Cisco Stealthwatch Cloud

Public Cloud Monitoring for Microsoft Azure Quick Start Guide

Public Cloud Monitoring Configuration for Microsoft Azure

Stealthwatch Cloud Public Cloud Monitoring (PCM) is a visibility, threat identification, and compliance service for Microsoft Azure. Stealthwatch Cloud consumes network traffic data, including Network Security Group (NSG) flow logs, from your Azure 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 NSG flow logs directly from your Azure storage account, and uses an application to gain additional context.

To configure Azure to generate and store flow log data, and Stealthwatch Cloud to ingest that flow log data:

- In Azure, have at least one resource group to monitor. See **Creating an Azure Resource Group** for more information.
- In Azure, obtain your Azure AD URL and subscription ID. See **Obtaining the Azure Active Directory URL and Subscription ID** for more information.
- In Azure, create an AD application, then associate roles with the application. See **Creating an Azure AD Application** and **Assigning an Azure Role to an Application** for more information.
- In Azure, create a storage account for the flow log data, then generate a SAS URL. See **Creating an Azure Storage Account to Store Flow Log Data** and **Generating an Azure Storage Account Shared Access Signature URL** for more information.
- In Azure, enable Network Watcher and flow logs. See **Enabling Azure Network Watcher** and **Enabling Azure NSG Flow Logs** for more information.
- In Azure, if you want additional visibility on activity taken, configure your storage account to store activity logs. See **Enabling Azure Activity Log Storage** for more information.
- In Stealthwatch Cloud, upload Azure credential and flow log storage information, including the AD URL, subscription ID, application ID and key, and blob service SAS URL. See **Stealthwatch Cloud Integration with Azure**for more information.

Creating an Azure Resource Group

First, ensure you have one or more resource groups that you want to monitor. You can use existing resource groups, or create a new resource group and populate it with resources, such as virtual machines.

Create the resource group:

Before You Begin

- Log into the Azure portal.

Procedure

1. Select **Resource Groups**.
2. Click **Add**.
3. Enter a **Resource group name**.
4. Select your **Subscription**.
5. Select a **Resource group location**.
6. Click **Review + create**.
7. Click **Create**.

Obtaining the Azure Active Directory URL and Subscription ID

To provide Stealthwatch Cloud access to Azure metadata services, obtain your Azure Active Directory (AD) URL and Azure subscription ID. Record this information; you will upload this information to the Stealthwatch Cloud web portal UI at the end of this process to complete your integration with Azure.

Obtain the AD URL and subscription ID:

Before You Begin

- Log into the Azure portal.

Procedure

1. Select **Azure Active Directory > Overview**.
2. Copy the AD URL and paste it into a plaintext editor.

3. Select **Subscriptions**, then select your subscription.
4. Copy the subscription ID and paste it into a plaintext editor.

Creating an Azure AD Application

After you obtain the AD URL and subscription ID, create an application to allow Stealthwatch Cloud to read metadata from your resource groups. Copy the application key after you finish creating the application.

> ⓘ Create **only one application** per Active Directory instance. You can monitor multiple subscriptions in an Active Directory instance by assigning roles to the application. See **Assigning an Azure Role to an Application** for more information.

Create an AD application:

Before You Begin

- Log into the Azure portal.

Procedure

1. Select **Azure Active Directory > App Registrations > New Registration**.
2. Enter `swc-reader` as the **Name**.
3. Select `Web` from the **Redirect URI** drop-down.
4. Do not change the default **Supported Account Types** selection.
5. Enter `https://obsrvbl.com/azure-api/swc-reader` as the **Redirect URI**.
6. Click **Register**.
7. Copy the **Application ID** and paste it into a plaintext editor.
8. Select **Certificates and Secrets > New Client Secret**.
9. Enter `SWC Reader` as the **Description**.
10. Select `Never expires` from the **Expires** drop-down.
11. Click **Save**.
12. Copy the application key **Value** and paste it into a plaintext editor.

> ⓘ Copy the application key now, as you cannot view the key after you navigate away from this page.

Assigning an Azure Role to an Application

After you register the `swc-reader` app in AD, assign the Network Contributor and Monitoring Reader roles to it, which allows it to read metadata from your resource groups. Perform the following procedure for each subscription you want to monitor.

Assign a role to an AD application:

Before You Begin

- Log into the Azure portal.

Procedure

1. Select **Subscriptions**, then select your subscription.
2. Select **Access Control (IAM)**.
3. Select **Add > Add role assignment**.
4. Select the `Network Contributor` **Role**.
5. Select `Azure AD user, group, or service principal` from the **Assign access to** drop-down.
6. Enter `swc-reader` in the **Search by name or email address** field and select it.
7. Click **Save**.
8. Select **Add > Add role assignment**.
9. Select the `Monitoring Reader` **Role**.
10. Select `Azure AD user, group, or service principal` from the **Assign access to** drop-down.
11. **Select** the `swc-reader` app from the drop-down.
12. Click **Save**.

Creating an Azure Storage Account to Store Flow Log Data

After you assign the Network Contributor and Monitoring Reader roles to the `swc-reader` app, create a storage account to store the flow log data. Create a binary large object (blob) storage account in the same location as your resource groups.

> ⓘ You can reuse an existing Storage Account if it can store blobs and is in the same location as your resource groups.

After you create the blob storage account, ensure that the firewall rules allow access to the storage account from the internet, so that Stealthwatch Cloud can properly integrate with your Azure deployment.

Create a blob storage account:

Before You Begin

- Log into the Azure portal.

Procedure

1. Select **Storage Accounts**.
2. Click **Add**.
3. Select your **Subscription**.
4. Select the **Resource group** you want to monitor.
5. Enter a **Storage account name**.
6. Select the same **Location** for the storage account as the resource group you specified.
7. Select `Storage v2 (general purpose)` for the **Account kind**.
8. Select a **Replication** option from the drop-down, based on your organization's requirements.
9. Select the `Hot` or `Cool` access tier, depending on how often you plan to have blobs accessed within the storage account.
10. Click **Review + create**.
11. Click **Create**.

Enable internet access to the blob storage account:

Procedure

1. From the blob storage account, select the **Firewalls and virtual networks** setting.
2. Select **Allow access from** `All networks`, then save your changes.

Generating an Azure Storage Account Shared Access Signature URL

After you create a storage account, generate a shared access signature (SAS) for the storage account to allow Stealthwatch Cloud permission to retrieve the flow log data from the storage account. Then, copy the Blob service SAS URL. Stealthwatch Cloud uses the Blob service SAS URL to retrieve the flow log data from the storage account.

> ⓘ SAS permissions are time-limited, based on configuration. If your SAS permissions expire, Stealthwatch Cloud cannot retrieve flow log data from the storage account.

Generate a SAS URL:

Before You Begin

- Log into the Azure portal.

Procedure

1. Select **More Services > Storage > Storage Accounts**.
2. Select the storage account configured to store flow log data.
3. Select **Shared access signature**.
4. Select the `Blob` **Allowed services**.
5. Select the `Service`, `Container`, and `Object` **Allowed resource types**.
6. Select the `Read` and `List` **Allowed permissions**.
7. Enter a **Start time** corresponding to your current time.
8. Enter an **End time** corresponding to at least one year from the current time.
9. Select the `HTTPS` Allowed protocols.
10. Click **Generate SAS and connection string**.
11. Copy the **Blob service SAS URL** and paste it into a plaintext editor.

Enabling Azure Network Watcher

After you generate the blob storage SAS URL, enable Network Watcher in the region containing your resource groups, if you have not already enabled it. Azure requires Network Watcher to enable flow logs for your network security groups.

Enable Network Watcher:

Before You Begin

- Log into the Azure portal.

Procedure

1. Select **Network Watcher > Overview**.
2. Select the regions list to expand it.
3. Select the context menu for the region containing your resource groups, then select **Enable Network Watcher**.

Enabling Azure NSG Flow Logs

After you enable Network Watcher, enable NSG flow logs for one or more network security groups. These network security groups should correspond with the resource groups you want to monitor.

> ⓘ Blob storage accounts do not support NSG flow log retention periods.

Enable flow logging:

Before You Begin

- Log into the Azure portal.

Procedure

1. Select **Network Watcher > NSG Flow Logs**.
2. Select a network security group.
3. Select the `On` **Status**.
4. Select **Flow Logs** `Version 2`.
5. Select the blob **Storage account** for which you configured an SAS in **Generating an Azure Storage Account Shared Access Signature URL**.
6. Select `Off` for the **Traffic Analytics** status.

   > ⓘ Stealthwatch Cloud does not require enabling Traffic Analytics, but you can enable it if your organization wants the functionality.

7. Click **Save**.
8. Repeat steps 2 through 7 for each network security group for which you want to enable flow logging.

Enabling Azure Activity Log Storage

Stealthwatch Cloud is adding additional visibility and security detections for subscription-level events. To enable this feature, configure an export of the activity log to a storage account.

Export the activity log to your storage account:

Procedure

1. From the Azure portal, select **Monitor > Activity Log > Diagnostic Settings**.
2. Click the banner to **launch the 'Export activity log' blade**.
3. In the blade that appears, specify the following:
    - Select your **Subscription** from the drop-down.
    - Select the **Regions** to export from the drop-down.
    - Select **Legacy experience**.
    - Select **Export to storage account**.
    - Select your configured storage account.
    - Select *7***Retention (days)**.
4. Click **Save**.

Stealthwatch Cloud Integration with Azure

After you configure flow logging, enter the following information in the Stealthwatch Cloud web portal UI to complete your integration with Azure:

- Azure AD URL
- Subscription ID
- Application ID
- Application Key
- Blob service SAS URL

Configure Stealthwatch Cloud to ingest flow log data from Azure:

Before You Begin

- Log into the Stealthwatch Cloud web UI as an administrator.
- See **Obtaining the Azure Active Directory URL and Subscription ID** for more information on the AD URL and subscription ID.
- See **Creating an Azure AD Application** for more information on the application ID and key.
- See **Generating an Azure Storage Account Shared Access Signature URL** for more information on the Blob Service SAS URL.

Procedure

1. Select **Settings > Integrations > Azure > Credentials**.
2. Click **Add New Credentials**.
3. Enter your **Azure AD URL**.
4. Enter the Azure **Application ID**.
5. Enter the Azure **Application Key**.
6. Click **Create**.
7. Click **Storage Access**.
8. Click **New Integration**.
9. Enter the **Blob Service SAS URL** in the **API Key** field.
10. Click **Create**.
11. Select Subscriptions and ensure that your subscription is listed.

Appendix: Azure Permissions Required for Stealthwatch Cloud Integration

The following table details the role memberships required to configure Azure for integration with Stealthwatch Cloud:

Action	Permission required for member user (native tenant member)	Permission required for guest user (collaboration guest)
Creating an Azure Resource Group	add member user to Storage Account Contributor role	add guest user to Storage Account Contributor role
Obtaining the Azure Active Directory URL and Subscription ID	default permission of member user	default permission of guest user to obtain AD URL, add guest user to Cognitive Services User role to obtain Subscription ID
Creating an Azure AD Application	default permission of member user to create the AD application registration, default permission of member user to generate a client secret if the user created the application registration	add guest user to Application Developer ole
Assigning an Azure Role to an Application	default permission of member user, if user created the application registration	add guest user to Application Developer role
Creating an Azure Storage Account to Store Flow Log Data	add member user to Storage Account Contributor role	add guest user to Storage Account Contributor role
Generating an Azure Storage Account Shared Access Signature URL	add member user to Storage Account Contributor role	add guest user to Storage Account Contributor role
Enabling Azure Network Watcher	add member user to Network Contributor role	add guest user to Network Contributor role
Enabling Azure NSG Flow Logs	add member user to Network Contributor role	add guest user to Network Contributor role
Enabling Azure Activity Log Storage	add member user to Monitoring Contributor role	add guest user to Monitoring Contributor role

For more information on roles and permissions, search for the following terms on Microsoft's Azure documentation:

- guest and member user permissions
- Application Developer role
- Cognitive Services User role
- Monitoring Contributor role
- Network Contributor role
- Storage Account Contributor role

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	6 December 2018	Initial version.
1.1	20 March 2019	Updated to remove mentions of beta.
1.2	1 November 2019	Updated with activity log storage information and additional role information.
1.3	10 January 2019	Updated with removal of flow log retention configuration.
1.4	26 August 2020	Update with information about internet access for blob storage account.
1.5	16 October 2020	Updates based on UI update.
1.6	2 February 2021	Updates for how to create the storage account.

Copyright Information