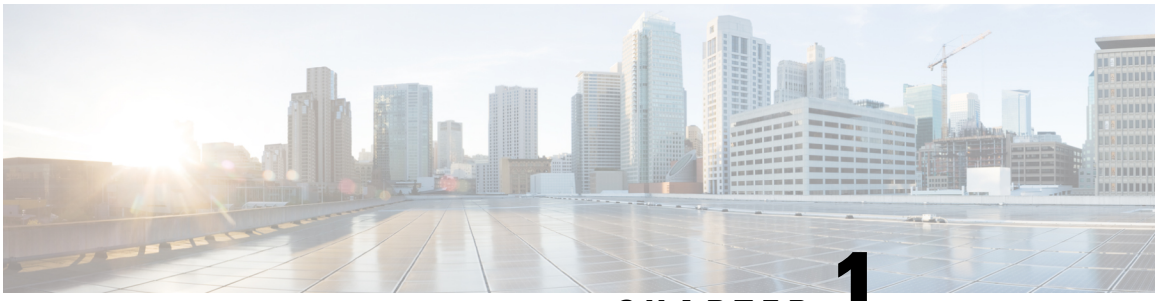
Cisco DNA Center 2.3.5 on AWS Deployment Guide

First Published: 2023-08-02

Last Modified: 2024-04-04

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

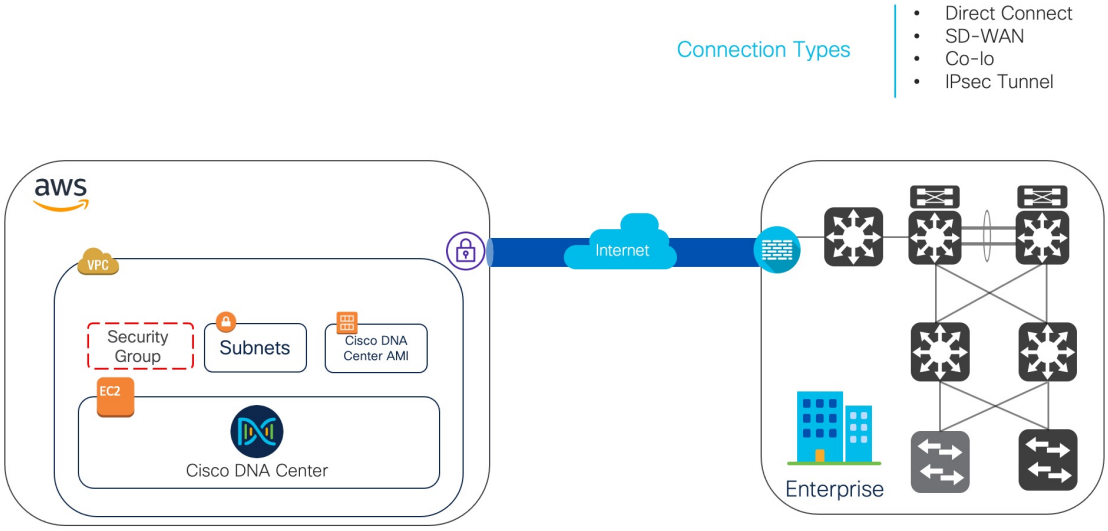
Get Started with Cisco DNA Center on AWS

Cisco DNA Center on AWS Overview

Note Cisco DNA Center has been rebranded as Catalyst Center, and Cisco DNA Center VA Launchpad has been rebranded as Cisco Global Launchpad. During the rebranding process, you will see the former and rebranded names used in different collaterals. However, Cisco DNA Center and Catalyst Center refer to the same product, and Cisco DNA Center VA Launchpad and Cisco Global Launchpad refer to the same product.

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 Amazon Web Services (AWS) provides the full functionality that a Cisco DNA Center appliance deployment offers. Cisco DNA Center on AWS runs in your AWS cloud environment and manages your network from the cloud.



Deployment Overview

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

- **Automated Deployment**: Cisco Global 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 Global Launchpad. You can download and install Cisco Global Launchpad on a local machine, or you can access Cisco Global Launchpad hosted by Cisco. Regardless of the method, Cisco Global Launchpad provides the tools you need to install and manage your Cisco DNA Center Virtual Appliance (VA).

  For more information, see Deploy Using Cisco Global Launchpad 1.8, on page 11 or Deploy Using Cisco Global Launchpad 1.7, on page 45.

- **Manual Deployment Using AWS CloudFormation**: You manually deploy the Cisco DNA Center AMI on your AWS. Instead of using the Cisco Global Launchpad deployment tool, 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 your Cisco DNA Center VA. For more information, see Deploy Using AWS CloudFormation, on page 79.

- **Manual Deployment Using AWS Marketplace**: You manually deploy the Cisco DNA Center AMI on your AWS account. Instead of using the Cisco Global Launchpad deployment tool, you use AWS Marketplace, which is an online software store within AWS. You launch the software through the 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 more information, see Deploy Using AWS Marketplace, on page 89.

If you have minimal experience with the AWS administration, the automated method with Cisco Global 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 Global Launchpad	Manual Deployment Using AWS CloudFormation	Manual Deployment Using AWS Marketplace
• 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.	• 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.	• The AWS CloudFormation file is *not* 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 with the same IP address. This ensures uninterrupted connectivity and minimizes disruptions during critical network operations.

Note If you deploy Cisco DNA Center on AWS using Cisco Global Launchpad, Release 1.5.0 or earlier and a Cisco DNA Center EC2 instance crashes, AWS automatically brings up another instance in the same AZ. In this case, AWS may assign Cisco DNA Center a different IP address.

- 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 Global 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 Global Launchpad cannot detect any out-of-band changes to entities that were created by Cisco Global 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 Global Launchpad from another application, and Cisco Global 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 Global 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 internet 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 Global Launchpad*.
- 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. The password must:

- Omit any tab or line breaks
- Have a minimum of eight characters
- Contain characters from at least three of the following categories:
  - Lowercase letters (a-z)
  - Uppercase letters (A-Z)
  - Numbers (0-9)
  - Special characters (for example, ! or #)

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 Global Launchpad, use the IP address and keys provided by Cisco Global Launchpad.
  - If you deployed Cisco DNA Center manually using AWS, use the IP address and keys provided by AWS.

Note The key must be a .pem file. If the key file is downloaded as a 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\Launchpad-desktop-server-1.x.0.tar.gz sha256
```

On Windows, you can also use Windows PowerShell to generate the digest. For example:

```
PS C:\Users\Administrator> Get-FileHash -Path
D:\Customers\Launchpad-desktop-server-1.x.0.tar.gz
Algorithm Hash Path
SHA256 <string> D:\Customers\Launchpad-desktop-server-1.x.0.tar.gz
```

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:

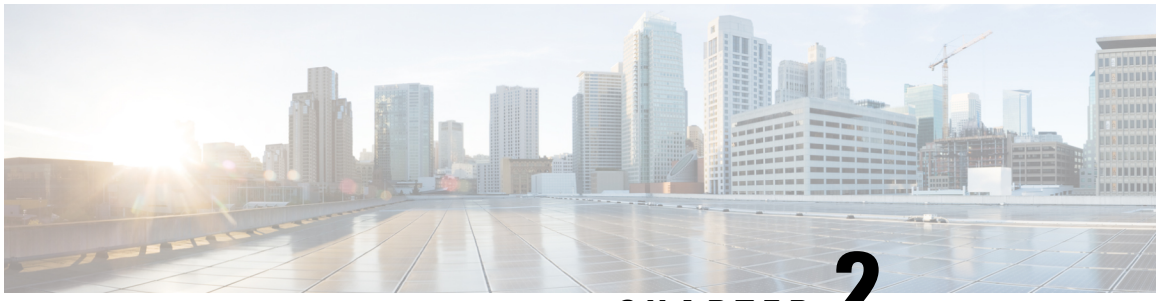
openssl dgst -sha512 -verify cisco_image_verification_key.pub -signature <signature-filename> <tar-file-filename>

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.

PART I

Deploy Cisco DNA Center 2.3.5.3 on AWS



CHAPTER 2

Deploy Using Cisco Global Launchpad 1.8

Use Cisco Global Launchpad to Automatically Deploy Cisco DNA Center on AWS

You provide Cisco Global Launchpad with the needed details to create the AWS infrastructure in your AWS account, which includes a VPC, an IPsec VPN tunnel, gateways, subnets, and security groups. As a result, Cisco Global Launchpad deploys the Cisco DNA Center AMI 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 AWS CloudFormation for monitoring, Amazon DynamoDB for state storage, and security groups.

Using Cisco Global Launchpad, you can also access and manage your VAs, as well as manage the user settings. For information, see the *Cisco Global Launchpad 1.8 Administrator Guide*.

Automated Deployment Workflow

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

1. Meet the prerequisites. See Prerequisites for Automated Deployment, on page 12.
2. (Optional) Integrate Cisco ISE on AWS and your 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 Global Launchpad or access Cisco Global Launchpad hosted by Cisco. See Install Cisco Global Launchpad, on page 15 or Access Hosted Cisco Global Launchpad, on page 17.

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're using an existing TGW and existing attachments, such as a VPC, as your preferred on-premises connectivity option, 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 30.
6. Create your new instance of Cisco DNA Center. See Create a New Cisco DNA Center VA, on page 31.
7. (Optional) If necessary, troubleshoot any issues that arise during the deployment. See Troubleshoot the Deployment, on page 35.
8. Manage your Cisco DNA Center VA using Cisco Global Launchpad. See the *Cisco Global Launchpad 1.8 Administrator Guide*.

Prerequisites for Automated Deployment

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

- Install Docker Community Edition (CE) on your platform.

  Cisco Global Launchpad supports Docker CE on Mac, Windows, and Linux platforms. See the documentation on the Docker website for the specific procedure for your platform.

- Regardless of how you access Cisco Global Launchpad to deploy your Cisco DNA Center VA, make sure that your cloud environment meets the following specifications:

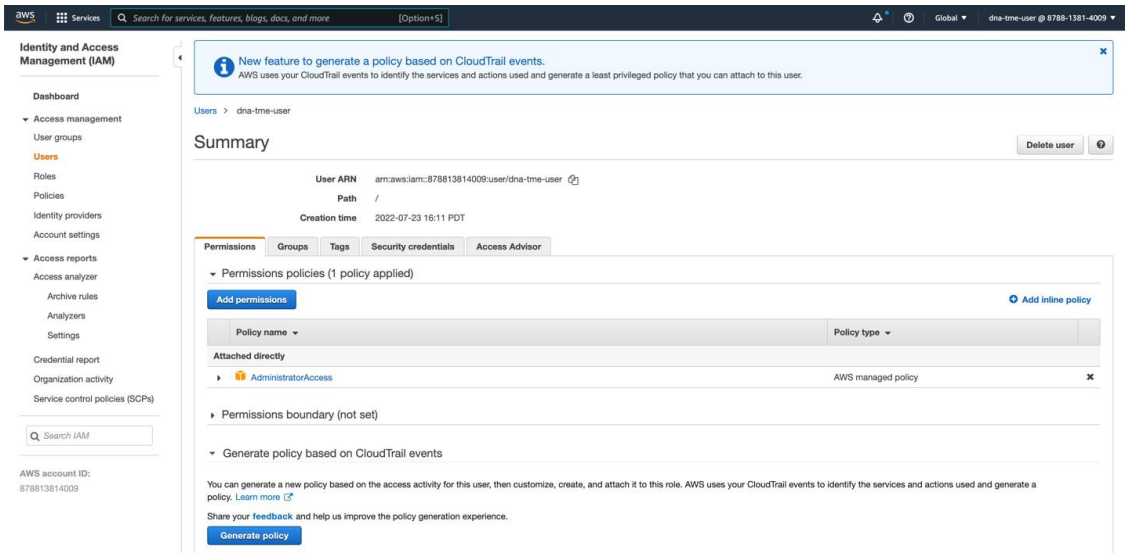
  - **Cisco DNA Center Instance**: r5a.8xlarge, 32 vCPUs, 256-GB RAM, and 4-TB storage

Important 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 in specific availability zones. To view the list of unsupported availability zones, see the *Release Notes for Cisco Global Launchpad 1.8.0*.

  - **Backup Instance**: T3.micro, 2 vCPUs, 500-GB storage, and 1-GB RAM

- You have valid credentials to access your AWS account.
- 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.
- **Important**: Your AWS account is subscribed to Cisco DNA Center Virtual Appliance - Bring Your Own License (BYOL) in AWS Marketplace.
- If you're an admin user, you must have 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.



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

  When an admin user logs in to Cisco Global 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 Global 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 Global Launchpad

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

Before you begin

Make sure you have Docker CE installed on your machine. For information, see Prerequisites for Automated Deployment, on page 12.

Procedure

Step 1 Go to the Cisco Software Download site and download the following files:

- `Launchpad-desktop-client-1.8.0.tar.gz`
- `Launchpad-desktop-server-1.8.0.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-1.8.0.tar.gz

docker load < Launchpad-desktop-server-1.8.0.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. In the files, the **TAG** column should display the numbers starting with **1.8**.

For example:

```
$ docker images

REPOSITORY                                                                  TAG       IMAGE ID       CREATED       SIZE
466518672524.dkr.ecr.us-west-2.amazonaws.com/val/valaunchpad-server         1.8.0     208375910fde   4 hours ago   546MB
466518672524.dkr.ecr.us-west-2.amazonaws.com/platform-ui/valaunchpad-client-docker   1.8.0     68a2452c4dfb   4 hours ago   2.08GB
```

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 208375910fde
```

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 68a2452c4dfb
```

Note Make sure that the exposed server port number and the REACT_APP_API_URL port number are the same. In Step 5, on page 15 and Step 6, on page 16, 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
d83bb3df1128   208375910fde   "/usr/bin/dumb-init …"   9 seconds ago    Up 8 seconds    0.0.0.0:9090->8080/tcp   aws-az-server
5de70c6e96f8   68a2452c4dfb   "docker-entrypoint.s…"   36 seconds ago   Up 35 seconds   0.0.0.0:90->80/tcp       aws-az-client
```

Note If you encounter an issue while running the server or client applications, see Troubleshoot Docker Errors, on page 35.

Step 8 Verify that the server application is accessible by entering the URL in the following format:

http://<localhost>**:**<server-port-number>**/api/valaunchpad/aws/v1/api-docs/**

For example:

```
http://192.0.2.2:9090/api/valaunchpad/aws/v1/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 Global Launchpad login window is displayed.

Note It can take a few minutes to load the Cisco Global Launchpad login window while the client and server applications load the artifacts.

Access Hosted Cisco Global Launchpad

You can access Cisco Global Launchpad through 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 Global 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 Global Launchpad.

Create a Cisco Account

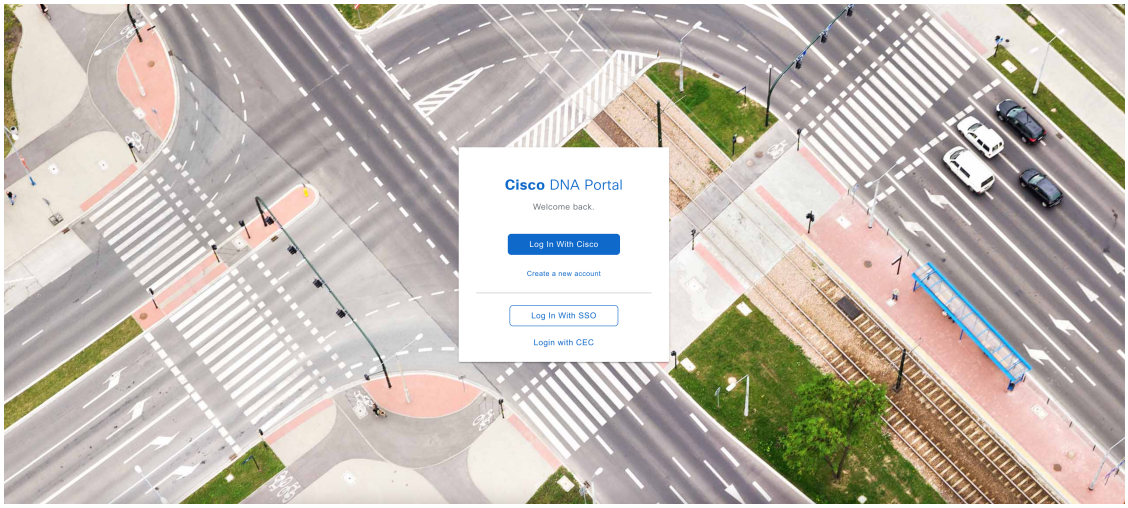
To access Cisco Global Launchpad through Cisco DNA Portal, you must create a Cisco account first.

Procedure

Step 1 In your browser, enter:

`dna.cisco.com`

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

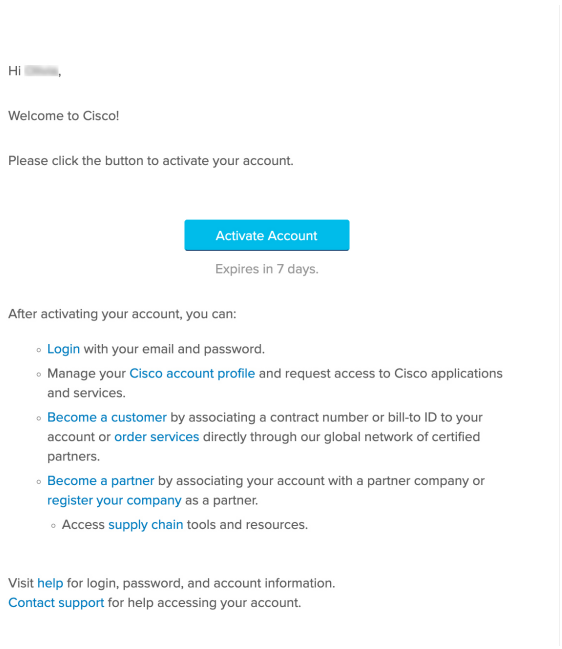


Step 2 Click **Create a new account**.

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**.

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


Hi [redacted],

Welcome to Cisco!

Please click the button to activate your account.

Activate Account

Expires in 7 days.

After activating your account, you can:

- Login with your email and password.
- Manage your Cisco account profile and request access to Cisco applications and services.
- Become a customer by associating a contract number or bill-to ID to your account or order services directly through our global network of certified partners.
- Become a partner by associating your account with a partner company or register your company as a partner.
  - Access supply chain tools and resources.

Visit help for login, password, and account information.
Contact support for help accessing your account.

Create a Cisco DNA Portal Account

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

Before you begin

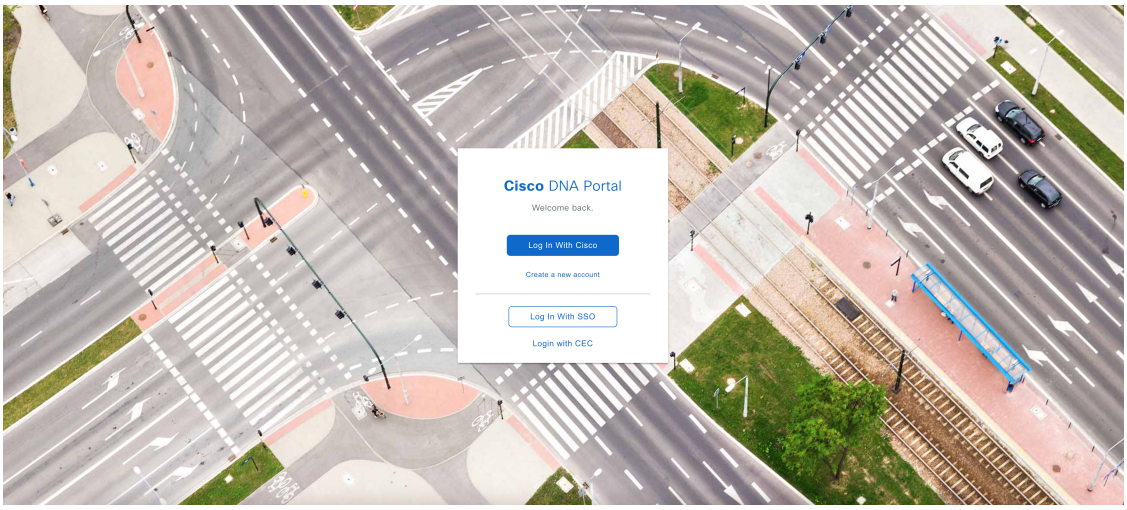
Make sure that you have a Cisco account. For more information, see Create a Cisco Account, on page 17.

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.

Step 5 Click **Log in**.

Step 6 On the **Cisco DNA Portal Welcome** window, enter the name of your organization or team in the **Name your account** field. Then click **Continue**.

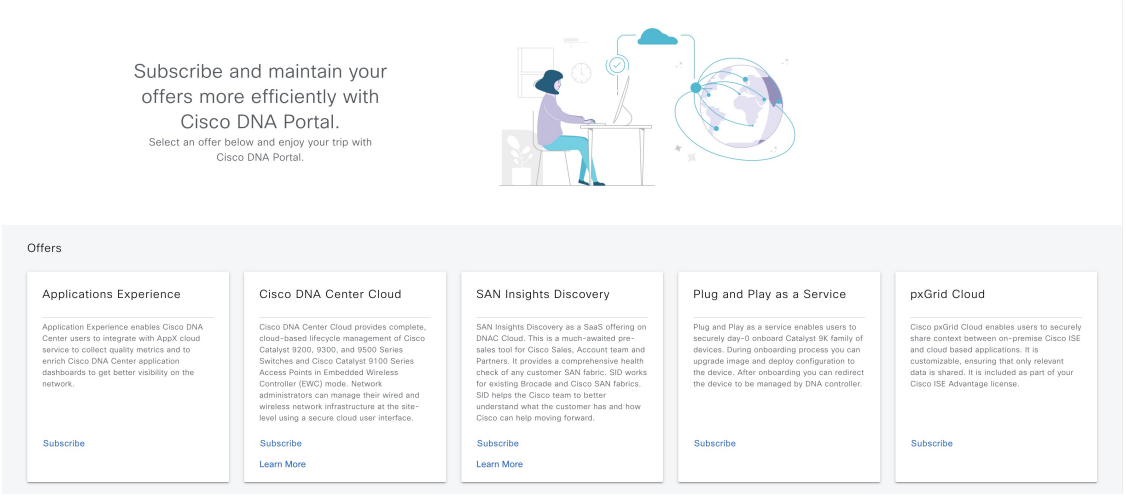
Step 7 On the **Cisco DNA Portal Confirm CCO Profile** window, do the following:

a) Verify the details are correct.

b) After reading, acknowledging, and agreeing with the conditions, check the check box.

c) Click **Create Account**.

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



Log In to the Cisco DNA Portal with Cisco

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

Before you begin

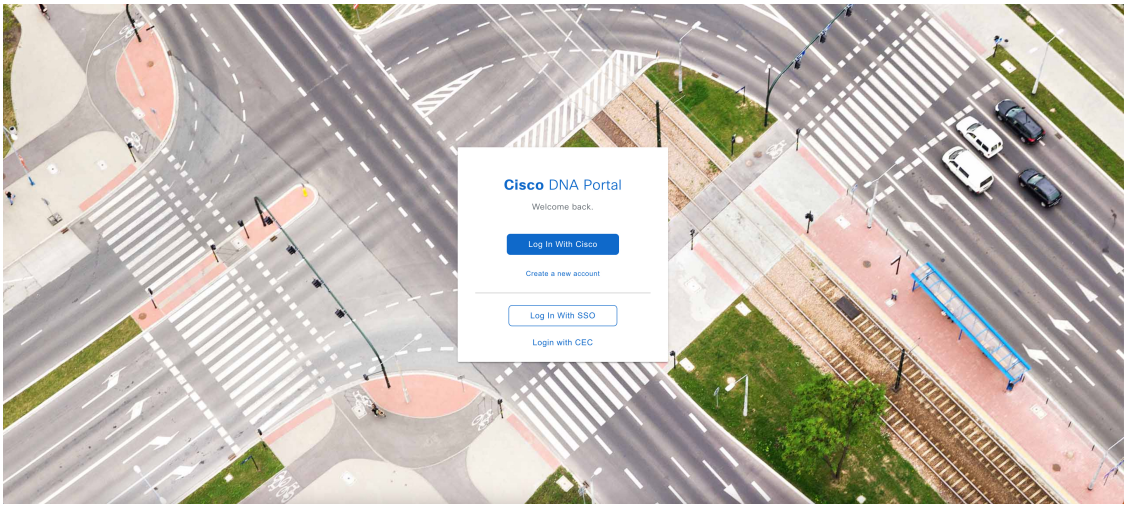
Make sure that you have a Cisco account and a Cisco DNA Portal account. For more information, see Create a Cisco Account, on page 17 and Create a Cisco DNA Portal Account, on page 18.

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**.

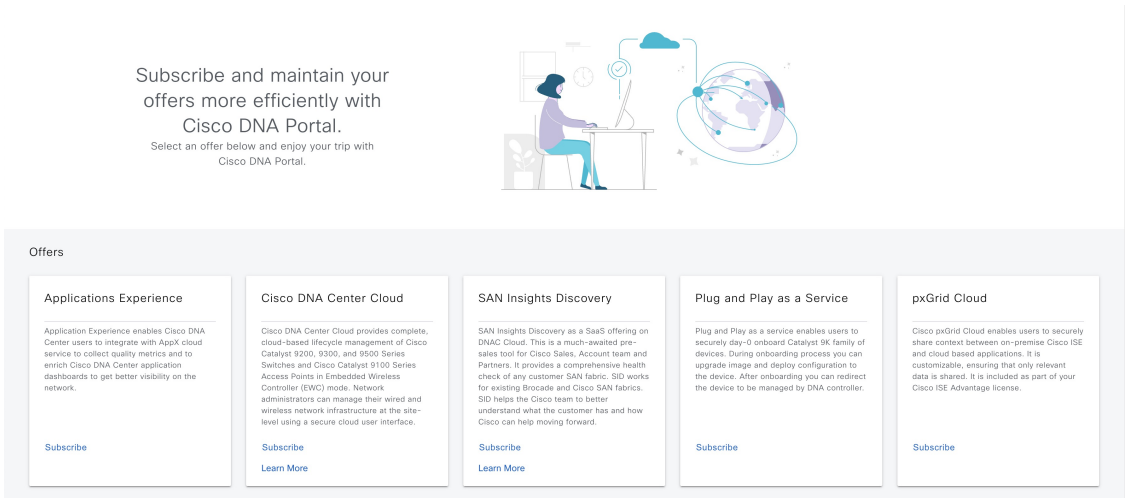
Step 4 Enter your Cisco account's password in the **Password** field.

Step 5 Click **Log in**.

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

Step 6 (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.

Using Cisco Global Launchpad, you can create multiple VA pods—one VA pod for each Cisco DNA Center VA.

Note

- The AWS Super Administrator user can set a limit on the number of VA pods that can be created in each region. The VPCs used for resources outside of Cisco Global Launchpad contribute to this number as well. 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 in the selected region.
- On some steps, all the resources must be set up successfully to proceed to the next step. If all the 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.
- Your VA pod configuration doesn't change when you update Cisco Global Launchpad to a later release, you downgrade to an earlier Cisco Global Launchpad release, or you update the region setup where your VA pod is located.

  For example, if you created a VA pod in Cisco Global Launchpad, Release 1.8.0, the backup password is a combination of the backup instance's stack name and the backup server's IP address. If you access this VA pod in an earlier release, such as Release 1.7.0, the backup password doesn't change.

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 12.

Procedure

Step 1 Log in to Cisco Global Launchpad using one of the following methods:

- **IAM Login**: This method uses user roles to define user access privileges. Cisco Global Launchpad supports multi-factor authentication (MFA) as an optional, additional form of authentication, if your company requires it. For more information, see "Log In to Cisco Global Launchpad Using IAM" in the *Cisco Global Launchpad Administrator Guide*.
- **Federated Login**: This method uses one identity to gain access to networks or applications managed by other operators. For more information, see "Generate Federated User Credentials Using saml2aws" or "Generate Federated User Credentials Using AWS CLI" in the *Cisco Global Launchpad Administrator Guide*.

For information about how to get an Access Key ID and Secret Access Key, see the AWS Managing access keys topic in the *AWS Identity and Access Management User Guide* on the AWS website.

If you encounter any login errors, you need to resolve them and log in again. For more information, see Troubleshoot Login Errors, on page 36.

Step 2 If you are an admin user logging in for the first time, enter your email address in the **Email ID** field and click **Submit**. If you are a subuser, proceed to Step 3, on page 23.

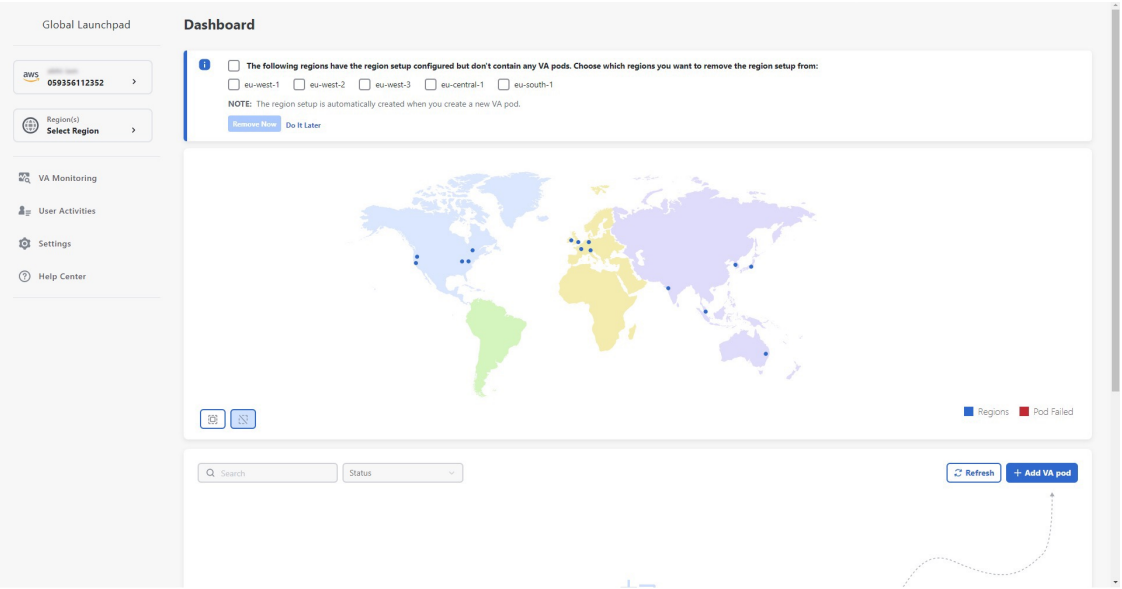
You can subscribe to the Amazon SNS to receive alerts about deployed resources, changes, and resource over-utilization. Further, alarms can be set up to notify you if Amazon CloudWatch detects any unusual behavior in Cisco Global Launchpad. In addition, AWS Config evaluates and assesses your configured resources and sends audit logs of the results as well. For more information, see "Subscribe to the Amazon SNS Email Subscription" and "View Amazon CloudWatch Alarms" in the *Cisco Global Launchpad Administrator Guide*.

After you enter your email, several processes happen:

- The CiscoDNACenter user group is created in your 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 Global Launchpad.
- An Amazon 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 Global Launchpad deployment workflow.
- If you are logging in to a region for the first time, Cisco Global 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, the **Dashboard** pane is displayed.

Note If you're prompted to update the region setup, follow the prompts to complete the update. For more information, see "Update a Region Setup" in the *Cisco Global Launchpad Administrator Guide*.



Step 3 Click + **Add VA pod**.

Step 4 Choose the region where you want to create the new VA pod by completing the following steps in the **Select a Region** dialog box:

a. From the **Region** drop-down list, choose a region.

If you already chose one region from the left navigation pane's **Region** drop-down list, this region is automatically chosen.

Note If you're prompted to update the region setup, follow the prompts to complete the update. For more information, see "Update a Region Setup" in the *Cisco Global Launchpad Administrator Guide*.

b. Click **Next**.

Step 5 Configure the AWS infrastructure, which includes the VPC, private subnet, routing table, security group, virtual gateway, and CGW, by completing the following steps:

a) In the **VA Pod Environmental Details** fields, configure the following fields:

- **VA Pod Name**: Assign a name to the new VA pod. Keep the following restrictions in mind:
  - The name must be unique within the region. (This means that you can use the same name across multiple regions.)
  - The name must have at least four characters and can have at most 12 characters.
  - The name can include letters (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 the AWS resources. Keep the following guidelines in mind:
  - The recommended CIDR range is /25.

- In IPv4 CIDR notation, the last octet (the fourth octet) of the IP address can only have the values 0 or 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 then 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 30.

c) Do one of the following:

- If you selected **Existing TGW** and **Existing Attachments** as your preferred connectivity options, proceed to Step 5.d, on page 24.
- If you selected **VPN GW**, **New VPN GW + New TGW**, or **Existing TGW + New VPN GW**, provide the following VPN details:
  - **CGW (Enterprise Firewall/Router)**: 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 Errors, on page 37.
  - **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:

- **Cisco Catalyst Center Instance**: r5a.8xlarge, 32 vCPU, 256-GB RAM, and 4-TB storage.

Important 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 in specific availability zones. To view the list of unsupported availability zones, see the *Release Notes for Cisco Global Launchpad 1.8.0*.

- **Backup Instance**: 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 the 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 in AWS.

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

  - **SSH IP Address**: <BACKUP VM IP>
  - **SSH Port**: 22
  - **Server Path**: /var/catalyst-backup/

    Note The directory is not automatically created in Cisco Global Launchpad, Release 1.8. You need to create the folder as required for configuring the backup. For more information, see "Configure an NFS Server" in *Cisco Global Launchpad Administrator Guide*.

  - **Username**: maglev
  - **Password**: <xxxx##########>

    Your backup server password is dynamically created. The password is composed of the first four characters of the VA pod name and the backup server's IP address without the periods.

    For example, if the VA pod name is DNAC-SJC and the backup server's IP address is 10.0.0.1, the backup server password is DNAC10001.

    Note
    - You can find the VA pod name on the **Dashboard** pane after you choose the region that it's deployed in.
    - You can find the backup server's IP address on the **View Catalyst Center** pane. For more information, see "View Catalyst Center VA Details" in the *Cisco Global Launchpad Administrator Guide*.

  - **Passphrase**: <Passphrase>

    Your passphrase is used to encrypt the security-sensitive components of the backup. These security-sensitive components include certificates and credentials.

    This passphrase is required and you will be prompted to enter this passphrase when restoring the backup files. Without this passphrase, backup files are not restored.

  - **Open Ports**: 22, 2049, 873, and 111

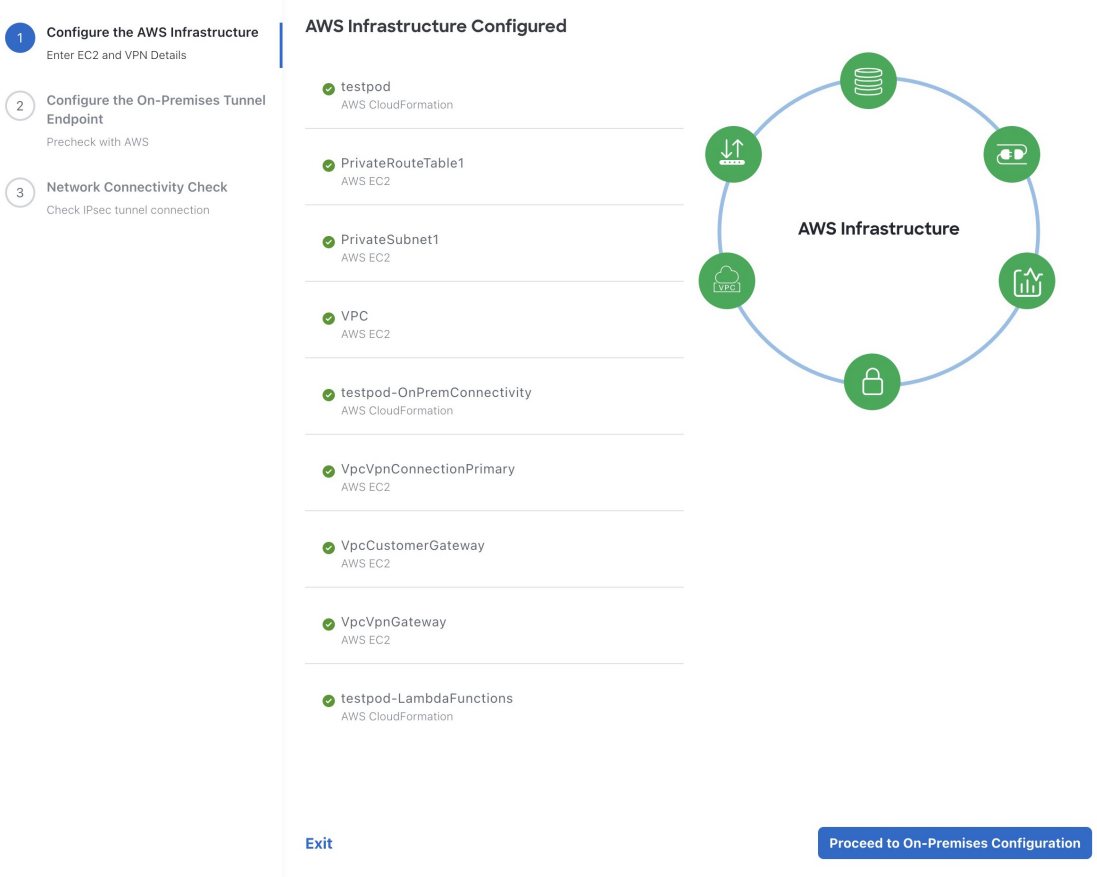
f) Click **Next**.

The **Summary** pane is displayed.

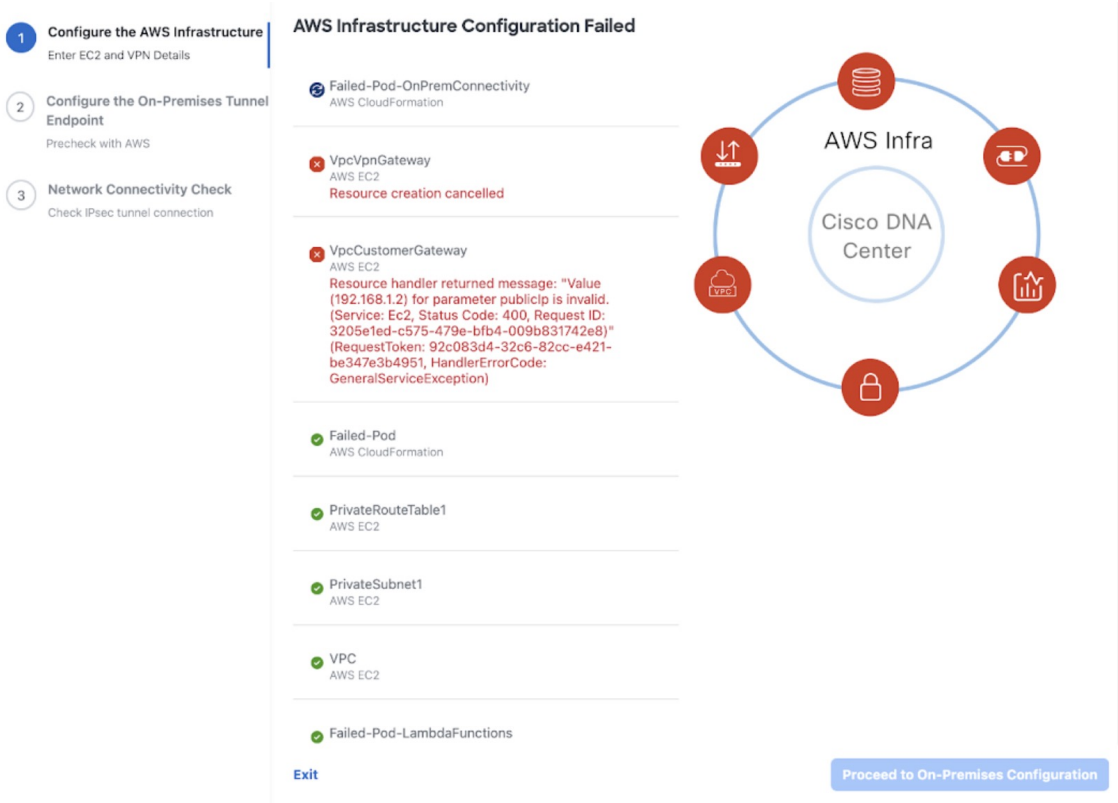
g) Review the environment and VPN details that you entered. If you are satisfied, click **Start Configuring AWS Infrastructure**.

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** pane is displayed.



If the AWS infrastructure configuration fails, exit Cisco Global Launchpad and see Troubleshoot VA Pod Configuration Errors, on page 37 for information about possible causes and solutions.



Step 6 Download the on-premises configuration file by completing the following steps:

a) After the AWS infrastructure is successfully configured, click **Proceed to On-Premises Configuration**.

b) In the **Configure the On-Premises Tunnel Endpoint** pane, 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 the IPsec tunnels.

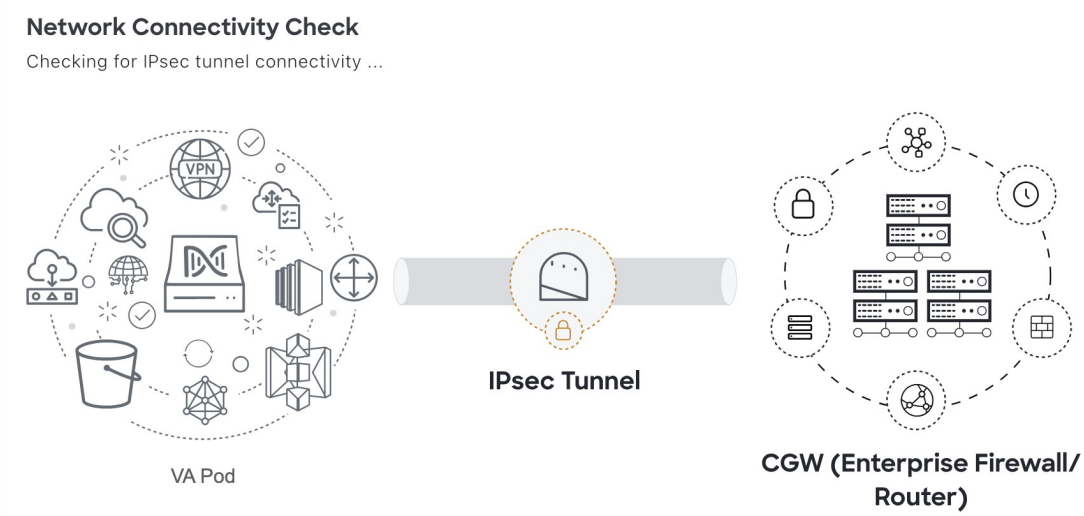
  The provided configuration file enables you to bring up two tunnels between AWS and the Enterprise router or firewall.

- 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.

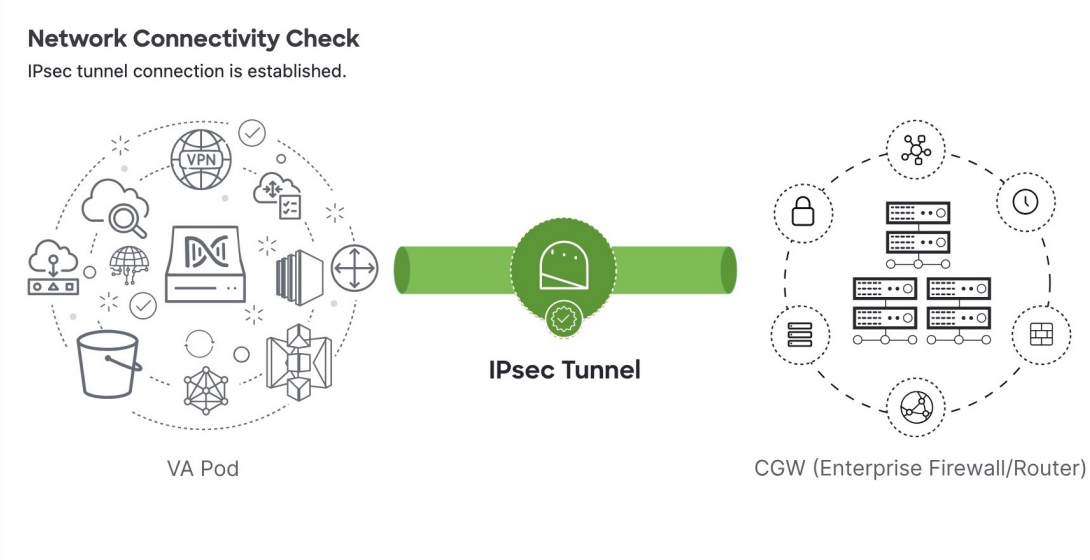
c) Click **Proceed to Network Connectivity Check** button.

Step 7 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:



Note If the IPsec tunnel is up and you cannot access Cisco DNA Center from the CGW, check that the correct values were passed during the IPsec tunnel configuration. Cisco Global Launchpad reports the tunnel status from AWS and doesn't perform additional checks.

- If you selected **New VPN GW + New TGW** or **Existing TGW and New VPN GW** as your preferred on-premises connectivity option, Cisco Global 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 is successfully established, the TGW connection is 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 30.

  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 is successfully established, the TGW connection is green:

Step 8 Click **Go to Dashboard** to return to the **Dashboard** pane, 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 option while creating a new VA pod, Cisco Global Launchpad creates a VPC to launch Cisco DNA Center and attaches this VPC to your existing TGW.

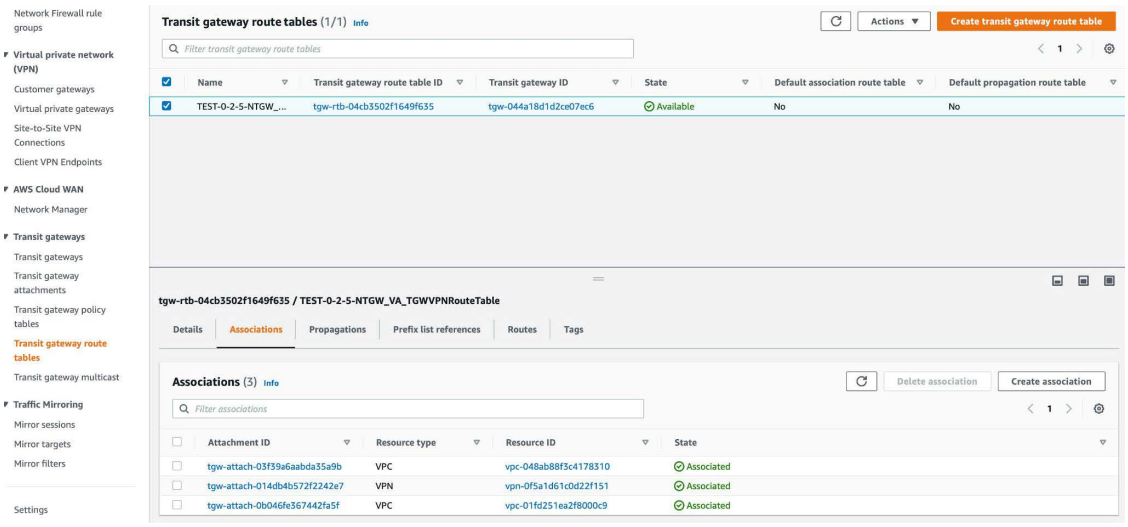
For Cisco Global Launchpad to establish the TGW connection, you must manually configure the TGW routing table on AWS and add the routing configuration to your existing CGW.

Procedure

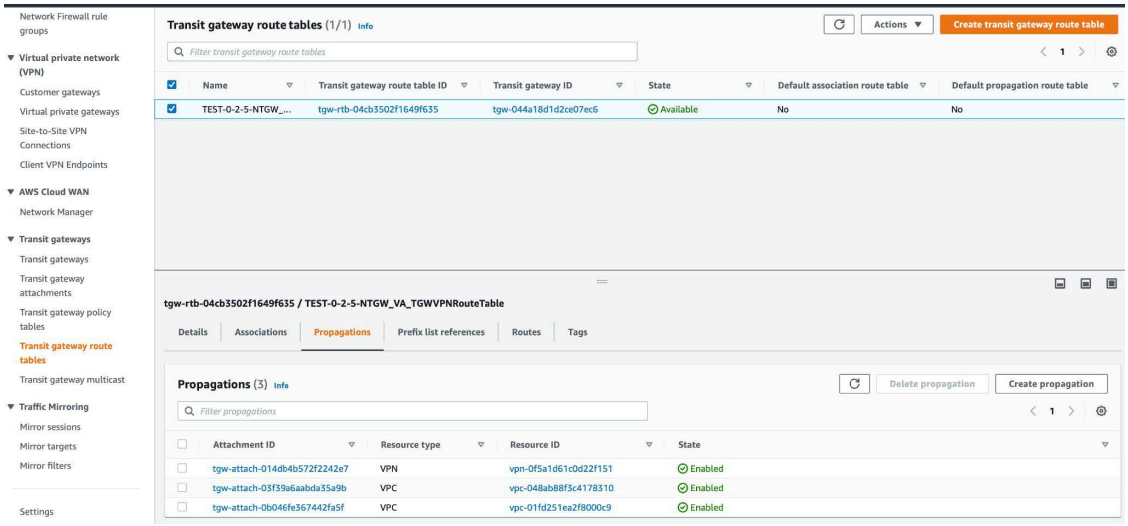
Step 1 From the AWS console, go to **VPC service**.

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 **Associations** tab and then click **Create association**.



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



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 is updated to route the network traffic destined for the CIDR ranges that are allocated to your CGW in your AWS environment.

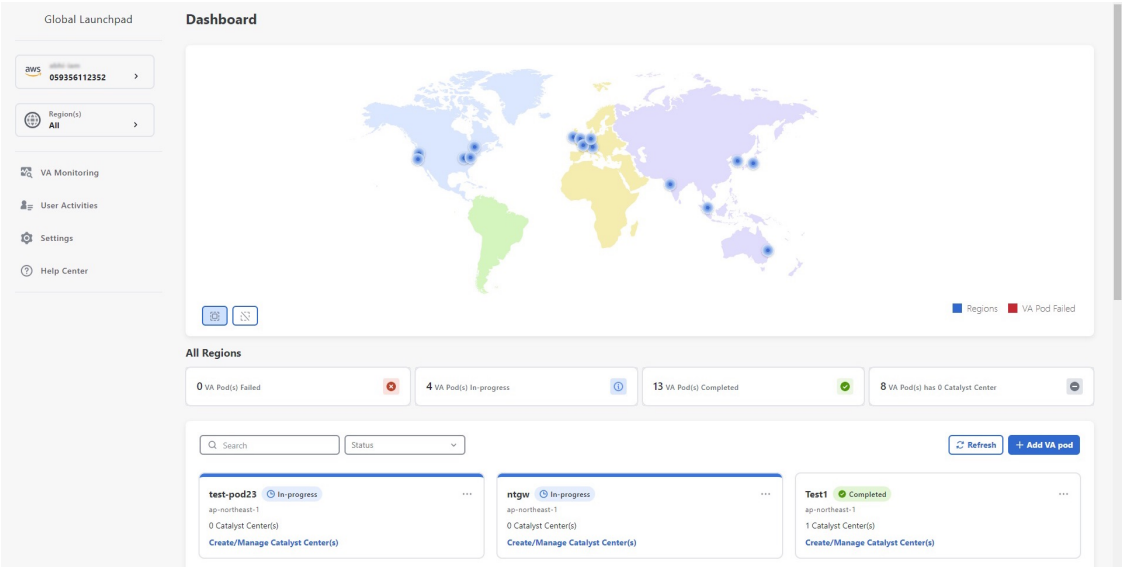
For example: `route tunnel-int-vpn-0b57b508d80a07291-1 10.0.0.0 255.255.0.0 192.168.44.37 200`

Create a New Cisco DNA Center VA

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

Procedure

Step 1 In the **Dashboard** pane, below the map, locate the VA pod where you want to create your Cisco DNA Center VA.



Step 2 In the VA pod card, click **Create/Manage Cisco Catalyst Center(s)**.

Step 3 In the **VA Pod Dashboard** pane, click **+ Create New Cisco Catalyst Center**.

Step 4 Enter the following details:

- **Cisco Catalyst Center Version**: From the drop-down list, choose a Cisco DNA Center version.
- **Enterprise DNS**: Enter the IP address of your Enterprise DNS. Ensure that the Enterprise DNS is reachable from the VA pod in which you're creating the Cisco DNA Center VA.

  Note
  - Cisco Global Launchpad checks the on-premises network connection using UDP port 53 with the DNS server IP address that you entered.
  - The DNS server cannot be updated through Cisco Global Launchpad after deploying Cisco DNA Center on AWS. However, you can update the DNS server using the AWS console. For more information, see Update the DNS Server on a Cisco DNA Center VA Using the AWS Console, on page 39.

- **FQDN (Fully Qualified Domain Name)**: Enter the FQDN for the Cisco DNA Center VA 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 Catalyst 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 server.

Note In Cisco Global Launchpad, Release 1.8.0, if the DNS server, proxy server, or FQDN checks fail, continue with your configuration as follows:

- If the DNS server validation fails, you cannot continue creating your Cisco DNA Center VA. Make sure that the entered DNS server IP address is reachable from the VA pod.
- If the proxy server 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 In the **Summary** window, review the configuration details.

Note The Cisco DNA Center IP address is a statically assigned IP address that is maintained across AWS availability zone outages to ensure uninterrupted connectivity and to minimize disruptions during critical network operations.

Step 7 If you are satisfied with the configuration, click **Generate PEM Key File**.

Step 8 In the **Download PEM Key File** dialog box, click **Download PEM Key File**. If you click **Cancel**, you're returned to the **Summary** window.

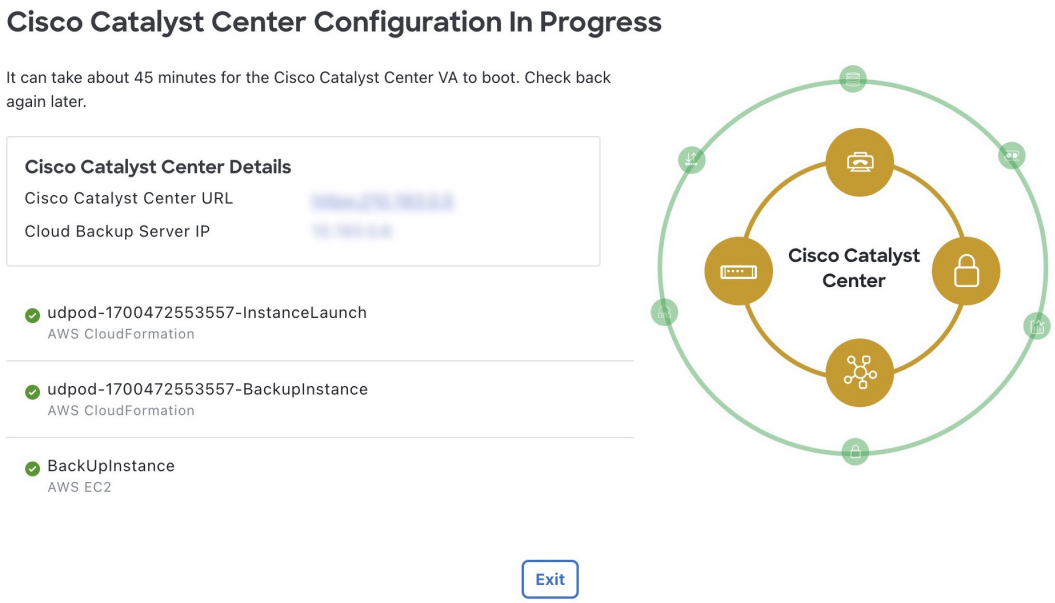
Important Because the PEM key isn't stored in your AWS account, you need to download it. You need the PEM key to access the Cisco DNA Center VA that is being created.

Step 9 After you downloaded the PEM file, click **Start Cisco Catalyst Center Configuration**.

Cisco Global Launchpad configures the Cisco DNA Center environment. After the environment is configured, Cisco DNA Center boots. Initially, Cisco Global 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.

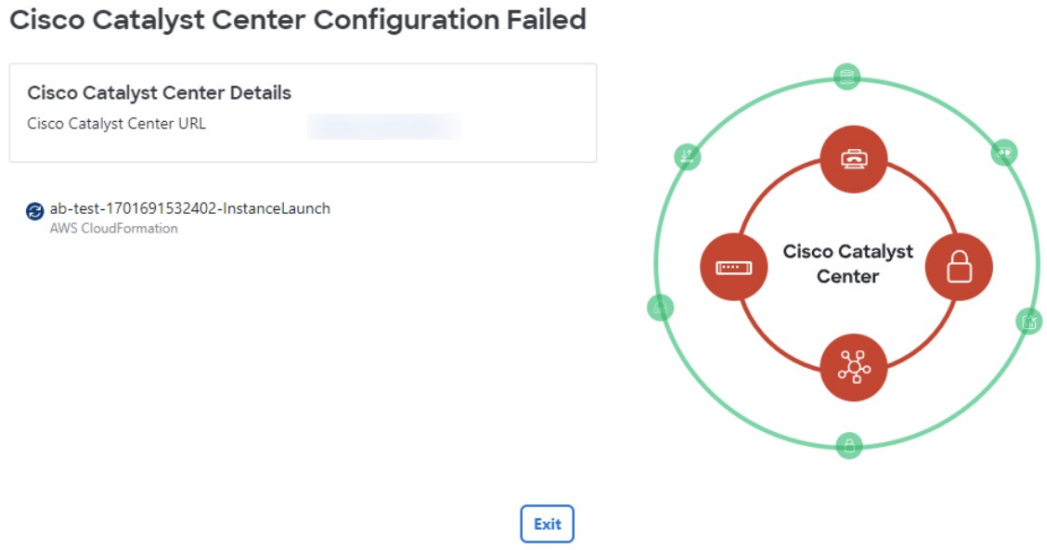
Note This process takes 45-60 minutes. Do not exit the application or close this window or tab. Otherwise, the setup will pause.

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



Tip While the **Cisco Catalyst Center Configuration In Progress** window is displayed, record the backup server's IP address for later use. Your backup server password is a combination of the first four characters of the VA pod name and the backup server's IP address without the periods.

If the Cisco DNA Center configuration fails, exit to the **VA Pod Dashboard** pane. For information, see Troubleshoot Cisco DNA Center VA Configuration Errors, on page 39.



Step 10 To return to the **VA Pod Dashboard** pane, click **Go to Manage Cisco Catalyst Center(s)**.

Troubleshoot the Deployment

Cisco Global 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 We recommend against making manual changes with Cisco Global Launchpad through the AWS console, because it can lead to issues that Cisco Global Launchpad cannot resolve.

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

Troubleshoot Docker Errors

If the error, `port is already in use`, displays while running the Docker images for Cisco Global Launchpad, you can troubleshoot it with the following possible solutions:

Error	Possible Solution
If you receive the following error while running the server application: `port is already in use`	On Docker, run the server application: **`docker run -d -p <server-port-number>:8080 -e SECRET_KEY=<your-secret-key> --name server --pull=always dockerhub.cisco.com/maglev-docker/server:x.x.x-latest`** **Note** You can use any available server port. While running the server application, run the client application: **`docker run -d -p 90:80 -e REACT_APP_API_URL=http://localhost:<client-port-number> --name client --pull=always dockerhub.cisco.com/maglev-docker/client:x.x.x`** **Note** You must use the same port number that you used to run the server application.
If you receive the following error while running the client application: `port is already in use`	On Docker, run the client application: **`docker run -d -p <client-port-name>:80 --name client --pull=always dockerhub.cisco.com/maglev-docker/client:x.x.x`** **Note** You can use any available server port.

Troubleshoot Login Errors

When you log in to Cisco Global Launchpad, you may encounter a login error. You can troubleshoot common login errors with the following possible solutions:

Error	Possible Solution
Invalid credentials.	Reenter your credentials and check that they're entered correctly.
You don't have enough access.	For admin users, verify that your account has administrator access permission. For subusers, verify that your administrator added you to the CiscoDNACenter user group.
An operation to delete is in progress, please try again after some time.	If an admin user deletes the `<AccountId>-cisco-dna-center` global bucket from your 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 Global Launchpad Error

On hosted Cisco Global Launchpad, when you trigger a root cause analysis (RCA) from the **Trigger RCA** pane, the **Rate exceeded** error can occur. If this error occurs, the following message is displayed in the top-right corner of the **Trigger RCA** pane:

```
Rate exceeded.
```

This error message 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 Region Issues

You can troubleshoot region issues with the following possible solutions:

Issue	Possible Solution
While creating a new VA pod in a new region, Cisco Global Launchpad displays an error message or the screen freezes for more than 5 minutes and does not display a configuration-in-progress message.	Make sure that any manual process on the AWS console has completed successfully and try this step again. If the problem persists, contact Cisco TAC. **Note** To avoid such conflicts, we recommend that you don't make any manual changes to the VA pods. Instead, use the Cisco Global Launchpad for all actions.
Your region setup fails and Cisco Global Launchpad displays a **Bucket [name] did not stabilize** error similar to the following: `Bucket 059356112352-cisco-dna-center-eu-south-1.va.storage did not stabilize`	Open a case with AWS and ask that they delete the failed resources from the backend.

Troubleshoot VA Pod Configuration Errors

You can troubleshoot VA pod configuration errors with the following possible solutions:

Error	Possible Solution
+ Create VA Pod button disabled	Hover your cursor over the disabled button to learn more about why it's disabled. The following are likely reasons why you can't create a new VA pod: • **You have reached the limit of VPC service quota**: 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. Note that any VPC used for resources outside of Cisco Global 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 in the selected region. 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. For more information, see the AWS Creating a service quota increase topic in the *AWS Support User Guide* on the AWS website. • **Pod deletion in progress**: 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.
AMI ID for this region is not available for your account.	When you click **+ Create New VA Pod**, Cisco Global Launchpad validates the AMI ID for your selected region. 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.
Your VPN configuration is invalid. At this step you cannot update it so please delete the instance and create a new one.	When configuring a VA pod, the following VPN vendors are not supported: • **Barracuda** • **Sophos** • **Vyatta** • **Zyxel** If you are using an unsupported VPN vendor, the following error message is displayed on the **Configure the On-Premises Tunnel Endpoint** window: `Your VPN configuration is invalid. At this step, you cannot update it, so please delete the instance and create a new one.`
CustomerGateway with type "ipsec.1", ip-address "xx.xx.xx.xx", and bgp-asn "65000" already exists (RequestToken: f78ad45d-b4f8-d02b-9040-f29e5f5f86cf, HandlerErrorCode: AlreadyExists)	You may encounter this error if you try to create more than one VA pod at a time. To resolve this error, delete the failed VA pod and recreate it. Ensure that you create only one VA pod at a time.

Error	Possible Solution
AWS Infrastructure Failed.	If the AWS configuration fails, return to the **Dashboard** pane and create a new VA pod. For more information, see Create a New VA Pod, on page 21. **Note** You can delete the VA pod that failed to configure.
AWS Configuration fails when editing a VA Pod	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 Cisco Global Launchpad for all actions.
Deleting VA Pod has failed	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 Cisco Global Launchpad for all actions.
The resource you are trying to delete has been modified recently. Please refresh the page get the latest changes and try again.	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 tunnel from the VA pod to TWG is green and the tunnel from the TWG to CGW 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 30.

Troubleshoot Cisco DNA Center VA Configuration Errors

You can troubleshoot errors that occur while configuring a Cisco DNA Center VA with the following possible solutions:

Error	Possible Solution
Environment Setup failed	**1.** On Cisco Global Launchpad, return to the **Create/Manage Cisco Catalyst Center(s)** pane. **2.** Delete the Cisco DNA Center VA. **3.** Create a new Cisco DNA Center VA.
Delete Failed	If the Cisco DNA Center VA deletion fails, contact Cisco TAC.

Update the DNS Server on a Cisco DNA Center VA Using the AWS Console

To update the DNS server IP address configured on a Cisco DNA Center VA, use the consent token you obtained from Cisco TAC and follow the steps in this procedure.

Before you begin

Contact Cisco TAC support to get a consent token to be able to get full shell access.

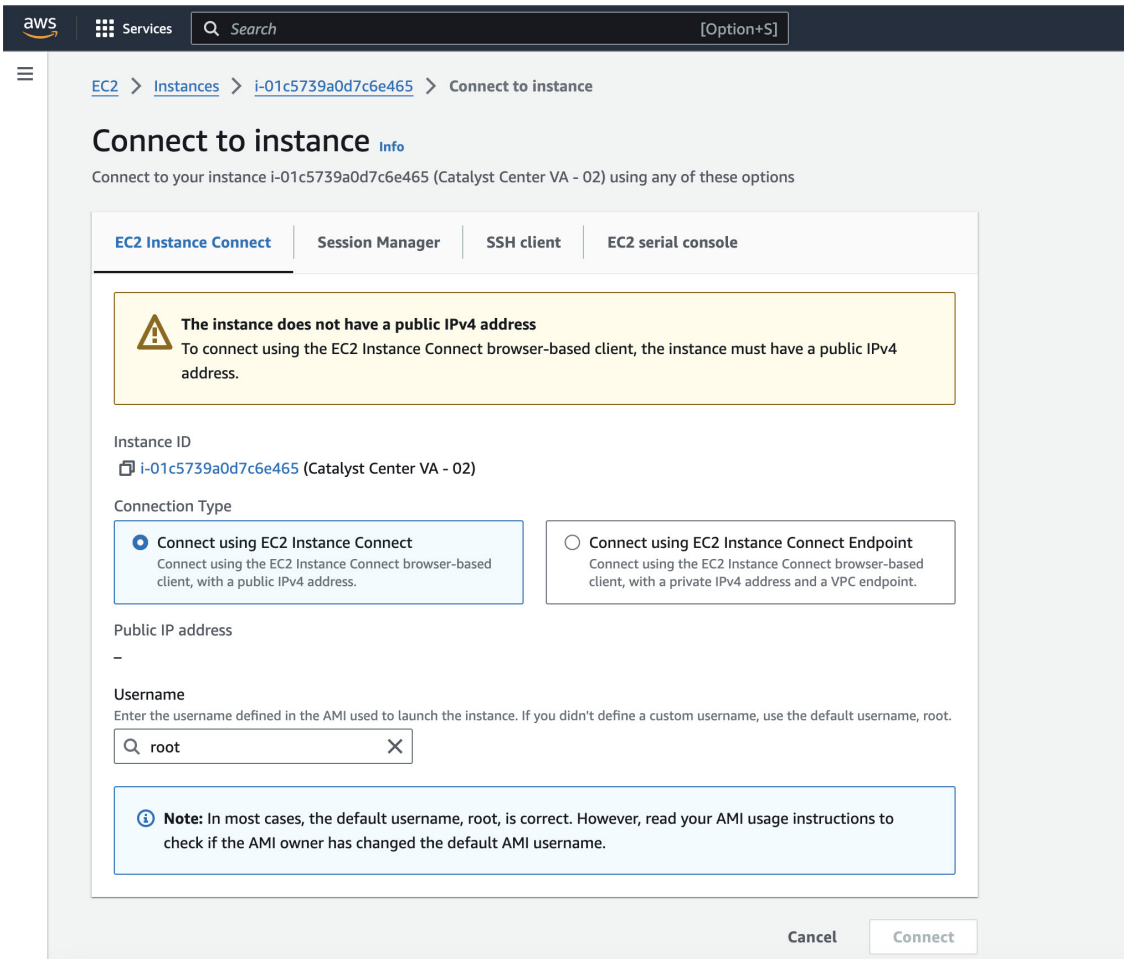
Procedure

Step 1 Log into the AWS console.

Step 2 Select **EC2** > **Instances**.

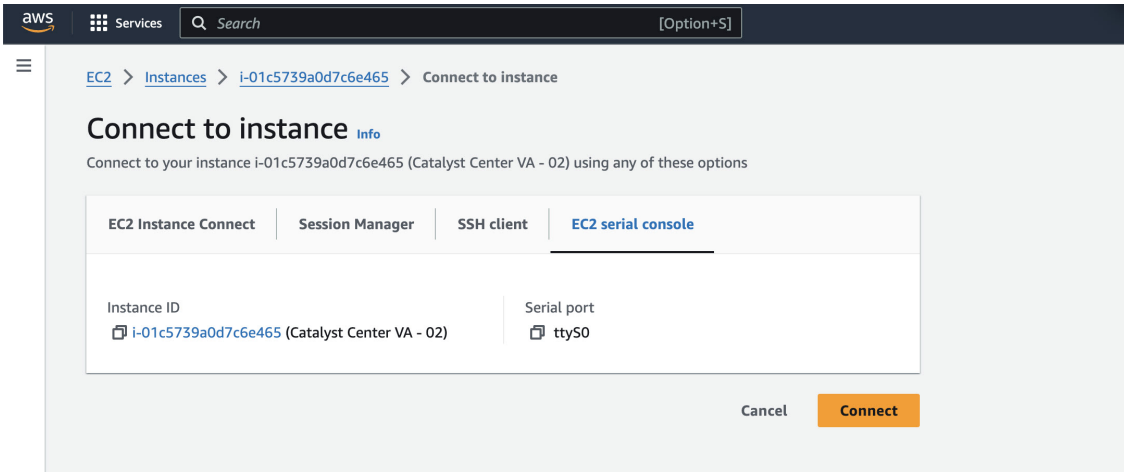
Step 3 Select the instance ID of the Cisco DNA Center you want to change and click **Connect**.

The **Connect to instance** page is displayed with the **EC2 Instance Connect** tab selected by default.



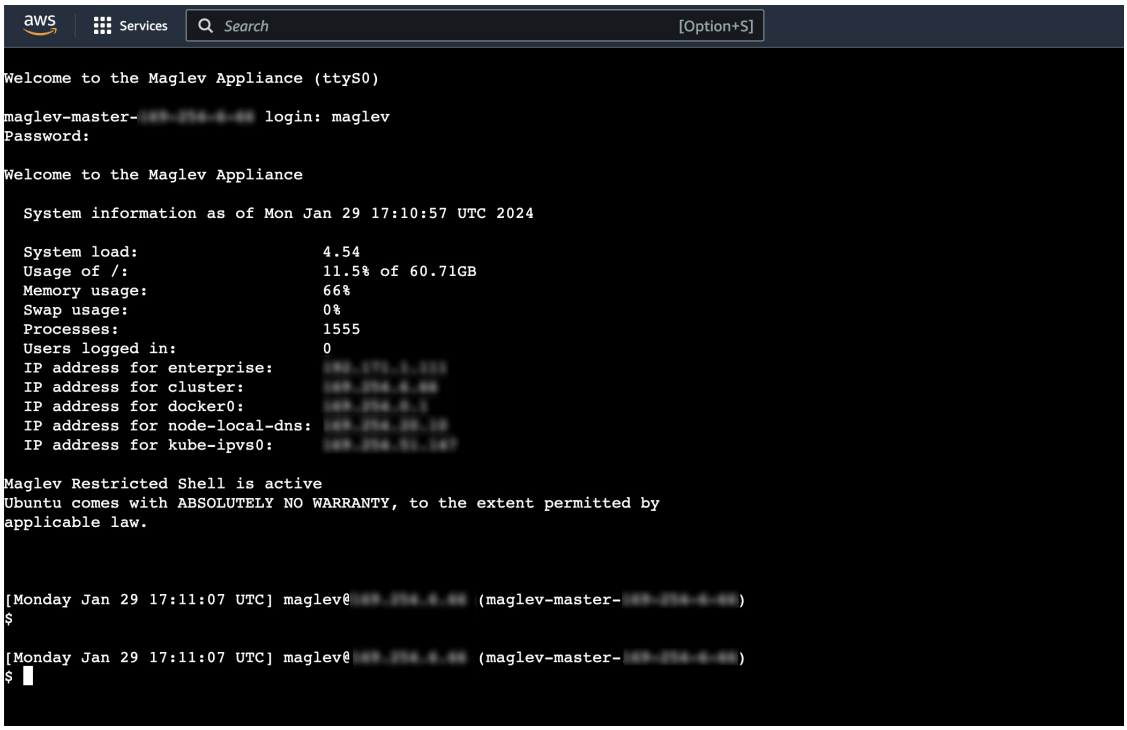
Step 4 Click the **EC2 serial console** tab.

The Cisco DNA Center VA instance ID and serial port are displayed.



Step 5 Click **Connect**.

The Maglev console is displayed.



Step 6 At the **Login** prompt, enter **maglev** as the username.

Step 7 At the **Password** prompt, enter the password that was configured during the initial deployment, regardless of whether you deployed your Cisco DNA Center VA using Cisco Global Launchpad, AWS CloudFormation, or AWS Marketplace.

Step 8 Gain full shell access using the consent token you obtained from Cisco TAC:

```
$ _shell -v _shell -vconsent-token
```

For example:

```
_shell -v _shell  -v n1+hPAAAAQ000AQAAAABAgAEAAAAAAMBYkk2bmhXcW14OGtqUXoy
a09UTXlzM252UnNlUnFwTEFEQVQvejJjQm9kNXloN2thSFk3MzZBek9CMEJRUUZad2QNCkhPNVZMNjhMUXMyb0h
1OXQ2eW1TR01yT1hwZkRPSmNuc1c2QUJ5ZGtVZ0N2OU1mMXZtTC90em1MNldWcVdjY2gNCkh3eEd5MytZWmRVUTN
kek1xOWNiWi9rLzVlTkozQ2RrYy9SMXEya2NOV09uMEdvZE11c1lZN01ENjZvVk5zZlMNCktseHZxTi9tVXF0cW1
vaG9NZFY4SnVOY3NBcXkxQkZOMzZHdS9XQ2N4S2tpdlNUV1VOTVVrRXU1TjVRUDl6d1YNCmYyWW1ZdUFnSGNOcnV
veUhoTzZYYjRIWnJWNDdxSG5qR0REUjV3TE90bnNXalpBL2tsRzNzN0lIa1ZaY0VzMVENCkVoc3FZUGU5Z2ZoTWF
6YXVKRmtxVmc9PQ==
```

Step 9 Set the terminal to display in color:

```
export TERM=xterm
```

Step 10 Run the **sudo-maglev-config** command.

The Configuration wizard presents an abbreviated version of the same series of screens shown in, for example, Configure a Secondary Node Using the Maglev Wizard in the *Cisco DNA Center Second-Generation Appliance Installation Guide*.

When the DNS server IP address setting is displayed, change the DNS server IP address to the preferred one. After you finish making changes on each screen, choose **next>>**, as needed, to proceed through the Configuration wizard.

Step 11 At the end of the configuration process, a message appears, stating that the Configuration wizard is now ready to apply your changes. The following options are available:

- **<<back**: Review and verify your changes.
- **<cancel>**: Discard your changes and exit the Configuration wizard.
- **proceed>>**: Save your changes and begin applying them.

Step 12 To complete the change, choose **proceed>>**. The Configuration wizard applies the changes you made.

At the end of the configuration process, a **CONFIGURATION SUCCEEDED!** message appears.

Troubleshoot Concurrency Errors

You troubleshoot the concurrency errors with the following possible solutions:

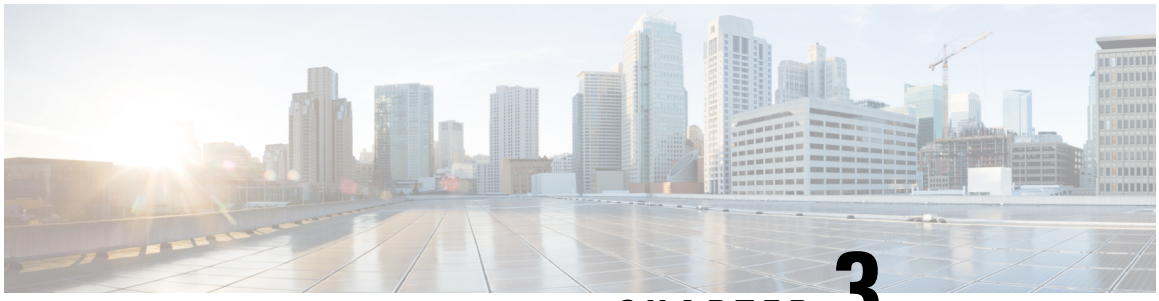
Error	Possible Solution
Unable to delete a Pod or a Cisco DNA Center created by another user.	You cannot delete a component, such as a VA pod or Cisco DNA Center VA, that another user has created while a different action is in progress on the component. After the action completes, you or any other user can delete the component. For example, you cannot delete a VA pod or Cisco DNA Center VA while it is in any of the following processes or states: • Another user is in the process of creating the Cisco DNA Center VA. • Another user is in the process of deleting the Cisco DNA Center VA. • The Cisco DNA Center VA is in a failed state after a deletion attempt.
The status of a Pod has been changed recently.	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. To view the updated status of the VA pod, click **Refresh**.

Troubleshoot Other Deployment Issues

You can troubleshoot other issues that occur while deploying a Catalyst Center VA on AWS with the following possible solutions:

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

Issue	Possible Reasons and Solutions
Failure when deploying multiple VA pods with the same CGW in single region.	Make sure that: • The CGW IP address is the IP address of your Enterprise firewall or router. • The CGW IP address is a valid public address. • The CGW IP address hasn't been used for another VA pod within the same 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.
Unable to SSH or ping the Cisco DNA Center VA.	You cannot connect via SSH or ping the Catalyst 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.
Session ended	If your session times out while operations are in progress, such as triggering an RCA, the operations may abruptly end and display a **Session ended** notification. If your session times out, click **Ok**, log back in, and restart the operations.



CHAPTER 3

Deploy Using Cisco Global Launchpad 1.7

Use Cisco Global Launchpad to Automatically Deploy Cisco DNA Center on AWS

You provide Cisco Global Launchpad with the needed details to create the AWS infrastructure in your AWS account, which includes a VPC, an IPsec VPN tunnel, gateways, subnets, and security groups. As a result, Cisco Global Launchpad deploys the Cisco DNA Center AMI 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 AWS CloudFormation for monitoring, Amazon DynamoDB for state storage, and security groups.

Using Cisco Global Launchpad, you can also access and manage your VAs, as well as manage the user settings. For information, see the *Cisco Global Launchpad 1.7 Administrator Guide*.

Automated Deployment Workflow

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

1. Meet the prerequisites. See Prerequisites for Automated Deployment, on page 46.
2. (Optional) Integrate Cisco ISE on AWS and your 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 Global Launchpad or access Cisco Global Launchpad hosted by Cisco. See Install Cisco Global Launchpad, on page 49 or Access Hosted Cisco Global Launchpad, on page 51.

4. Create a new VA pod to contain your Cisco DNA Center VA instance. See Create a New VA Pod, on page 55.
5. If you're using an existing TGW and existing attachments, such as a VPC, as your preferred on-premises connectivity option, 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 64.
6. Create your new instance of Cisco DNA Center. See Create a New Cisco DNA Center VA, on page 65.
7. (Optional) If necessary, troubleshoot any issues that arise during the deployment. See Troubleshoot the Deployment, on page 69.
8. Manage your Cisco DNA Center VA using Cisco Global Launchpad. See the *Cisco Global Launchpad 1.7 Administrator Guide*.

Prerequisites for Automated Deployment

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

- Install Docker Community Edition (CE) on your platform.

  Cisco Global Launchpad supports Docker CE on Mac, Windows, and Linux platforms. See the documentation on the Docker website for the specific procedure for your platform.

- Regardless of how you access Cisco Global Launchpad to deploy your Cisco DNA Center VA, make sure that your cloud environment meets the following specifications:

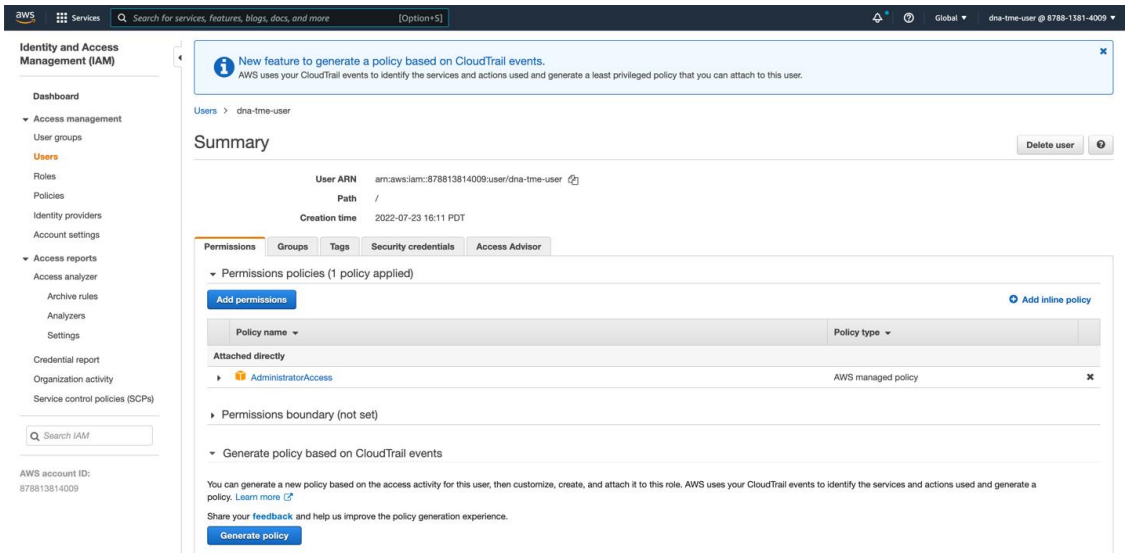
  - **Cisco DNA Center Instance**: r5a.8xlarge, 32 vCPUs, 256-GB RAM, and 4-TB storage

Important 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 in specific availability zones. To view the list of unsupported availability zones, see the *Release Notes for Cisco Global Launchpad 1.7.0*.

  - **Backup Instance**: T3.micro, 2 vCPUs, 500-GB storage, and 1-GB RAM

- You have valid credentials to access your AWS account.
- 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.
- **Important**: Your AWS account is subscribed to Cisco DNA Center Virtual Appliance - Bring Your Own License (BYOL) in AWS Marketplace.
- If you're an admin user, you must have 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.



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

  When an admin user logs in to Cisco Global 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 Global 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 Global Launchpad

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

Before you begin

Make sure you have Docker CE installed on your machine. For information, see Prerequisites for Automated Deployment, on page 46.

Procedure

Step 1 Go to the Cisco Software Download site and download the following files:

- `Launchpad-desktop-client-1.7.0.tar.gz`
- `Launchpad-desktop-server-1.7.0.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-1.7.0.tar.gz

docker load < Launchpad-desktop-server-1.7.0.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. In the files, the **TAG** column should display the numbers starting with **1.7**.

For example:

```
$ docker images

REPOSITORY                                                                TAG                 IMAGE ID            CREATED             SIZE
466518672524.dkr.ecr.us-west-2.amazonaws.com/val/valaunchpad-server       1.7.1               854a1630d3a7        3 hours ago         546MB
466518672524.dkr.ecr.us-west-2.amazonaws.com/platform-ui/valaunchpad-client-docker   1.7.1               63ff53f197c9        5 hours ago         1.98GB
```

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 854a1630d3a7
```

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 63ff53f197c9
```

Note Make sure that the exposed server port number and the REACT_APP_API_URL port number are the same. In Step 5, on page 49 and Step 6, on page 50, 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
ad1b7f7ee6ea   466518672524.dkr.ecr.us-west-2.amazonaws.com/val/valaunchpad-server:1.7.1   "/usr/bin/dumb-init …"   About a minute ago   Up About a minute       0.0.0.0:9494->8080/tcp   server
a6eb2e93f57a   466518672524.dkr.ecr.us-west-2.amazonaws.com/platform-ui/valaunchpad-client-docker:1.7.1   "docker-entrypoint.s…"   2 minutes ago        Up 2 minutes            0.0.0.0:94->80/tcp       client
```

Note If you encounter an issue while running the server or client applications, see Troubleshoot Docker Errors, on page 69.

Step 8 Verify that the server application is accessible by entering the URL in the following format:

http://<localhost>**:**<server-port-number>**/api/valaunchpad/aws/v1/api-docs/**

For example:

http://192.0.2.2:9090/api/valaunchpad/aws/v1/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 Global Launchpad login window is displayed.

Note It can take a few minutes to load the Cisco Global Launchpad login window while the client and server applications load the artifacts.

Access Hosted Cisco Global Launchpad

You can access Cisco Global Launchpad through 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 Global 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 Global Launchpad.

Create a Cisco Account

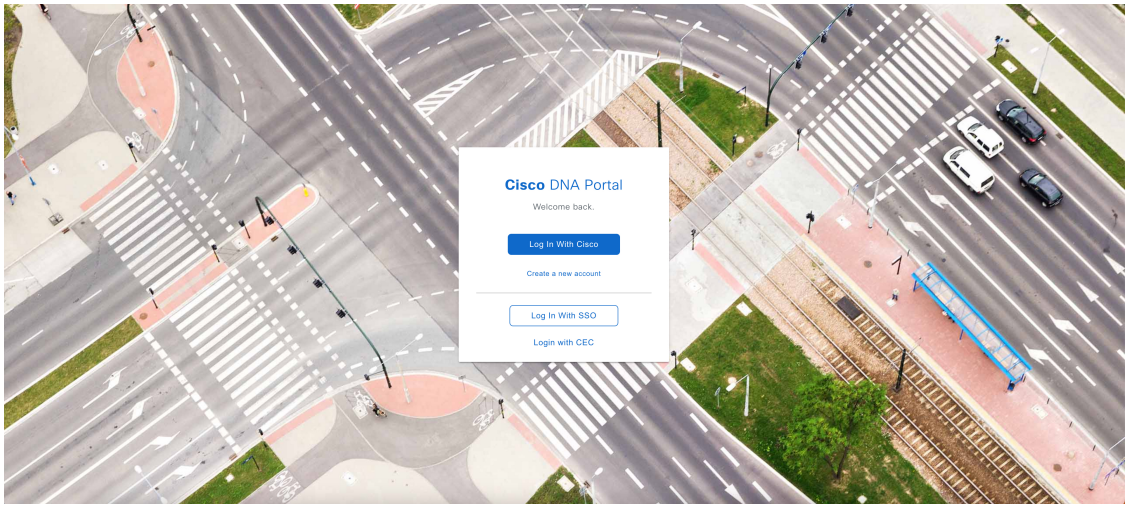
To access Cisco Global Launchpad through Cisco DNA Portal, you must create a Cisco account first.

Procedure

Step 1 In your browser, enter:

`dna.cisco.com`

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

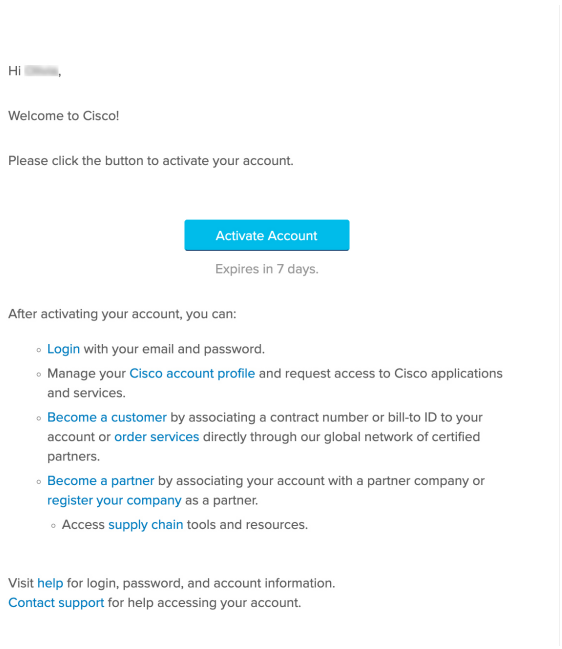


Step 2 Click **Create a new account**.

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**.

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


Hi [redacted],

Welcome to Cisco!

Please click the button to activate your account.

Activate Account

Expires in 7 days.

After activating your account, you can:

- Login with your email and password.
- Manage your Cisco account profile and request access to Cisco applications and services.
- Become a customer by associating a contract number or bill-to ID to your account or order services directly through our global network of certified partners.
- Become a partner by associating your account with a partner company or register your company as a partner.
  - Access supply chain tools and resources.

Visit help for login, password, and account information.
Contact support for help accessing your account.

Create a Cisco DNA Portal Account

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

Before you begin

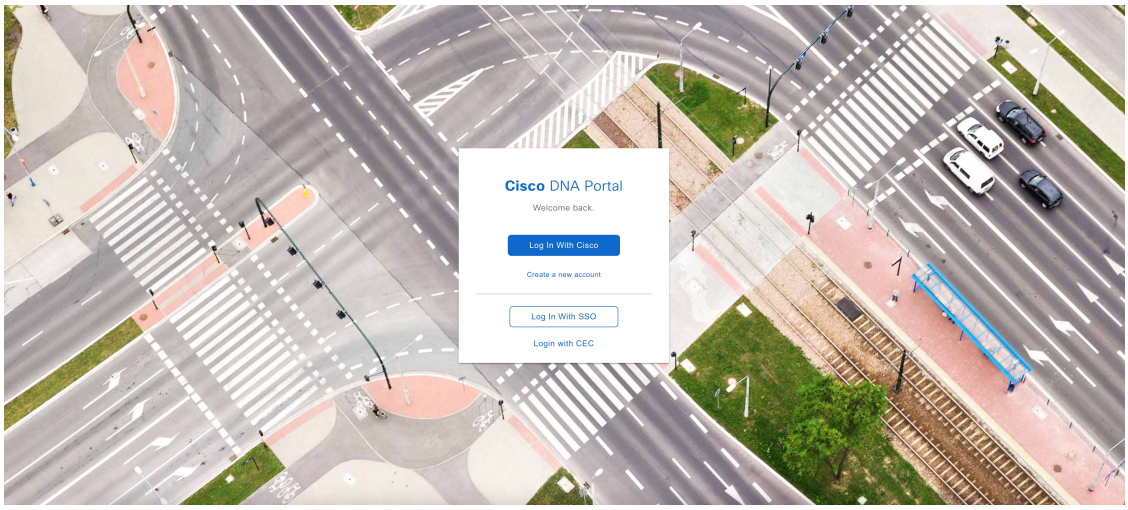
Make sure that you have a Cisco account. For more information, see Create a Cisco Account, on page 51.

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.

Step 5 Click **Log in**.

Step 6 On the **Cisco DNA Portal Welcome** window, enter the name of your organization or team in the **Name your account** field. Then click **Continue**.

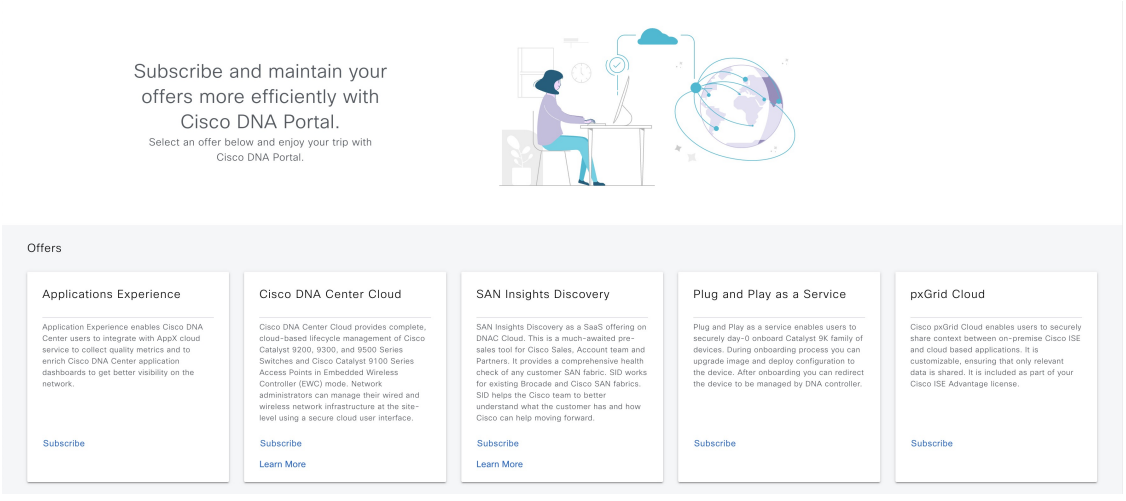
Step 7 On the **Cisco DNA Portal Confirm CCO Profile** window, do the following:

a) Verify the details are correct.

b) After reading, acknowledging, and agreeing with the conditions, check the check box.

c) Click **Create Account**.

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



Log In to the Cisco DNA Portal with Cisco

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

Before you begin

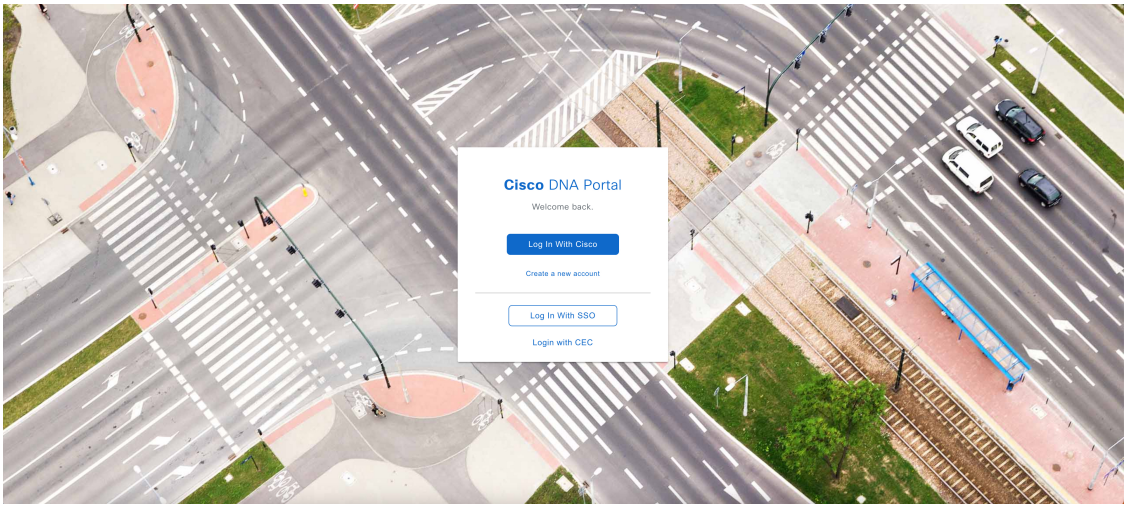
Make sure that you have a Cisco account and a Cisco DNA Portal account. For more information, see Create a Cisco Account, on page 51 and Create a Cisco DNA Portal Account, on page 52.

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**.

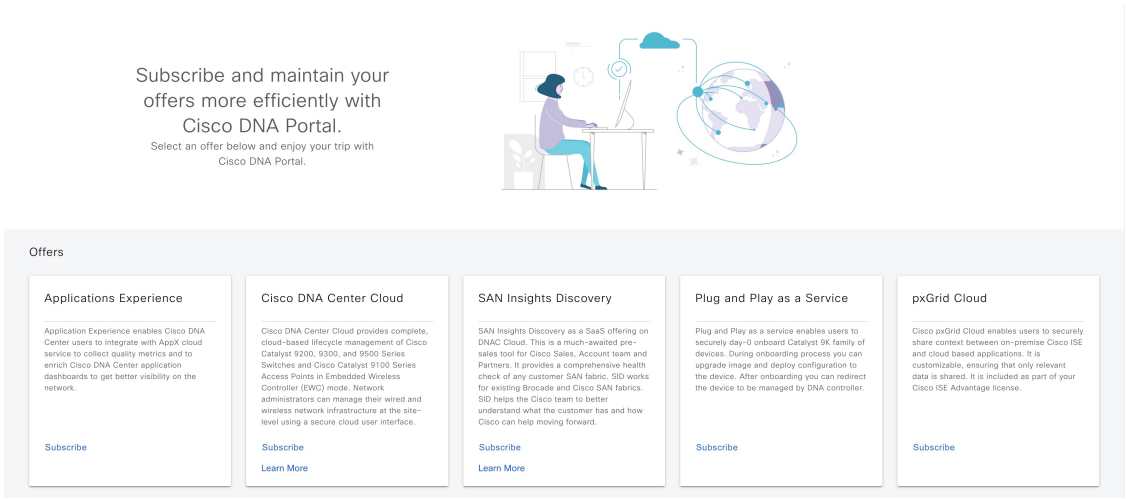
Step 4 Enter your Cisco account's password in the **Password** field.

Step 5 Click **Log in**.

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

Step 6 (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.

Using Cisco Global Launchpad, you can create multiple VA pods—one VA pod for each Cisco DNA Center VA.

Note

- The AWS Super Administrator user can set a limit on the number of VA pods that can be created in each region. The VPCs used for resources outside of Cisco Global Launchpad contribute to this number as well. 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 in the selected region.
- On some steps, all the resources must be set up successfully to proceed to the next step. If all the 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.
- Your VA pod configuration doesn't change when you update Cisco Global Launchpad to a later release, you downgrade to an earlier Cisco Global Launchpad release, or you update the region setup where your VA pod is located.

  For example, if you created a VA pod in Cisco Global Launchpad, Release 1.7.0, the backup password is a combination of the backup instance's stack name and the backup server's IP address. If you access this VA pod in an earlier release, such as Release 1.6.0, the backup password doesn't change.

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 46.

Procedure

Step 1 Log in to Cisco Global Launchpad using one of the following methods:

- **IAM Login**: This method uses user roles to define user access privileges. Cisco Global Launchpad supports multi-factor authentication (MFA) as an optional, additional form of authentication, if your company requires it. For more information, see "Log In to Cisco Global Launchpad Using IAM" in the *Cisco Global Launchpad 1.7 Administrator Guide*.
- **Federated Login**: This method uses one identity to gain access to networks or applications managed by other operators. For more information, see "Generate Federated User Credentials Using saml2aws" or "Generate Federated User Credentials Using AWS CLI" in the *Cisco Global Launchpad 1.7 Administrator Guide*.

For information about how to get an Access Key ID and Secret Access Key, see the AWS Managing access keys topic in the *AWS Identity and Access Management User Guide* on the AWS website.

If you encounter any login errors, you need to resolve them and log in again. For more information, see Troubleshoot Login Errors, on page 70.

Step 2 If you are an admin user logging in for the first time, enter your email address in the **Email ID** field and click **Submit**. If you are a subuser, proceed to Step 3, on page 57.

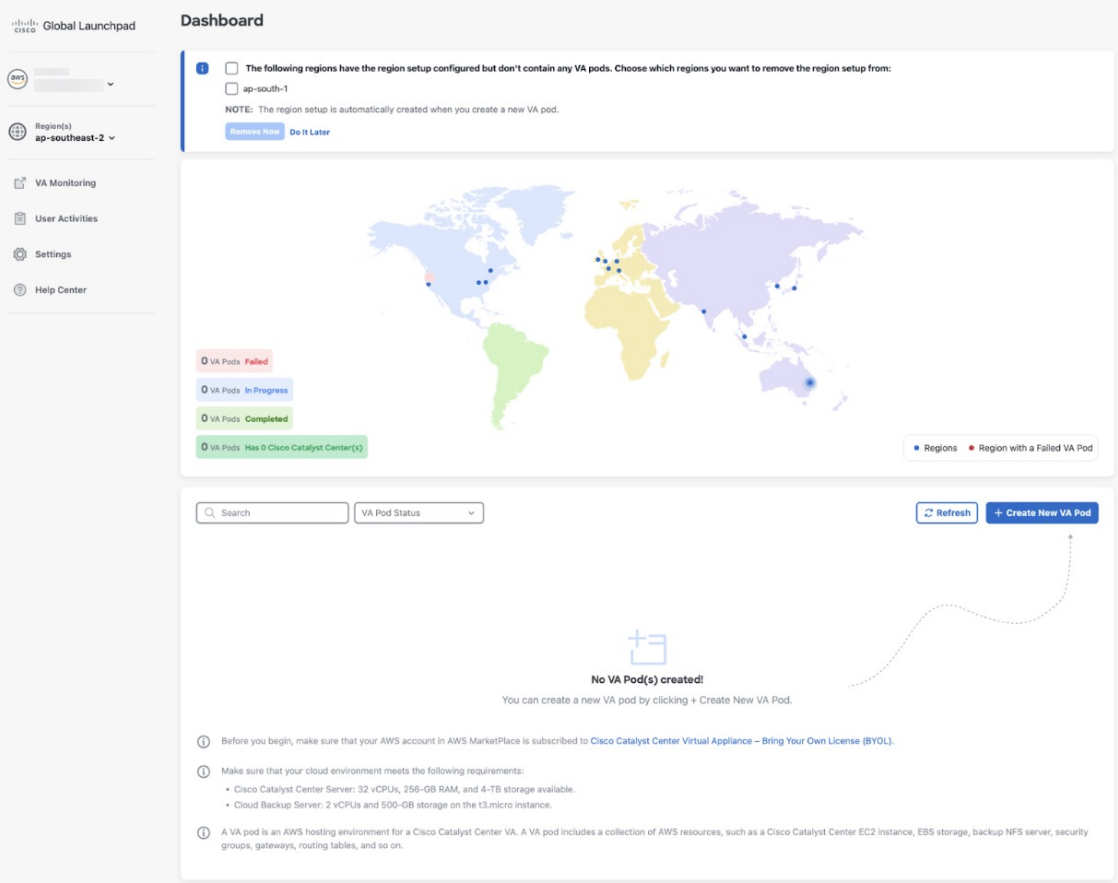
You can subscribe to the Amazon SNS to receive alerts about deployed resources, changes, and resource over-utilization. Further, alarms can be set up to notify you if Amazon CloudWatch detects any unusual behavior in Cisco Global Launchpad. In addition, AWS Config evaluates and assesses your configured resources and sends audit logs of the results as well. For more information, see "Subscribe to the Amazon SNS Email Subscription" and "View Amazon CloudWatch Alarms" in the *Cisco Global Launchpad 1.7 Administrator Guide*.

After you enter your email, several processes happen:

- The CiscoDNACenter user group is created in your 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 Global Launchpad.
- An Amazon 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 Global Launchpad deployment workflow.
- If you are logging in to a region for the first time, Cisco Global 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, the **Dashboard** pane is displayed.

Note If you're prompted to update the region setup, follow the prompts to complete the update. For more information, see "Update a Region Setup" in the *Cisco Global Launchpad 1.7 Administrator Guide*.



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

Step 4 Choose the region where you want to create the new VA pod by completing the following steps in the **Select a Region** dialog box:

a. From the **Region** drop-down list, choose a region.

If you already chose one region from the left navigation pane's **Region** drop-down list, this region is automatically chosen.

Note If you're prompted to update the region setup, follow the prompts to complete the update. For more information, see "Update a Region Setup" in the *Cisco Global Launchpad 1.7 Administrator Guide*.

b. Click **Next**.

Step 5 Configure the AWS infrastructure, which includes the VPC, private subnet, routing table, security group, virtual gateway, and CGW, by completing the following steps:

a) In the **VA Pod Environmental Details** fields, configure the following fields:

- **VA Pod Name**: Assign a name to the new VA pod. Keep the following restrictions in mind:
  - The name must be unique within the region. (This means that you can use the same name across multiple regions.)
  - The name can have a maximum of 12 characters.

- The name can include letters (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 the AWS resources. Keep the following guidelines in mind:
  - The recommended CIDR range is /25.
  - In IPv4 CIDR notation, the last octet (the fourth octet) of the IP address can only have the values 0 or 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 then 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 64.

c) Do one of the following:

- If you selected **Existing TGW** and **Existing Attachments** as your preferred connectivity options, proceed to Step 5.d, on page 59.
- If you selected **VPN GW**, **New VPN GW + New TGW**, or **Existing TGW + New VPN GW**, provide the following VPN details:
  - **CGW (Enterprise Firewall/Router)**: 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 Errors, on page 71.
  - **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:

- **Cisco Catalyst Center Instance**: r5a.8xlarge, 32 vCPU, 256-GB RAM, and 4-TB storage.

  Important 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 in specific availability zones. To view the list of unsupported availability zones, see the *Release Notes for Cisco Global Launchpad 1.7.0*.

- **Backup Instance**: 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 the 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 in AWS.

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

  - **SSH IP Address**: <BACKUP VM IP>
  - **SSH Port**: 22
  - **Server Path**: /var/dnac-backup/
  - **Username**: maglev
  - **Password**: <xxxx##########>

    Your backup server password is dynamically created. The password is composed of the first four characters of the backup instance's stack name and the backup server's IP address without the periods.

    For example, if the backup instance's stack name is DNAC-ABC-0123456789987 and the backup server's IP address is 10.0.0.1, the backup server password is DNAC10001.

    Note
    - You can find the backup instance's stack name either on the **Cisco Catalyst Center Configuration In Progress** window (see Step 9, on page 67 in Create a New Cisco DNA Center VA, on page 65) or on the **AWS Console** > **CloudFormation** > **Stacks** window.
    - You can find the backup server's IP address also on the **Cisco Catalyst Center Configuration In Progress** window (see Step 9, on page 67 in Create a New Cisco DNA Center VA, on page 65) or on the **View Catalyst Center** pane (see "View Catalyst Center VA Details" in the *Cisco Global Launchpad 1.7 Administrator Guide*).

  - **Passphrase**: <Passphrase>

Your passphrase is used to encrypt the security-sensitive components of the backup. These security-sensitive components include certificates and credentials.

This passphrase is required and you will be prompted to enter this passphrase when restoring the backup files. Without this passphrase, backup files are not restored.

- **Open Ports**: 22, 2049, 873, and 111

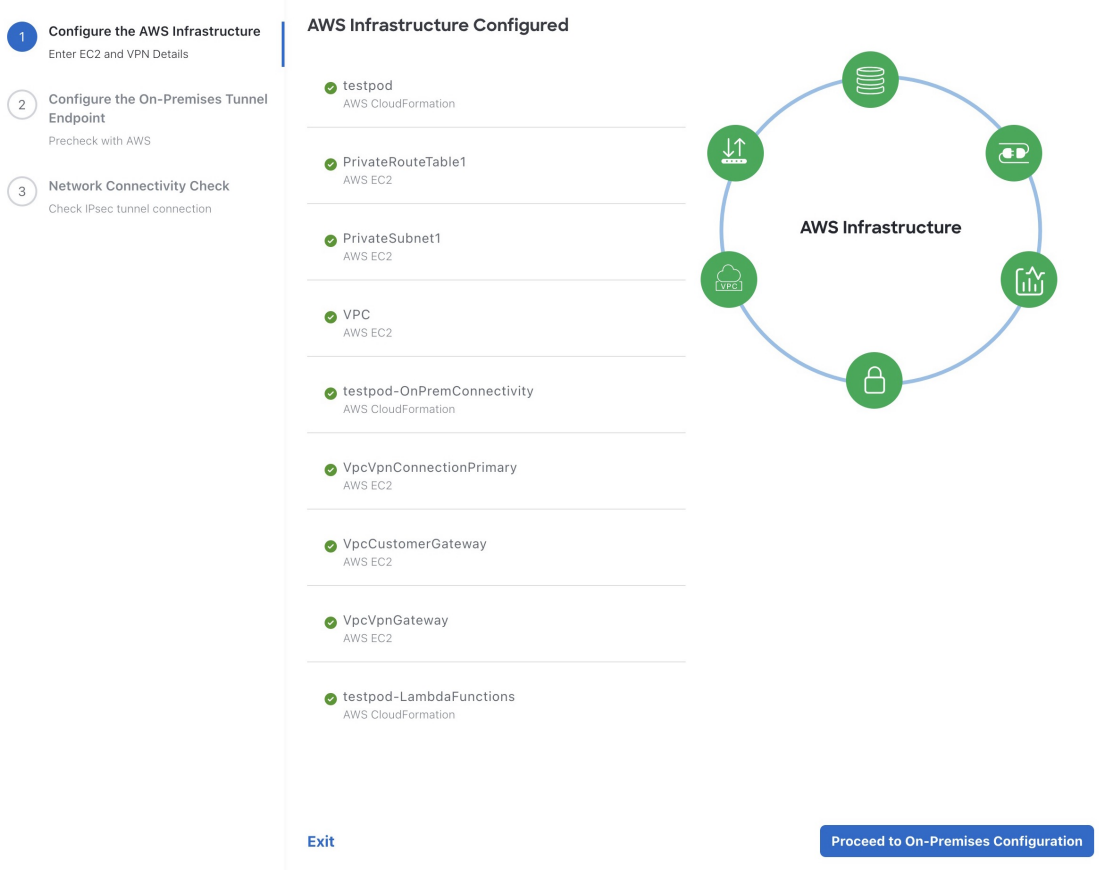
f) Click **Next**.

The **Summary** pane is displayed.

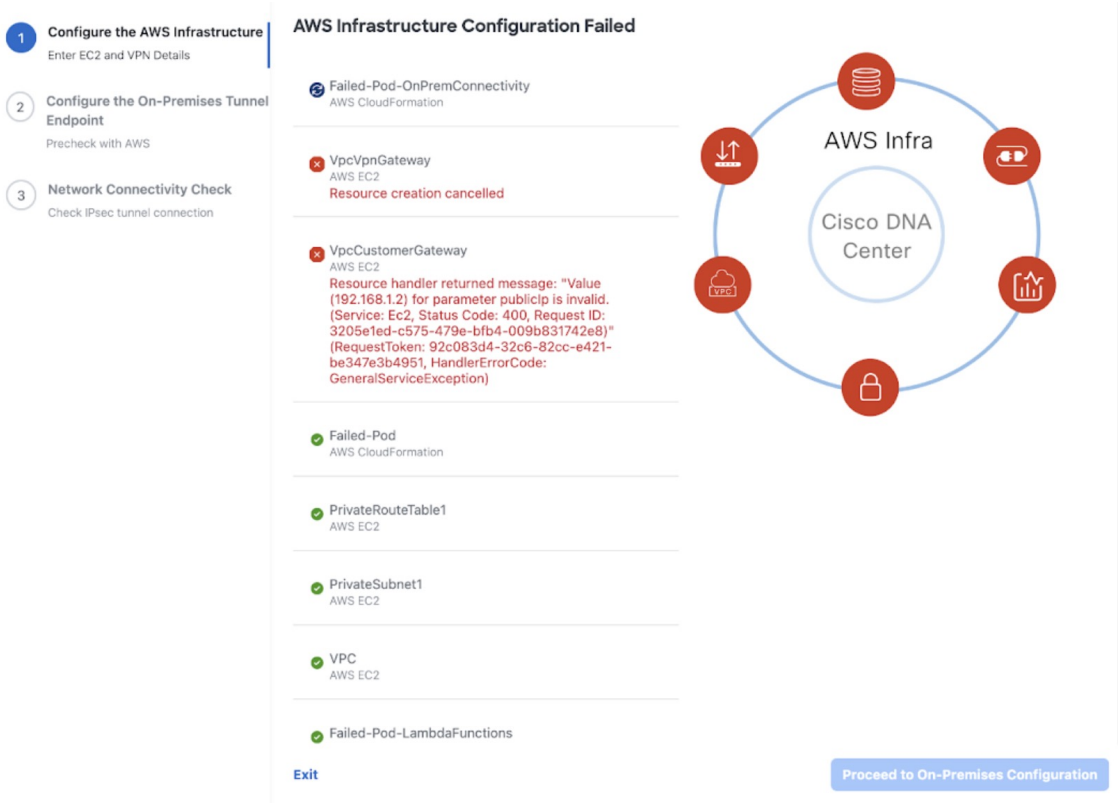
g) Review the environment and VPN details that you entered. If you are satisfied, click **Start Configuring AWS Infrastructure**.

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** pane is displayed.



If the AWS infrastructure configuration fails, exit Cisco Global Launchpad and see Troubleshoot VA Pod Configuration Errors, on page 71 for information about possible causes and solutions.



Step 6 Download the on-premises configuration file by completing the following steps:

a) After the AWS infrastructure is successfully configured, click **Proceed to On-Premises Configuration**.

b) In the **Configure the On-Premises Tunnel Endpoint** pane, 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 the IPsec tunnels.

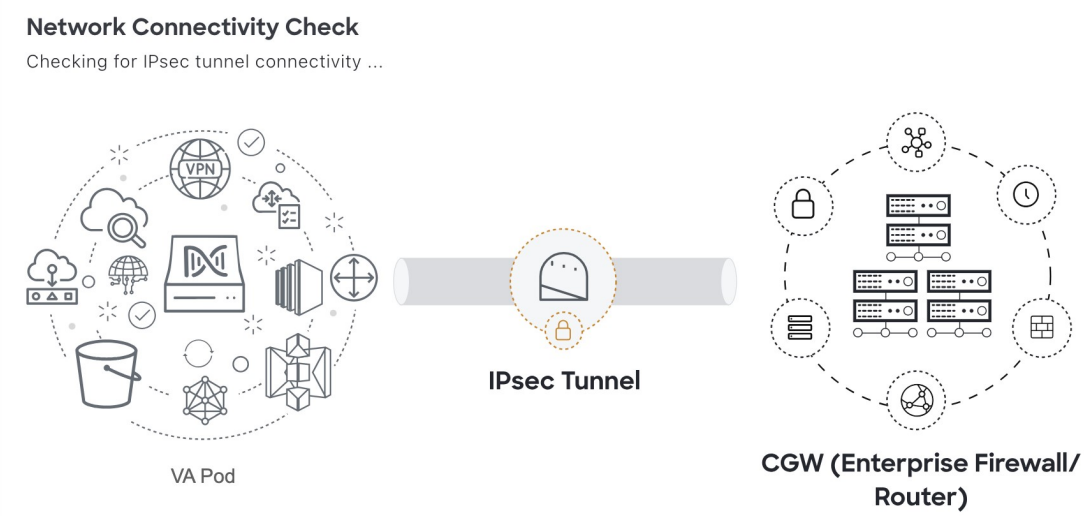
  The provided configuration file enables you to bring up two tunnels between AWS and the Enterprise router or firewall.

- 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.

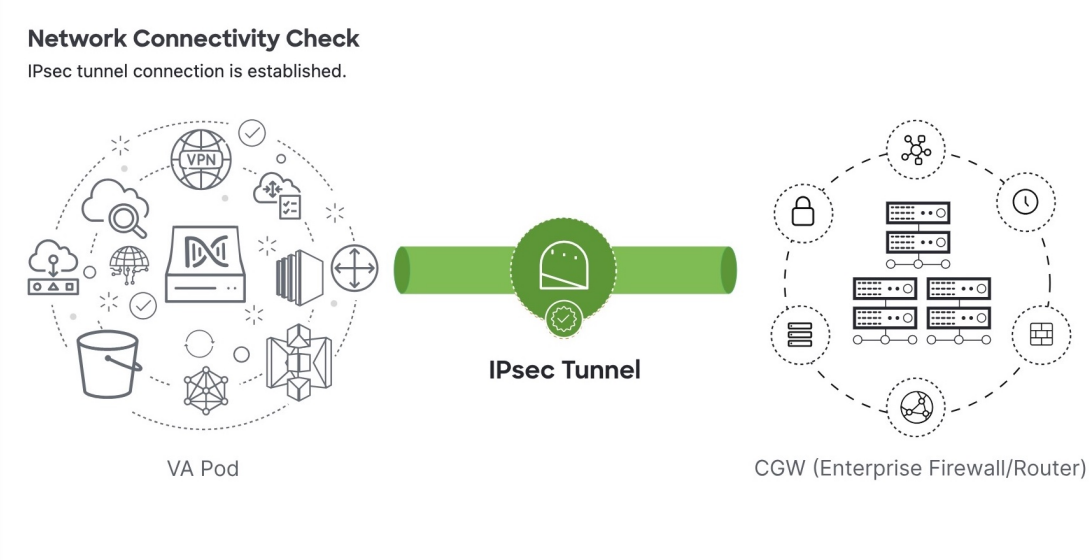
c) Click **Proceed to Network Connectivity Check** button.

Step 7 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:



Note If the IPsec tunnel is up and you cannot access Cisco DNA Center from the CGW, check that the correct values were passed during the IPsec tunnel configuration. Cisco Global Launchpad reports the tunnel status from AWS and doesn't perform additional checks.

- If you selected **New VPN GW + New TGW** or **Existing TGW and New VPN GW** as your preferred on-premises connectivity option, Cisco Global 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 is successfully established, the TGW connection is 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 64.

  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 is successfully established, the TGW connection is green:

Step 8 Click **Go to Dashboard** to return to the **Dashboard** pane, 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 option while creating a new VA pod, Cisco Global Launchpad creates a VPC to launch Cisco DNA Center and attaches this VPC to your existing TGW.

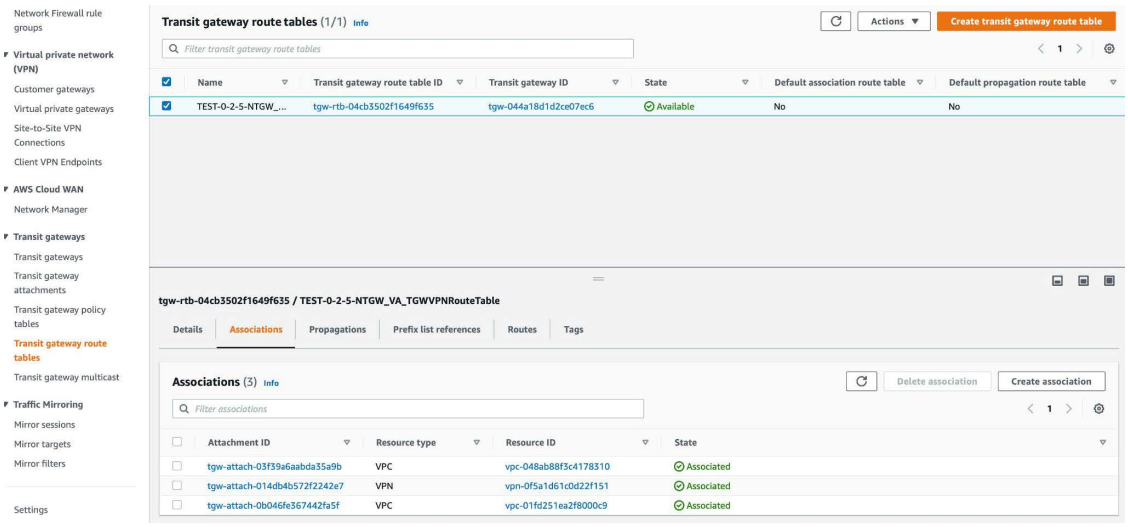
For Cisco Global Launchpad to establish the TGW connection, you must manually configure the TGW routing table on AWS and add the routing configuration to your existing CGW.

Procedure

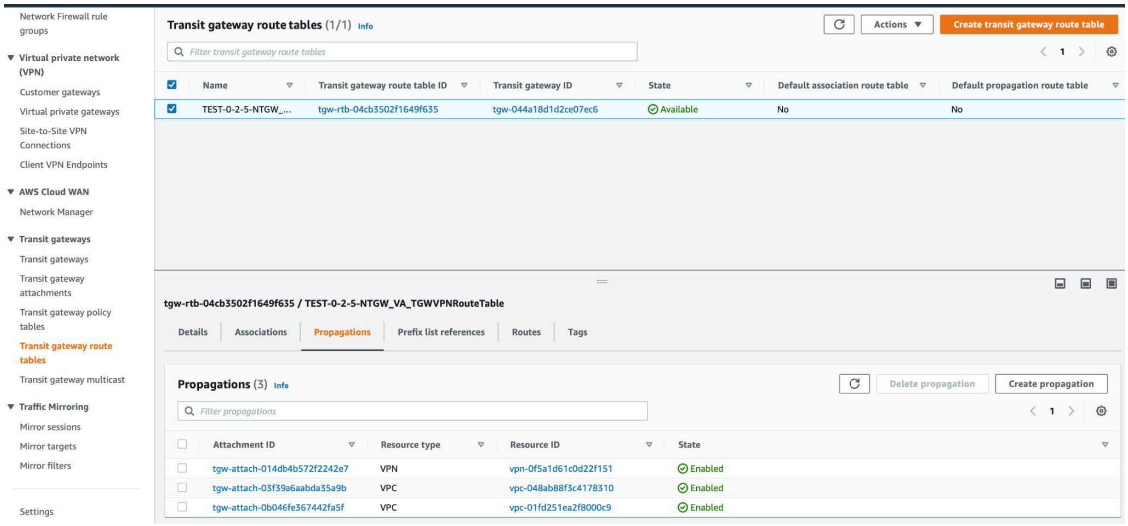
Step 1 From the AWS console, go to **VPC service**.

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 **Associations** tab and then click **Create association**.



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



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 is updated to route the network traffic destined for the CIDR ranges that are allocated to your CGW in your AWS environment.

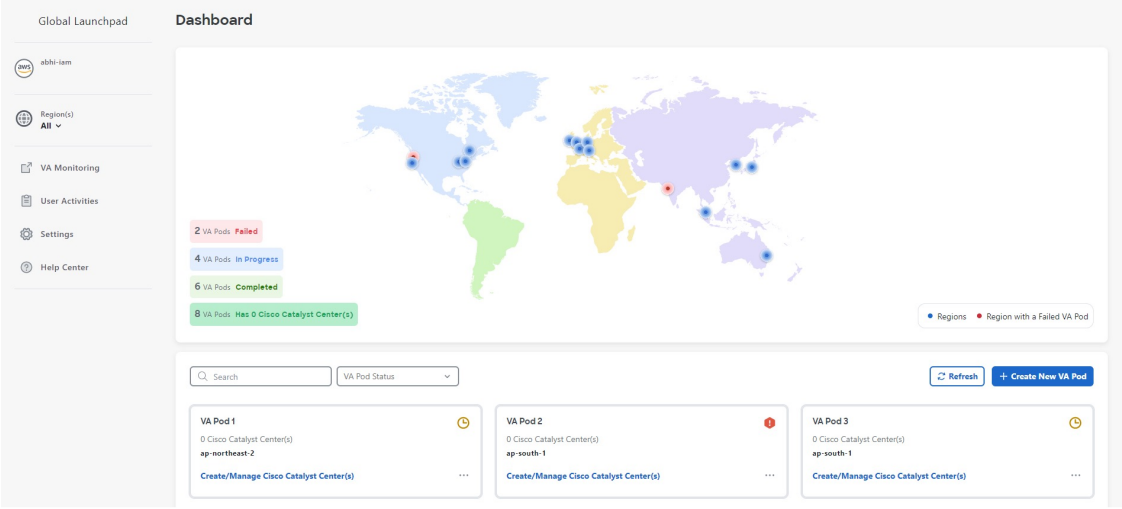
For example: `route tunnel-int-vpn-0b57b508d80a07291-1 10.0.0.0 255.255.0.0 192.168.44.37 200`

Create a New Cisco DNA Center VA

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

Procedure

Step 1 In the **Dashboard** pane, below the map, locate the VA pod where you want to create your Cisco DNA Center VA.



Step 2 In the VA pod card, click **Create/Manage Cisco Catalyst Center(s)**.

Step 3 In the **VA Pod Dashboard** pane, click **+ Create New Cisco Catalyst Center**.

Step 4 Enter the following details:

- **Cisco Catalyst Center Version**: From the drop-down list, choose a Cisco DNA Center version.
- **Enterprise DNS**: Enter the IP address of your Enterprise DNS. Ensure that the Enterprise DNS is reachable from the VA pod in which you're creating the Cisco DNA Center VA.

  Note
  - Cisco Global Launchpad checks the on-premises network connection using UDP port 53 with the DNS server IP address that you entered.
  - The DNS server cannot be updated through Cisco Global Launchpad after deploying Cisco DNA Center on AWS. However, you can update the DNS server using the AWS console. For more information, Update the DNS Server on a Cisco DNA Center VA Using the AWS Console, on page 73.

- **FQDN (Fully Qualified Domain Name)**: Enter the FQDN for the Cisco DNA Center VA 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 Catalyst 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 server.

Note In Cisco Global Launchpad, Release 1.7.0, if the DNS server, proxy server, or FQDN checks fail, continue with your configuration as follows:

- If the DNS server validation fails, you cannot continue creating your Cisco DNA Center VA. Make sure that the entered DNS server IP address is reachable from the VA pod.
- If the proxy server 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 In the **Summary** window, review the configuration details.

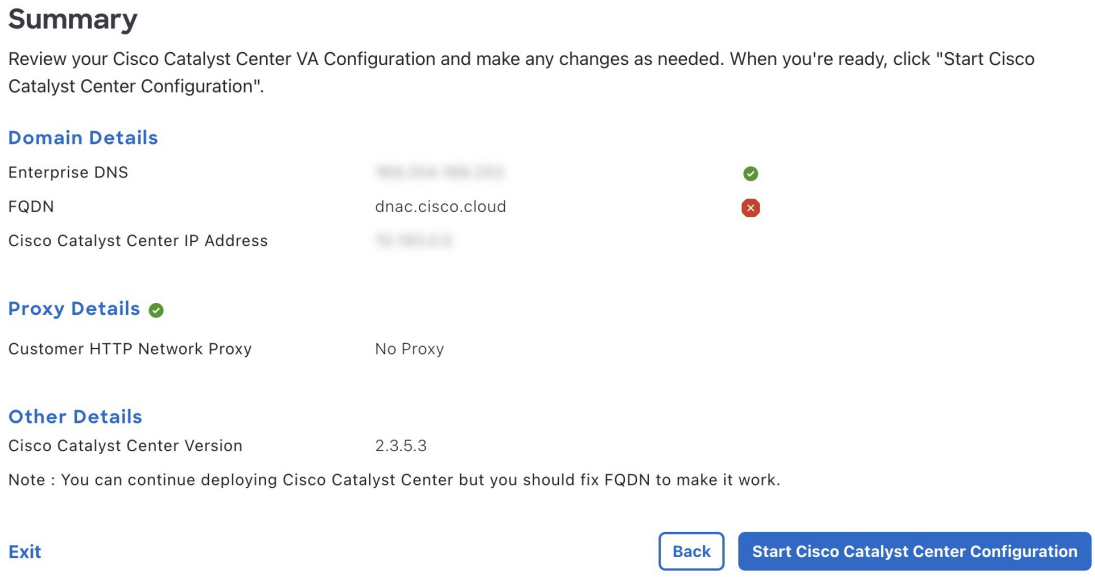
Note The Cisco DNA Center IP address is a statically assigned IP address that is maintained across AWS availability zone outages to ensure uninterrupted connectivity and to minimize disruptions during critical network operations.

Step 7 If you are satisfied with the configuration, click **Generate PEM Key File**.

Step 8 In the **Download PEM Key File** dialog box, click **Download PEM Key File**. If you click **Cancel**, you're returned to the **Summary** window.

Important Because the PEM key isn't stored in your AWS account, you need to download it. You need the PEM key to access the Cisco DNA Center VA that is being created.

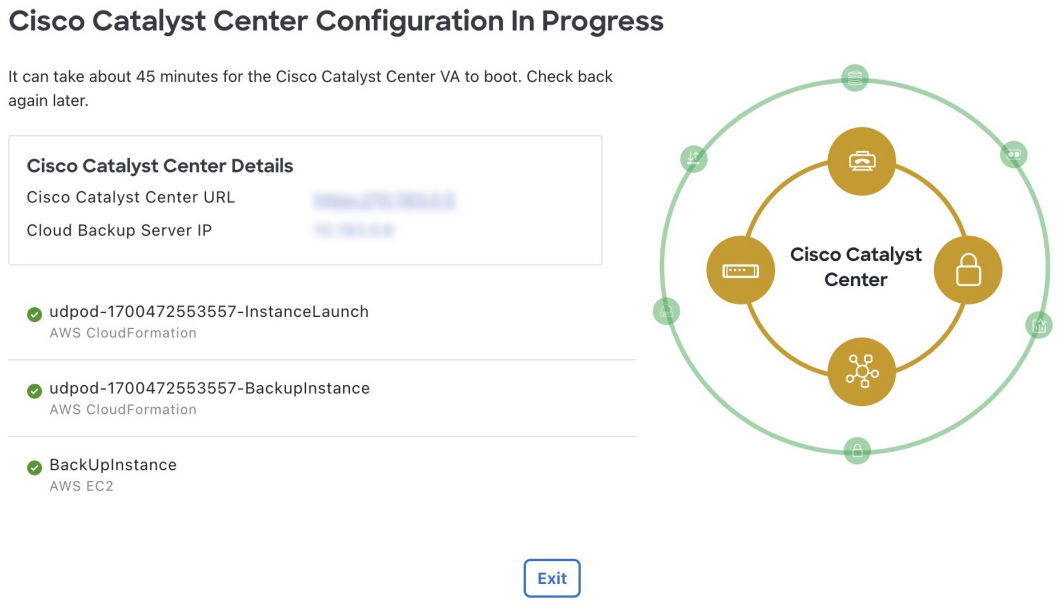
Step 9 After you downloaded the PEM file, click **Start Cisco Catalyst Center Configuration**.



Cisco Global Launchpad configures the Cisco DNA Center environment. After the environment is configured, Cisco DNA Center boots. Initially, Cisco Global 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.

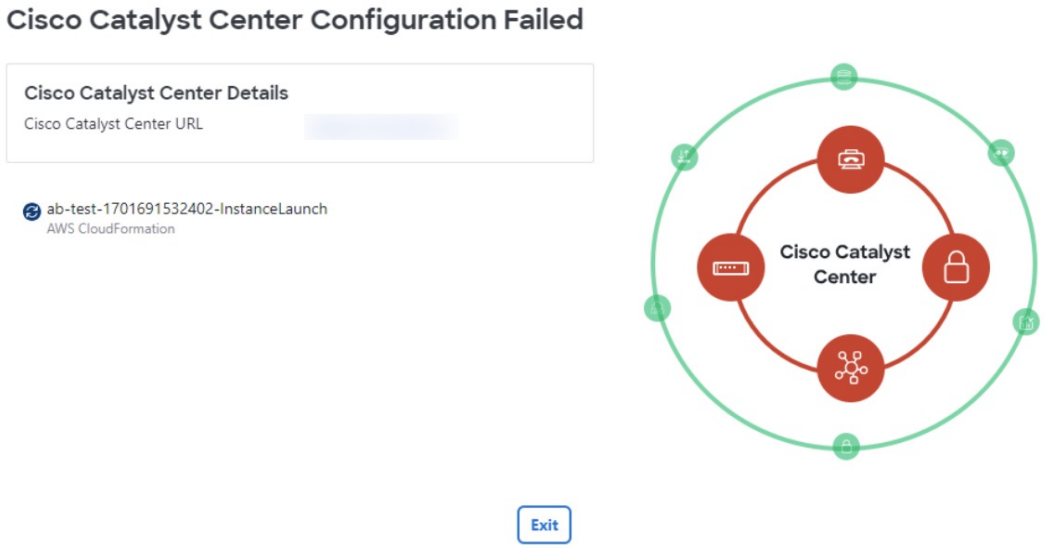
Note This process takes 45-60 minutes. Do not exit the application or close this window or tab. Otherwise, the setup will pause.

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



Tip While the **Cisco Catalyst Center Configuration In Progress** window is displayed, record the backup server's IP address and the backup instance's stack name for later use. Your backup server password is a combination of the first four characters of the backup instance's stack name and the backup server's IP address without the periods.

If the Cisco DNA Center configuration fails, exit to the **VA Pod Dashboard** pane. For information, see Troubleshoot Cisco DNA Center VA Configuration Errors, on page 73.



Step 10 To return to the **VA Pod Dashboard** pane, click **Go to Manage Cisco Catalyst Center(s)**.

Troubleshoot the Deployment

Cisco Global 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 We recommend against making manual changes with Cisco Global Launchpad through the AWS console, because it can lead to issues that Cisco Global Launchpad cannot resolve.

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

Troubleshoot Docker Errors

If the error, `port is already in use`, displays while running the Docker images for Cisco Global Launchpad, you can troubleshoot it with the following possible solutions:

Error	Possible Solution
If you receive the following error while running the server application: `port is already in use`	On Docker, run the server application: **`docker run -d -p <server-port-number>:8080 -e SECRET_KEY=<your-secret-key> --name server --pull=always dockerhub.cisco.com/maglev-docker/server:x.x.x-latest`** **Note** You can use any available server port. While running the server application, run the client application: **`docker run -d -p 90:80 -e REACT_APP_API_URL=http://localhost:<client-port-number> --name client --pull=always dockerhub.cisco.com/maglev-docker/client:x.x.x`** **Note** You must use the same port number that you used to run the server application.
If you receive the following error while running the client application: `port is already in use`	On Docker, run the client application: **`docker run -d -p <client-port-name>:80 --name client --pull=always dockerhub.cisco.com/maglev-docker/client:x.x.x`** **Note** You can use any available server port.

Troubleshoot Login Errors

When you log in to Cisco Global Launchpad, you may encounter a login error. You can troubleshoot common login errors with the following possible solutions:

Error	Possible Solution
Invalid credentials.	Reenter your credentials and check that they're entered correctly.
You don't have enough access.	For admin users, verify that your account has administrator access permission. For subusers, verify that your administrator added you to the CiscoDNACenter user group.
An operation to delete is in progress, please try again after some time.	If an admin user deletes the `<AccountId>-cisco-dna-center` global bucket from your 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 Global Launchpad Error

On hosted Cisco Global Launchpad, when you trigger a root cause analysis (RCA) from the **Trigger RCA** pane, the **Rate exceeded** error can occur. If this error occurs, the following message is displayed in the top-right corner of the **Trigger RCA** pane:

```
Rate exceeded.
```

This error message 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 Region Issues

You can troubleshoot region issues with the following possible solutions:

Issue	Possible Solution
While creating a new VA pod in a new region, Cisco Global Launchpad displays an error message or the screen freezes for more than 5 minutes and does not display a configuration-in-progress message.	Make sure that any manual process on the AWS console has completed successfully and try this step again. If the problem persists, contact Cisco TAC. **Note** To avoid such conflicts, we recommend that you don't make any manual changes to the VA pods. Instead, use the Cisco Global Launchpad for all actions.
Your region setup fails and Cisco Global Launchpad displays a **Bucket [name] did not stabilize** error similar to the following: `Bucket 059356112352-cisco-dna-center-eu-south-1.va.storage did not stabilize`	Open a case with AWS and ask that they delete the failed resources from the backend.

Troubleshoot VA Pod Configuration Errors

You can troubleshoot VA pod configuration errors with the following possible solutions:

Error	Possible Solution
+ Create VA Pod button disabled	Hover your cursor over the disabled button to learn more about why it's disabled. The following are likely reasons why you can't create a new VA pod: • **You have reached the limit of VPC service quota**: 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. Note that any VPC used for resources outside of Cisco Global 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 in the selected region. 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. For more information, see the AWS Creating a service quota increase topic in the *AWS Support User Guide* on the AWS website. • **Pod deletion in progress**: 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.

Error	Possible Solution
AMI ID for this region is not available for your account.	When you click **+ Create New VA Pod**, Cisco Global Launchpad validates the AMI ID for your selected region. 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.
Your VPN configuration is invalid. At this step you cannot update it so please delete the instance and create a new one.	When configuring a VA pod, the following VPN vendors are not supported: • **Barracuda** • **Sophos** • **Vyatta** • **Zyxel** If you are using an unsupported VPN vendor, the following error message is displayed on the **Configure the On-Premises Tunnel Endpoint** window: `Your VPN configuration is invalid. At this step, you cannot update it, so please delete the instance and create a new one.`
CustomerGateway with type "ipsec.1", ip-address "xx.xx.xx.xx", and bgp-asn "65000" already exists (RequestToken: f78ad45d-b4f8-d02b-9040-f29e5f5f86cf, HandlerErrorCode: AlreadyExists)	You may encounter this error if you try to create more than one VA pod at a time. To resolve this error, delete the failed VA pod and recreate it. Ensure that you create only one VA pod at a time.
AWS Infrastructure Failed.	If the AWS configuration fails, return to the **Dashboard** pane and create a new VA pod. For more information, see Create a New VA Pod, on page 55. **Note** You can delete the VA pod that failed to configure.
AWS Configuration fails when editing a VA Pod	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 Cisco Global Launchpad for all actions.
Deleting VA Pod has failed	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 Cisco Global Launchpad for all actions.
The resource you are trying to delete has been modified recently. Please refresh the page get the latest changes and try again.	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 tunnel from the VA pod to TWG is green and the tunnel from the TWG to CGW 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 64.

Troubleshoot Cisco DNA Center VA Configuration Errors

You can troubleshoot errors that occur while configuring a Cisco DNA Center VA with the following possible solutions:

Error	Possible Solution
Environment Setup failed	**1.** On Cisco Global Launchpad, return to the **Create/Manage Cisco Catalyst Center(s)** pane. **2.** Delete the Cisco DNA Center VA. **3.** Create a new Cisco DNA Center VA.
Delete Failed	If the Cisco DNA Center VA deletion fails, contact Cisco TAC.

Update the DNS Server on a Cisco DNA Center VA Using the AWS Console

To update the DNS server IP address configured on a Cisco DNA Center VA, use the consent token you obtained from Cisco TAC and follow the steps in this procedure.

Before you begin

Contact Cisco TAC support to get a consent token to be able to get full shell access.

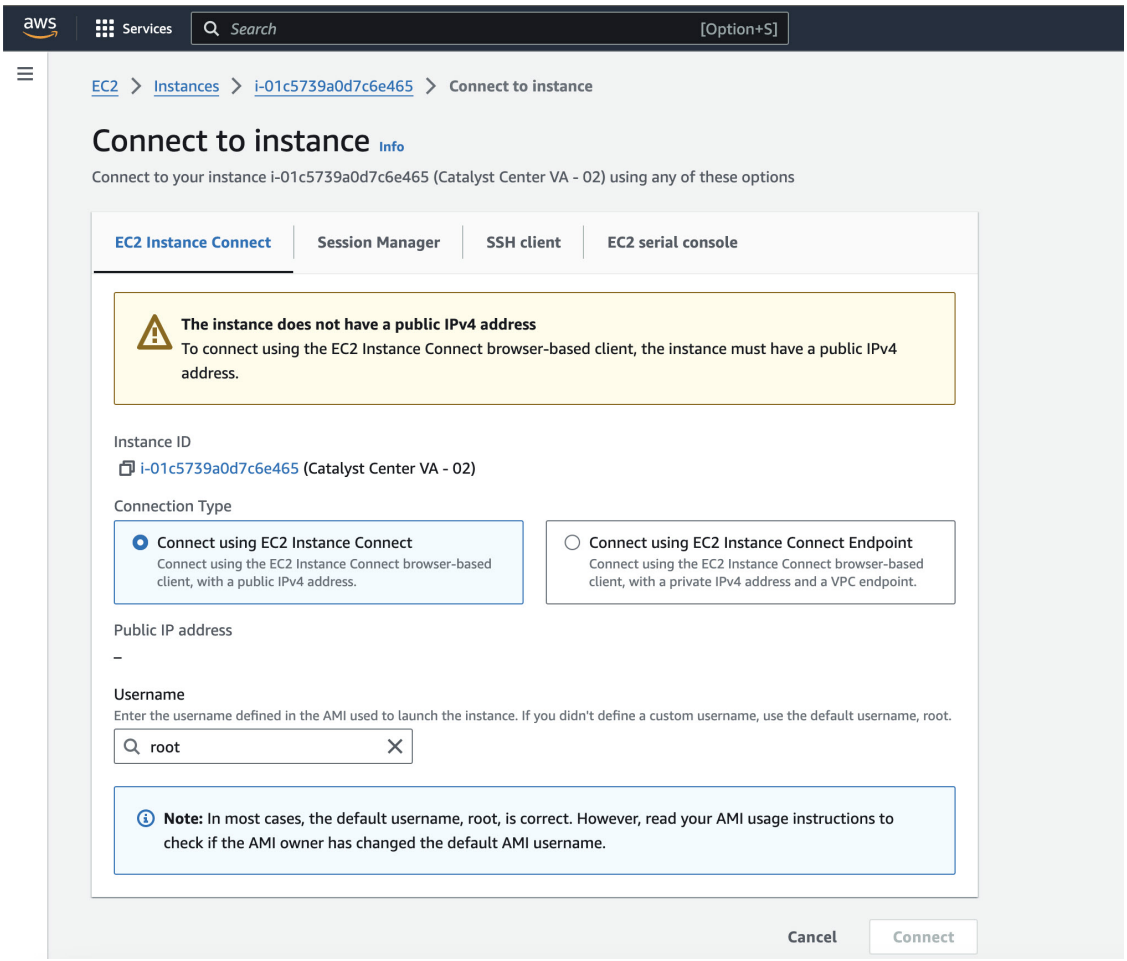
Procedure

Step 1 Log into the AWS console.

Step 2 Select **EC2** > **Instances**.

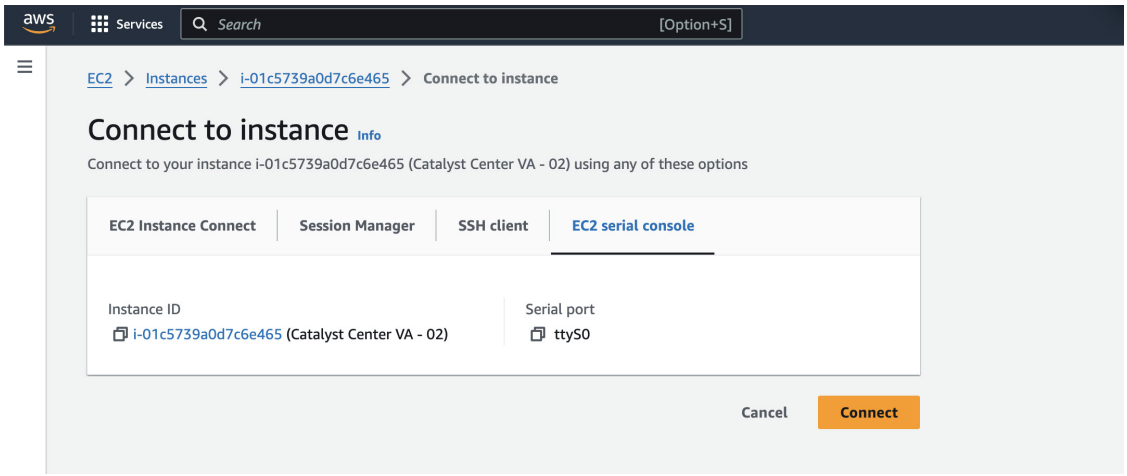
Step 3 Select the instance ID of the Cisco DNA Center you want to change and click **Connect**.

The **Connect to instance** page is displayed with the **EC2 Instance Connect** tab selected by default.



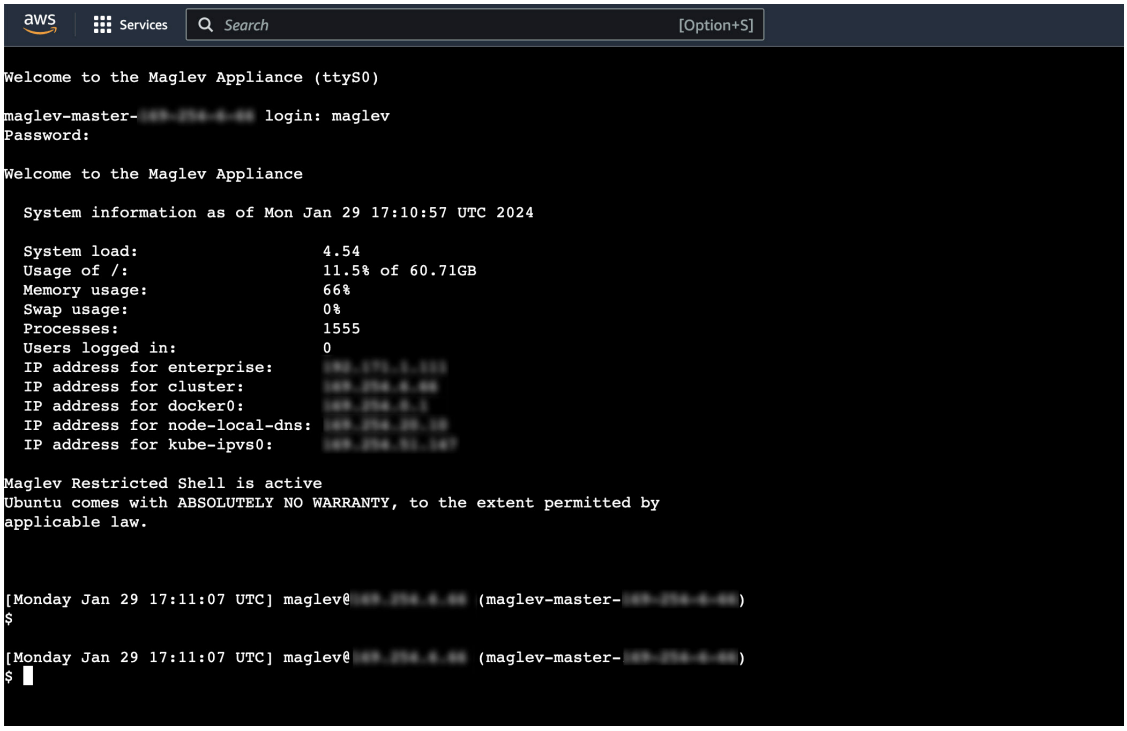
Step 4 Click the **EC2 serial console** tab.

The Cisco DNA Center VA instance ID and serial port are displayed.



Step 5 Click **Connect**.

The Maglev console is displayed.



Step 6 At the **Login** prompt, enter **maglev** as the username.

Step 7 At the **Password** prompt, enter the password that was configured during the initial deployment, regardless of whether you deployed your Cisco DNA Center VA using Cisco Global Launchpad, AWS CloudFormation, or AWS Marketplace.

Step 8 Gain full shell access using the consent token you obtained from Cisco TAC:

```
$ _shell -v _shell -vconsent-token
```

For example:

```
_shell -v _shell  -v n1+hPAAAAQ000AQAAAABAgAEAAAAAAMBYkk2bmhXcW14OGtqUXoy
a09UTXlzM252UnNlUnFwTEFEQVQvejJjQm9kNXloN2thSFk3MzZBek9CMEJRUUZad2QNCkhPNVZMNjhMUXMyb0h
1OXQ2eW1TR01yT1hwZkRPSmNuc1c2QUJ5ZGtVZ0N2OU1mMXZtTC90em1MNldWcVdjY2gNCkh3eEd5MytZWmRVUTN
kek1xOWNiWi9rLzVlTkozQ2RrYy9SMXEya2NOV09uMEdvZE11c1lZN01ENjZvVk5zZlMNCktseHZxTi9tVXF0cW1
vaG9NZFY4SnVOY3NBcXkxQkZOMzZHdS9XQ2N4S2tpdlNUV1VOTVVrRXU1TjVRUDl6d1YNCmYyWW1ZdUFnSGNOcnV
veUhoTzZYYjRIWnJWNDdxSG5qR0REUjV3TE90bnNXalpBL2tsRzNzN0lIa1ZaY0VzMVENCkVoc3FZUGU5Z2ZoTWF
6YXVKRmtxVmc9PQ==
```

Step 9 Set the terminal to display in color:

```
export TERM=xterm
```

Step 10 Run the **sudo-maglev-config** command.

The Configuration wizard presents an abbreviated version of the same series of screens shown in, for example, Configure a Secondary Node Using the Maglev Wizard in the *Cisco DNA Center Second-Generation Appliance Installation Guide*.

When the DNS server IP address setting is displayed, change the DNS server IP address to the preferred one. After you finish making changes on each screen, choose **next>>**, as needed, to proceed through the Configuration wizard.

Step 11 At the end of the configuration process, a message appears, stating that the Configuration wizard is now ready to apply your changes. The following options are available:

- **<<back**: Review and verify your changes.
- **<cancel>**: Discard your changes and exit the Configuration wizard.
- **proceed>>**: Save your changes and begin applying them.

Step 12 To complete the change, choose **proceed>>**. The Configuration wizard applies the changes you made.

At the end of the configuration process, a **CONFIGURATION SUCCEEDED!** message appears.

Troubleshoot Concurrency Errors

You troubleshoot the concurrency errors with the following possible solutions:

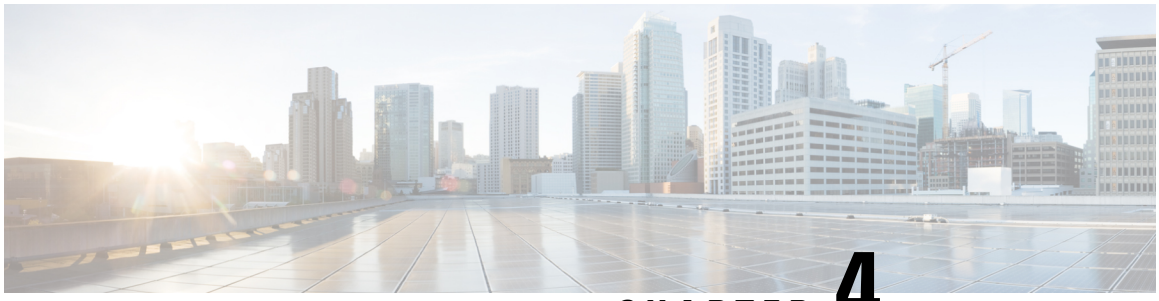
Error	Possible Solution
Unable to delete a Pod or a Cisco DNA Center created by another user.	You cannot delete a component, such as a VA pod or Cisco DNA Center VA, that another user has created while a different action is in progress on the component. After the action completes, you or any other user can delete the component. For example, you cannot delete a VA pod or Cisco DNA Center VA while it is in any of the following processes or states: • Another user is in the process of creating the Cisco DNA Center VA. • Another user is in the process of deleting the Cisco DNA Center VA. • The Cisco DNA Center VA is in a failed state after a deletion attempt.

Error	Possible Solution
The status of a Pod has been changed recently.	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. To view the updated status of the VA pod, click **Refresh**.

Troubleshoot Other Deployment Issues

You can troubleshoot other issues that occur while deploying a Catalyst Center VA on AWS with the following possible solutions:

Issue	Possible Reasons and Solutions
Resources are green, but the Proceed button is disabled.	On some steps, you can only proceed if all the resources have been successfully set up. To ensure the integrity of the deployment, the **Proceed** button remains disabled until the setup is complete and all the resources have been configured and loaded. Sometimes, the screen shows that the resources have been successfully set up, but the **Proceed** button is still disabled. In this case, you need to wait a few more seconds for some resources to load. After all the resources have been configured and loaded, the **Proceed** button is enabled.
Failure when deploying multiple VA pods with the same CGW in single region.	Make sure that: • The CGW IP address is the IP address of your Enterprise firewall or router. • The CGW IP address is a valid public address. • The CGW IP address hasn't been used for another VA pod within the same 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.
Unable to SSH or ping the Cisco DNA Center VA.	You cannot connect via SSH or ping the Catalyst 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.
Session ended	If your session times out while operations are in progress, such as triggering an RCA, the operations may abruptly end and display a **Session ended** notification. If your session times out, click **Ok**, log back in, and restart the operations.



CHAPTER 4

Deploy Using AWS CloudFormation

Use AWS CloudFormation to Manually Deploy Cisco DNA Center on AWS

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. Meet the prerequisites. See Prerequisites for Manual Deployment Using AWS CloudFormation, on page 80.
2. (Optional) Integrate Cisco ISE on AWS and your 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 84.
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 87.

Prerequisites for Manual Deployment Using AWS CloudFormation

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 server IP address
- (Optional) HTTPS Network Proxy details

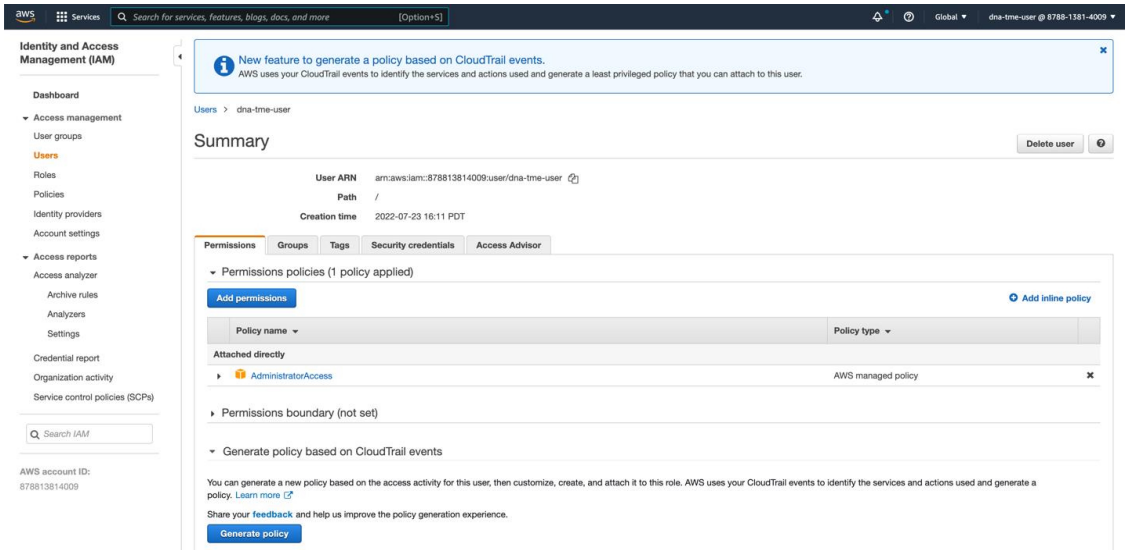
AWS Environment

You must meet the following AWS environment requirements:

- You have valid credentials to access your AWS account.

Note We recommend that your 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.

- **Important**: Your AWS account is subscribed to Cisco DNA Center Virtual Appliance - Bring Your Own License (BYOL) in AWS Marketplace.
- You must have administrator access permission for your AWS account. (In AWS, the policy name is displayed as **AdministratorAccess**.)



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

- **VPC**: The recommended CIDR range is /25. In IPv4 CIDR notation, the last octet (the fourth octet) of the IP address can only have the values 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 your Cisco DNA Center VA on AWS and the devices in your Enterprise network, the AWS security group that you attach to your Cisco DNA Center VA on AWS must allow the following ports:
  - TCP 22, 80, 443, 9991, 25103, 32626
  - UDP 123, 162, 514, 6007, 21730

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. Certificate download from Cisco DNA Center through HTTPS:443, HTTP:80 (Cisco 9800 Wireless Controller, PnP), Sensor/Telemetry. **Note** 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. **Note** 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.
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.

Port	Service Name	Purpose	Recommended Action
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 the 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 TGW Attachments and TGW 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

Important 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 in specific availability zones. To view the list of unsupported availability zones, see the *Release Notes for Cisco Global Launchpad*.

  - 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 and password
- Static IP
- FQDN for the Cisco DNA Center VA IP address

Deploy Cisco DNA Center on AWS Manually Using AWS CloudFormation

You can manually deploy Cisco DNA Center on AWS using AWS CloudFormation. The provided AWS CloudFormation template contains the relevant details for all required parameters.

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 80.
- The VPN tunnel is up.

Procedure

Step 1 Depending on which file you want to download, do one of the following:

- Go to the Cisco Software Download site and download the following file:

  `Catalyst_Center_2.3.5.3_VA_InstanceLaunch_CFT-1.8.0.tar.gz`

- Go to the Cisco Software Download site and download the following file:

  `DNA_Center_VA_InstanceLaunch_CFT-1.7.0.tar.gz`

Both TAR files contain 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-0e15eb31bcb994472
ap-northeast-2 (Seoul)	ami-043e1b9f3ccace4b2
ap-south-1 (Mumbai)	ami-0bbdbd7bcc1445c5f
ap-southeast-1 (Singapore)	ami-0c365aa4cfb5121a9
ap-southeast-2 (Sydney)	ami-0d2d9e5ebb58de8f7

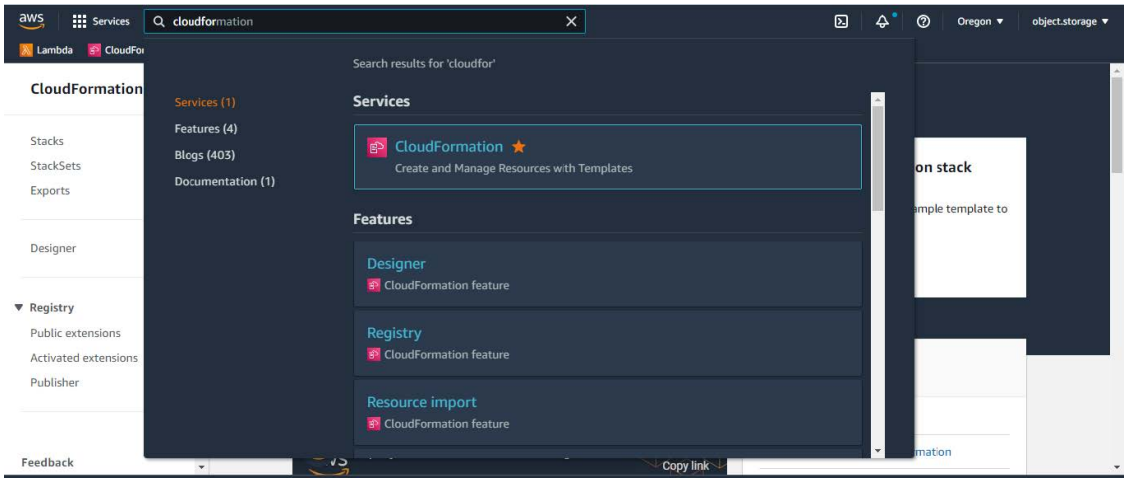
Region	Cisco DNA Center AMI ID
ca-central-1 (Canada)	ami-0485cfdbda5244c6e
eu-central-1 (Frankfurt)	ami-0677a8e229a930434
eu-south-1 (Milan)	ami-091f667a02427854d
eu-west-1 (Ireland)	ami-0a8a59b277dff9306
eu-west-2 (London)	ami-0cf5912937286b42e
eu-west-3 (Paris)	ami-0b12cfdd092ef754e
us-east-1 (Virginia)	ami-08ad555593196c1de
us-east-2 (Ohio)	ami-0c52ce38eb8974728
us-west-1 (Northern California)	ami-0b83a898072e12970
us-west-2 (Oregon)	ami-02b6cd5eee1f3b521

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 In the search bar, enter **`cloudformation`**.



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

Step 6 Click **Create stack** and choose **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, on page 84.

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:
  - **CatalystCenterInstanceIP**: Cisco DNA Center IP address.
  - **CatalystCenterNetmask**: Cisco DNA Center netmask.
  - **CatalystCenterGateway**: Cisco DNA Center gateway address.
  - **CatalystCenterDnsServer**: Enterprise DNS Server.
  - **CatalystCenterPassword**: 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. The password must:
    - Omit any tab or line breaks
    - Have a minimum of eight characters
    - Contain characters from at least three of the following categories:
      - Lowercase letters (a-z)
      - Uppercase letters (A-Z)
      - Numbers (0-9)
      - Special characters (for example, ! or #)

  - **CatalystCenterFQDN**: Cisco DNA Center FQDN.
  - **CatalystCenterHttpsProxy**: (Optional) Enterprise HTTPS proxy.
  - **CatalystCenterHttpsProxyUsername**: (Optional) HTTPS proxy username.
  - **CatalystCenterHttpsProxyPassword**: (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 From the Amazon EC2 console, validate the network and system configuration and verify that the Cisco DNA Center IP address is correct.

Step 2 Send a ping to the Cisco DNA Center IP address to ensure that your host details and network connection are valid.

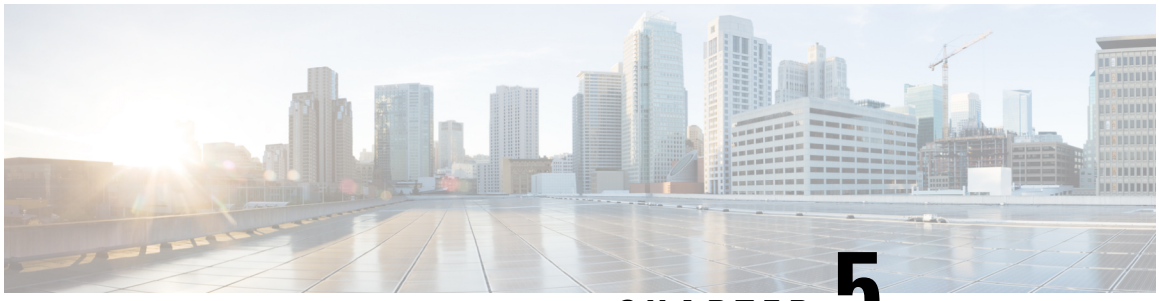
Step 3 Establish an SSH connection with Cisco DNA Center to verify that Cisco DNA Center is authenticated.

Step 4 Test HTTPS accessibility to the Cisco DNA Center GUI using one of the following methods:

- Use a browser.

  For more information about browser compatibility, see the *Cisco DNA Center Release Notes*.

- Use Telnet through the CLI.
- Use curl through the CLI.



CHAPTER 5

Deploy Using AWS Marketplace

Use AWS Marketplace to Manually Deploy Cisco DNA Center on AWS

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. Meet the prerequisites. See Prerequisites for Manual Deployment Using AWS Marketplace, on page 89.
2. (Optional) Integrate Cisco ISE on AWS and your 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 94.
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 94.

Prerequisites for Manual Deployment Using AWS Marketplace

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 server IP address
- (Optional) HTTPS Network Proxy details

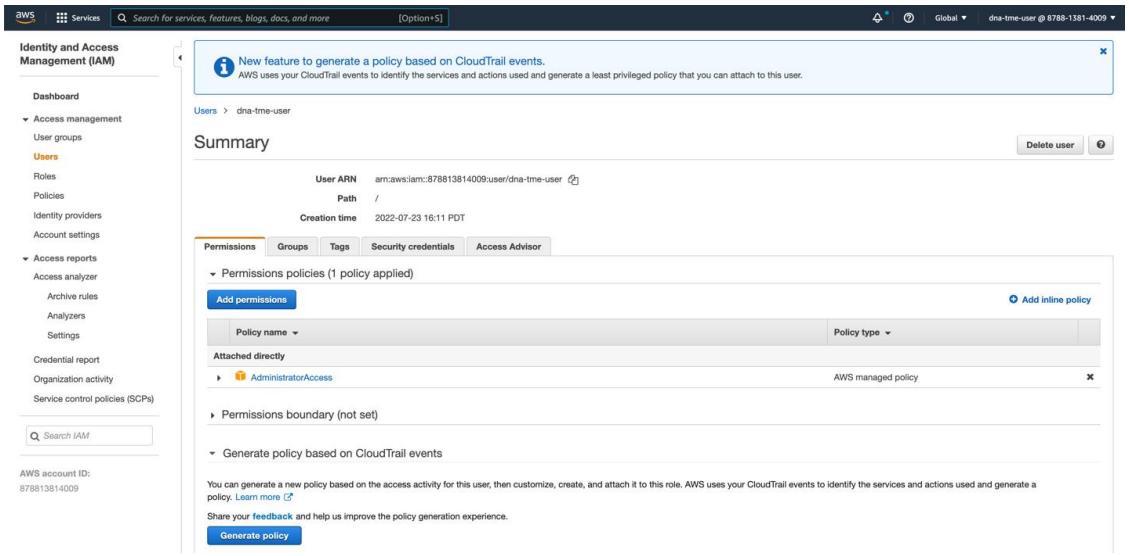
AWS Environment

You must meet the following AWS environment requirements:

- You have valid credentials to access your AWS account.

Note We recommend that your 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.

- **Important**: Your AWS account is subscribed to Cisco DNA Center Virtual Appliance - Bring Your Own License (BYOL) in AWS Marketplace.
- You must have administrator access permission for your AWS account. (In AWS, the policy name is displayed as **AdministratorAccess**.)



- The following resources and services must be set up in AWS:
  - **VPC**: The recommended CIDR range is /25. In IPv4 CIDR notation, the last octet (the fourth octet) of the IP address can only have the values 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

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. Certificate download from Cisco DNA Center through HTTPS:443, HTTP:80 (Cisco 9800 Wireless Controller, PnP), Sensor/Telemetry. **Note** 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. **Note** 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.
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.

Port	Service Name	Purpose	Recommended Action
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 your 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 TGW Attachments and TGW 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

Important 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 in specific availability zones. To view the list of unsupported availability zones, see the *Release Notes for Cisco Global Launchpad*.

  - 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 and password

- Static IP
- FQDN for the Cisco DNA Center 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, do one of the following:

- Go to the Cisco Software Download site and download the following file:

  `Deploy-cisco-dna-center-using-aws-marketplace-1.8.0.tar.gz`

- Go to the Cisco Software Download site and download the following file:

  `Deploy-cisco-dna-center-on-aws-using-aws-marketplace-1.7.0.zip`

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 From the Amazon EC2 console, validate the network and system configuration and verify that the Cisco DNA Center IP address is correct.

Step 2 Send a ping to the Cisco DNA Center IP address to ensure that your host details and network connection are valid.

Step 3 Establish an SSH connection with Cisco DNA Center to verify that Cisco DNA Center is authenticated.

Step 4 Test HTTPS accessibility to the Cisco DNA Center GUI using one of the following methods:

- Use a browser.

  For more information about browser compatibility, see the *Cisco DNA Center Release Notes*.

- Use Telnet through the CLI.
- Use curl through the CLI.