



Cisco Global Launchpad 1.9 Administrator Guide

First Published: 2024-05-10

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	Cisco Global Launchpad Overview 1
	Cisco Global Launchpad Overview 1
CHAPTER 2	Access Cisco Global Launchpad 3
	Access Hosted Cisco Global Launchpad 3
	Log In to the Cisco DNA Portal with Cisco 3
	Log In to Cisco Global Launchpad 4
	Log In Using IAM 4
	Log In Using Federated Identity 6
	Generate Federated User Credentials Using saml2aws 8
	Generate Federated User Credential Using AWS CLI 10
	Log Out 15
CHAPTER 3	Manage Regions 17
	Regions Overview 17
	Configure a Region 17
	Update a Region 18
	Remove a Region 19
CHAPTER 4	Manage VA Pods 21
	Edit a VA Pod 21
	Delete a VA Pod 23
CHAPTER 5	Manage Cisco Catalyst Center VAs 25
	View Catalyst Center VA Details 25
	Delete an Existing Catalyst Center VA 26

CHAPTER 6	Understand the Dashboard and User Activity Details	27
	View, Search, and Filter Dashboard Details	27
	View, Search, and Filter User Activity Details	29

CHAPTER 7	Manage Amazon Email Subscriptions, Logs, and Alarms	31
	Subscribe to the Amazon SNS Email Subscription	31
	Configure Log Retention	32
	Trigger a Root Cause Analysis	32
	AWS Config and Audit Log Details	34
	View Amazon CloudWatch Alarms	34

CHAPTER 8	Backup and Restore	37
	About Backup and Restore	37
	Backup and Restore—Hardware Appliance to VA	37
	Backup and Restore—VA to VA	38
	Configure Backup	39
	Restore a Backup	40
	Access the Catalyst Center Backup VM	40

CHAPTER 9	Operational Best Practices	41
	Encrypt Amazon EBS Volumes Attached to Catalyst Centers	41



CHAPTER 1

Cisco Global Launchpad Overview

- [Cisco Global Launchpad Overview, on page 1](#)

Cisco Global Launchpad Overview



Note Cisco DNA Center has been rebranded as Cisco 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 Global Launchpad provides you with the tools you need to install and manage your Catalyst Center Virtual Appliance (VA). It helps you create and manage the services and components that are required for the AWS cloud infrastructure.

For specific information about deploying Catalyst Center using Cisco Global Launchpad, see the [Cisco DNA Center on AWS Deployment Guide](#).



CHAPTER 2

Access Cisco Global Launchpad

- [Access Hosted Cisco Global Launchpad, on page 3](#)
- [Log In to Cisco Global Launchpad, on page 4](#)
- [Log Out, on page 15](#)

Access Hosted Cisco Global Launchpad

You can access Cisco Global Launchpad with 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.

Log In to the Cisco DNA Portal with Cisco

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

-
- Step 1** In your browser, enter:
- `dna.cisco.com/valaunchpad`**
- The **Cisco DNA Portal** login window is displayed.
- Step 2** Perform one of these actions:
- a) If you have a Cisco account, click **Log In With Cisco**.
 - b) If you do not have a Cisco account, click **Create a new account**. In the window that appears, enter the information for your account and click **Continue**. For more information, see [Creating a Cisco account](#).
- Step 3** Enter your Cisco account email in the **Email** field, and click **Next**.
- Step 4** Enter your Cisco account password in the **Password** field, and click **Log in**.
- The **VA Launchpad** page appears.
-

Log In to Cisco Global Launchpad

The Cisco Global Launchpad supports the following authentication methods:

- [Log In Using IAM, on page 4](#): This method uses the credentials from your Cisco account.
- [Log In Using Federated Identity, on page 6](#): Federated access ensures that an identity provider (IdP), such as your organization, is responsible for user authentication and sending information to Cisco Global Launchpad to help determine the scope of resource access to be granted after login. For the first-time login, the user will have an admin user role, which creates the CiscoDNACenter role. The admin can assign this role to subsequent users. The CiscoDNACenter role has the same permissions as the CiscoDNACenter user group. For details about the permissions granted by this role, see the [Cisco DNA Center on AWS Deployment Guide](#).

You can use the saml2aws CLI or the AWS CLI to generate tokens to log in to Cisco Global Launchpad as a federated user. For information, see the following topics:

- [Generate Federated User Credentials Using saml2aws, on page 8](#)
- [Generate Federated User Credential Using AWS CLI, on page 10](#)



Note Cisco Global Launchpad does not store your AWS credentials.

Log In Using IAM

This procedure shows you how to log in to Cisco Global Launchpad using identity and access management (IAM). If your company uses MFA, you can choose to log in using this method.



Note Do not open the application in more than one browser tab, in multiple browser windows, or in multiple browser applications at the same time.

Before you begin

Make sure the following requirements are met:

- Your AWS account has the administrator access permission assigned to it.
- Cisco Global Launchpad is installed or you have access to the hosted Cisco Global Launchpad.
- You have your AWS Access Key ID and Secret Access Key on hand.
- If your company uses multi-factor authentication (MFA), MFA needs to be set up in AWS before you log in. For information, see the [Enabling a virtual multi-factor authentication \(MFA\) device \(console\)](#) topic in the AWS documentation.

Step 1 From a browser window, do one of the following:

- If you installed Cisco Global Launchpad locally, enter the Cisco Global Launchpad URL in the following format:

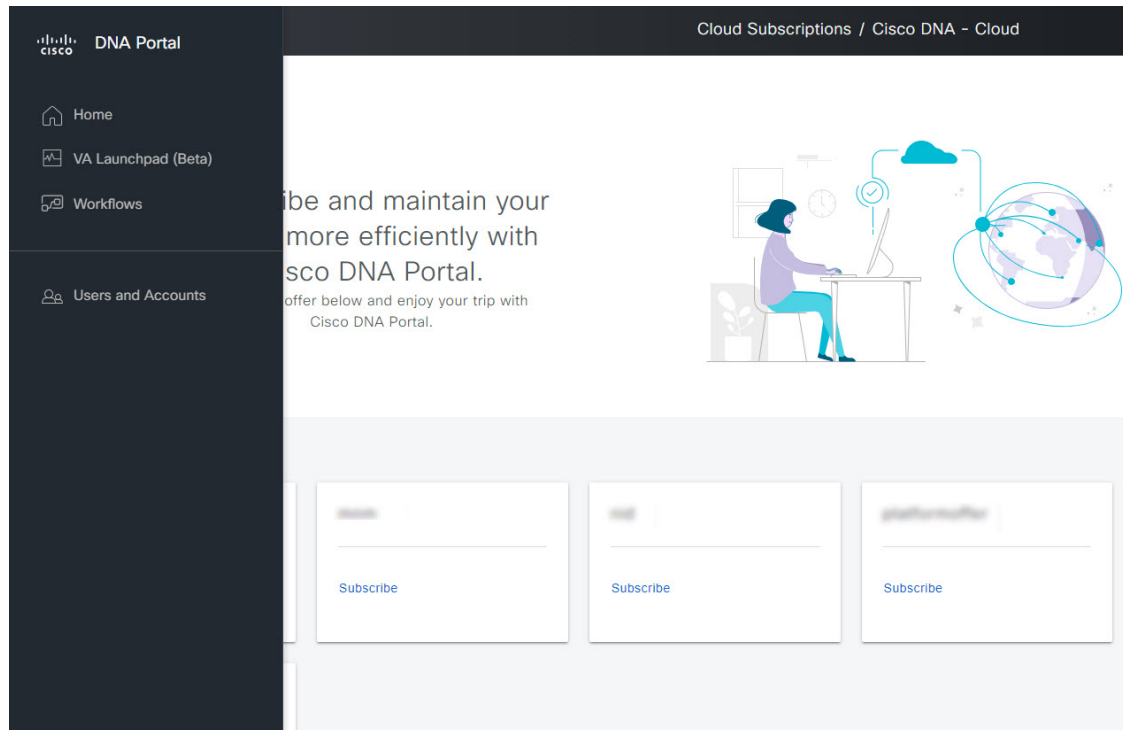
http://<localhost>:<client-port-number>/valaunchpad

For example:

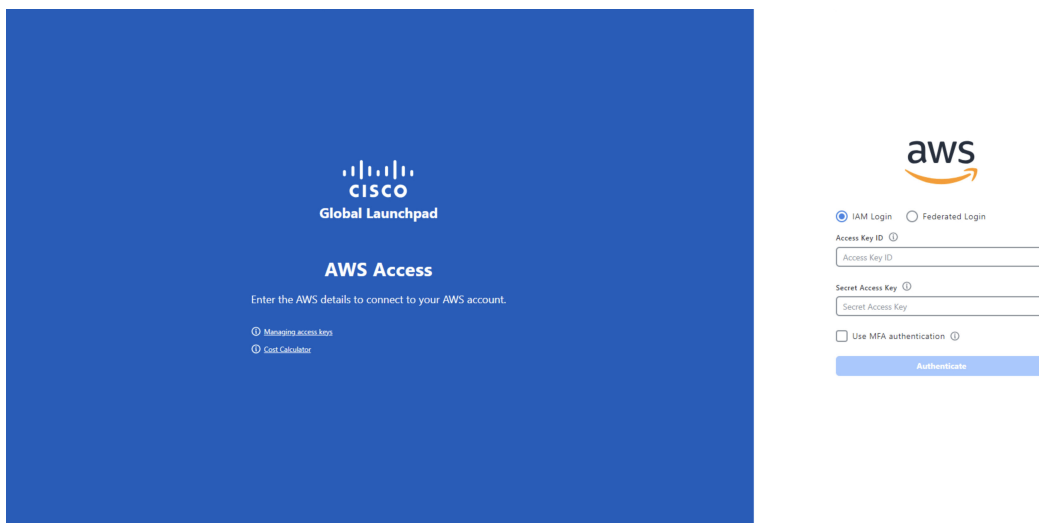
http://192.0.2.1:90/valaunchpad

- If you are accessing the hosted Cisco Global Launchpad, enter **dna.cisco.com** and follow the on-screen prompts to log in. (For information, see [Log In to the Cisco DNA Portal with Cisco, on page 3.](#))

From the **Cisco DNA Portal** home page, click the menu icon and choose **VA Launchpad**.



The AWS login window is displayed.



Step 2 Under the AWS logo, click the **IAM Login** radio button.

Step 3 Enter your credentials in the fields.

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.

Step 4 (Optional) If your company uses MFA, click the **Use MFA authentication** check box.

Step 5 Click **Authenticate**.

If you are logging in with MFA, choose your MFA device from the drop-down list and enter your MFA passcode.

After logging in successfully, the **Login Status** screen is displayed. This page displays the statuses of various operations that the system performs when you log in. Then the **Dashboard** pane is displayed and the us-east-1 region is selected by default.

Step 6 If you're prompted to update the region version, follow the prompts to complete the update. For more information, see [Update a Region, on page 18](#).

Step 7 If you encounter any login errors, you need to resolve them and log in again.

Log In Using Federated Identity

This procedure shows you how to log in to Cisco Global Launchpad using a federated identity.



Note Do not open the application in more than one browser tab, in multiple browser windows, or in multiple browser applications at the same time.

Before you begin

Make sure the following requirements are met:

- Your AWS account has the administrator access permission assigned to it. For information, see the [Cisco DNA Center 2.3.5 on AWS Deployment Guide](#).

- Cisco Global Launchpad is installed or you have access to the hosted Cisco Global Launchpad.
- You have your AWS Account ID, Access Key ID, and Secret Access Key on hand. For information about how to obtain these credentials, see [Generate Federated User Credentials Using saml2aws](#), on page 8 or [Generate Federated User Credential Using AWS CLI](#), on page 10.

Step 1

From a browser window, do one of the following:

- If you installed Cisco Global Launchpad locally, enter the Cisco Global Launchpad URL in the following format:

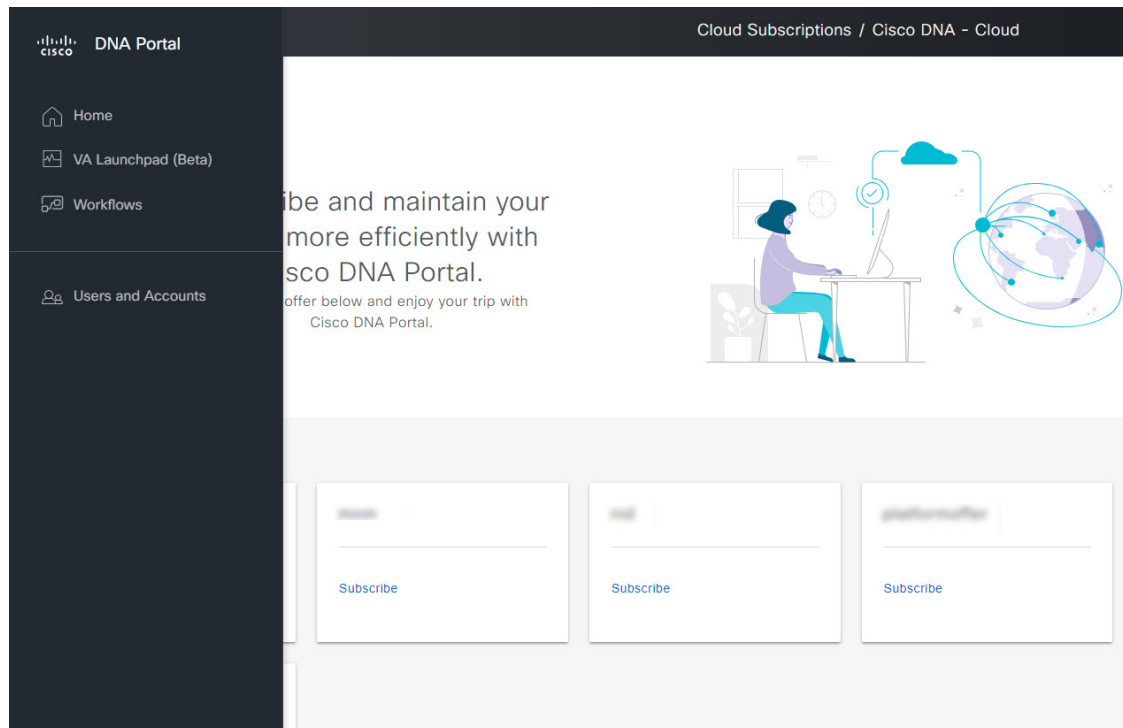
http://<localhost>:<client-port-number>/valaunchpad

For example:

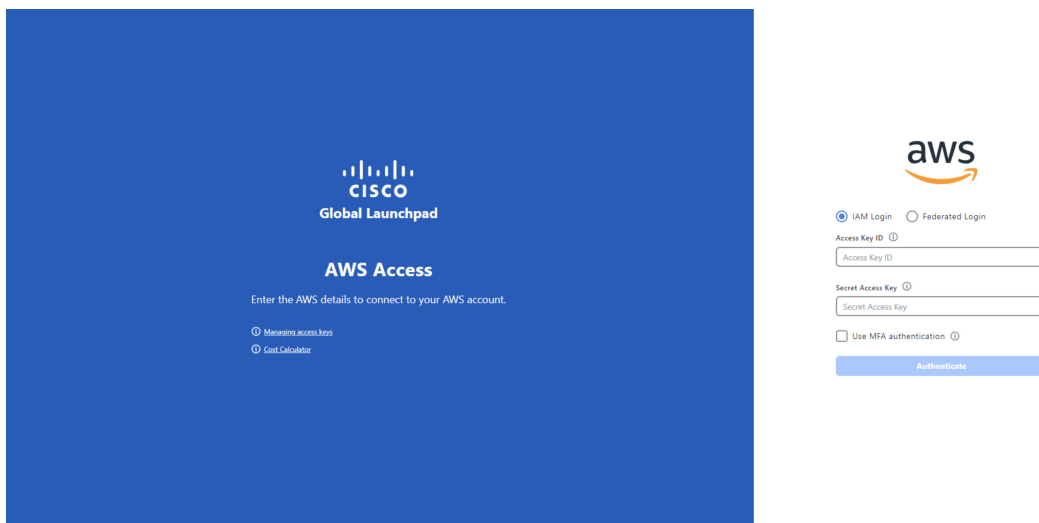
http://192.0.2.1:90/valaunchpad

- If you are accessing the hosted Cisco Global Launchpad, enter **dna.cisco.com** and follow the on-screen prompts to log in.

From the **Cisco DNA Portal** home page, click the menu icon and choose **VA Launchpad**.



The AWS login window is displayed.



Step 2 Under the AWS logo, click the **Federated Login** radio button.

Step 3 Enter your credentials in the fields.

For more information, see [Generate Federated User Credentials Using saml2aws, on page 8](#) or [Generate Federated User Credential Using AWS CLI, on page 10](#).

Step 4 Click **Authenticate**.

After you log in successfully, the **Login Status** screen is displayed. This page displays the statuses of various operations that the system performs when you log in. Then the **Dashboard** pane is displayed and the us-east-1 region is selected by default.

Step 5 If you're prompted to update the region version, follow the prompts to complete the update. For more information, see [Update a Region, on page 18](#).

Step 6 If you encounter any login errors, you need to resolve them and log in again. For more information, see the [Cisco DNA Center 2.3.5 on AWS Deployment Guide](#).

Generate Federated User Credentials Using saml2aws

You can generate temporary AWS credentials using a Command Line Interface (CLI) tool and use the generated credentials to log in to Cisco Global Launchpad.

Step 1 From the CLI, install saml2aws. For information, see the detailed instructions on [Github](#).

Step 2 Verify the installation by entering **saml2aws**.

If the installation is successful, the following output is displayed:

```

[redacted] ~ % saml2aws
usage: saml2aws [<flags>] <command> [<args> ...]

A command line tool to help with SAML access to the AWS token service.

Flags:
  --help                Show context-sensitive help (also try --help-long
                        and --help-man).
  --version             Show application version.
  --verbose             Enable verbose logging
  --quiet              silences logs
  -i, --provider=PROVIDER This flag is obsolete. See:
                        https://github.com/Versent/saml2aws#configuring-i
dp-accounts
  --config=CONFIG       Path/filename of saml2aws config file (env:
                        SAML2AWS_CONFIGFILE)
  -a, --idp-account="default" The name of the configured IDP account. (env:
                        SAML2AWS_IDP_ACCOUNT)
  --idp-provider=IDP-PROVIDER The configured IDP provider. (env:
                        SAML2AWS_IDP_PROVIDER)
  --mfa=MFA             The name of the mfa. (env: SAML2AWS_MFA)
  -s, --skip-verify     Skip verification of server certificate. (env:

```

Step 3 Configure your account.

- Enter **saml2aws configure**.
- At the **Please choose a provider** prompt, use the up- or down-arrow keys to choose a provider or enter the provider name. When done, press **Enter**.
- At the **AWS Profile** prompt, press **Enter** to use the default AWS profile.
- At the **URL** prompt, enter the URL of your identity provider (IdP) and press **Enter**.

Note You can get this information from your IdP.

- At the prompts, enter your username and password and press **Enter**.

Step 4 Generate your federated credentials.

- Enter **saml2aws login**.
- At the prompts, enter your username and password.
- At the prompt, select either the **Admin** or **CiscoDNACenter** role and press **Enter**.

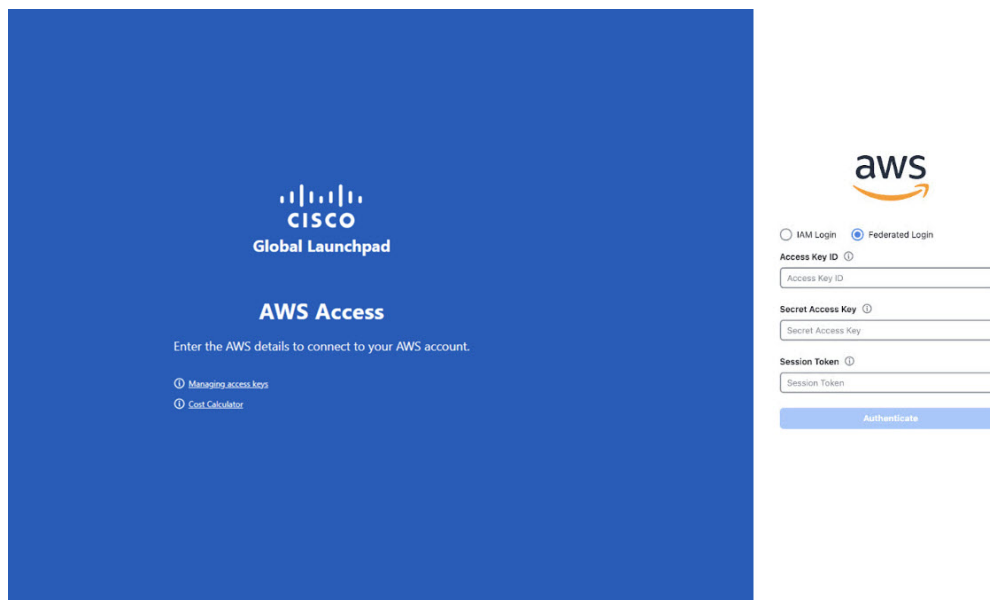
Note Ensure that the tokens created for these roles have a minimum expiry of 180 minutes (3 hours).

Your credentials are generated and stored in `~/aws/credentials`.

Step 5 Download the credentials by entering **saml2aws script**.**Step 6** Note the values of the following parameters as you will use them to log in to Cisco Global Launchpad as a federated user:

- `AWS_ACCESS_KEY_ID`
- `AWS_SECRET_ACCESS_KEY`
- `AWS_SESSION_TOKEN`

Step 7 On the Cisco Global Launchpad login window, select **Federated Login** and enter the generated credentials in the corresponding fields.



CISCO
Global Launchpad

AWS Access

Enter the AWS details to connect to your AWS account.

① Managing access keys
① Cost Calculator

aws

☐ IAM Login ☒ Federated Login

Access Key ID ①

Access Key ID

Secret Access Key ①

Secret Access Key

Session Token ①

Session Token

Authenticate

Generate Federated User Credential Using AWS CLI

You can generate temporary AWS credentials using the AWS Command Line Interface (CLI) and use these credentials to log in to Cisco Global Launchpad.

Step 1 In a browser window, navigate to the **AWS Single Sign On (SSO)/Active Directory (AD)** window.

Step 2 In the **AWS Single Sign On (SSO)/Active Directory (AD)** window, click the AWS Console link.

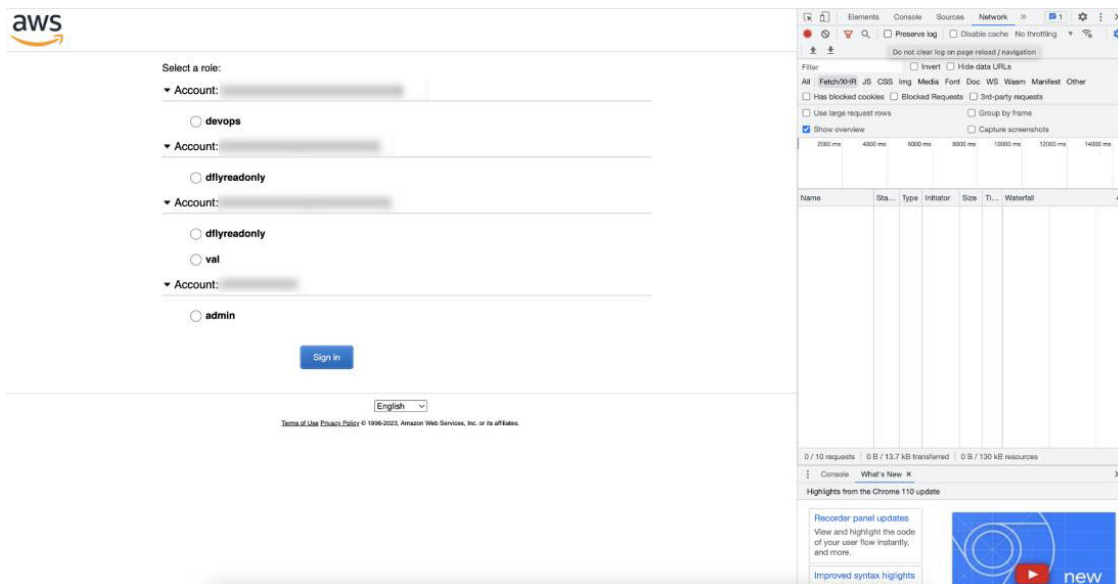
The following window is displayed.

Step 3

Right-click anywhere in the window, and from the drop-down menu, choose **Inspect Element** or **Inspect** (depending on the browser).

Note You can also press the **F12** key to open the **Developer Tools** panel.

The **Developer Tools** panel is displayed, similar to the following window.

**Step 4**

In the **Developer Tools** panel, click the **Network** tab and check the **Preserve Log** check box. (This option can be found on the tool panel, right beside the Magnifying Glass icon.)

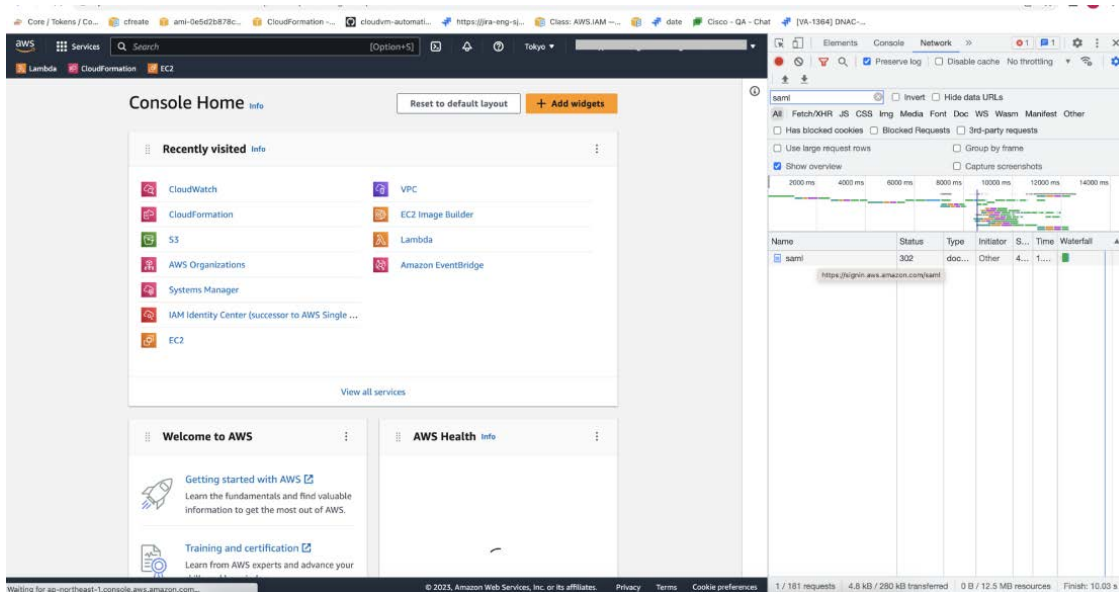
Step 5

In the **AWS Console**, click **Sign In**.

Step 6

In the **Developer Tools** panel, filter the required API calls by entering **saml** in the **Filter** field.

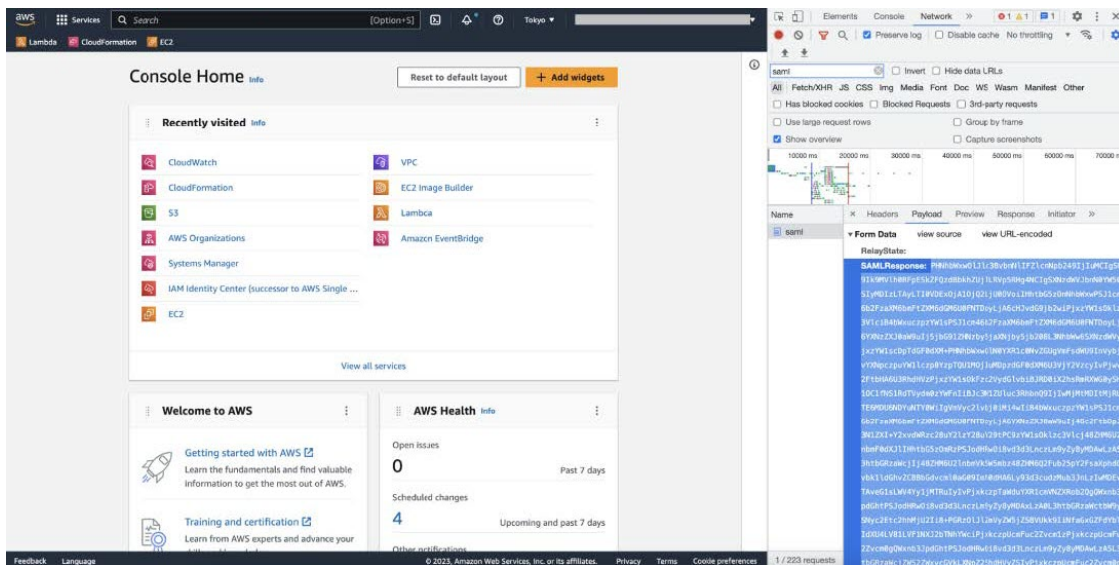
Generate Federated User Credential Using AWS CLI



Step 7 Click the API request named **saml**.

Step 8 Click the **Payload** tab.

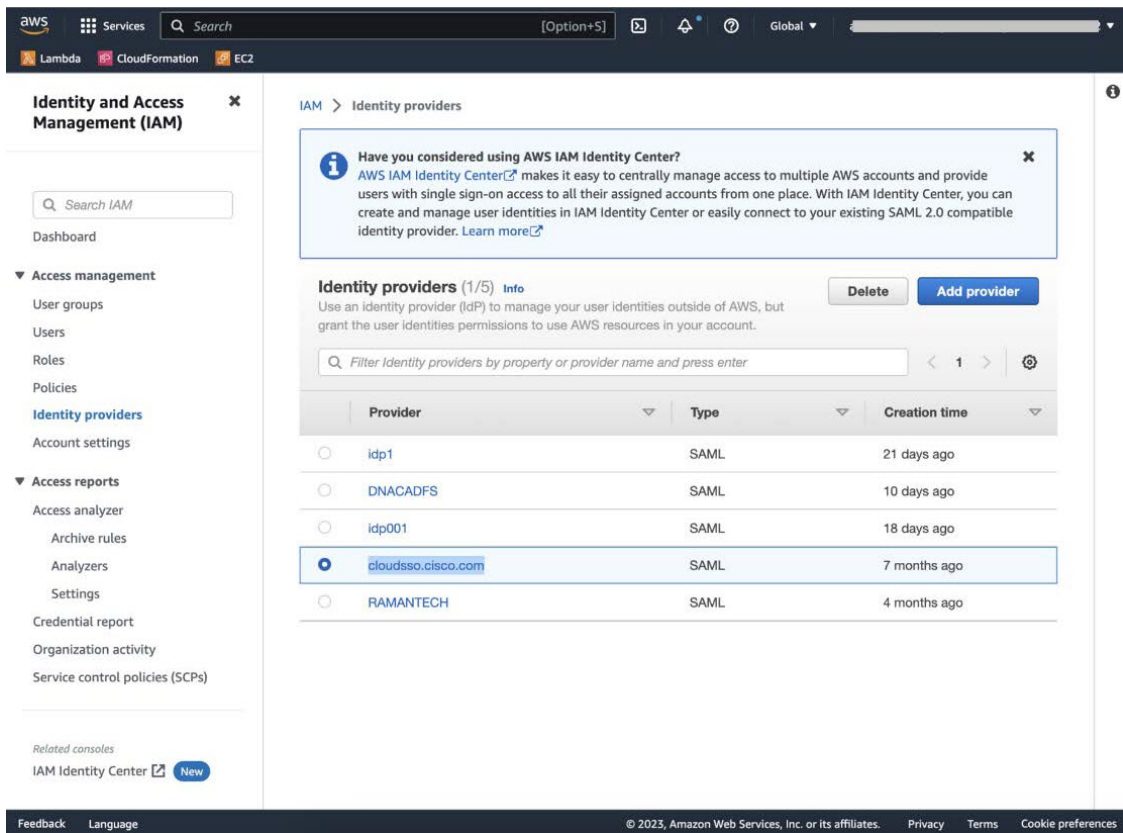
The saml API response is displayed under the Form Data tab.



Step 9 Copy the value of the SAML response.

Note Be sure to copy the entire value, but do not copy the SAMLResponse field name.

Step 10 Navigate to your AWS Console, choose **IAM > Access Management > Identity Providers**, and select your IdP.



Step 11 Obtain the following details for your IdP:

- Role assigned to the IdP
- Amazon Resource Name (ARN) of the IdP

Step 12 From the AWS CLI, enter the following command:

```
aws sts assume-role-with-saml --role-arn <Role-Arn> --principal-arn <IDP-Arn> --saml-assertion <SAML response>
```

The variables in this command refer to the values obtained earlier, as follows:

- **<Role-Arn>**: Role assigned to the IdP, obtained in Step 11.
- **<IDP-Arn>**: Amazon Resource Name (ARN) of the IdP, obtained in Step 11.
- **<SAML response>**: Value of the SAML response, obtained in Step 9.

For example:

```
aws sts assume-role-with-saml --role-arn
arn:aws:iam::059356109852:role/ADFS-AWS-ADMIN --principal-arn
arn:aws:iam::059356109852:saml-provider/cloudsso.cisco.com --saml-
assertion
MIIC6jCCAdKgAwIBAgIQPP5He1K6QoZPQRiUPjzCUTANBgkqhkiG9w0BAQsFADAxMS8wLQY
DVQDEyZBREZTIFNpZ25pbmcgLSEFQzJBTUFaLU1IMUYzQ0Quc3NvLmNvbTAeFw0yMzAyMDY
wNTUyNDJaFw0yNDYyMDYwNTUNDJAMDExLzAtBgNVBAMTJkFERlMgU2lnbmluZyAtIEVDMkF
NQVotTUgXRjNDRC5zc28uY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAsl
Sx/rQJ/wAOJ6ZRBbgYkfe7TMPsnOTqX0C+dh+yQ3O+X9xqRDPVKuSDHrv72bsGwk/
2VRdb38xdVueuFYRavyVPzjsSF95fkjC3qFDN+R5Dk1Cnba7GT6i+HGfacEpL8Vqd3jzNgh
guskM1OrHDHKDv5ksNMxppHIDPlVhyRCdKEtP1PG5gBftoKvBZX+RxYcTaVUK/
NrMfkWmklyQTNRmpUDj+NawGGjr4byjH8hUu59cFJetatzJo8qxuWWtPBtd+ESs/
DVR5dpilfyEBi4Dc22X91kOShJpeDuO8EGfR6O5/nmRErlyy/p5f2sPKM0/
ix+XlQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQA7kt4HeU/
zohOSDnnfmXYpYi8WrJFxmVTS6CjwE8eYZ6BwByEI4PjxcjPOu+sVNxrtBzJUwyPM+LKKMs
zYn5VQ/skrwcljW5P4msUMj4/J5K4vuYcKbJS4VyASKVZmWUWC23WhpC3U8ft6F7Jynp/
omrEh6Xrc4f4SqFdvIz35h2Sd/
HbcDp+sH2zm4TgnA2XuSuvv0NJPf2VsRHMCMsn3eBTQfbbD5naLEpitjU8Zy5qW+Ic8Up5l
ATNzPP+kmaQY6SxPLeuAarrnp4vDrD7hpzhneRfWX8h9v/Fg+wlnOsEeD1FYyLRoc
```

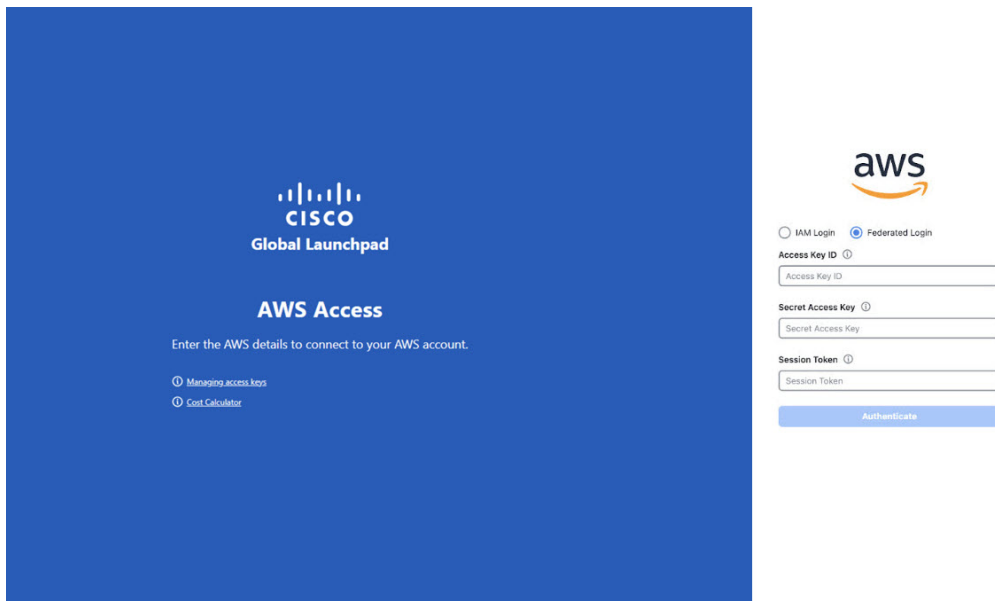
Output similar to the following output is displayed:

```
{
  "Credentials": {
    "AccessKeyId": "xxxx",
    "SecretAccessKey": "xxxxx",
    "SessionToken": "xxxxxxxxxx",
    "Expiration": "2023-03-10T18:07:15+00:00"
  },
  "AssumedRoleUser": {
    "AssumedRoleId": "xxx:user@sso.com",
    "Arn": "arn:aws:sts::059356109852:assumed-role/ADFS-AWS-ADMIN/user@sso.com"
  },
  "Subject": "SSO\\USER",
  "SubjectType": "transient",
  "Issuer": "http://EC2AMAZ-MH1F3CD.sso.com/adfs/services/trust",
  "Audience": "https://signin.aws.amazon.com/saml",
  "NameQualifier": "POIUYTRFVNMKJGFKJHJHJcYLQCePSAZg="
}
```

Step 13 Note the values of the following generated credentials:

- AccessKeyId
- SecretAccessKey
- SessionToken

Step 14 On the Cisco Global Launchpad login window, select **Federated Login** and enter the generated credentials from Step 13 in the corresponding fields.



Log Out

Depending on how you accessed your Cisco Global Launchpad account, you either need to log out of only Cisco Global Launchpad or both Cisco Global Launchpad and Cisco DNA Portal.

Step 1 To log out of Cisco Global Launchpad, do the following:

- a. In the left navigation pane, click **Log out**.
- b. In the **Confirmation** dialog box, click **Log Out**.

Step 2 (Optional) If you accessed Cisco Global Launchpad through Cisco DNA Portal, you must also log out of Cisco DNA Portal. Do the following:

- a) In the upper-right corner of the Cisco DNA Portal GUI, click your displayed username.
- b) Click **Log Out**.



CHAPTER 3

Manage Regions

- [Regions Overview, on page 17](#)
- [Configure a Region, on page 17](#)
- [Update a Region, on page 18](#)
- [Remove a Region, on page 19](#)

Regions Overview

A region is an isolated area containing dedicated resources. To achieve the greatest possible fault tolerance and stability, resources are not shared or replicated in other regions.

A region is created when you create the first VA pod in that region. After a region has been created, you can add more VA pods to it. A region is created based on its AWS configuration template. Whenever AWS updates a region template version, Cisco Global Launchpad notifies you that you need to update the corresponding region in Cisco Global Launchpad. You are notified of the region version update when you first log in to Cisco Global Launchpad or when you change the region view.

When you delete all the VA pods from a region, the region is not automatically deleted. Cisco Global Launchpad permits empty regions. You can always create other VA pods in it later. However, if you no longer want to use an empty region and you want to delete it, you must do so manually using Cisco Global Launchpad.

Configure a Region

A region is created when you create the first VA pod in that region. After a region has been created, you can add more VA pods to it. The region configuration is based on its AWS template.

You can choose a region from the list of supported regions in Cisco Global Launchpad.

Before you begin

Confirm with your AWS administrator that the relevant regions are enabled in AWS. On Cisco Global Launchpad, the **Region** drop-down list only displays enabled regions.

Step 1 On the **Dashboard** pane, if you're prompted to update the region version, follow the prompts to complete the update.

Note You must update a region when an updated version is available. Cisco Global Launchpad automatically checks if an updated region version is available whenever you log in or change the selected region. If an updated region version is detected, Cisco Global Launchpad prompts you to update it. Follow the on-screen prompts. For information, see [Update a Region, on page 18](#).

The update may take a few minutes. Do not close the tab or window until the process has completed.

If the update fails, Cisco Global Launchpad restores the region to the last working version and displays an error. In this case, contact Cisco TAC for assistance.

Step 2 In the left navigation pane, from the **Region** drop-down list, choose a region from the list.

Note Only enabled regions are displayed in the **Region** drop-down list.

- 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)

Step 3 After you choose a region, if you're prompted to update it, follow the prompts to complete the update. For information, see [Update a Region, on page 18](#).

Update a Region

Whenever you log in or change the selected region, Cisco Global Launchpad automatically checks if an updated region is available. If an updated region is detected, Cisco Global Launchpad prompts you to update it.

If you choose to update the region, click **Upgrade Now** and follow the prompts. The update may take a few minutes. Do not close the tab or window until the process has completed. If the update succeeds, click **Ok** to

continue. If the update fails, Cisco Global Launchpad restores the region to the last working version and displays an error. In this case, contact Cisco TAC for assistance.

If you choose not to update the region, click **Do It Later**. Note that if you choose not to update the region, you may experience issues with the VA pod operation.

Remove a Region

When there are no VA pods in a region and you want to delete the region, complete the following procedure.



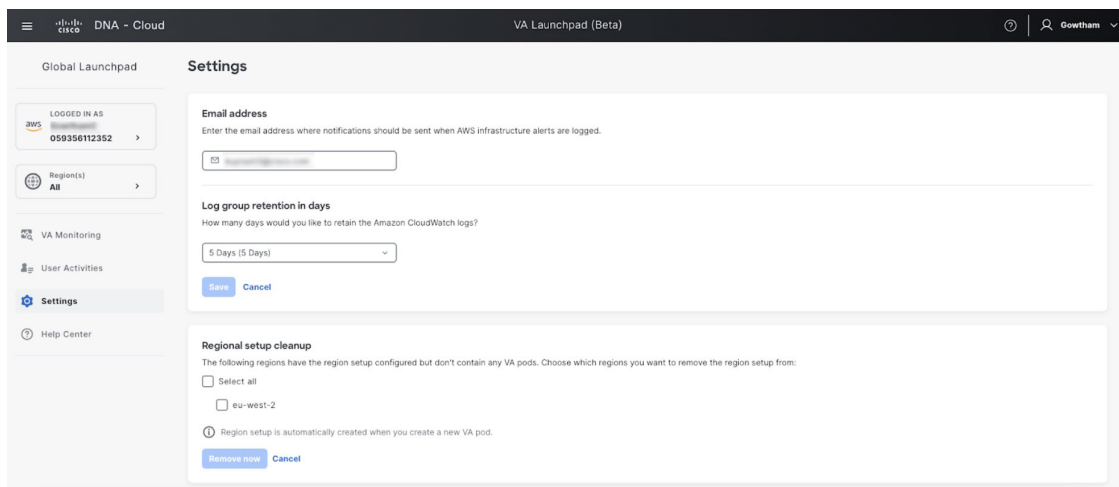
Note

When the last VA pod is deleted in a region, the region itself isn't deleted. This means that + **Create New VA Pod** will remain enabled, allowing you to create new VA pods in the region.

Step 1 Make sure that all VA pods in the selected region are deleted. For information, see [Delete a VA Pod, on page 23](#).

Step 2 In the left navigation pane, click the settings icon (⚙️).

The **Settings** pane is displayed.



Step 3 In the **Regional setup cleanup** area, check the check box for each region that you want to remove, then click **Remove now**.

The removal process can take up to a minute. You can't create any new VA pods during this process.

When the region is deleted, a successful notification message is displayed.

Note When you create a new VA pod in the selected region for the first time, a new region is created automatically.



CHAPTER 4

Manage VA Pods

- [Edit a VA Pod, on page 21](#)
- [Delete a VA Pod, on page 23](#)

Edit a VA Pod

You can edit your VA pod only if you chose **VPN GW** as your preference while creating the VA pod.



Note While editing a VA pod, you will not receive email notifications about the VA pod because Amazon EventBridge (an AWS service that's used to trigger email notifications) is disabled. When the VA pod edits are configured successfully, you'll receive email notifications about this VA pod again because Amazon EventBridge is re-enabled.

For information about creating a VA pod, see "Create a New VA Pod" in the [Cisco DNA Center 2.3.5 on AWS Deployment Guide](#).

Step 1 On the **Dashboard** pane, locate the VA pod that you want to edit.

Step 2 In the bottom-right corner of the VA pod card, click the ellipsis icon (...) and choose **Edit VA Pod**.

Step 3 In the **Modify VPN Details** page, make the relevant edits:

a) Update any of the following VPN details. For information, see "Create a New VA Pod" in the [Cisco DNA Center 2.3.5 on AWS Deployment Guide](#).

- CGW (Enterprise Firewall/Router)

Note Make sure that the Customer Gateway IP is a valid public address.

- VPN Vendor
- Platform
- Software

b) Click **Next**.

Step 4 Review the edited details, and when you're ready, click **Proceed to On-Prem Configuration**.

Step 5 Configure the on-premises connectivity.

- a) From the **Configure On-premise** screen, click **Download Configuration File**.
- b) Forward this file to your network administrator to configure the on-premises-side IPsec tunnel.

The network administrator can make the necessary changes to this file and apply this configuration to your Enterprise firewall or router to bring up IPsec tunnels.

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

Step 6 Check the status of your network configuration.

When your network administrator is configuring the IPsec tunnel, the IPsec tunnel configuration status displays as not configured with a padlock icon.



When your network administrator completes the configuration and the IPsec tunnel configures successfully, the IPsec tunnel configuration status displays green with a success icon.



Step 7 (Optional) To return to the **Dashboard** pane, click **Go to Dashboard**.

Delete a VA Pod

You can delete a VA pod on Cisco Global Launchpad.

**Note**

- You can't delete a VA pod while you are deleting a Catalyst Center VA that is in the pod. You must wait for the Catalyst Center VA to be deleted first.
- Deleting a VA pod doesn't delete the following resources because these resources are retained by Global Launchpad for use by other VA pods:
 - Transit gateway (TGW)
 - TGW route table
 - Customer gateway (CGW)
 - VPN connection

If you want to delete these resources, delete them manually. In this case, ensure that the resources are properly deleted to maintain the integrity of your network infrastructure and enable resources to be properly managed and optimized.

Step 1 On the **Dashboard** pane, locate the VA pod.

Step 2 In the bottom-right corner of the VA pod card, click the ellipsis icon (...) and choose **Delete VA Pod**.

Note If a Catalyst Center VA in a VA pod is in the process of being deleted, the **Delete VA Pod** option is not available.

Step 3 In the **Confirmation** dialog box, in the text field, type **DELETE**.

Step 4 Click **Delete** to confirm that the deletion of the VA pod.

Deleting a VA pod takes approximately 20 to 40 minutes.



CHAPTER 5

Manage Cisco Catalyst Center VAs

- [View Catalyst Center VA Details, on page 25](#)
- [Delete an Existing Catalyst Center VA, on page 26](#)

View Catalyst Center VA Details

You can view Catalyst Center VA details in Cisco Global Launchpad.

- Step 1** On the **Dashboard** pane, locate the VA pod containing the Catalyst Center VA you want to view, and in the VA pod card, click **Create/Manage Cisco Catalyst Center(s)**.
- Step 2** In the bottom-right corner of the Catalyst Center VA card, click the ellipsis icon (...) and choose **View Details**.
- Step 3** In the **View Catalyst Center** pane, view information, such as the Catalyst Center domain FQDN and network proxy.

The screenshot shows the 'View Catalyst Center Details' page in the Cisco Global Launchpad. The page is divided into several sections:

- Domain details:**
 - Enterprise DNS: [View details](#)
 - FQDN (Fully Qualified Domain Name): dnac.example.com
- Proxy details:**
 - Customer HTTPS network proxy: No proxy
- Other details:**
 - Catalyst Center version: 2.3.5.3
 - Catalyst Center URL: [View details](#)
 - Catalyst Center AMI: ami-0d2d9e5eb058de8f7
 - Cloud backup server IP: [View details](#)
 - Rsync: /var/catalyst-backup
 - NFS share: /var/infShare
 - Created by: Prashant
 - Created date: Apr 29 2024 03:58 PM
- VA Pod details:**
 - Environment details:
 - VA pod name: TestNewTgw
 - Region: ap-southeast-2
 - Availability zone: ap-southeast-2a
 - AWS VPC CIDR: 10.10.0.0/25
 - On-premises connectivity:
 - Transit gateway (TGW): New VPN GW + New TGW
 - VPN attachment:
 - Attachment type: New VPN GW
 - VPN details:
 - Customer gateway IP: 18.197.49.204
 - VPN vendor: Openswan
 - Platform: Openswan
 - Software: Openswan 2.6.38+
 - Other details:
 - Customer profile: Medium
 - Backup target: Cloud backup
 - Created by:

- Step 4** (Optional) To exit this window, click **Back to Catalyst Center(s)**.

Delete an Existing Catalyst Center VA

You can delete an existing Catalyst Center VA from Cisco Global Launchpad.

-
- Step 1** On the **Dashboard** pane, locate the VA pod containing the Catalyst Center VA you want to delete, and in the VA pod card, click **Create/Manage Cisco Catalyst Center(s)**.
 - Step 2** In the bottom-right corner of the Catalyst Center VA card, click the ellipsis icon (...) and choose **Delete Cisco Catalyst Center**.
 - Step 3** In the **Confirmation** dialog box, in the text field, type **DELETE**.
 - Step 4** Click **Delete** to confirm that the deletion of the Catalyst Center VA.
-



CHAPTER 6

Understand the Dashboard and User Activity Details

- [View, Search, and Filter Dashboard Details, on page 27](#)
- [View, Search, and Filter User Activity Details, on page 29](#)

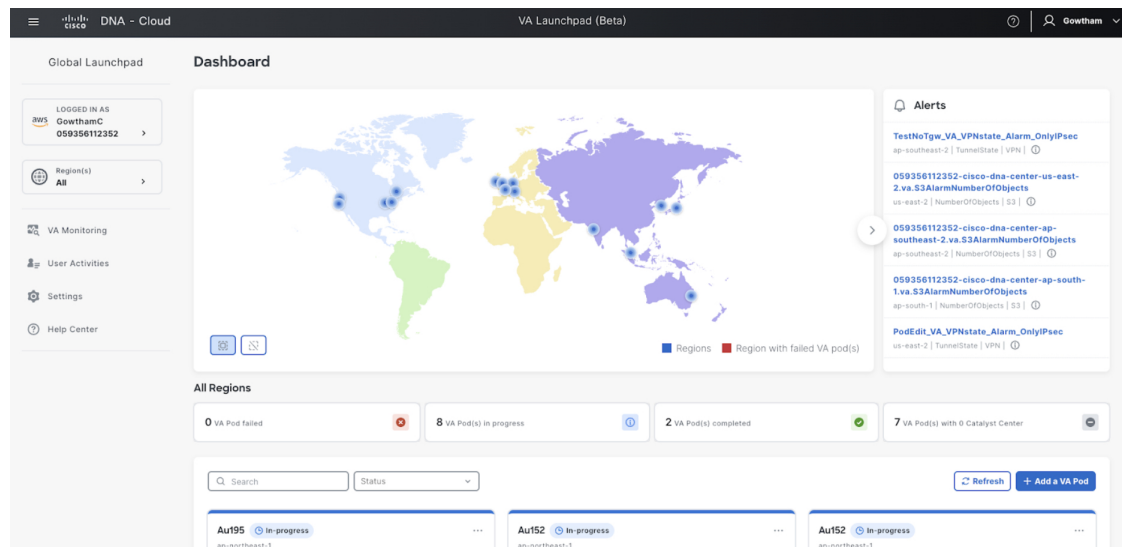
View, Search, and Filter Dashboard Details

The **Global Dashboard** pane provides insights into all deployed VA pods and Catalyst Center VAs across all available regions.

Step 1

After you log in, the **Dashboard** pane is displayed and the us-east-1 region is selected by default.





At the top of the **Dashboard** is a global map that displays the available regions. On the map, a blue region icon indicates an available region. A red blinking region icon indicates a region with a failed VA pod creation. Below the map, a card is displayed for each VA pod in the selected region.



Step 2

From the left navigation pane, click the **Region** drop down list and check the check box next to the region or regions you want to view. Check the **Select All** check box to display information about all the regions.

Step 3 From the **Dashboard** pane, you can perform the actions described in the following table:

Action	Steps
Select or deselect regions.	<p>In the map, do one of the following:</p> <ul style="list-style-type: none"> To select a single region, click its icon on the map. To deselect it, click the same icon again. To select multiple regions, click the relevant region icons. To deselect multiple regions, click the regions that you want to deselect. To select all regions, click the  icon. To deselect all regions, click the  icon.
Display region details.	<p>a. On the map, hover your cursor over a region icon (). The region's name is displayed.</p> <p>b. On the map, select one or more regions. For details, see the Select regions action in this topic.</p> <p>When selected, a region icon () is shown . Details about the selected regions are displayed:</p> <ul style="list-style-type: none"> VA Pods Failed: Number of failed VA pods VA Pods In Progress: Number of VA pods in the process of being created. VA Pods Completed: Number of VA pods that have completed the creation process. VA Pods that have Catalyst Centers: Number of VA pods that have Catalyst Center VAs and the total number of Catalyst Center VAs among them. <p>VA pod information is displayed in the card view below the map.</p>
Display detailed information about critical alerts.	<p>In the Alerts area, which displays alerts that are in the ALARM state:</p> <ul style="list-style-type: none"> Click the name of an alert to display the corresponding AWS CloudWatch Alarm page. Hover your cursor over the Info icon to display the reason that the alert was generated.
Search for a VA pod.	<p>a. In the Search by VA Pod Name field, enter either the partial or full name of the VA pod.</p> <p>b. Press the Enter key.</p> <p>The Dashboard pane displays the VA pods in the card view below the map, and the status highlights are updated.</p>

Action	Steps
Filter by region and VA pod status.	From the VA Pod Status drop-down list, choose a VA pod status. The Dashboard pane displays the filter results based on the chosen status.
Update VA pod status.	To fetch the latest status of the VA pods, click Refresh . The Dashboard pane updates the status highlights and the information displayed in the VA pod card view.

View, Search, and Filter User Activity Details

On the **User Activities** pane, you can view, search for, and filter all the user activity details for one or more chosen regions.

Step 1 From the left navigation pane, click the **Region** drop-down list and check the check box next to the region or regions that you want to view user activity details for. Check the **Select All** check box to display user activity information about all the regions.

Step 2 In the left navigation pane, click **User Activities**.

The **User Activities** pane displays in a table format.

Global Launchpad

User Activities

Search on Activity Select Start Date Select End Date All Users Refresh Download

Created Date & Time	Region	Activity	User
14 Nov 2023 22:01	us-west-2	VA Pod TEST10 has been created successfully.	demo-aws
14 Nov 2023 22:01	us-west-2	VA Pod TEST10 has been created successfully.	demo-aws
14 Nov 2023 22:01	us-west-2	VA Pod TEST10 has been created successfully.	demo-aws
14 Nov 2023 22:00	us-west-2	VA Pod TEST10 has been created successfully.	demo-aws
14 Nov 2023 22:00	us-west-2	VA Pod TEST10 has been created successfully.	demo-aws
14 Nov 2023 22:00	us-west-2	VA Pod TEST10 has been created successfully.	demo-aws
14 Nov 2023 22:00	us-west-2	VA Pod TEST10 has been created successfully.	demo-aws
14 Nov 2023 22:00	us-west-2	VA Pod TEST10 has been created successfully.	demo-aws
14 Nov 2023 22:00	us-west-2	VA Pod TEST10 has been created successfully.	demo-aws
14 Nov 2023 22:00	us-west-2	VA Pod TEST10 has been created successfully.	demo-aws

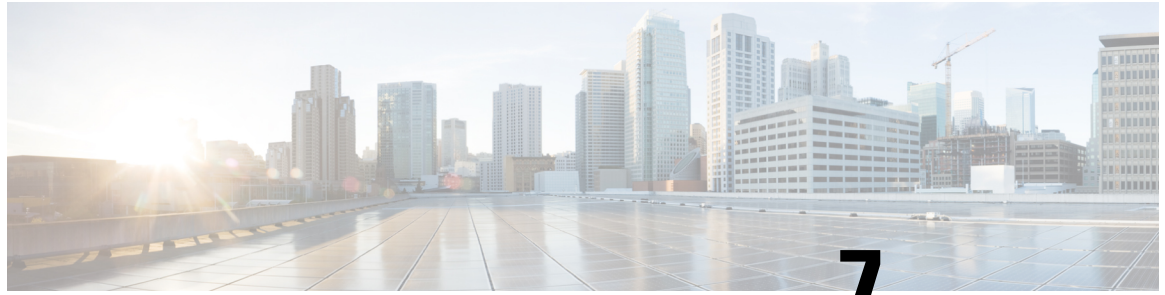
Rows per page 10 < 1 2 3 4 5 ... 40 >

Global Launchpad 1.6.0 - © 2023 Cisco Systems, Inc. Privacy policy Terms of service

Step 3 On the **User Activities** pane, you can view, search, and filter the data in the **User Activities** table by doing the following:

- To search for an activity, use the **Search on Activity** bar.

- To filter for an activity by date, click **Select Start Date** to choose a start date and click **Select End Date** to choose an end date.
 - To filter for an activity by user, from the **All User** drop-down list, choose a user account.
 - To update the data displayed, click **Refresh**.
 - To download all the user activity data as a CSV file, click **Download**.
-




CHAPTER 7

Manage Amazon Email Subscriptions, Logs, and Alarms

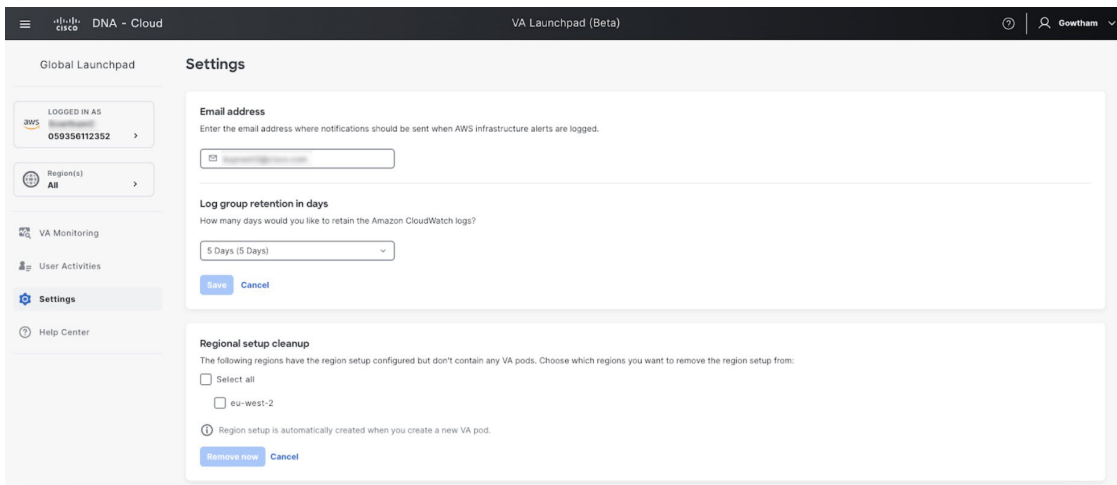
- [Subscribe to the Amazon SNS Email Subscription, on page 31](#)
- [Configure Log Retention, on page 32](#)
- [Trigger a Root Cause Analysis, on page 32](#)
- [AWS Config and Audit Log Details, on page 34](#)
- [View Amazon CloudWatch Alarms, on page 34](#)

Subscribe to the Amazon SNS Email Subscription

To receive email notifications from Amazon Simple Notification System (SNS), you can subscribe to the Amazon SNS email subscription in Cisco Global Launchpad settings. Amazon SNS sends AWS alerts about deployed resources, changes, or resource over-utilization to the provided email.

Step 1 In the left navigation pane, click the settings icon (.

Step 2 In the **Settings** pane, in the **Email to notify** area, enter the preferred email address in the **Email ID** field.



The screenshot shows the Cisco Global Launchpad interface. The top navigation bar includes the Cisco logo, 'DNA - Cloud', and 'VA Launchpad (Beta)'. The left sidebar shows the 'Settings' icon selected. The main content area is titled 'Settings' and contains three sections:

- Email address:** A text input field for the email address where notifications should be sent when AWS infrastructure alerts are logged.
- Log group retention in days:** A dropdown menu set to '5 Days (5 Days)' with a 'Save' button and a 'Cancel' button.
- Regional setup cleanup:** A section with a checkbox for 'Select all' and a checkbox for 'eu-west-2'. Below these is a note: 'Region setup is automatically created when you create a new VA pod.' and buttons for 'Remove now' and 'Cancel'.

When you update an email ID, the old email address is unsubscribed and the new email address is subscribed. Alerts about VA pods that are created after the email change are sent to the new email address. Alerts about existing VA Pods are not sent to the new email address.


If an existing user account has not confirmed their email subscription and updates their subscription with a new email address, both the old and new email addresses are subscribed and remain configured in Amazon SNS.

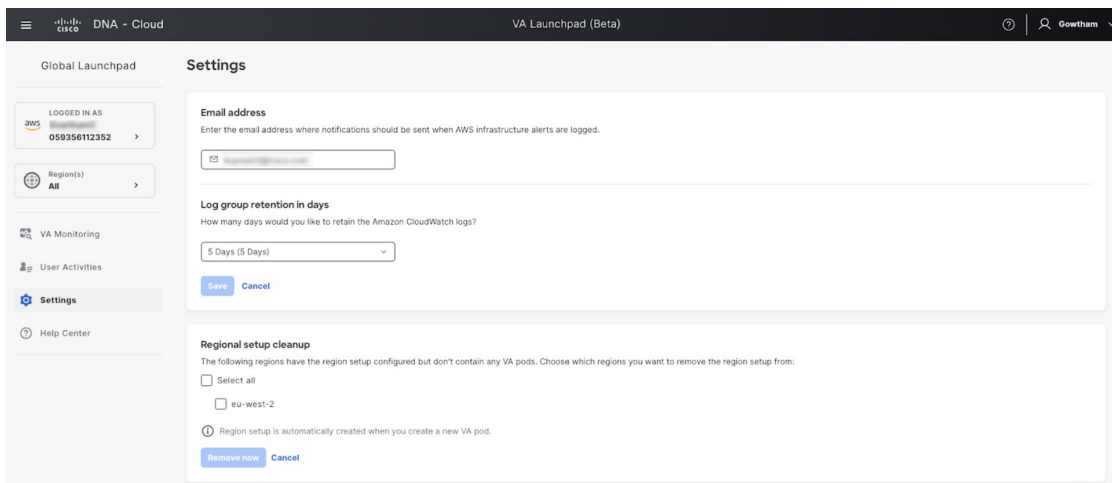
Note Multiple user accounts should not concurrently update their email ID. If this occurs, the latest updated email ID is used for email notification.

Step 3 Click **Save**.

Configure Log Retention

You can set the number of days to keep Amazon CloudWatch logs. By default, the logs are kept indefinitely.

Step 1 In the left navigation pane, click the settings icon ().
The **Settings** pane is displayed.



Step 2 Under **Log Group Retention In Days**, click the **Select Log Group Retention In Days** drop-down list and choose a retention period for the Amazon CloudWatch logs.

Step 3 Click **Save**.

Trigger a Root Cause Analysis

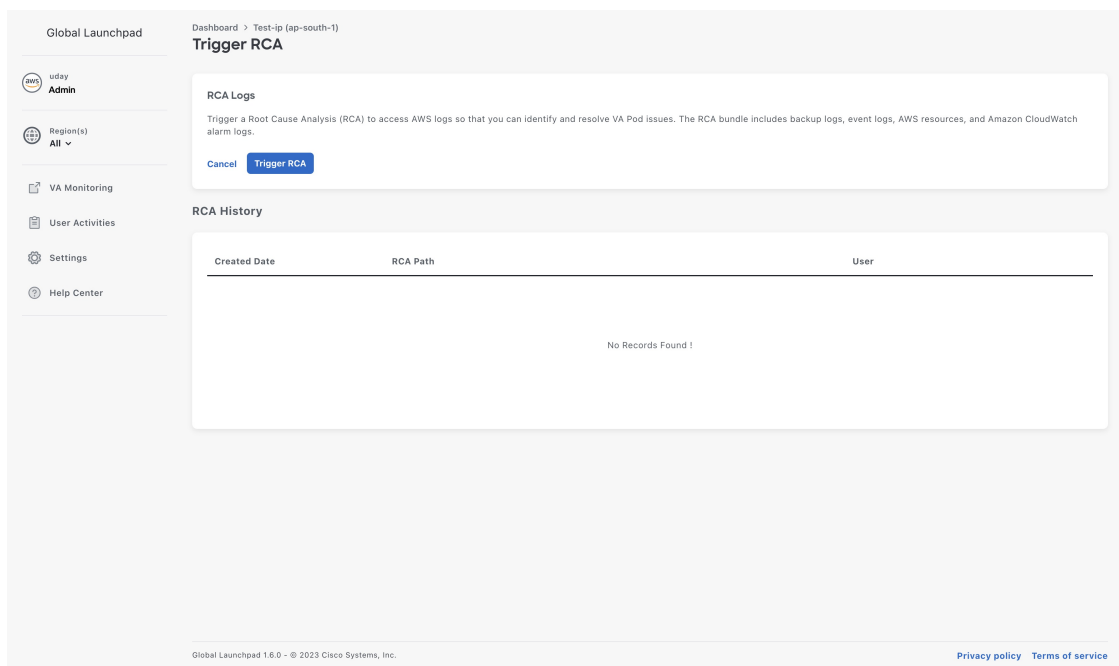
On Cisco Global Launchpad, you can trigger a root cause analysis (RCA) to help you identify the root cause of AWS infrastructure or Catalyst Center VA deployment issues. The RCA operation collects logs from AWS

and stores them in the AWS S3 bucket. The RCA bundle includes backup logs, backend logs, Amazon CloudWatch alarm logs, and AWS resources and event logs.

- Step 1** On the **Dashboard** pane, locate the VA pod containing the Catalyst Center VA that you want to trigger an RCA on, and in the VA pod card, click **Create/Manage Cisco Catalyst Center(s)**.
- Step 2** In the bottom-right corner of the Catalyst Center VA card, click the ellipsis icon (...) and choose **Trigger RCA**.
- Step 3** In the **Trigger RCA** window, in the **RCA Logs** area, click **Trigger RCA** to gather and bundle the AWS logs.

Cisco Global Launchpad uses AWS Config and Amazon CloudWatch to record, assess, and audit the used resources.

Note In the **Trigger RCA** window, if previous RCAs have been performed, you can view the last five successfully triggered RCAs in the **RCA Logs** table.



This process takes a few minutes. After the process completes, the URL to the S3 bucket, where the AWS logs are located, is displayed.

- Step 4** Under **Destination**, click the URL displayed to go to the AWS S3 bucket.

The AWS console opens in a new browser window. After you log in to AWS, the contents of the S3 bucket are displayed. Depending on the resources created, the number of log groups varies.

Objects

Properties

Objects (14)

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

↻

Copy S3 URI

Copy URL

Download

Open

Delete

Actions

Create folder

Upload

Find objects by prefix

</

AWS Config and Audit Log Details

AWS Config is an AWS tool that continually assesses, monitors, and evaluates resource configurations to aid in operational troubleshooting by correlating configuration changes to specified events and states. Cisco Global Launchpad uses AWS Config to audit the configuration. When AWS Config detects a change in the configuration, Cisco Global Launchpad generates an email notifying you that configuration changes have taken place.

View Amazon CloudWatch Alarms

Cisco Global Launchpad uses Amazon CloudWatch alarms to monitor resource usage and check for unusual behavior. The AWS RCA feature also uses Amazon CloudWatch alarms.

If a threshold is met, alerts are sent to the email ID that you configured during your first log in to Cisco Global Launchpad or to the email ID in the user settings, if it was updated. For more information, see [Subscribe to the Amazon SNS Email Subscription, on page 31](#).



Note

- The Amazon CloudWatch alarms for lambda functions remain in the insufficient data state unless a failure occurs in the corresponding lambda function execution. When a lambda function fails, Amazon CloudWatch gathers the metrics and triggers the alarm. The threshold for all lambda alarms is one, so Amazon CloudWatch can capture alerts if there are any failure.
- For some alarms, like S3, the metrics are only reported once per day at midnight in Greenwich Mean Time (GMT). So it may take 24 to 48 hours for the dashboard metrics to update, which is an expected behavior.

Before you begin

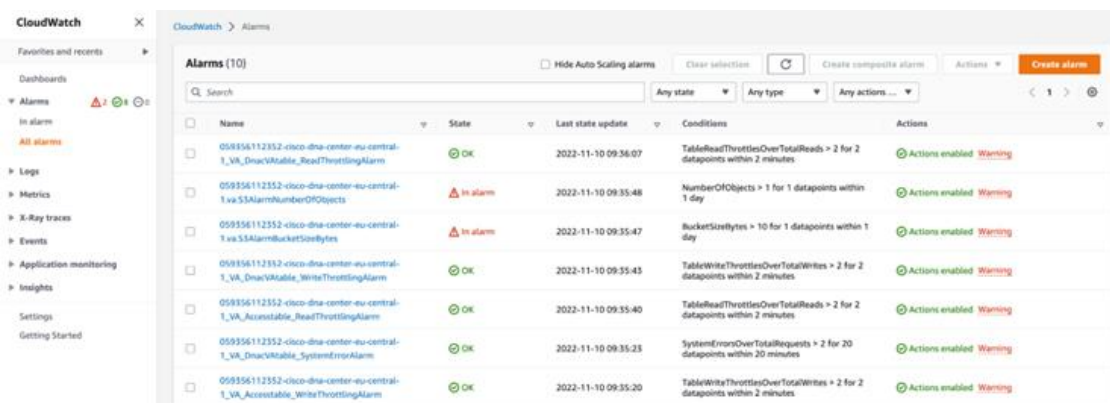
Make sure you successfully configured your AWS account. For more information, see the [Cisco DNA Center 2.3.5 on AWS Deployment Guide](#).

Step 1 Log in to the AWS console.

The AWS console is displayed. The **Alerts** area displays critical alerts from AWS CloudWatch. This area shows the name of the alarm that generated each alert, and shows the region name, metric name, and namespace for each alarm.

Step 2 In the **Alerts** area

- Hover your cursor over an **Information** icon to see the reason that the corresponding alarm was triggered.
- Click the name of an alarm to display the **Alarms** page.



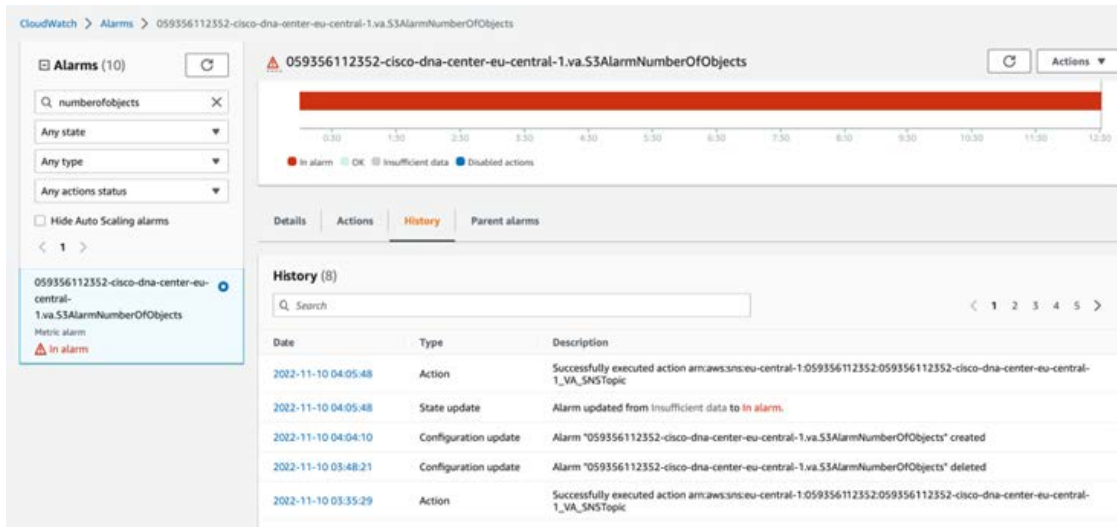
Step 3 On the **Alarms** page, enter the environment name used to deploy Catalyst Center in the **Search** field.

Alarms pertaining to the Catalyst Center instance with the specified environment name are displayed.

Step 4 Click the name of an alarm.

Details about the alarm are displayed in the **Details** tab. To view other information, click the **Actions**, **History**, or **Parent alarms** tabs.

View Amazon CloudWatch Alarms





CHAPTER 8

Backup and Restore

- [About Backup and Restore, on page 37](#)
- [Backup and Restore—Hardware Appliance to VA , on page 37](#)
- [Backup and Restore—VA to VA, on page 38](#)
- [Configure Backup, on page 39](#)
- [Restore a Backup, on page 40](#)
- [Access the Catalyst Center Backup VM, on page 40](#)

About Backup and Restore

Use the backup and restore functions in Catalyst Center VA to create backup files. You can restore the backup files to the same appliance (in case your Catalyst Center becomes unusable) or use them to migrate your Catalyst Center to a different appliance, for example:

- Back up data from a Catalyst Center hardware appliance and restore the data to a Catalyst Center VA.
- Back up data from one Catalyst Center VA and restore the data to another Catalyst Center VA.

For more information about backup and restore, see the [Cisco DNA Center Administrator Guide, Release 2.3.5](#).

Backup and Restore—Hardware Appliance to VA

This procedure provides a high-level overview of how you can back up the data from a Catalyst Center hardware appliance and restore it to a Catalyst Center VA. For detailed instructions, see the "Backup and Restore" chapter in the [Cisco DNA Center Administrator Guide, Release 2.3.5](#).

Before you begin

- Make sure that the hardware appliance used for the backup is a 44-core Catalyst Center appliance.
- If you're using a Cloud backup (NFS) server, you'll need to know the backup password in order to log into the server.

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 in the **View Catalyst Center** pane.

-
- Step 1** Back up the data from the Catalyst Center hardware appliance.
Make sure that the backup server is connected to Catalyst Center through a VPN.
- Step 2** Create a Catalyst Center VA. For more information, see "Create a New Catalyst Center VA" in the [Cisco DNA Center 2.3.5 on AWS Deployment Guide](#).
Make sure the Catalyst Center VA is up and running.
- Step 3** Connect the Catalyst Center VA to the backup server from Step 1.
Make sure that the backup server is reachable from the Catalyst Center VA.
- Step 4** Configure the backup server on the Catalyst Center VA.
- Step 5** Restore the data on to the Catalyst Center VA.
-

Backup and Restore—VA to VA

This procedure provides a high-level overview of how you can back up the data from one (source) Catalyst Center VA and restore it to another (target) Catalyst Center VA. For detailed instructions, see the "Backup and Restore" chapter in the [Cisco DNA Center Administrator Guide, Release 2.3.5](#).

Before you begin

- Make sure that you successfully deployed two Catalyst Center VAs with Cisco Global Launchpad, AWS CloudFormation, or AWS Marketplace. For more information, see [Cisco DNA Center 2.3.5 on AWS Deployment Guide](#).
- Make sure that both Catalyst Center VAs are up and running.
- Make sure that the backup server is connected to the source Catalyst Center VA through a VPN.
- Make sure that the backup server is reachable from the target Catalyst Center VA.
- If you're using a Cloud backup (NFS) server, you'll need to know the backup password in order to log into the server.

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 in the **View Catalyst Center** pane.

-
- Step 1** Back up the data from the source Catalyst Center VA to a backup server.
 - Step 2** Bring up the target Catalyst Center VA that you want to restore the data to.
 - Step 3** Connect the target Catalyst Center VA to the backup server. (See Step 1.)
 - Step 4** Configure the backup server on the target Catalyst Center VA.
 - Step 5** Restore the data to the target Catalyst Center VA.
-

Configure Backup

To configure backup for Catalyst Center:

-
- Step 1** Perform these actions to log in to Catalyst Center:
 - a) Enter **https://server-ip** in your browser, where *server-ip* is the IP address of the server on which Catalyst Center is installed.
 - b) Enter your Catalyst Center username and password.
 - Step 2** From the left pane in the **DNA Center** page, choose **System > Backup & Restore**.
 - Step 3** Click **Configure Settings**.
 - Step 4** Click **Add NFS**.

These steps are required if you're adding NFS for the first time on this Catalyst Center.
 - Step 5** In the **Add NFS** area:
 - a) In the **NFS Server** field, enter the IP address of the NFS server to use for the backup.
 - b) In the **Destination Folder** field, enter **/var/nfsShare**.
 - c) In the **NFS 4** field, accept the default value.
 - d) In the **Port** field, enter **2049**.
 - e) In the **Port Mapper** field, accept the default value.
 - f) Click **Save**.
 - Step 6** In the Warning dialog box, click **Proceed**.
 - Step 7** Click **View NFS List** and verify that the information for the NFS that you configured is correct.
 - Step 8** Perform these actions to mount the NFS path that you created:
 - a) In the **Encryption Passphrase** and **Confirm Passphrase** fields, enter a passphrase,

This passphrase is used when you restore a backup.
 - b) Click **Submit**.

- Step 9** Perform these actions to schedule your backups:
- From the left pane in the **DNA Center** page, choose **Settings > Backup & Restore > .**
 - Click **Scheduled Backup**.
 - In the **Scheduled Backup** pane, configure the options for your backup as desired.
 - Click **Save**.
-

Restore a Backup

To restore backup for Catalyst Center:

- Step 1** Perform these actions to log in to Catalyst Center:
- Enter **https://server-ip** in your browser, where *server-ip* is the IP address of the server on which Catalyst Center is installed.
 - Enter your Catalyst Center username and password.
- Step 2** From the left pane in the **DNA Center** page, choose **System > Backup & Restore**.
- Step 3** In the **Actions** column that corresponds to the backup that you want to restore, click **...** and choose **Restore**.
-

Access the Catalyst Center Backup VM

The following guidelines and restrictions apply when you access the Catalyst Center backup VM:

- You can access the Catalyst Center backup VM only through the subnet that contains the Catalyst Center VM.
- When you created Catalyst Center on Launchpad, you downloaded a PEM file that is used to access the Catalyst Center VM. To access your backup VM, log in to Catalyst Center and use this same PEM file.
- The ports in the backup VM security group communicate only through the backup VM IP address.



CHAPTER 9

Operational Best Practices

- [Encrypt Amazon EBS Volumes Attached to Catalyst Centers, on page 41](#)

Encrypt Amazon EBS Volumes Attached to Catalyst Centers

You can encrypt Amazon Elastic Block Store (Amazon EBS) volumes that are attached to Catalyst Centers that are running in AWS. This procedure is optional and applies only if you want to encrypt EBS volumes that are attached to already running Catalyst Centers in AWS (possibly due to an organization mandate). If your organization does not require encryption of EBS volumes, you can disregard this procedure and continue with non-encrypted EBS volumes.

Encrypting Amazon EBS volumes, which includes encrypting the root volume of an EC2 instance, improves data security in AWS environments. By encrypting Amazon EBS volumes, you can protect sensitive data from unauthorized access and mitigate the risks that are associated with data breaches and theft. Encryption safeguards data and ensures compliance with regulatory standards and industry best practices.

By creating encrypted snapshots and volumes, and potentially replacing the root volume of an EC2 instance, you can seamlessly integrate encryption into your AWS infrastructure.

This procedure includes steps for manually encrypting the existing Amazon EBS volumes from the AWS console. During this process, you create snapshots, which need to be deleted after successfully completing the procedure. Also, expect some downtime because you need to restart the Amazon EC2 instance.

-
- Step 1** Determine the Amazon EBS volume ID of the volume that you want to encrypt.
- You can find this information in the **AWS Management Console** under the **Volumes** in the **EC2** dashboard.
- Step 2** For backup purposes, create a snapshot of the volume that you are encrypting, which is the volume that is attached to Catalyst Center:
- From the **AWS Management Console**, choose **Actions > Create snapshot**.
 - In the **Create snapshot** window, enter a description of the snapshot in the **Description** field.
 - (Optional) Click **Add tag** and add a tag for the snapshot.
 - Click **Create snapshot**.
- Step 3** Make a copy of the snapshot that you created and apply encryption to this copy:

- a. Open the **AWS Management Console**.
- b. In the **EC2** dashboard, go to the **Volumes** area and choose the volume that you want to encrypt.
- c. Choose **Actions > Create snapshot**.
- d. After the snapshot is created, choose **Actions > Copy snapshot**.
- e. In the **Copy snapshot** window:
 1. Check the **Encrypt this snapshot** check box.
 2. From the **KMS key** drop-down list, choose the Key Management Service (KMS) key that you want to use for encryption
 3. Click **Copy snapshot** to create a copy of the snapshot with encryption enabled.

Step 4 Create an encrypted volume from the snapshot:

- a. After the encrypted snapshot is created, go to the **Snapshots** section in the **EC2** dashboard. and choose the encrypted snapshot.
- b. Choose **Actions > Create volume**.
- c. In the **Create volume** window, configure settings for the new volume, including volume type, size, and availability zone, then click **Create volume**.

The new encrypted volume is created from the encrypted snapshot.

Step 5 (Optional) Replace the root volume of an EC2 instance with an encrypted instance:

- a. From the **AWS Management Console**, stop the existing EC2 instance.
- b. Go to the **Snapshots** section in the **EC2** dashboard and choose the root volume to replace.
- c. Choose **Actions > Detach volume** to detach the existing root volume from the instance.
- d. Choose **Actions > Attach volume** to attach the new encrypted volume as the root volume from the instance.
You can identify the encrypted volume by finding the volume whose **Encrypted** field shows **yes** in the **EC2** dashboard **Storage** tab.
- e. Click **Attach volume**.
- f. Choose **Instance state > Start instance** to start the instance.

Step 6 After Catalyst Center is running the new encrypted volume:

- a. Delete snapshots that you created of the volume that you encrypted (in Step 2) and the volume that you copied (in Step 3). Deleting these items frees storage space and prevents unnecessary backups,
- b. Remove the volume that you detached from the instance (in Step 5). This volume is not needed after the snapshot is created and copied.

This clean-up process is important for maintaining an organized cloud environment and minimizing storage costs. This process does not affect the new encrypted Amazon EBS volume that is attached to the running Catalyst Center. Global Launchpad does not maintain snapshots of the Amazon EBS volume.
