EASTWIND

Eastwind for AWS 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
AWS

The Benefits:

- Complete cyber security and visibility of your IaaS solutions.
- Enhance your Breach Analytics with Eastwind for AWS telemetry.
- Streamline your procurement; No POs required; Be up and running in minutes.

Overview

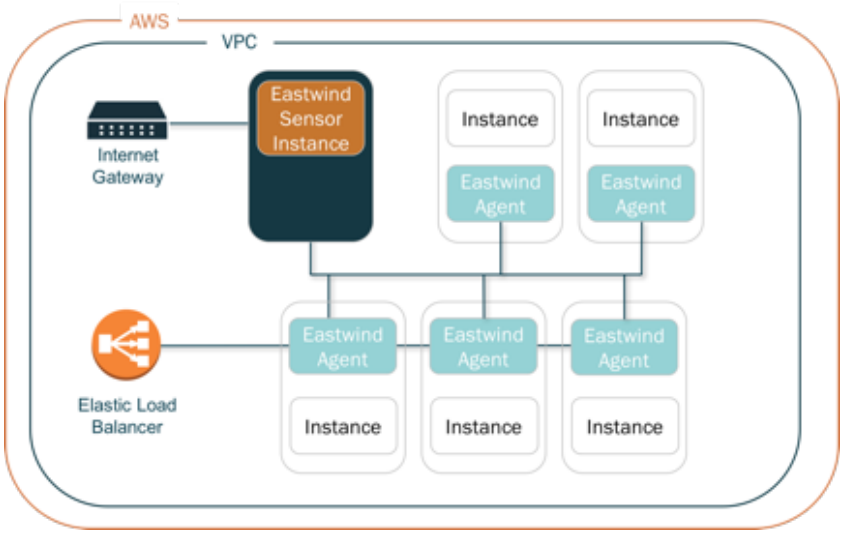
The Eastwind for AWS solution provides complete visibility of your AWS network traffic going to and from your EC2 cloud. The solution operates by creating an Eastwind Sensor instance in your EC2 network, then configuring existing components to mirror packets to that Sensor instance. This Setup Guide provides step-by-step instructions for launching an Eastwind for AWS Sensor connected to the Eastwind Breach Analytics Cloud.

This document outlines the following steps required to setup Eastwind for AWS:

1. Link your Eastwind Account to your AWS Account ID
2. Install Eastwind Sensor
3. Install Eastwind Traffic Agent
4. Verify and View Data in the Eastwind Portal

Before you get started note the following

You must have an Eastwind Networks account to access the Eastwind Portal. You must have an Eastwind Networks account to access the Eastwind Portal. Click here if you have not already created an Eastwind Account.



Note: this Setup guide provides an introductory example of deploying Eastwind for AWS, and does not show all the capabilities of the solution. For more detailed information, please see https://www.eastwindnetworks.com/ Additionally, this guide assumes a working knowledge of AWS/EC2, for further information please refer to appropriate AWS documentation.

Link Your Eastwind Account to your AWS Account ID

To link your Eastwind account to your AWS Account ID, follow these steps:

- Login to the Eastwind Portal with your Eastwind Username and Password
- Navigate to Data Sources -> Sensors -> AWS Account ID tab
- Enter your AWS Account ID

Configure and Launch the Eastwind for AWS Sensor

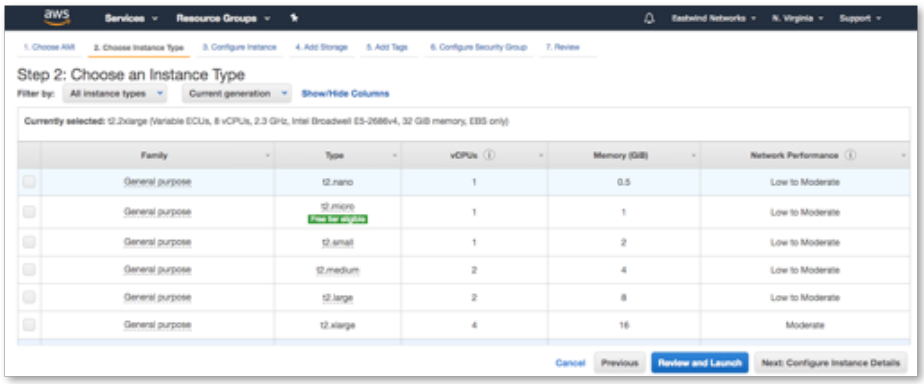
To install the Eastwind Sensor you will Logon to the EC2 Console, Launch the Eastwind AMI, Configure the Instance, create a Security Group, then Launch the Instance.

Choose AMI

Logon to the EC2 Management Console and click on Launch Instance to launch AWS instance Launch wizard. Click on the AWS Marketplace, search for Eastwind and select the Eastwind Sensor - Production AMI.

Choose Instance Type

Eastwind has pre-filtered the available instance types to appropriate sizes to run the Eastwind for AWS Sensor. You will need to select an Instance Type that closely matches your expected Bandwidth requirements listed under the Network Performance column. For more information see performance details at: https://aws.amazon.com/ec2/instance-types/ or contact Eastwind support.



Note: Eastwind recommends the following instance types to support your network load:

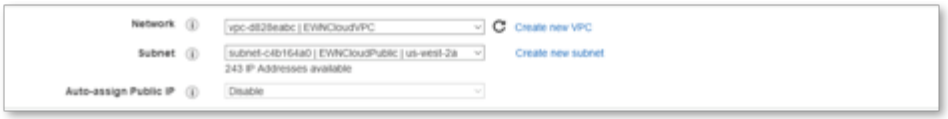
- *10Mbps*	*t2.small*	- *400Mbps*	*c4.2xlarge*
- *25Mbps*	*t2.medium*	- *450Mbps*	*c5.2xlarge*
- *50Mbps*	*t2.large*	- *600Mbps*	*c4.4xlarge*
- *100Mbps*	*c4.large*	- *650Mbps*	*c5.4xlarge*
- *150Mbps*	*c5.large*	- *1000Mbps*	*c4.8xlarge*
- *200Mbps*	*c4.xlarge*	- *2000Mbps*	*c5.9xlarge*
- *250Mbps*	*c5.xlarge*	- *5000Mbps*	*c5.18xlarge*

Choose Next: Configure Instance Details.

Configure Instance Details

SETUP NETWORKING

Choose a VPC and subnet that has access to the internet. If necessary, add any additional Network Interfaces to provide monitoring for instances on alternate subnets.



Add Storage.

The minimum storage volume is 64GB, the storage used to buffer data in case the sensor is temporarily unable to deliver data to the cloud.

Add Tags

Add tags as needed.

Configure Security Group.

Add a custom UDP rule to allow data to enter the Eastwind Sensor,

Click on Add Rule and add a new inbound rule for type SSH Traffic to destination 22 from Anywhere.

Click on Add Rule and add a new inbound rule for type Custom UDP Traffic to destination 7141 from Anywhere.

Then click on Outbound and remove the default outbound rule.

Review and Launch the instance.

Install Eastwind Traffic Agent on Source Instances

Install Eastwind Traffic Agent on Source Instances

Once the Eastwind Sensor is running, you will need to Install the Eastwind Traffic Agent on each of the AWS Source Instances you wish to monitor. These Agents are responsible for routing and delivering traffic to the Eastwind Sensor. You will need the IP address of the Eastwind Sensor configured previously, you can find this information in the EC2 Management Console.

Eastwind Traffic Agent Install

To install on a Linux Instance deployed in AWS follow these steps: Open an SSH connection the IP address of the AWS instance which want to monitor. Download the installation script from the Eastwind portal at: https://portal.eastwindnetworks.com/app/portal#/data_sources/sensors click on the “Download Traffic Agent”, then copy it to the instance where it is to be run.

Make the file executable:

 # chmod 755 EWNTrafficAgentInstaller

The command requires root access, run with sudo:

 # sudo EWNTrafficAgentInstaller -i address_of_sensor <-b “bpf filter”>

Examples:

Capture all traffic and forward to sensor

 # sudo EWNTrafficAgentInstaller -i 10.44.22.11

capture all traffic except ports 22 and 4422

 # sudo EWNTrafficAgentInstaller -i 10.44.22.11 -b “not port 22 and not port 4422”

Verify and View Data in the Eastwind Portal

Once Installed, you can view the Eastwind Sensor telemetry in the Eastwind Breach Analytics Cloud. To view the data, logon to the Eastwind Portal at portal.eastwindnetworks.com. For additional resources see https://www.eastwindnetworks.com/resources/.

EASTWIND

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