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 2.
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.
3. Deploy Cisco DNA Center on AWS using AWS CloudFormation. See Deploy Cisco DNA Center on AWS Manually Using AWS CloudFormation, on page 6.
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 9.

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

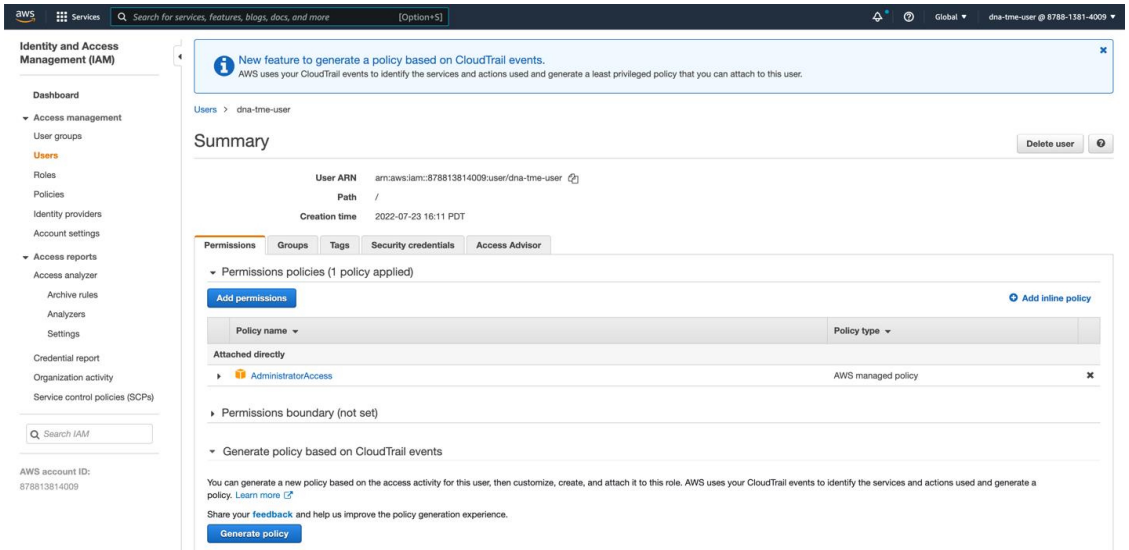
AWS Environment

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:

- Default gateway setting
- CLI password
- 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 2.
- 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-1.9.0.tar.gz`

- 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`

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
ca-central-1 (Canada)	ami-0485cfdbda5244c6e
eu-central-1 (Frankfurt)	ami-0677a8e229a930434

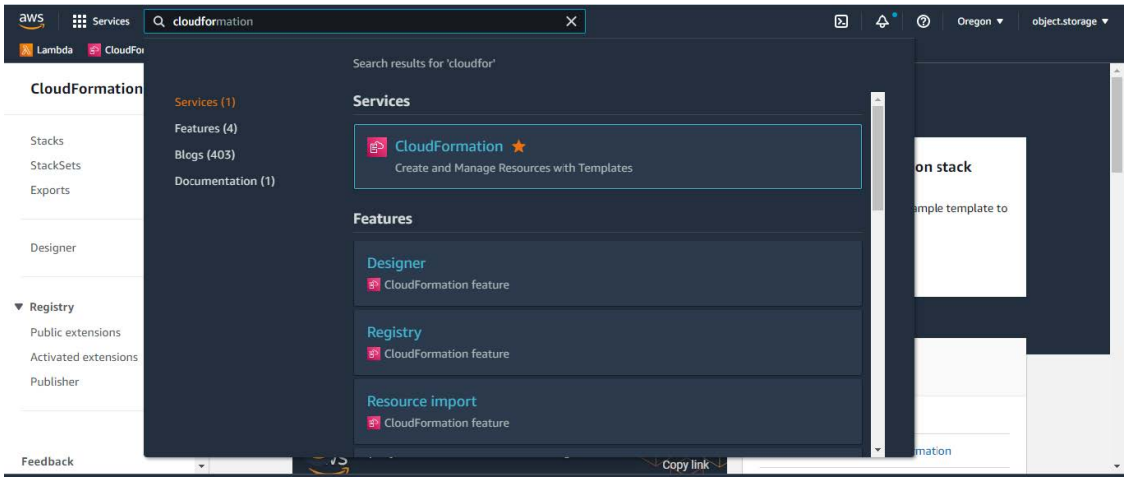
Region	Cisco DNA Center AMI ID
eu-south-1 (Milan)	ami-091f667a02427854d
eu-west-1 (Ireland)	ami-0a8a59b277dff9306
eu-west-2 (London)	ami-0cf5912937286b42e
eu-west-3 (Paris)	ami-0b12cfdd092ef754e
us-east-1 (Virginia)	ami-08ad555593196c1de
us-east-2 (Ohio)	ami-0c52ce38eb8974728
us-west-1 (Northern California)	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.

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 6.

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.