Get Started with Cisco DNA Center on AWS

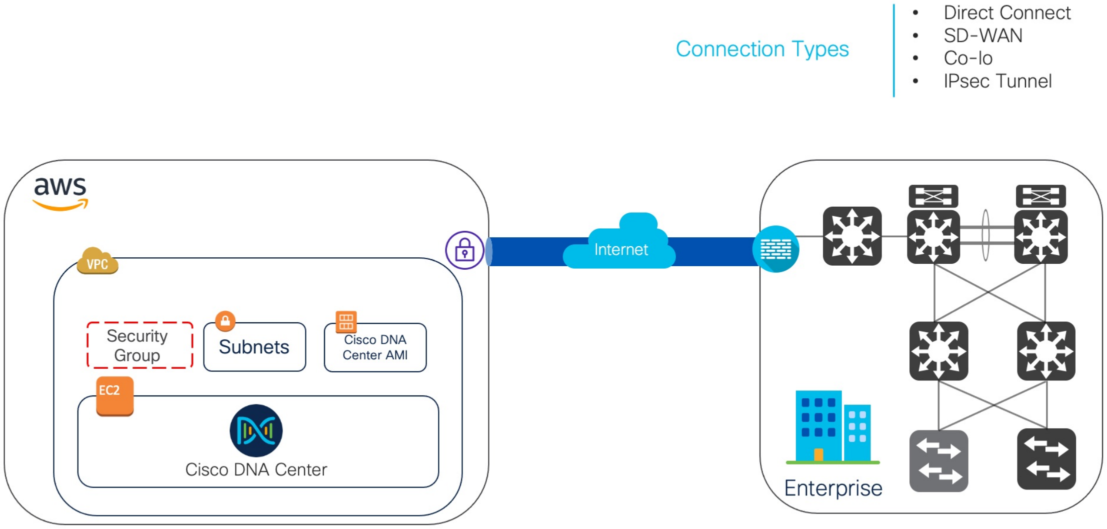
- Cisco DNA Center on AWS Overview, on page 1
- Deployment Overview, on page 2
- Prepare for the Deployment, on page 3

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 or Deploy Using Cisco Global Launchpad 1.9.

- **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.

- **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.

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.