EASTWIND

Eastwind for Logs Setup Guide

The Challenge:

Enterprises today fight a complicated battle: there is a global army of hackers who never sleep and who are looking for new and creative ways to break into networks, whether hosted or on-premise. Eastwind arms security teams with comprehensive visibility.

The Solution:

EASTWIND
Logs

The Benefits:

- Combine logs with telemetry from network sensors, SaaS, IaaS, and DNS.
- End to end cyber security and visibility of your infrastructure.
- Enhance your Breach Analytics with Eastwind for Logs telemetry.

Overview

Eastwind for Logs allows organizations to monitor connections to their Log telemetry and feeds data to the Eastwind Breach Analytics Cloud. Eastwind for Logs requires a simple connections and configurations to IaaS providers as well as on-prem log sources.

This document outlines the following steps required to connect Eastwind to a growing number of log sources:

1. - Connect to and configure AWS log sources.
2 - Connect to and configure Azure log sources

Once you are connected to the Eastwind Portal, it will provide insights into data, such as:

- Failed/Successful Logon Attempts
- Login IP metadata such as country and blacklist/whitelist designation
- Document Create/View/Update/Delete/Download operations
- API Authorization Failed/Success

Before you get started note the following

Eastwind for Logs requires a pre-existing cloud services account or access to physical and virtural hosts on your network with sufficient rights to connect those sources to the Eastwind Breach Analytics Cloud. You must also have an Eastwind Networks account to access the Eastwind Portal. Click here if you have not already created an Eastwind Account.

Connect to and Configure AWS Log Sources

Create AWS IAM user access keys

Obtain the AWS API Keys

To connect Eastwind to the AWS Logs API logon to the AWS console:

- Select Security, Identity & Compliance -> IAM -> Users -> Add user
- User name: Eastwind_for_AWS -> Select Programmatic access* -> Next:permissions
- Select Create Group: type in: Group name: Eastwind_for_AWS: Type in and select: AWSCloudTrailFullAccess under policy type -> Create Group
- Click on Next Review -> Create User

Either Download the CSV or record the Access key ID and Secret access key, this is the only time you will have access to the Secret access key.

Grant Eastwind for Logs Access to your AWS implementation

In order to Collect and analyze the AWS Logs, you will need to enter the Access Keys into the Eastwind portal.

- Logon to the Eastwind portal, click on Data Sources -> AWS
- Enter the AWS API keys created earlier.
- Click on Authorize access to AWS Cloud Telemetry

Connect to and Configure Microsoft Azure Log Sources

Obtain the Azure Subscription ID

To connect Eastwind to the Azure Logs service, logon to the Azure Portal:

- Cost Management + Billing –> Subscriptions -> My Subscriptions
- Copy the Subscription ID that you would like Eastwind for Logs to read

Grant Eastwind for Logs Access to your Azure implementation

In order to Collect and analyze the AWS Logs, you will need to enter the Access Keys into the Eastwind portal.

- Logon to the Eastwind portal, click on Data Sources -> Azure
- Enter the Azure Subscription ID you was copied in the previous section.
- Click on Authorize access to Azure Telemetry

You will get redirect to Azure portal where you will need to provide the consent to integrate Eastwind with Azure. Upon consent and successful authentication, you will automatically get redirected back to the Eastwind Azure configuration page.

Troubleshooting Issues when Connecting

If the Logs connection to the Eastwind Breach Analytics Cloud was unsuccessful you will see a warning banner showing at the top of the Eastwind Portal. Please either retry the steps or contact Eastwind support.

View Logs Data in the Eastwind Portal

Once connected, any communication to the Logs API on a monitored network will be logged in the Eastwind Breach Analytics Cloud and viewed in the Eastwind Portal. To view the data, logon to the Eastwind portal at portal.eastwindnetworks.com using the provided credentials and follow the steps below:

1. Click on the Dashboard link in the left navigation panel.
2. Click on the Open link in the top right-hand menu navigation.
3. Select the specific Logs Telemetry link in the Featured Dashboards menu.

For more information on Eastwind for AWS Logs,
please see eastwindnetworks.com