Deploy Using AWS Marketplace

- Use AWS Marketplace to Manually Deploy Cisco DNA Center on AWS, on page 1
- Manual Deployment Using AWS Marketplace Workflow, on page 1
- Prerequisites for Manual Deployment Using AWS Marketplace, on page 1
- Deploy Cisco DNA Center on AWS Manually Using AWS Marketplace, on page 6
- Validate the Deployment, on page 6

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 1.

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 Marketplace. See Deploy Cisco DNA Center on AWS Manually Using AWS Marketplace, 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 6.

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

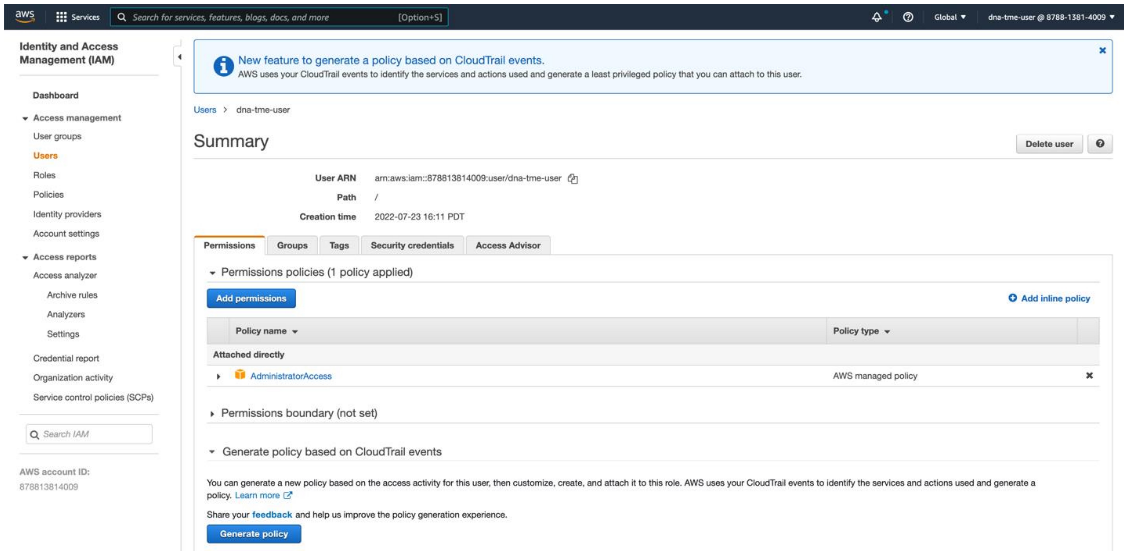
AWS Environment

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**.)



New feature to generate a policy based on CloudTrail events.
AWS uses your CloudTrail events to identify the services and actions used and generate a least privileged policy that you can attach to this user.

AWS account ID: 878813814009

Summary

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

Permissions policies (1 policy applied)

Policy name	Policy type
Attached directly	
AdministratorAccess	AWS managed policy

Permissions boundary (not set)

Generate policy based on CloudTrail events

You can generate a new policy based on the access activity for this user, then customize, create, and attach it to this role. AWS uses your CloudTrail events to identify the services and actions used and generate a policy. Learn more

Share your feedback and help us improve the policy generation experience.

- 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-1.9.0.tar.gz`

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

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

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.