

CLOUDLENS PUBLIC WITH RIVERBED STEELCENTRAL APPRESPONSE 11 DEPLOYMENT GUIDE IN AWS

PROBLEM:

Organizations, even those not typically associated with technology, are migrating to the cloud. This trend is growing because the cloud offers increased flexibility and agility. With this mass migration, organizations have more segments to manage and more potential blind spots in their networks. Regardless of where infrastructure and applications reside, security and compliance needs remain the same. Organizations are finding that their traditional network visibility solutions are unable to meet their needs for visibility of cloud-based data.

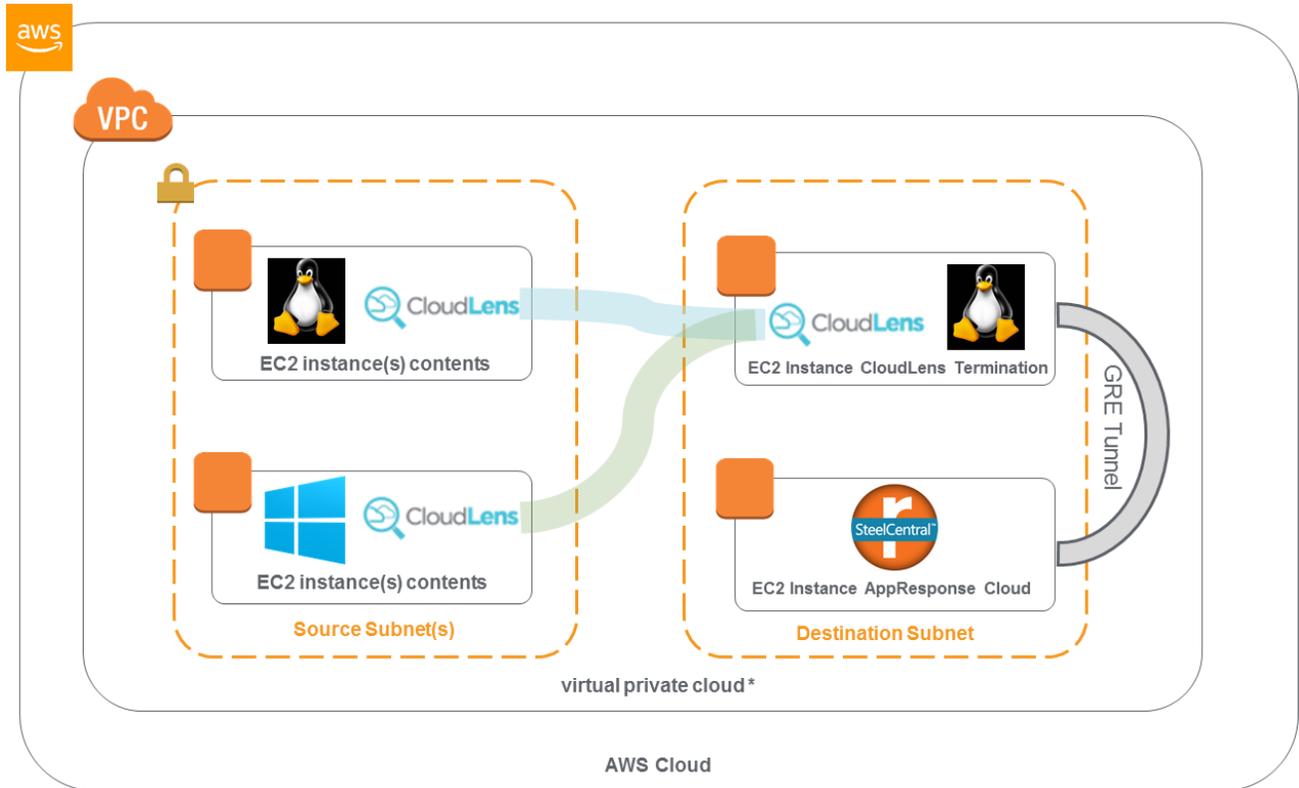
SOLUTION:

CloudLens™, Ixia's platform for public, private and hybrid cloud visibility addresses the challenges of granular data access in the cloud. CloudLens is the first network-level solution that provides Visibility-as-a-Service (VaaS) through a Software-as-a-Service (SaaS). It is also the industry's first cloud service-provider agnostic visibility platform.

KEY FEATURES:

- Elastically scales on-demand – so visibility auto-scales horizontally along with the instances monitored and the cluster of instances that are needed to do the monitoring
- Automates cloud visibility management by providing it as a service – so no architectural changes required
- Reduces errors by eliminating manual configuration
- Easy to use and setup with a drag and drop interface
- Reduces bandwidth to tools by filtering packets at the source instances, eliminating unwanted traffic so tools operate optimally

SAMPLE DEPLOYMENT ARCHITECTURE



* Shown above is a sample deployment, while destination components need to be in the same subnet, monitored source instances can be located in any subnet, VPC, or AWS Region. CloudLens Sensors run on customer AWS instances, register up to the CloudLens SaaS which manages them and forwards desired traffic to the destination

CLOUDLENS APPRESPONSE DEPLOYMENT GUIDE FOR AWS

PREPARE AWS ENVIRONMENT

NOTE: IN THIS EXAMPLE WE ARE ASSUMING THE TWO SOURCE INSTANCES DO NOT ALREADY EXIST, IF THEY ALREADY EXIST YOU DO NOT NEED TO CREATE THEM, YOU CAN ATTACH THOSE AND ANY OTHER SOURCE INSTANCES TO CLOUDLENS AS DESCRIBED ON P 6-11 OF THIS DOCUMENT. YOU DO ALWAYS NEED TO CREATE ONE LINUX INSTANCE, THIS ONE WILL BE USED FOR FORWARDING TRAFFIC FROM CLOUDLENS TO RIVERBED VIA GRE AS DESCRIBED ON P 12. ALSO, WE ARE ASSUMING IN THIS EXAMPLE THAT AN INSTANCE OF RIVERBED APPRESPONSE IS ALREADY INSTALLED IN AWS, PLEASE CONTACT RIVERBED FOR ASSISTANCE IF NEEDED.

In this sample set up we will be creating one sample Windows 2012 R2 instance and two sample Ubuntu 16.04 Linux instances (other Linux types are also supported). We will use one Ubuntu 16.04 Linux instance as the source instance and one Ubuntu 16.04 Linux instance to forward traffic from CloudLens P2P VPN Tunnels to GRE Tunnel origination point. The GRE Tunnel will terminate on Riverbed Steelcentral Appresponse 11.

Step 1 – Log into the AWS Portal. Click “Launch Instance” within the EC2 service.

Create Instance

To start using Amazon EC2 you will want to launch a virtual server, known as an Amazon EC2 instance.

Launch Instance

Note: Your instances will launch in the US East (N. Virginia) region

Step 2 – Choose Windows 2012 R2 Server. Click “Select”

**Microsoft Windows Server 2012 R2 Base** - ami-f6529b8c **Select**
Windows Microsoft Windows 2012 R2 Standard edition with 64-bit architecture. [English] 64-bit
Free tier eligible Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

and

**Ubuntu Server 16.04 LTS (HVM), SSD Volume Type** - ami-da05a4a0 **Select**
Free tier eligible Ubuntu Server 16.04 LTS (HVM),EBS General Purpose (SSD) Volume Type. Support available from Canonical (<http://www.ubuntu.com/cloud/services>). 64-bit
Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

Step 3 – Enter Virtual Machine instance type (e.g. t2.xlarge)

<input checked="" type="checkbox"/>	General purpose	t2.xlarge	4	16	EBS only	-	Moderate	Yes
-------------------------------------	-----------------	-----------	---	----	----------	---	----------	-----

Step 4 – Select configuration details

Note: Recommended - choosing an IAM role (e.g. ec2_metadata_access) which allows metadata access will permit AWS Tags to be shared with CloudLens

CLOUDLENS APPRESPONSE DEPLOYMENT GUIDE FOR AWS

Number of instances [Launch into Auto Scaling Group](#)

Purchasing option Request Spot instances

Network [Create new VPC](#)

Subnet [Create new subnet](#)
251 IP Addresses available

Auto-assign Public IP

Domain join directory [Create new directory](#)

IAM role [Create new IAM role](#)

Shutdown behavior

Enable termination protection Protect against accidental termination

Monitoring Enable CloudWatch detailed monitoring
[Additional charges apply.](#)

Tenancy [Additional charges will apply for dedicated tenancy.](#)

Elastic GPU Add GPU
[Additional charges apply.](#)

Network interfaces

Device	Network Interface	Subnet	Primary IP	Secondary IP addresses	IPv6 IPs
eth0	<input type="text" value="New network interface"/>	<input type="text" value="subnet-71b2fa4c"/>	<input type="text" value="Auto-assign"/>	Add IP	

[Add Device](#)

Step 5 – Add storage

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encrypted
Root	/dev/sda1	snap-06e63d2ab92ae9507	<input type="text" value="30"/>	General Purpose SSD (GP2)	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted

[Add New Volume](#)

Step 6 – Add Tags as desired, allows for easier identification and grouping of instances in CloudLens

Key (127 characters maximum)	Value (255 characters maximum)	Instances	Volumes
Name	Demo Windows 2012 R2 Server	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
CreatedBy		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[Add another tag](#) (Up to 50 tags maximum)

Step 7 – Assign a security group

Please see list of CloudLens required port numbers on P 15-16 of this document for guidance when creating or editing your security group.

CLOUDLENS APPRESPONSE DEPLOYMENT GUIDE FOR AWS

Assign a security group: Create a new security group
 Select an existing security group

Security Group ID	Name	Description	Actions
<input checked="" type="checkbox"/> sg-43fd2f3d	CloudLens-Demo-Security-Group	CloudLens-Demo-Security-Group	Copy to new
<input type="checkbox"/> sg-e1e0329f	default	default VPC security group	Copy to new

Step 8 – Launch the instance with the correct key pair

AMI Details [Edit AMI](#)

Microsoft Windows Server 2012 R2 Base - ami-f6529b8c
Free tier eligible
Microsoft Windows 2012 R2 Standard edition with 64-bit architecture. [English]
Root Device Type: ebs Virtualization type: hvm
If you plan to use this AMI for an application that benefits from Microsoft License Mobility, fill out the [License Mobility Form](#). Don't show me this again

Instance Type [Edit instance type](#)

Security Group [Edit security groups](#)

Instance Details [Edit instance details](#)

Storage [Edit storage](#)

Tags [Edit tags](#)

Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Choose an existing key pair

Select a key pair

sks_key

I acknowledge that I have access to the selected private key file (sks_key.pem), and that without this file, I won't be able to log into my instance.

[Cancel](#) [Launch Instances](#)

[Cancel](#) [Previous](#) [Launch](#)

INSTALL CLOUDLENS CONTAINER IN UBUNTU 16.04 VM

Note: Customers are assumed to have already created an account at <http://ixia.cloud> before completing the next step. If you don't have an account, you can sign up for a 45-day free trial. After login please create or view your CloudLens Project, and make note of the Project Key (aka API key) which you will need in step 7

Step 0 – If Docker Engine is not already present, install Docker from <https://docs.docker.com/install/>

e.g. (commands will vary by OS type and version, see link above for more details)

```
sudo apt update
```

```
sudo apt-get install -y docker.io
```

Step 1 – Download CloudLens container from Docker Hub

The following command downloads the latest version of CloudLens Public container; `sudo docker pull ixiacom/cloudlens-agent:latest`

```
ubuntu@ip-10-150-1-88:~$ sudo docker pull ixiacom/cloudlens-agent:latest
latest: Pulling from ixiacom/cloudlens-agent
22ecafbbcc4a: Pull complete
580435e0a086: Pull complete
8321ffd10031: Pull complete
08b8f28a13c2: Pull complete
2b401702069a: Pull complete
a3ed95caeb02: Pull complete
eae027dcdc0e: Pull complete
93bc98227159: Pull complete
43f64d736e1f: Pull complete
18f4140f91f9: Extracting [=====] 154.9 MB/210.4 MB
695127c83df0: Download complete
cf6796e91e8a: Download complete
ee87eb3bacec: Download complete
cabad2a7cad3: Download complete
267ac30ea81e: Download complete
d7b7f7a88663: Download complete
ba635e456d83: Download complete
1c70211bb7e9: Download complete
73de50ac0bb9: Download complete
c9a62f82ef78: Download complete
439ccc17055d: Download complete
ced32024733c: Download complete
210024445f82: Download complete
105928bb3d84: Download complete
8b05a0d09881: Download complete
616b3c7ae818: Download complete
d341e4a550bc: Download complete
ad4766c02248: Waiting
2e2058f93cef: Waiting
```

LAUNCH CLOUDLENS CONTAINER IN UBUNTU 16.04 VM

Step 1 – Launch CloudLens container with the following parameters. You will need to substitute your CloudLens Project Key (aka API key) here

```
sudo docker run \  
--name CloudLens \  
-v /:/host \  
-v /var/run/docker.sock:/var/run/docker.sock \  
-d --restart=always \  
--net=host \  
--privileged \  
ixiacom/cloudlens-agent:latest \  
--server agent.ixia.cloud \  
--accept_eula y \  
--apikey <Project Key from CloudLens Portal> \  
--custom_tags CloudServiceProvider=AWS \  
Location=Oregon \  
DeviceName=Riverbed-AR11
```

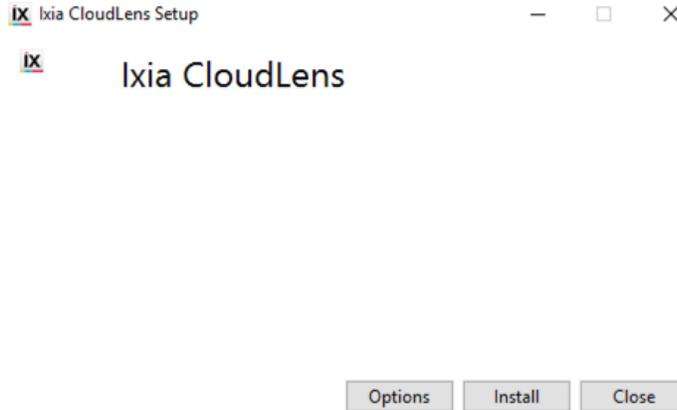
INSTALL CLOUDLENS AGENT IN WINDOWS SERVER VM

Step 1 – Download Ixia’s CloudLens agent from the link provided

<https://agent.ixia.cloud/updates/windows/latest>



Step 2 – Install CloudLens agent



Step 3 – Installation wizard goes through the CloudLens agent installation and all dependent package installations.

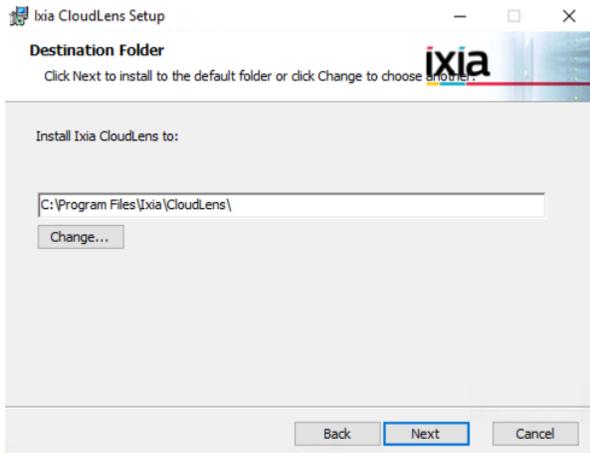


CLOUDLENS APPRESPONSE DEPLOYMENT GUIDE FOR AWS

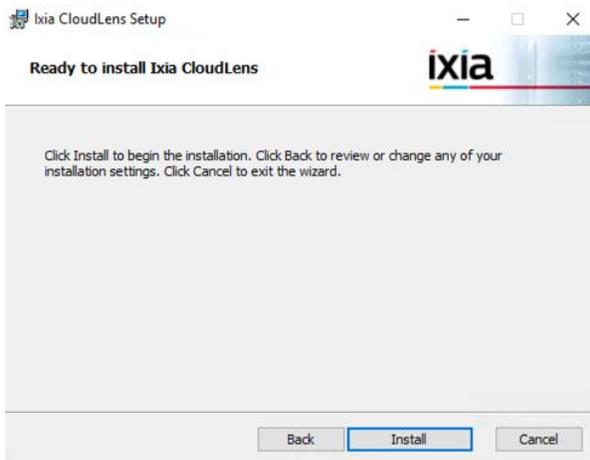
Step 4 – Accept End User License Agreement



Step 5 – Accept End User License Agreement

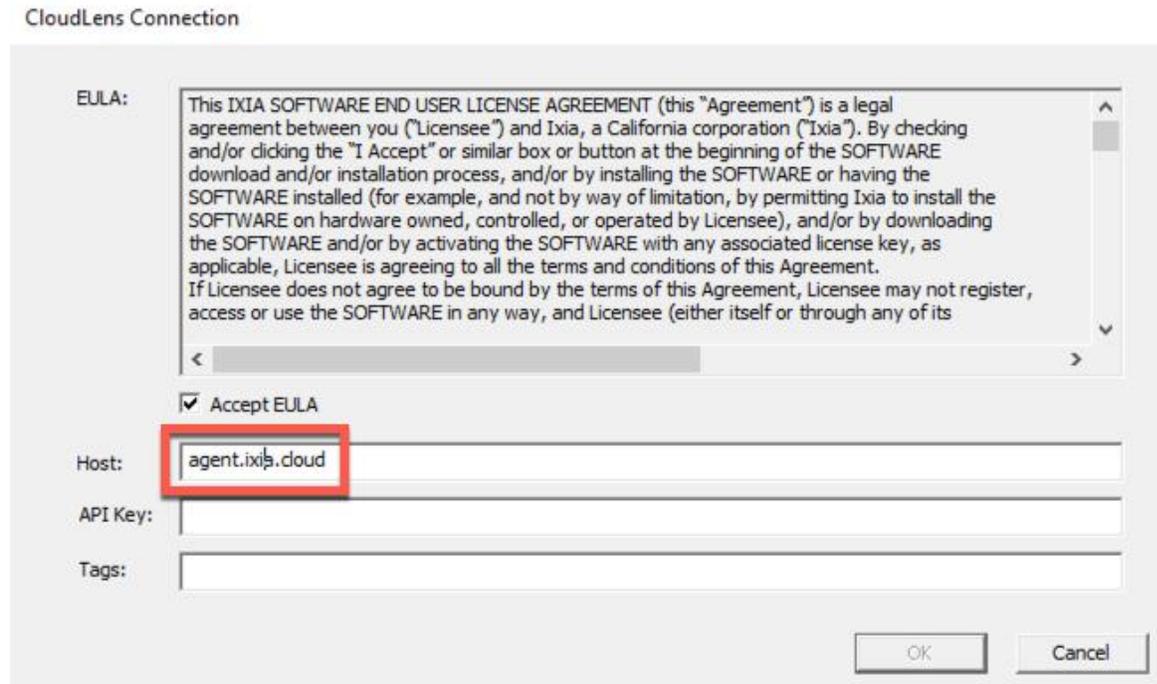


Step 6 – Click "Install"



CLOUDENS APPRESPONSE DEPLOYMENT GUIDE FOR AWS

Step 7 – The Windows instance should be associated with a Project created in <https://ixia.cloud>. The value of Host: agent.ixia.cloud . You must also specify your own Project Key (aka API key)



Step 8 – Finish CloudLens sensor installation



Step 9 – Restart the instance and verify the instance is associated with the CloudLens project created.



CREATE GRE INTERFACE ON ONE OF THE UBUNTU 16.04 INSTANCE.

Step 1 – Log into AWS EC2 instance

Step 2 – Switch to super user mode.

Step 3 – ip link provides the ability to display link layer information, activate an interface, deactivate an interface, change link layer state flags, change MTU, the name of the interface etc. Create a GRETAP interface.

```
ip link add gre2 type gretap local <local Private ipv4 address> remote
<Riverbed Steelcentral Private ipv4 address> dev eth0 ttl 255 key 1

ip link set gre2 up
```

Step 4 – Verify “gre2” interface is available and operational.

```
gre2      Link encap:Ethernet  HWaddr ee:3e:5d:63:06:10
          inet6 addr: fe80::ec3e:5dff:fe63:610/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:8959 Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:16885852 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:3864521055 (3.8 GB)
```

Note: above commands will not persist after reboot. There are several ways to automate persistence, here is one example (details may vary by OS type/version, as well as interfaces names)

Edit the interface config file e.g.

```
vi /etc/network/interfaces.d/50-cloud-init.cfg
```

and add the following lines e.g.

```
down ip link set gre2 down
```

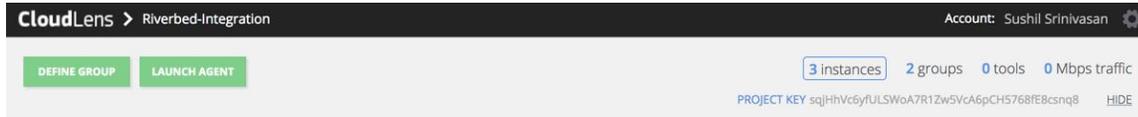
```
down ip link delete gre2
```

```
up ip link add gre2 type gretap local <local Private ipv4 address> remote <Riverbed Steelcentral
Private ipv4 address> dev eth0 ttl 255 key 1
```

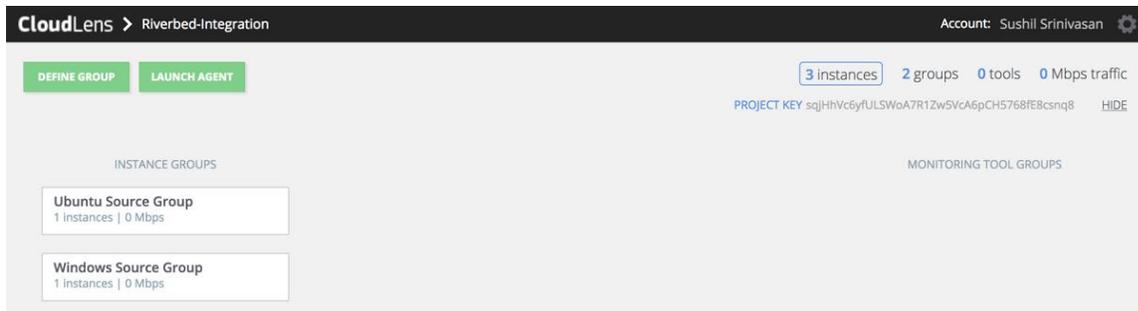
```
up ip link set gre2 up
```

USING CLOUDBLANS SAAS PORTAL

Step 1 – Verify the VMs are reflected in the CloudLens SaaS portal once they are launched with the correct project key.

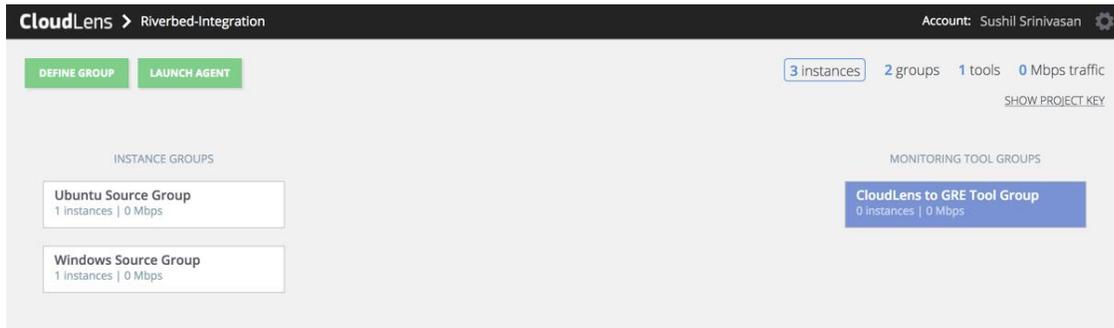


Step 2 - Use CloudLens tags ingested from AWS to create
Windows Source Group
Ubuntu Source Group



CloudLens to GRE Tool Group

The screenshot shows a "SAVE SEARCH" dialog box. It has two radio buttons: "Save as an instance group" (unselected) and "Save as a tool" (selected). Below the radio buttons, there are three input fields: "Name" with the value "CloudLens to GRE Tool Group", "Aggregation Interface" with the value "gre2", and "Comment" which is empty. At the bottom, there are "OK" and "Cancel" buttons.



CLOUDLENS APPRESPONSE DEPLOYMENT GUIDE FOR AWS

Step 3 – Create secure visibility path between source and tool groups



Step 4 – login to Riverbed AppReponse Cloud hosted in AWS

Verify traffic from windows and ubuntu source instances are available in Riverbed Steelcentral Appresponse Cloud.

The screenshot shows the Riverbed AppResponse SteelCentral interface. At the top, it displays 'Beta trial expires in 83 days' and various system information. The main navigation bar includes 'HOME', 'INSIGHTS', 'NAVIGATOR', 'ADMINISTRATION', and 'HELP'. The current view is 'Summary: All Traffic' for the time period 'Aug 8 10:58 PM - 11:58 PM'. The interface is divided into several sections:

- All Traffic:** A table showing traffic metrics:

Throughput [Mbps]	< 0.01
Traffic [MB]	2
Packet Throughput [#s]	3.95
Round Trip Time [ms]	4.26
% Request Retrans [%]	0
% Response Retrans [%]	0
Connections Failed [#]	58
- Total Throughput:** A line graph showing throughput over time, with a peak around 23:30.
- Bandwidth Usage:** A horizontal bar chart showing bandwidth usage for 'Default-10.x.x.x' and 'Default-Internet'.
- Busiest Apps > User Response Time:** A table showing user response times for various applications:

Application	Server Turns [#]	User Response Time [ms]
HTTP	1,080	0.62
SSL	198	129.73
Amazon-Web-Services	63	17.59
TCP/50228	0	
TCP/45870	0	
TCP/445 microsoft-ds	0	
TCP/41070	0	
TCP/40080	0	
- Busiest Server IPs > Server Response Time:** A table showing server response times for various IP addresses:

TCP Server	Server Turns [#]	Server Response Time [ms]
instance-data.us-west-2.compute.internal	1,080	0.20
54.240.251.131	27	19.73
54.240.253.45	24	13.12
ec2-34-231-205-212.compute-1.amazonaws.com	21	18.22
ec2-54-88-254-181.compute-1.amazonaws.com	21	9.70
ec2-107-23-16-158.compute-1.amazonaws.com	18	35.51
ec2-34-199-170-68.compute-1.amazonaws.com	15	16.06
ec2-52-3-123-212.compute-1.amazonaws.com	12	34.29
- Most Active Client IPs > User Response Time:** A table showing user response times for various client IP addresses:

TCP Client	Active Connections [#]	User Response Time [ms]
ip-10-150-1-78.us-west-2.compute.internal	1,147	16.21
50-203-199-146-static.hfc.comcastbusiness.net	3	
146.0.77.142	2	
146.185.222.28	2	
185.208.209.6	2	
181.214.87.113	2	
187.95.16.62	1	
42.118.200.184	1	

FIREWALL PORTS TO OPEN FOR CLOUDLENS

Note: default Security rule settings for AWS Instances is Outbound is open for All Traffic.
But for **Inbound** a few ports numbers need to be explicitly opened:

Source Instances:

- UDP 19993 (CloudLens Tunnel) *
- TCP 22 (if Linux) **
- TCP 3389 (if Windows) **

GRE Intermediary Node:

- UDP 19993 (CloudLens Tunnel) *
- GRE Protocol *
- TCP 22 **

Riverebed SteelCentral Instance:

- GRE Protocol *
- TCP 22 **
- TCP 443 **

* Leave open all IP addresses, however if stricter controls are required contact Ixia support

** Specify IP addresses of customer administrators

WHERE TO GET HELP

If you experience technical difficulties, please email cloudlens@keysight.com for assistance

IXIA WORLDWIDE

26601 W. AGOURA ROAD
CALABASAS, CA 91302

(TOLL FREE NORTH AMERICA)

1.877.367.4942

(OUTSIDE NORTH AMERICA)

+1.818.871.1800

(FAX) 818.871.1805

www.ixiacom.com

© Keysight Technologies, 2017

IXIA EUROPE

CLARION HOUSE, NORREYS DRIVE
MAIDENHEAD SL6 4FL
UNITED KINGDOM

SALES +44.1628.408750

(FAX) +44.1628.639916

IXIA ASIA PACIFIC

101 THOMSON ROAD,
#29-04/05 UNITED SQUARE,
SINGAPORE 307591

SALES +65.6332.0125

(FAX) +65.6332.0127