VA Launchpad, you can also access and manage your VAs, as well as manage the user settings.

Automated Deployment Workflow

To deploy Cisco DNA Center on AWS using the automated method, follow these high-level steps:

1. Make sure the prerequisites are met. See [Prerequisites for Automated Deployment, on page 8](#).
2. If you plan on integrating Cisco ISE on AWS and Cisco DNA Center VA together, see [Guidelines for Integrating Cisco ISE on AWS with Cisco DNA Center on AWS, on page 4](#).
3. Install Cisco DNA Center VA Launchpad or access Cisco DNA Center VA Launchpad hosted by Cisco. See [Install Cisco DNA Center VA Launchpad, on page 11](#) or [Access Hosted Cisco DNA Center VA Launchpad, on page 12](#).
4. Create a new VA pod to contain your Cisco DNA Center VA instance. See [Create a New VA Pod, on page 21](#).
5. If you are using an existing TGW and existing attachments, such as a VPC, as your preferred on-premises connectivity, you must manually configure the TGW routing table on AWS and add the routing configuration to your existing Customer Gateway (CGW). See [Manually Configure Routing on Existing Transit and Customer Gateways, on page 31](#).
6. Create your new instance of Cisco DNA Center. See [Create a New Cisco DNA Center VA, on page 32](#).
7. If necessary, troubleshoot any issues that arise during the deployment. See [Troubleshoot the Deployment, on page 37](#).
8. After successfully deploying Cisco DNA Center VA, you can use Cisco DNA Center VA Launchpad to manage your VAs. See [Manage VA Pods and User Settings Using Cisco DNA Center VA Launchpad, on page 60](#).

Prerequisites for Automated Deployment

These prerequisites are for the automated deployment. You can also deploy Cisco DNA Center VA manually using AWS CloudFormation or AWS Marketplace. To understand the benefits and drawbacks of each method, see [Deployment Overview, on page 1](#).



Note To enable access to the new regions added in Release 1.2.x, your admin user needs to log in to Cisco DNA Center VA Launchpad after the Cisco DNA Center VA Launchpad, Release 1.2.x has been installed. After the admin user has logged in, access to all regions is enabled for all other users.

Before you can begin to deploy Cisco DNA Center on AWS, make sure that the following requirements are met:

- If you choose to deploy and manage Cisco DNA Center VA via Cisco DNA Center VA Launchpad, you must install Docker Desktop on your platform.

Cisco DNA Center VA Launchpad supports Docker Desktop on Mac, Windows, and Linux platforms. See the following documentation on the Docker website for the specific procedure for your platform:

- For Mac platforms, see <https://docs.docker.com/desktop/install/mac-install/>.
- For Windows platforms, see <https://docs.docker.com/desktop/install/windows-install/>.
- For Linux platforms, see <https://docs.docker.com/desktop/install/linux-install/>.
- Regardless of how you access Cisco DNA Center VA Launchpad to deploy Cisco DNA Center VA, make sure that your cloud environment meets the following specifications:
 - **DNACInstance:** r5a.8xlarge, 32 vCPUs, 256-GB RAM, and 4-TB storage



Note The r5a.8xlarge instance size is not supported for the us-east-1e availability zone in the us-east-1 region.

- **BackupInstance:** T3.micro, 2 vCPUs, 500-GB storage, and 1-GB RAM
- Your AWS account is a subaccount (a child account) to maintain resource independence and isolation. With a subaccount, this ensures that the Cisco DNA Center deployment doesn't impact your existing resources.
- You have valid credentials to access your AWS account.
- If you're an admin user, you must have the administrator access permission for your AWS account. (In AWS, the policy name is displayed as **AdministratorAccess**.)

The administrator access policy must be attached to your AWS account directly and not to a group. The application doesn't enumerate through a group policy. So, if you are added to a group with the administrator access permission, you will not be able to create the required infrastructure.

The screenshot shows the AWS IAM console interface. At the top, there is a navigation bar with the AWS logo, a search bar, and the user's profile information. Below the navigation bar, there is a notification banner with a blue background and a white '1' icon, stating: "New feature to generate a policy based on CloudTrail events. AWS uses your CloudTrail events to identify the services and actions used and generate a least privileged policy that you can attach to this user." Below the notification, the main content area is titled "Users > dna-tme-user" and "Summary". The summary section shows the user's ARN as "arn:aws:iam::878813814009:user/dna-tme-user", the path as "/", and the creation time as "2022-07-23 16:11 PDT". There are tabs for "Permissions", "Groups", "Tags", "Security credentials", and "Access Advisor". The "Permissions" tab is active, showing "Permissions policies (1 policy applied)". There is a blue "Add permissions" button and a blue "Add inline policy" button. Below this, there is a table with columns "Policy name" and "Policy type". Under "Attached directly", there is one entry: "AdministratorAccess" with a yellow icon and "AWS managed policy". Below this, there are sections for "Permissions boundary (not set)" and "Generate policy based on CloudTrail events". The "Generate policy based on CloudTrail events" section contains a paragraph: "You can generate a new policy based on the access activity for this user, then customize, create, and attach it to this role. AWS uses your CloudTrail events to identify the services and actions used and generate a policy. [Learn more](#)" and a blue "Generate policy" button.

- If you're a subuser, your administrator must add you to the CiscoDNACenter user group.

When an admin user logs in to Cisco DNA Center VA Launchpad for the first time, the CiscoDNACenter user group is created on their AWS account with all the required policies attached. The admin user can add subusers to this group to allow them to log in to Cisco DNA Center VA Launchpad.

The following policies are attached to the CiscoDNACenter user group:

- AmazonDynamoDBFullAccess
- IAMReadOnlyAccess
- AmazonEC2FullAccess
- AWSCloudFormationFullAccess
- AWSLambda_FullAccess
- CloudWatchFullAccess
- ServiceQuotasFullAccess
- AmazonEventBridgeFullAccess
- service-role/AWS_ConfigRole
- AmazonS3FullAccess
- ClientVPNServiceRolePolicy (Version: 2012-10-17) This policy allows the following rules:
 - ec2:CreateNetworkInterface
 - ec2:CreateNetworkInterfacePermission
 - ec2:DescribeSecurityGroups
 - ec2:DescribeVpcs
 - ec2:DescribeSubnets
 - ec2:DescribeInternetGateways

- ec2:ModifyNetworkInterfaceAttribute
 - ec2>DeleteNetworkInterface
 - ec2:DescribeAccountAttributes
 - ds:AuthorizeApplication
 - ds:DescribeDirectories
 - ds:GetDirectoryLimits
 - ds:UnauthorizeApplication
 - logs:DescribeLogStreams
 - logs>CreateLogStream
 - logs:PutLogEvents
 - logs:DescribeLogGroups
 - acm:GetCertificate
 - acm:DescribeCertificate
 - iam:GetSAMLProvider
 - lambda:GetFunctionConfiguration
- ConfigPermission (Version: 2012-10-17, Sid: VisualEditor0) This policy allows the following rules:
 - config:Get
 - config:*
 - config:*ConfigurationRecorder
 - config:Describe*
 - config:Deliver*
 - config:List*
 - config>Select*
 - tag:GetResources
 - tag:GetTagKeys
 - cloudtrail:DescribeTrails
 - cloudtrail:GetTrailStatus
 - cloudtrail:LookupEvents
 - config:PutConfigRule
 - config>DeleteConfigRule
 - config>DeleteEvaluationResults

- PassRole (Version: 2012-10-17, Sid: VisualEditor0) This policy allows the following rules:
 - iam:GetRole
 - iam:PassRole

Install Cisco DNA Center VA Launchpad

This procedure shows you how to install Cisco DNA Center VA Launchpad using Docker containers for the server and client applications.



Note You cannot update from a previous version of Cisco DNA Center VA Launchpad to Cisco DNA Center VA Launchpad, Version 1.2.x. You need to reinstall Docker Desktop and then install Cisco DNA Center VA Launchpad, Version 1.2.x.

Before you begin

Make sure you have Docker Desktop installed on your machine. For information, see [Prerequisites for Automated Deployment, on page 8](#).

Procedure

- Step 1** Go to the [Cisco Software Download](#) site and download the following files:
- Launchpad-desktop-client-1.2.1.tar.gz
 - Launchpad-desktop-server-1.2.1.tar.gz
- Step 2** Verify that the TAR file is genuine and from Cisco. For detailed steps, see [Verify the Cisco DNA Center VA TAR File, on page 6](#).
- Step 3** Load the Docker images from the downloaded files:
- ```
docker load < Launchpad-desktop-client-1.2.1.tar.gz
docker load < Launchpad-desktop-server-1.2.1.tar.gz
```
- Step 4** Use the **docker images** command to display a list of the Docker images in the repository and verify that you have the latest copies of the server and client applications. The files should display **1.2.1** in the **TAG** column. For example:
- ```
$ docker images
```
- | REPOSITORY | TAG | IMAGE ID | CREATED | SIZE |
|--|-------|--------------|------------|-------|
| dockerhub.cisco.com/maglev-docker/server | 1.2.1 | f87ff30d4c6a | 6 days ago | 435MB |
| dockerhub.cisco.com/maglev-docker/client | 1.2.1 | dd50d550aa7c | 6 days ago | 832MB |
- Step 5** Run the server application:
- ```
docker run -d -p <server-port-number>:8080 -e DEBUG=true --name server
<server_image_id>
```

For example:

```
$ docker run -d -p 9090:8080 -e DEBUG=true --name server f87ff30d4c6a
```

### Step 6

Run the client application:

```
docker run -d -p <client-port-number>:80 -e CHOKIDAR_USEPOLLING=true -e
REACT_APP_API_URL=http://localhost:<server-port-number> --name client
<client_image_id>
```

For example:

```
$ docker run -d -p 90:80 -e CHOKIDAR_USEPOLLING=true -e
REACT_APP_API_URL=http://localhost:9090 --name client dd50d550aa7c
```

**Note** Make sure that the exposed server port number and the REACT\_APP\_API\_URL port number are the same. In steps 5 and 6, port number 9090 is used in both examples.

### Step 7

Use the **docker ps -a** command to verify that the server and client applications are running. The **STATUS** column should show that the applications are up.

For example:

```
$ docker ps -a
```

| CONTAINER ID | IMAGE                                          | COMMAND                  | CREATED        | STATUS        | PORTS                  | NAMES  |
|--------------|------------------------------------------------|--------------------------|----------------|---------------|------------------------|--------|
| 5584b62d4170 | dockerhub.cisco.com/maglev-docker/server:1.2.1 | "docker-entrypoint.s..." | 33 seconds ago | Up 32 seconds | 0.0.0.0:9090->8080/tcp | server |
| c771a7eb9c10 | dockerhub.cisco.com/maglev-docker/client:1.2.1 | "docker-entrypoint.s..." | 58 seconds ago | Up 57 seconds | 0.0.0.0:90->80/tcp     | client |

**Note** If you encounter an issue while running the server or client applications, see [Troubleshoot Docker Issues, on page 37](#).

### Step 8

Verify that the server application is accessible by entering the URL in the following format:

```
http://<localhost>:<server-port-number>/api/valaunchpad/api-docs/
```

For example:

```
http://192.0.2.2:9090/api/valaunchpad/api-docs/
```

The application programming interfaces (APIs) being used for the Cisco DNA Center VA are displayed in the window.

### Step 9

Verify that the client application is accessible by entering the URL in the following format:

```
http://<localhost>:<client-port-number>/valaunchpad
```

For example:

```
http://192.0.2.1:90/valaunchpad
```

The Cisco DNA Center VA Launchpad login window is displayed.

**Note** It can take a few minutes to load the Cisco DNA Center VA Launchpad login window as the client and server applications load the artifacts.

## Access Hosted Cisco DNA Center VA Launchpad

You can access Cisco DNA Center VA Launchpad with Cisco DNA Portal.

If you are new to Cisco DNA Portal, you must create a Cisco account and a Cisco DNA Portal account. Then you can log in to Cisco DNA Portal to access Cisco DNA Center VA Launchpad.

If you are familiar with Cisco DNA Portal and have a Cisco account and a Cisco DNA Portal account, you can directly log in to Cisco DNA Portal to access Cisco DNA Center VA Launchpad.

## Create a Cisco Account

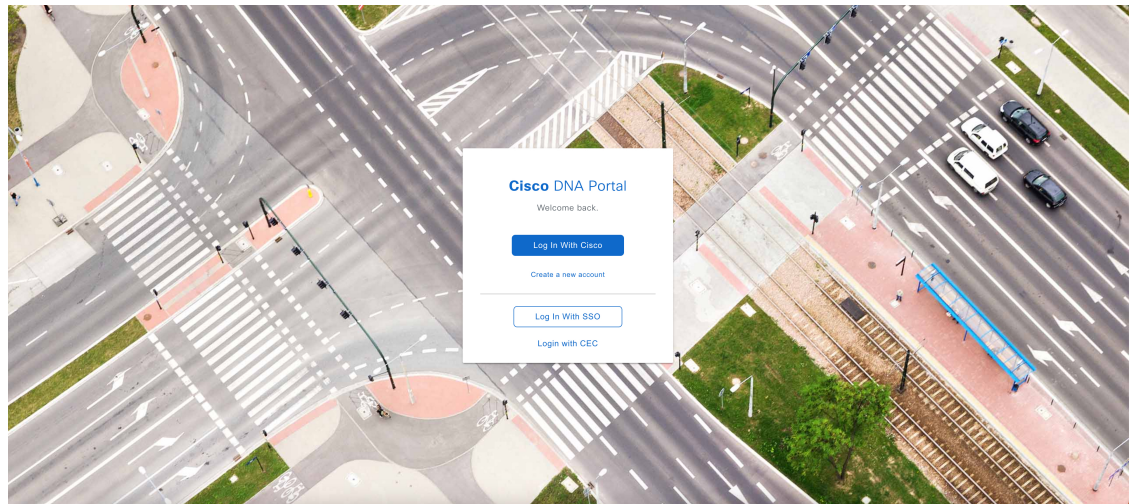
To access Cisco DNA Center VA Launchpad through Cisco DNA Portal, you first must create a Cisco account.

### Procedure

**Step 1** In your browser, enter:

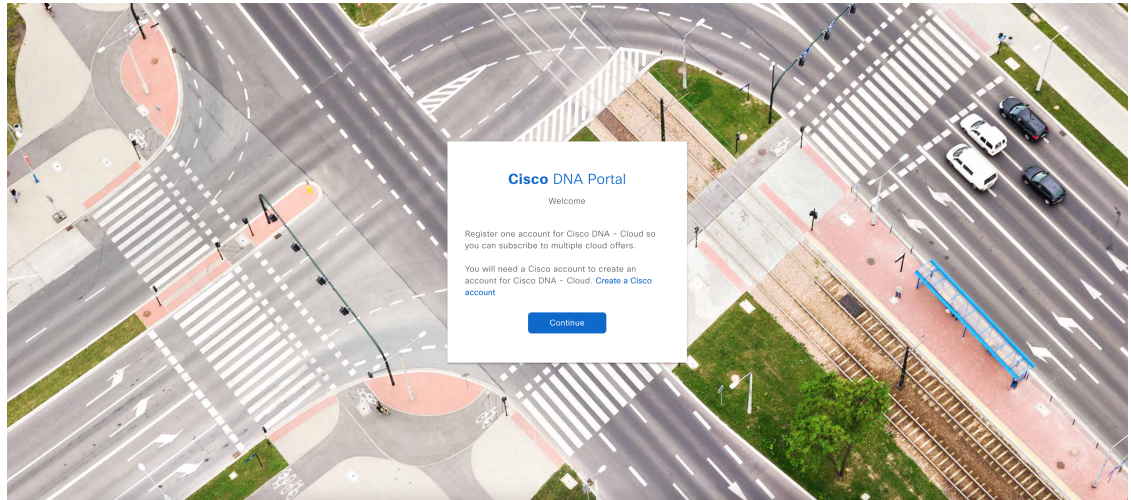
**`dna.cisco.com`**

The **Cisco DNA Portal** login window is displayed.



**Step 2** Click **Create a new account**.

**Step 3** On the **Cisco DNA Portal Welcome** window, click **Create a Cisco account**.



**Step 4** On the **Create Account** window, complete the required fields and then click **Register**.

US  
EN

**CREATE ACCOUNT**

\* Indicates required field

Email \*

Password \*

First name \*

Last name \*

Country or region \*

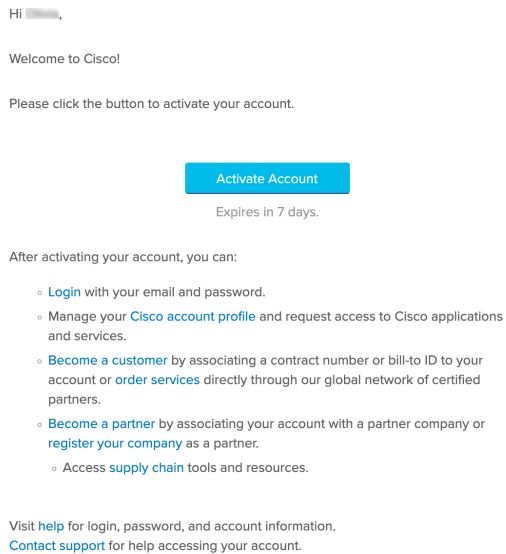
Please select \*

By clicking Register, I confirm that I have read and agree to the [Cisco Online Privacy Statement](#) and the [Cisco Web Site Terms and Conditions](#).

Register

[Back to log in](#)

**Step 5** Verify your account by going to the email that you assigned to your account and clicking **Activate Account**.



---

## Create a Cisco DNA Portal Account

To access Cisco DNA Center VA Launchpad through Cisco DNA Portal, you must create a Cisco DNA Portal account.

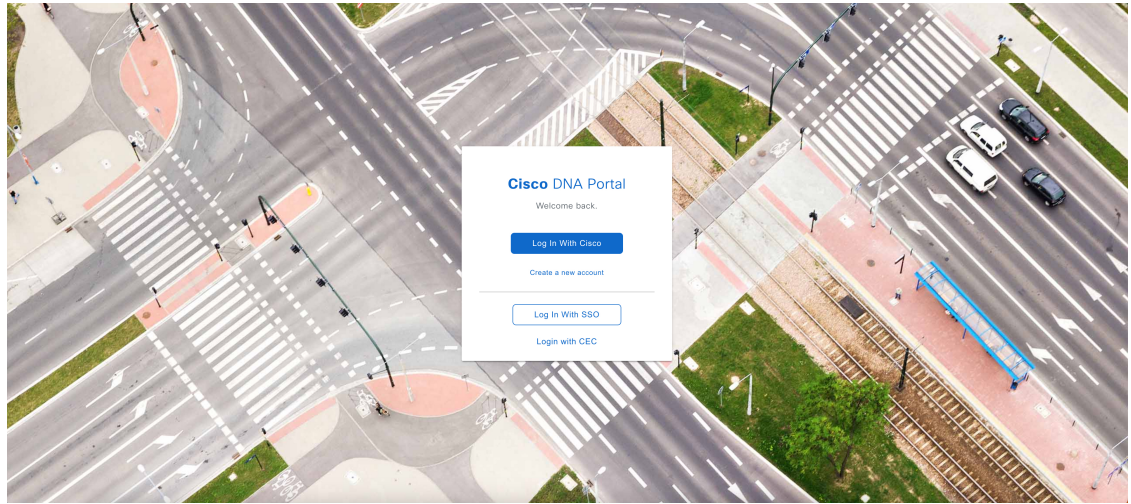
### Before you begin

Make sure that you have a Cisco account. For more information, see [Create a Cisco Account, on page 13](#).

### Procedure

---

- Step 1** In your browser, enter:
- `dna.cisco.com`**
- The **Cisco DNA Portal** login window is displayed.



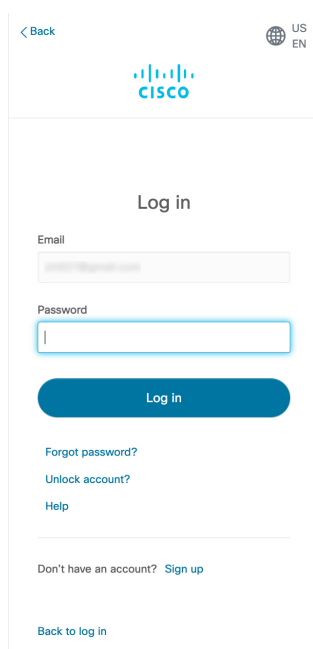
**Step 2** Click **Log In With Cisco**.

**Step 3** Enter your Cisco account's email in the **Email** field, and click **Next**.

A screenshot of the Cisco DNA Portal login page. At the top left is the Cisco logo. At the top right is a language selector with a globe icon and 'US' and 'EN' options. Below the logo is the heading 'Log in'. Underneath is an 'Email' label followed by an empty text input field. Below the input field is a blue 'Next' button. Under the button are three links: 'Unlock account?', 'Forgot email address?', and 'Help'. At the bottom of the form is a link: 'Don't have an account? Sign up'.

**Step 4** Enter your Cisco account's password in the **Password** field, and click **Log in**.





The screenshot shows the Cisco DNA Portal login interface. At the top left is a '< Back' link. The Cisco logo is centered at the top. To the right is a globe icon with 'US' and 'EN' labels. Below the logo is the heading 'Log in'. There are two input fields: 'Email' and 'Password'. Below the password field is a blue 'Log in' button. Underneath are links for 'Forgot password?', 'Unlock account?', and 'Help'. At the bottom, there is a link 'Don't have an account? Sign up' and a 'Back to log in' link.

- Step 5** On the **Cisco DNA Portal Welcome** window, enter the name of your organization or team in the **Name your account** field. Then click **Continue**.

## Cisco DNA Portal

Welcome, [blurred]

What's the name of your organization, company, or team?

Name your account\*

Ex. Hearst or Hearst Construction

Cancel

Continue

- Step 6** On the **Cisco DNA Portal Confirm CCO Profile** window, do the following:
- Verify the details are correct.
  - After reading, acknowledging, and agreeing with the conditions, check the check box.
  - Click **Create Account**.

## Log In to the Cisco DNA Portal With Cisco

### Cisco DNA Portal

Confirm CCO Profile

Confirm that this is the Cisco profile you would like to register with, or [login to a different CCO](#).

Your Name   
 Your Email   
 Organization Name

I agree that Cisco DNA Portal is governed by the [Cisco End User License Agreement](#) and that I have read and acknowledge the [Cisco Privacy Statement](#).

*Note: If you do not have the authority to bind your company and its affiliates, or if you do not agree with the terms of the Cisco Universal Cloud Agreement, do not check this box.*

Create Account

After successfully creating an account, the **Cisco DNA Portal** home page is displayed.

Subscribe and maintain your offers more efficiently with Cisco DNA Portal.

Select an offer below and enjoy your trip with Cisco DNA Portal.

Offers

| Applications Experience                                                                                                                                                                                              | Cisco DNA Center Cloud                                                                                                                                                                                                                                                                                                                                              | SAN Insights Discovery                                                                                                                                                                                                                                                                                                                                                           | Plug and Play as a Service                                                                                                                                                                                                                                              | pxGrid Cloud                                                                                                                                                                                                                                      |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Application Experience enables Cisco DNA Center users to integrate with AppX cloud service to collect quality metrics and to enrich Cisco DNA Center application dashboards to get better visibility on the network. | Cisco DNA Center Cloud provides complete, cloud-based lifecycle management of Cisco Catalyst 9200, 9300, and 9500 Series Switches and Cisco Catalyst 9100 Series Access Points in Embedded Wireless Controller (EWC) mode. Network administrators can manage their wired and wireless network infrastructure at the site-level using a secure cloud user interface. | SAN Insights Discovery as a SaaS offering on DNAC Cloud. This is a much-awaited pre-sales tool for Cisco Sales, Account team and Partners. It provides a comprehensive health check of any customer SAN fabric. SID works for existing Brocade and Cisco SAN fabrics. SID helps the Cisco team to better understand what the customer has and how Cisco can help moving forward. | Plug and Play as a service enables users to securely day-0 onboard Catalyst 9K family of devices. During onboarding process you can upgrade image and deploy configuration to the device. After onboarding you can redirect the device to be managed by DNA controller. | Cisco pxGrid Cloud enables users to securely share context between on-premise Cisco ISE and cloud based applications. It is customizable, ensuring that only relevant data is shared. It is included as part of your Cisco ISE Advantage license. |
| <a href="#">Subscribe</a>                                                                                                                                                                                            | <a href="#">Subscribe</a><br><a href="#">Learn More</a>                                                                                                                                                                                                                                                                                                             | <a href="#">Subscribe</a><br><a href="#">Learn More</a>                                                                                                                                                                                                                                                                                                                          | <a href="#">Subscribe</a>                                                                                                                                                                                                                                               | <a href="#">Subscribe</a>                                                                                                                                                                                                                         |

## Log In to the Cisco DNA Portal With Cisco

To access Cisco DNA Center VA Launchpad through Cisco DNA Portal, you must log in to Cisco DNA Portal.

### Before you begin

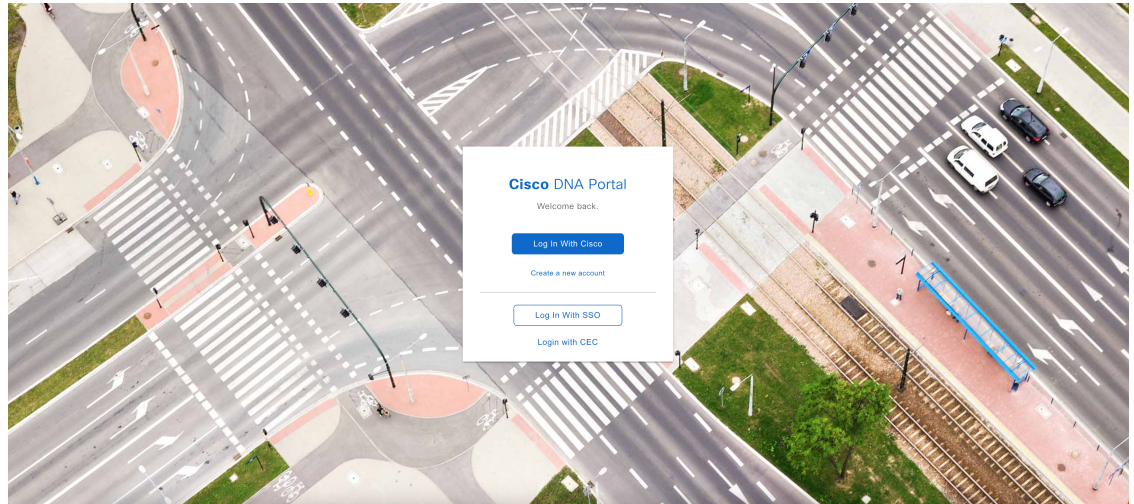
Make sure that you have a Cisco account and a Cisco DNA Portal account. For more information, see [Create a Cisco Account](#), on page 13 and [Create a Cisco DNA Portal Account](#), on page 15.

## Procedure

**Step 1** In your browser, enter:

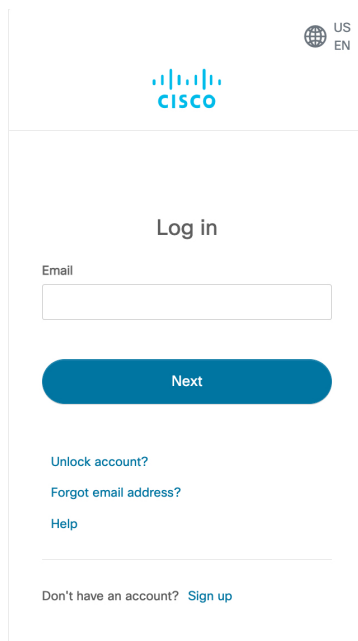
**`dna.cisco.com`**

The **Cisco DNA Portal** login window is displayed.



**Step 2** Click **Log In With Cisco**.

**Step 3** Enter your Cisco account's email in the **Email** field, and click **Next**.



**Step 4** Enter your Cisco account's password in the **Password** field, and click **Log in**.

If you only have one Cisco DNA Portal account, the **Cisco DNA Portal** home page displays.

- Step 5** (Optional) If you have multiple Cisco DNA Portal accounts, choose the account that you want to log in to by clicking the account's adjacent **Continue** button.

The **Cisco DNA Portal** home page is displayed.

## Create a New VA Pod

A VA pod is the AWS hosting environment for the Cisco DNA Center VA. The hosting environment includes AWS resources, such as the Cisco DNA Center VA EC2 instance, Amazon Elastic Block Storage (EBS), backup NFS server, security groups, routing tables, Amazon CloudWatch logs, Amazon Simple Notification System (SNS), VPN Gateway (VPN GW), TGW, and so on.

On Cisco DNA Center VA Launchpad, you can create multiple VA pods. You can use each VA pod to create and manage a Cisco DNA Center VA instance.



### Note

- The AWS Super Administrator user can set a limit on the number of VA pods that can be created in each region. VPCs used for resources outside of the Cisco DNA Center VA Launchpad contribute to this number as well. For example, if your AWS account has a limit of five VPCs, two of which are already in use, then you can only create a maximum of three VA pods for the selected region.
- On some steps, all the resources must be set up successfully to proceed to the next step. If all resources haven't been set up successfully, the proceed button is disabled. If all the resources have been set up successfully and the proceed button is disabled, wait a few seconds because the resources are still loading. After all the configurations are complete, the button is enabled.

This procedure guides you through the steps to create a new VA pod.

### Before you begin

Your AWS account must have administrator access permission to perform this procedure. For information, see [Prerequisites for Automated Deployment, on page 8](#).

## Procedure

**Step 1** Log in to Cisco DNA Center VA Launchpad.

**Note** Do not open the application in more than one browser tab, in multiple browser windows, or in multiple browser applications at the same time.

a) From a browser window, do one of the following:

- If you installed Cisco DNA Center VA Launchpad locally, enter the Cisco DNA Center VA Launchpad URL in the following format:

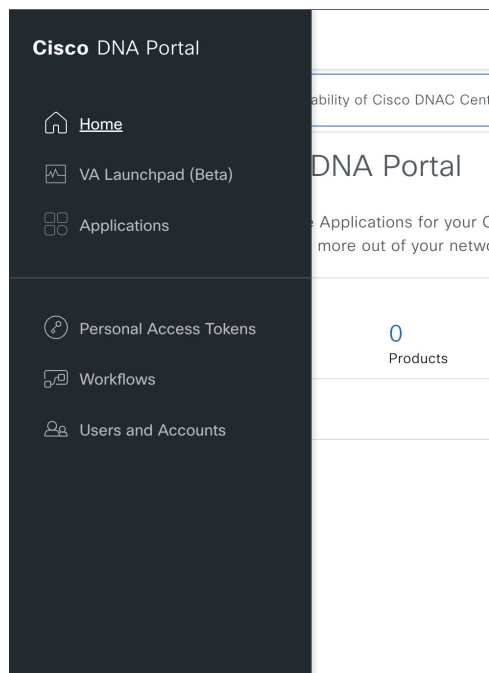
**http://<localhost>:<client-port-number>/valaunchpad**

For example:

**http://192.0.2.1:90/valaunchpad**

- If you are accessing the hosted Cisco DNA Center VA Launchpad, enter **dna.cisco.com** and follow the steps to log in. (For information, see [Log In to the Cisco DNA Portal With Cisco, on page 18.](#))

From the **Cisco DNA Portal** home page, click the menu icon ( ≡ ) and choose **VA Launchpad (Beta)**.



The AWS login window is displayed.

**AWS Access**

Fill the AWS details to connect to your AWS account.

For more details, check <https://docs.aws.amazon.com/general/latest/gr/aws-sec-cred-types.html>

IAM Login  Federated Login

AWS Account ID ⓘ

Access Key ID ⓘ

Secret Access Key ⓘ

Authenticate

b) Choose your user login, and then enter your credentials in the fields:

- **IAM Login**

For more information, see [Log In with Cisco](#), on page 60.

- **Federated Login**

For more information, see [Log In as a Federated User Using saml2aws-Generated Credentials](#), on page 63 or [Log In as a Federated User Using AWS CLI-Generated Credentials](#), on page 66.

For information about how to get an Access Key ID and Secret Access Key, see the [AWS Account and Access Keys](#) topic in the *AWS Tools for PowerShell User Guide* on the AWS website.

c) Click **Authenticate**. If you encounter any login errors, you need to resolve them and log in again. For more information, see [Troubleshoot the Deployment](#), on page 37.

If you are an admin user logging in for the first time, several processes happen:

- You are prompted to enter your email address. Enter your email address in the **Email ID** field and click **Submit**.

#### Email to Notify

Please enter the Email address where notification needs to be sent if there are any Alerts on AWS Infrastructure.

Email ID ⓘ

Updating the email address will be used for newer VA Pods and not for existing VA Pods

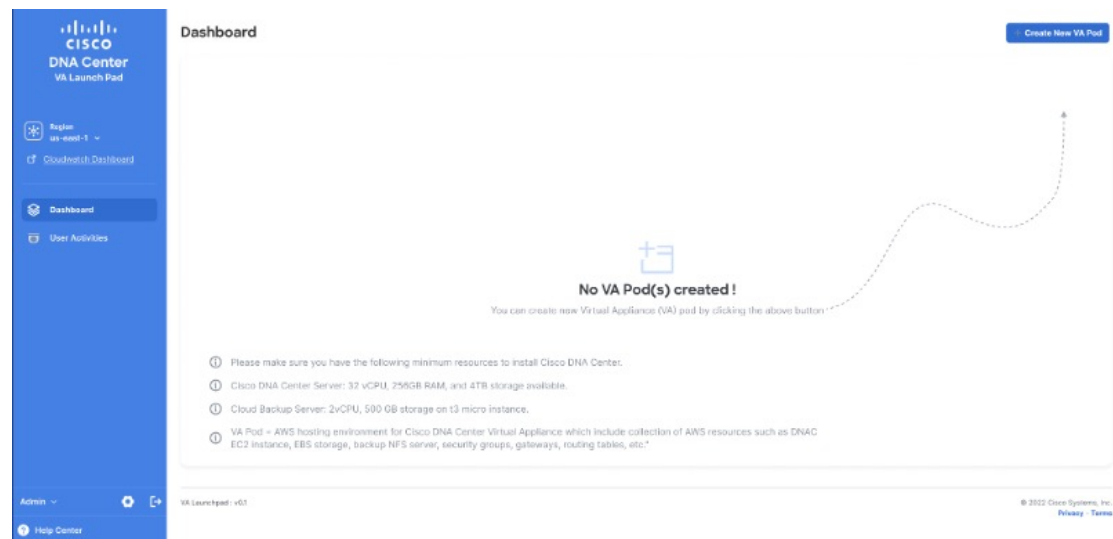
Your email address is used to notify you of alarms and to send you audit logs of your configured resources. Alarms can be triggered if Amazon CloudWatch detects any unusual behavior in Cisco DNA Center VA Launchpad. In addition, AWS Config evaluates and assesses your configured resources and sends audit logs of the results as well. For more information about updating your email

address, see [Configure Amazon CloudWatch Notifications, on page 82](#), and for details about Amazon CloudWatchalarms, see [View Amazon CloudWatch Alarms, on page 83](#).

- The CiscoDNACenter user group is created on their AWS account with all the required policies attached. The admin user can add subusers to this group to allow subusers to log in to Cisco DNA Center VA Launchpad.
- An S3 bucket is automatically created to store the state of the deployment. We recommend that you do not delete this or any other bucket from the AWS account, either globally or for each region. Doing so could impact the Cisco DNA Center VA Launchpad deployment workflow.
- If you are also logging in to a region for the first time, Cisco DNA Center VA Launchpad creates several resources in AWS. This process can take some time, depending on whether the region was previously enabled or not. Until the process completes, you cannot create a new VA pod. During this time, the following message is displayed: "**Setting up the initial region configuration. This might take a couple of minutes.**"

After you log in successfully, **Dashboard** is displayed.

If you're prompted to update the region version, follow the prompts to complete the update. Note that you need to be at a minimum release of 1.0.4 (Limited Availability release) before you can install Release 1.2.x and update a region version. For more information, see [Update a Region Version, on page 73](#).



**Step 2** To create the new VA pod in a region other than the default (us-east-1), click the **Region** drop-down list and choose a region.

**Note** To enable access to the new regions added in Release 1.2.x, your admin user needs to log in to Cisco DNA Center VA Launchpad after the Cisco DNA Center VA Launchpad, Release 1.2.x has been installed. After the admin user has logged in, access to all regions is enabled for all other users.

If you're prompted to update the region version, follow the prompts to complete the update. Note that you need to be at a minimum release of 1.0.4 (Limited Availability release) before you can install Release 1.2.x and update a region version. For more information, see [Update a Region Version, on page 73](#).

**Step 3** Click + **Create New VA Pod**.



- Step 4** Configure the AWS infrastructure, which includes the VPC, private subnet, routing table, security group, virtual gateway, and customer gateway, by completing the following steps:
- a) In the **Environmental Details** fields, configure the following fields:
- **VA Pod Name:** Assign a name to the new VA pod. The name must be unique across all regions and can include letters (A-Z and a-z), numbers (0-9), and dashes (-).
  - **Availability Zone:** Click this drop-down list and choose an availability zone, which is an isolated location within your selected region.
  - **AWS VPC CIDR:** Enter a unique VPC subnet to use to launch AWS resources. Keep the following guidelines in mind:
    - The recommended range for CIDR is /25.
    - The last octet of CIDR can only be 0 or 128. That is, x.x.x.0 or x.x.x.128.
    - This subnet should not overlap with your corporate subnet.
- b) Under **Transit Gateway (TGW)**, choose one of the following options:
- **VPN GW:** Choose this option if you have a single VA pod, and you want to use a VPN gateway. A VPN GW is the VPN endpoint on the Amazon side of your Site-to-Site VPN connection. It can be attached to only a single VPC.
  - **New VPN GW + New TGW:** Choose this option if you have multiple VA pods or VPCs, and you want to use the TGW as a transit hub to interconnect multiple VPCs and on-premises networks. It can also be used as a VPN endpoint for the Amazon side of the Site-to-Site VPN connection.
- Note** You can create only one TGW per region.
- **Existing TGW:** Choose this option if you have an existing TGW that you want to use to create a new VA pod, and choose one of the following options:
    - **New VPN GW:** Choose this option if you want to create a new VPN gateway for your existing TGW.
    - **Existing Attachment:** Choose this option if you want to use an existing VPN or direct-connect attachment. From the **Select Attachment ID**, drop-down list, choose an attachment ID.

If you choose this option, you must also configure the routing on the existing TGW and CGW. For information, see [Manually Configure Routing on Existing Transit and Customer Gateways, on page 31](#).
- c) Do one of the following:
- If you selected **Existing TGW** and **Existing Attachments** as your preferred connectivity options, proceed to Step 5.
  - If you selected **VPN GW**, **New VPN GW + New TGW**, or **Existing TGW + New VPN GW**, provide the following VPN details:
    - **Customer Gateway IP:** Enter the IP address of your Enterprise firewall or router to form an IPsec tunnel with the AWS VPN gateway.
    - **VPN Vendor:** From the drop-down list, choose a VPN vendor.

The following VPN vendors are not supported: **Barracuda**, **Sophos**, **Vyatta**, and **Zyxel**. For more information, see [Troubleshoot VA Pod Configuration Issues, on page 39](#).

- **Platform:** From the drop-down list, choose a platform.
- **Software:** From the drop-down list, choose a software.

d) For the **Customer Profile** size, leave the default **Medium** setting.

The customer profile size applies to both the Cisco DNA Center VA instance and the backup instance. The **Medium** configures the instances as follows:

- **DNACInstance:** r5a.8xlarge, 32 vCPU, 256-GB RAM, and 4-TB storage.

**Note** Cisco DNA Center supports only the r5a.8xlarge instance size. Any changes to this configuration aren't supported.

Additionally, the r5a.8xlarge instance size isn't supported for the us-east-1e availability zone in the us-east-1 region.

- **BackupInstance:** T3.micro, 2 vCPU, 500-GB storage, and 1-GB RAM

e) For the **Backup Target**, choose one of the following options as the destination for backups of your Cisco DNA Center databases and files:

- **Enterprise Backup (NFS):** Choose this option if you want the backup to be stored in the on-premises servers.
- **Cloud Backup (NFS):** Choose this option if you want the backup to be stored on AWS.

Note the following backup details. You will use this information later to log into the cloud backup server:

- **SSH IP Address:** <BACKUP VM IP>
- **SSH Port:** 22
- **Server Path:** /var/dnac-backup/
- **Username:** maglev
- **Password:** maglev1@3
- **Passphrase:** maglev1@
- **Open Ports:** 22, 2049, 873, and 111

f) Click **Next**.

The summary page is displayed.

**1** Configure AWS Infrastructure  
With EC2, VPN Details

**2** Configure On-premise  
Precheck with AWS

**3** Network Connectivity Check  
Check IPsec tunnel connection

### Summary

Review your AWS Infrastructure details and make changes. If you are satisfied with your selection, click the "Start Configuring AWS Infrastructure"

#### VA Pod Environment Details

|                   |             |
|-------------------|-------------|
| VA Pod Name       | LA-101-1a   |
| Region            | us-east-1   |
| Availability Zone | us-east-1a  |
| AWS VPC CIDR      | 10.0.0.0/16 |

#### On-prem Connectivity

|                       |        |
|-----------------------|--------|
| Transit Gateway (TGW) | VPN GW |
|-----------------------|--------|

#### VPN Attachment

|                        |            |
|------------------------|------------|
| Customer Gateway (CGW) | New VPN GW |
|------------------------|------------|

#### VPN DETAILS

|                                  |                     |
|----------------------------------|---------------------|
| CGW (Enterprise Firewall/Router) | 10.0.0.0/16         |
| VPN Vendor                       | Cisco Systems, Inc. |
| Platform                         | ASA 5500 Series     |
| Software                         | ASA 9.7+ VTI        |

#### Other Details

|                  |                    |
|------------------|--------------------|
| Customer Profile | Medium             |
| Backup Target    | Cloud Backup (NFS) |

Exit Back Start Configuring AWS Infrastructure

- g) Review the environment and VPN details that you entered. If you are satisfied, click **Start Configuring AWS Environment**.

**Important** This setup takes about 20 minutes to complete. Do not exit the application or close this window or tab. Otherwise, the setup will pause.

- h) After the AWS infrastructure is successfully configured, the **AWS Infrastructure Configured** page is displayed.

### AWS Infrastructure Configured

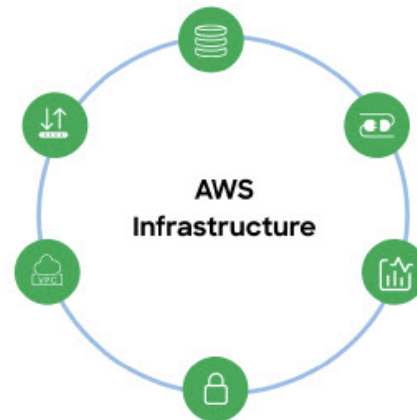
AWS::EC2::VPNGatewayRoutePropagation

AWS::EC2::VPNGatewayAttachment

AWS::EC2::VPNGateway

AWS::EC2::CustomerGateway

AWS::EC2::VPNConnectionRoute



**Note** If the AWS infrastructure configuration fails, exit Cisco DNA Center VA Launchpad and see [Troubleshoot the Deployment, on page 37](#) for information about possible causes and solutions.

### AWS Infrastructure Configured

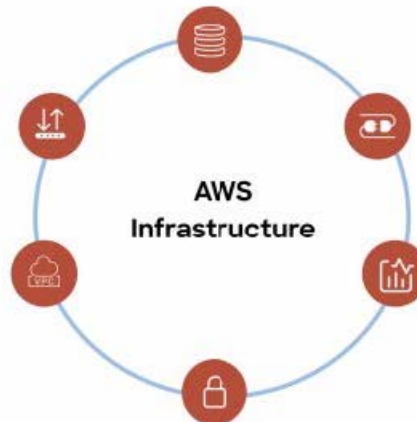
AWS::EC2::VPNGatewayRoutePropagation

AWS::EC2::VPNGatewayAttachment

AWS::EC2::VPNGateway

AWS::EC2::CustomerGateway

AWS::EC2::VPNConnectionRoute



**Step 5** Download the on-premises configuration file by completing the following steps:

- After the AWS infrastructure is successfully configured, click **Proceed to On-Prem Configuration**.
- From the **Configure On-premise** screen, click **Download Configuration File**. Forward this file to your network administrator to configure the on-premises-side IPsec tunnel.

Make sure your network administrator configures only one IPsec tunnel.

**Note**

- The network administrator can make the necessary changes to this configuration file and apply it to your Enterprise firewall or router to bring up IPsec tunnels.

The provided configuration file enables you to bring up two tunnels between AWS and the Enterprise router or firewall.

- Most virtual private gateway solutions have one tunnel up and the other down. You can have both tunnels up and use the Equal Cost Multiple Path (ECMP) networking feature. ECMP processing enables the firewall or router to use equal-cost routes to transmit traffic to the same destination. To do this, your router or firewall must support ECMP. Without ECMP, we recommend that you either keep one tunnel down and manually failover or use a solution, such as an IP SLA, to automatically bring up the tunnel in a failover scenario.

c) Click **Proceed to Network Connectivity Check** button.

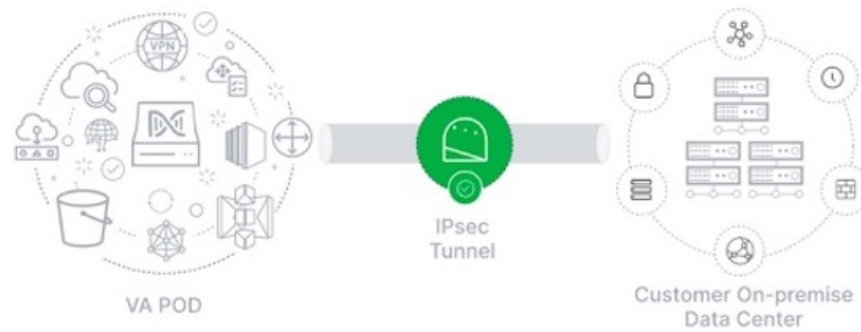
**Step 6**

Check the status of your network configuration based on the on-premises connectivity preferences that you selected during the AWS infrastructure configuration by completing one of the following actions:

- If you selected **VPN GW** as your preferred on-premises connectivity option, the IPsec tunnel configuration status is displayed, as follows:
  - If the network administrator hasn't configured the IPsec tunnel yet, a padlock is displayed on the IPsec tunnel:



- Ask your network administrator to verify that the IPsec tunnel on the Enterprise firewall or router is up. After the IPsec tunnel comes up, the IPsec tunnel turns green:



- If you selected **New VPN GW + New TGW** or **Existing TGW and New VPN GW** as your preferred on-premises connectivity option, Cisco DNA Center VA Launchpad checks whether your VPC is connected to the TGW, which in turn is connected to your on-premises firewall or router.

**Note** For the TGW-to-Enterprise firewall or router connection to succeed, your network administrator must add the configuration to your on-premises firewall or router.

The connection status is displayed, as follows:

- If the connection from the TGW to your on-premises firewall or router isn't connected yet, it's grayed out:



- After TGW connectivity has been successfully established, the TGW connections are green:



- If you selected **Existing TGW** and **Existing Attachment** as your preferred on-premises connectivity option, make sure that routing is configured between the existing TGW and the newly attached VPC, where Cisco DNA Center is launched. For information, see [Manually Configure Routing on Existing Transit and Customer Gateways](#), on page 31.

The connection status is displayed, as follows:

- If your VPC is not attached to the TGW, the TGW connection is grayed out:



- After TGW connectivity has been successfully established, the TGW connection is green:



- Step 7** Click **Go to Dashboard** to return to the Cisco DNA Center VA Launchpad where you can create more VA pods and manage your existing ones.

## Manually Configure Routing on Existing Transit and Customer Gateways

If you selected **Existing Transit Gateway** and **Existing Attachments** as your preferred connectivity while creating a new VA pod, Cisco DNA Center VA Launchpad creates a VPC to launch Cisco DNA Center and attaches this VPC to your existing TGW.

For Cisco DNA Center VA Launchpad to establish the TGW connection, you must manually configure the TGW routing table on AWS and add the routing configuration to your existing CGW.

### Procedure

- Step 1** From the AWS console, go to **VPC service**.
- Step 2** In the left navigation pane, under **Transit Gateways**, choose **Transit gateway route tables** and select the existing TGW route table.
- Step 3** In the **Transit gateway route tables** window, click the **Association** tab and then click **Create association**.

## Create a New Cisco DNA Center VA

Transit gateway route tables (1/1) Info

| Name               | Transit gateway route table ID | Transit gateway ID    | State     | Default association route table | Default propagation route table |
|--------------------|--------------------------------|-----------------------|-----------|---------------------------------|---------------------------------|
| TEST-0-2-5-NTGW... | tgw-rtb-04cb3502f1649f635      | tgw-044a18d1d2ce07ec6 | Available | No                              | No                              |

tgw-rtb-04cb3502f1649f635 / TEST-0-2-5-NTGW\_VA\_TGWVPNRouteTable

Associations (3) Info

| Attachment ID                | Resource type | Resource ID           | State      |
|------------------------------|---------------|-----------------------|------------|
| tgw-attach-03f39a6aabda35a9b | VPC           | vpc-048ab88f3c4178310 | Associated |
| tgw-attach-014db4b572f2242e7 | VPN           | vpn-0f5a1d61cd22f151  | Associated |
| tgw-attach-0b046fe367442fa5f | VPC           | vpc-01fd251ea2f8000c9 | Associated |

**Step 4** In the **Transit gateway route tables** window, click the **Propagation** tab and then click **Create propagation**.

Transit gateway route tables (1/1) Info

| Name               | Transit gateway route table ID | Transit gateway ID    | State     | Default association route table | Default propagation route table |
|--------------------|--------------------------------|-----------------------|-----------|---------------------------------|---------------------------------|
| TEST-0-2-5-NTGW... | tgw-rtb-04cb3502f1649f635      | tgw-044a18d1d2ce07ec6 | Available | No                              | No                              |

tgw-rtb-04cb3502f1649f635 / TEST-0-2-5-NTGW\_VA\_TGWVPNRouteTable

Propagations (3) Info

| Attachment ID                | Resource type | Resource ID           | State   |
|------------------------------|---------------|-----------------------|---------|
| tgw-attach-014db4b572f2242e7 | VPN           | vpn-0f5a1d61cd22f151  | Enabled |
| tgw-attach-03f39a6aabda35a9b | VPC           | vpc-048ab88f3c4178310 | Enabled |
| tgw-attach-0b046fe367442fa5f | VPC           | vpc-01fd251ea2f8000c9 | Enabled |

**Step 5** To ensure that the static route between the respective VPC and VPN is active, click the **Routes** tab and then click **Create static route**.

**Step 6** Ensure that your on-premises router configuration has been updated to route the network traffic destined for the CIDR ranges that are allocated to your AWS environment to your CGW.

For example: `route tunnel-int-vpn-0b57b508d80a07291-1 10.0.0.0 255.255.0.0 192.168.44.37 200`

## Create a New Cisco DNA Center VA

Use this procedure to configure a new Cisco DNA Center VA.

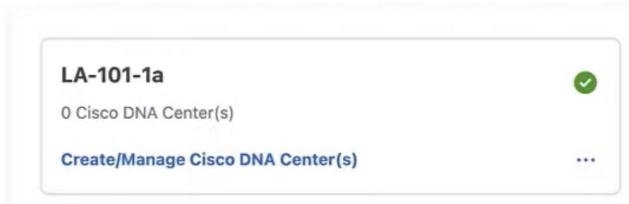


## Procedure

**Step 1** Log in to Cisco DNA Center VA Launchpad.

**Step 2** On **Dashboard**, locate one of the VA pods that you created, and in the VA pod card, click **Create/Manage Cisco DNA Center(s)**.

### Dashboard



**Step 3** On the **Create/Manage Cisco DNA Center(s)** page for the VA pod, click + **Create New Cisco DNA Center**.



**Step 4** Enter the following details:

- **Enterprise DNS:** Enter the IP address of your Enterprise DNS. Ensure that the Enterprise DNS is reachable from the VA pod on which you're creating the Cisco DNA Center VA.
- **FQDN (Fully Qualified Domain Name):** Enter the IP address of the Cisco DNA Center as configured on your DNS server.
- **Proxy Details:** Select one of the following HTTPS network proxy options:
  - **No Proxy:** No proxy server is used.
  - **Unauthenticated:** The proxy server does not require authentication. Enter the URL and port number of the proxy server.
  - **Proxy Authentication:** The proxy server requires authentication. Enter the URL, port number, username, and password details for the proxy server.

- **Cisco DNA Center Virtual Appliance Credentials:** Enter a CLI password to use to log in to the Cisco DNA Center VA.

The password must conform to the following constraints:

- Cannot contain any tab or line breaks.
- Must have at least 8 characters
- Must have a character from at least three of the following categories:
  - Lowercase letter
  - Uppercase letter
  - Number
  - Special character

Save this password for future reference.

**Note** The username is maglev.

**Step 5** Click **Validate** to validate the Enterprise DNS server and FQDN configured on the DNS.

**Note** In Cisco DNA Center VA Launchpad Release 1.0.4 and earlier, even if the DNS, Proxy and FQDN checks were invalid, you could still proceed with creating your Cisco DNA Center VA. However, in Cisco DNA Center VA Launchpad Release 1.2.x, if the DNS, Proxy, or FQDN checks fail, continuing with your configuration depends on as follows:

- If the DNS validation fails, you cannot continue with creating your Cisco DNA Center VA. Make sure that the entered DNS is reachable from the VA pod.
- If the Proxy validation fails, you can still continue with your configuration because even if the invalid proxy details aren't fixed, the Cisco DNA Center VA works.
- If the FQDN validation fails, you can still continue with creating your Cisco DNA Center VA. However, for the Cisco DNA Center VA to work, you need to fix the FQDN configuration.

**Step 6** Review the configuration details.

Note that even if the DNS, FQDN, and proxy precheck validations fail, you can still create a Cisco DNA Center VA.

## Summary

Review your Cisco DNA Center Virtual Appliance Configuration details and make any changes if needed. If you are satisfied, Start Cisco DNA Center Configuration now.

### DOMAIN DETAILS

|                                    |                           |   |
|------------------------------------|---------------------------|---|
| Enterprise DNS                     | <input type="checkbox"/>  | ✓ |
| FQDN (Fully Qualified Domain Name) | dnac01.ciscodnacenter.com | ✓ |

### PROXY DETAILS ✓

|                             |          |
|-----------------------------|----------|
| Customer HTTP Network Proxy | No Proxy |
|-----------------------------|----------|

[Exit](#)[Back](#)[Start Cisco DNA Center Configuration](#)

**Step 7** If you are satisfied with the configuration, click **Start Cisco DNA Center Configuration**.

Cisco DNA Center VA Launchpad begins configuring your environment.

After the environment is configured, Cisco DNA Center boots. Initially, Cisco DNA Center VA Launchpad displays the outer ring in gray. When Port 2222 is validated, the image turns amber. When Port 443 is validated, the image turns green.

**Note** This process takes 45-60 minutes. Do not exit the application or close this window or tab. Otherwise, the setup will pause.

After Cisco DNA Center is done booting, the configuration is complete. You can now view your Cisco DNA Center VA details.

## Done! Cisco DNA Center Virtual Appliance Configured

It will take around 45 - 60 minutes to complete the setup.

**Please do not leave the application or close the tab/window. Otherwise, the setup will pause.**

Cisco DNA Center is booting up...

|            |                                                                        |    |
|------------|------------------------------------------------------------------------|----|
| IP Address | <div style="background-color: #ccc; height: 15px; width: 100%;"></div> |    |
| SSH Key    | <div style="background-color: #ccc; height: 15px; width: 100%;"></div> | 📄  |
| PEM File   | VA_Instance01.pem                                                      | ⬇️ |

ⓘ Note: Please download and save the PEM file to accessing Cisco DNA Center. This is the only time that you will have access to download the pem file.

✅ Environment Setup completed

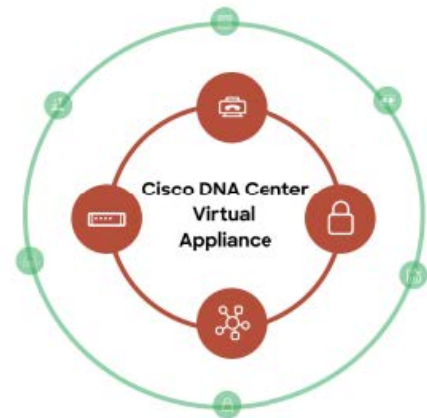


Exit [Go to Manage Cisco DNA Center\(s\)](#)

If the Cisco DNA Center configuration fails, exit to the [Create/Manage Cisco DNA Center\(s\)](#) page. For information, see [Troubleshoot the Deployment, on page 37](#)

## Cisco DNA Center Configuration In progress

ⓘ Environment Setup failed



**Step 8** Click the Copy icon (📄) to copy your SSH key and then click the Download icon (⬇️) to download your PEM file for future reference.

**Important** Be sure to download the SSH key, because you will not be able to do it later.

**Step 9** To return to your VA pod page, click **Go to Manage Cisco DNA Center(s)**.

## Troubleshoot the Deployment

Cisco DNA Center VA Launchpad is designed to help you seamlessly configure Cisco DNA Center on AWS with minimal intervention. This section shows you how to troubleshoot common issues during the deployment of Cisco DNA Center on AWS.



**Note** Unless specified, we recommended that you avoid making changes manually through the AWS console, as these changes can lead to issues with Cisco DNA Center VA Launchpad.

If you have any issues that are not addressed in this section, contact Cisco TAC.

### Troubleshoot Docker Issues

If the error, `port is already in use`, displays while running the docker images for Cisco DNA Center VA Launchpad, you can troubleshoot it with the following possible solutions.

| Error                                                                                                             | Possible Solution                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>If you receive the following error while running the server application:</p> <pre>port is already in use</pre> | <p>On Docker Desktop, run the server application:</p> <pre>docker run -d -p &lt;server-port-number&gt;:8080 -e SECRET_KEY=&lt;your-secret-key&gt; --name server --pull=always dockerhub.cisco.com/maglev-docker/server:x.x.x-latest</pre> <p><b>Note</b> You can use any available server port.</p> <p>While running the server application, run the client application:</p> <pre>docker run -d -p 3001:3000 -e REACT_APP_API_URL=http://localhost:&lt;client-port-number&gt; --name client --pull=always dockerhub.cisco.com/maglev-docker/client:x.x.x</pre> <p><b>Note</b> You must use the same port number that you used to run the server application.</p> |
| <p>If you receive the following error while running the client application:</p> <pre>port is already in use</pre> | <p>On Docker Desktop, run the client application:</p> <pre>docker run -d -p &lt;client-port-name&gt;:3000 --name client --pull=always dockerhub.cisco.com/maglev-docker/client:x.x.x</pre> <p><b>Note</b> You can use any available server port.</p>                                                                                                                                                                                                                                                                                                                                                                                                             |

### Troubleshoot Login Errors

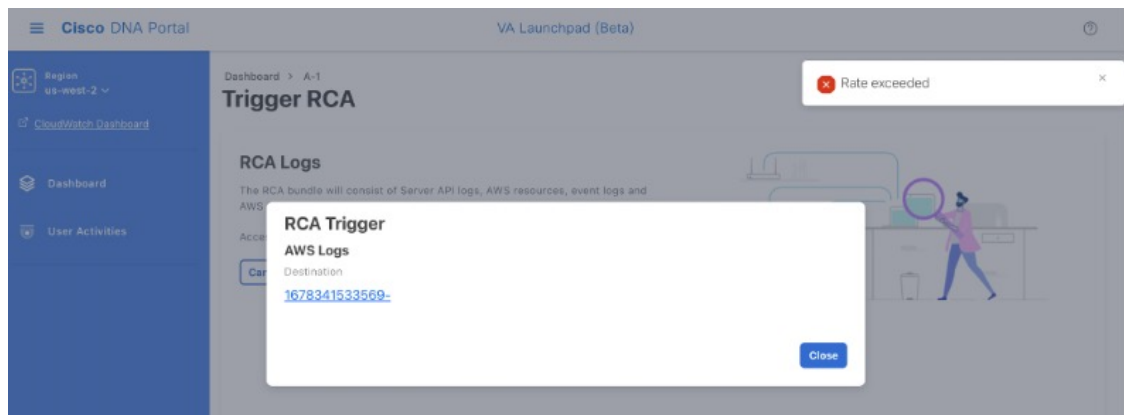
When you log in to Cisco DNA Center VA Launchpad, you may encounter a login error. We provide troubleshooting methods to the following common login issues.

If you encounter one of the following errors, do the following:

| Error                                                                           | Possible Solution                                                                                                                                                                               |
|---------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Invalid credentials.</b>                                                     | Reenter your credentials and check that they're entered correctly.                                                                                                                              |
| <b>You don't have enough access.</b>                                            | For admin users, verify that your account has the administrator access permission.<br>For subusers, verify that your administrator added you to the CiscoDNACenter user group.                  |
| <b>An operation to delete is in progress, please try again after some time.</b> | If an admin user deletes the <AccountId>-cisco-dna-center global bucket from the AWS account and then tries to log in, this login error can occur. Wait 5 minutes for the deletion to complete. |

## Troubleshoot a Hosted Cisco DNA Center VA Launchpad Error

On hosted Cisco DNA Center VA Launchpad, when you trigger a root cause analysis (RCA), the **Rate exceeded** error can occur. If this error occurs, the following banner is displayed:



This error banner displays when the maximum number of API requests (10,000 per second) are received for a region. To resolve this issue, increase the limit in AWS with the Service Quotas service, or retry the operation after a few seconds.

## Troubleshoot the Frozen Region Configuration Screen

When you click **Create a VA Pod** to create a new VA pod in a new region, Cisco DNA Center VA Launchpad configures the region. The configuration takes approximately 2 to 3 minutes and the following configuration-in-progress message is displayed:



If an error message is displayed or the screen freezes for more than 5 minutes and does not display the configuration-in-progress message, make sure that any manual process on the AWS console has been completed successfully and try this step again. If the problem persists, contact Cisco TAC.

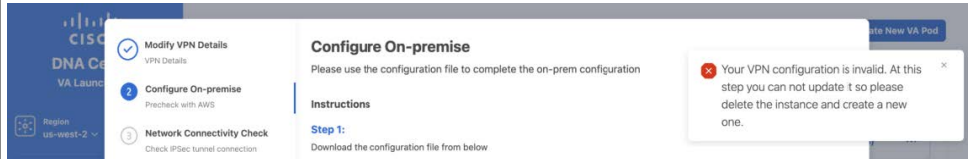


**Note** To avoid such conflicts, we recommend that you do not make any manual changes to the VA pods. Instead, use the Cisco DNA Center VA Launchpad for all actions.

## Troubleshoot VA Pod Configuration Issues

You can troubleshoot VA pod configuration issues that are related to creating a new VA pod.

If you encounter the following errors while trying to create a new VA pod, do the following:

| Error                                                                                                                    | Possible Solution                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| + Create VA Pod button disabled                                                                                          | <p>Hover your cursor over the disabled button to learn more about why it's disabled.</p> <p>The following are likely reasons why you can't create a new VA pod:</p> <ul style="list-style-type: none"> <li>• <b>You have reached the limit of VPC service quota:</b> For every region, a limit is set by your AWS administrator for how many VPCs can be created. Typically, there are 5 VPCs per region, and each VPC can have only one VA pod. However, you may want to contact your AWS administrator for the exact number.</li> </ul> <p>Note that any VPC used for resources outside of Cisco DNA Center VA Launchpad contribute to this limit. For example, if your AWS account has a limit of five VPCs and two are in use, you can only create three more VA pods for the selected region.</p> <p>To create new VA pods, ask your AWS administrator to change the limit, or delete some of your existing VA pods or VPCs on your AWS account.</p> <ul style="list-style-type: none"> <li>• <b>Pod deletion in progress:</b> The deletion of the last VA pod in the region is in progress. Wait a few minutes, and then retry creating a new VA pod.</li> </ul> |
| AMI ID for this region is not available for your account.                                                                | <p>When you click + <b>Create New VA Pod</b>, Cisco DNA Center VA Launchpad validates the AMI ID for your selected region.</p> <p>If you encounter this error, the validation has failed and you can't create a new pod in this region. Contact Cisco TAC to help you resolve the issue.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Your VPN configuration is invalid. At this step you cannot update it so please delete the instance and create a new one. | <p>When configuring a VA pod, the following VPN vendors are not supported:</p> <ul style="list-style-type: none"> <li>• Barracuda</li> <li>• Sophos</li> <li>• Vyatta</li> <li>• Zyxel</li> </ul> <p>If you are using an unsupported VPN vendor, Cisco DNA Center VA Launchpad displays the following warning:</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

| Error                                                                                                                                  | Possible Solution                                                                                                                                                                                                                                                                                                                          |
|----------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>AWS Infrastructure Failed.</b>                                                                                                      | If the AWS configuration fails, return to <b>Dashboard</b> and create a new VA pod. For information, see <a href="#">Create a New VA Pod, on page 21</a> .<br><br><b>Note</b> You can delete the VA pod that failed to configure.                                                                                                          |
| <b>AWS Configuration fails when editing a VA Pod</b>                                                                                   | Make sure that any manual process on the AWS console has been completed successfully and try this step again. If the problem persists, contact Cisco TAC.<br><br><b>Note</b> To avoid such conflicts, we recommend that you do not make any manual changes to the VA pods. Instead, use the Cisco DNA Center VA Launchpad for all actions. |
| <b>Deleting VA Pod has failed</b>                                                                                                      | Make sure that any manual process on the AWS console has been completed successfully and try this step again. If the problem persists, contact Cisco TAC.<br><br><b>Note</b> To avoid such conflicts, we recommend that you do not make any manual changes to the VA pods. Instead, use the Cisco DNA Center VA Launchpad for all actions. |
| <b>The resource you are trying to delete has been modified recently. Please refresh the page get the latest changes and try again.</b> | If you encounter this error while deleting a VA pod, contact Cisco TAC.                                                                                                                                                                                                                                                                    |

## Troubleshoot a Network Connectivity Error

While creating a VA pod, if the IPsec tunnel or TGW connection isn't established, make sure that the tunnel is up on your on-premises firewall or router.

If the VA pod to TGW tunnel is green and the TGW to CGW tunnel is gray, make sure that:



- You forwarded the correct configuration file to your network administrator.
- Your network administrator made the necessary changes to the configuration file.
- Your network administrator finished applying this configuration to your Enterprise firewall or router.
- If you chose **Existing TGW** and **Existing Attachments** as your network connectivity preference, make sure that you correctly followed [Manually Configure Routing on Existing Transit and Customer Gateways, on page 31](#).



## Troubleshoot Cisco DNA Center VA Configuration Errors

You can troubleshoot errors that occur while configuring a Cisco DNA Center VA.

If you encounter the following errors, do the following:

| Error                           | Possible Solution                                                                                                                                                                                                                             |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Environment Setup failed</b> | <ol style="list-style-type: none"> <li>1. On Cisco DNA Center VA Launchpad, return to the <b>Create/Manage Cisco DNA Center(s)</b> page.</li> <li>2. Delete the Cisco DNA Center VA.</li> <li>3. Create a new Cisco DNA Center VA.</li> </ol> |
| <b>Delete Failed</b>            | If the deletion of a Cisco DNA Center VA fails, contact Cisco TAC.                                                                                                                                                                            |

## Troubleshoot Concurrency Errors

Use the following table to help you troubleshoot the following concurrency errors:

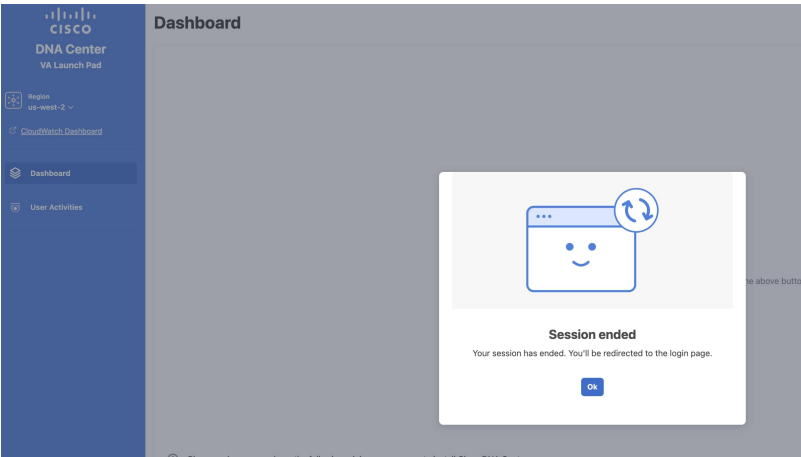
| Error                                                                        | Possible Solution                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Unable to delete a Pod or a Cisco DNA Center created by another user.</b> | <p>You cannot delete a component, such as a VA pod or Cisco DNA Center VA, that another user has created while a different action is in progress on the component. After the action completes, you or any other user can delete the component.</p> <p>For example, you cannot delete a VA pod or Cisco DNA Center VA while it is in any of the following processes or states:</p> <ul style="list-style-type: none"> <li>• Another user is in the process of creating the Cisco DNA Center VA.</li> <li>• Another user is in the process of deleting the Cisco DNA Center VA.</li> <li>• The Cisco DNA Center VA is in a failed state after a deletion attempt.</li> </ul> |
| <b>The status of a Pod has been changed recently.</b>                        | <p>If you tried to delete a VA pod, the original user account that created the VA pod may have performed a concurrent action. This concurrency issue changes the status of the selected VA pod.</p> <p>To view the updates status of the VA pod, click <b>Refresh</b>.</p>                                                                                                                                                                                                                                                                                                                                                                                                 |

## Troubleshoot Other Deployment Issues

You can troubleshoot other issues that occur while deploying a Cisco DNA Center VA on AWS.

If you encounter the following issues, do the following:

| Issue                                                           | Possible Reasons and Solutions                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Resources are green, but the Proceed button is disabled.</b> | <p>On some steps, you can only proceed if all resources have been successfully set up. To ensure the integrity of the deployment, the <b>Proceed</b> button remains disabled until the setup is complete and all resources have been configured and loaded.</p> <p>Sometimes, the screen shows that the resources have been successfully set up, but the <b>Proceed</b> button is still disabled. In this case, you need to wait a few more seconds for some resources to load. After all resources have been configured and loaded, the <b>Proceed</b> button is enabled.</p> |

| Issue                                                                              | Possible Reasons and Solutions                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Failure when deploying multiple VA pods with the same CGW in single region.</b> | <p>Make sure that:</p> <ul style="list-style-type: none"> <li>• The CGW IP address is the IP address of your Enterprise firewall or router.</li> <li>• The CGW IP address is a valid public address.</li> <li>• The CGW IP address hasn't been used for another VA pod within this region. Currently, in each region, multiple VA pods cannot have the same CGW IP address. To use the same CGW IP address for more than one VA pod, deploy each VA pod in a different region.</li> </ul> |
| <b>Unable to SSH or ping the Cisco DNA Center VA.</b>                              | <p>You cannot connect via SSH or ping the Cisco DNA Center VA, although the tunnel is up and the application status is complete (green). This issue might occur if the on-premises CGW is configured incorrectly. Verify the CGW configuration and try again.</p>                                                                                                                                                                                                                         |
| <b>Session ended</b>                                                               | <p>If your session times out while operations are in progress, such as triggering an RCA, the operations may abruptly end and display the following notification:</p>  <p>If your session times out, log back in and restart the operations.</p>                                                                                                                                                       |

## Deploy Cisco DNA Center on AWS Manually Using AWS CloudFormation

If you're familiar with AWS administration, you have the option of deploying the Cisco DNA Center AMI manually on your AWS account using AWS CloudFormation.

With this method, you need to create the AWS infrastructure, establish a VPN tunnel, and deploy Cisco DNA Center.

### Manual Deployment Using AWS CloudFormation Workflow

To deploy Cisco DNA Center on AWS using this method, follow these high-level steps:

1. Make sure the prerequisites are met. See [Prerequisites for Manual Deployment Using AWS CloudFormation, on page 43](#).

2. If you plan on integrating Cisco ISE on AWS and Cisco DNA Center VA together, see [Guidelines for Integrating Cisco ISE on AWS with Cisco DNA Center on AWS, on page 4](#).
3. Deploy Cisco DNA Center on AWS using AWS CloudFormation. See [Deploy Cisco DNA Center on AWS Manually Using AWS CloudFormation, on page 48](#).
4. Make sure that your environment setup and the Cisco DNA Center VA configuration are installed correctly and working as expected. See [Validate the Deployment, on page 52](#).

## Prerequisites for Manual Deployment Using AWS CloudFormation

These prerequisites are for manual deployment using AWS CloudFormation. You can also deploy Cisco DNA Center either using the automated method or manual deployment method using AWS Marketplace. To understand the benefits and drawbacks of each method, see [Deployment Overview, on page 1](#).

Before you can begin to deploy Cisco DNA Center on AWS, make sure that the following network, AWS, and Cisco DNA Center requirements have been met:

### Network Environment

You must have the following information about your network environment on hand:

- Enterprise DNS IP address
- (Optional) HTTPS Network Proxy details

### AWS Environment

You must meet the following AWS environment requirements:

- You have valid credentials to access your AWS account.



---

**Note** We recommend that the AWS account be a subaccount (a child account) to maintain resource independence and isolation. A subaccount ensures that the Cisco DNA Center deployment does not impact your existing resources.

---

- You must have the administrator access permission for your AWS account. (In AWS, the policy name is displayed as **AdministratorAccess**.)

The screenshot shows the AWS IAM console interface. On the left is a navigation menu with options like 'Dashboard', 'Access management', 'User groups', 'Users', 'Roles', 'Policies', etc. The main content area shows the 'Summary' page for a user named 'dna-tme-user'. Key details include:
 

- User ARN: arn:aws:iam:878813814009:user/dna-tme-user
- Path: /
- Creation time: 2022-07-23 16:11 PDT

 Below this, there are tabs for 'Permissions', 'Groups', 'Tags', 'Security credentials', and 'Access Advisor'. The 'Permissions' tab is active, showing a list of permissions policies. One policy, 'AdministratorAccess', is listed as an 'Attached directly' policy. At the bottom, there is a section titled 'Generate policy based on CloudTrail events' with a 'Generate policy' button.

• The following resources and services must be set up in AWS:

- **VPC:** The recommended range for CIDR is /25. The last octet of CIDR can only be 0 or 128. For example: x.x.x.0 or x.x.x.128.
- **Subnets:** The recommended subnet range is /28 and should not overlap with your corporate subnet.
- **Route Tables:** Make sure that your VPC subnet is allowed to communicate with your Enterprise network via your VPN GW or TGW.
- **Security Groups:** For communication between the Cisco DNA Center on AWS and the devices in your Enterprise network, the AWS security group that you attach to the Cisco DNA Center on AWS must allow the following ports:
  - TCP 22, 80, 443, 9991, 25103, 32626
  - UDP 123, 162, 514, 6007, 21730

You must also configure the inbound and outbound ports. To configure inbound ports, refer to the following figure:

The screenshot shows a table of inbound rules for a security group. The table has the following columns: Name, Security group rule, IP version, Type, Protocol, Port range, Source, and Description. There are 22 rows of rules, each with a checkbox in the first column. The rules include various protocols like TCP, UDP, and ICMP, and port ranges such as 111, 9005, 0-65555, 21730, 162, 443, 2049, 9004, 25103, 2049, 9991, 6007, 22, 2222, 0-65555, 873, 111, 80, 32626, 514, and 123. The source IP addresses are mostly 0.0.0/0, with some specific ranges like 172.16.2.0/28.

| Name | Security group rule   | IP version | Type            | Protocol | Port range | Source        | Description |
|------|-----------------------|------------|-----------------|----------|------------|---------------|-------------|
| -    | sg-0482eb11896826fec  | IPv4       | Custom TCP      | TCP      | 111        | 0.0.0/0       | -           |
| -    | sg-06112d893a265c2... | IPv4       | Custom TCP      | TCP      | 9005       | 0.0.0/0       | -           |
| -    | sg-0e6511be2e699ad... | IPv4       | All TCP         | TCP      | 0 - 65555  | 172.16.2.0/28 | -           |
| -    | sg-0c67e0ac5b8dfde3   | IPv4       | Custom UDP      | UDP      | 21730      | 0.0.0/0       | -           |
| -    | sg-04bd504b473cd7c6   | IPv4       | Custom UDP      | UDP      | 162        | 0.0.0/0       | -           |
| -    | sg-09f72040be517ac12  | IPv4       | HTTPS           | TCP      | 443        | 0.0.0/0       | -           |
| -    | sg-0a7098c3b2babc6a1  | IPv4       | NFS             | TCP      | 2049       | 0.0.0/0       | -           |
| -    | sg-07ac799f8c942056   | IPv4       | Custom TCP      | TCP      | 9004       | 0.0.0/0       | -           |
| -    | sg-048d0db2face92a23  | IPv4       | Custom TCP      | TCP      | 25103      | 0.0.0/0       | -           |
| -    | sg-0a2ba3dea618510... | IPv4       | Custom UDP      | UDP      | 2049       | 0.0.0/0       | -           |
| -    | sg-01b8e84fa1d0e9031  | IPv4       | Custom TCP      | TCP      | 9991       | 0.0.0/0       | -           |
| -    | sg-065328ee42f1fbfd   | IPv4       | Custom UDP      | UDP      | 6007       | 0.0.0/0       | -           |
| -    | sg-0b0f86cb88d098324  | IPv4       | SSH             | TCP      | 22         | 0.0.0/0       | -           |
| -    | sg-0015c86702bd994f3  | IPv4       | Custom TCP      | TCP      | 2222       | 0.0.0/0       | -           |
| -    | sg-0901d46c360997...  | IPv4       | All UDP         | UDP      | 0 - 65555  | 172.16.2.0/28 | -           |
| -    | sg-0d5787d5a064fae8   | IPv4       | All ICMP - IPv4 | ICMP     | All        | 0.0.0/0       | -           |
| -    | sg-0530e1360ffe7588d9 | IPv4       | Custom TCP      | TCP      | 873        | 0.0.0/0       | -           |
| -    | sg-0af12dadce93f014   | IPv4       | Custom UDP      | UDP      | 111        | 0.0.0/0       | -           |
| -    | sg-0d3f55a192c58fb4a  | IPv4       | HTTP            | TCP      | 80         | 0.0.0/0       | -           |
| -    | sg-0897d44466641b...  | IPv4       | Custom TCP      | TCP      | 32626      | 0.0.0/0       | -           |
| -    | sg-05e4179da8996b0fb  | IPv4       | Custom UDP      | UDP      | 514        | 0.0.0/0       | -           |
| -    | sg-0b4533d3134fba...  | IPv4       | Custom UDP      | UDP      | 123        | 0.0.0/0       | -           |

To configure outbound ports, refer to the following figure:

| Name | Security group rule... | IP version | Type            | Protocol | Port range | Destination   | Description |
|------|------------------------|------------|-----------------|----------|------------|---------------|-------------|
| -    | sg-0e208c10731f6fde    | IPv4       | NFS             | TCP      | 2049       | 0.0.0.0/0     | -           |
| -    | sg-0a67f0e542c9e8d3e   | IPv4       | Custom UDP      | UDP      | 123        | 0.0.0.0/0     | -           |
| -    | sg-02eb060f15d6998...  | IPv4       | Custom TCP      | TCP      | 49         | 0.0.0.0/0     | -           |
| -    | sg-0d51e1643d50fe72a   | IPv4       | Custom TCP      | TCP      | 9991       | 0.0.0.0/0     | -           |
| -    | sg-03b22337742ea66...  | IPv4       | Custom UDP      | UDP      | 111        | 0.0.0.0/0     | -           |
| -    | sg-0c1d1d9a7e4f55bbf   | IPv4       | Custom UDP      | UDP      | 1812       | 0.0.0.0/0     | -           |
| -    | sg-0b5e884f4021dd0b9   | IPv4       | Custom TCP      | TCP      | 23         | 0.0.0.0/0     | -           |
| -    | sg-0795765cabe1c2095   | IPv4       | HTTPS           | TCP      | 443        | 0.0.0.0/0     | -           |
| -    | sg-097c931b815b43...   | IPv4       | Custom UDP      | UDP      | 1645       | 0.0.0.0/0     | -           |
| -    | sg-0fada929aefc05db    | IPv4       | Custom TCP      | TCP      | 8910       | 0.0.0.0/0     | -           |
| -    | sg-0c9d0454fc1c8bb2e   | IPv4       | All TCP         | TCP      | 0 - 65535  | 172.16.2.0/28 | -           |
| -    | sg-0341f0b3e872b73...  | IPv4       | HTTP            | TCP      | 80         | 0.0.0.0/0     | -           |
| -    | sg-014ced79443b904fc   | IPv4       | Custom TCP      | TCP      | 9060       | 0.0.0.0/0     | -           |
| -    | sg-01ab82ce5b06d8...   | IPv4       | Custom UDP      | UDP      | 2049       | 0.0.0.0/0     | -           |
| -    | sg-0c22f51a7396d4f25   | IPv4       | Custom TCP      | TCP      | 873        | 0.0.0.0/0     | -           |
| -    | sg-0f0a1426fabee5234   | IPv4       | DNS (UDP)       | UDP      | 53         | 0.0.0.0/0     | -           |
| -    | sg-0d70c7499320d3...   | IPv4       | Custom TCP      | TCP      | 5222       | 0.0.0.0/0     | -           |
| -    | sg-0c78b55393f77fb78   | IPv4       | Custom UDP      | UDP      | 161        | 0.0.0.0/0     | -           |
| -    | sg-01973931a8d884...   | IPv4       | SSH             | TCP      | 22         | 0.0.0.0/0     | -           |
| -    | sg-061ef5612e74dad4b   | IPv4       | Custom TCP      | TCP      | 111        | 0.0.0.0/0     | -           |
| -    | sg-0b3d8a9ef60abd56    | IPv4       | Custom TCP      | TCP      | 850        | 0.0.0.0/0     | -           |
| -    | sg-06e5b54277c7da2...  | IPv4       | All ICMP - IPv4 | ICMP     | All        | 0.0.0.0/0     | -           |
| -    | sg-06e40371754806...   | IPv4       | All UDP         | UDP      | 0 - 65535  | 172.16.2.0/28 | -           |

The following table lists information about the ports that Cisco DNA Center uses, the services communicating over these ports, the appliance's purpose in using them, and the recommended action.

| Port            | Service Name      | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                  | Recommended Action                                                                                                                                                                                                            |
|-----------------|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| —               | ICMP              | Devices use ICMP messages to communicate network connectivity issues.                                                                                                                                                                                                                                                                                                                                                    | Enable ICMP.                                                                                                                                                                                                                  |
| TCP 22, 80, 443 | HTTPS, SFTP, HTTP | Software image download from Cisco DNA Center through HTTPS:443, SFTP:22, HTTP:80.<br><br>Certificate download from Cisco DNA Center through HTTPS:443, HTTP:80 (Cisco 9800 Wireless Controller, PnP), Sensor/Telemetry.<br><br><b>Note</b> Block port 80 if you don't use Plug and Play (PnP), Software Image Management (SWIM), Embedded Event Management (EEM), device enrollment, or Cisco 9800 Wireless Controller. | Ensure that firewall rules limit the source IP of the hosts or network devices allowed to access Cisco DNA Center on these ports.<br><br><b>Note</b> We do not recommend the use of HTTP 80. Use HTTPS 443 wherever possible. |
| UDP 123         | NTP               | Devices use NTP for time synchronization.                                                                                                                                                                                                                                                                                                                                                                                | Port must be open to allow devices to synchronize the time.                                                                                                                                                                   |
| UDP 162         | SNMP              | Cisco DNA Center receives SNMP network telemetry from devices.                                                                                                                                                                                                                                                                                                                                                           | Port must be open for data analytics based on SNMP.                                                                                                                                                                           |

| Port      | Service Name                                                                                     | Purpose                                                                                                                                                   | Recommended Action                                                                              |
|-----------|--------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|
| UDP 514   | Syslog                                                                                           | Cisco DNA Center receives syslog messages from devices.                                                                                                   | Port must be open for data analytics based on syslog.                                           |
| UDP 6007  | NetFlow                                                                                          | Cisco DNA Center receives NetFlow network telemetry from devices.                                                                                         | Port must be open for data analytics based on NetFlow.                                          |
| TCP 9991  | Wide Area Bonjour Service                                                                        | Cisco DNA Center receives multicast Domain Name System (mDNS) traffic from the Service Discovery Gateway (SDG) agents using the Bonjour Control Protocol. | Port must be open on Cisco DNA Center if the Bonjour application is installed.                  |
| UDP 21730 | Application Visibility Service                                                                   | Application Visibility Service CBAR device communication.                                                                                                 | Port must be open when CBAR is enabled on a network device.                                     |
| TCP 25103 | Cisco 9800 Wireless Controller and Cisco Catalyst 9000 switches with streaming telemetry enabled | Used for telemetry.                                                                                                                                       | Port must be open for telemetry connections between Cisco DNA Center and Catalyst 9000 devices. |
| TCP 32626 | Intelligent Capture (gRPC) collector                                                             | Used for receiving traffic statistics and packet - capture data used by the Cisco DNA Assurance Intelligent Capture (gRPC) feature.                       | Port must be open if you are using the Cisco DNA Assurance Intelligent Capture (gRPC) feature.  |

- **VPN Gateway (VPN GW) or Transit Gateway (TGW):** You must have an existing connection to your Enterprise network, which is your Customer Gateway (CGW).

For your existing connection from the CGW to AWS, make sure that the correct ports are open for traffic flow to and from Cisco DNA Center VA, whether you open them using the firewall settings or a proxy gateway. For more information about the well-known network service ports that the appliance uses, see "Required Network Ports" in the "Plan the Deployment" chapter of the [Cisco DNA Center First-Generation Appliance Installation Guide, Release 2.3.5](#).

- **Site-to-Site VPN Connection:** You can use Transit Gateway Attachments and Transit Gateway Route Tables.

- Your AWS environment must be configured with one of the following regions:
  - ap-northeast-1 (Tokyo)
  - ap-northeast-2 (Seoul)
  - ap-south-1 (Mumbai)
  - ap-southeast-1 (Singapore)
  - ap-southeast-2 (Sydney)
  - ca-central-1 (Canada)
  - eu-central-1 (Frankfurt)

- eu-south-1 (Milan)
  - eu-west-1 (Ireland)
  - eu-west-2 (London)
  - eu-west-3 (Paris)
  - us-east-1 (Virginia)
  - us-east-2 (Ohio)
  - us-west-1 (N. California)
  - us-west-2 (Oregon)
- If you want to enable multiple IAM users with the ability to configure Cisco DNA Center using the same environment setup, you need to create a group with the following policies and then add the required users to that group:
    - IAMReadOnlyAccess
    - AmazonEC2FullAccess
    - AWSCloudFormationFullAccess
  - The Cisco DNA Center instance size must meet the following minimum resource requirements:
    - r5a.8xlarge (The AWS instance type is an example of the minimum recommended sizing specifications.)



---

**Note** The r5a.8xlarge instance size is not supported for the us-east-1e availability zone in the us-east-1 region.

---

- 32 vCPU
  - 256-GB RAM
  - 4-TB storage
  - 2500 disk input/output operations per second (IOPS)
  - 180 MBps disk bandwidth
- You have the following AWS information on hand:
    - Subnet ID
    - Security Group ID
    - Keypair ID
    - Environment Name
    - CIDR Reservation

### Cisco DNA Center Environment

You must meet the following requirements for your Cisco DNA Center environment:

- You have access to the Cisco DNA Center GUI.
- You have the following Cisco DNA Center information on hand:
  - NTP Setting
  - Default Gateway Setting
  - CLI Password
  - UI Username/Password
  - Static IP
  - FQDN for the Cisco DNA Center VA IP address

## Deploy Cisco DNA Center on AWS Manually Using AWS CloudFormation

Cisco DNA Center VA deployment can be done manually through AWS CloudFormation. The provided AWS CloudFormation template contains the relevant details for all required parameters.

As a part of the deployment process, the AWS CloudFormation template for the Cisco DNA Center instance automatically creates the following Amazon CloudWatch dashboard and alarms:

- **DNACDashboard (VA\_Instance\_MonitoringBoard)**
- **DnacCPUAlarm:** When the CPU usage is greater than or equal to 80% for Cisco DNA Center instances, this alarm is triggered. The default threshold for CPU usage is 80%.
- **DnacSystemStatusAlarm:** If the system status check fails for a Cisco DNA Center instance, the recovery process is started. The default threshold for the system status check is 0.

### Before you begin

- You have the AWS environment set up with all the required components. For information, see [Prerequisites for Manual Deployment Using AWS CloudFormation, on page 43](#).
- The VPN tunnel is up.

### Procedure

#### Step 1

Go to the [Cisco Software Download](#) site and download the following file:

```
DNA_Center_VA_InstanceLaunch_CFT-1.2.1.tar.gz
```

This TAR file contains the AWS CloudFormation template that you use to create your Cisco DNA Center VA instance. The AWS CloudFormation template contains several AMIs, each having a different AMI ID based on a specific region. Use the appropriate AMI ID for your region:

| Region                 | Cisco DNA Center AMI ID |
|------------------------|-------------------------|
| ap-northeast-1 (Tokyo) | ami-0292a2a796f24d457   |



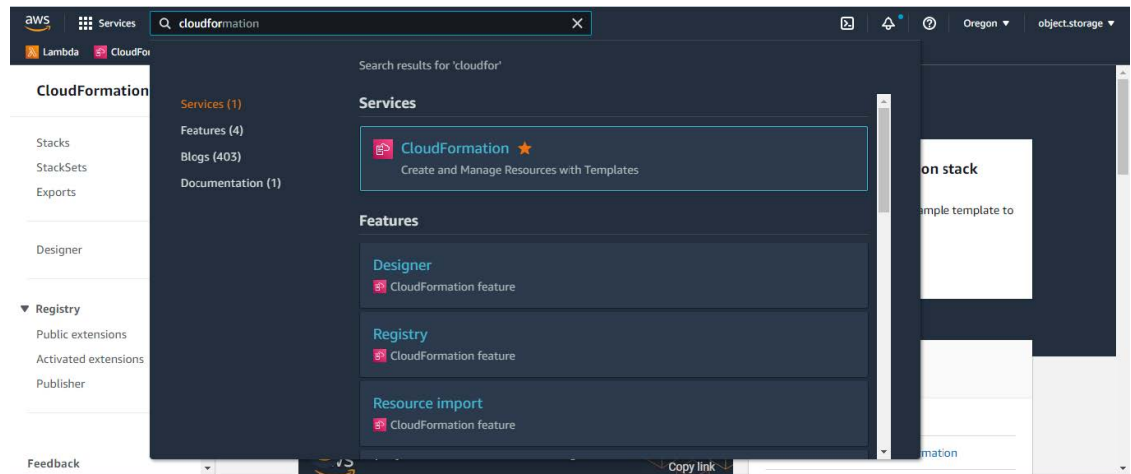
| Region                          | Cisco DNA Center AMI ID |
|---------------------------------|-------------------------|
| ap-northeast-2 (Seoul)          | ami-0fb5fe41c1d98ff7e   |
| ap-south-1 (Mumbai)             | ami-02a01cc5a2e40240c   |
| ap-southeast-1 (Singapore)      | ami-07fbfa61958e4fff2   |
| ap-southeast-2 (Sydney)         | ami-039328de5f5106989   |
| ca-central-1 (Canada)           | ami-050e7c5cb5b4cece8   |
| eu-central-1 (Frankfurt)        | ami-0d3d92adeed66a4d9   |
| eu-south-1 (Milan)              | ami-05704e7bc8afdaa38   |
| eu-west-1 (Ireland)             | ami-0cfe4ac465932e476   |
| eu-west-2 (London)              | ami-05e40b011d8790a71   |
| eu-west-3 (Paris)               | ami-06641fae3a82af9ae   |
| us-east-1 (Virginia)            | ami-06ebf482b1cd486ef   |
| us-east-2 (Ohio)                | ami-059277f0e3593e102   |
| us-west-1 (Northern California) | ami-0393e4436b9097ec6   |
| us-west-2 (Oregon)              | ami-065c6dab76f4c0909   |

**Step 2** Verify that the TAR file is genuine and from Cisco. For detailed steps, see [Verify the Cisco DNA Center VA TAR File, on page 6](#).

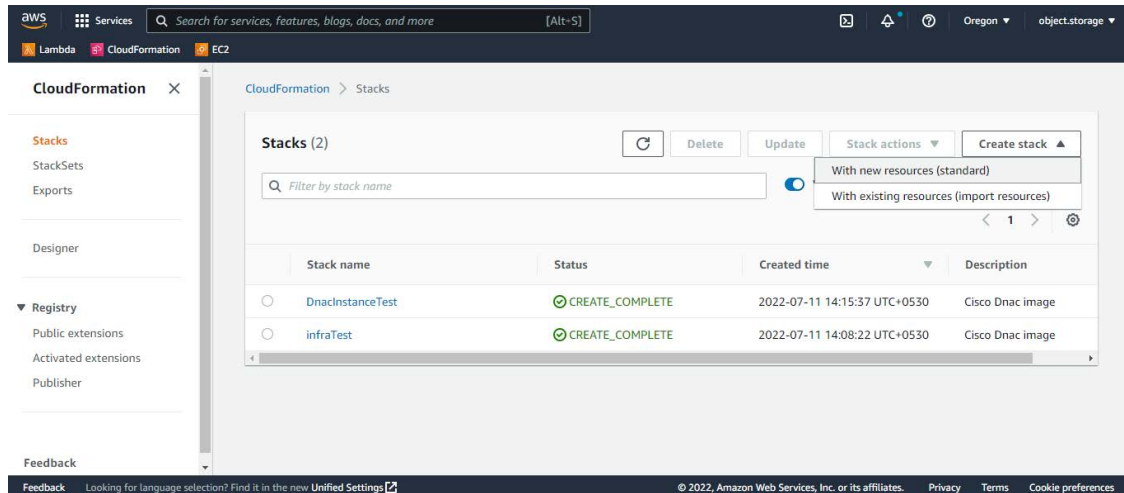
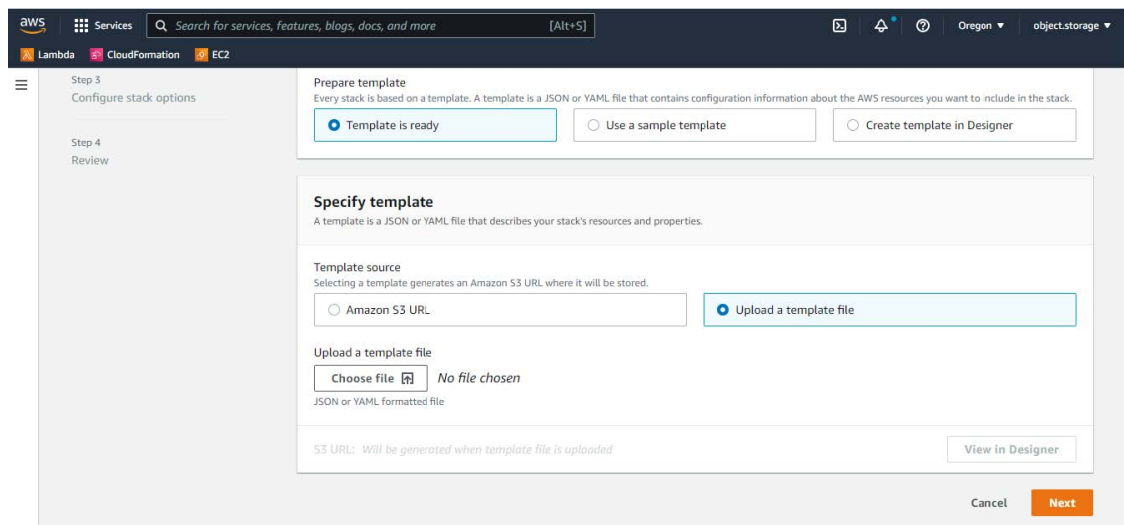
**Step 3** Log in to the AWS console.

The AWS console is displayed.

**Step 4** On the search bar, enter **cloudformation**.



**Step 5** From the drop-down menu, choose **CloudFormation**.

**Step 6** Click **Create stack** and select **With new resources (standard)**.**Step 7** Under **Specify template**, select **Upload a template file**, and choose the AWS CloudFormation template that you downloaded in Step 1.**Step 8** Enter a stack name and review the following parameters:• **EC2 Instance Configuration**

- **Environment Name:** Assign a unique environment name.

The environment name is used to differentiate the deployment and is prepended to your AWS resource names. If you use the same environment name as a previous deployment, the current deployment will fail.

- **Private Subnet ID:** Enter the VPC subnet to be used for Cisco DNA Center.
- **Security Group:** Enter the security group to be attached to the Cisco DNA Center VA that you are deploying.
- **Keypair:** Enter the SSH keypair used to access the CLI of Cisco DNA Center VA that you are deploying.

• **Cisco DNA Center Configuration:** Enter the following information:

- **DnacInstanceIP:** Cisco DNA Center IP address.
- **DnacNetmask:** Cisco DNA Center netmask.
- **DnacGateway:** Cisco DNA Center gateway address.
- **DnacDnsServer:** Enterprise DNS Server.
- **DnacPassword:** Cisco DNA Center password.

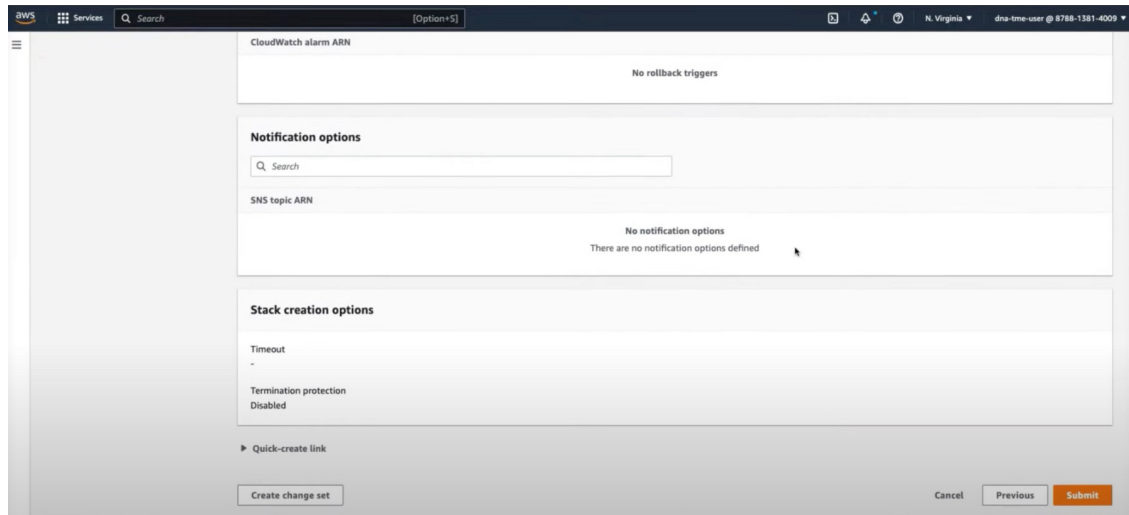
**Note** You can use the Cisco DNA Center password to access the Cisco DNA Center VA CLI through the AWS EC2 Serial Console.

- **DnacFQDN:** Cisco DNA Center FQDN.
- **DnacHttpsProxy:** (Optional) Enterprise HTTPS proxy.
- **DnacHttpsProxyUsername:** (Optional) HTTPS proxy username.
- **DnacHttpsProxyPassword:** (Optional) HTTPS proxy password.

**Step 9** (Optional) Click **Next** to configure the stack options.

**Step 10** Click **Next** to review your stack information.

**Step 11** If you are satisfied with the configuration, click **Submit** to finish.



The stack creation process usually takes from 45 to 60 minutes.

## Validate the Deployment

To ensure that your environment setup and Cisco DNA Center VA configuration are working, perform the following validation checks.

### Before you begin

Ensure that your stack creation on AWS CloudFormation has no errors.

### Procedure

- Step 1** Send a ping to the Cisco DNA Center IP address to ensure that your host details and network connection are valid.
- Step 2** Establish an SSH connection with Cisco DNA Center to verify that Cisco DNA Center is authenticated.
- Step 3** Use a browser to test HTTPS accessibility to the Cisco DNA Center GUI.

For more information about browser compatibility, see the [Release Notes for Cisco DNA Center on AWS, Release 1.2.x](#).

## Deploy Cisco DNA Center on AWS Manually Using AWS Marketplace

If you're familiar with AWS administration, you have the option of deploying Cisco DNA Center manually on your AWS account using AWS Marketplace.

## Manual Deployment Using AWS Marketplace Workflow

To deploy Cisco DNA Center on AWS using this method, follow these high-level steps:

1. Make sure the prerequisites are met. See [Prerequisites for Manual Deployment Using AWS Marketplace, on page 53](#).
2. If you plan on integrating Cisco ISE on AWS and Cisco DNA Center VA together, see [Guidelines for Integrating Cisco ISE on AWS with Cisco DNA Center on AWS, on page 4](#).
3. Deploy Cisco DNA Center on AWS using AWS Marketplace. See [Deploy Cisco DNA Center on AWS Manually Using AWS Marketplace, on page 58](#).
4. Make sure that your environment setup and the Cisco DNA Center VA configuration are installed correctly and working as expected. See [Validate the Deployment, on page 58](#).

## Prerequisites for Manual Deployment Using AWS Marketplace

These prerequisites are for manual deployment using AWS Marketplace. You can also deploy Cisco DNA Center either using the automated method or manual deployment method using AWS Marketplace. To understand the benefits and drawbacks of each method, see [Deployment Overview, on page 1](#).

Before you can begin to deploy Cisco DNA Center on AWS, make sure that the following network, AWS, and Cisco DNA Center requirements have been met:

### Network Environment

You must have the following information about your network environment on hand:

- Enterprise DNS IP address
- (Optional) HTTPS Network Proxy details

### AWS Environment

You must meet the following AWS environment requirements:

- You have valid credentials to access your AWS account.



---

**Note** We recommend that the AWS account be a subaccount (a child account) to maintain resource independence and isolation. A subaccount ensures that the Cisco DNA Center deployment does not impact your existing resources.

---

- You must have the administrator access permission for your AWS account. (In AWS, the policy name is displayed as **AdministratorAccess**.)

The screenshot shows the AWS IAM console interface. On the left is a navigation menu with options like 'Dashboard', 'Access management', 'Users', 'Roles', 'Policies', etc. The main content area shows the 'Summary' page for a user named 'dna-tme-user'. Key details include:
 

- User ARN: arn:aws:iam:878813814009:user/dna-tme-user
- Path: /
- Creation time: 2022-07-23 16:11 PDT
- Permissions: A list of policies is shown, including 'AdministratorAccess' (AWS managed policy).
- There is a section for 'Generate policy based on CloudTrail events' with a 'Generate policy' button.

- The following resources and services must be set up in AWS:
  - **VPC:** The recommended range for CIDR is /25. The last octet of CIDR can only be 0 or 128. For example: x.x.x.0 or x.x.x.128.
  - **Subnets:** The recommended subnet range is /28 and should not overlap with your corporate subnet.
  - **Route Tables:** Make sure that your VPC subnet is allowed to communicate with your Enterprise network via your VPN GW or TGW.
  - **Security Groups:** For communication between the Cisco DNA Center on AWS and the devices in your Enterprise network, the AWS security group that you attach to the Cisco DNA Center on AWS must allow the following ports:
    - TCP 22, 80, 443, 9991, 25103, 32626
    - UDP 123, 162, 514, 6007, 21730

You must also configure the inbound and outbound ports. To configure inbound ports, refer to the following figure:

| Inbound rules (22) |                        |            |                 |          |            |               |             |  |  |  |
|--------------------|------------------------|------------|-----------------|----------|------------|---------------|-------------|--|--|--|
| Name               | Security group rule... | IP version | Type            | Protocol | Port range | Source        | Description |  |  |  |
| -                  | sg-0482eb11896826fec   | IPv4       | Custom TCP      | TCP      | 111        | 0.0.0.0/0     | -           |  |  |  |
| -                  | sg-06112d893a265c2...  | IPv4       | Custom TCP      | TCP      | 9005       | 0.0.0.0/0     | -           |  |  |  |
| -                  | sg-0e6511be2e699ad...  | IPv4       | All TCP         | TCP      | 0 - 65535  | 172.16.2.0/28 | -           |  |  |  |
| -                  | sg-0c67e0ac5b8dfde3    | IPv4       | Custom UDP      | UDP      | 21730      | 0.0.0.0/0     | -           |  |  |  |
| -                  | sg-04bd504b473cd7c6    | IPv4       | Custom UDP      | UDP      | 162        | 0.0.0.0/0     | -           |  |  |  |
| -                  | sg-09f72040be517ac12   | IPv4       | HTTPS           | TCP      | 443        | 0.0.0.0/0     | -           |  |  |  |
| -                  | sg-0a7098c3b2babc6a1   | IPv4       | NFS             | TCP      | 2049       | 0.0.0.0/0     | -           |  |  |  |
| -                  | sg-07ac799f8c942056    | IPv4       | Custom TCP      | TCP      | 9004       | 0.0.0.0/0     | -           |  |  |  |
| -                  | sg-048d0db2face92a23   | IPv4       | Custom TCP      | TCP      | 25103      | 0.0.0.0/0     | -           |  |  |  |
| -                  | sg-0a2ba3de618510...   | IPv4       | Custom UDP      | UDP      | 2049       | 0.0.0.0/0     | -           |  |  |  |
| -                  | sg-01b8e84fa1d0e9031   | IPv4       | Custom TCP      | TCP      | 9991       | 0.0.0.0/0     | -           |  |  |  |
| -                  | sg-065328ee42f1fbfd    | IPv4       | Custom UDP      | UDP      | 6007       | 0.0.0.0/0     | -           |  |  |  |
| -                  | sg-0b0f86cb88d098324   | IPv4       | SSH             | TCP      | 22         | 0.0.0.0/0     | -           |  |  |  |
| -                  | sg-0015c86702bd994f3   | IPv4       | Custom TCP      | TCP      | 2222       | 0.0.0.0/0     | -           |  |  |  |
| -                  | sg-0901d46c360997...   | IPv4       | All UDP         | UDP      | 0 - 65535  | 172.16.2.0/28 | -           |  |  |  |
| -                  | sg-0d5787d5a064fae8    | IPv4       | All ICMP - IPv4 | ICMP     | All        | 0.0.0.0/0     | -           |  |  |  |
| -                  | sg-0530e1360fe7588d9   | IPv4       | Custom TCP      | TCP      | 873        | 0.0.0.0/0     | -           |  |  |  |
| -                  | sg-0af12dadce93f014    | IPv4       | Custom UDP      | UDP      | 111        | 0.0.0.0/0     | -           |  |  |  |
| -                  | sg-0d3f55a192c58fb4a   | IPv4       | HTTP            | TCP      | 80         | 0.0.0.0/0     | -           |  |  |  |
| -                  | sg-0897d44466641b...   | IPv4       | Custom TCP      | TCP      | 32626      | 0.0.0.0/0     | -           |  |  |  |
| -                  | sg-05e4179da8996b0fb   | IPv4       | Custom UDP      | UDP      | 514        | 0.0.0.0/0     | -           |  |  |  |
| -                  | sg-0b4533d3134fba...   | IPv4       | Custom UDP      | UDP      | 123        | 0.0.0.0/0     | -           |  |  |  |

To configure outbound ports, refer to the following figure:

| Name | Security group rule... | IP version | Type            | Protocol | Port range | Destination   | Description |
|------|------------------------|------------|-----------------|----------|------------|---------------|-------------|
| -    | sg-0e208c10731f6fde    | IPv4       | NFS             | TCP      | 2049       | 0.0.0.0/0     | -           |
| -    | sg-0a67f0e542c9e8d3e   | IPv4       | Custom UDP      | UDP      | 123        | 0.0.0.0/0     | -           |
| -    | sg-02eb060f15d6998...  | IPv4       | Custom TCP      | TCP      | 49         | 0.0.0.0/0     | -           |
| -    | sg-0d51e1643d50fe72a   | IPv4       | Custom TCP      | TCP      | 9991       | 0.0.0.0/0     | -           |
| -    | sg-03b22337742ea66...  | IPv4       | Custom UDP      | UDP      | 111        | 0.0.0.0/0     | -           |
| -    | sg-0c1d1d9a7e4f55bbf   | IPv4       | Custom UDP      | UDP      | 1812       | 0.0.0.0/0     | -           |
| -    | sg-0b5e884f4021dd0b9   | IPv4       | Custom TCP      | TCP      | 23         | 0.0.0.0/0     | -           |
| -    | sg-0795765cabe1c2095   | IPv4       | HTTPS           | TCP      | 443        | 0.0.0.0/0     | -           |
| -    | sg-097c931b815b43...   | IPv4       | Custom UDP      | UDP      | 1645       | 0.0.0.0/0     | -           |
| -    | sg-0fada929aef005db    | IPv4       | Custom TCP      | TCP      | 8910       | 0.0.0.0/0     | -           |
| -    | sg-0c9d0454fc1c8bb2e   | IPv4       | All TCP         | TCP      | 0 - 65535  | 172.16.2.0/28 | -           |
| -    | sg-0341f0b3e872b73...  | IPv4       | HTTP            | TCP      | 80         | 0.0.0.0/0     | -           |
| -    | sg-014ced79443b904fc   | IPv4       | Custom TCP      | TCP      | 9060       | 0.0.0.0/0     | -           |
| -    | sg-01ab82ce5b06d8...   | IPv4       | Custom UDP      | UDP      | 2049       | 0.0.0.0/0     | -           |
| -    | sg-0c22f51a7396d4f25   | IPv4       | Custom TCP      | TCP      | 873        | 0.0.0.0/0     | -           |
| -    | sg-0f0a1426fabee5234   | IPv4       | DNS (UDP)       | UDP      | 53         | 0.0.0.0/0     | -           |
| -    | sg-0d70c7499320d3...   | IPv4       | Custom TCP      | TCP      | 5222       | 0.0.0.0/0     | -           |
| -    | sg-0c78b55393f77fb78   | IPv4       | Custom UDP      | UDP      | 161        | 0.0.0.0/0     | -           |
| -    | sg-01973931a8d884...   | IPv4       | SSH             | TCP      | 22         | 0.0.0.0/0     | -           |
| -    | sg-061ef5612e74dad4b   | IPv4       | Custom TCP      | TCP      | 111        | 0.0.0.0/0     | -           |
| -    | sg-0b3d8a9ef60abd56    | IPv4       | Custom TCP      | TCP      | 850        | 0.0.0.0/0     | -           |
| -    | sg-06e5b54277c7da2...  | IPv4       | All ICMP - IPv4 | ICMP     | All        | 0.0.0.0/0     | -           |
| -    | sg-06e40371754806...   | IPv4       | All UDP         | UDP      | 0 - 65535  | 172.16.2.0/28 | -           |

The following table lists information about the ports that Cisco DNA Center uses, the services communicating over these ports, the appliance's purpose in using them, and the recommended action.

| Port            | Service Name      | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                  | Recommended Action                                                                                                                                                                                                            |
|-----------------|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| —               | ICMP              | Devices use ICMP messages to communicate network connectivity issues.                                                                                                                                                                                                                                                                                                                                                    | Enable ICMP.                                                                                                                                                                                                                  |
| TCP 22, 80, 443 | HTTPS, SFTP, HTTP | Software image download from Cisco DNA Center through HTTPS:443, SFTP:22, HTTP:80.<br><br>Certificate download from Cisco DNA Center through HTTPS:443, HTTP:80 (Cisco 9800 Wireless Controller, PnP), Sensor/Telemetry.<br><br><b>Note</b> Block port 80 if you don't use Plug and Play (PnP), Software Image Management (SWIM), Embedded Event Management (EEM), device enrollment, or Cisco 9800 Wireless Controller. | Ensure that firewall rules limit the source IP of the hosts or network devices allowed to access Cisco DNA Center on these ports.<br><br><b>Note</b> We do not recommend the use of HTTP 80. Use HTTPS 443 wherever possible. |
| UDP 123         | NTP               | Devices use NTP for time synchronization.                                                                                                                                                                                                                                                                                                                                                                                | Port must be open to allow devices to synchronize the time.                                                                                                                                                                   |
| UDP 162         | SNMP              | Cisco DNA Center receives SNMP network telemetry from devices.                                                                                                                                                                                                                                                                                                                                                           | Port must be open for data analytics based on SNMP.                                                                                                                                                                           |

| Port      | Service Name                                                                                     | Purpose                                                                                                                                                   | Recommended Action                                                                              |
|-----------|--------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|
| UDP 514   | Syslog                                                                                           | Cisco DNA Center receives syslog messages from devices.                                                                                                   | Port must be open for data analytics based on syslog.                                           |
| UDP 6007  | NetFlow                                                                                          | Cisco DNA Center receives NetFlow network telemetry from devices.                                                                                         | Port must be open for data analytics based on NetFlow.                                          |
| TCP 9991  | Wide Area Bonjour Service                                                                        | Cisco DNA Center receives multicast Domain Name System (mDNS) traffic from the Service Discovery Gateway (SDG) agents using the Bonjour Control Protocol. | Port must be open on Cisco DNA Center if the Bonjour application is installed.                  |
| UDP 21730 | Application Visibility Service                                                                   | Application Visibility Service CBAR device communication.                                                                                                 | Port must be open when CBAR is enabled on a network device.                                     |
| TCP 25103 | Cisco 9800 Wireless Controller and Cisco Catalyst 9000 switches with streaming telemetry enabled | Used for telemetry.                                                                                                                                       | Port must be open for telemetry connections between Cisco DNA Center and Catalyst 9000 devices. |
| TCP 32626 | Intelligent Capture (gRPC) collector                                                             | Used for receiving traffic statistics and packet - capture data used by the Cisco DNA Assurance Intelligent Capture (gRPC) feature.                       | Port must be open if you are using the Cisco DNA Assurance Intelligent Capture (gRPC) feature.  |

- **VPN Gateway (VPN GW) or Transit Gateway (TGW):** You must have an existing connection to your Enterprise network, which is your Customer Gateway (CGW).

For your existing connection from the CGW to AWS, make sure that the correct ports are open for traffic flow to and from Cisco DNA Center VA, whether you open them using the firewall settings or a proxy gateway. For more information about the well-known network service ports that the appliance uses, see "Required Network Ports" in the "Plan the Deployment" chapter of the [Cisco DNA Center First-Generation Appliance Installation Guide, Release 2.3.5](#).

- **Site-to-Site VPN Connection:** You can use Transit Gateway Attachments and Transit Gateway Route Tables.

- Your AWS environment must be configured with one of the following regions:
  - ap-northeast-1 (Tokyo)
  - ap-northeast-2 (Seoul)
  - ap-south-1 (Mumbai)
  - ap-southeast-1 (Singapore)
  - ap-southeast-2 (Sydney)
  - ca-central-1 (Canada)
  - eu-central-1 (Frankfurt)



- eu-south-1 (Milan)
  - eu-west-1 (Ireland)
  - eu-west-2 (London)
  - eu-west-3 (Paris)
  - us-east-1 (Virginia)
  - us-east-2 (Ohio)
  - us-west-1 (N. California)
  - us-west-2 (Oregon)
- If you want to enable multiple IAM users with the ability to configure Cisco DNA Center using the same environment setup, you need to create a group with the following policies and then add the required users to that group:
    - IAMReadOnlyAccess
    - AmazonEC2FullAccess
    - AWSCloudFormationFullAccess
  - The Cisco DNA Center instance size must meet the following minimum resource requirements:
    - r5a.8xlarge (The AWS instance type is an example of the minimum recommended sizing specifications.)



---

**Note** The r5a.8xlarge instance size is not supported for the us-east-1e availability zone in the us-east-1 region.

---

- 32 vCPU
  - 256-GB RAM
  - 4-TB storage
  - 2500 disk input/output operations per second (IOPS)
  - 180 MBps disk bandwidth
- You have the following AWS information on hand:
    - Subnet ID
    - Security Group ID
    - Keypair ID
    - Environment Name
    - CIDR Reservation

### Cisco DNA Center Environment

You must meet the following requirements for your Cisco DNA Center environment:

- You have access to the Cisco DNA Center GUI.
- You have the following Cisco DNA Center information on hand:
  - NTP Setting
  - Default Gateway Setting
  - CLI Password
  - UI Username/Password
  - Static IP
  - FQDN for the Cisco DNA Center VA IP address

## Deploy Cisco DNA Center on AWS Manually Using AWS Marketplace

For instructions on how to deploy Cisco DNA Center on AWS using AWS Marketplace, go to the [Cisco Software Download](#) site and download the following file:

*Deploy Cisco DNA Center on AWS Using AWS Marketplace*

## Validate the Deployment

To ensure that your environment setup and Cisco DNA Center VA configuration are working, perform the following validation checks.

### Before you begin

Ensure that your stack creation on AWS Marketplace has no errors.

### Procedure

- 
- Step 1** Send a ping to the Cisco DNA Center IP address to ensure that your host details and network connection are valid.
  - Step 2** Establish an SSH connection with Cisco DNA Center to verify that Cisco DNA Center is authenticated.
  - Step 3** Use a browser to test HTTPS accessibility to the Cisco DNA Center GUI.

For more information about browser compatibility, see the [Release Notes for Cisco DNA Center on AWS, Release 1.2.x](#).

---

## Backup and Restore

You can use the backup and restore functions to create backup files to restore to a different appliance. With Cisco DNA Center VAs, there are two methods to back up and restore data:

- Back up data from a Cisco DNA Center hardware appliance and restore the data on to a Cisco DNA Center VA.
- Back up data from one Cisco DNA Center VA and restore the data on to another Cisco DNA Center VA.

## Backup and Restore—Hardware Appliance to VA

You can back up the data from a Cisco DNA Center hardware appliance and restore the data on to a Cisco DNA Center VA.

### Before you begin

For hardware appliances, use the 44-core Cisco DNA Center appliance to back up and restore data.

### Procedure

---

- Step 1** Back up the data from the Cisco DNA Center hardware appliance. For instructions, see the "Backup and Restore" chapter in the [Cisco DNA Center Administrator Guide, Release 2.3.5](#).  
Make sure that the backup server is connected to Cisco DNA Center through a VPN.
- Step 2** Create a Cisco DNA Center VA. For more information, see [Create a New Cisco DNA Center VA, on page 32](#).  
Make sure the Cisco DNA Center VA is up and running.
- Step 3** Connect the Cisco DNA Center VA to the backup server from Step 1.  
Make sure that the backup server is reachable from the Cisco DNA Center VA.
- Step 4** Configure the backup server on the Cisco DNA Center VA.
- Step 5** Restore the data on to the Cisco DNA Center VA.
- 

## Backup and Restore—VA to VA

You can back up the data from one Cisco DNA Center VA and restore the data on to another Cisco DNA Center VA.

### Before you begin

Make sure that you successfully deployed two Cisco DNA Center VAs with Cisco DNA Center VA Launchpad or AWS CloudFormation. For more information, see [Deploy Cisco DNA Center on AWS Using the Automated Deployment Method, on page 7](#) or [Deploy Cisco DNA Center on AWS Manually Using AWS CloudFormation, on page 42](#).

### Procedure

---

- Step 1** Back up the data from a Cisco DNA Center VA. For instructions, see the "Backup and Restore" chapter in the [Cisco DNA Center Administrator Guide, Release 2.3.5](#).

Make sure that the backup server is connected to a Cisco DNA Center VA through a VPN.

- Step 2** Bring up the Cisco DNA Center VA that you want to restore.  
Make sure that this Cisco DNA Center VA is up and running.
- Step 3** Connect the Cisco DNA Center VA that you want to restore to the backup server from Step 1.  
Make sure that the backup server is reachable from the Cisco DNA Center VA.
- Step 4** Configure the backup server on the Cisco DNA Center VA that you want to restore.
- Step 5** Restore the data on to the Cisco DNA Center VA.
- 

## Manage VA Pods and User Settings Using Cisco DNA Center VA Launchpad

On Cisco DNA Center VA Launchpad, you can manage your VA pods, Cisco DNA Center VAs, and user settings.

### Log In to the Cisco Launchpad

The Cisco DNA Center VA Launchpad supports the following authentication methods:

- [Log In to the Cisco DNA Portal With Cisco](#): This method uses the credentials from your Cisco account.
- **Log In as a Federated User**: Federated access ensures that an identity provider (IdP), such as your organization, is responsible for user authentication and sending information to Cisco DNA Center VA Launchpad to help determine the scope of resource access to be granted after login. For the first-time login, the user will have an admin user role, which creates the CiscoDNACenter role. The admin can assign this role to subsequent users. The CiscoDNACenter role has the same permissions as the CiscoDNACenter user group. For details about the permissions granted by this role, see [Prerequisites for Automated Deployment, on page 8](#).

You can use the saml2aws CLI or the AWS CLI to generate tokens to log in to Cisco DNA Center VA Launchpad as a federated user. For information, see the following topics:

- [Log In as a Federated User Using saml2aws-Generated Credentials, on page 63](#)
- [Log In as a Federated User Using AWS CLI-Generated Credentials, on page 66](#)

### Log In with Cisco

This procedure shows you how to log in to Cisco DNA Center VA Launchpad.

#### Before you begin

Make sure the following requirements are met:

- Your AWS account has the administrator access permission assigned to it. For information, [Prerequisites for Automated Deployment, on page 8](#).
- Cisco DNA Center VA Launchpad is installed or you have access to the hosted Cisco DNA Center VA Launchpad.

- You have your AWS Account ID, Access Key ID, and Secret Access Key on hand.

## Procedure

**Step 1** From a browser window, do one of the following:


- If you installed Cisco DNA Center VA Launchpad locally, enter the Cisco DNA Center VA Launchpad URL in the following format:

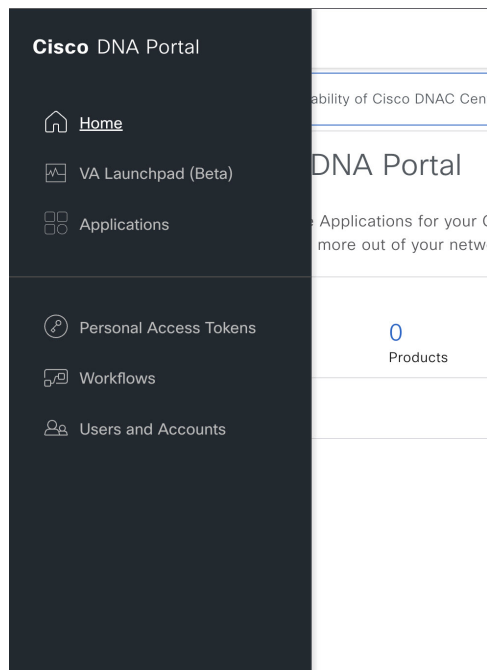
**http://<localhost>:<client-port-number>/valaunchpad**

For example:

**http://192.0.2.1:90/valaunchpad**

- If you are accessing the hosted Cisco DNA Center VA Launchpad, enter **dna.cisco.com** and follow the on-screen prompts to log in. (For information, see [Log In to the Cisco DNA Portal With Cisco](#), on page 18.)

From the **Cisco DNA Portal** home page, click the menu icon (  ) and choose **VA Launchpad (Beta)**.



The AWS login window is displayed.

**aws**

IAM Login  Federated Login

**AWS Account ID** ⓘ

AWS Account ID

**Access Key ID** ⓘ

Access Key ID

**Secret Access Key** ⓘ

Secret Access Key

**Authenticate**

**AWS Access**

Fill the AWS details to connect to your AWS account.

For more details, check <https://docs.aws.amazon.com/general/latest/gr/aws-sec-cred-types.html>

**Step 2** Choose your user login, and then enter your credentials in the fields:

- **IAM Login**
- **Federated Login**

For more information, see [Log In as a Federated User Using saml2aws-Generated Credentials](#), on page 63 or [Log In as a Federated User Using AWS CLI-Generated Credentials](#), on page 66.

For information about how to get an Access Key ID and Secret Access Key, see the [AWS Account and Access Keys](#) topic in the *AWS Tools for PowerShell User Guide* on the AWS website.

**Step 3** Click **Authenticate**.

After you log in successfully, **Dashboard** is displayed and the us-east-1 region is selected by default.

If you're prompted to update the region version, follow the prompts to complete the update. For information, see [Update a Region Version](#), on page 73.

**CISCO DNA Center VA Launch Pad**

Region: us-east-1

Cloudwatch Dashboard

Dashboard

User Activities

Admin

Help Center

**Dashboard**

**Create New VA Pod**

**No VA Pod(s) created!**

You can create new Virtual Appliance (VA) pod by clicking the above button.

ⓘ Please make sure you have the following minimum resources to install Cisco DNA Center:

- ⓘ Cisco DNA Center Server: 32 vCPU, 256GB RAM, and 4TB storage available.
- ⓘ Cloud Backup Server: 2vCPU, 500 GB storage on t3 micro instance.
- ⓘ VA Pod = AWS hosting environment for Cisco DNA Center Virtual Appliance which include collection of AWS resources such as DNAC EC2 instance, EBS storage, backup NFS server, security groups, gateways, routing tables, etc.\*

VA Launchpad: v63

© 2022 Cisco Systems, Inc. Privacy Terms

- Step 4** If you encounter any login errors, you need to resolve them and log in again. For more information, see [Troubleshoot Login Errors, on page 37](#).

## Log In as a Federated User Using saml2aws-Generated Credentials

You can generate temporary AWS credentials using a Command Line Interface (CLI) tool and use the generated credentials to log in to Cisco DNA Center VA Launchpad.

### Procedure

- Step 1** From the CLI, install saml2aws. For information, see the detailed instructions on [Github](#).

- Step 2** Verify the installation by entering **saml2aws**.

If the installation is successful, the following output is displayed:

```
[redacted] ~ % saml2aws
usage: saml2aws [<flags>] <command> [<args> ...]

A command line tool to help with SAML access to the AWS token service.

Flags:
 --help Show context-sensitive help (also try --help-long
 and --help-man).
 --version Show application version.
 --verbose Enable verbose logging
 --quiet silences logs
 -i, --provider=PROVIDER This flag is obsolete. See:
 https://github.com/Versent/saml2aws#configuring-i
dp-accounts
 --config=CONFIG Path/filename of saml2aws config file (env:
 SAML2AWS_CONFIGFILE)
 -a, --idp-account="default" The name of the configured IDP account. (env:
 SAML2AWS_IDP_ACCOUNT)
 --idp-provider=IDP-PROVIDER The configured IDP provider. (env:
 SAML2AWS_IDP_PROVIDER)
 --mfa=MFA The name of the mfa. (env: SAML2AWS_MFA)
 -s, --skip-verify Skip verification of server certificate. (env:
```

- Step 3** Configure your account.

- Enter **saml2aws configure**.
- At the **Please choose a provider** prompt, choose a provider and press **Enter**.

```
[redacted] ~ % saml2aws configure
? Please choose a provider: [Use arrows to move, type to filter]
 Akamai
 Auth0
 AzureAD
> Browser
 F5APM
 GoogleApps
 JumpCloud
```

- c) At the **AWS Profile** prompt, press **Enter** to use the default AWS profile.

```

~ % saml2aws configure
? Please choose a provider: Browser
? AWS Profile (saml)

```

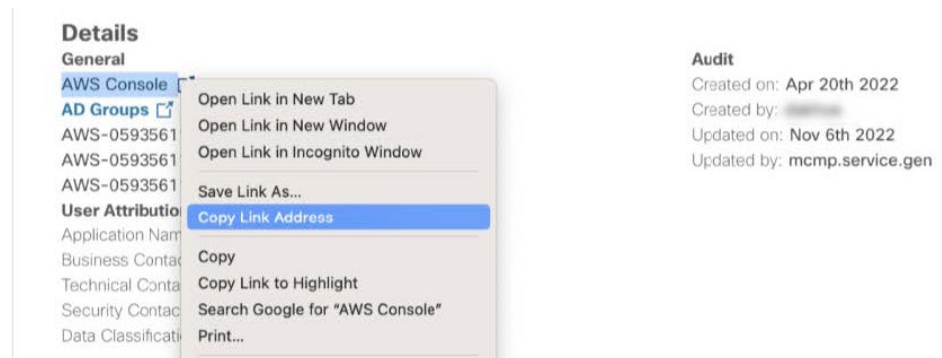
- d) At the **URL** prompt, enter the URL of your identity provider (IdP) and press **Enter**.

```

~ % saml2aws configure
? Please choose a provider: Browser
[? AWS Profile saml
? URL (https://cloudsso.cisco.com/idp/startSSO.ping?PartnerSpId=https://signin.a
ws.amazon.com/saml)

```

**Note** You can get this information from your IdP.



- e) At the prompts, enter your username and password and press **Enter**.



```

exec [<flags>] [<command>...]
 Exec the supplied command with env vars from STS token.

console [<flags>]
 Console will open the aws console after logging in.

list-roles [<flags>]
 List available role ARNs.

script [<flags>]
 Emit a script that will export environment variables.

```

```

[redacted] ~ % saml2aws configure
? Please choose a provider: Browser
? AWS Profile saml
? URL https://cloudsso.cisco.com/idp/startSSO.ping?PartnerSpId=https://signin.aws.amazon.com/saml
? Username [redacted]
? Password [redacted]

```

**Step 4** Generate your federated credentials.

- Enter **saml2aws login**.
- At the prompts, enter your username and password.
- At the prompt, select either the **Admin** or **CiscoDNACenter** role and press **Enter**.

**Note** Ensure that the tokens created for these roles have a minimum expiry of 180 minutes (3 hours).

Your credentials are generated and stored in `~/aws/credentials`.

```

[redacted] ~ % saml2aws script
export AWS_ACCESS_KEY_ID=
export AWS_SECRET_ACCESS_KEY=
export AWS_SESSION_TOKEN=

export AWS_SECURITY_TOKEN=IqoJb3JpZ2luX2VjEQAQcXVzLWVhc3QtMSJIMEYICQ57/JKbcFRmVhjeAC/48J6VXn3anqxs/LhFqy1ERf2twIhAJft15wqZ83sHyBE
rPnbu6xMZPjSj9+r5Ewy73PRNEpKvoCCLz//////////wEQABoMMDU5MzU2MTEyMzUyIgx/PgnuyGmIFxpRKJcqzGJx+973k27K54YYewpv8mF0MbAmiZUCT3txuqkUb0
qjuOWrXPjRAi19bgBLC2jXe19q9VJIfeQYUGnQ+8WuuECXzy1tXF+/ZaDpjVnyry4Bw30ggZhpRJJiohT2T0+KxTZPLshMdhPGTqi2U/Jf1g1AipRDux/Myd1LDKveSIP
ptVpTnAmgLA0tTYpZDmTGNwKc9Hs66S0qcreTWpGSuCNxjzvUENSky6uAZV0TivtgmEFz6VjixY0aoBLWLEk+LGziXeVucpyGSugCjzJVzNACZQF0fEePb21KjJzra
EX7ioLc07LbomZ0UP6ME2pza5uWZ0/AEicPUhpvRfkn5fS+fS0syHdvprYIDWLX25zmNrqzhxT6vqR7EjJmnl20GfsYRheJQFDIBY0/5dyian4zPjGFhtaGCSWHX74T
HfZyCfzu+yAr9b0zMMaGvKAG0poBBkUU70tSu4raGjuu8W81DhXUqEhvkvt0qhPzmpcjgV25MKyL4rM1aGCXXtIpoJ9/IVEfuRIWL123qYdYLpTnN9x0qDDghh/Ys0gd
+Nuu+BPNYG4qjMCRGni1oypnN1Bj6TCLNmWQjYGG5d17owrFCPquoRoas+80mE86GHKYlu0siCeeA9SCMSf8+2zoJvyyAjME0tXPFgvVA==
export SAML2AWS_PROFILE=saml
export AWS_CREDENTIAL_EXPIRATION=2023-03-13T17:34:38+05:30

```

**Step 5** Download the credentials by entering **saml2aws script**.

**Step 6** Note the values of the following parameters as you will use them to log into Cisco DNA Center VA Launchpad as a federated user:

- `AWS_ACCESS_KEY_ID`
- `AWS_SECRET_ACCESS_KEY`

- `AWS_SESSION_TOKEN`

**Step 7** On Cisco DNA Center VA Launchpad login window, select **Federated Login**.

**Step 8** Enter the generated credentials in the corresponding fields:

- **Access Key ID:** Enter the value obtained from the `AWS_ACCESS_KEY_ID` parameter.
- **Secret Access Key:** Enter the value obtained from the `AWS_SECRET_ACCESS_KEY` parameter.
- **Session Token:** Enter the value obtained from the `AWS_SESSION_TOKEN` parameter.

**Step 9** Click **Authenticate**.

## Log In as a Federated User Using AWS CLI-Generated Credentials

You can generate temporary AWS credentials using a the AWS Command Line Interface (CLI) and use these credentials to log in to Cisco DNA Center VA Launchpad.

### Procedure

**Step 1** In a browser window, navigate to the **AWS Single Sign On (SSO)/Active Directory (AD)** window.

**Step 2** In the **AWS Single Sign On (SSO)/Active Directory (AD)** window, click the AWS Console link.

The following window is displayed.

**Step 3** Right-click anywhere in the window, and from the drop-down menu, choose **Inspect Element** or **Inspect** (depending on the browser).

**Note** You can also press the **F12** key to open the **Developer Tools** panel.)

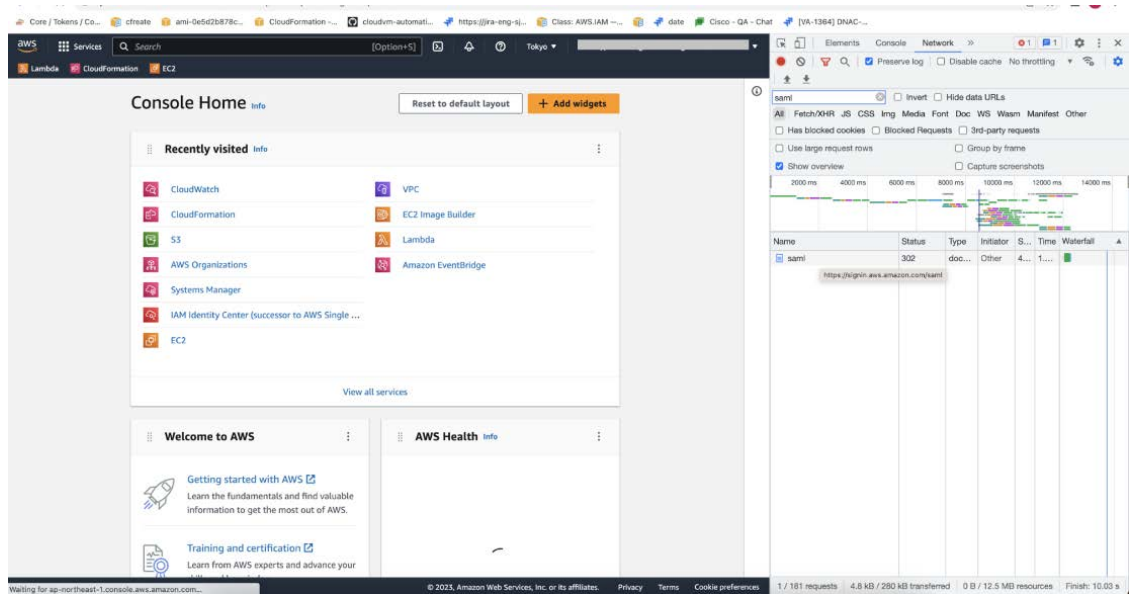
The **Developer Tools** panel is displayed, similar to the following window.

**Step 4** In the **Developer Tools** panel, click the **Network** tab and check the **Preserve Log** check box. (This option can be found on the tool panel, right beside the Magnifying Glass icon.)

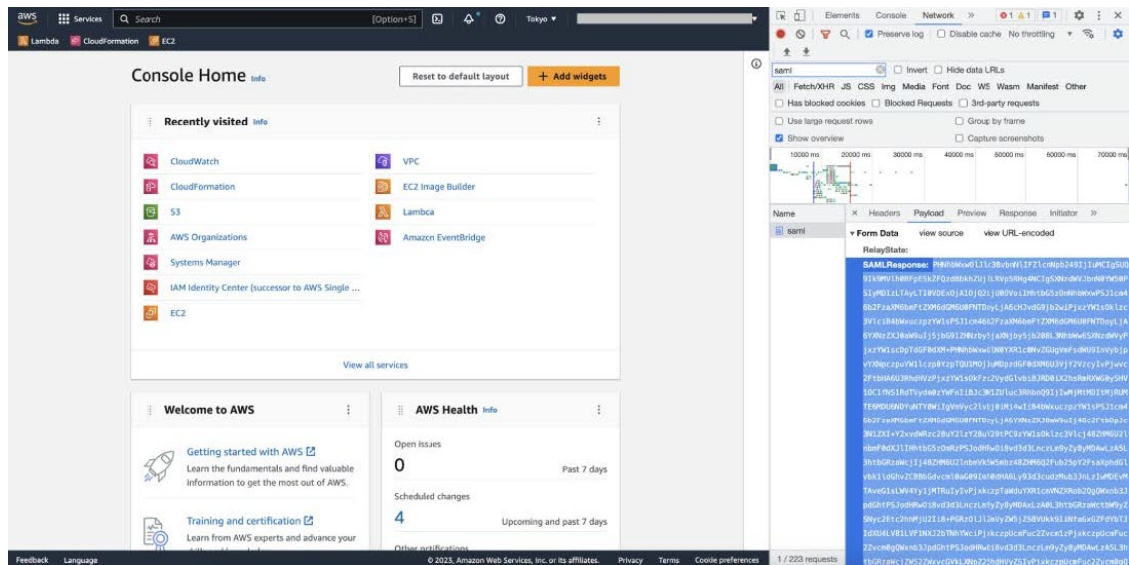
**Step 5** In the **AWS Console**, click **Sign In**.

**Step 6** In the **Developer Tools** panel, filter the required API calls by entering **sam1** in the **Filter** field.

## Log In as a Federated User Using AWS CLI-Generated Credentials



- Step 7** Click the API request named **saml**.
- Step 8** Click the **Payload** tab.
- Step 9** Copy the value of the SAML response.



- Step 10** Navigate to your AWS Console, choose **IAM > Access Management > Identity Providers**, and select your IdP.

The screenshot shows the AWS IAM console interface. On the left is the navigation menu for 'Identity and Access Management (IAM)'. The main content area is titled 'IAM > Identity providers'. At the top of this area is a notification banner about AWS IAM Identity Center. Below that, there's a section for 'Identity providers (1/5)' with a 'Delete' button and an 'Add provider' button. A search bar is present with the text 'Filter Identity providers by property or provider name and press enter'. Below the search bar is a table of identity providers:

| Provider                                            | Type | Creation time |
|-----------------------------------------------------|------|---------------|
| <input type="radio"/> idp1                          | SAML | 21 days ago   |
| <input type="radio"/> DNACADFS                      | SAML | 10 days ago   |
| <input type="radio"/> idp001                        | SAML | 18 days ago   |
| <input checked="" type="radio"/> cloudsso.cisco.com | SAML | 7 months ago  |
| <input type="radio"/> RAMANTECH                     | SAML | 4 months ago  |

At the bottom of the console, there are links for 'Feedback', 'Language', and '© 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences'.

**Step 11** Obtain the following details for your IdP:

- Role assigned to the IdP
- Amazon Resource Name (ARN) of the IdP

**Step 12** From the AWS CLI, enter the following command:

```
aws sts assume-role-with-saml --role-arn <Role-Arn> --principal-arn <IDP-Arn> --saml-assertion <SAML response>
```

The variables in this command refer to the values obtained earlier, as follows:

- **<Role-Arn>**: Role assigned to the IdP, obtained in Step 11.
- **<IDP-Arn>**: Amazon Resource Name (ARN) of the IdP, obtained in Step 11.
- **<SAML response>**: Value of the SAML response, obtained in Step 9.

For example:

```
aws sts assume-role-with-saml --role-arn
arn:aws:iam::059356109852:role/ADFS-AWS-ADMIN --principal-arn
arn:aws:iam::059356109852:saml-provider/cloudsso.cisco.com --saml-
assertion
MIIC6jCCAdKgAwIBAgIQPP5He1K6QoZPQRiUPjzCUTANBgkqhkiG9w0BAQsFADAxMS8wLQY
DVQDEyZBREZTIFNpZ25pbmcgLSBFQzJBTUFaLU1IMUYzQ0Quc3NvLmNvbTAeFw0yMzAyMDY
wNTUyNDJaFw0yNDYwNTUNDJamDEXLzAtBgNVBAMTJkFERlMgU2lnbmluZyAtIEVDMkF
NQVotTUgXRjNDRC5zc28uY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAsl
Sx/rQJ/wAOJ6ZRBbgYkFE7TMPsnOTqX0C+dh+yQ30+X9xqRDPVKuSDHrv72bsGwk/
2VRdb38xdVueuFYRavyVPzjsSF95fkjC3qFDN+R5Dk1Cnba7GT6i+HGfacEpL8Vqd3jzNgh
guskM1OrHDHKDv5ksNMxppHIDPlVhyRCdKEtP1PG5gBftoKvBZX+RxYcTaVUK/
NrMfkWmklyQTNrmpUDj+NAwGGjr4byjH8hUu59cFJetatzJo8qxuWWtPBtd+ESS/
DVR5dpilfyEBi4Dc22X91kOShJpeDu08EGfR605/nmRErlyy/p5f2sPKM0/
ix+XLQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQA7kt4HeU/
zohOSDnnfmXYpYi8WrJFxmVrTS6CjwE8eYZ6BwByEI4PjxcjPOu+sVNXrtBzJUwyPM+LKKMs
zYn5VQ/skrwcljW5P4msUMj4/J5K4vuYcKbJS4VyASKVZmWUWC23WhpC3U8ft6F7Jynp/
omrEh6Xrc4f4SgFdvIz35h2Sd/
HbcDp+shZzm4TgnA2XuSuvv0NJPF2VsRHMCMsn3eBTQfbbD5naLEpitjU8Zy5qW+Ic8Up51
ATNzPP+kmaQY6SxPLeuAarrnp4vDrD7hpszneRfWX8h9v/Fg+wlnOsEeD1FYyLRoc
```

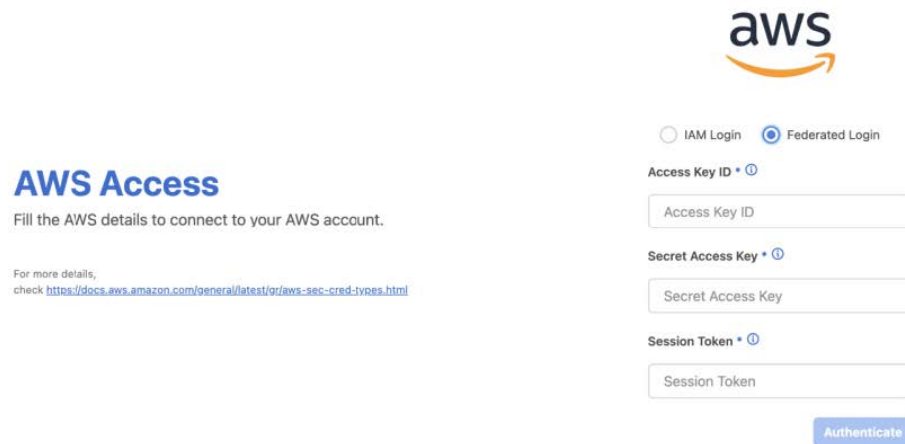
Output similar to the following is displayed:

```
{
 "Credentials": {
 "AccessKeyId": "xxxx",
 "SecretAccessKey": "xxxxx",
 "SessionToken": "xxxxxxxxxx",
 "Expiration": "2023-03-10T18:07:15+00:00"
 },
 "AssumedRoleUser": {
 "AssumedRoleId": "xxx:user@sso.com",
 "Arn": "arn:aws:sts::059356109852:assumed-role/ADFS-AWS-ADMIN/user@sso.com"
 },
 "Subject": "SSO\\USER",
 "SubjectType": "transient",
 "Issuer": "http://EC2AMAZ-MH1F3CD.sso.com/adfs/services/trust",
 "Audience": "https://signin.aws.amazon.com/saml",
 "NameQualifier": "POIUYTRFVNMKJGFKJHJHJcYLQCePSAZg="
}
```

**Step 13** Note the values of the following generated credentials:

- AccessKeyId
- SecretAccessKey
- SessionToken

**Step 14** On Cisco DNA Center VA Launchpad login window, select **Federated Login**.



**AWS Access**

Fill the AWS details to connect to your AWS account.

For more details, check <https://docs.aws.amazon.com/general/latest/gr/aws-sec-cred-types.html>

IAM Login  Federated Login

Access Key ID \* ⓘ

Access Key ID

Secret Access Key \* ⓘ

Secret Access Key

Session Token \* ⓘ

Session Token

Authenticate

- Step 15** Enter the generated credentials that you obtained in Step 13 in the corresponding fields:
- **Access Key ID:** Enter the value of the AccessKeyId credential.
  - **Secret Access Key:** Enter the value of the SecretAccessKey credential.
  - **Session Token:** Enter the value of the SessionToken credential.

- Step 16** Click **Authenticate**.

## Configure the Cisco DNA Center VA Launchpad Region

You can choose a region from the list of supported regions in Cisco DNA Center VA Launchpad.

### Before you begin

Make sure that you successfully installed Cisco DNA Center VA Launchpad. For more information, see [Install Cisco DNA Center VA Launchpad, on page 11](#).

Confirm with your AWS administrator that the relevant regions are enabled in AWS. On Cisco DNA Center VA Launchpad, the **Region** drop-down list only displays enabled regions.

### Procedure

- Step 1** Log in to Cisco DNA Center VA Launchpad.

For more information, see [Log In with Cisco, on page 60](#).

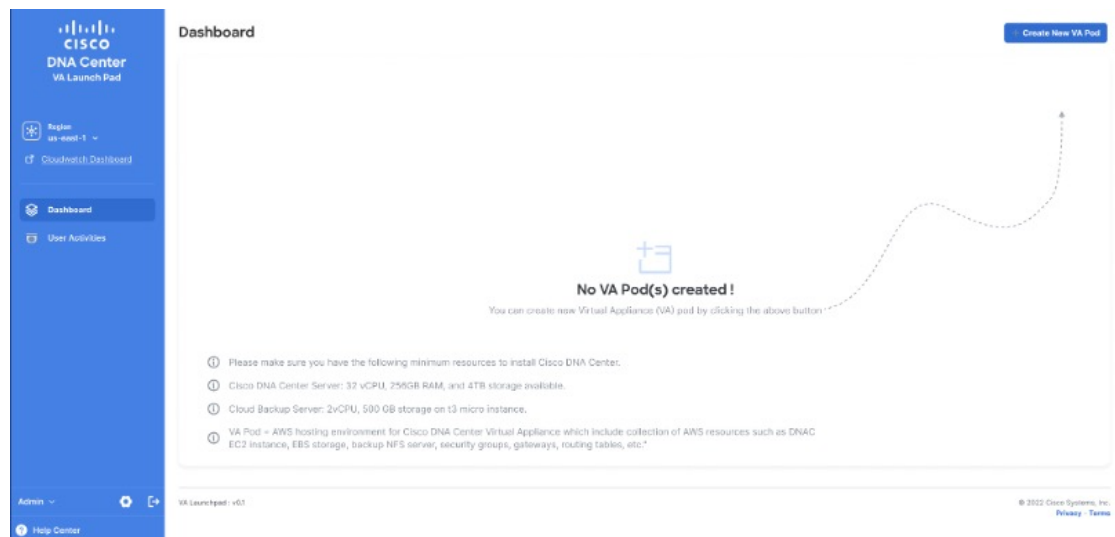
**Dashboard** is displayed.

If you're prompted to update the region version, follow the prompts to complete the update. Note that you need to be at a minimum release of 1.0.4 (Limited Availability release) before you can install Release 1.2.x and update a region version. For information, see [Update a Region Version, on page 73](#).

**Note** You must update a region when an updated version is available. Cisco DNA Center VA Launchpad automatically checks if an updated region version is available whenever you log in or change the selected region. If an updated region version is detected, Cisco DNA Center VA Launchpad prompts you to update it. Follow the on-screen prompts.

The update may take a few minutes. Do not close the tab or window until the process has completed.

If the update fails, Cisco DNA Center VA Launchpad restores the region to the last working version and displays an error. In this case, contact Cisco TAC for assistance.



**Step 2** In **Dashboard's** top-left corner, from the **Region** drop-down list, choose one of the following regions:

- ap-northeast-1 (Tokyo)
- ap-northeast-2 (Seoul)
- ap-south-1 (Mumbai)
- ap-southeast-1 (Singapore)
- ap-southeast-2 (Sydney)
- ca-central-1 (Canada)
- eu-central-1 (Frankfurt)
- eu-south-1 (Milan)
- eu-west-1 (Ireland)
- eu-west-2 (London)



- eu-west-3 (Paris)
- us-east-1 (Virginia)
- us-east-2 (Ohio)
- us-west-1 (N. California)
- us-west-2 (Oregon)

If you're prompted to update the region version, follow the prompts to complete the update. Note that you need to be at a minimum release of 1.0.4 (Limited Availability release) before you can install Release 1.2.x and update a region version. For information, see [Update a Region Version, on page 73](#).

- Note**
- Only enabled regions are displayed in the **Region** drop-down list.
  - To enable access to the new regions added in Release 1.2.x, your admin user needs to log in to Cisco DNA Center VA Launchpad after the Cisco DNA Center VA Launchpad, Release 1.2.x has been installed. After the admin user has logged in, access to all regions is enabled for all other users.

---

## Update a Region Version

You must update a region when an updated version is available. Cisco DNA Center VA Launchpad automatically checks if an updated region version is available whenever you log in or change the selected region. If an updated region version is detected, Cisco DNA Center VA Launchpad prompts you to update it. Follow the on-screen prompts.



- 
- Note** You need to be at a minimum release of 1.0.4 (Limited Availability release) before you can install Release 1.2.x and update a region version.
- 

The update may take a few minutes. Do not close the tab or window until the process has completed.

If the update succeeds, click **Ok** to continue.

If the update fails, Cisco DNA Center VA Launchpad restores the region to the last working version and displays an error. In this case, contact Cisco TAC for assistance.

## Edit a VA Pod

You can edit your VA pod only if you chose **VPN GW** as your preference while creating the VA pod.

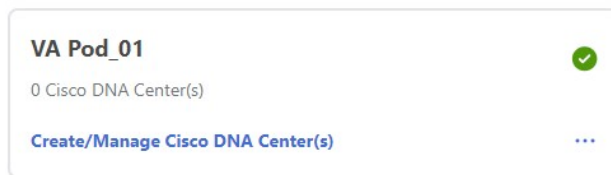
### Before you begin

Make sure that you successfully installed Cisco DNA Center VA Launchpad. For more information, see [Install Cisco DNA Center VA Launchpad, on page 11](#).

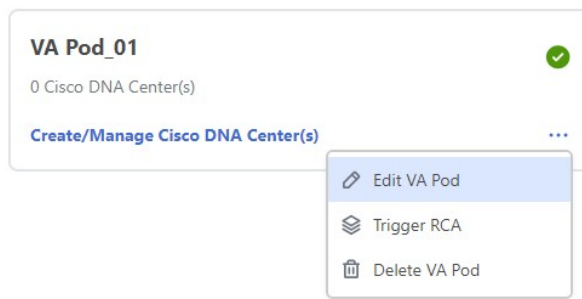
## Procedure

**Step 1** Log in to Cisco DNA Center VA Launchpad.  
For more information, see [Log In with Cisco, on page 60](#).

**Step 2** On **Dashboard**, locate the VA pod.



**Step 3** In the bottom-right corner of the VA pod card, click the ellipsis icon (...) and choose **Edit VA Pod**.



**Step 4** In the **Modify VPN Details** page, make the desired edits to the following VPN details and then click **Next**:

- Customer Gateway IP  
Make sure that the Customer Gateway IP is a valid public address.
- VPN Vendor
- Platform
- Software

**Step 5** Review the edited details, and when you're ready, click **Proceed to On-Prem Configuration**.

**Step 6** Configure the on-premises connectivity.

- a) From the **Configure On-premise** screen, click **Download Configuration File**.
- b) Forward this file to your network administrator to configure the on-premises-side IPsec tunnel.  
  
The network administrator can make the necessary changes to this file and apply this configuration to your Enterprise firewall or router to bring up IPsec tunnels.  
  
For more information, see [Create a New VA Pod, on page 21](#).
- c) Click **Proceed to Network Connectivity Check**.

**Step 7** Check the status of your network configuration.

When your network administrator is configuring the IPsec tunnel, the IPsec tunnel configuration status displays as not configured with a padlock icon.



When your network administrator completes the configuration and the IPsec tunnel configures successfully, the IPsec tunnel configuration status displays green with a success icon.



**Step 8** (Optional) To return to **Dashboard**, click **Go to Dashboard**.

## Delete a VA Pod

You can delete a VA pod on Cisco DNA Center VA Launchpad.



### Note

- You can't delete a VA pod while you are deleting a Cisco DNA Center VA that is in the pod. You must wait for the Cisco DNA Center VA to delete first.
- Deleting a VA pod doesn't delete the TGW because the TGW can be in use by a preexisting VPN or VPC.

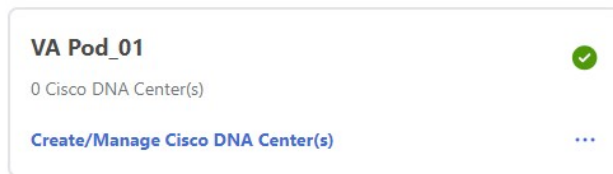
**Before you begin**

Make sure that you successfully installed Cisco DNA Center VA Launchpad. For more information, see [Install Cisco DNA Center VA Launchpad, on page 11](#).

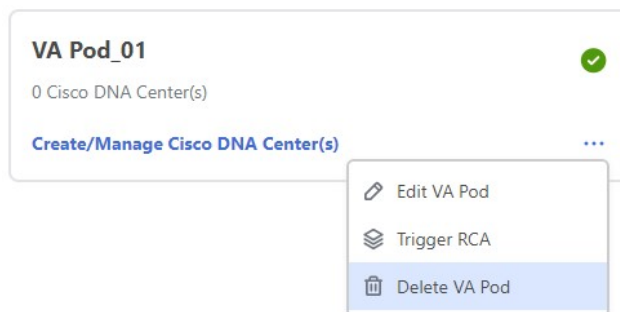
**Procedure**

**Step 1** Log in to Cisco DNA Center VA Launchpad.  
For more information, see [Log In with Cisco, on page 60](#).

**Step 2** On **Dashboard**, locate the VA pod.



**Step 3** In the bottom-right corner of the VA pod, click the ellipsis icon (...) and choose **Delete VA Pod**.  
Note that if you are deleting a Cisco DNA Center VA that's in the VA pod, the **Delete VA Pod** option is not available.



**Step 4** In the **Confirmation** dialog box, in the text field, type **DELETE**.

**Confirmation**

Are you sure you want to delete **VA Pod\_01**?  
This will permanently delete all the DNAC instances in this VA Pod.

Please type **DELETE** to confirm the operation

Cancel Delete

**Step 5** Click **Delete** to confirm that the deletion of the VA pod on Cisco DNA Center VA Launchpad.  
The deletion of VA pods takes approximately 20 to 40 minutes.

## View Cisco DNA Center VA Details

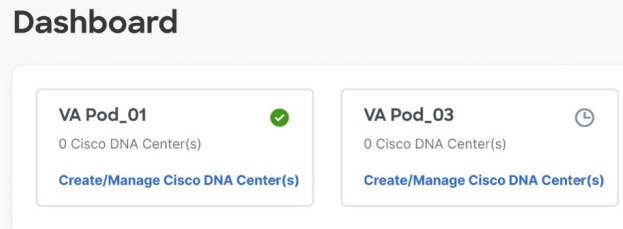
You can view Cisco DNA Center VA details on Cisco DNA Center VA Launchpad.

### Before you begin

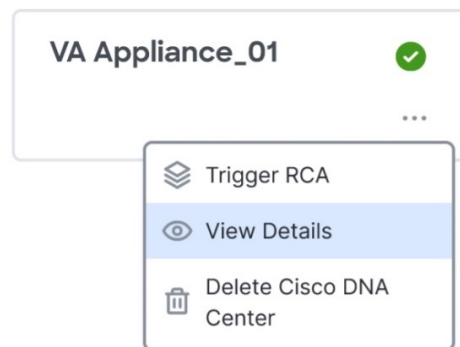
Make sure that you successfully installed Cisco DNA Center VA Launchpad. For more information, see [Install Cisco DNA Center VA Launchpad, on page 11](#).

### Procedure

- Step 1** Log in to Cisco DNA Center VA Launchpad.  
For more information, see [Log In with Cisco, on page 60](#).
- Step 2** On **Dashboard**, locate the VA pod containing the Cisco DNA Center VA you want to view, and in the VA pod card, click **Create/Manage Cisco DNA Center(s)**.



- Step 3** In the bottom-right corner of the Cisco DNA Center VA card, click the ellipsis icon (...) and choose **View Details**.



- Step 4** In the **Cisco DNA Center Virtual Appliance Details** window, view the following details.

### Cisco DNA Center Virtual Appliance Details

#### Domain Details

Enterprise DNS [REDACTED]

FQDN (Fully Qualified Domain Name) dna01.ciscodnacenter.com

#### Proxy Details

Customer HTTPS Network Proxy No Proxy

Cisco DNA Center URL [REDACTED]

Cloud Backup Server IP [REDACTED]

**Step 5** (Optional) To exit this window, click **Close**.

## Delete an Existing Cisco DNA Center VA

You can delete an existing Cisco DNA Center VA on Cisco DNA Center VA Launchpad.

### Before you begin

Make sure that you successfully installed Cisco DNA Center VA Launchpad. For more information, see [Install Cisco DNA Center VA Launchpad, on page 11](#).

### Procedure

**Step 1** Log in to your AWS account.

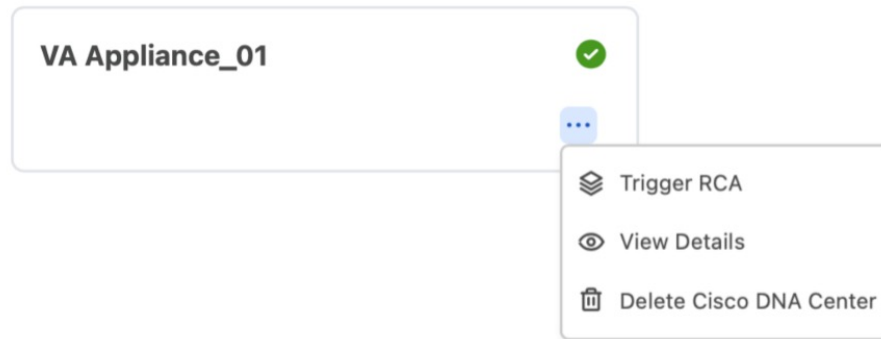
For more information, see [Log In with Cisco, on page 60](#)

**Step 2** On **Dashboard**, locate the VA pod containing the Cisco DNA Center VA you want to delete, and in the VA pod card, click **Create/Manage Cisco DNA Center(s)**.

### Dashboard

| VA Pod    | Status               | Action                                            |
|-----------|----------------------|---------------------------------------------------|
| VA Pod_01 | OK (Green checkmark) | <a href="#">Create/Manage Cisco DNA Center(s)</a> |
| VA Pod_03 | Error (Clock icon)   | <a href="#">Create/Manage Cisco DNA Center(s)</a> |

**Step 3** In the bottom-right corner of the Cisco DNA Center VA card, click the ellipsis icon (...) and choose **Delete Cisco DNA Center**.



**Step 4** In the **Confirmation** dialog box, in the text field, type **DELETE**.

### Confirmation

Are you sure you want to delete **VA Appliance\_01**  
This will permanently delete the DNAC instance.

Please type **DELETE** to confirm the operation

Cancel

Delete

**Step 5** Click **Delete** to confirm that the deletion of the Cisco DNA Center VA on Cisco DNA Center VA Launchpad.

## Trigger a Root Cause Analysis (RCA)

On Cisco DNA Center VA Launchpad, you can trigger a root cause analysis (RCA) to help you identify the root cause of an issue pertaining to the AWS infrastructure or the Cisco DNA Center VA deployment. The RCA operation collects logs from AWS and stores them in the AWS S3 bucket. The RCA bundle includes backup logs, backend logs, Amazon CloudWatch alarm logs, and AWS resources and event logs.

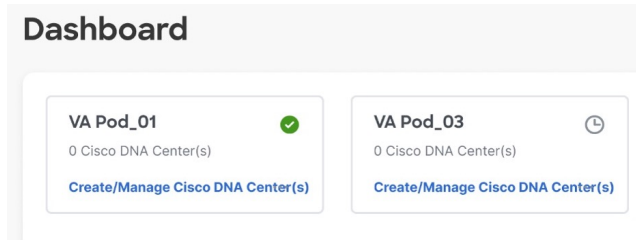
### Before you begin

Make sure that you successfully installed Cisco DNA Center VA Launchpad. For more information, see [Install Cisco DNA Center VA Launchpad, on page 11](#).

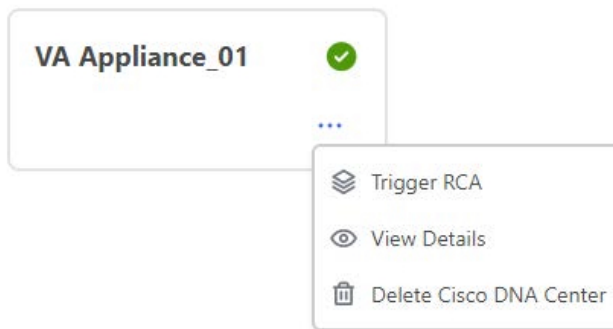
### Procedure

**Step 1** Log in to your AWS account.  
For more information, see [Log In with Cisco, on page 60](#).

**Step 2** On **Dashboard**, locate the VA pod containing the Cisco DNA Center VA that you want to trigger an RCA on, and in the VA pod card, click **Create/Manage Cisco DNA Center(s)**.



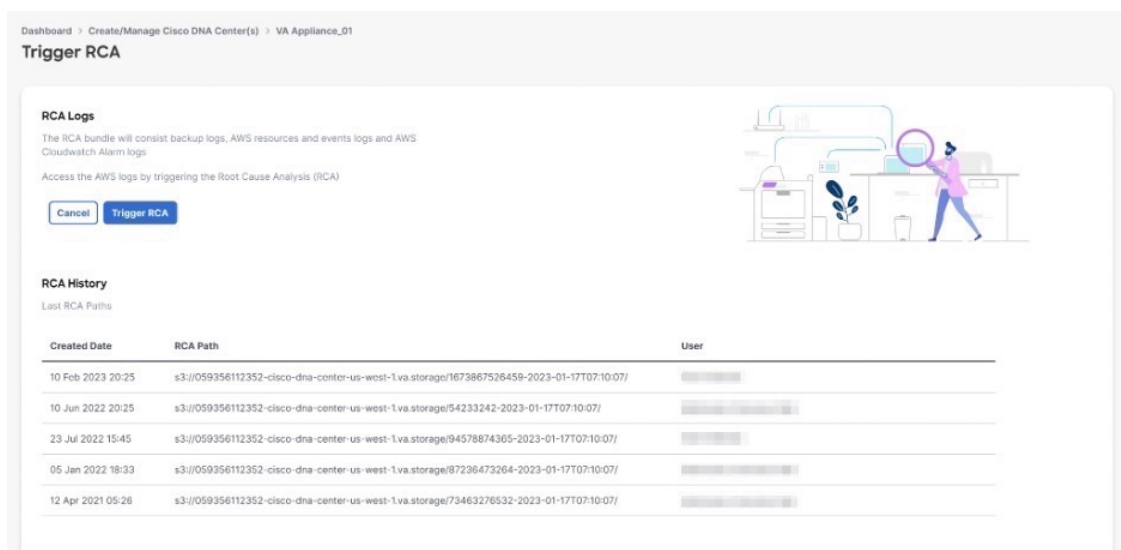
**Step 3** In the bottom-right corner of the Cisco DNA Center VA card, click the ellipsis icon (...) and choose **Trigger RCA**.



**Step 4** On the **Trigger RCA** window, in the **RCA Logs** area, click **Trigger RCA** to gather and bundle the AWS logs.

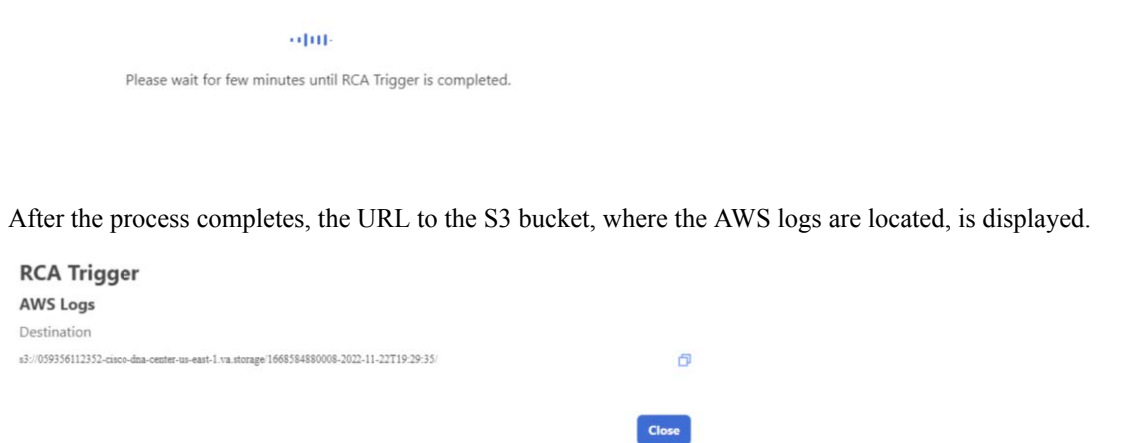
Cisco DNA Center VA Launchpad uses AWS Config and Amazon CloudWatch to record, assess, and audit the used resources.

**Note** On the **Trigger RCA** window, you can view the last five successfully triggered RCAs in the **RCA Logs** table.





This process takes a few minutes.



After the process completes, the URL to the S3 bucket, where the AWS logs are located, is displayed.

### RCA Trigger

#### AWS Logs

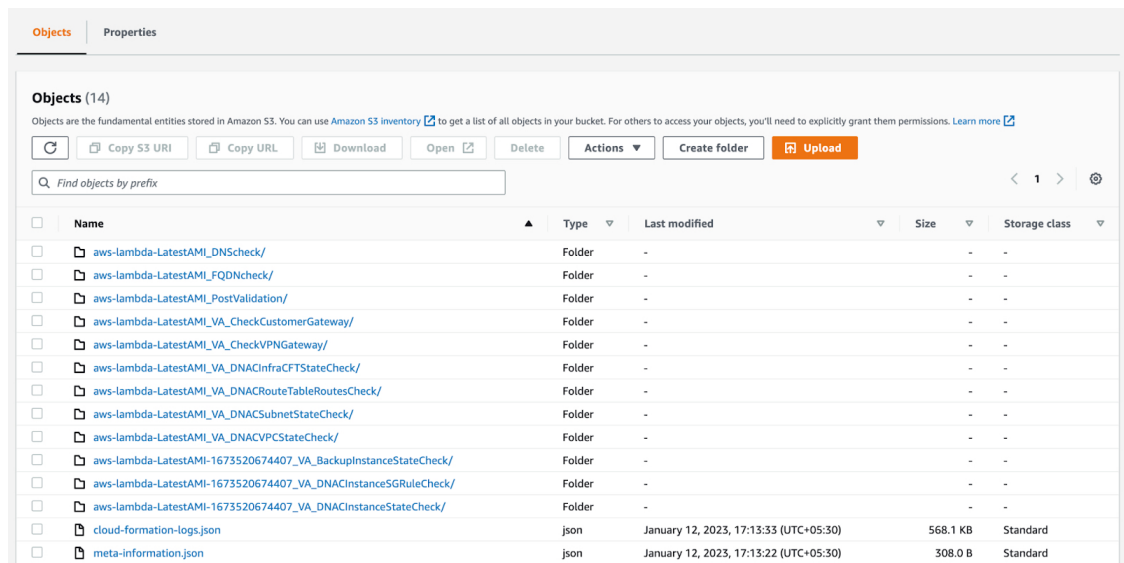
Destination

s3://059256112352-cisco-dna-center-us-east-1-va.storage.1668584880008-2022-11-22T19:29:35/

Close

**Step 5** Under **Destination**, click the URL displayed to go to the AWS S3 bucket.

The contents of the S3 bucket are displayed.



Depending on the resources created, the number of log groups vary.

## AWS Config and Audit Log Details

AWS Config is an AWS tool that continually assesses, monitors, and evaluates resource configurations to aid in operational troubleshooting by correlating configuration changes to specified events and states. Cisco DNA Center VA Launchpad uses AWS Config to audit the configuration. When AWS Config detects a change in the configuration, Cisco DNA Center VA Launchpad generates an email notifying you that configuration changes have taken place.

## Configure Amazon CloudWatch Notifications

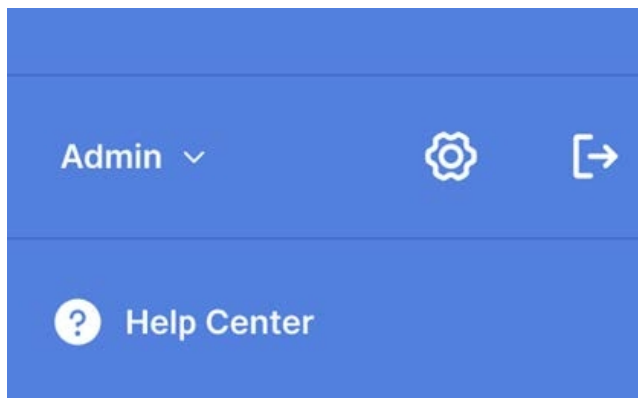
To receive Amazon CloudWatch notifications, you can configure your user settings by updating your email address. Amazon CloudWatch sends alerts about deployed resources, changes, or resource over-utilization to the provided email.

### Before you begin

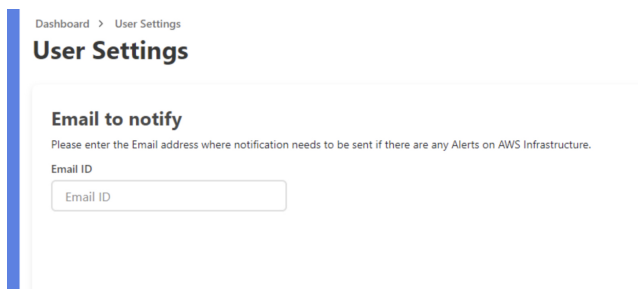
Make sure that you successfully installed Cisco DNA Center VA Launchpad. For more information, see [Install Cisco DNA Center VA Launchpad, on page 11](#).

### Procedure

- Step 1** Log in to the Cisco DNA Center VA Launchpad.  
For more information, see [Log In with Cisco, on page 60](#).
- Step 2** In **Dashboard**'s bottom-left corner, from the user account drop-down list, choose a user account and then click the settings icon.



- Step 3** In the **User Settings** window, in the **User Email Configuration** area, enter the preferred email address in the **Email ID** field.



The old email address is unsubscribed, and the new email address is used for VA pods that are created after the email change. The new email address is not used for existing VA pods.

If an existing user account has not confirmed their email subscription and updates their subscription with a new email address, both the old and new email addresses are subscribed and remain configured in the Amazon Simple Notification System (SNS).

**Note** Multiple user accounts should not concurrently update their email ID. If this occurs, the latest updated email ID is used for email notification.

**Step 4** Click **Submit**.

---

## View Amazon CloudWatch Alarms

Cisco DNA Center VA Launchpad uses Amazon CloudWatch alarms to monitor resource usage and check for unusual behavior. The AWS RCA feature also uses Amazon CloudWatch alarms.

If a threshold is met, alerts are sent to the email ID that you configured during your first log in to Cisco DNA Center VA Launchpad or to the email ID in the user settings, if it was updated. For more information, see [Configure Amazon CloudWatch Notifications, on page 82](#).



- Note**
- The Amazon CloudWatch alarms for lambda functions remain in the insufficient data state unless a failure occurs in the corresponding lambda function execution. When a lambda function fails, Amazon CloudWatch gathers the metrics and triggers the alarm. The threshold for all lambda alarms is one, so Amazon CloudWatch can capture alerts if there are any failure.
  - For some alarms, like S3, the metrics are only reported once per day at midnight in Greenwich Mean Time (GMT). So it may take 24 to 48 hours for the dashboard metrics to update, which is an expected behavior.
- 

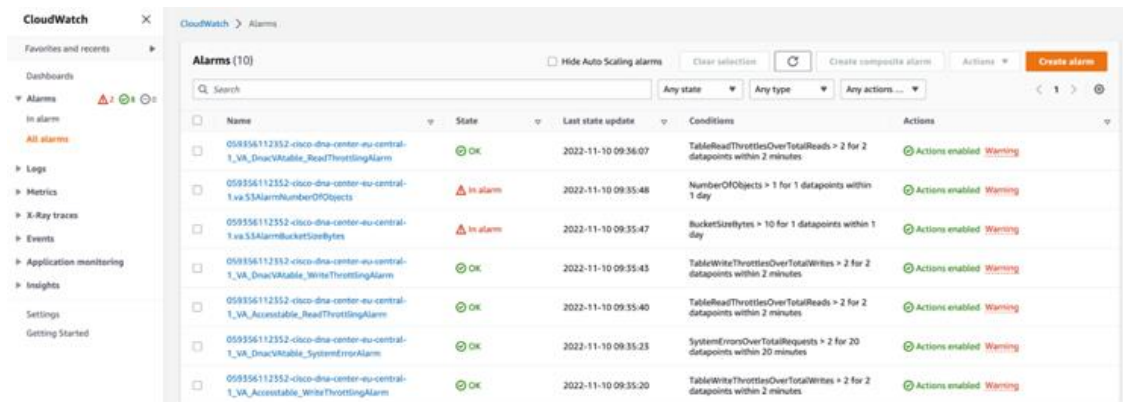
### Before you begin

Make sure you successfully configured your AWS account. For more information, see [Prerequisites for Automated Deployment, on page 8](#).

### Procedure

---

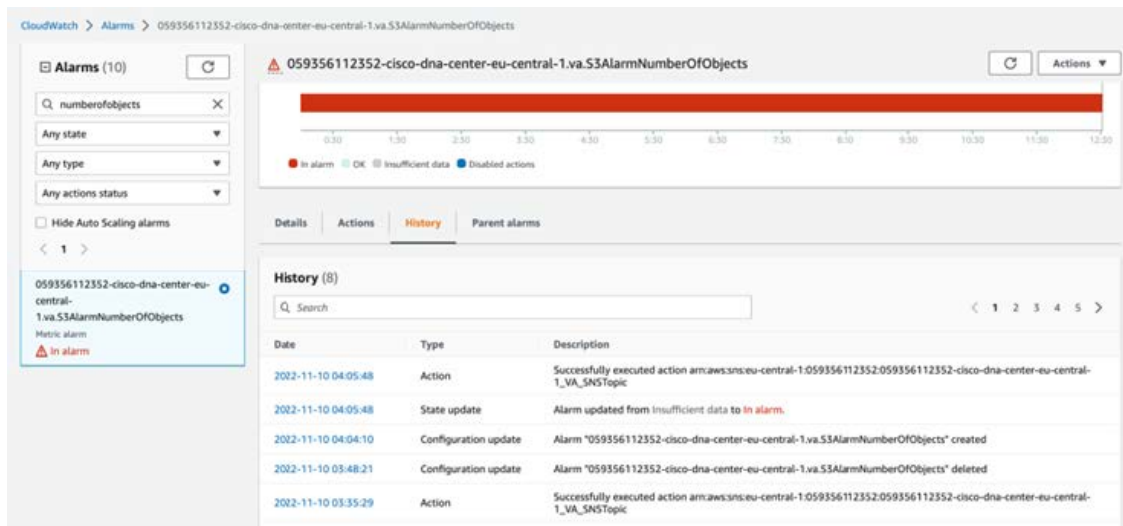
- Step 1** Log in to the AWS console.  
The AWS console is displayed.
- Step 2** From the AWS dashboard, click **CloudWatch > Alarms > All Alarms**.  
The **Alarms** page displays the status of all the alarms.



**Step 3** On the **Alarms** page, enter the environment name used to deploy Cisco DNA Center in the **Search** field. Alarms pertaining to the Cisco DNA Center instance with the specified environment name are displayed.

**Step 4** Click the name of an alarm.

Details about the alarm are displayed in the **Details** tab. To view other information, click the **Actions**, **History**, or **Parent alarms** tabs.

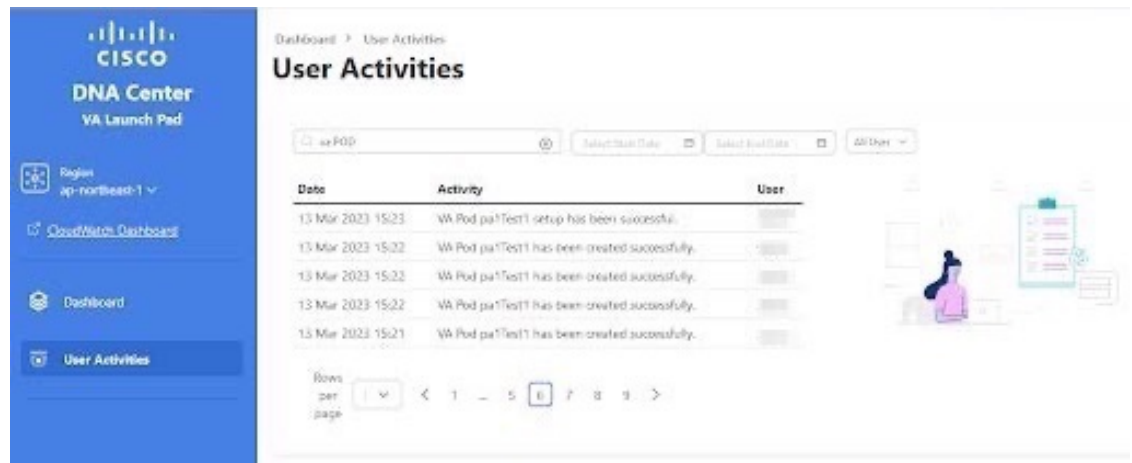


## View User Activities

On the **User Activities** window, you can view all the activities that you've performed in your selected region.

### Procedure

**Step 1** On **Dashboard**, in the left pane, click **User Activities**.



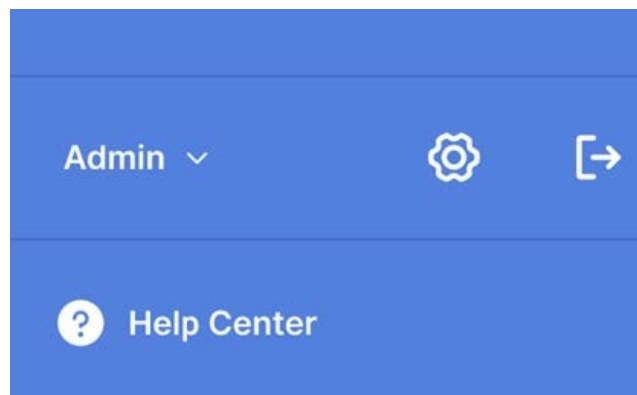
- Step 2** On the **User Activities** window, you can search and filter the **User Activities** table for information by doing the following:
- To search for an activity, use the **Search on Activity** bar.
  - To filter for an activity by date, click **Select Start Date** to choose a start date and click **Select End Date** to choose an end date.
  - To filter for an activity by user, from the **All User** drop-down list, choose a user account.

## Log Out

Depending on how you accessed your Cisco DNA Center VA Launchpad account, you either need to log out of only Cisco DNA Center VA Launchpad or both Cisco DNA Center VA Launchpad and Cisco DNA Portal.

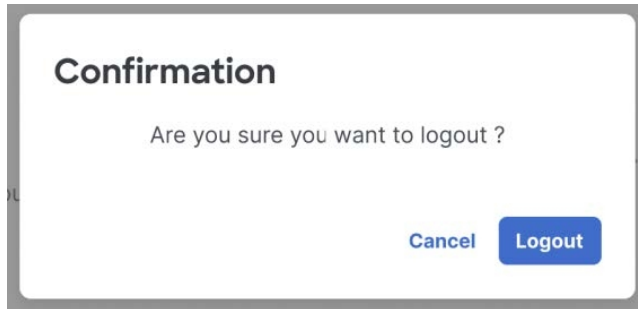
### Procedure

- Step 1** To log out of Cisco DNA Center VA Launchpad, in **Dashboard**'s bottom-left corner, click your user account and then click the log out icon.



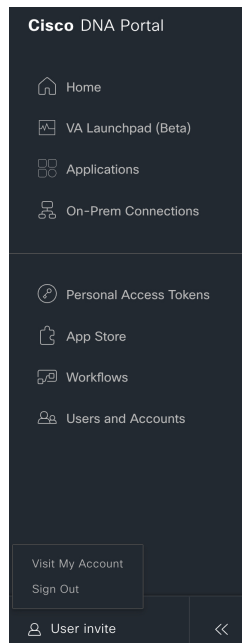
- Step 2** In the **Confirmation** dialog box, click **Logout**.

Your progress is automatically saved when you log out.



**Step 3** (Optional) If you accessed Cisco DNA Center VA Launchpad through Cisco DNA Portal, you must also log out of Cisco DNA Portal. Do the following:

- a) Click the menu icon (☰).
- b) Hover your cursor over your user account.
- c) Click **Sign Out**.



---

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2023 Cisco Systems, Inc. All rights reserved.