CloudLens: Visibility in Public Cloud

Introduction

Organizations in every market sector, even those not typically associated with technology, are migrating to the public cloud. This trend is growing because of the increased flexibility and agility the cloud offers. Whether these applications are web servers or critical business apps, they must ensure the same level of performance, security, and compliance available in their traditional data centers.

In a traditional datacenter, these needs are met with robust tools in combination with a zero-packet-loss, application-aware visibility network. In the public cloud, access to packet data is limited, but needs for visibility remain—including the need to see active threats, monitor applications, and diagnose problems.

Problem Statement

To understand these challenges within the context of a cloud environment, let us take a step back to see why organizations opt to move to the cloud.

There are several perceived advantages:

1. Flexibility & agility – Data is accessible from anywhere across a variety of devices with strong SLAs.

2. Elasticity & scale – Organizations have the ability to scale up and scale down depending on demand, minimizing costs. Resources are pooled by a cloud provider, and can dynamically increase or decrease by self-provisioning; either by deploying new instances (horizontal scale) or by increasing the resources within an instance (vertical scale).

Tese advantages are recognized as a new approach to designing cloud-based applications. Cloud-based applications are generally built as a collection of services that decouple the data from the application and are modeled to scale by spinning up additional resource instances when needed. A significant issue of moving workloads to the public cloud is the absence of independent application-level monitoring and analytics of workload behavior.

Also, the tools offered by public cloud providers to monitor the performance of your environment do not include packet data, which is critical for network visibility. To support a distributed application architecture built to leverage the full power of the public cloud, there are two main network visibility challenges:

1. Capturing and filtering traffic
In a traditional data center, there is physical access to the network; taps and network packet brokers can be inserted with full control over the network domain. However, in the transient environment of the public cloud, there is no way to insert physical devices, and control to the network domain is limited.

2. Allowing for horizontal scaling while providing consistent data to tools
The cloud is designed to scale to meet peak demand. As applications scale to meet demand, new instances are created and destroyed dynamically. Any cloud-based network visibility solution must be able to accommodate the dynamic nature of events to be effective.

It is important to note that any network visibility solution in the cloud must support a distributed design where individual instances spin up and spin down based on demand. Visibility solutions that use a single dedicated instance to handle the inspection of packets introduce a single point of failure and will not scale, because they inevitably will require some level of human intervention.

The Solution: Purpose Built Network Visibility for Public Clouds

Ixia's CloudLens SaaS is a software as a service (SaaS) platform for cloud visibility. It is a collection of Amazon Web Services (AWSs) coordinated to support cloud agility and allowing for horizontal scale. At its core, it is an implicit microservices architecture that is orchestrated via application program interfaces (APIs). As a serverless design, it meets the cloud needs of highly available and scalable service. The solution has two primary components:

1. Source and tool sensors - Installed within both the source instances (that require monitoring) and the tool instances (that will analyze the data), the source sensor filters traffic before sending it to the tools.

2. Centralized management platform – Users can control and operate the sensors installed in the source and tool instances. The management platform creates a secure visibility path that transfers packet data from the source to the tool sensors.

These components work together to provide the benefits of a cloud visibility solution and address core needs in a cloud environment.

Step 1: The Sensors

The CloudLens visibility sensors are installed as Docker containers on both the source and tool instances; this allows sensors to leverage information that is inherent to the instance and forward it as metadata to the central management platform:

- **Gathering and filtering traffic**
  - Network data gathering is possible, as packets from the source machine can be obtained at the OS layer directly.
  - Gathering data from within the instance is secure, as this allows the sensors to inherit the existing security context, preventing cross-tenant security violations.
  - Network blind spots normally caused by SSL are eliminated, because the sensors are running directly on the source instances themselves, which are behind SSL off-load services.

- **Scaling tools to parallel cloud elasticity**
  - Filtering data allows for more robust options, as the sensor has access to additional instance-level metadata. This provides administrators access to a larger set of criteria when setting filtering rules. For example, packet collection or filtering decisions could include metadata including OS, instance metadata, or even metrics, like CPU and memory load.
  - Elasticity and scaling events are handled implicitly; the visibility sensors scale dynamically along with the source instances based on applications' needs.

Step 2: The Centralized Management Platform

Ixia’s CloudLens serverless architecture uses cloud-native services, providing elastic and on-demand solutions at scale. The centralized management service takes a holistic approach to providing visibility.

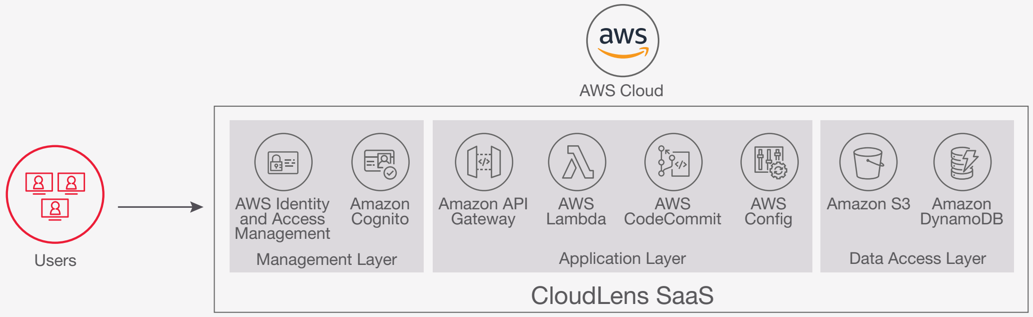

Figure 1. CloudLens SaaS Architecture

Configuring visibility begins by logging into CloudLens’ management portal and creating a “Project,” so a unique “Project Key” is created. This key is loaded into the visibility sensors running in the source and tool instances, which will be isolated as part of a “Project.”

Once the key is installed in the visibility sensors, they phone home to the central management platform with metadata about the instances.

Examples of metadata include the following:

- Underlying instance architecture
- Operating system information
- Hypervisor type
- Kernel versions and other software versions
- Prepopulated user data
- CPU and memory utilization and performance metrics

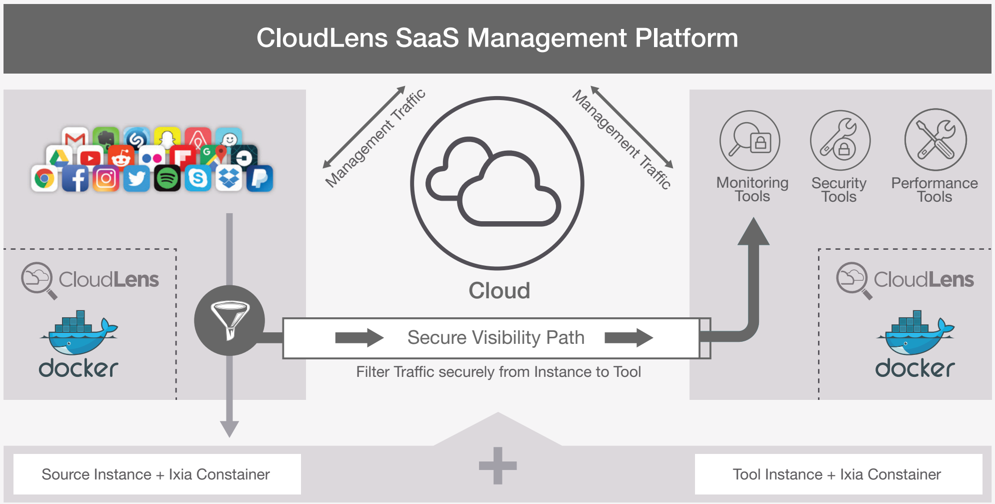
CloudLens SaaS Management Platform
Management Traffic
Management Traffic
Cloud
Monitoring Tools
Security Tools
Performance Tools
CloudLens
docker
CloudLens
docker
Secure Visibility Path
Filter Traffic securely from Instance to Tool
Source Instance + Ixia Constainer
Tool Instance + Ixia Constainer

Figure 2. CloudLens SaaS Solution Overview

The management interface has a smart search capability, which allows users to create source groups and tool groups based on metadata. This metadata information is auto populated as search criteria in the management platform. The metadata can also be user defined, allowing maximum flexibility. **As new instances are created, they are automatically added to groups based on their metadata.** This retains scalability and elasticity in a cloud visibility solution.

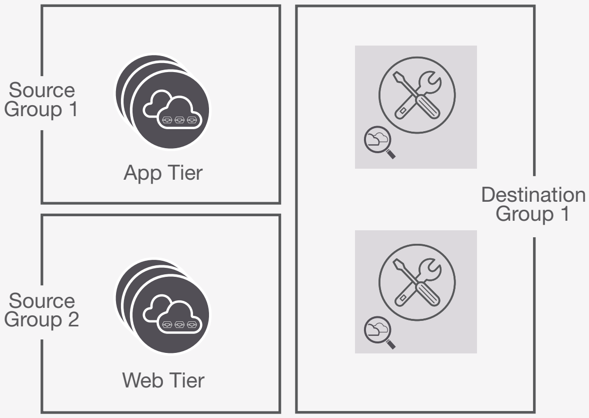

Figure 3. Source and Tool Groups

For example, a user might create a group composed of all instances with the metadata tag “Role” having the value “Web Server;” every instance with that value gets automatically added to this group regardless of when it is created.

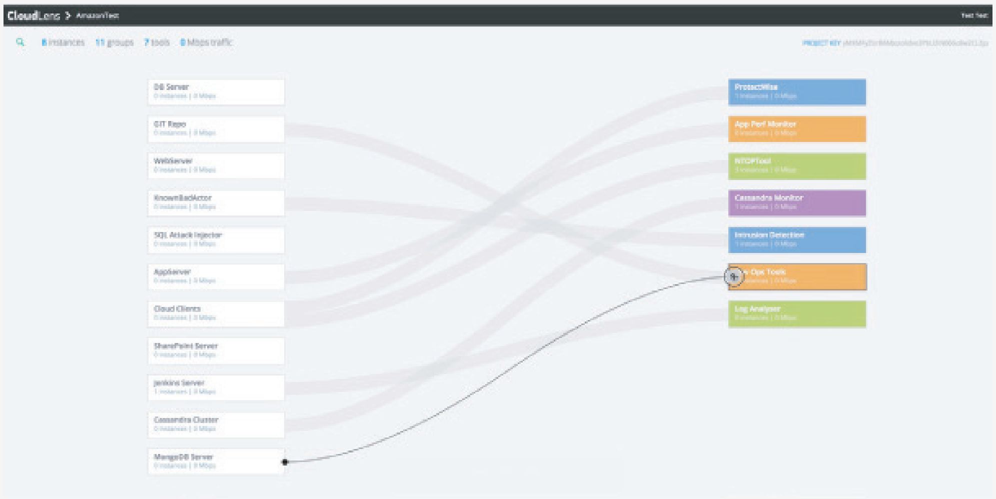

Figure 4. CloudLens SaaS Solution Overview

The next step in configuration is for the users to associate source groups with tool groups to create an encrypted secure visibility path. In CloudLens SaaS, this is done in a point-and-click visual interface (see image). Once defined, the secure visibility path transfers filtered packet data from source to tool instances.

Together, the sensor, management platform, and secure visibility path address the challenge of providing visibility within the public cloud.

Conclusion

Since enterprises are moving to the public cloud, visibility solutions that provide security and compliance that meet public cloud standards are required. To scale, filtering rules cannot be static; rather they must be based on workload attributes and type of traffic. Ixia's CloudLens SaaS has a serverless architecture that scales with distributed software systems built for cloud scale, which delivers intelligent, resilient, and proactive public-cloud visibility.

Learn how you can easily start eliminating the visibility blind spots of your public cloud environment and access the data you need, where and when you need it at http://www.ixiacom.com/solutions/ixia-cloud-solution.

Learn more at: www.keysight.com

For more information on Keysight Technologies' products, applications or services, please contact your local Keysight office. The complete list is available at: www.keysight.com/find/contactus

KEYSIGHT TECHNOLOGIES