Security with EastWind and CloudLens

Quick Start Reference Deployment

June 2018

Ixia, a Keysight business
AWS Quick Start Reference Team

Contents

Overview..2
EastWind and CloudLens on AWS..2
Costs and Licenses..3
Architecture..3
Prerequisites..4
Specialized Knowledge..4
Technical Requirements..4
Deployment Options..4
Deployment Steps..4
Step 1. Prepare Your AWS Account..4
Step 2. Prepare Your CloudLens Account..5
Step 3. Prepare Your Eastwind Account..5
Step 4. Launch the Quick Start..6
Step 5. Test the Deployment..8
FAQ..8
Git Repository..9

Additional Resources 9
Document Revisions 9

This Quick Start deployment guide was created by Amazon Web Services (AWS) in partnership with Ixia, a Keysight business.

Quick Starts are automated reference deployments that use AWS CloudFormation templates to deploy key technologies on AWS, following AWS best practices.

Overview

This Quick Start reference deployment guide provides step-by-step instructions for deploying Eastwind and CloudLens on the Amazon Web Services (AWS) Cloud.

This Quick Start is for users who need to identify malicious activity, insider threats and data leakage within your AWS Services.

EastWind and CloudLens on AWS

Eastwind Cloud Network Sensors, powered by Ixia CloudLens, provides complete visibility across your Infrastructure as a Service (IaaS) networks and leverages the cloud provider to scale up or down as needed. With this solution, security teams benefit from Eastwind Breach Analytics and the breadth of Ixia CloudLens visibility to better understand and address your expanding attack surface.

Benefits include:

- Intelligence: A concise picture of what is happening across all your cloud infrastructure providers is a must to all organizations. With support from AWS, your teams work in lock-step to securely deploy line-of-business applications across a wide range of public and private infrastructure.
- Insight: Understanding and integrating the activity inside and out of the traditional corporate network allows teams to evaluate which threats and threat actors are active and posing risk.
- Integrated Response and Incident Data: Giving incident responders the integrated data they need to more effectively identify and remediate threats and breaches is critical to business success.

Costs and Licenses

You are responsible for the cost of the AWS services used while running this Quick Start reference deployment. There is no additional cost for using the Quick Start.

The AWS CloudFormation template for this Quick Start includes configuration parameters that you can customize. Some of these settings, such as instance type, will affect the cost of deployment. For cost estimates, see the pricing pages for each AWS service you will be using. Prices are subject to change.

Eastwind and CloudLens tools will be configured to use a free trial account, the user can convert at any time to a paid account.

Architecture

Deploying this Quick Start for a new virtual private cloud (VPC) with **default parameters** builds the following EastWind and CloudLens environment in the AWS Cloud.

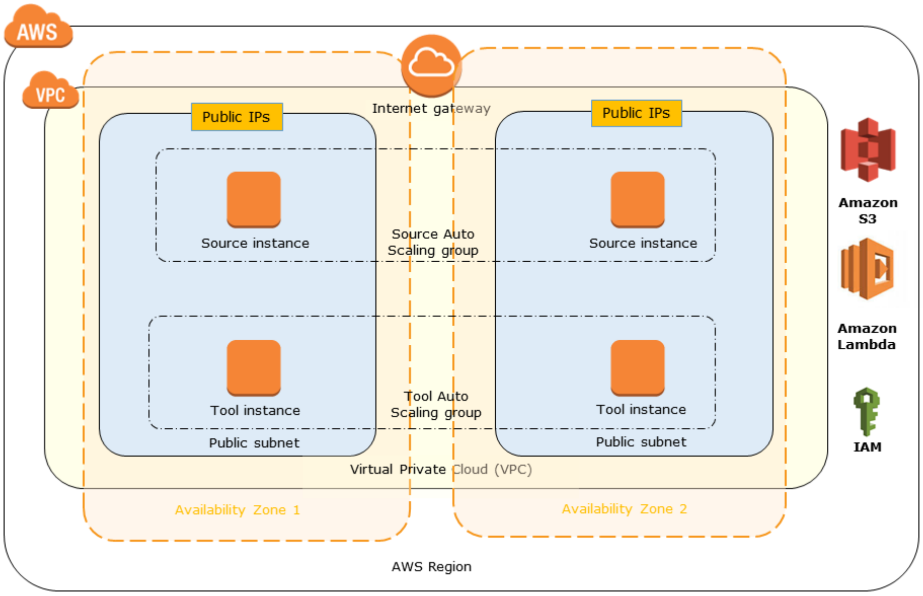

Figure 1: Quick Start architecture for EastWind and CloudLens on AWS

The Quick Start sets up the following:

- A highly available architecture that spans over two Availability Zones.

- A VPC configured with public subnets according to AWS best practices, to provide you with your own virtual network on AWS.
- An internet gateway to allow access to the internet.

Prerequisites

Specialized Knowledge

Before you deploy this Quick Start, we recommend that you become familiar with the following AWS services. (If you are new to AWS, see Getting Started with AWS.)

- Amazon EC2
- Amazon VPC
- AWS CloudFormation

Technical Requirements

Deployment Options

This Quick Start provides only the option to **Deploy Eastwind and Cloudlens into a new VPC** (end-to-end deployment). This option builds a new AWS environment consisting of the VPC, subnets, NAT gateways, security groups, bastion hosts, and other infrastructure components, and then deploys Eastwind and Cloudlens into this new VPC. Deploying into an existing VPC is not in scope for the current version of the Quick Start.

The Quick Start provides separate templates for this deployment. It also lets you configure CIDR blocks, instance types, and Eastwind and Cloudlens settings, as discussed later in this guide.

Deployment Steps

> **Note** You need to mandatory create and open free accounts on both CloudLens and Eastwind.

Step 1. Prepare Your AWS Account

1. If you don't already have an AWS account, create one at https://aws.amazon.com by following the on-screen instructions.
2. Use the region selector in the navigation bar to choose the AWS Region where you want to deploy Eastwind and CloudLens on AWS.
3. Create a key pair in your preferred region.

4. If necessary, request a service limit increase for the selected Amazon EC2 instance type. You might need to do this if you already have an existing deployment that uses this instance type, and you think you might exceed the default limit with this deployment.

Step 2. Prepare Your CloudLens Account

1. Create a CloudLens free trial account at https://ixia.cloud/free-trial?isQuickstart=true by following the on-screen instructions.
2. Activate your free trial account by visiting the link provided in the email.
3. Login to CloudLens. A project will be automatically created for you with all the required infrastructure: one group for source instances and one group for tool instances, a connection between the two groups. The groups are automatically configured with filters that match the agents that will be started later by the Quick Start deployment.
4. Select the project by clicking the tile having the name “QUICKSTART_PROJECT”.
5. On the project page click on SHOW PROJECT KEY to display the project key and copy it for later use in the CloudFormation template.

Step 3. Prepare Your Eastwind Account

1. Open up Eastwind CloudVu listing on the AWS marketplace:

   https://aws.amazon.com/marketplace/pp/B07D6P1Z9H?qid=1528824042526&sr=0-2&ref_=srh_res_product_title

2. Click on “Continue to Subscribe”, then click on “Subscribe”.
3. Click on to “Set up your account”. This redirects to the Eastwind portal account creation page.
4. Enter a company name and email address. An email is then dispatched to verify the email address.
5. Open the email and click the link to set the password.
6. Log in to the Eastwind portal using this new account.
7. Accept the EULA.
8. You will be redirected to the “Data Sources” page. Choose AWS as data source.
9. Enter AWS account ID and press Save. This automatically shares the Eastwind Sensor AMIs used by the cloudfront template with user account. Your Amazon account id is available on the Support page in the AWS Console.

10. At this point Eastwind account creation is complete and the Eastwind Sensor AMI in each region should show up under Private Images section inside AMI section of EC2 console.

Step 4. Launch the Quick Start

> **Note** You are responsible for the cost of the AWS services used while running this Quick Start reference deployment. There is no additional cost for using this Quick Start. For full details, see the pricing pages for each AWS service you will be using in this Quick Start. Prices are subject to change.

1. Use the following button to launch the AWS CloudFormation template into your AWS account.

   Deploy Eastwind and CloudLens into a new VPC on AWS

   Launch

   Each deployment takes about 10 minutes to complete.

2. Check the region that's displayed in the upper-right corner of the navigation bar, and change it if necessary. This is where the network infrastructure for Eastwind and CloudLens will be built. The template is launched in the US East (Ohio) Region by default.

3. On the **Select Template** page, keep the default setting for the template URL, and then choose **Next**.

4. On the **Specify Details** page, change the stack name if needed. Review the parameters for the template. Provide values for the parameters that require input. For all other parameters, review the default settings and customize them as necessary. When you finish reviewing and customizing the parameters, choose **Next**.

   In the following table, parameters are listed by category:

   – Parameters for deploying Eastwind and CloudLens into a new VPC

- ## Parameters for deploying Eastwind and CloudLens into a new VPC

View template

<The following parameter tables are generated automatically from the templates. Don't enter the parameter information manually. The information below is provided only as an example. We recommend that you use these group and parameter labels if you're providing similar functionality in your CloudFormation templates.>

VPC Network Configuration:

Parameter label (name)	Default	Description
Availability Zones (AvailabilityZones)	*Requires input*	The list of Availability Zones to use for the subnets in the VPC. The Quick Start uses two Availability Zones from your list and preserves the logical order you specify.
VPC CIDR (VPCCIDR)	10.0.0.0/16	The CIDR block for the VPC.
Private Subnet 1 CIDR (PrivateSubnet1CIDR)	10.0.0.0/19	The CIDR block for the private subnet located in Availability Zone 1.
Private Subnet 2 CIDR (PrivateSubnet2CIDR)	10.0.32.0/19	The CIDR block for the private subnet located in Availability Zone 2.
Public Subnet 1 CIDR (PublicSubnet1CIDR)	10.0.128.0/20	The CIDR block for the public (DMZ) subnet located in Availability Zone 1.
Public Subnet 2 CIDR (PublicSubnet2CIDR)	10.0.144.0/20	The CIDR block for the public (DMZ) subnet located in Availability Zone 2.
Permitted IP range (AccessCIDR)	*Requires input*	The CIDR IP range that is permitted to access Eastwind and CloudLens. We recommend that you set this value to a trusted IP range. For example, you might want to grant only your corporate network access to the software.

Amazon EC2 Configuration:

Parameter label (name)	Default	Description
Key Name (KeyPairName)	*Requires input*	A public/private key pair, which allows you to connect securely to your instance after it launches. When you created an AWS account, this is the key pair you created in your preferred region.

AWS Quick Start Configuration:

Parameter label (name)	Default	Description
Quick Start S3 Bucket Name (QSS3BucketName)	quickstart-reference	The S3 bucket you have created for your copy of Quick Start assets, if you decide to customize or extend the Quick Start for your own use. The bucket name can include numbers, lowercase letters, uppercase letters, and hyphens, but should not start or end with a hyphen.
Quick Start S3 Key Prefix (QSS3KeyPrefix)	atlassian/bitbucket /latest/	The S3 key name prefix used to simulate a folder for your copy of Quick Start assets, if you decide to customize or extend the Quick Start for your own use. This prefix can include numbers, lowercase letters, uppercase letters, hyphens, and forward slashes.

Step 5. Test the Deployment

As part of deployment, a simulated attack is started on the source instance to highlight the solution capabilities. The user of the Quick Start will be able to watch the attacks in real time inside Eastwind Portal, using either the Dashboard or the Visualize sections – more details TBD.

FAQ

Q. I encountered a CREATE_FAILED error when I launched the Quick Start.

A. If AWS CloudFormation fails to create the stack, we recommend that you relaunch the template with **Rollback on failure** set to **No**. (This setting is under **Advanced** in the AWS CloudFormation console, **Options** page.) With this setting, the stack's state will be retained and the instance will be left running, so you can troubleshoot the issue. (Look at the log files in `%ProgramFiles%\Amazon\EC2ConfigService` and `C:\cfn\log`.)

> **Important** When you set **Rollback on failure** to **No**, you will continue to incur AWS charges for this stack. Please make sure to delete the stack when you finish troubleshooting.

For additional information, see Troubleshooting AWS CloudFormation on the AWS website.

Q. I encountered a size limitation error when I deployed the AWS Cloudformation templates.

A. We recommend that you launch the Quick Start templates from the location we have provided or from another S3 bucket. If you deploy the templates from a local copy on your computer or from a non-S3 location, you might encounter template size limitations when you create the stack. For more information about AWS CloudFormation limits, see the AWS documentation.

Git Repository

You can visit our GitHub repository to download the templates and scripts for this Quick Start, to post your comments, and to share your customizations with others.

Additional Resources

AWS services

- Amazon EC2
  https://aws.amazon.com/documentation/ec2/
- Amazon VPC
  https://aws.amazon.com/documentation/vpc/
- AWS CloudFormation
  https://aws.amazon.com/documentation/cloudformation/

Eastwind and CloudLens documentation

- CloudLens Public

  https://www.ixiacom.com/products/cloudlens-public
- Eastwind powered by Ixia CloudLens

  https://www.eastwindnetworks.com/cloudlens

Quick Start reference deployments

- AWS Quick Start home page
  https://aws.amazon.com/quickstart/

Document Revisions

Date	Change	In sections
June 2018	Initial publication	—

Notices

This document is provided for informational purposes only. It represents AWS's current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS's products or services, each of which is provided "as is" without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.