




Manage Amazon Email Subscriptions, Logs, and Alarms

- [Subscribe to the Amazon SNS Email Subscription, on page 1](#)
- [Configure Log Retention, on page 2](#)
- [Trigger a Root Cause Analysis \(RCA\), on page 4](#)
- [AWS Config and Audit Log Details, on page 5](#)
- [View Amazon CloudWatch Alarms, on page 5](#)

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.

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.

Global Launchpad

 **059356112352** >

 Region(s)
All >

 VA Monitoring

 User Activities

 **Settings**

 Help Center

Settings

Email Address

Enter the email address to which notifications should be sent when AWS infrastru

Email Id

Log Group Retention in Days

How many days would you like to retain the Amazon CloudWatch logs?

Log Group Retention in Days

Save **Cancel**

Trigger a Root Cause Analysis (RCA)

- 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 (RCA)

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.

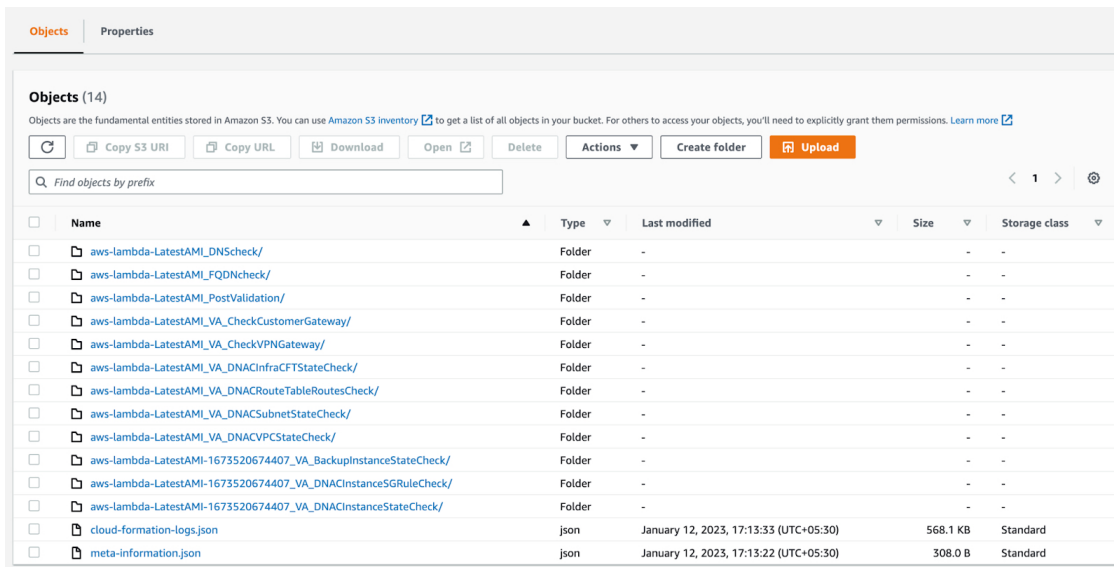
The screenshot displays the 'Trigger RCA' interface in the Cisco Global Launchpad. On the left is a sidebar with navigation items: Admin, Region(s) (All), VA Monitoring, User Activities, Settings, and Help Center. The main content area is titled 'Trigger RCA' and includes an 'RCA Logs' section with a description and a 'Trigger RCA' button. Below this is an 'RCA History' section with a table that currently shows 'No Records Found!'.

Created Date	RCA Path	User
No Records Found !		

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 vary.



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 1](#).

**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 on AWS Deployment Guide](#).

Step 1 Log in to the AWS console.

The AWS console is displayed.

Step 2 From the AWS dashboard, click **CloudWatch** > **Alarms** > **All Alarms**.

The **Alarms** page displays the status of all the alarms.

Name	State	Last state update	Conditions	Actions
059356112352-cisco-dna-center-eu-central-1_VA_DnacVtKublx_ReadThrottlingAlarm	OK	2022-11-10 09:36:07	TableReadThrottlesOverTotalReads > 2 for 2 datapoints within 2 minutes	Actions enabled Warning
059356112352-cisco-dna-center-eu-central-1_vv53AlarmNumberOfObjects	In alarm	2022-11-10 09:35:48	NumberOfObjects > 1 for 1 datapoints within 1 day	Actions enabled Warning
059356112352-cisco-dna-center-eu-central-1_vv53AlarmBucketSizeBytes	In alarm	2022-11-10 09:35:47	BucketSizeBytes > 10 for 1 datapoints within 1 day	Actions enabled Warning
059356112352-cisco-dna-center-eu-central-1_VA_DnacVtKublx_WriteThrottlingAlarm	OK	2022-11-10 09:35:43	TableWriteThrottlesOverTotalWrites > 2 for 2 datapoints within 2 minutes	Actions enabled Warning
059356112352-cisco-dna-center-eu-central-1_VA_Accessible_ReadThrottlingAlarm	OK	2022-11-10 09:35:40	TableReadThrottlesOverTotalReads > 2 for 2 datapoints within 2 minutes	Actions enabled Warning
059356112352-cisco-dna-center-eu-central-1_VA_DnacVtKublx_SystemErrorAlarm	OK	2022-11-10 09:35:28	SystemErrorsOverTotalRequests > 2 for 20 datapoints within 20 minutes	Actions enabled Warning
059356112352-cisco-dna-center-eu-central-1_VA_Accessible_WriteThrottlingAlarm	OK	2022-11-10 09:35:20	TableWriteThrottlesOverTotalWrites > 2 for 2 datapoints within 2 minutes	Actions enabled Warning

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.

CloudWatch > Alarms > 059356112352-cisco-dna-center-eu-central-1.va.S3AlarmNumberOfObjects

Alarms (10)

numberofobjects

Any state

Any type

Any actions status

Hide Auto Scaling alarms


< 1 >

059356112352-cisco-dna-center-eu-central-1.va.S3AlarmNumberOfObjects

Metric alarm

▲ In alarm

▲ 059356112352-cisco-dna-center-eu-central-1.va.S3AlarmNumberOfObjects



Details | Actions | **History** | Parent alarms

History (8)

Search

< 1 2 3 4 5 >

Date	Type	Description
2022-11-10 04:05:48	Action	Successfully executed action arn:aws:sns:eu-central-1:059356112352:059356112352-cisco-dna-center-eu-central-1_VA_SNSTopic
2022-11-10 04:05:48	State update	Alarm updated from Insufficient data to In alarm .
2022-11-10 04:04:10	Configuration update	Alarm "059356112352-cisco-dna-center-eu-central-1.va.S3AlarmNumberOfObjects" created
2022-11-10 03:48:21	Configuration update	Alarm "059356112352-cisco-dna-center-eu-central-1.va.S3AlarmNumberOfObjects" deleted
2022-11-10 03:35:29	Action	Successfully executed action arn:aws:sns:eu-central-1:059356112352:059356112352-cisco-dna-center-eu-central-1_VA_SNSTopic

