Cisco Stealthwatch Cloud

Stealthwatch Cloud Public Cloud Monitoring for AWS Quick Start Guide

Public Cloud Monitoring Configuration for Amazon Web Services

Stealthwatch Cloud Public Cloud Monitoring (PCM) is a visibility, threat identification, and compliance service for Amazon Web Services (AWS). Stealthwatch Cloud consumes network traffic data, 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 consumes VPC flow logs directly from your AWS account using a cross-account IAM role with the proper permissions. In addition, Stealthwatch Cloud can consume other sources of data, like CloudTrail and IAM, for additional context and monitoring.

To configure an **S3 bucket** to store your flow logs, and Stealthwatch Cloud to ingest these flow logs:

1. In AWS, enable VPC flow logging for a VPC, then configure an S3 bucket to which you export the flow logs. See **Configuring S3 Bucket Flow Log Data Storage** for more information.
2. In AWS, configure an IAM access policy and IAM role to allow Stealthwatch Cloud the permission to access and ingest the flow logs. See **Configuring AWS Permission to Access Flow Log Data** and **Configuring an IAM Role to Access Flow Log Data** for more information.
3. In the Stealthwatch Cloud web portal UI, update the configuration with the S3 bucket and IAM role to enable AWS flow log data ingestion. See **Configuring Stealthwatch Cloud to Access Flow Log Data from an S3 Bucket** for more information.

Configuring S3 Bucket Flow Log Data Storage

You can store your flow log data in an existing S3 bucket. You can also create a new S3 bucket when you enable flow logging.

Associate an S3 bucket with a VPC:

Before You Begin

- Log into your AWS Management Console, and access the VPC Dashboard.

Procedure

1. Select **Your VPCs**.
2. Right-click a VPC, then select **Create Flow Log**.
3. Select one of the following options from the **Filter** drop-down:
    - Select `All` to log both accepted and rejected IP traffic, allowing Stealthwatch Cloud to see both types of traffic.
    - Select `Accept` to log only accepted IP traffic, allowing Stealthwatch Cloud to see only accepted traffic.
4. Select the `Send to an S3 bucket` **Destination**.
5. 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.

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

What to Do Next

- Configure AWS permission to allow Stealthwatch Cloud to access flow log data. See **Configuring AWS Permission to Access Flow Log Data** for more information.

Configuring AWS Permission to Access Flow Log Data

Create a new IAM policy, using the JSON configuration displayed in the Stealthwatch Cloud web UI. This policy contains permissions to allow Stealthwatch Cloud 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 Stealthwatch Cloud lists the required permissions in the JSON object that starts with `"Sid": "CloudCompliance"`.

If you are a customer integrating Stealthwatch Cloud 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:

Before You Begin

- Log into your AWS Management Console, and access the IAM Dashboard.
- Log into the Stealthwatch Cloud web portal UI as an administrator.

Procedure

1. In the Stealthwatch Cloud web UI, select **Settings > Integrations > AWS > About**.
2. Review the instructions to access AWS resources.
3. Copy the **Policy Document** JSON configuration and paste it into a plaintext editor.
4. Review the JSON object that starts with `"Sid": "CloudCompliance"` for the additional permissions Stealthwatch Cloud 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 Stealthwatch Cloud. Continue to the next step.
    - If you want to grant these additional permissions to evaluate your AWS cloud posture, continue to the next step.
5. In the IAM dashboard, select **Policies**.
6. Click **Create policy**.
7. Select the **JSON** tab.
8. Copy the policy JSON configuration from your plaintext editor and paste it into the JSON editor.
9. Click **Review policy**.

    If the policy validator throws an error, review the text that you copied and pasted.
10. Enter `swc_policy` in the Name field.
11. Enter a Description, such as `Policy to allow Cisco Stealthwatch Cloud to read events and log data.`
12. Click **Create policy**.

What to Do Next

- Create a new role to allow Stealthwatch Cloud access to flow log data. See **Configuring an IAM Role to Access Flow Log Data** for more information.

Configuring an IAM Role to Access Flow Log Data

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

Configure an IAM role with permission to access flow log data:

Before You Begin

- Log into your AWS Management Console, and access the IAM Dashboard.

Procedure

1. Select **Roles**.
2. Select **Create role**.
3. Select the `Another AWS account` role type.
4. Enter `757972810156` in the Account ID field.
5. Select the `Require external ID` option.
6. Enter your Stealthwatch Cloud 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.

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

What to Do Next

- Add the IAM role and S3 bucket name to the Stealthwatch Cloud web UI, then upload a new S3 bucket policy in AWS. See **Configuring Stealthwatch Cloud to Access Flow Log Data from an S3 Bucket** for more information.

Configuring Stealthwatch Cloud 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 Stealthwatch Cloud web portal UI, then modify the S3 bucket policy in AWS using the configuration provided by Stealthwatch Cloud when you add the S3 bucket name.

If you recently enabled VPC flow logging in your account, wait ten minutes before configuring Stealthwatch Cloud 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 Stealthwatch Cloud to ingest flow log data stored in an S3 bucket:

Before You Begin

- Log into the Stealthwatch Cloud web UI as an administrator.

Procedure

1. Select **Settings > Integrations > AWS > Credentials**.
2. Click **Add New Credentials**.
3. Enter a descriptive **Name**.
4. Copy the saved role ARN from the plaintext editor and paste it into the **Role ARN** field.
5. Click **Create**.
6. Select **Settings > Integrations > AWS > VPC Flow Logs**.
7. Click **Add VPC Flowlog**.
8. 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 Stealthwatch Cloud integration with AWS.

9. 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.

10. Copy the displayed bucket policy JSON configuration and paste it into a plaintext editor.

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

Configure the S3 bucket policy to allow Stealthwatch Cloud to ingest flow log data:

Before You Begin

- Log into your AWS Management Console, and access the IAM dashboard.
- Log into the Stealthwatch Cloud web UI as an administrator.

Procedure

1. In the IAM dashboard, select **Policies**.
2. Click **Create Policy**.
3. Select the JSON tab.
4. Copy the bucket policy JSON configuration from the plaintext editor and paste it into the policy editor, overwriting the existing bucket policy.
5. Click **Review policy**.
6. Enter a policy **Name**.
7. Enter an optional policy **Description**.
8. Click **Create policy**.
9. In the IAM dashboard, select **Roles**.
10. Select `swc_role`.
11. In the Permissions tab, click **Attach policies**.
12. Select the policy name you entered in step 6.
13. Click **Attach policy**.
14. In the Stealthwatch Cloud web portal UI, 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 support@obsrvbl.com with your portal name and S3 bucket name.

What to Do Next

- Verify the AWS integration. See **Verifying AWS Integration** for more information.

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 PCM configuration to start displaying traffic and entity data.

Verify AWS integration:

Before You Begin

- Log into the Stealthwatch Cloud web portal UI as an administrator.

Procedure

1. In the Stealthwatch Cloud web UI, select **Settings > Sensors**. Verify that the page displays the S3 bucket name.
2. Select **Integrations > AWS > Permissions**. Verify that the displayed AWS permissions match your expectations.

Additional Resources and Support

For further assistance, email support@obsrvbl.com.

For more information on Stealthwatch Cloud, see 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 Stealthwatch Cloud 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 Stealthwatch Cloud Free Trial Guide

Change History

Revision	Revision Date	Description
1.0	7 March 2018	Initial version.
1.1	30 May 2019	Update with S3 bucket integration information.
1.2	14 June 2019	Minor updates to configuration.
1.3	22 October 2019	Updated configuration instructions.
1.4	13 August 2020	Corrected rendering on flow log syntax format.
1.5	16 October 2020	Updates based on UI updates, and clarification on flow log format.
1.6	26 January 2021	Updates for Cloud Posture Management, including required permissions.
1.7	18 February 2021	Updates for UI restructure.

Copyright Information