Cisco Stealthwatch Cloud

Stealthwatch Cloud on GovCloud Integration Guide

Stealthwatch Cloud on GovCloud Introduction

Stealthwatch Cloud Public Cloud Monitoring (PCM) on GovCloud is a visibility, threat identification, and compliance service for Amazon Web Services (AWS) GovCloud. Stealthwatch Cloud 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. Stealthwatch Cloud on GovCloud consumes VPC flow logs directly from your AWS GovCloud account using a cross-account IAM role with the proper permissions. In addition, Stealthwatch Cloud 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:

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

> Contact swatchc-support@cisco.com if you are interested in these features, to help Cisco prioritize these features in future releases.

To use Stealthwatch Cloud on GovCloud:

- Go to the Stealthwatch Cloud on GovCloud AWS Marketplace trial page to sign up for a Stealthwatch Cloud on GovCloud 60-day free trial.
- See Stealthwatch Cloud on GovCloud Public Cloud Monitoring Integration to integrate Stealthwatch Cloud on GovCloud with your AWS GovCloud deployment. Optionally, see Stealthwatch Cloud on GovCloud Private Network Monitoring Deployment to add a sensor to your Stealthwatch Cloud on GovCloud portal.

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

Stealthwatch Cloud on GovCloud Free Trial Signup

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

Stealthwatch Cloud Public Cloud Monitoring on GovCloud Integration

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

- Your Stealthwatch Cloud on GovCloud portal URL contains **.gov** (`https://portal-name.gov.obsrvbl.com`). If it does not, contact swatchc-support@cisco.com for assistance.
- You can integrate your Stealthwatch Cloud 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 Stealthwatch Cloud 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 Stealthwatch Cloud permission to access flow log data, refer to the Stealthwatch Cloud on GovCloud portal UI for the policy document.
- When configuring an IAM role to access flow log data:
    - The **Account ID** is `523133480950` for Stealthwatch Cloud on GovCloud integrations.
    - Your Stealthwatch Cloud 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.

Stealthwatch Cloud Private Network Monitoring on GovCloud Deployment

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

- When configuring firewall rules to allow traffic between the sensor and the external internet, Stealthwatch Cloud 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 Stealthwatch Cloud on GovCloud-specific host:

Procedure

1. Log in to the 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 Stealthwatch Cloud service.

What to Do Next

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

Stealthwatch Cloud on GovCloud Portal Notes

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

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

In addition, note the following:

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

Change History

Revision	Revision Date	Description
1.0	2020 April 13	Initial version.

Copyright Information