Cisco Catalyst Center 3.1.x on AWS Deployment Guide

Cisco Catalyst Center
Updated July 24, 2026



© 2023–2025 Cisco Systems, Inc. All rights reserved.

Abbreviated Cisco Trademarks

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

Topics included

1 Get Started with Catalyst Center on AWS....6
Catalyst Center on AWS....7
Deployment methods....7
Deployment preparation....8
High availability and Catalyst Center on AWS....8
Guidelines for integrating Cisco ISE on AWS with Catalyst Center on AWS....9
Guidelines for accessing Catalyst Center on AWS....9

2 Deploy Using AWS CloudFormation....12
Manual deployment using AWS CloudFormation....13
Manual deployment using AWS CloudFormation workflow....13
Prerequisites for manual deployment using AWS CloudFormation....13
Deploy Catalyst Center on AWS manually using AWS CloudFormation....17
Verify the Catalyst Center VA TAR file....19
Validate the deployment....20

3 Deploy Using AWS Marketplace....22
Manual deployment using AWS Marketplace....23
Manual deployment using AWS Marketplace workflow....23
Prerequisites for manual deployment using AWS Marketplace....23
Deploy Catalyst Center on AWS using AWS Marketplace....27
Subscribe to and configure the AWS Marketplace launch....27
Configure and launch the Amazon EC2 instance....28
Validate the deployment....33

4 Postdeployment Changes....34
(Optional) Update the DNS server on your Catalyst Center VA using the AWS console 35

1 Get Started with Catalyst Center on AWS

Topics:

- Catalyst Center on AWS
- Deployment methods
- Deployment preparation

Catalyst Center on AWS

Defines Catalyst Center on AWS as a VA that runs in your AWS cloud environment, providing the full functionality of a hardware appliance while managing your network remotely from the cloud.

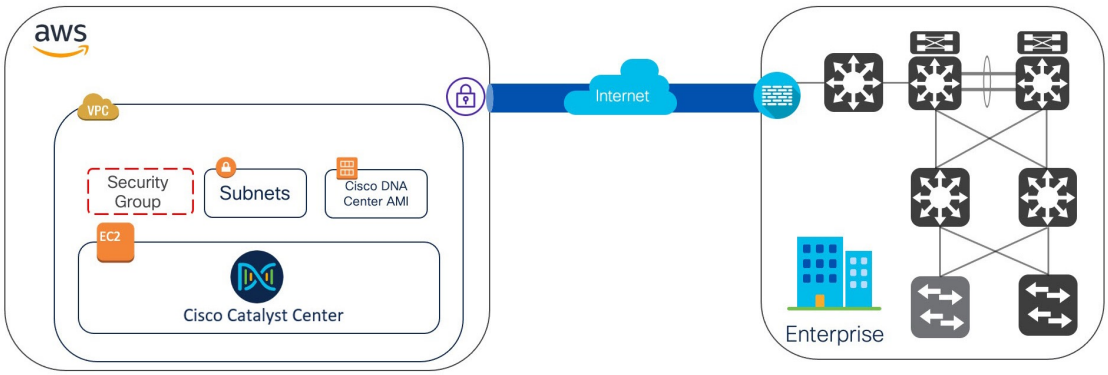
Catalyst Center on AWS

Catalyst Center on Amazon Web Services (AWS) is a deployment model that

- provides the full functionality of a Catalyst Center appliance deployment
- runs in your AWS cloud environment, and
- manages your network from the cloud.

Catalyst Center offers centralized, intuitive management that makes it fast and easy to design, provision, and apply policies across your network environment. The Catalyst 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.

Catalyst Center on AWS topology



Deployment methods

Describes and compares the available deployment methods for Catalyst Center on AWS.

You can manually deploy Catalyst Center on AWS using either AWS CloudFormation or AWS Marketplace.

Manual deployment using AWS CloudFormation

You manually deploy the Catalyst Center AMI on AWS using the AWS CloudFormation deployment tool. Then you manually configure Catalyst Center by creating the AWS infrastructure, establishing a VPN tunnel, and deploying your Catalyst Center VA.

Manual deployment using AWS Marketplace

You manually deploy the Catalyst Center AMI on AWS using AWS Marketplace, an online software store. You launch the software through the Amazon EC2 console. Then you manually deploy Catalyst Center by creating the AWS infrastructure, establishing a VPN tunnel, and configuring your Catalyst Center VA. Only Launch through EC2 is supported for this method. The other two launch options–Launch from Website and Copy to Service Catalog–are not supported.

Choose a deployment method

Consider the benefits and drawbacks of each manual deployment method using this table.

Manual deployment using AWS CloudFormation	Manual deployment using AWS Marketplace
The AWS CloudFormation file is required to create Catalyst Center on AWS.	The AWS CloudFormation file is *not* required to create Catalyst Center 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 Catalyst Center.	
Deployment time may take from a couple of hours to a couple of days.	
You need to manually configure monitoring through the AWS console.	
You can only configure an on-premises NFS for backups.	

Deployment preparation

Provides information about preparing for the deployment of Catalyst Center on AWS.

Network requirements and access considerations

Before you deploy Catalyst Center on AWS, consider

- your network requirements
- whether you need to implement supported Catalyst Center on AWS integrations, and
- how you will access Catalyst Center on AWS.

Preparation resources

Use these resources to prepare for the deployment:

- Review high availability guidelines. See High availability and Catalyst Center on AWS on page 8.
- Review Cisco ISE integration guidelines. See Guidelines for integrating Cisco ISE on AWS with Catalyst Center on AWS on page 9.
- Review Catalyst Center access guidelines. See Guidelines for accessing Catalyst Center on AWS on page 9.

High availability and Catalyst Center on AWS

Explains the single-node EC2 HA implementation and its recovery objectives.

The Catalyst Center on AWS high availability (HA) implementation features:

- A single-node EC2 HA within an Availability Zone (AZ) is enabled by default.
- If a Catalyst Center EC2 instance crashes, AWS automatically brings up another instance with the same IP address. This process ensures uninterrupted connectivity and minimizes disruptions during critical network operations.
- The experience and Recovery Time Objective (RTO) are similar to a power outage sequence in a bare-metal Catalyst Center appliance.

Guidelines for integrating Cisco ISE on AWS with Catalyst Center on AWS

Lists the VPC and TGW peering guidelines and required inbound ports for integrating Cisco ISE on AWS with Catalyst Center on AWS.

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

- Cisco ISE on AWS should be deployed in a separate VPC from the one reserved for Catalyst Center on AWS.
- The VPC for Cisco ISE on AWS can be in the same region as or a different region from the VPC for Catalyst Center on AWS.
- Use VPC or Transit Gateway (TGW) peering depending on your environment.
- To connect the Catalyst 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 Catalyst Center on AWS or Cisco ISE on AWS.

Inbound ports for Cisco ISE integration

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

- Allow TCP ports 9060 and 8910 for Catalyst Center on AWS and Cisco ISE on AWS integration.
- Allow UDP ports 1812, 1813, and any other enabled ports for radius authentication.
- Allow TCP port 49 for device administration via TACACS.
- 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 Catalyst Center on AWS

Provides guidelines for secure Catalyst Center GUI and CLI access, including browser compatibility and credential management.

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

> ⚠ **Caution**
>
> The Catalyst Center GUI and CLI are accessible only through the enterprise network, not from the public network. You need to ensure Catalyst Center is not accessible on the public internet for security reasons.

Guidelines for accessing the Catalyst Center on AWS GUI

Use these guidelines to access the Catalyst Center GUI:

- Use a compatible browser.

  For the current list of compatible browsers, see the *Cisco Catalyst Center Release Notes*.

- In a browser, enter the IP address of your Catalyst Center instance in this format:

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

For example:

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

- Use these credentials for the initial login:
  - Username: **admin**
  - Password: **P@ssword9**

> **Note**
>
> You must change this password when you log in for the first time.
>
> The password must:
> - Omit any tab or line breaks.
> - Have at least nine characters.
> - Contain characters from at least three of these categories:
>   - Lowercase letters (a to z)
>   - Uppercase letters (A to Z)
>   - Numbers (0 to 9)
>   - Special characters (for example, ! or #)

Guidelines for accessing the Catalyst Center CLI

Use these guidelines to access the Catalyst Center CLI:

- 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 by using the Linux **chmod** command.

  For example:

  chmod 400 key.pem

- Use this Linux command to access the Catalyst Center CLI:

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

  For example:

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

2 Deploy Using AWS CloudFormation

Topics:

- Manual deployment using AWS CloudFormation
- Manual deployment using AWS CloudFormation workflow
- Prerequisites for manual deployment using AWS CloudFormation
- Deploy Catalyst Center on AWS manually using AWS CloudFormation
- Verify the Catalyst Center VA TAR file
- Validate the deployment

Manual deployment using AWS CloudFormation

Introduces the manual deployment method using AWS CloudFormation for those who have existing VPCs.

This chapter explains how to manually deploy the Catalyst Center AMI on your AWS account using AWS CloudFormation. You will create the AWS infrastructure, establish a VPN tunnel, and deploy Catalyst Center.

This deployment method is an option for those who

- are familiar with AWS administration, and
- have existing VPCs.

Manual deployment using AWS CloudFormation workflow

Outlines the high-level steps for deploying Catalyst Center on AWS using AWS CloudFormation.

Follow these high-level steps to deploy Catalyst Center on AWS using AWS CloudFormation:

1. Meet the prerequisites. See Prerequisites for manual deployment using AWS CloudFormation on page 13.
2. (Optional) Integrate Cisco ISE and your Catalyst Center VA together. See Guidelines for integrating Cisco ISE on AWS with Catalyst Center on AWS on page 9.
3. Deploy Catalyst Center on AWS using AWS CloudFormation. See Deploy Catalyst Center on AWS manually using AWS CloudFormation on page 17.
4. Verify that your environment setup and the Catalyst Center VA configuration are installed correctly and working as expected. See Validate the deployment on page 20.

Prerequisites for manual deployment using AWS CloudFormation

Lists the network, AWS infrastructure, and Catalyst Center instance requirements—including VPC, security group, and region settings—needed to prepare for a Catalyst Center on AWS deployment using AWS CloudFormation.

Before deploying Catalyst Center on AWS, ensure you meet these network, AWS, and Catalyst Center requirements.

Network environment requirements

You have this information about your network environment on hand:

- Enterprise DNS server IP address
- (Optional) HTTPS network proxy details

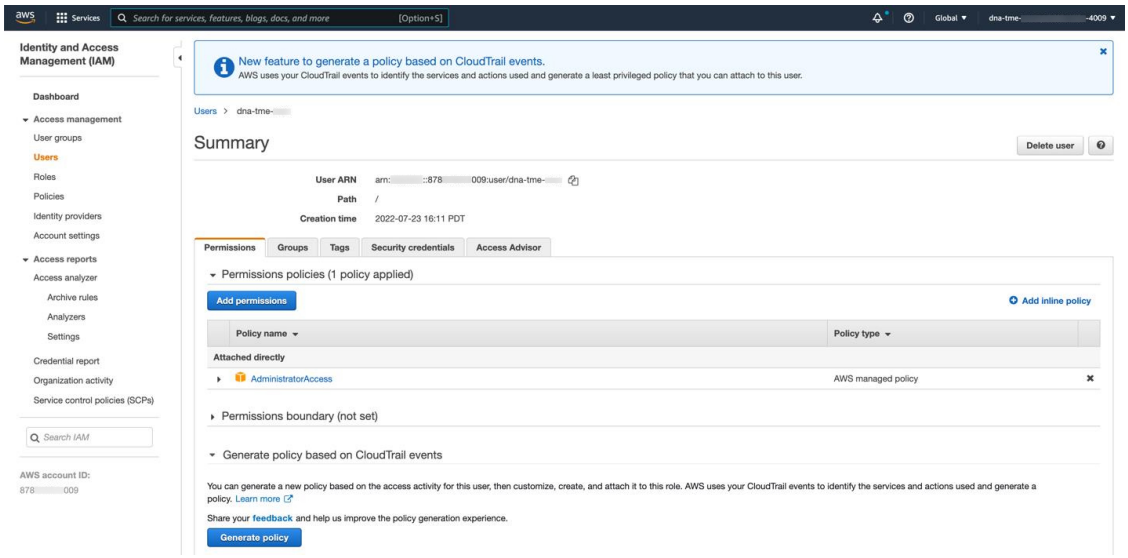
AWS account requirements

You must meet these AWS account requirements:

- You have valid credentials to access your AWS account.

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

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



AWS network infrastructure requirements

You must set up these resources and services 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 be 0 or 128. For example, x.x.x.0 or x.x.x.128 are valid options.
- **Subnets**: The recommended subnet range is /28, and it should not overlap with your corporate subnet.
- **Route tables**: Make sure that your VPC subnet is allowed to communicate with your enterprise network through your VPN Gateway (VPN GW) or Transit Gateway (TGW).
- **Security groups**: For communication between Catalyst Center on AWS and the devices in your enterprise network, the AWS security group attached to Catalyst Center on AWS must allow these ports:
  - TCP ports: 22, 80, 443, 9991, 25,103, and 32,626
  - UDP ports: 123, 162, 514, 6007, and 21,730

  For more information about the ports that Catalyst Center uses, see "Communication ports" in the "Plan the Deployment" chapter in the *Cisco Catalyst Center Installation Guide*.
- **VPN GW or 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, ensure that the correct ports are open for traffic flow to and from your Catalyst Center VA. You can open them using either the firewall settings or a proxy gateway. For 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 Catalyst Center Appliance Installation Guide*.

- **Site-to-Site VPN connection**: You can use TGW attachments and TGW route tables.

AWS region configuration requirements

You must meet these AWS region configuration requirements:

- Your AWS environment must be configured with one of these 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)
  - me-south-1 (Bahrain)
  - sa-east-1 (Sao Paulo)
  - us-east-1 (Virginia)
  - us-east-2 (Ohio)
  - AWS GovCloud (US-East)
  - AWS GovCloud (US-West)
  - us-west-1 (Northern California)
  - us-west-2 (Oregon)
- The Catalyst Center r5a.8xlarge instance size isn't supported in these availability zones:
  - The us-east-1e availability zone in the us-east-1 region
  - The ap-northeast-2b and ap-northeast-2d availability zones in the ap-northeast-2 region
  - The ca-central-1d availability zone in the ca-central-1 region

IAM user group requirement (optional)

If you want to enable multiple IAM users with the ability to configure Catalyst Center using the same environment setup, you need to create a group with these policies and then add the required users to that group:

- IAMReadOnlyAccess
- AmazonEC2FullAccess

- AWSCloudFormationFullAccess

Catalyst Center instance requirements

The Catalyst Center instance size must meet these minimum resource requirements:

- r5a.8xlarge

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

- 32 virtual CPUs (vCPUs)
- 256-GB RAM
- 3-terabyte (TB) storage, provisioned as three separate EBS-gp3 disks:
  - 100-GiB disk
  - 550-GiB disk
  - 2350-GiB disk
- 2500 disk input and output operations per second (IOPS)
- 180-MBps disk bandwidth

Catalyst Center backup instance requirements

The Catalyst Center backup instance must meet these minimum resource requirements based on if you use a cloud server or an enterprise (on-premises) server:

- **Cloud backup**: t3.micro, 2 vCPUs, 1-GB RAM, and for storage, see "Backup storage requirements" in the *Cisco Catalyst Center Administrator Guide*.
- **Enterprise backup**: See "Backup server requirements" and "Backup storage requirements" in the *Cisco Catalyst Center Administrator Guide*.

AWS information requirements

You have this AWS information on hand:

- Subnet ID
- Security group ID
- Keypair ID
- Environment name
- CIDR reservation

Catalyst Center environment requirements

You must meet these requirements for your Catalyst Center environment:

- You have access to the Catalyst Center GUI.

- You have this Catalyst Center information on hand:
  - Default gateway setting
  - CLI password
  - FQDN for the Catalyst Center VA IP address

Deploy Catalyst Center on AWS manually using AWS CloudFormation

Provides step-by-step instructions for creating the stack and configuring the parameters to deploy Catalyst Center on AWS.

Follow these steps to manually deploy Catalyst Center on AWS using AWS CloudFormation. The provided AWS CloudFormation template contains the relevant details for all required parameters.

Before you begin

Ensure that

- the VPN tunnel is up, and
- the AWS environment is set up with all the required components.

  For information, see Prerequisites for manual deployment using AWS CloudFormation on page 13.

Procedure

1. Go to the Cisco Software Download site and download this file:

   CatC-3.1.6-75524.200-VA_InstanceLaunch_CFT.tar.gz

   The file contains the AWS CloudFormation template that you use to create your Catalyst Center VA instance. The AWS CloudFormation template contains several AMIs, each with a different AMI ID based on a specific region. Ensure that you use the appropriate AMI ID for your region.

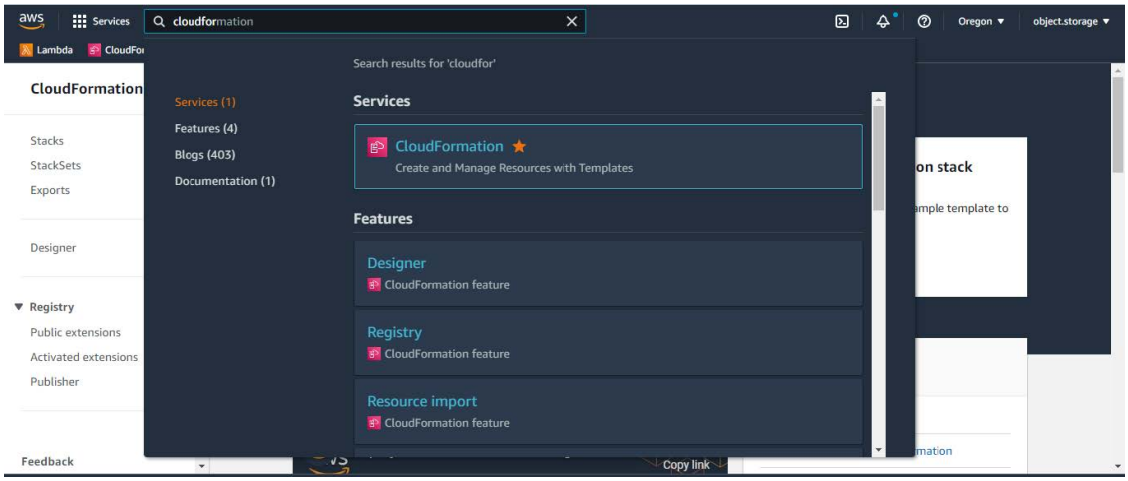
2. Verify that the TAR file is genuine and from Cisco Systems, Inc.

   For detailed steps, see Verify the Catalyst Center VA TAR file on page 19.

3. Log in to the AWS console.

   The AWS console is displayed.

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



5. From the drop-down menu, choose **CloudFormation**.
6. Click **Create stack** and choose **With new resources (standard)**.
7. Under **Specify template**, select **Upload a template file**, and choose the AWS CloudFormation template that you downloaded in Step 1.
8. Enter a stack name and review these 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 Catalyst Center.
     - **Security Group**: Enter the security group to be attached to the Catalyst Center VA that you are deploying.
     - **Keypair**: Enter the SSH keypair used to access the CLI of Catalyst Center VA that you are deploying.
   - **Catalyst Center Configuration**: Enter this information:
     - **CatalystCenterInstanceIP**: Catalyst Center IP address.
     - **CatalystCenterNetmask**: Catalyst Center netmask.
     - **CatalystCenterGateway**: Catalyst Center gateway address.
     - **CatalystCenterDnsServer**: Enterprise DNS Server.
     - **CatalystCenterPassword**: Catalyst Center password.

> **Note**
>
> You can use the Catalyst Center password to access the Catalyst Center VA CLI through the AWS EC2 Serial Console.
>
> The password must
>
> - omit any tab or line breaks
> - have at least eight characters, and
> - contain characters from at least three of these categories.
>   - Lowercase letters (a-z)
>   - Uppercase letters (A-Z)
>   - Numbers (0-9)
>   - Special characters (for example, ! or #)

- **CatalystCenterFQDN**: Catalyst Center FQDN.
- **CatalystCenterHttpsProxy**: (Optional) Enterprise HTTPS proxy.
- **CatalystCenterHttpsProxyUsername**: (Optional) HTTPS proxy username.
- **CatalystCenterHttpsProxyPassword**: (Optional) HTTPS proxy password.

9. Optional: Click **Next** to configure the stack options.
10. Click **Next** to review your stack information.
11. Click **Submit** when you are satisfied with the configuration.

    Stack creation usually takes 45 to 60 minutes.

Verify the Catalyst Center VA TAR file

Details the Catalyst Center VA TAR file verification process using Cisco public keys and signatures to ensure file integrity.

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

Before you begin

Ensure that you downloaded the Catalyst Center VA TAR file from the Cisco Software Download site.

Procedure

1. Download the Cisco public key (cisco_image_verification_key.pub) for signature verification from the location specified by Cisco.
2. Download the secure hash algorithm (SHA512) checksum file for the TAR file from the location specified by Cisco.

3. Obtain the signature file (.sig) for the TAR file from Cisco support through email or by download from the secure Cisco website (if available).
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 these commands:

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

   On Microsoft Windows, use the certutil tool because it does not include a built-in checksum utility:

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

   For example:

   ```
   certutil -hashfile D:\Customers\Catalyst_Center_<release
   number>_VA_Instance_CFT-x.y.z.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\Catalyst_Center_<release number>_VA_Instance_CFT-x.y.z.tar.gz

   Algorithm Hash Path
   SHA256 <string> D:\Customers\Catalyst_Center_<release
   number>_VA_Instance_CFT-x.y.z.tar.gz
   ```

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

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.

Validate the deployment

Explains how to verify a successful deployment, including network connectivity checks, system authentication, and Catalyst Center GUI access testing.

Perform these validation checks to ensure that your environment setup and Catalyst Center VA configuration work.

Before you begin

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

Procedure

1. From the Amazon EC2 console, validate the network and system configuration and verify that the Catalyst Center IP address is correct.
2. Send a ping to the Catalyst Center IP address to ensure that your host details and network connection are valid.
3. Establish an SSH connection with Catalyst Center to verify that Catalyst Center is authenticated.
4. Test HTTPS accessibility to the Catalyst Center GUI using one of these methods:
   - Use a browser.

     For more information about browser compatibility, see the *Release Notes for Cisco Catalyst Center*.
   - Use Telnet through the CLI.
   - Use curl through the CLI.

3 Deploy Using AWS Marketplace

Topics:

- Manual deployment using AWS Marketplace
- Manual deployment using AWS Marketplace workflow
- Prerequisites for manual deployment using AWS Marketplace
- Deploy Catalyst Center on AWS using AWS Marketplace
- Validate the deployment

Manual deployment using AWS Marketplace

Introduces the manual deployment method using AWS Marketplace for those who have existing VPCs.

This chapter explains how to manually deploy Catalyst Center on your AWS account using AWS Marketplace.

This deployment method is an option for those who

- are familiar with AWS administration, and
- have existing VPCs.

Manual deployment using AWS Marketplace workflow

Outlines the high-level steps for deploying Catalyst Center on AWS using AWS Marketplace.

Follow these high-level steps to deploy Catalyst Center on AWS using AWS Marketplace:

1. Meet the prerequisites. Refer to Prerequisites for manual deployment using AWS Marketplace on page 23.
2. (Optional) Integrate Cisco ISE on AWS and your Catalyst Center VA together. Refer to Guidelines for integrating Cisco ISE on AWS with Catalyst Center on AWS on page 9.
3. Deploy Catalyst Center on AWS using AWS Marketplace. Refer to Deploy Catalyst Center on AWS using AWS Marketplace on page 27.
4. Verify that your environment setup and the Catalyst Center VA configuration are installed correctly and working as expected. Refer to Validate the deployment on page 33.

Prerequisites for manual deployment using AWS Marketplace

Lists the network, AWS infrastructure, and Catalyst Center instance requirements—including VPC, security group, and region settings—needed to prepare for a Catalyst Center on AWS deployment using AWS Marketplace.

Before deploying Catalyst Center on AWS, ensure you meet these network, AWS, and Catalyst Center requirements.

Network environment requirements

You have this information about your network environment on hand:

- Enterprise DNS server IP address
- (Optional) HTTPS network proxy details

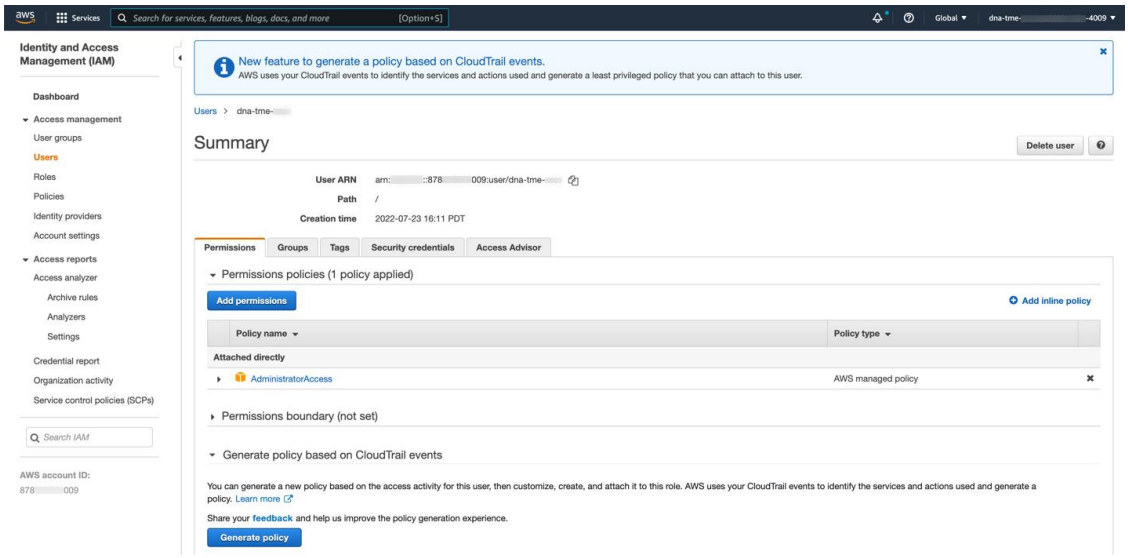
AWS account requirements

You must meet these AWS account requirements:

- You have valid credentials to access your AWS account.

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

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



AWS network infrastructure requirements

You must set up these resources and services 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 be 0 or 128. For example, x.x.x.0 or x.x.x.128 are valid options.
- **Subnets**: The recommended subnet range is /28, and it should not overlap with your corporate subnet.
- **Route tables**: Make sure that your VPC subnet is allowed to communicate with your enterprise network through your VPN Gateway (VPN GW) or Transit Gateway (TGW).
- **Security groups**: For communication between Catalyst Center on AWS and the devices in your enterprise network, the AWS security group attached to Catalyst Center on AWS must allow these ports:
  - TCP ports: 22, 80, 443, 9991, 25,103, and 32,626
  - UDP ports: 123, 162, 514, 6007, and 21,730

  For more information about the ports that Catalyst Center uses, see "Communication ports" in the "Plan the Deployment" chapter in the *Cisco Catalyst Center Installation Guide*.
- **VPN GW or 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, ensure that the correct ports are open for traffic flow to and from your Catalyst Center VA. You can open them using either the firewall settings or a proxy gateway. For information

about well-known network service ports that the appliance uses, see "Required network ports" in the "Plan the Deployment" chapter of the *Cisco Catalyst Center Appliance Installation Guide*.

- **Site-to-site VPN connection**: You can use TGW attachments and TGW route tables.

AWS region configuration requirements

You must meet these AWS region configuration requirements:

- Your AWS environment must be configured with one of these 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)
  - me-south-1 (Bahrain)
  - sa-east-1 (Sao Paulo)
  - us-east-1 (Virginia)
  - us-east-2 (Ohio)
  - AWS GovCloud (US-East)
  - AWS GovCloud (US-West)
  - us-west-1 (N. California)
  - us-west-2 (Oregon)
- The Catalyst Center r5a.8xlarge instance size isn't supported in these availability zones:
  - The us-east-1e availability zone in the us-east-1 region
  - The ap-northeast-2b and ap-northeast-2d availability zones in the ap-northeast-2 region
  - The ca-central-1d availability zone in the ca-central-1 region

IAM user group requirement (optional)

If you want to enable multiple IAM users with the ability to configure Catalyst Center using the same environment setup, you need to create a group with these policies and then add the required users to that group:

- IAMReadOnlyAccess
- AmazonEC2FullAccess

- AWSCloudFormationFullAccess

Catalyst Center instance requirements

The Catalyst Center instance size must meet these minimum resource requirements:

- r5a.8xlarge

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

- 32 virtual CPUs (vCPUs)
- 256-GB RAM
- 3-terabyte (TB) storage, provisioned as three separate EBS-gp3 disks:
  - 100-GiB disk
  - 550-GiB disk
  - 2350-GiB disk
- 2500 disk input and output operations per second (IOPS)
- 180-MBps disk bandwidth

Catalyst Center backup instance requirements

The Catalyst Center backup instance must meet these minimum resource requirements based on if you use a cloud server or an enterprise (on-premises) server:

- **Cloud backup**: t3.micro, 2 vCPUs, 1-GB RAM, and for storage, see "Backup storage requirements" in the *Cisco Catalyst Center Administrator Guide*.
- **Enterprise backup**: See "Backup server requirements" and "Backup storage requirements" in the *Cisco Catalyst Center Administrator Guide*.

AWS information requirements

You have this AWS information on hand:

- Subnet ID
- Security group ID
- Keypair ID
- Environment name
- CIDR reservation

Catalyst Center environment requirements

You must meet these requirements for your Catalyst Center environment:

- You have access to the Catalyst Center GUI.

- You have this Catalyst Center information on hand:
  - NTP setting
  - Default gateway setting
  - CLI password
  - UI username and password
  - Static IP
  - FQDN for the Catalyst Center VA IP address

Deploy Catalyst Center on AWS using AWS Marketplace

Outlines the high-level steps for deploying Catalyst Center on AWS using AWS Marketplace.

Follow these steps to manually deploy Catalyst Center on AWS using AWS Marketplace.

Before you begin

Ensure that you meet all the prerequisites. Refer to Prerequisites for manual deployment using AWS Marketplace on page 23.

Procedure

1. Subscribe to and configure the AWS Marketplace launch.
2. Configure and launch the Amazon EC2 instance on page 28.

Catalyst Center on AWS is deployed using AWS Marketplace.

Subscribe to and configure the AWS Marketplace launch

Provides the steps for subscribing to Catalyst Center in AWS Marketplace and opening the EC2 launch workflow.

Follow these steps to subscribe to Catalyst Center in AWS Marketplace and configure the AWS Marketplace launch options.

Before you begin

Ensure that you meet all the prerequisites. Refer to Prerequisites for manual deployment using AWS Marketplace on page 23.

Procedure

1. Log in to the Amazon Management Console.
2. Search for **`AWS Marketplace Subscriptions`**.
3. In the **Manage Subscriptions** window, click **Discover Products** in the left pane and enter **`Cisco Catalyst Center Virtual Appliance`** in the search bar.
4. Click the product name.
5. Click **Continue to Subscribe**.
6. In the **Configure this software** page, choose a fulfillment option (architecture), software version, and region from the drop-down lists.

7. In the **Launch this software** page, do these steps:
   a) From the **Choose Action** drop-down list, choose **Launch through EC2**.
   b) Click **Launch**.

The **EC2 Launch an instance** page is displayed.

Configure and launch the Amazon EC2 instance

Lists the steps for configuring the Amazon EC2 instance, entering cloud-init user data, launching the instance, and verifying that it was created.

Follow these steps to configure and launch the Amazon EC2 instance for Catalyst Center on AWS.

Before you begin

Ensure that you subscribed to and configured the AWS Marketplace launch. Refer to Subscribe to and configure the AWS Marketplace launch.

Procedure

1. From the **EC2 Launch an instance** page, in the **Name** field, enter a name for the Catalyst Center VA.

   The **Amazon Machine Image (AMI)** and **Instance type** settings are configured by default.
2. In the **Key pair (login)** section, choose an existing key pair from the **Key pair name** drop-down list or click **Create new key pair** to create a new one.
3. In the **Network Settings** section, click **Edit** and configure these settings:
   a) From the **VPC** drop-down list, choose a VPC.
   b) From the **Subnet** drop-down list, choose a subnet.
   c) Make sure that the **Auto-assign public IP** field is set to **Disabled**.
   d) For **Firewall (security groups)**, click **Create security group** or **Select existing security group** to configure a security group containing the necessary inbound and outbound rules.
4. In the **Advanced Network Configuration** section, enter the same IP address that is configured for Catalyst Center in the **User Data** field.
5. In the **Storage** section, ensure that the **Root volume** field matches this configuration:
   - `1x: 100 GiB`
   - `1x: 550 GiB`
   - `1x: 2350 GiB`
   - `Disk type: gp3`
6. In the **File systems** section, do not configure a file system. Instead, proceed to the next step.

   Note

   For backup instructions, refer to the "Backup and Restore" chapter in the *Cisco Catalyst Center Administrator Guide*.
7. In the **Advanced Details** section, in the **User Data** field, enter the mandatory user data script that specifies your on-premises network configuration in YAML formatting.

This table lists the required cloud-init script keys and their descriptions.

Key	Description
`mks_cloudinit_version`	Do not modify this field.
`addressing_mode`	Do not modify this field.
Network configuration	
`address`	Enter the IP address for Catalyst Center.
`netmask`	Enter the netmask for Catalyst Center.
`gateway`	Enter the gateway address for Catalyst Center.
`routes`	Do not modify this field.
`name`	Do not modify this field.
Domain Name System (DNS) configuration	
`upstream_dns_servers`	Enter the enterprise DNS server address. **Note** The DNS server must be reachable.
Proxy configuration	
`server`	(Optional) Enter the enterprise HTTP proxy server address. **Note** The proxy server address must use the HTTP protocol. The HTTPS protocol is not supported.
`username`	(Optional) Enter the HTTP proxy username.
`password`	(Optional) Enter the HTTP proxy password.
Network Time Protocol (NTP) configuration	

Key	Description
`servers`	Do not modify this field. **Note** The default AWS NTP server address, `169.254.169.123`, is used in the examples.
Catalyst Center configuration	
`fqdn`	Enter the fully-qualified domain name (FQDN) for Catalyst Center.

Key	Description

`cli_password`	Enter the CLI password for Catalyst Center.
	
	Note
	
	The password must:
	• Have at least nine characters and at most 127 characters.
	• Contain characters from at least three of these categories:
	  ◦ Lowercase letters (a to z)
	  ◦ Uppercase letters (A to Z)
	  ◦ Numbers (0 to 9)
	  ◦ Special characters (for example, ! or #)
	
	The password must not include:
	• the username or any two consecutive characters of the username
	• more than three repeated characters, such as aaaa or 1111
	• common keyboard patterns, such as qwer or asdf, and
	• whitespace, such as spaces and tabs.

Note

- Each key in the user data script specifies a mandatory value used by Catalyst Center.
- For each field that you configure, use the correct syntax.
- When the input is entered, the syntax is not validated. If the incorrect syntax is used, Catalyst Center might not come up when you launch the AMI. Make sure that you validate the user data script using a YAML validator, such as YAMLlint.
- Ensure that all fields, including the path and NTP, are configured as specified in this step.
- For any unused variables, remove the variable keys.

If you are using a proxy, enter the proxy details in the cloud-init script. For example:

Example

```
#cloud-config
write_files:
  - path: /etc/cloud.json
```

```
    content: |
      {
        "mks_cloudinit_version": 1,
        "addressing_mode": "ipv4",
        "network": [
          {
            "address": "10.10.0.10",
            "netmask": "255.255.255.0",
            "gateway": "10.10.0.1",
            "routes": [],
            "name": "enterprise"
          }
        ],
        "upstream_dns_servers": ["10.0.0.2"],
        "proxy": {
          "server": "http://10.30.0.42:3128",
          "username": "proxyadmin",
          "password": "Proxypass"
        },
        "ntp": {
          "servers": ["169.254.169.123"]
        },
        "fqdn": "catalyst.center.example.com",
        "cli_password": "Public1@3"
      }
```

If you are not using a proxy, remove the proxy fields from the cloud-init script. For example:

Example

```
#cloud-config
write_files:
  - path: /etc/cloud.json
    content: |
      {
        "mks_cloudinit_version": 1,
        "addressing_mode": "ipv4",
        "network": [
          {
            "address": "10.10.0.10",
            "netmask": "255.255.255.0",
            "gateway": "10.10.0.1",
            "routes": [],
            "name": "enterprise"
          }
        ],
        "upstream_dns_servers": ["10.0.0.2"],
        "ntp": {
          "servers": ["169.254.169.123"]
        },
        "fqdn": "catalyst.center.example.com",
        "cli_password": "Public1@3"
      }
```

8. In the **Summary** pane, review the configuration.
9. If you're satisfied with the configuration, click **Launch instance** and proceed to **Instance Creation**.

What to do next

To view the newly created instance, navigate to **EC2** > **Instances**.

Validate the deployment

Explains how to verify a successful deployment, including network connectivity checks, system authentication, and Catalyst Center GUI access testing.

Perform these validation checks to ensure that your environment setup and Catalyst Center VA configuration work.

Before you begin

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

Procedure

1. From the Amazon EC2 console, validate the network and system configuration and then verify that the Catalyst Center IP address is correct.
2. Send a ping to the Catalyst Center IP address to ensure that your host details and network connection are valid.
3. Establish an SSH connection with Catalyst Center to verify that Catalyst Center is authenticated.
4. Test HTTPS accessibility to the Catalyst Center GUI using one of these methods:
   - Use a browser.

     For more information about browser compatibility, see the *Release Notes for Cisco Catalyst Center*.
   - Use Telnet through the CLI.
   - Use curl through the CLI.

4 Postdeployment Changes

Topics:

- (Optional) Update the DNS server on your Catalyst Center VA using the AWS console

(Optional) Update the DNS server on your Catalyst Center VA using the AWS console

Provides the prerequisite and step-by-step instructions to update the DNS server IP address that is configured on your Catalyst Center VA using the AWS console.

Use this procedure to update the DNS server IP address that is configured on your Catalyst Center VA.

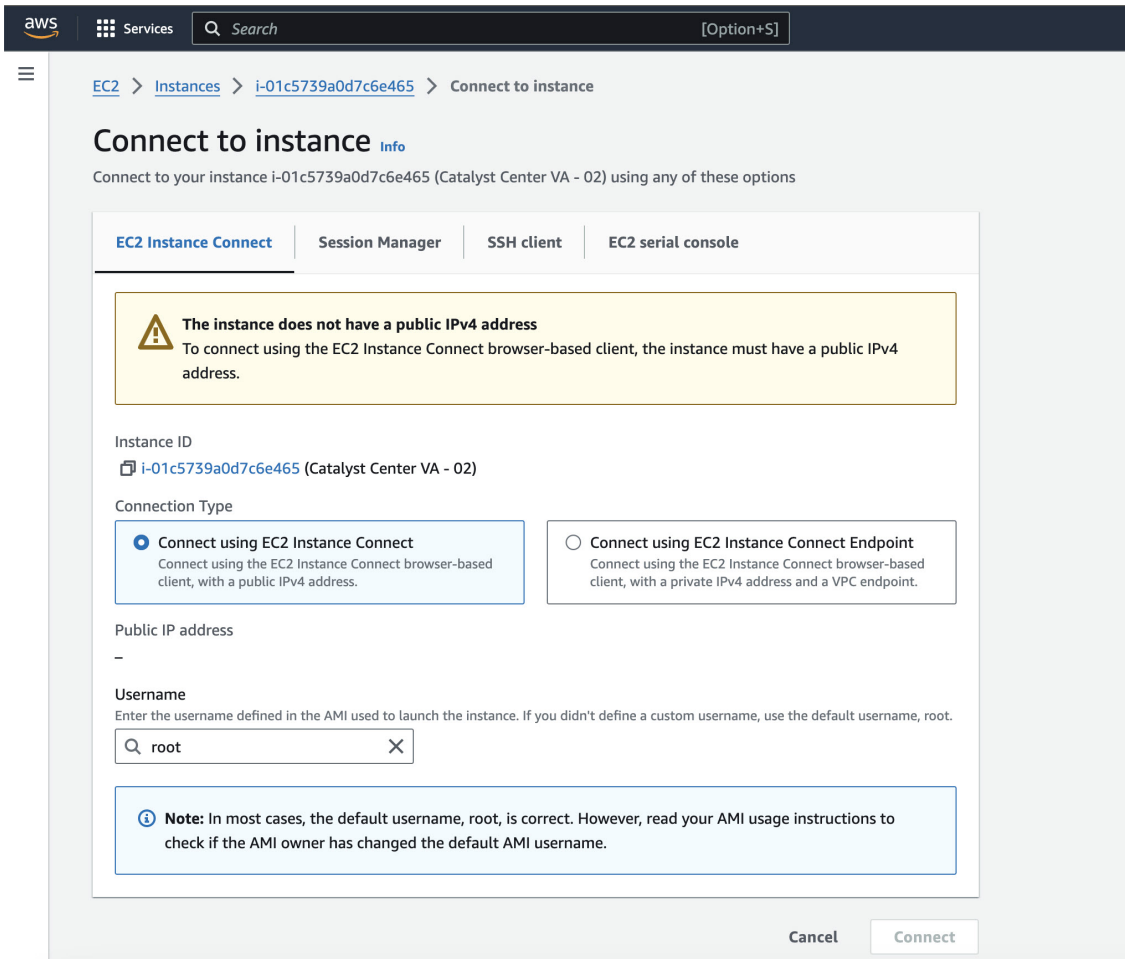
Before you begin

Get a consent token from Cisco TAC for full shell access.

Procedure

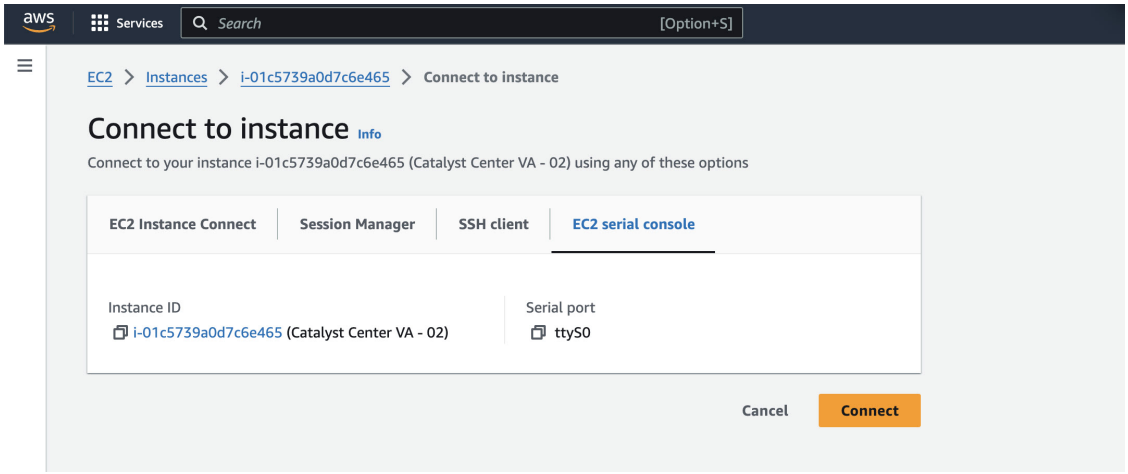
1. Log in to the AWS console.
2. Choose **EC2** > **Instances**.
3. Choose the instance ID that you want to change and click **Connect**.

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



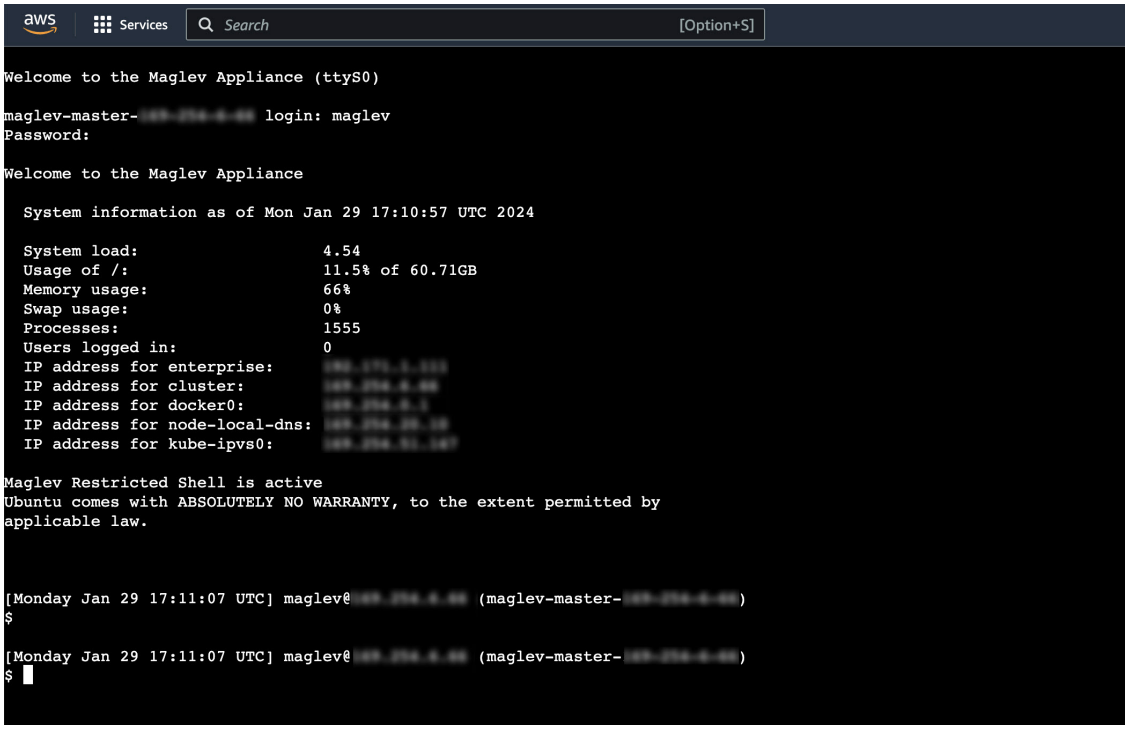
4. Click the **EC2 serial console** tab.

   The Catalyst Center VA instance ID and serial port are displayed.



5. Click **Connect**.

   The Maglev console is displayed.



6. In the Maglev console, update the DNS server IP address to your preferred IP address.
   a. At the **Login** prompt, enter **`maglev`** as the username.
   b. At the **Password** prompt, enter the password that was configured during the initial deployment, regardless of the deployment method.
   c. Gain full shell access by using the consent token that you received from Cisco TAC:

```
$ _shell -v consent-token
```

   For example:

```
_shell -v n1+hPAAAAQ000AQAAAABAgAEAAAAAAMBYkk2bmhXcW14OGtqUXoy
a09UTXlzM252UnNlUnFwTEFEQVQvejJjQm9kNXloN2thSFk3MzZBek9CMEJRUUZad2QNCkhPNVZMNjhMUXMyb0h
```

```
1OXQ2eW1TR01yT1hwZkRPSmNuc1c2QUJ5ZGtVZ0N2OU1mMXZtTC90em1MNldWcVdjY2gNCkh3eEd5MytZWmRVUTN
kek1xOWNiWi9rLzVlTkozQ2RrYy9SMXEya2NOV09uMEdvZE11c1lZN01ENjZvVk5zZlMNCktseHZxTi9tVXF0cW1
vaG9NZFY4SnVOY3NBcXkxQkZOMzZHdS9XQ2N4S2tpdlNUV1VOTVVrRXU1TjVRUDl6d1YNCmYyWW1ZdUFnSGNOcnV
veUhoTzZYYjRIWnJWNDdxSG5qR0REUjV3TE90bnNXalpBL2tsRzNzN0lIa1ZaY0VzMVENCkVoc3FZUGU5Z2ZoTWF
6YXVKRmtxVmc9PQ==
```

d. Set the terminal to display in color:

```
export TERM=xterm
```

e. Run the **sudo maglev-config update** command.

The Configuration wizard presents a shortened series of screens like those described in "Configure a Secondary Node Using the Maglev Wizard" in the *Cisco Catalyst Center Appliance Installation Guide*.

When the DNS server IP address setting is displayed, update it to the preferred IP address. After making changes on each screen, choose **next>>** to continue through the Configuration wizard. At the end of the configuration process, a message states that the Configuration wizard is ready to apply your changes.

f. Review and verify your changes using the available options:

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

g. Click **proceed>>** to save and apply the changes.

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