Cisco Secure Cloud Analytics

GovCloud Integration Guide

Table of Contents

Introduction

Cisco Secure Cloud Analytics (formerly Stealthwatch Cloud) Cisco Secure Cloud Analytics public cloud monitoring (formerly Stealthwatch Cloud Public Cloud Monitoring) on GovCloud is a visibility, threat identification, and compliance service for Amazon Web Services (AWS) GovCloud. Secure Cloud Analytics on GovCloud consumes network traffic telemetry, including Virtual Private Cloud (VPC) flow logs, from your AWS public cloud network. It then performs dynamic entity modeling by running analytics on that data to detect threats and indicators of compromise. Secure Cloud Analytics on GovCloud consumes VPC flow logs directly from your AWS GovCloud account using a cross-account IAM role with the proper permissions. In addition, Secure Cloud Analytics on GovCloud can consume other sources of data, like CloudTrail and IAM, for additional context and monitoring.

> Some services, including email notifications, DNS resolution, and front-end static assets, are served through the AWS public cloud infrastructure.

Note the following:

- Secure Cloud Analytics is not currently FedRAMP certified.
- Your Secure Cloud Analytics on GovCloud deployment can monitor AWS GovCloud accounts, premises networks, GCP deployments, and Azure deployments. Your Secure Cloud Analytics on GovCloud deployment cannot monitor AWS public cloud accounts. If you want to monitor an AWS public cloud deployment, sign up for a Secure Cloud Analytics free trial.
- Secure Cloud Analytics on GovCloud does not support Cisco Secure Sign-On. Customers use local accounts to access the Secure Cloud Analytics on GovCloud portal.

> Contact Cisco Support if you are interested in these features, to help Cisco prioritize these features in future releases.

To use Secure Cloud Analytics on GovCloud:

- Go to the Secure Cloud Analytics on GovCloud AWS Marketplace trial page to sign up for a Secure Cloud Analytics on GovCloud 60-day free trial.
- See Secure Cloud Analytics on GovCloud Public Cloud Monitoring Integration to integrate Secure Cloud Analytics on GovCloud with your AWS GovCloud deployment. Optionally, see Secure Cloud Analytics on GovCloud Cisco Secure Cloud Analytics private network monitoring (formerly Stealthwatch Cloud Private

Network Monitoring) Deployment to add a Cisco Secure Cloud Analytics sensor (formerly Stealthwatch Cloud Sensor) to your Secure Cloud Analytics on GovCloud portal.

- See Secure Cloud Analytics on GovCloud Portal Notes for information about using the Secure Cloud Analytics on GovCloud portal.

Free Trial Signup

You can request a free Secure Cloud Analytics on GovCloud 60-day trial from the AWS Marketplace. The trial page lists various features of Secure Cloud Analytics on GovCloud and billing details.

Secure Cloud Analytics on GovCloud Integration

After you sign up for the Secure Cloud Analytics on GovCloud free trial, you can integrate your Secure Cloud Analytics on GovCloud portal with your AWS GovCloud deployment. Follow the instructions in the Secure Cloud Analytics for Amazon Web Services Quick Start Guide, with the following differences:

- Your Secure Cloud Analytics on GovCloud portal URL contains **.gov** (`https://portal-name.gov.obsrvbl.com`). If it does not, contact Cisco Support for assistance.
- You can integrate your Secure Cloud Analytics on GovCloud portal with an AWS GovCloud deployment only, not an AWS public cloud deployment.
- Create all AWS objects, including the S3 bucket, role, and policies, within an AWS GovCloud deployment. If you create any of these objects within an AWS public cloud deployment, your Secure Cloud Analytics on GovCloud integration fails.
- When configuring your S3 bucket to store flow log data, the **S3 bucket ARN** must belong to the **aws-us-gov** partition, and within an AWS GovCloud deployment.
- When configuring the AWS policy to allow Secure Cloud Analytics permission to access flow log data, refer to the Secure Cloud Analytics on GovCloud portal UI for the policy document.
- When configuring an IAM role to access flow log data:
    - The **Account ID** is `523133480950` for Secure Cloud Analytics on GovCloud integrations.
    - Your Secure Cloud Analytics on GovCloud web portal name for the External ID is embedded in the portal URL, in the format `https://portal-name.gov.obsrvbl.com`. For example, if your web portal URL is `https://example-client.gov.obsrvbl.com`, enter **example-client** as the External ID. The integration configuration fails if you enter the entire URL.

Secure Cloud Analytics on GovCloud Deployment

A GovCloud-hosted instance of Secure Cloud Analytics can monitor premises networks. To collect local network telemetry, deploy an on-premises sensor. Follow the instructions at Sensor Installation, with the following differences:

- When configuring firewall rules to allow traffic between the sensor and the external internet, Secure Cloud Analytics on GovCloud does not support the remote troubleshooting option. Do not allow inbound traffic to the sensor from a remote troubleshooting appliance IP address (54.83.42.41:22/TCP).
- After you deploy your sensor, and before you configure the web portal to add the sensor, you must update the `config.local` configuration file with a GovCloud-specific host, then restart the sensor. See the following procedure for more information.

Configure your sensor to connect to a Secure Cloud Analytics on GovCloud-specific host:

Procedure

1. Log in to your sensor as an administrator via SSH.
2. At the command prompt, enter `sudo nano opt/obsrvbl-ona/config.local` and press Enter to edit the configuration file.
3. Add the following line at the bottom of the file:

   ```
   OBSRVBL_HOST=https://sensor.us-gov.gov.obsrvbl.com
   ```
4. Press Ctrl + 0 to save the change.
5. Press Ctrl + x to exit.
6. At the command prompt, enter `sudo service obsrvbl-ona restart` and press Enter to restart the Secure Cloud Analytics service.

What to Do Next

- Proceed with configuration in Secure Cloud Analytics on GovCloud portal UI to add the sensor.

Secure Cloud Analytics on GovCloud Portal Notes

The Secure Cloud Analytics on GovCloud portal differs from the Secure Cloud Analytics portal in the following ways:

- Secure Cloud Analytics on GovCloud does not support Cisco Secure Sign-On. Local user accounts are used to access the Secure Cloud Analytics on GovCloud portal.
- Your Secure Cloud Analytics on GovCloud portal URL contains **.gov** (`https://portal-name.gov.obsrvbl.com`).
- You can integrate your Secure Cloud Analytics on GovCloud portal with an AWS GovCloud deployment, not an AWS public cloud deployment.
- Cisco Security Analytics and Logging integration with Secure Cloud Analytics on GovCloud is **not supported**. See https://www.cisco.com/c/en/us/products/security/security-analytics-logging/index.html for more information on CSAL.
- Secure Cloud Analytics on GovCloud supports AWS-related webhooks. However, note that data sent via webhook may contain sensitive material, and we **do not recommend** using these webhooks with Secure Cloud Analytics on GovCloud.
- The Secure Cloud Analytics account number is `523133480950` for the cross-account role.

In addition, note the following:

- GCP, Azure, Kubernetes, Meraki, and Umbrella integrations with Secure Cloud Analytics on GovCloud are supported. However, check your organization's security policies to ensure this does not violate your organization's guidelines and best practices.
- Secure Cloud Analytics on GovCloud supports all other webhooks. However, note that data sent via webhook may contain sensitive material, and we **do not recommend** using these webhooks with Secure Cloud Analytics on GovCloud.

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/products/security/stealthwatch/stealthwatch-cloud-free-offer.html to sign up for a 60-day Free Trial
- 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
- For Secure Cloud Analytics Free Trial customers, open a case by email: swatchc-support@cisco.com

Change History

Revision	Revision Date	Description
1.0	2020 April 13	Initial version.
2.0	2021 November 3	Updated product branding.
2.1	2022 August 2	Added Contacting Support section.

Copyright Information