EASTWIND

Eastwind for AWS, powered by Ixia CloudLens 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 - Ixia

The Benefits:

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

Overview

Eastwind has partnered with Ixia to provide a fine-grained security architecture for workloads migrated to public cloud. Ixia CloudLens acts as the data collection resource, dynamically passing copies of the desired packet level data to the Eastwind breach analytics cloud.

This document outlines the following steps required to setup Eastwind for AWS, powered by Ixia:

1. Link your Eastwind Account to your AWS Account ID
2. Install Eastwind Sensor Powered by Ixia CloudLens
3. Install Ixia CloudLens Agents
4. Route Traffic to the Eastwind Sensor Instance
5. 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. Click here if you have not already created an Eastwind Account.

Please ensure you have access to the following items in order to complete the install:

- CloudLens account created https://ixia.cloud/
- Admin access to the AWS console.
  - Create and Apply Security Groups and Policies
  - Access to Account Settings in the AWS Console to acquire the Amazon Account Id.
- SSH access with sudo to the newly created Eastwind Sensor.
- SSH access with sudo to any workload instances that are to be monitored.
- Admin access to any Windows workload instances that are to be monitored.
- Access can be limited by firewall if the following ports are allowed access to the internet.
  - Cloudlens access
    - UDP port 19993 to Destination ANY IP (0.0.0.0/0)
  - Eastwind Access
    - TCP ports 80,443 to ANY IP (0.0.0.0/0)
    - TCP ports 8443,40000-40007,41000-41003 to Destination 208.53.59.200

Technical Overview Eastwind for AWS, powered by Ixia CloudLens

The Ixia CloudLens Agent deploys onto the Operating System of Source Instances i.e. Cloud Servers (e.g. Linux Servers, Windows Servers) running application workloads which you wish to monitor. The CloudLens Sensor also deploys onto the OS of Tool Instances (e.g. Eastwind Cloud Sensor). In both cases the CloudLens Sensors register outbound to the CloudLens Management Portal.

The Ixia CloudLens Agent has been tested on all major Linux Distributions, Linux Kernel 3.10 or newer is officially supported (type ‘uname -r’ as the Linux CLI to check your kernel). If you have an older kernel, please contact Ixia to check if support can be enabled. The CloudLens Agent is also tested on Window Server 2012 or newer.

The CloudLens Agent co-exists with whatever application workloads which are already running on the Cloud Server instance. The footprint of the CloudLens agent is light; however it is recommended that 1vCPU, 1G of RAM, and 5 GB of Disk is available as overhead, on top of the minimum resources required for the existing workloads. If your instance is not heavily utilized, additional resources may not be needed.

The CloudLens Agent forwards copies of packets from Source Instances to Tool Instances. AWS Instance Types have built in throttle limits on network throughput, and the copies of packets will be additive to actual production application traffic forwarded out the network. Please consider these limits for your choice of AWS Instance types, and when deciding whether to assign CloudLens filters controlling which packets to forward to Tool instances. The Ixia CloudLens Sensor itself is capable of forwarding (or on the Eastwind Power by Ixia CloudLens tool, receiving) up to 1.5 Gbps. Horizontal scaling is supported for additional capacity.

Ixia CloudLens Agents send metadata about the Cloud Instances to the Ixia CloudLens Management Portal (also hosted on AWS). Metadata is used to identify source and tool instance so that traffic flow and be managed from the Portal. (Please note that application workload packet data itself, is NOT sent up to the Management portal. Rather the customers application packet data is sent over encrypted VPN tunnels directly from their own source instances to the own tool instances in AWS, thus the customer's data remains under the scope of their existing cloud security controls). For best results choose an AWS IAM Role which allows CloudLens sufficient access to metadata; e.g. AmazonEC2ReadOnlyAccess.

Adding Custom AWS Tags to your Instances is optional, but can make for more efficient grouping and management of Instances in Ixia CloudLens. For example;

- On Source Instance you might add a Tag; with 'Key' Type, and 'Value' WebServer
- On Tool Instance you might add a Tag; with 'Key' Tool, and 'Value' Eastwind

Link Your Eastwind Account to your AWS Account ID

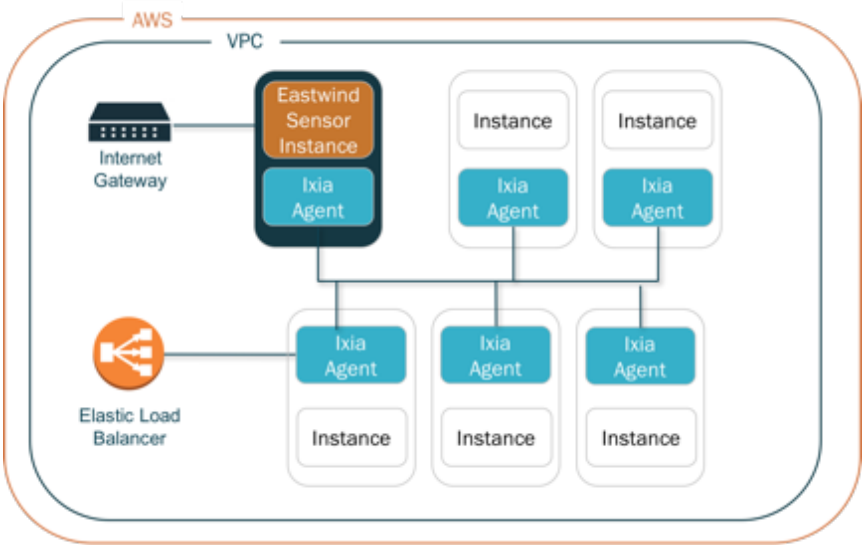
To link your Eastwind account to your AWS Account ID, follow these steps:

- 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

Install Eastwind Sensor Powered by Ixia CloudLens

To complete the Eastwind powered by Ixia configuration, you will complete the following steps.

- Configure and Launch the Eastwind Sensor
- Create an Ixia Project to obtain Project Key
- Install Ixia CloudLens Agent on Eastwind Sensor Instance
- Install Ixia CloudLens Agent on Source Instances
- Route Traffic to the Eastwind Sensor Instance



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

Configure and Launch the Eastwind 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.

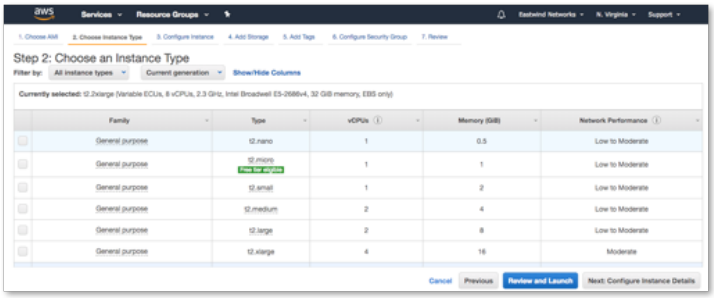
Choose AMI

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 w/Ixia 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.

Then click: Configure Instance Details



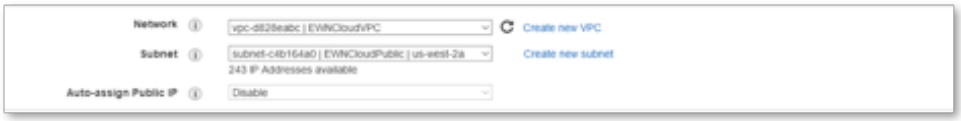
Note: Eastwind recommends the following instance types to support your network load:

- *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*

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.

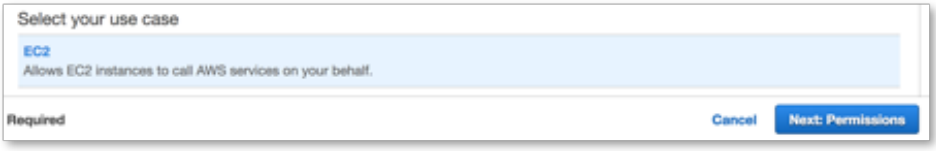


CREATE IAM ROLE

Under IAM role select Create new IAM role and perform the following steps.

CREATE ROLE

Click on Create Role, in the box labeled "Choose the service that will use this role", select EC2. A new box will appear labeled Select your use case, select EC2 then click on Next: Permissions



CREATE POLICY

Next create a policy by clicking on Create policy then click on JSON and remove any existing text.

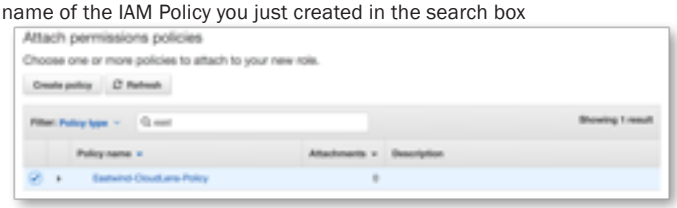
Copy/paste this link or the IAM Policy JSON from https://ixia.cloud/wizard to ensure proper formatting.

Sample:


```
{"Version":"2012-10-17","Statement":[{"Sid":"ReadOnly","Effect":"Allow","Action":"ec2:Describe*","Resource"
:"*"},{"Sid":"Related","Effect":"Allow","Action":["cloudwatch:DescribeAlarms","cloudwatch:GetMetricStatisti
cs","sts:DecodeAuthorizationMessage"],"Resource":"*"}]}
```


Click on Review Policy, and in the Name box give the policy a name, for example Eastwind-CloudLens-Policy. Complete the IAM by clicking on Create Policy.

Go back to the Attach permissions policies tab in the browser. Click the Refresh button to allow your new policy to be found. Enter the name of the IAM Policy you just created in the search box



Click Next: Review. Now give the Role a name, for example Eastwind-CloudLens-Role and click Create Role. Back on the Configure Instance Details page click on the refresh icon next to the IAM role Dialog and select the role just created.

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.

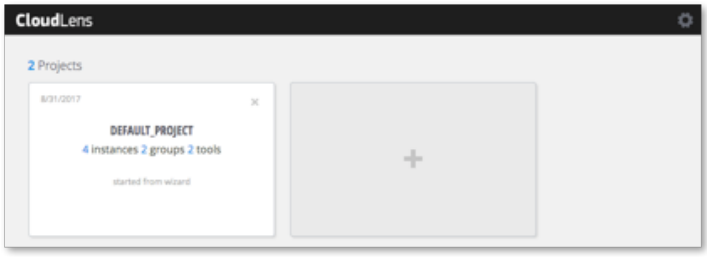
Add a rule to allow CloudLens data to enter the Eastwind Sensor, click on Add rule for Custom UDP port, with a port value of 19993 from source Anywhere (0.0.0.0/0) or enter the CIDR of the subnet of the instances that will be delivering CloudLens data to the Eastwind Sensor. Ensure that an Inbound ssh rule from anywhere exists.

Review and Launch the instance.

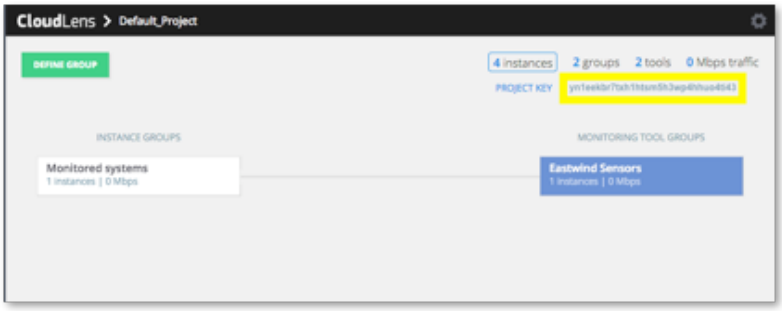
Install Ixia CloudLens Agents

Create an Ixia Project to obtain Project Key

In order to Install Eastwind and Ixia you will need to create a new project in the Ixia Portal. To create a project logon to https://ixia.cloud/login, then either utilize the initial 'Default Project' or create your own by click the + symbol in the box. You will need to sign up for an Ixia account if you do not already have one.



Once created, open the project and document the unique Project Key which you will need later.



Configure Ixia CloudLens Agent on Eastwind Sensor Instance

Once the Ixia CloudLens Agent is configured, you will need to Install the Agent on each of the AWS Source Instances (Instance Groups) you wish to monitor. These Agents are responsible for routing to Eastwind Sensor.

Open an SSH connection to the IP address of the Eastwind Sensor Instance, you can find the IP address in the EC2 Console. Once logged in, run the following commands;

(substitute the Project Key and IP Address created earlier).

Local Machine: # *ssh ubuntu@IP Address*

AWS Instance: # *sudo setupIxiaAgent Project Key*

Install Ixia CloudLens Agent on Source Instances

The CloudLens Agent runs on either Linux (as a Docker Container) or Windows (as a Service). Use the appropriate method outlined below to direct any or all traffic to your Eastwind Sensor depending your environment.

Ixia Agent Linux Install

To install on a Linux Instance deployed in AWS follow these steps:

Open an SSH connection the Public IP address of the AWS instance which want to monitor. Once connected, enable root access to the OS CLI (e.g. sudo su -).

Install Docker CE using yum/apt, then start the service.

```
AWS Instance:  # yum update
AWS Instance:  # yum –y install docker
AWS Instance:  # service docker start
```

OR

```
AWS Instance:  # sudo apt-get -y remove docker docker-engine docker.io
AWS Instance:  # sudo apt-get -y install \
               apt-transport-https \
               ca-certificates \
               curl \
               software-properties-common
AWS Instance: # curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo apt-key add -
AWS Instance: # sudo add-apt-repository \
                  "deb [arch=amd64] https://download.docker.com/linux/ubuntu \
                  $(lsb_release -cs) \
                  stable"
AWS Instance: # sudo apt-get -y update
AWS Instance: # sudo apt-get -y install docker-ce
```

Use the 'docker run' command outlined below to access the Ixia repository and obtain the cloudlens-s-Container.

Note: You will need to insert your (Project Key) from the Ixia Portal into the docker command. Copy/paste this link or the "Start the CloudLens agent" docker command from https://ixia.cloud/wizard to ensure proper formatting.

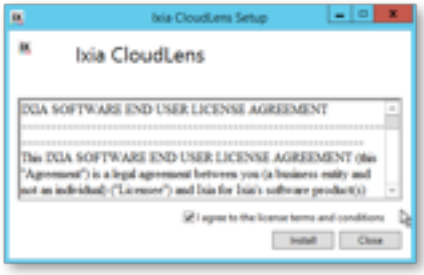
```
AWS Instance: # docker run \
        -v /:/host \
        -v /var/run/docker.sock:/var/run/docker.sock \
        --privileged \
        --name cloudlens-agent -d --restart=on-failure \
        --net=host ixiacom/cloudlens-agent \
        --accept_eula yes \
        --server agent.ixia.cloud \
        --apikey (Project Key)
```

Note: the --name field is arbitrary but useful to specify when troubleshooting (here it is 'cloudlens').

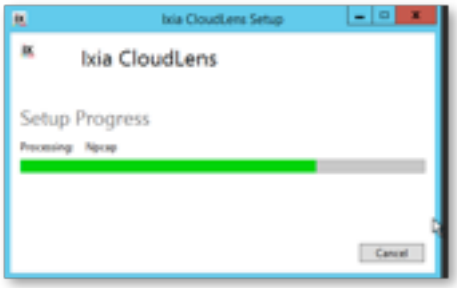
Ixia Agent Windows Install

To install on a Windows Instance deployed in AWS, download the Ixia CloudLens Windows Agent onto the Server: https://win-agent.ixia.cloud/cloudlens-win-agent-latest.exe

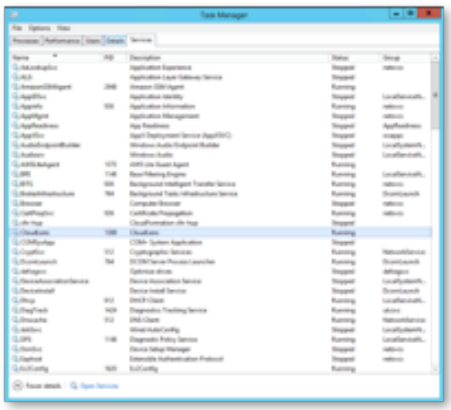
Double-Click the Sensor installer, then accept the EULA



The Ixia CloudLens wizard goes through the agent installation and installs all dependent packages. When prompted, enter your applicable Project Key which you setup earlier.



To verify CloudLens Service is Running – Go to Task Manager – Services



Route Traffic to the Eastwind Sensor Instance

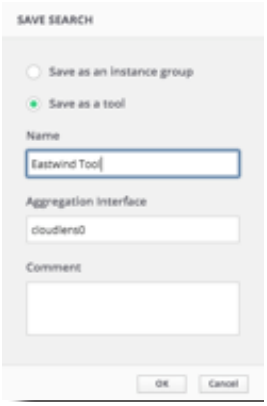
Once the Agents are installed on the systems to be monitored, you will need to logon to the CloudLens Management Portal https://ixia.cloud/login to define a Monitoring Tool Group, Source Instance Monitoring Group(s), and Connections.

To begin, double click the Project created earlier (to obtain the Project Key) and click on either the Define A Group Button or Instances on the upper right of the screen.

Create a Monitoring Tool Group

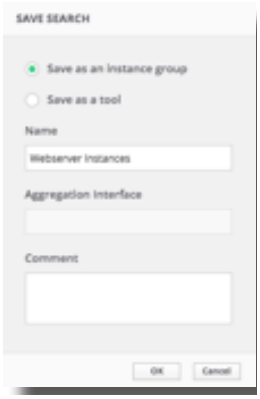
The Monitoring Tool Group will only contain the Eastwind Sensor Instance. Use the Filters to select this Instance. Filters include: Tag, Instance Id, or any other options that. The filters control the table of instances on the right side of the screen, ensure that only the Eastwind Sensor Instance is displayed, then click Save Group.

Choose Save as a Tool, give it a Name, leave the Aggregation Interface as cloudlens0 (unless you have explicitly modified this on the Eastwind Sensor Instance), then click OK.



Create a Source Instance Monitoring Group

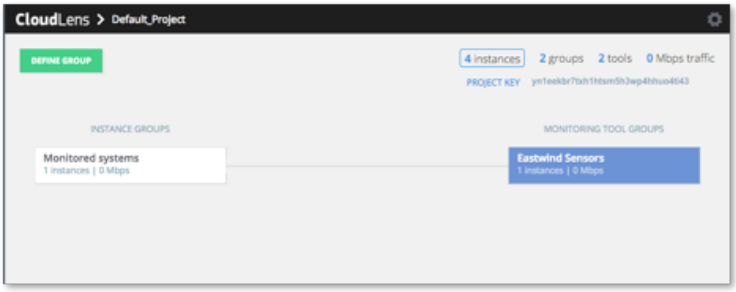
The Source Instance Monitoring Group will contain all the systems to be monitored. Follow the previous step but this time choose any or all of the Source Instances you wish to monitor. Choose the applicable filters, then click on Save Group.



Choose Save as instance group, give it a Name, then click OK and Close

Connect the Instance Groups and Monitoring Tool Groups

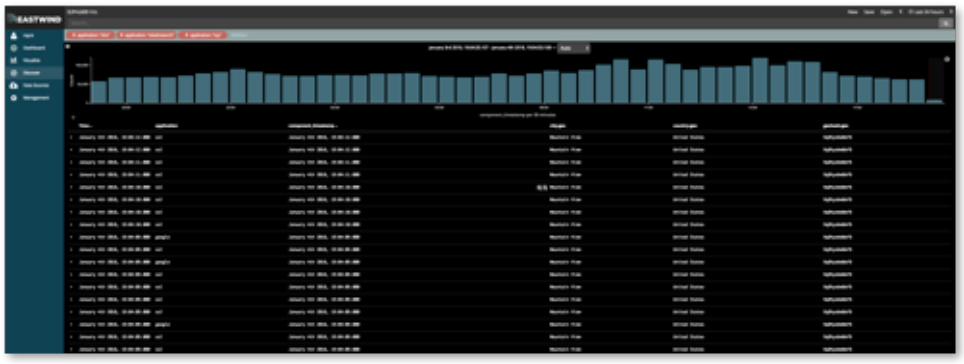
To connect the Source and Monitoring groups, drag a connection between the Instance Group, and Tool Group. Copies of the Source Instance traffic will now be copied over to the Eastwind Sensor (traffic is securely forwarded over an Encrypted Peer to Peer VPN Tunnel established by CloudLens).



Note: Use of Tagging allows future Instances to automatically join the desired group. In this example, future AWS Instances with CloudLens Sensor enabled, and with Name Tag equal to 'Source-AWS-Workload' will automatically be added to the Source Groups and available to have their traffic forwarded to Eastwind powered by Ixia CloudLens.

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 www.eastwindnetworks.com/resources/.



Additional Support

For additional support, contact an Eastwind representative at support@eastwindnetworks.com or 385-355-3455.

To purchase the Eastwind for AWS product, please visit us at www.eastwindnetworks.com or aws.amazon.com.

Sign up for Ixia CloudLens, please visit the Ixia store at store.ixiacom.com or email cloudlens@ixiacom.com.

EASTWIND

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