Security with CloudLens and Eastwind on the AWS Cloud

Quick Start Reference Deployment

January 2019

Ixia, a Keysight business
Amazon Web Services (AWS)

Contents

Overview ................................................................................................................................. 2
Costs and Licenses.............................................................................................................. 2
Architecture ......................................................................................................................... 3
Prerequisites ......................................................................................................................... 5
Technical Requirements .................................................................................................... 5
Specialized Knowledge ....................................................................................................... 5
Deployment Options .............................................................................................................. 5
Deployment Steps .................................................................................................................. 6
  Step 1. Prepare Your AWS Account .................................................................................... 6
  Step 2. Prepare Your CloudLens Account .......................................................................... 6
  Step 3. Prepare Your Eastwind Account ............................................................................ 7
  Step 4. Launch the Quick Start .......................................................................................... 8
  Step 5. Test the Deployment ............................................................................................ 12
FAQ....................................................................................................................................... 14
GitHub Repository ............................................................................................................... 15
Additional Resources ........................................................................................................... 15
Document Revisions ............................................................................................................ 16
This Quick Start was created by Ixia, a Keysight business, in collaboration with Amazon Web Services (AWS).

**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 the Ixia CloudLens platform with Eastwind Cloud Network Sensors on the AWS Cloud.

CloudLens is a data visibility platform that provides data access and capture, data grooming, and data delivery to security and monitoring tools. Eastwind Cloud Network Sensors are powered by CloudLens to provide intelligence and insight to help you identify and respond to threats in the cloud. This Quick Start deploys the Eastwind CloudVu sensor.

This Quick Start is for users who would like to use these technologies to identify malicious activity, insider threats, and data leakage in their virtual private clouds (VPCs) and Amazon Elastic Compute Cloud (Amazon EC2) instances.

Container-based CloudLens agents are deployed on your monitored instances, capturing packet traffic as they flow through these instances. The packets are sent over a secure tunnel to be analyzed and visualized in Eastwind’s software as a service (SaaS) platform. This gives you clear visibility into your network traffic so you can identify unexpected network behavior, perform network analysis, and detect any intrusions.

**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.
**Tip** After you deploy the Quick Start, we recommend that you enable the AWS Cost and Usage Report to track costs associated with the Quick Start. This report delivers billing metrics to an S3 bucket in your account. It provides cost estimates based on usage throughout each month, and finalizes the data at the end of the month. For more information about the report, see the AWS documentation.

This Quick Start requires a 45-day trial license for CloudLens, as described in Deployment Steps, later in this guide. You can convert the trial license to a standard license at any time.

The Quick Start uses an Amazon Machine Image (AMI) from AWS Marketplace for Eastwind CloudVu. Before you deploy the Quick Start, you must subscribe to Eastwind CloudVu in AWS Marketplace, as described in the Deployment Steps section, and additional pricing, terms, and conditions may apply.

**Architecture**

Deploying this Quick Start for a new 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 two Availability Zones.*
- A VPC configured with public subnets according to AWS best practices, to provide you with your own virtual network on AWS.*
- In the public subnets:
  - Managed NAT gateways to allow outbound internet access for resources in the subnets.*
  - A source instance in an Auto Scaling group (of size 1). This is the application instance that you want to monitor. You can add more instances to monitor in the CloudLens project dashboard after deployment (see step 5 for details).

The source instance has a container-based CloudLens agent deployed. This agent listens on all available interfaces and sends a copy of the packet stream to the tool instance for analysis.
– The Eastwind Cloud Network Sensor, CloudVu, in an Auto Scaling group (of size 1). This is the tool instance that analyzes the packet stream sent over by the CloudLens agent.

* The template that deploys the Quick Start into an existing VPC skips the tasks marked by asterisks and prompts you for your existing VPC configuration.

Prerequisites

Technical Requirements
This Quick Start requires free accounts for both CloudLens and Eastwind.

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

Deployment Options
This Quick Start provides two deployment options:

- **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, and other infrastructure components, and then deploys the Eastwind and CloudLens software into this new VPC.

- **Deploy Eastwind and CloudLens into an existing VPC**. This option provisions the Eastwind and CloudLens software in your existing AWS infrastructure.

The Quick Start provides separate templates for these options. It also lets you configure CIDR blocks and settings for the source and tool instances, as discussed later in this guide.
Deployment Steps

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 instance types you select for the source and tool instances. You might need to do this if you already have existing deployments that use these instance types, and you think you might exceed the default limits with this deployment.

Step 2. Prepare Your CloudLens Account

1. Sign up for a CloudLens free trial account by following the on-screen instructions. You will receive a confirmation email.

2. Activate your free trial account by visiting the link provided in the email.

3. Log in to CloudLens. A project will be created automatically with the required infrastructure: groups for source and tool instances and a filter for the CloudLens agents deployed as part of the Quick Start.

4. Choose the project tile that has the name QUICKSTART_PROJECT.

5. On the project page, choose SHOW PROJECT KEY to display the project key, and copy it for later use. You will be prompted for this key when you deploy the Quick Start.

Figure 2: Selecting the project key
Step 3. Prepare Your Eastwind Account

This Quick Start requires a subscription to the AMI for Eastwind CloudVu in AWS Marketplace.

To subscribe:

1. Log in to your AWS account.
2. Open the page for the Eastwind CloudVu AMI in AWS Marketplace.
3. Choose Continue to Subscribe.
4. Review the terms and conditions for software usage, and then choose Subscribe.
5. Choose Set up your account. This redirects you to the Eastwind portal account creation page.
6. Provide your company name and email. A verification email will be sent to you with a link to set a password.
7. Log in to the Eastwind portal using this new account.
8. You will be redirected to the Data Sources page. Choose AWS as the data source.
9. Choose the plus sign (+ symbol) to add a new account, enable the Sensor option, and then enter your AWS account number (you can find this in the AWS Support Center) to associate your AWS account with Eastwind SaaS.
This completes your Eastwind account creation and will make the Eastwind AMI available for your Quick Start launch.

**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. Choose one of the following options to launch the AWS CloudFormation template into your AWS account. For help choosing an option, see deployment options earlier in this guide.

![Launch](image)

**Option 1**
Deploy the Quick Start into a new VPC on AWS

**Option 2**
Deploy the Quick Start into an existing VPC on AWS

**Important** If you’re deploying Eastwind and CloudLens into an existing VPC, make sure that your VPC has two public subnets in different Availability Zones for the source and tool instances. These subnets require internet connectivity through an internet gateway or NAT gateway to allow the instances to download packages and software. You will be prompted for your VPC settings when you launch the Quick Start.

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 tables, parameters are listed by category and described separately for the two deployment options:

- **Parameters for deploying Eastwind and CloudLens into a new VPC**
- **Parameters for deploying Eastwind and CloudLens into an existing VPC**
• **Option 1: Parameters for deployment into a new VPC**

**View template**

**VPC network configuration:**

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Availability Zones</strong> (AvailabilityZones)</td>
<td><strong>Requires input</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>VPC CIDR</strong> (VPCCIDR)</td>
<td>10.0.0.0/16</td>
<td>The CIDR block for the VPC.</td>
</tr>
<tr>
<td><strong>Public subnet 1 CIDR</strong> (PublicSubnet1CIDR)</td>
<td>10.0.128.0/20</td>
<td>The CIDR block for the public (DMZ) subnet located in Availability Zone 1.</td>
</tr>
<tr>
<td><strong>Public subnet 2 CIDR</strong> (PublicSubnet2CIDR)</td>
<td>10.0.144.0/20</td>
<td>The CIDR block for the public (DMZ) subnet located in Availability Zone 2.</td>
</tr>
</tbody>
</table>

**CloudLens configuration:**

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Project key</strong> (CloudLensProjectKey)</td>
<td><strong>Requires input</strong></td>
<td>The CloudLens project key from step 2 of the deployment.</td>
</tr>
</tbody>
</table>

**Source instance configuration:**

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Optional source AMI</strong> (CustomAMIId)</td>
<td>Optional</td>
<td>The operating system AMI ID for the source instance. If you leave this setting blank, Ubuntu 16.04 is used.</td>
</tr>
<tr>
<td><strong>Source instance type</strong> (SourceInstanceType)</td>
<td>m4.large</td>
<td>The EC2 instance type for the source instance.</td>
</tr>
</tbody>
</table>

**Tool instance configuration:**

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Tool instance type** (ToolInstanceType) | m4.large | The EC2 instance type for the tool (CloudVu) instance.
**SSH configuration:**

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH configuration (SSHKeyName)</td>
<td>Requires input</td>
<td>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.</td>
</tr>
</tbody>
</table>

**AWS Quick Start configuration:**

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quick Start S3 bucket name (QSS3BucketName)</td>
<td>aws-quickstart</td>
<td>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.</td>
</tr>
<tr>
<td>Quick Start S3 key prefix (QSS3KeyPrefix)</td>
<td>quickstart-ixia-eastwind/</td>
<td>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.</td>
</tr>
</tbody>
</table>

- **Option 2: Parameters for deployment into an existing VPC**
  
  View template

**Network configuration:**

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPC ID (VPCID)</td>
<td>Requires input</td>
<td>The ID of your existing VPC (e.g., vpc-0343606e).</td>
</tr>
<tr>
<td>Public subnet 1 ID (PublicSubnet1ID)</td>
<td>Requires input</td>
<td>The ID of the public subnet in Availability Zone 1 in your existing VPC (e.g., subnet-a0246dcd).</td>
</tr>
<tr>
<td>Public subnet 2 ID (PublicSubnet2ID)</td>
<td>Requires input</td>
<td>The ID of the public subnet in Availability Zone 2 in your existing VPC (e.g., subnet-b58c3d67).</td>
</tr>
</tbody>
</table>

**CloudLens configuration:**

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project key (CloudLensProjectKey)</td>
<td>Requires input</td>
<td>The CloudLens project key from step 2 of the deployment.</td>
</tr>
</tbody>
</table>
Source instance configuration:

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Optional source AMI</td>
<td>Optional</td>
<td>The operating system AMI ID for the source instance. If you leave this setting blank, Ubuntu 16.04 is used.</td>
</tr>
<tr>
<td>(CustomAMIId)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Source instance type</td>
<td>m4.large</td>
<td>The EC2 instance type for the source instance.</td>
</tr>
<tr>
<td>(SourceInstanceType)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Tool instance configuration:

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tool instance type</td>
<td>m4.large</td>
<td>The EC2 instance type for the tool (CloudVu) instance.</td>
</tr>
<tr>
<td>(ToolInstanceType)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

SSH configuration:

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH configuration</td>
<td>Requires input</td>
<td>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.</td>
</tr>
<tr>
<td>(SSHKeyName)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

5. On the Options page, you can specify tags (key-value pairs) for resources in your stack and set advanced options. When you’re done, choose Next.

6. On the Review page, review and confirm the template settings. Under Capabilities, select the two check boxes to acknowledge that the template will create IAM resources and that it might require the capability to auto-expand macros.

7. Choose Create to deploy the stack.

8. Monitor the status of the stack. When the status is CREATE_COMPLETE, the deployment is complete.

Step 5. Test the Deployment

This Quick Start includes a simulated attack on the source instance, to show you how to visualize and identify actual attacks in a production environment. To validate the deployment and view the simulated threats, please follow these steps:
1. Log into the CloudLens portal, using the credentials you created in step 2.

2. Choose the project tile that has the name QUICKSTART_PROJECT.

3. Make sure you see two instances connected to the project, and that traffic is being tapped.

![Figure 4: Checking instances in the CloudLens portal](image)

4. (Optional) Monitor additional application instances by launching more CloudLens agents. Choose the Launch Agent button for instructions on how to deploy a new agent. Make sure to define a group for the newly launched agents. (For more information, see the sections Adding Instances to a Group and Connecting Instance and Tool Groups in the CloudLens User Guide.)

5. Log into the Eastwind portal, using the credentials you created in step 3.

   The threat intelligence dashboard is displayed. Here you should see information about the simulated threat.
6. If you want to dig deeper, the portal provides access to several tools to assist in viewing and searching the network metadata that is generated by the Eastwind sensor. To access these tools, use the links in the left navigation pane. The main tools are **Dashboard**, **Visualize**, and **Discover**.

**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 `/var/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](https://aws.amazon.com/documentation/cloudformation/tutorials/troubleshoot/) 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 links in this guide 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.

Q. No instances were connected back to the CloudLens portal.

A. Did you input the right project key when you deployed the Quick Start in step 4? If yes, connect to your instances by using Secure Shell (SSH) and check that the CloudLens agent containers are running. If they aren’t, check the cloud-init logs (usually found at /var/log/cloud-init-output.log) for more information about what went wrong. If the Docker containers are running, check the agent logs for more information:

```
sudo docker logs -f CloudLensQuickStart
```

Q. I don’t see any information displayed in the Eastwind portal.

A. Is tapped traffic reaching the cloudlens0 virtual interface on the tool instances? Use the tcpdump utility to check. If not, please contact CloudLens support.

GitHub 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

<table>
<thead>
<tr>
<th>Date</th>
<th>Change</th>
<th>In sections</th>
</tr>
</thead>
<tbody>
<tr>
<td>January 2019</td>
<td>Initial publication</td>
<td>—</td>
</tr>
</tbody>
</table>

© 2019, Amazon Web Services, Inc. or its affiliates, and Ixia, a Keysight business. All rights reserved.

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.

The software included with this paper is licensed under the Apache License, Version 2.0 (the "License"). You may not use this file except in compliance with the License. A copy of the License is located at http://aws.amazon.com/apache2.0/ or in the "license" file accompanying this file. This code is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.