



Cisco Secure Cloud Analytics

Amazon Web Services Integration Quick Start Guide



Table of Contents

Configuring S3 Bucket Flow Log Data Storage	4
Associate an S3 Bucket with a VPC	4
Configure S3 Bucket to Minimize Cost (Recommended)	5
Configuring AWS Permission to Access Flow Log Data	6
Create a Policy with Permission to Access Flow Log Data	6
Configuring an IAM Role to Access Flow Log Data	8
Configure an IAM Role with Permission to Access Flow Log Data	8
Configuring Secure Cloud Analytics to Access Flow Log Data from an S3 Bucket	9
Configure Secure Cloud Analytics to Ingest Flow Log Data Stored in a S3 Bucket	9
Configure the S3 Bucket Policy to Allow Secure Cloud Analytics to Ingest Flow Log Data	10
Verifying AWS Integration	11
Verify AWS Integration	11
Configuring S3 Bucket CloudTrail Collection	12
Create a CloudTrail S3 Path	12
Troubleshooting: Virtual Private Cloud (VPC) Flow Logs	14
NAT Gateways	15
Can AWS Store VPC Flows That Navigate From a NAT Gateway?	15
How Can I Tell if the Custom VPC Flow Log Configuration is Set Up in My Tenant?	15
How Does Secure Cloud Analytics Manage VPC Flow Logs From AWS?	15
What Should I Expect From Traffic that Navigates Through a NAT Gateway Regarding Flows?	16
How Does Secure Cloud Analytics Model the Endpoint and the NAT Gateway It Navigates Through?	16
What Kind of Flows Are Visible With the pkt- srcaddr and pkt- dstaddr Fields Included?	16
AWS Load Balancers	17
How Does Secure Cloud Analytics Capture Traffic that Navigates through a Network Load Balancer (NLB)?	17

How Does Secure Cloud Analytics Capture Traffic that Navigates through an Application Load Balancer	17
Additional Resources	19
Contacting Support	20
Change History	21

Configuring S3 Bucket Flow Log Data Storage

You can store your flow log data in an existing S3 bucket, or you can create a new S3 bucket when you enable flow logging. Then, we recommend you configure the bucket to delete the flow logs after they are no longer needed to reduce the storage costs of flow log monitoring.



To configure VPC Flow Logs on multiple existing VPCs, a script is available to assist with configuration: <https://github.com/obsrvbl-oss/aws-setup>. For more information on how to use AWS Cloudshell to run the script, go to <https://docs.aws.amazon.com/cloudshell/latest/userguide/getting-started.html>.

Associate an S3 Bucket with a VPC

1. Log in to your AWS Management Console, then access the VPC dashboard.
2. Select **Your VPCs**.
3. Right-click a VPC, then select **Create Flow Log**.
4. Select one of the following options from the **Filter** drop-down:
 - Select **All** to log both accepted and rejected IP traffic, allowing Secure Cloud Analytics to see both types of traffic.
 - Select **Accept** to log only accepted IP traffic, allowing Secure Cloud Analytics to see only accepted traffic.
5. Select the **Send to an S3 bucket Destination**.
6. Enter an **S3 bucket ARN** in which you want to store flow log data.



If the S3 bucket does not exist, AWS creates it after you commit your changes.

7. In the Log record format pane, select **Custom format**.
8. Select all attributes from the **Log format** drop-down list.



Make sure to follow Steps 7 and 8. The [Troubleshooting: Virtual Private Cloud \(VPC\) Flow Logs](#) section provides information that may help if these steps are missed.

9. Click **Create**.



If restricting access to this S3 bucket based on IP, make sure that communication with the relevant IPs is allowed. Go to your Secure Cloud Analytics web portal, select **Settings > Integrations > AWS > About** to see the list of public IPs used by Secure Cloud Analytics.

Configure S3 Bucket to Minimize Cost (Recommended)



The following configuration will delete any objects in the bucket, including flow logs, after 1 day. We recommend this configuration if you are only storing VPC flow logs in this bucket for use with Secure Cloud Analytics.

1. Log in to the AWS Console for S3.
2. In the **Buckets** list, choose the name of the bucket where you want to store VPC flow logs.
3. Select the **Management** tab.
4. In the Lifecycle rules section, click **Create lifecycle rule**.
5. Enter a unique name for the Lifecycle rule, for example `Expire after 1 day`.
6. For the scope of the lifecycle rule, select **This rule applies to all objects in the bucket**.
7. Check the **I acknowledge that this rule will apply to all objects in the bucket** check box.
8. Under Lifecycle rule actions, select **Permanently delete previous versions of objects**.
9. Under Permanently delete noncurrent versions of objects, set **Days after objects become noncurrent** to **1**.
10. Click **Create rule**.
11. Back in Lifecycle Configuration, click the radio button next to the rule just created, and in the Actions drop-down, click **Enable rule**.

Configuring AWS Permission to Access Flow Log Data

Create a new IAM policy, using the JSON configuration displayed in the Secure Cloud Analytics web portal. This policy contains permissions to allow Secure Cloud Analytics access to the flow log data.

To evaluate your AWS cloud posture, you must grant additional permissions to the IAM policy in AWS. The AWS About page in Secure Cloud Analytics lists the required permissions in the JSON object that starts with "Sid": "CloudCompliance".

If you are a customer integrating Secure Cloud Analytics with AWS for the first time, and do not want to grant these additional permissions, you can remove this object, but you will not be able to use the Cloud Posture report.

Create a Policy with Permission to Access Flow Log Data

1. Log in to your Secure Cloud Analytics web portal as an administrator.
2. Select **Settings > Integrations > AWS > About**.
3. Review the instructions to access AWS resources.
4. Copy the **Policy Document** JSON configuration and paste it into a plaintext editor.
5. Review the JSON object that starts with "Sid": "CloudCompliance" for the additional permissions Secure Cloud Analytics requires to evaluate your AWS cloud posture. You have the following options:
 - If you do not want to grant these additional permissions, delete the JSON object that starts with "Sid": "CloudCompliance". You will not be able to evaluate your AWS cloud posture in Secure Cloud Analytics. Continue to the next step.
 - If you want to grant these additional permissions to evaluate your AWS cloud posture, continue to the next step.
6. Log in to your AWS Management Console, and access the IAM dashboard.
7. Select **Policies**.
8. Click **Create policy**.
9. Select the **JSON** tab.
10. Copy the policy JSON configuration from your plaintext editor and paste it into the JSON editor.

11. Click **Review policy**.

If the policy validator throws an error, review the text that you copied and pasted.

12. Enter `swc_policy` in the Name field.

13. Enter a Description, such as `Policy to allow Secure Cloud Analytics to read events and log data.`

14. Click **Create policy**.

Configuring an IAM Role to Access Flow Log Data

After you create the IAM policy, create an IAM role that allows Secure Cloud Analytics to access flow log data.

Configure an IAM Role with Permission to Access Flow Log Data

1. Log in to your AWS Management Console, then access the IAM dashboard.
2. Select **Roles**.
3. Select **Create role**.
4. Select the `Another AWS account` role type.
5. Enter `757972810156` in the `Account ID` field.
6. Select the `Require external ID` option.
7. Enter your Secure Cloud Analytics web portal name as the **External ID**.

Your web portal name is embedded in the portal URL, in the format `https://portal-name.obsrvbl.com`. For example, if your web portal URL is `https://example-client.obsrvbl.com`, enter **example-client** as the External ID. The integration configuration fails if you enter the entire URL.

8. Click **Next: Permissions**.
9. Select the `swc_policy` policy that you just created.
10. Click **Next: Tagging**.
11. Click **Next: Review**.
12. Enter `swc_role` as the **Role name**.
13. Enter a **Description**, such as `Role to allow cross-account access`.
14. Click **Create role**.
15. Copy the role ARN and paste it into a plaintext editor.

Configuring Secure Cloud Analytics to Access Flow Log Data from an S3 Bucket

To complete your flow log configuration, enter the IAM role and S3 bucket name in the Secure Cloud Analytics web portal, then modify the S3 bucket policy in AWS using the configuration provided by Secure Cloud Analytics when you add the S3 bucket name.

If you recently enabled VPC flow logging in your account, wait ten minutes before configuring Secure Cloud Analytics to ingest flow log data. The system may return an error when you add the **S3 Path** name, if the S3 bucket contains no logs; AWS generates VPC flow logs approximately every ten minutes.


Configure Secure Cloud Analytics to Ingest Flow Log Data Stored in a S3 Bucket

1. Log in to your Secure Cloud Analytics web portal as an administrator.
2. Select **Settings > Integrations > AWS > Credentials**.
3. Click **Add New Credentials**.
4. Enter a descriptive **Name**.
5. Copy the saved role ARN from the plaintext editor and paste it into the **Role ARN** field.
6. Click **Create**.
7. Select **Settings > Integrations > AWS > VPC Flow Logs**.
8. Click **Add VPC Flowlog**.
9. Enter the name of the S3 bucket that contains your flow log data in the **S3 Path** field.




You can add more than one configured S3 bucket. You only need to configure one IAM access policy and role for your Secure Cloud Analytics integration with AWS.

10. Select **Credentials** for the S3 bucket, then click **Setup Instructions**.
The system displays a bucket policy JSON configuration, updated with the S3 bucket path and credentials.
11. Copy the displayed bucket policy JSON configuration and paste it into a plaintext editor.

 Keep this browser window open. You complete the Secure Cloud Analytics web portal configuration after configuring the S3 bucket policy.

Configure the S3 Bucket Policy to Allow Secure Cloud Analytics to Ingest Flow Log Data

1. Log in to your AWS Management Console, then access the IAM dashboard.
2. In the IAM dashboard, select **Policies**.
3. Click **Create Policy**.
4. Select the JSON tab.
5. Copy the bucket policy JSON configuration from the plaintext editor and paste it into the policy editor, overwriting the existing bucket policy.
6. Click **Review policy**.
7. Enter a policy **Name**.
8. Enter an optional policy **Description**.
9. Click **Create policy**.
10. In the IAM dashboard, select **Roles**.
11. Select `swc_role`.
12. In the Permissions tab, click **Attach policies**.
13. Select the policy name you entered in step 6.
14. Click **Attach policy**.
15. In the Secure Cloud Analytics web portal, click **Create** for the S3 bucket path and credentials you just entered.

 The system displays an error if it does not have the correct permissions to ingest flow log data from the S3 bucket. For assistance, contact [Cisco Support](#) with your portal name and S3 bucket name.

Verifying AWS Integration

After you complete the AWS integration, in the **Settings** menu, the Sensors page displays a new sensor with the following name:

AWS: *S3-bucket-name*

This sensor entry displays the health of the integration, or the S3 bucket name, but does not directly allow configuration from the sensors page.



It may take the web portal up to 24 hours after you complete AWS configuration to start displaying traffic and entity data.

Verify AWS Integration

1. Log in to your Secure Cloud Analytics web portal as an administrator.
2. Select **Settings > Sensors**. Verify that the page displays the S3 bucket name.
3. Select **Integrations > AWS > Permissions**. Verify that the displayed AWS permissions match your expectations.

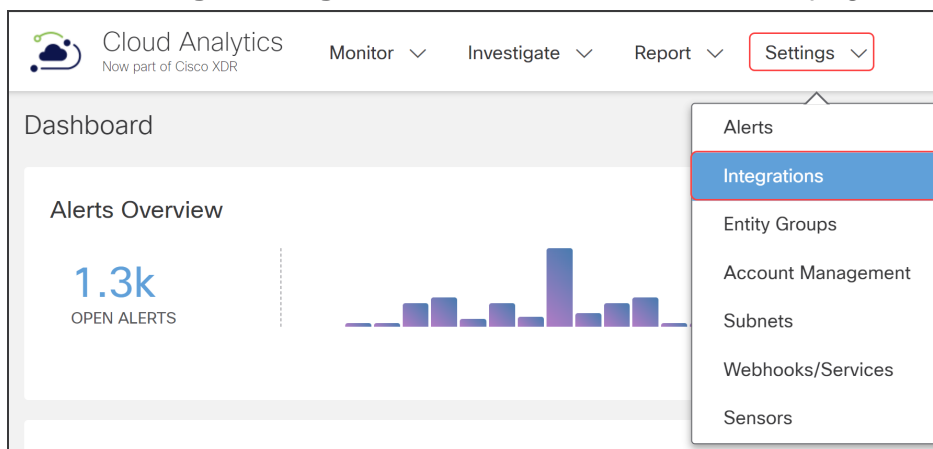
Configuring S3 Bucket CloudTrail Collection

AWS CloudTrail is an AWS service that helps you enable operational and risk auditing, governance, and compliance of your AWS account. Actions taken by a user, role, or an AWS service are recorded as events in CloudTrail.

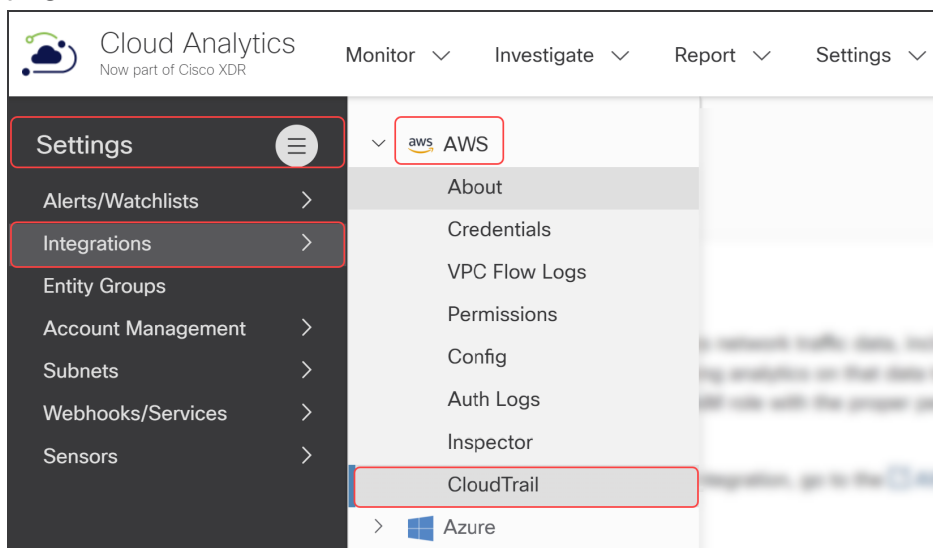
Create a CloudTrail S3 Path

To create a new CloudTrail S3 path, do the following:

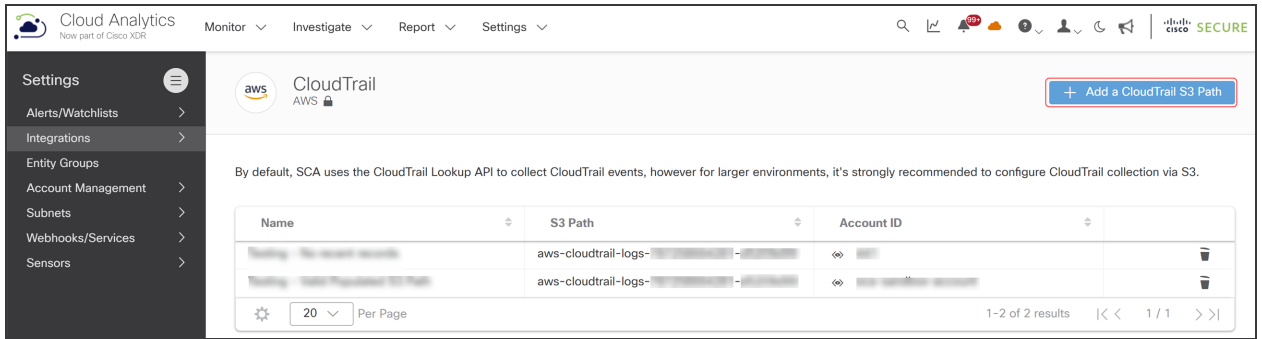
1. Log in to your Secure Cloud Analytics web portal as an administrator.
2. Select **Settings > Integrations** to access the About AWS page.



3. Select **Settings > Integrations > AWS > CloudTrail** to access the CloudTrail AWS page.



4. Click **+Add a CloudTrail S3 Path**.



The Create a CloudTrail S3 Path dialog box displays.

The dialog box is titled 'Create a CloudTrail S3 Path' and has a close button (X) in the top right. It contains the following fields:

- Name***: A text input field.
- S3 Path***: A text input field.
- Account ID***: A dropdown menu with the text 'Select Account ID'.
- Policy Document**: A dropdown menu with a right-pointing chevron and the text 'Policy Document'.

 At the bottom right, there are two buttons: 'Cancel' and 'Create', with the 'Create' button highlighted by a red box.

5. Enter a unique **Name** for the CloudTrail S3 path you'd like to add.

i Make sure the S3 path includes the bucket_name and prefix_name (if a prefix is configured). The S3 path should not include the AWSLogs portion of the path and beyond. For more details, refer to [Finding your CloudTrail Log Files](#).

6. Enter the **S3 Path** information for the new CloudTrail S3 path.

7. Select an **Account ID**.

8. Click **Create**.

Troubleshooting: Virtual Private Cloud (VPC) Flow Logs

This section provides information about how Cisco Secure Cloud Analytics manages AWS Virtual Private Cloud (VPC) flow logs, particularly traffic that uses Network Address Translation (NAT) gateways and AWS load balancers.

Acronyms used in this section:

Acronym	Meaning
ALB	Application Load Balancer
AWS	Amazon Web Service
EC2	Elastic Cloud Compute
ENI	Elastic Network Interface
NAT	Network Address Translation
NLB	Network Load Balancer
S3	Simple Storage Service
TCP	Transmission Control Protocol
VPC	Virtual Private Cloud

NAT Gateways

A NAT gateway is a Network Address Translation (NAT) service. When using a NAT gateway, instances in a private subnet can connect to services outside your VPC, but external services can't initiate a connection within those instances. The NAT Gateway only allows outbound access.

Can AWS Store VPC Flows That Navigate From a NAT Gateway?

AWS provides the ability to store VPC flows both from the private Elastic Cloud Compute (EC2) node to the NAT gateway and also to the external internet using a custom VPC flow log configuration. AWS stores the originating traffic source in the **pkt-srcaddr** and **pkt-dstaddr** fields.



For more details about how AWS manages traffic from NAT devices in a VPC, refer to [Traffic Through a NAT Gateway](#).

When customers add the required fields (**pkt-dstaddr** and **pkt-srcaddr**), Secure Cloud Analytics collects and displays the originating sources reported by AWS:

- AWS releases traffic with the endpoint and NAT stored under the **pkt-addr** fields.
- The **pkt-dstaddr** and **pkt-srcaddr** fields display both the originating endpoint traffic and the NAT gateway traffic.

How Can I Tell if the Custom VPC Flow Log Configuration is Set Up in My Tenant?

To verify your current configuration, review the header of your VPC flow log files in Amazon Simple Storage Service (S3). Then search for the **pkt-srcaddr** and **pkt-dstaddr** fields.



Without these fields in S3, Secure Cloud Analytics doesn't have visibility into the traffic sent from a private IP to the internet when it's behind the NAT gateway.

How Does Secure Cloud Analytics Manage VPC Flow Logs From AWS?

If the **pkt-dstaddr** and/or **pkt-srcaddr** are present in the flow, Secure Cloud Analytics uses these fields instead of the **srcaddr** and the **dstaddr** to determine the destinations (reporting the “true” network source). AWS releases flows with the NAT gateway labeled as the **pkt-dstaddr** and/or **pkt-srcaddr**. Secure Cloud Analytics treats these flow as if they originate directly from the NAT gateway.



For more information about these fields, refer to [Traffic Through a NAT Gateway](#).

What Should I Expect From Traffic that Navigates Through a NAT Gateway Regarding Flows?

In Secure Cloud Analytics, we see and record the following two flows:

- flow for the endpoint navigation through the NAT gateway
- flow for the NAT gateway itself

How Does Secure Cloud Analytics Model the Endpoint and the NAT Gateway It Navigates Through?

Secure Cloud Analytics models both the endpoint and the NAT Gateway itself as two separate entities. Flows associated with the endpoint device are associated with the endpoint; flows associated with the NAT Gateway device are associated with the NAT gateway.

Typically, you will not see a one-to-one match in the detections released for the NAT gateway with the endpoint navigation through the NAT gateway. Secure Cloud Analytics searches for anomalies based on past behavior. The endpoints have different behavioral profiles. For example, an outbound traffic spike for an endpoint navigation through a NAT Gateway may not be anomalous for the NAT Gateway itself.

What Kind of Flows Are Visible With the `pkt-srcaddr` and `pkt-dstaddr` Fields Included?

The following example shows how AWS VPC flow log traffic as it transitions through a NAT gateway when both the `pkt-srcaddr` and `pkt-dstaddr` fields are included.



i Multiple flows are provided in the logs that represent unidirectional flow of data.

In this example:

- The blue line represents traffic *from* the EC2 node *to* the internet when the `pkt-srcaddr` and `pkt-dstaddr` fields are available.
- The black line represents traffic *from* the NAT Gateway *to* the internet regardless of additional `pkt-srcaddr` and `pkt-dstaddr` fields.

i Secure Cloud Analytics always uses the `pkt-srcaddr` and `pkt-dstaddr` fields if available.

AWS Load Balancers

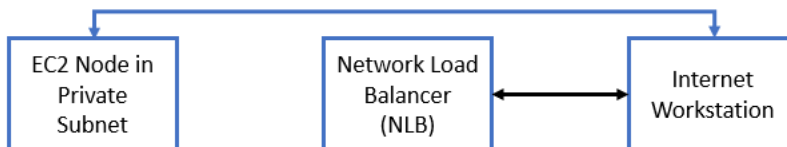
There are two types of AWS load balancers: Network Load Balancer (NLB) and Application Load Balancer (ALB).

How Does Secure Cloud Analytics Capture Traffic that Navigates through a Network Load Balancer (NLB)?

SCA manages NLB traffic similar to the way NAT Gateways traffic is managed, with the exception that the **pkt-dstaddr** and/or **pkt-srcaddr** fields aren't required. AWS replicates the flows across Elastic Network Interfaces (ENIs).

i For more details about how AWS preserves the client IPs that navigate through a NLB, refer to the [AWS documentation](#).

The following example shows how traffic navigates through a NLB.



In this example:

- The blue line represents traffic *from* the EC2 node *to* the internet.
- The black line represents traffic *from* the NLB *to* the internet.

i The **pkt-srcaddr** and **pkt-dstaddr** fields are not required to see the traffic as shown.

How Does Secure Cloud Analytics Capture Traffic that Navigates through an Application Load Balancer

In AWS VPC flow logs, Application Load Balancers (ALBs) terminate the TCP connections. Additionally:

- The outbound bytes from the EC2 node to the internet are visible and appear in the logs.
- The inbound flows from the internet to the EC2 node are routed through the ALB and are not shown in the EC2 node directly.

The following example shows how traffic navigates through an Application Load Balancer (ALB).



In this example:

- The red line represents traffic *from* the EC2 node *to* the ALB.
- The black line represents traffic *from* the ALB *to* the internet.



The **pkt-srcaddr** and **pkt-dstaddr** fields are not required to see the traffic shown as shown.

Additional Resources

For more information about Secure Cloud Analytics, refer to the following:

- <https://www.cisco.com/c/en/us/products/security/stealthwatch-cloud/index.html> for a general overview
- <https://www.cisco.com/c/en/us/support/security/stealthwatch-cloud/tsd-products-support-series-home.html> for documentation resources
- <https://www.cisco.com/c/en/us/support/security/stealthwatch-cloud/products-installation-guides-list.html> for installation and configuration guides, including the Secure Cloud Analytics Initial Deployment Guide

Contacting Support

If you need technical support, please do one of the following:

- Contact your local Cisco Partner
- Contact Cisco Support
- To open a case by web: <http://www.cisco.com/c/en/us/support/index.html>
- To open a case by email: tac@cisco.com
- For phone support: 1- 800- 553- 2447 (U.S.)
- For worldwide support numbers:
<https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html>

Change History

Document Version	Published Date	Description
1_0	March 7, 2018	Initial version.
1_1	May 30, 2019	Update with S3 bucket integration information.
1_2	June 14, 2019	Minor updates to configuration.
1_3	October 22, 2019	Updated configuration instructions.
1_4	August 13, 2020	Corrected rendering on flow log syntax format.
1_5	October 16, 2020	Updates based on UI updates, and clarification on flow log format.
1_6	January 26, 2021	Updates for Secure Cloud Analytics Posture Management, including required permissions.
1_7	February 18, 2021	Updates for UI restructure.
2_0	November 3, 2021	Updated product branding.
3_0	August 1, 2022	Added Contacting Support section, added a note for public IPs, and updated document title.
3_1	January 20, 2023	Added Configure S3 Bucket to Minimize Cost section.
3_2	January 12, 2024	Added two new sections: <ul style="list-style-type: none"> Configuring S3 Bucket CloudTrail Collection Troubleshooting: Virtual

		Private Cloud (VPC) Flow Logs
--	--	----------------------------------

Copyright Information

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/go/trademarks>. 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)

