KEYSIGHT CLOUDLENS WITH RIVERBED APPRESPONSE QUICKSTART 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™, Keysight's platform for public, private and hybrid cloud visibility addresses the challenges of granular data access in the cloud. CloudLens is a solution that provides network tap and packet brokering services in the cloud. It is also the industry's first cloud service-provider agnostic visibility platform. This guide describes how to deploy Riverbed AppResponse together with CloudLens visibility in AWS (but CloudLens is also avaibale in Azure, GCP or other clouds).

KEY CLOUDLENS FEATURES:

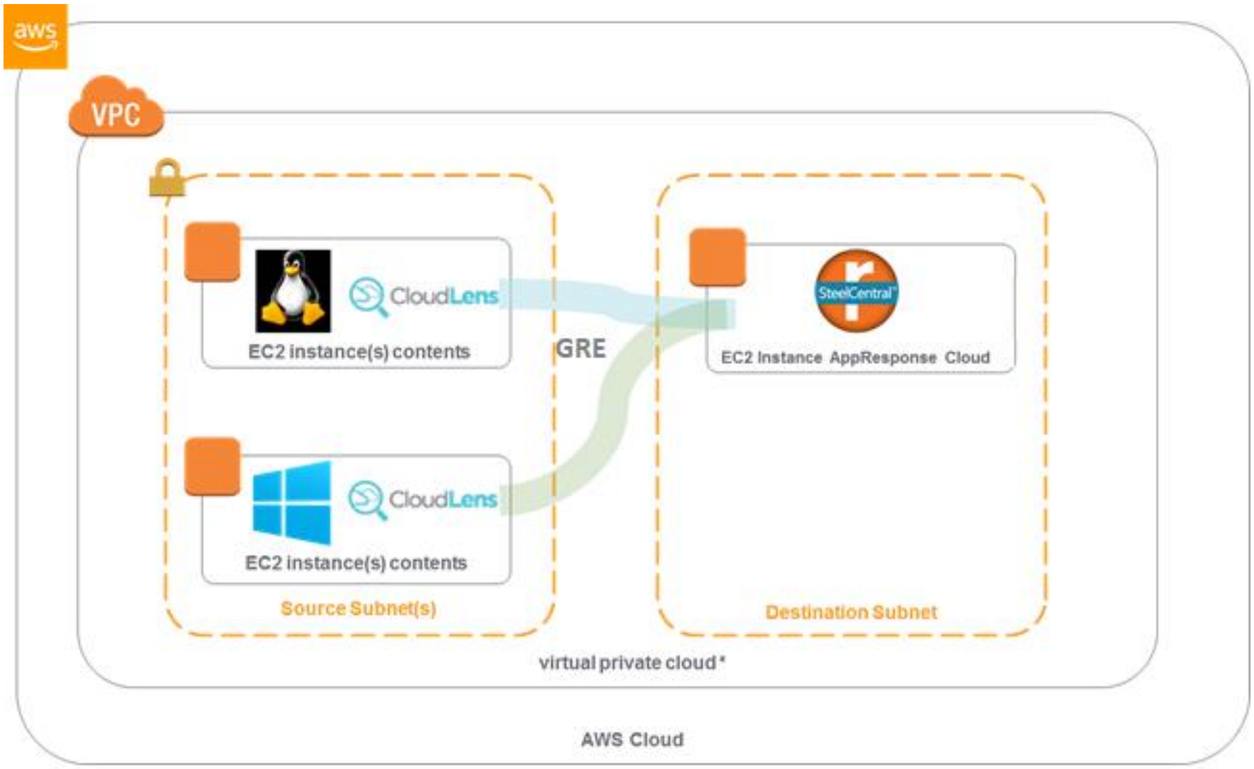
- Cloud visibility management is controlled by the cloud customer, not reliant on the cloud provider
- Elastically scales on-demand – so visibility auto-scales horizontally along with the Virtual Machines monitored and the Virtual Machines that are needed to do the monitoring
- Reduces errors occurring due to complex and manual cloud configuration
- Easy to use and setup with a drag and drop interface
- Reduces bandwidth to tools by filtering packets at the source Virtual Machines, eliminating unwanted traffic so tools operate optimally
- Supports monitoring of Linux, Windows, and Containers
- Allows sharing of monitor traffic to multiple destinations.
- Supports monitoring of multi-cloud environments

ABOUT THIS GUIDE;

This guide is meant to summarize steps required for interoperability of Keysight CloudLens and Riverbed AppResponse Cloud. Not all details of every configuration step of each product is detailed here. Full product installation and user guides are available from cloudlens.support@keysight.com and support@riverbed.com respectively. This guide also assumes working familiarity with configuration of AWS. Examples shown in this guide were tested with Keysight CloudLens v6.1.0, and AppResponse Cloud v 11.11.5

Contents

1. Sample deployment architecture



* Shown above is a sample deployment, monitored sources instances can be located in any subnet, VPC, or AWS Region. CloudLens Sensors run on customer AWS instances, register up to the CloudLens Manager which manages them and forwards desired traffic to the destination using GRE tunneling.

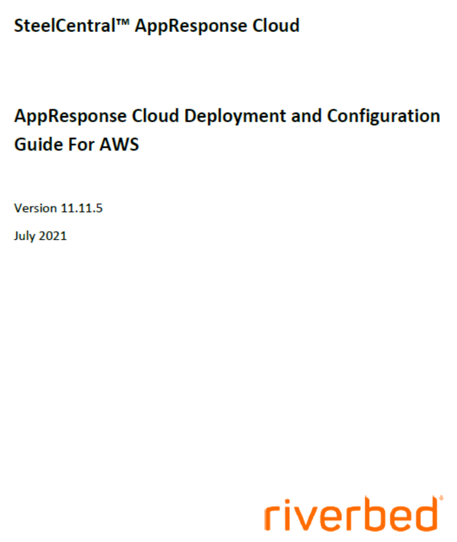
In this sample set up we will be creating one sample Windows 2019 instance and an AWS Linux instances (other Linux types are also supported) as source instances. Mirrored and filterer traffic will be sent over GRE tunnels to Riverbed AppResponse.

Only two source instances are shown in this diagram, however many source instances are permitted (your CloudLens license determines now many CloudLens Sensors which the CloudLens manager is allowed to control. **(see CloudLens documentation for instructions on Licensing)**

NOTE: in this guide it is assumed you have already installed CloudLens Manager into your AWS account. Please see CloudLens User Guide for details of that installation procedure

2. Deploying Riverbed AppResponse.

Please refer to Riverbed’s guide for complete details on how deploy AppResponse in AWS. Here below are the main steps.



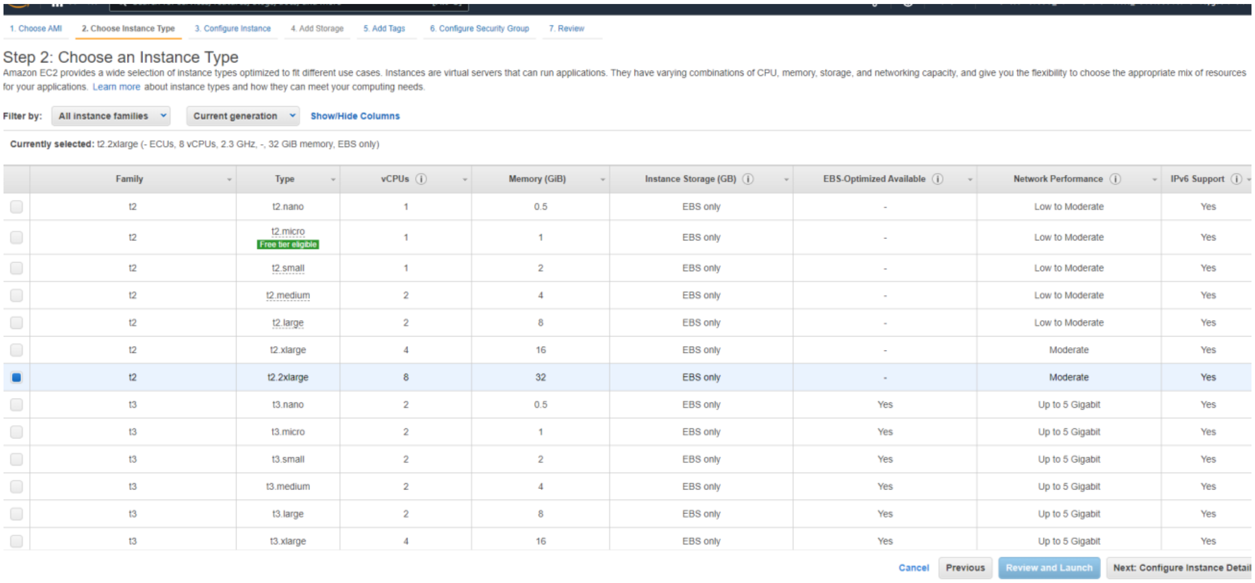
SteelCentral™ AppResponse Cloud

AppResponse Cloud Deployment and Configuration Guide For AWS

Version 11.11.5

July 2021

2.1. Log into the AWS Portal. Click “Launch Instance” within the EC2 service.



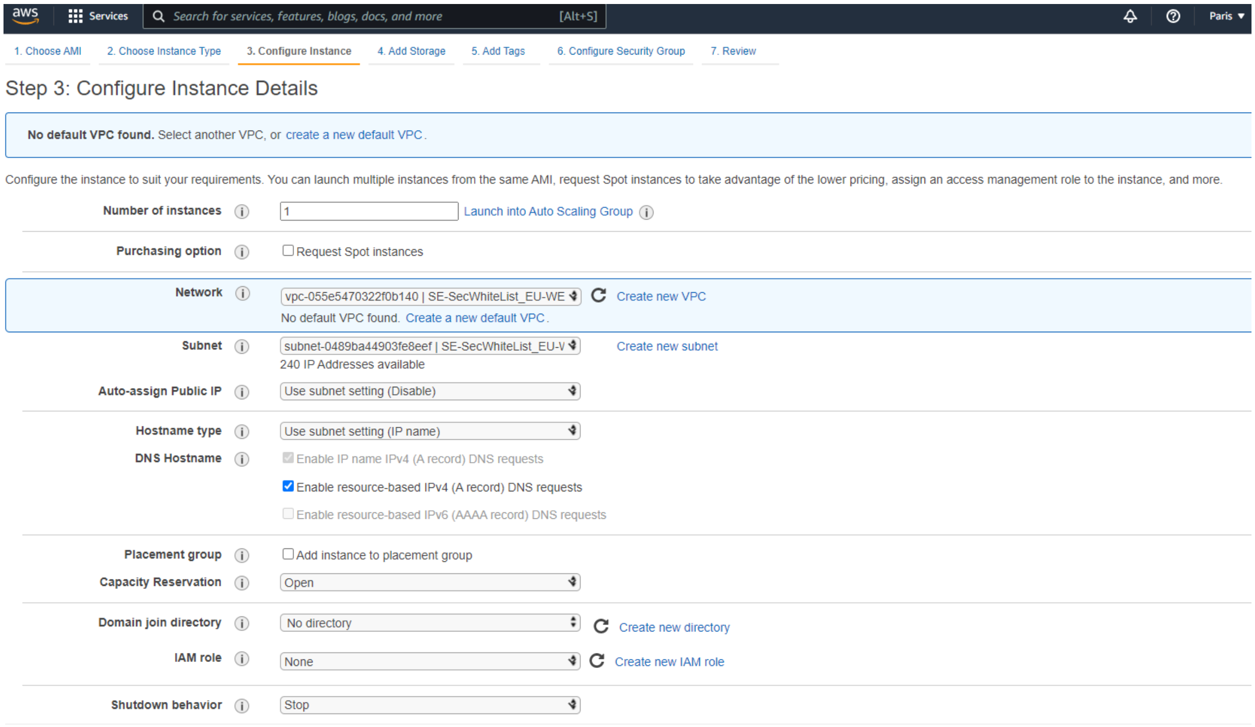
Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. Learn more about instance types and how they can meet your computing needs.

Filter by: All instance families Current generation Show/Hide Columns

Currently selected: t2.2xlarge (- ECUs, 8 vCPUs, 2.3 GHz, -, 32 GiB memory, EBS only)

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
□	t2	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
□	t2	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate	Yes
□	t2	t2.small	1	2	EBS only	-	Low to Moderate	Yes
□	t2	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
□	t2	t2.large	2	8	EBS only	-	Low to Moderate	Yes
□	t2	t2.xlarge	4	16	EBS only	-	Moderate	Yes
■	t2	t2.2xlarge	8	32	EBS only	-	Moderate	Yes
□	t3	t3.nano	2	0.5	EBS only	Yes	Up to 5 Gigabit	Yes
□	t3	t3.micro	2	1	EBS only	Yes	Up to 5 Gigabit	Yes
□	t3	t3.small	2	2	EBS only	Yes	Up to 5 Gigabit	Yes
□	t3	t3.medium	2	4	EBS only	Yes	Up to 5 Gigabit	Yes
□	t3	t3.large	2	8	EBS only	Yes	Up to 5 Gigabit	Yes
□	t3	t3.xlarge	4	16	EBS only	Yes	Up to 5 Gigabit	Yes



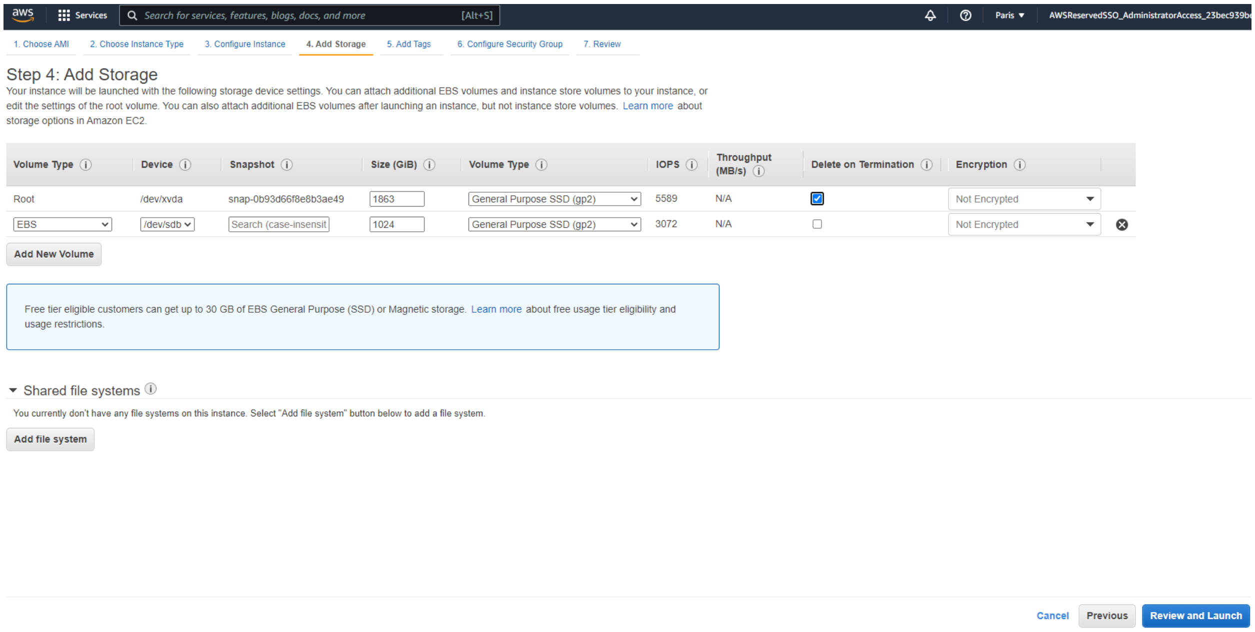
Step 3: Configure Instance Details

No default VPC found. Select another VPC, or create a new default VPC.

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances	1 — Launch into Auto Scaling Group
Purchasing option	□ Request Spot instances
Network	vpc-055e5470322f0b140 | SE-SecWhiteList_EU-WE — Create new VPC No default VPC found. Create a new default VPC.
Subnet	subnet-0489ba44903fe8eef | SE-SecWhiteList_EU-V — Create new subnet 240 IP Addresses available
Auto-assign Public IP	Use subnet setting (Disable)
Hostname type	Use subnet setting (IP name)
DNS Hostname	☑ Enable IP name IPv4 (A record) DNS requests ☑ Enable resource-based IPv4 (A record) DNS requests □ Enable resource-based IPv6 (AAAA record) DNS requests
Placement group	□ Add instance to placement group
Capacity Reservation	Open
Domain join directory	No directory — Create new directory
IAM role	None — Create new IAM role
Shutdown behavior	Stop

2.2. Add a second storage as recommended by Riverbed


aws
Services
Search for services, features, blogs, docs, and more [Alt+S]
Paris
AWSReservedSSO_AdministratorAccess_23bec939b
1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. Learn more about storage options in Amazon EC2.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encryption
Root	/dev/xvda	snap-0b93d66f8e8b3ae49	1863	General Purpose SSD (gp2)	5589	N/A	☑	Not Encrypted
EBS	/dev/sdb	Search (case-insensit	1024	General Purpose SSD (gp2)	3072	N/A	□	Not Encrypted

Add New Volume

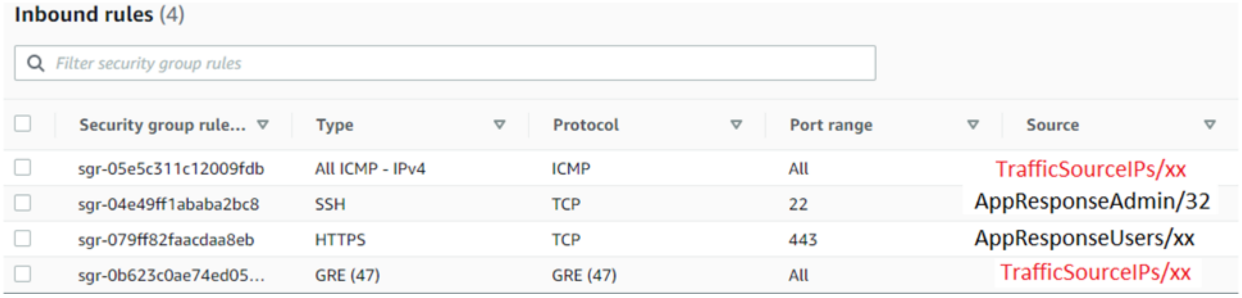
Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. Learn more about free usage tier eligibility and usage restrictions.

Shared file systems

You currently don't have any file systems on this instance. Select "Add file system" button below to add a file system.

Add file system

Configure Security Group Inbound rules to allow GRE and ICMP traffic from CloudLens Sensors



Inbound rules (4)

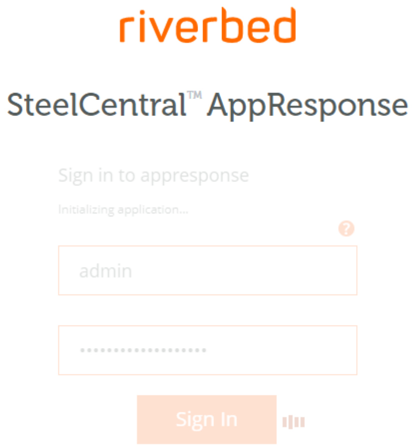
Filter security group rules

□	Security group rule...	Type	Protocol	Port range	Source
□	sgr-05e5c311c12009fdb	All ICMP - IPv4	ICMP	All	TrafficSourceIPs/xx
□	sgr-04e49ff1ababa2bc8	SSH	TCP	22	AppResponseAdmin/32
□	sgr-079ff82faacdaa8eb	HTTPS	TCP	443	AppResponseUsers/xx
□	sgr-0b623c0ae74ed05...	GRE (47)	GRE (47)	All	TrafficSourceIPs/xx

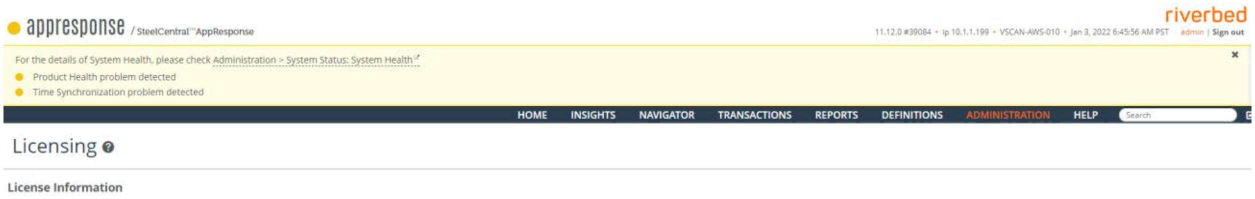
TrafficSourceIP.xx is the range of IPs from the Cloudlens Source Instances, ie, the VMs from which you will get traffic from

Cloudlens 6.1.0 note. It is possible to not require the opening of ICMP port from Cloudlens source instances running Linux, see Section 9 for more details.

2.3. Log in to AppResponse. User is admin and default password is your AWS <instance-id>



2.4. Add Riverbed licenses. Administration – OTHER- Licensing



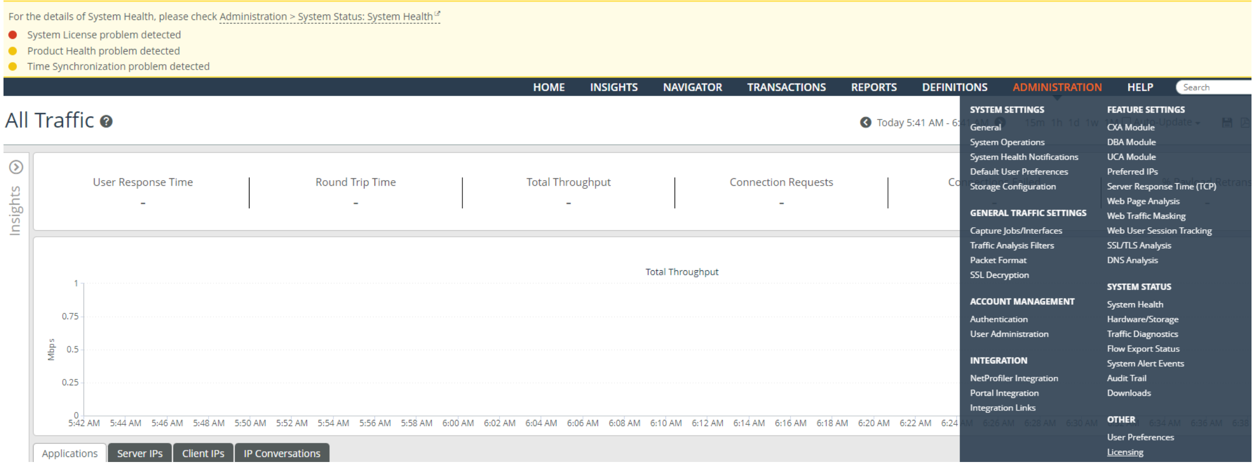
appresponse / SteelCentral™ AppResponse
riverbed
11.12.0 #39084 • ip 10.1.1.199 • VSCAN-AWS-010 • Jan 3, 2022 6:45:56 AM PST
admin | Sign out
HOME
INSIGHTS
NAVIGATOR
TRANSACTIONS
REPORTS
DEFINITIONS
ADMINISTRATION
HELP
Search

For the details of System Health, please check Administration > System Status: System Health

- Product Health problem detected
- Time Synchronization problem detected

Licensing

License Information



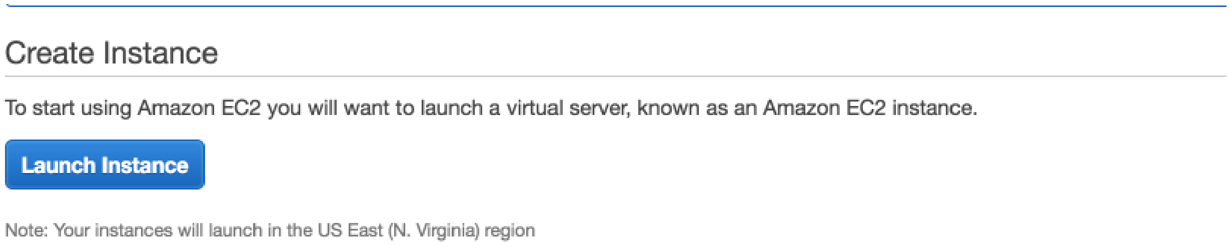
For the details of System Health, please check Administration > System Status: System Health

- ● System License problem detected
- ● Product Health problem detected
- ● Time Synchronization problem detected

3. Creating a Windows Source Instance in AWS.

Note: this assumes you don’t already have a Windows instance running that you want to monitor, if your Windows instance is already running you can skip ahead to Step 5. (however please also make note of required security group settings in Section 9).

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



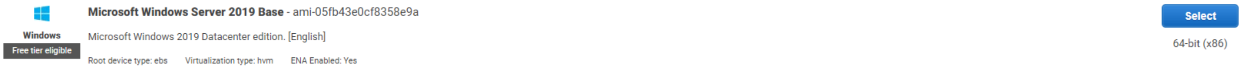
Create Instance

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

3.2. Choose Windows 2019 Server. Click “Select”



Windows
Free tier eligible

Microsoft Windows Server 2019 Base - ami-05fb43e0cf8358e9a

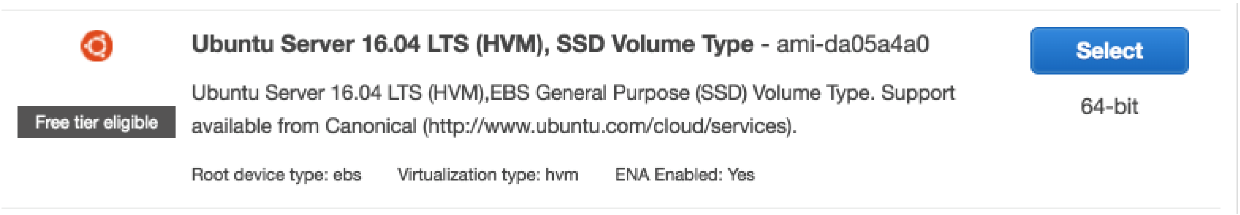
Microsoft Windows 2019 Datacenter edition. [English]

Root device type: ebs   Virtualization type: hvm   ENA Enabled: Yes

Select

64-bit (x86)

and



Free tier eligible

Ubuntu Server 16.04 LTS (HVM), SSD Volume Type - ami-da05a4a0

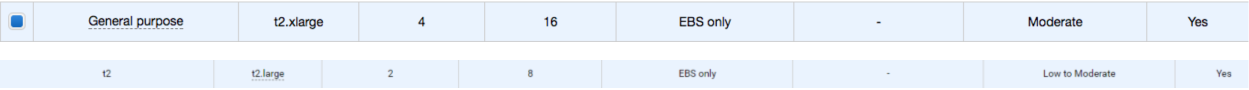
Ubuntu Server 16.04 LTS (HVM),EBS General Purpose (SSD) Volume Type. Support available from Canonical (http://www.ubuntu.com/cloud/services).

Root device type: ebs   Virtualization type: hvm   ENA Enabled: Yes

Select

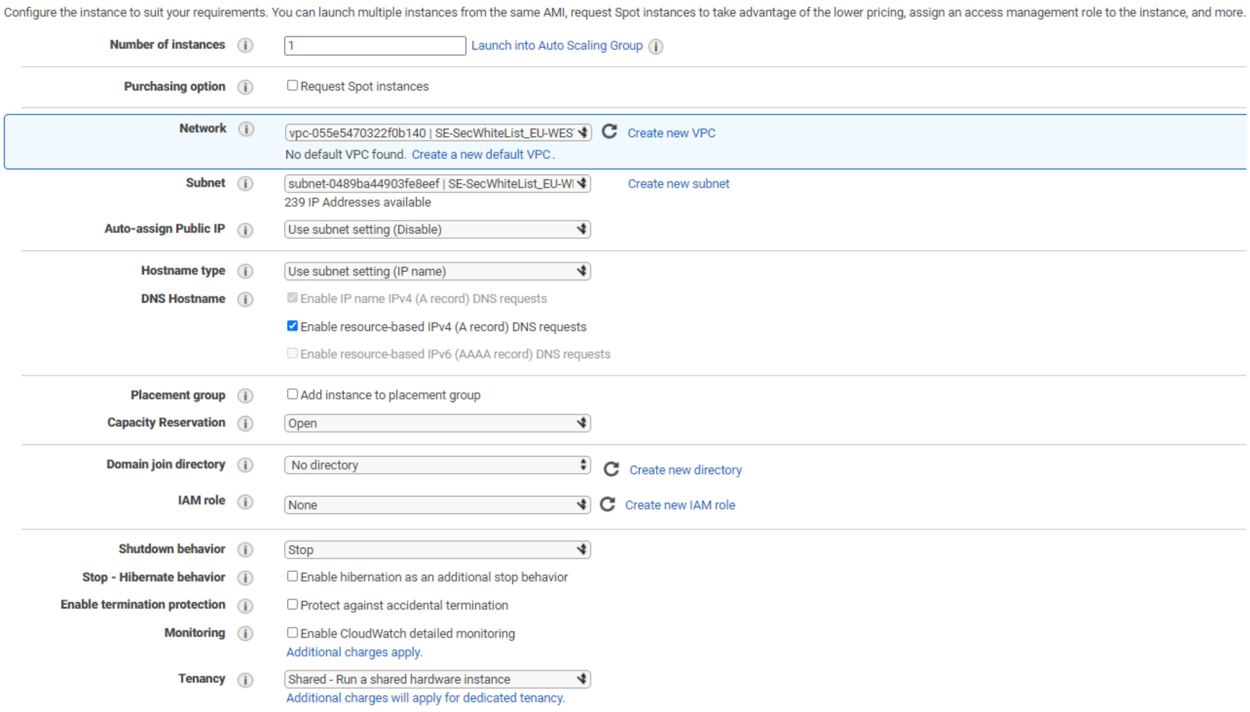
64-bit

3.3. Enter Virtual Machine instance type (e.g. t2.xlarge)



■	General purpose	t2.xlarge	4	16	EBS only	-	Moderate	Yes
	t2	t2.large	2	8	EBS only	-	Low to Moderate	Yes

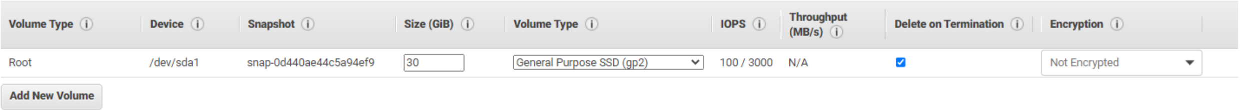
3.4. Select configuration details



Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

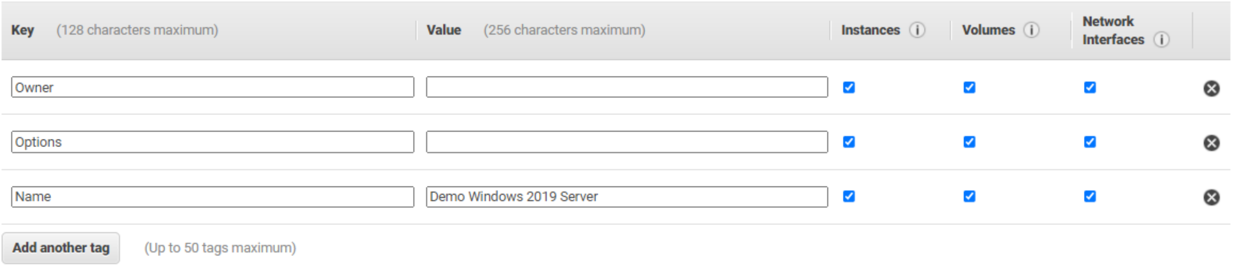
Number of instances	1 Launch into Auto Scaling Group
Purchasing option	☐ Request Spot instances
Network	vpc-055e5470322f0b140 | SE-SecWhiteList_EU-WES Create new VPC No default VPC found. Create a new default VPC.
Subnet	subnet-0489ba44903fe8eef | SE-SecWhiteList_EU-W Create new subnet 239 IP Addresses available
Auto-assign Public IP	Use subnet setting (Disable)
Hostname type	Use subnet setting (IP name)
DNS Hostname	☑ Enable IP name IPv4 (A record) DNS requests ☑ Enable resource-based IPv4 (A record) DNS requests ☐ Enable resource-based IPv6 (AAAA record) DNS requests
Placement group	☐ Add instance to placement group
Capacity Reservation	Open
Domain join directory	No directory Create new directory
IAM role	None Create new IAM role
Shutdown behavior	Stop
Stop - Hibernate behavior	☐ Enable hibernation as an additional stop behavior
Enable termination protection	☐ Protect against accidental termination
Monitoring	☐ Enable CloudWatch detailed monitoring Additional charges apply.
Tenancy	Shared - Run a shared hardware instance Additional charges will apply for dedicated tenancy.

3.5. Add storage



Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encryption
Root	/dev/sda1	snap-0d440ae44c5a94ef9	30	General Purpose SSD (gp2)	100 / 3000	N/A	☑	Not Encrypted

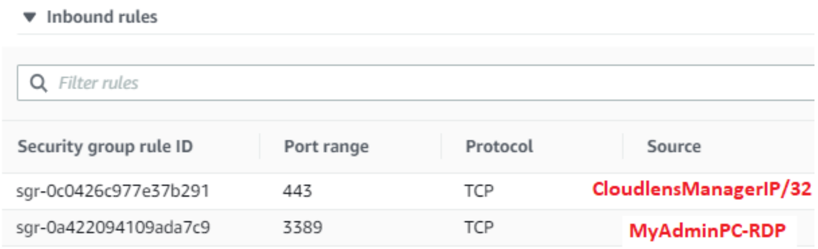
3.6. Add Tags as desired, allows for easier identification and grouping of instances in CloudLens



Key (128 characters maximum)	Value (256 characters maximum)	Instances	Volumes	Network Interfaces
Owner		☑	☑	☑
Options		☑	☑	☑
Name	Demo Windows 2019 Server	☑	☑	☑

3.7. Assign a security group

Please see list of CloudLens required port numbers in Section 7 of this document for guidance when creating or editing your security group.

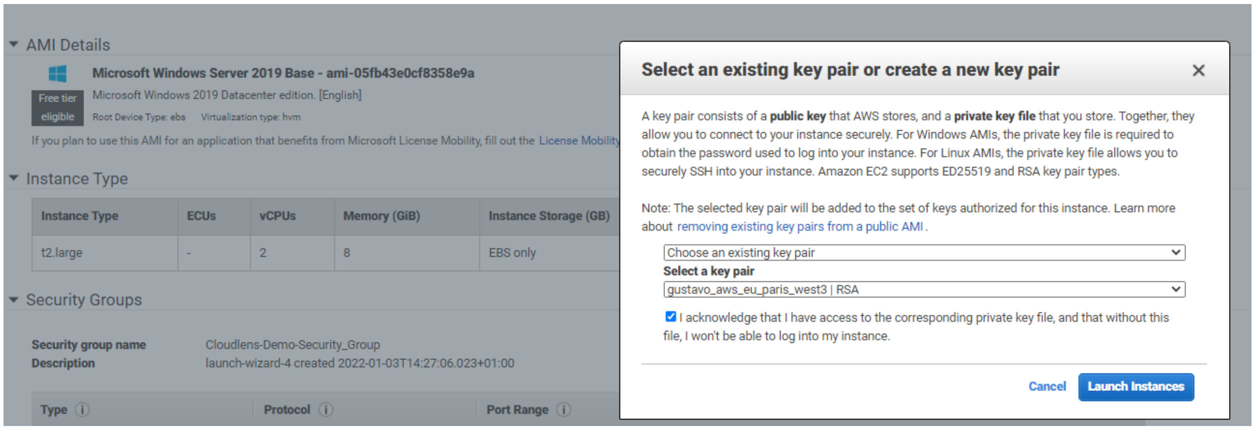


▼ Inbound rules

Filter rules

Security group rule ID	Port range	Protocol	Source
sgr-0c0426c977e37b291	443	TCP	CloudlensManagerIP/32
sgr-0a422094109ada7c9	3389	TCP	MyAdminPC-RDP

3.8. Launch the instance with the correct key pair



▼ AMI Details

Microsoft Windows Server 2019 Base - ami-05fb43e0cf8358e9a

Free tier eligible

Microsoft Windows 2019 Datacenter edition. [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

▼ Instance Type

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)
t2.large	-	2	8	EBS only

▼ Security Groups

Security group name Cloudlens-Demo-Security_Group
Description launch-wizard-4 created 2022-01-03T14:27:06.023+01:00

Type ⓘ	Protocol ⓘ	Port Range ⓘ

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. Amazon EC2 supports ED25519 and RSA key pair types.

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

gustavo_aws_eu_paris_west3 | RSA

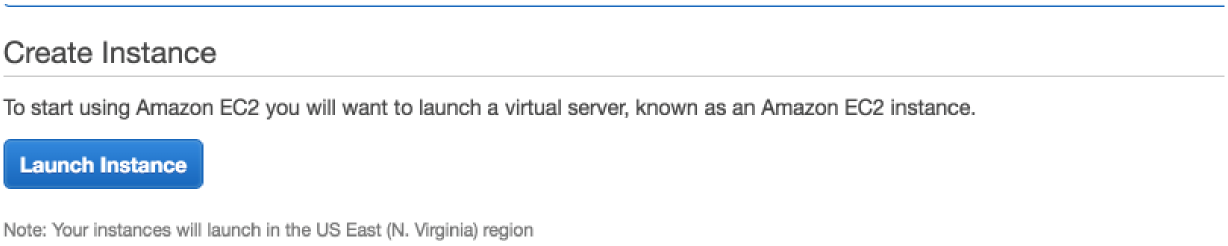
☑ I acknowledge that I have access to the corresponding private key file, and that without this file, I won't be able to log into my instance.

4. Creating a Linux Source Instance in AWS

Note: this assumes you don’t already have a Linux instance running that you want to monitor, if your Windows instance is already running you can skip ahead to Step 6. (however please also make note of required security group settings in Section 9).

In this example we will deploy Cloudlens in an Amazon Linux instance. The process is similar for any other Linux OS instances.

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

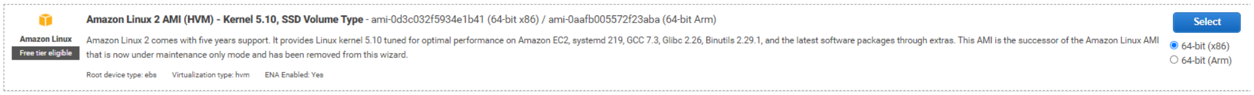


Create Instance

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

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

4.2. Choose Amazon Linux 2 AMI (HVM) Kernel 5.10 Click “Select”



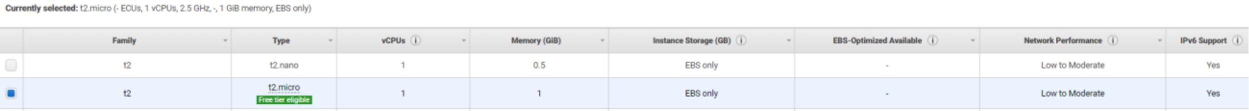
Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type - ami-0d3c032f5934e1b41 (64-bit x86) / ami-0aafb005572f23aba (64-bit Arm)

Amazon Linux 2 comes with five years support. It provides Linux kernel 5.10 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibc 2.26, Binutils 2.29.1, and the latest software packages through extras. This AMI is the successor of the Amazon Linux AMI that is now under maintenance only mode and has been removed from this wizard.

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

● 64-bit (x86)
○ 64-bit (Arm)

4.3. Enter Virtual Machine instance type (e.g. t2.micro)

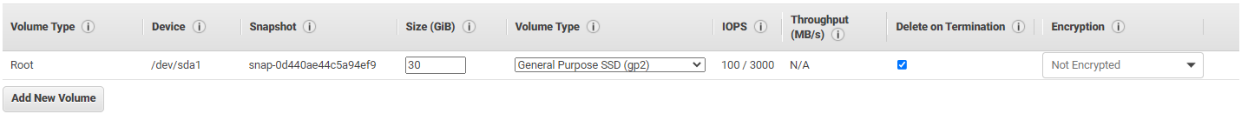


Currently selected: t2.micro (- ECUs, 1 vCPUs, 2.5 GHz, -, 1 GiB memory, EBS only)

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
□	t2	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
■	t2	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate	Yes

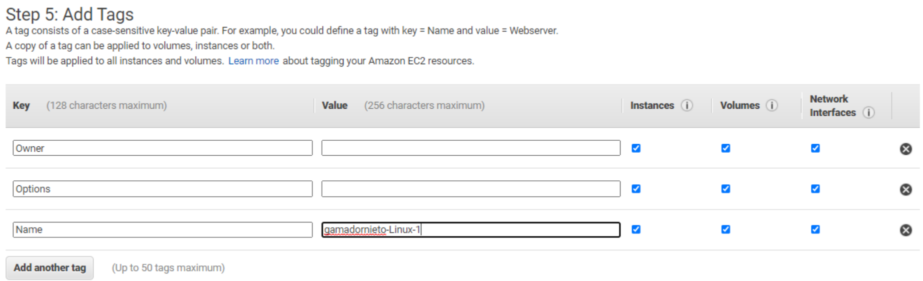
4.4. Select your VPC and Subnet in configuration details

4.5. Specify storage, otherwise keep default.



Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encryption
Root	/dev/sda1	snap-0d440ae44c5a94ef9	30	General Purpose SSD (gp2)	100 / 3000	N/A	☑	Not Encrypted

4.6. Add Tags as desired, allows for easier identification and grouping of instances in CloudLens



Step 5: Add Tags

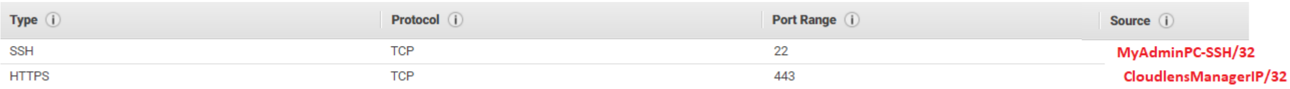
A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.
A copy of a tag can be applied to volumes, instances or both.
Tags will be applied to all instances and volumes. Learn more about tagging your Amazon EC2 resources.

Key (128 characters maximum)	Value (256 characters maximum)	Instances	Volumes	Network Interfaces	
Owner		☑	☑	☑	⊗
Options		☑	☑	☑	⊗
Name	gamadornieto-Linux-1	☑	☑	☑	⊗

(Up to 50 tags maximum)

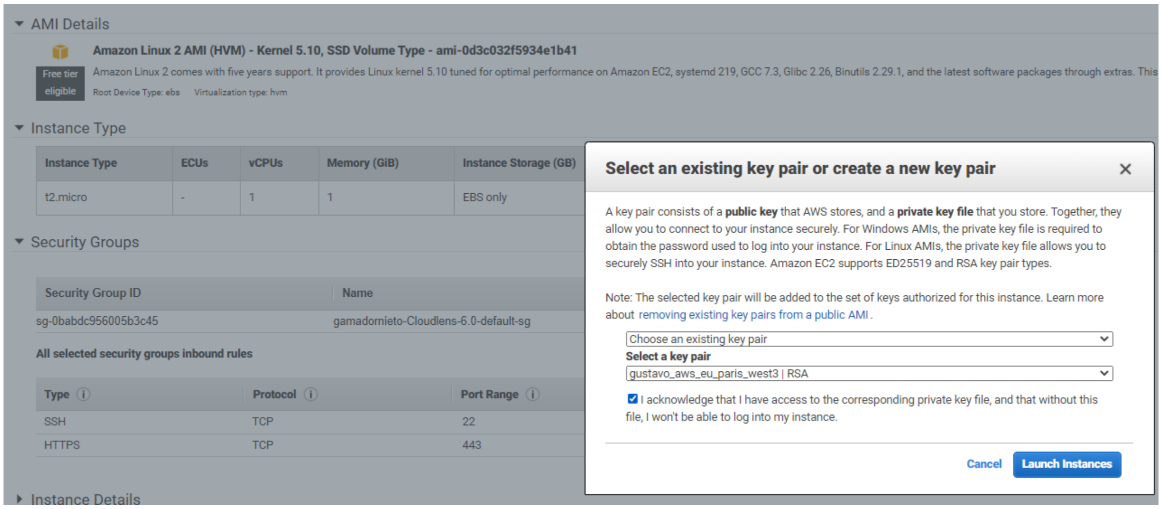
4.7. Assign a security group

Please see list of CloudLens required port numbers on Section 9 of this document for guidance when creating or editing your security group.



Type	Protocol	Port Range	Source
SSH	TCP	22	MyAdminPC-SSH/32
HTTPS	TCP	443	CloudlensManagerIP/32

4.8. Launch the instance with the correct key pair



AMI Details

Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type - ami-0d3c032f5934e1b41

Free tier eligible

Amazon Linux 2 comes with five years support. It provides Linux kernel 5.10 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibc 2.26, Binutils 2.29.1, and the latest software packages through extras. This

Root Device Type: ebs   Virtualization type: hvm

Instance Type

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)
t2.micro	-	1	1	EBS only

Security Groups

Security Group ID	Name
sg-0babdc956005b3c45	gamadornieto-Cloudlens-6.0-default-sg

All selected security groups inbound rules

Type	Protocol	Port Range
SSH	TCP	22
HTTPS	TCP	443

Instance Details

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. Amazon EC2 supports ED25519 and RSA key pair types.

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

gustavo_aws_eu_paris_west3 | RSA

☑ I acknowledge that I have access to the corresponding private key file, and that without this file, I won't be able to log into my instance.

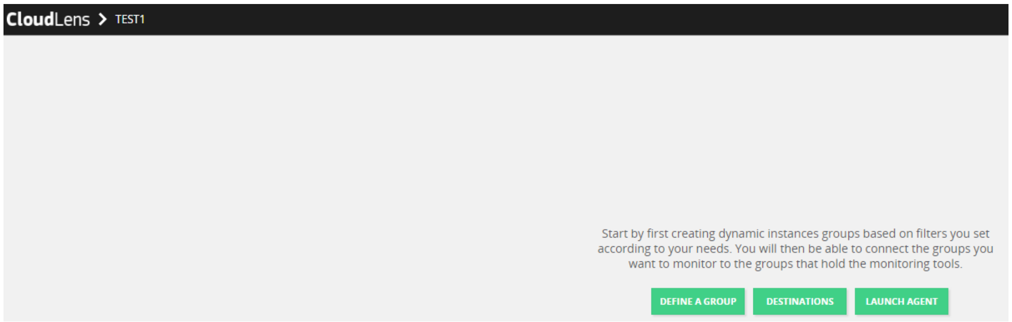
5. Installing Cloudlens Agent in Windows Server VM

5.1. Go inside a project of your Cloudlens Manager Log into https://<ipaddress-cloudlens-manager/startup>

Note: default credentials are admin / Cl0udLens@dm!n

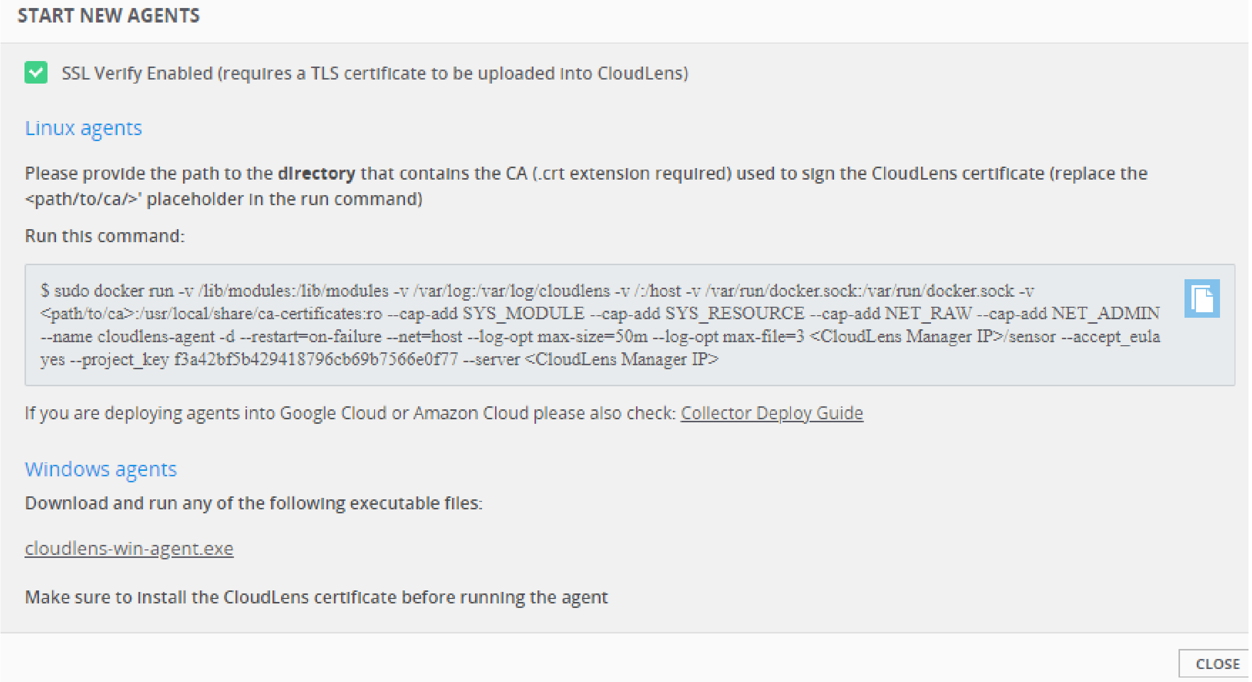
Create a new Project or open an existing Project

(make a copy of the Project Key, aka API Key, you will need this later in step 5.8)



Start by first creating dynamic instances groups based on filters you set according to your needs. You will then be able to connect the groups you want to monitor to the groups that hold the monitoring tools.

5.2. Click on Launch Agent to see information about the CloudLens Agent.



START NEW AGENTS

☑ SSL Verify Enabled (requires a TLS certificate to be uploaded into CloudLens)

Linux agents

Please provide the path to the **directory** that contains the CA (.crt extension required) used to sign the CloudLens certificate (replace the <path/to/ca/>' placeholder in the run command)

Run this command:

```
$ sudo docker run -v /lib/modules:/lib/modules -v /var/log:/var/log/cloudlens -v /:/host -v /var/run/docker.sock:/var/run/docker.sock -v
<path/to/ca>:/usr/local/share/ca-certificates:ro --cap-add SYS_MODULE --cap-add SYS_RESOURCE --cap-add NET_RAW --cap-add NET_ADMIN
--name cloudlens-agent -d --restart=on-failure --net=host --log-opt max-size=50m --log-opt max-file=3 <CloudLens Manager IP>/sensor --accept_eula
yes --project_key f3a42bf5b429418796cb69b7566e0f77 --server <CloudLens Manager IP>
```

If you are deploying agents into Google Cloud or Amazon Cloud please also check: Collector Deploy Guide

Windows agents

Download and run any of the following executable files:

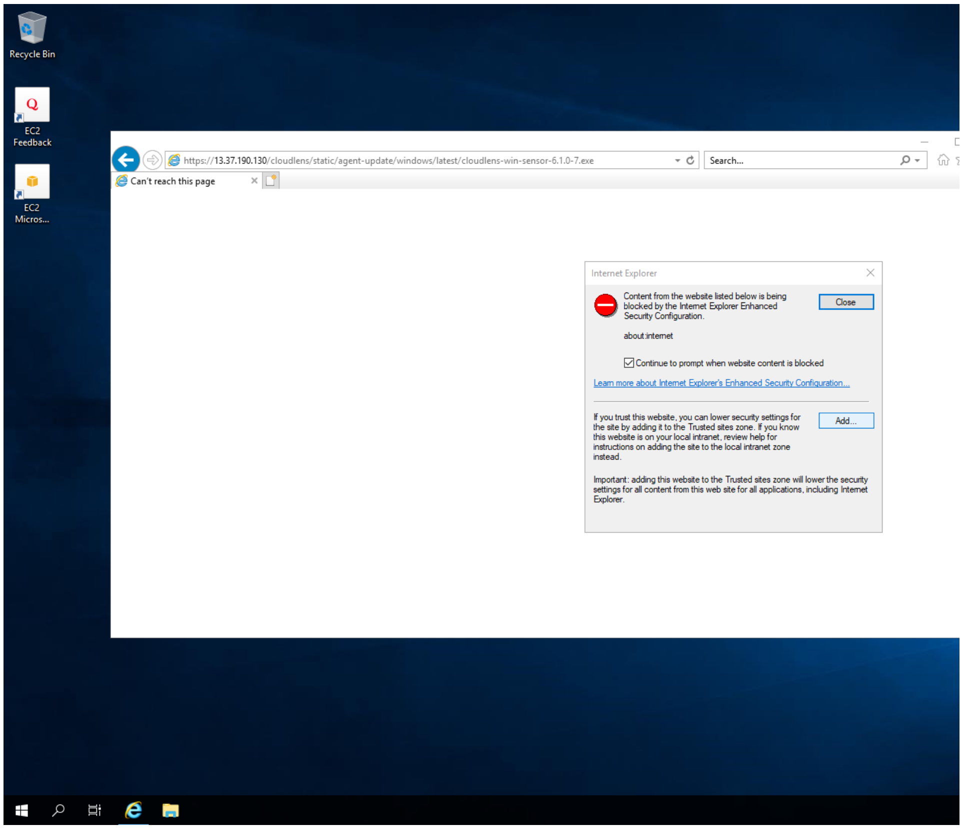
cloudlens-win-agent.exe

Make sure to install the CloudLens certificate before running the agent

The link to download the exe file has the following structure:

From the Windows Server browse to and then save the .exe file

https:// <CloudlensManagerIP>/cloudlens/static/agent-update/windows/latest/cloudlens-win-sensor-6.1.0-7.exe


Recycle Bin
EC2 Feedback
EC2 Micros...
https://13.37.190.130/cloudlens/static/agent-update/windows/latest/cloudlens-win-sensor-6.1.0-7.exe
Search...
Can't reach this page

Internet Explorer

Content from the website listed below is being blocked by the Internet Explorer Enhanced Security Configuration.

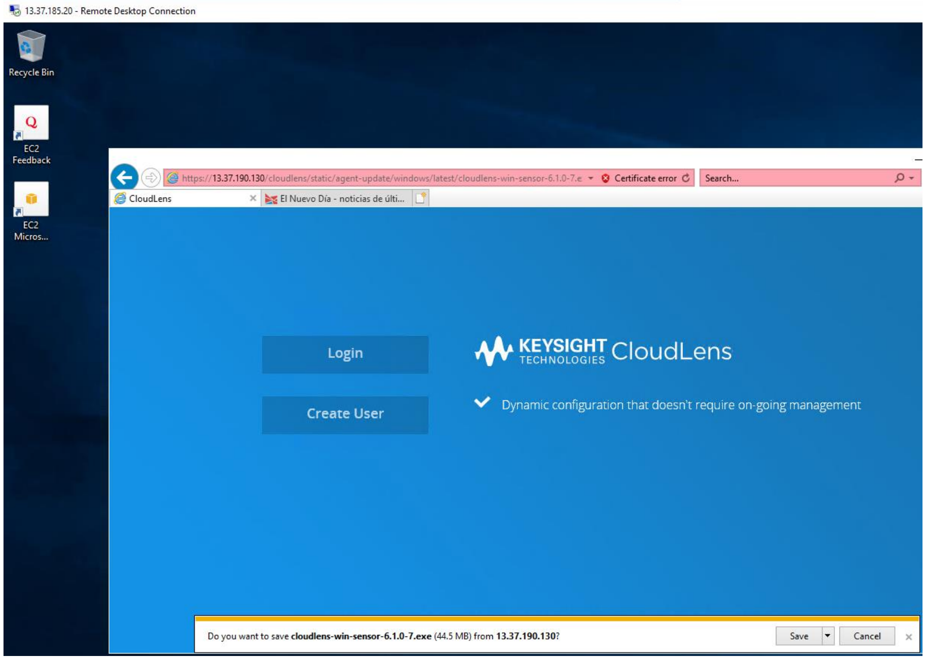
about:internet

☑ Continue to prompt when website content is blocked

Learn more about Internet Explorer's Enhanced Security Configuration...

If you trust this website, you can lower security settings for the site by adding it to the Trusted sites zone. If you know this website is on your local intranet, review help for instructions on adding the site to the local intranet zone instead.

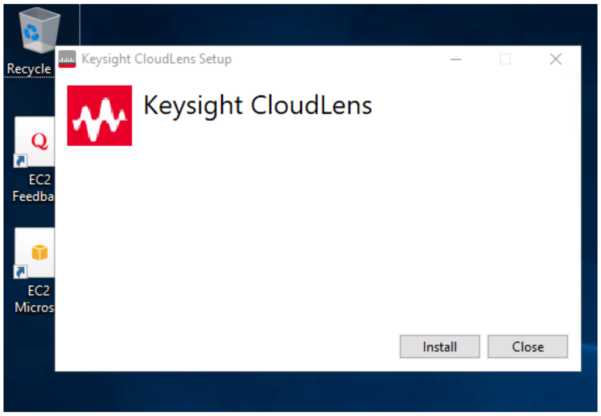
Important: adding this website to the Trusted sites zone will lower the security settings for all content from this web site for all applications, including Internet Explorer.


13.37.185.20 - Remote Desktop Connection
Recycle Bin
EC2 Feedback
EC2 Micros...
https://13.37.190.130/cloudlens/static/agent-update/windows/latest/cloudlens-win-sensor-6.1.0-7.e
Certificate error
Search...
CloudLens
El Nuevo Día - noticias de últi...
Login
Create User
KEYSIGHT TECHNOLOGIES CloudLens

✓ Dynamic configuration that doesn't require on-going management

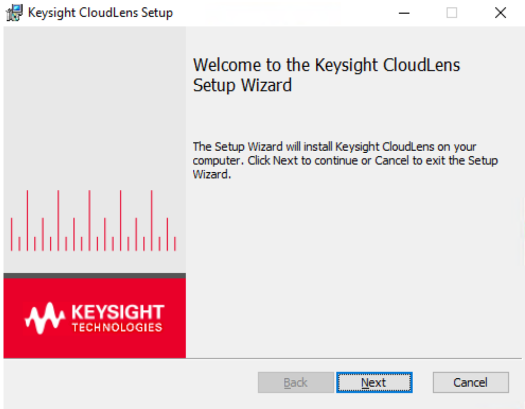
Do you want to save **cloudlens-win-sensor-6.1.0-7.exe** (44.5 MB) from **13.37.190.130**?

5.3. From the Windows Server Install the CloudLens .exe file which you just saved.


Keysight CloudLens Setup

Keysight CloudLens

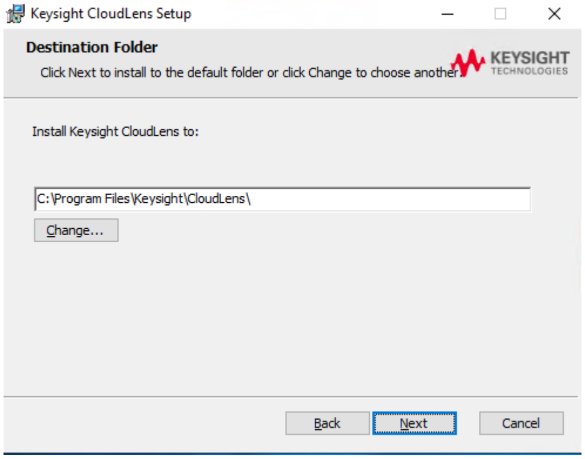
5.4. Installation wizard goes through the CloudLens agent installation and all dependent package installations.


Keysight CloudLens Setup

Welcome to the Keysight CloudLens Setup Wizard

The Setup Wizard will install Keysight CloudLens on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

5.5. Accept End User License Agreement


Keysight CloudLens Setup

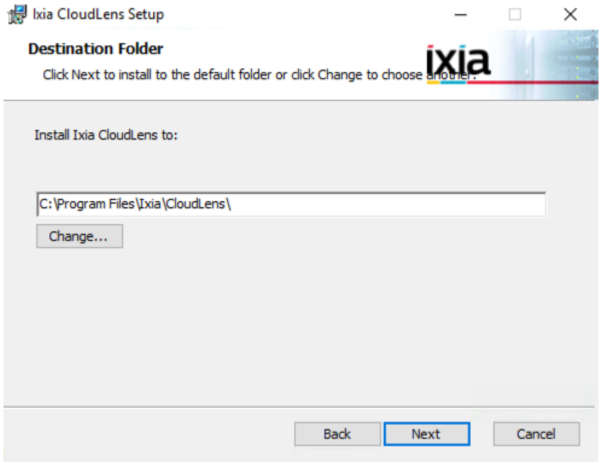
Destination Folder

Click Next to install to the default folder or click Change to choose another.

Install Keysight CloudLens to:

C:\Program Files\Keysight\CloudLens\

5.6. Accept End User License Agreement



Ixia CloudLens Setup

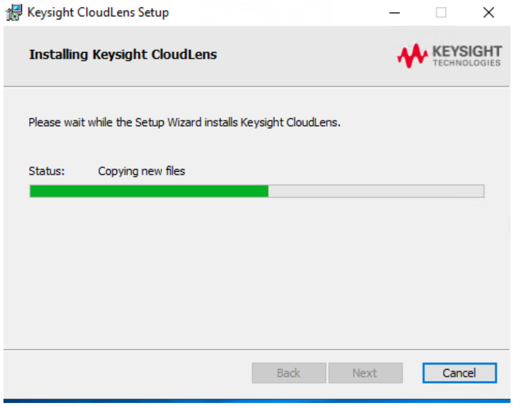
Destination Folder

Click Next to install to the default folder or click Change to choose another.

Install Ixia CloudLens to:

C:\Program Files\Ixia\CloudLens\

5.7. Click “Install”



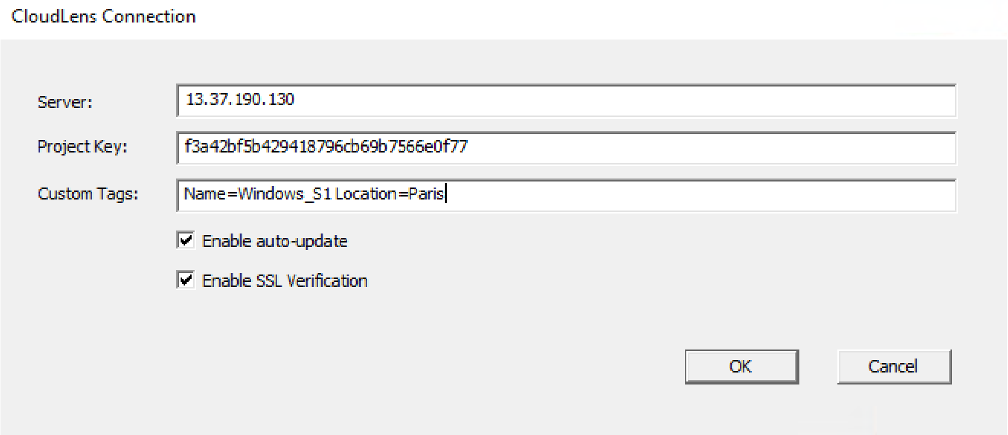
Keysight CloudLens Setup

Installing Keysight CloudLens

Please wait while the Setup Wizard installs Keysight CloudLens.

Status: Copying new files

5.8. The Windows instance needs to be associated with the IP address of your Cloudlens Manager. You must specify your Project Key (aka API key). You may want to define your custom Tags to automatically allocate the instance to the appropriate source group.



CloudLens Connection

Server: 13.37.190.130

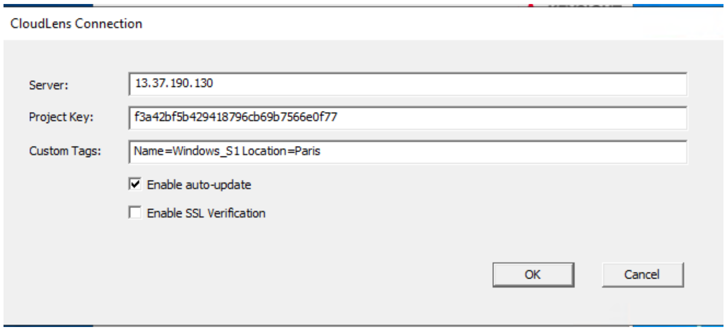
Project Key: f3a42bf5b429418796cb69b7566e0f77

Custom Tags: Name=Windows_S1 Location=Paris

☑ Enable auto-update

☑ Enable SSL Verification

5.9. Finish CloudLens sensor installation



CloudLens Connection

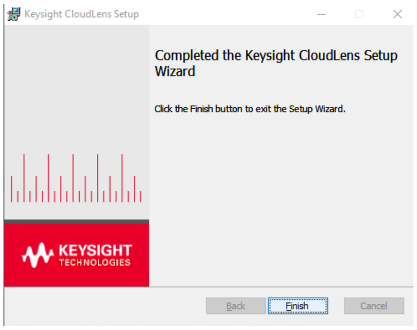
Server: 13.37.190.130

Project Key: f3a42bf5b429418796cb69b7566e0f77

Custom Tags: Name=Windows_S1 Location=Paris

☑ Enable auto-update

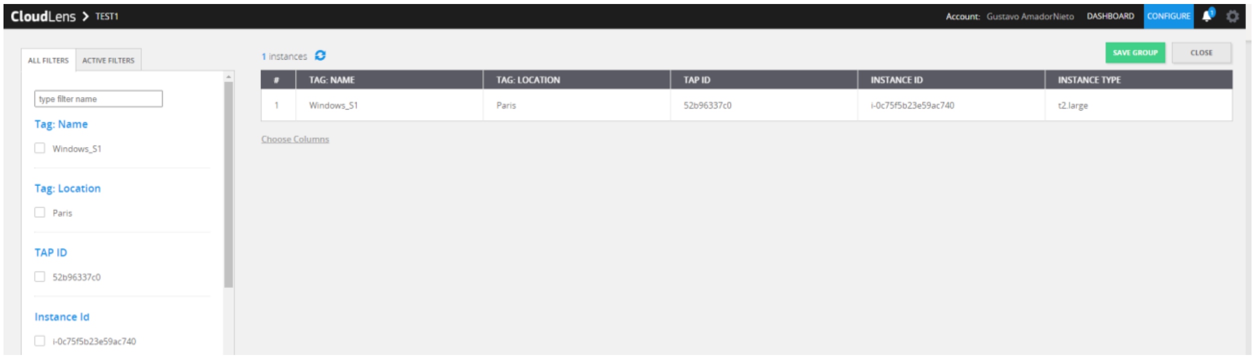
☐ Enable SSL Verification



Completed the Keysight CloudLens Setup Wizard

Click the Finish button to exit the Setup Wizard.

5.10. Return to the CloudLens Manager and verify that the instance is associated with the CloudLens project created.



Tag: Name
☐ Windows_S1

Tag: Location
☐ Paris

TAP ID
☐ 52b96337c0

Instance Id
☐ i-0c75f5b23e59ac740

1 instances

#	TAG: NAME	TAG: LOCATION	TAP ID	INSTANCE ID	INSTANCE TYPE
1	Windows_S1	Paris	52b96337c0	i-0c75f5b23e59ac740	t2.large

6. Installing Cloudlens Agent in Linux VM

Note: Before you begin

Go inside a project of your Cloudlens Manager

Log into https://<ipaddress-cloudlens-manager/startup>

Note: default credentials are admin / Cl0udLens@dm!n

Create a new Project or open an existing Project

(make a copy of the Project Key, aka API Key, you will need this later in step 6.3)

6.1. SSH to your Linux VM and install Docker

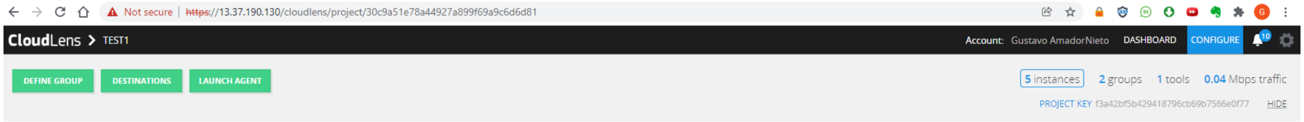
```
sudo yum update -y
sudo yum -y install docker
sudo service docker start
sudo systemctl enable docker
```

6.2. Specify CloudlensManager as a Docker registry and restart Docker Service

```
echo  ""{\"insecure-registries\":[\"<CloudlensManagerIP>\"]}" | sudo tee /etc/docker/daemon.json
sudo service docker restart
```

6.3. Start Cloudlens docker

Find your Cloudlens Project Key ID



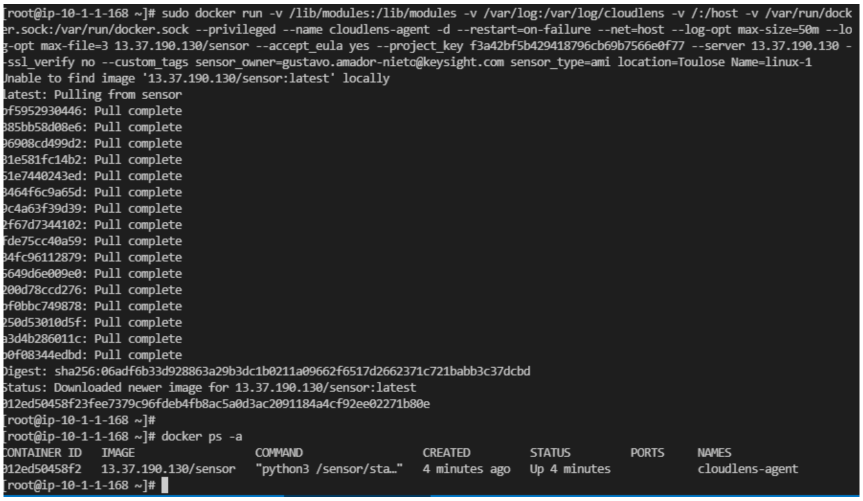
https://13.37.190.130/cloudlens/project/30c9a51e78a44927a899f69a9c6d6d81

Account: Gustavo AmadorNieto

5 instances 2 groups 1 tools 0.04 Mbps traffic

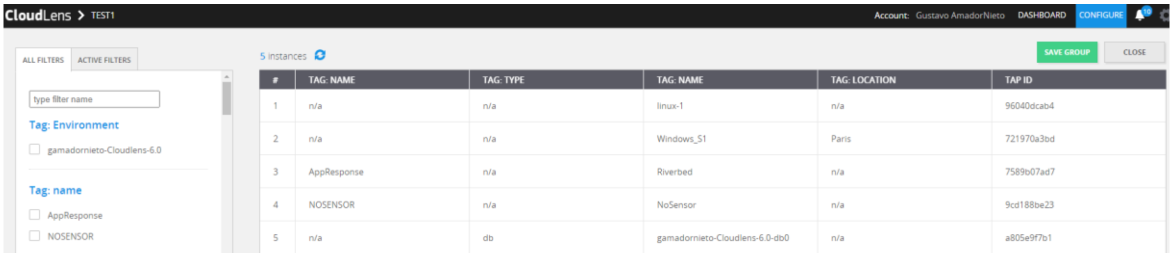
PROJECT KEY f3a42bf5b429418796cb69b7566e0f77

```
sudo docker run -v /lib/modules:/lib/modules -v /var/log:/var/log/cloudlens -v /:/host -v
/var/run/docker.sock:/var/run/docker.sock --privileged --name cloudlens-agent -d --restart=on-failure --
net=host --log-opt max-size=50m --log-opt max-file=3 <CloudlensManagerIP>/sensor --accept_eula
yes --project_key <CloudlensProjectKey> --server <CloudlensManagerIP> --ssl_verify no --
custom_tags sensor_owner=gustavo.amador-nieto@keysight.com sensor_type=ami
location=Toulose Name=linux-1
```



```
[root@ip-10-1-1-168 ~]# sudo docker run -v /lib/modules:/lib/modules -v /var/log:/var/log/cloudlens -v /:/host -v /var/run/dock
er.sock:/var/run/docker.sock --privileged --name cloudlens-agent -d --restart=on-failure --net=host --log-opt max-size=50m --lo
g-opt max-file=3 13.37.190.130/sensor --accept_eula yes --project_key f3a42bf5b429418796cb69b7566e0f77 --server 13.37.190.130 -
-ssl_verify no --custom_tags sensor_owner=gustavo.amador-nieto@keysight.com sensor_type=ami location=Toulose Name=linux-1
Unable to find image '13.37.190.130/sensor:latest' locally
latest: Pulling from sensor
bf5952930446: Pull complete
385bb58d08e6: Pull complete
96908cd499d2: Pull complete
31e581fc14b2: Pull complete
51e7440243ed: Pull complete
3464f6c9a65d: Pull complete
9c4a63f39d39: Pull complete
2f67d7344102: Pull complete
fde75cc40a59: Pull complete
34fc96112879: Pull complete
5649d6e009e0: Pull complete
200d78ccd276: Pull complete
bf0bbc749878: Pull complete
250d53010d5f: Pull complete
a3d4b286011c: Pull complete
b0f08344edbd: Pull complete
Digest: sha256:06adf6b33d928863a29b3dc1b0211a09662f6517d2662371c721babb3c37dcbd
Status: Downloaded newer image for 13.37.190.130/sensor:latest
012ed50458f23fee7379c96fdeb4fb8ac5a0d3ac2091184a4cf92ee02271b80e
[root@ip-10-1-1-168 ~]#
[root@ip-10-1-1-168 ~]# docker ps -a
CONTAINER ID   IMAGE                 COMMAND                  CREATED         STATUS         PORTS     NAMES
012ed50458f2   13.37.190.130/sensor  "python3 /sensor/sta…"   4 minutes ago   Up 4 minutes             cloudlens-agent
[root@ip-10-1-1-168 ~]#
```

Go inside the project of your Cloudlens Manager to check that the instance has registered



Tag: Environment

□ gamadornieto-Cloudlens-6.0

Tag: name

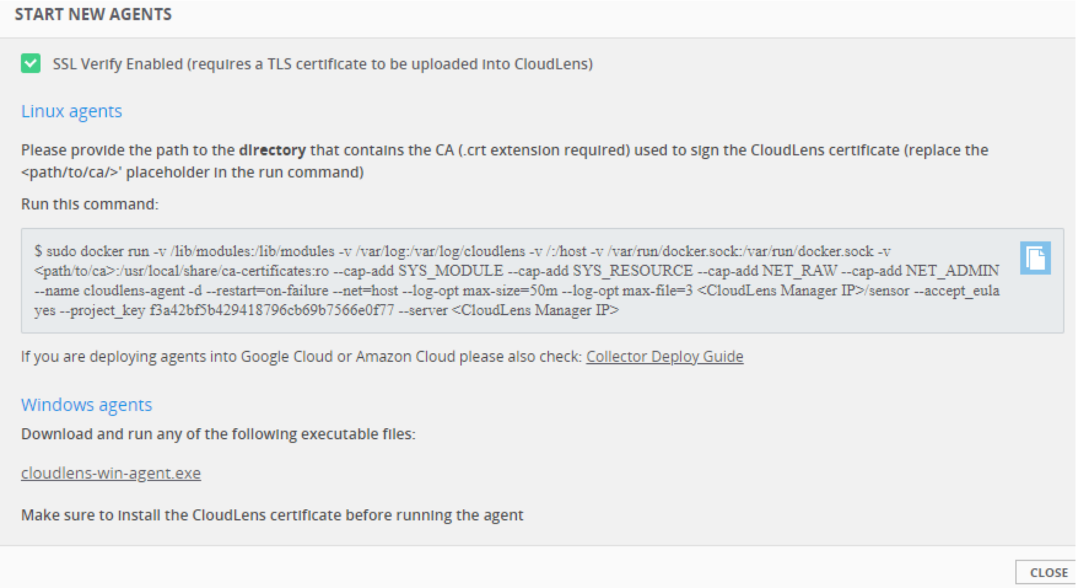
□ AppResponse

□ NOSENSOR

5 instances

#	TAG: NAME	TAG: TYPE	TAG: NAME	TAG: LOCATION	TAP ID
1	n/a	n/a	linux-1	n/a	96040dcab4
2	n/a	n/a	Windows_S1	Paris	721970a3bd
3	AppResponse	n/a	Riverbed	n/a	7589b07ad7
4	NOSENSOR	n/a	NoSensor	n/a	9cd188be23
5	n/a	db	gamadornieto-Cloudlens-6.0-db0	n/a	a805e9f7b1

Note: If you optionally want to verify SSL between the Cloudlens Docker and the CloudlensManager SSL or use additional flags please refer to CloudlensManager wizard and help



START NEW AGENTS

☑ SSL Verify Enabled (requires a TLS certificate to be uploaded into CloudLens)

Linux agents

Please provide the path to the **directory** that contains the CA (.crt extension required) used to sign the CloudLens certificate (replace the <path/to/ca/>' placeholder in the run command)

Run this command:

```
$ sudo docker run -v /lib/modules:/lib/modules -v /var/log:/var/log/cloudlens -v /:/host -v /var/run/docker.sock:/var/run/docker.sock -v
<path/to/ca>:/usr/local/share/ca-certificates:ro --cap-add SYS_MODULE --cap-add SYS_RESOURCE --cap-add NET_RAW --cap-add NET_ADMIN
--name cloudlens-agent -d --restart=on-failure --net=host --log-opt max-size=50m --log-opt max-file=3 <CloudLens Manager IP>/sensor --accept_eula
yes --project_key f3a42bf5b429418796cb69b7566e0f77 --server <CloudLens Manager IP>
```

If you are deploying agents into Google Cloud or Amazon Cloud please also check: Collector Deploy Guide

Windows agents

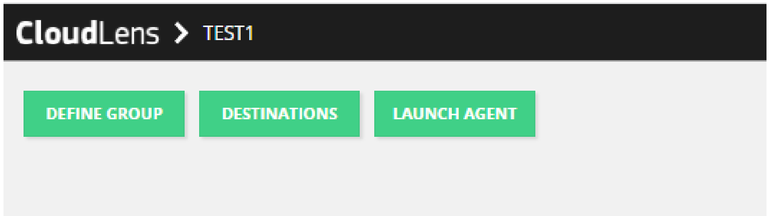
Download and run any of the following executable files:

cloudlens-win-agent.exe

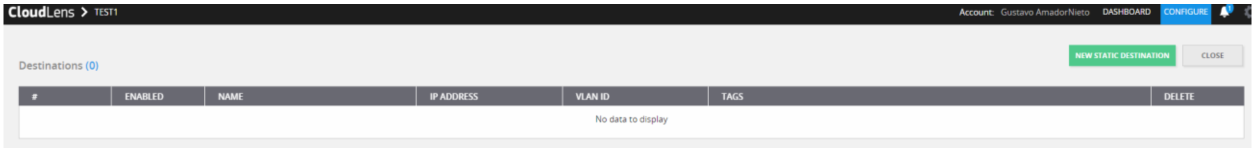
Make sure to install the CloudLens certificate before running the agent

7. Setting up AppResponse as a Static Destination

7.1. Log into your Cloudlens Project. Click on Destinations



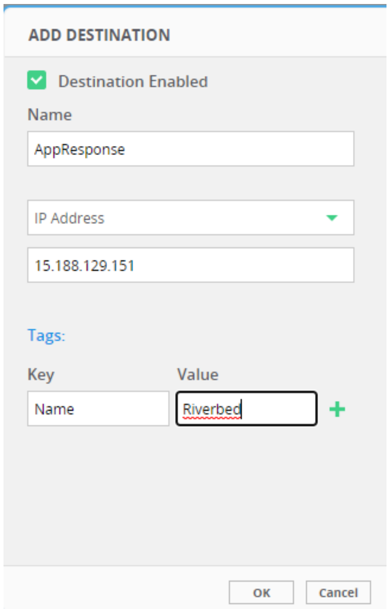
7.2. Click on New Static Destinations



Destinations (0)

#	ENABLED	NAME	IP ADDRESS	VLAN ID	TAGS	DELETE
No data to display						

7.3. Specify the IP address of the Riverbed AppResponse. Although no mandatory, it's a good practice to specify some custom tags to simplify the allocate of the the instance to the appropriate destination group.



☑ Destination Enabled

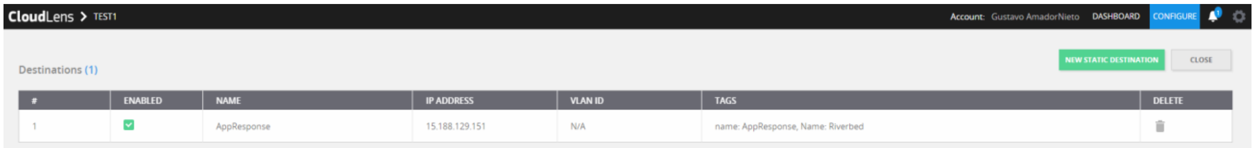
Name: AppResponse

IP Address: 15.188.129.151

Tags:

Key	Value
Name	Riverbed

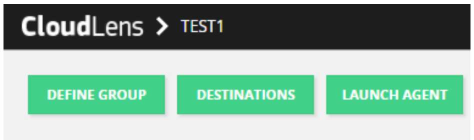
7.4. Riverbed AppResponse will appear on the list of static destinations



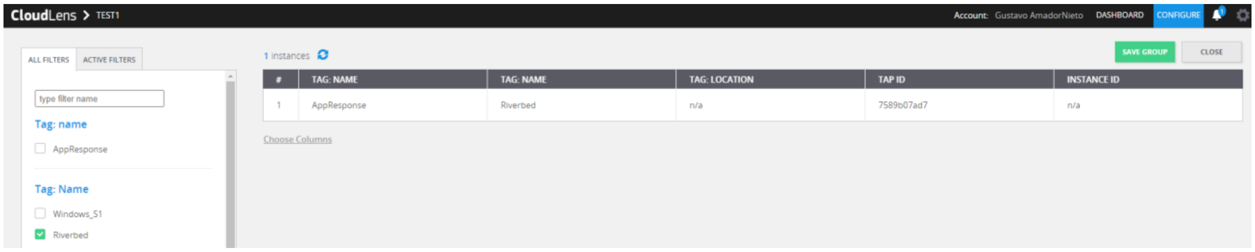
Destinations (1)

#	ENABLED	NAME	IP ADDRESS	VLAN ID	TAGS	DELETE
1	✓	AppResponse	15.188.129.151	N/A	name: AppResponse, Name: Riverbed	🗑

7.5. Go back to your Cloudlens project. Define a new group



7.6. Filter on the relevant tags to only select the Riverbed instance.



Tag: name

□ AppResponse

Tag: Name

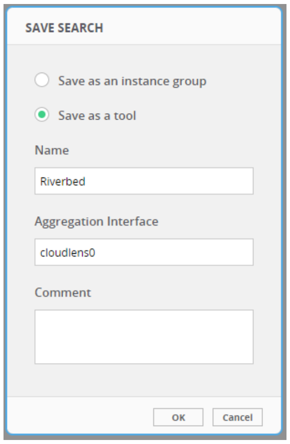
□ Windows_S1

☑ Riverbed

1 instances

#	TAG: NAME	TAG: NAME	TAG: LOCATION	TAP ID	INSTANCE ID
1	AppResponse	Riverbed	n/a	7589b07ad7	n/a

7.7. Save it as a tool.



○ Save as an instance group

● Save as a tool

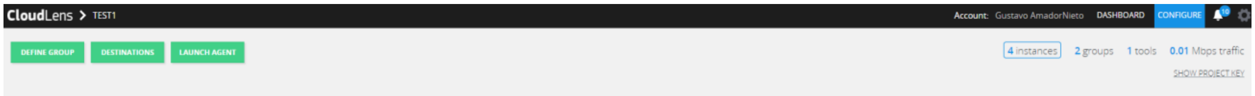
Name: Riverbed

Aggregation Interface: cloudlens0

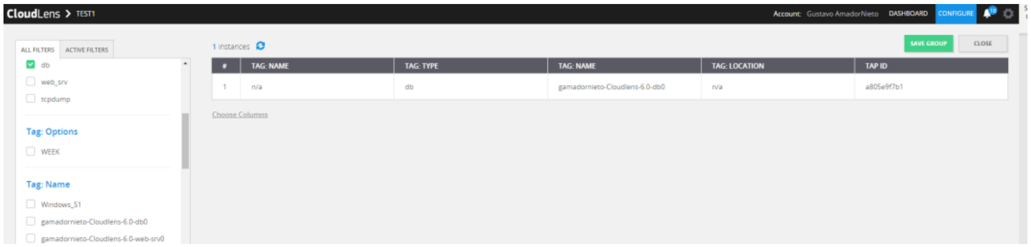
Comment:

8. Configuring traffic from VM Sources to Riverbed AppResponse

8.1. Verify the VMs are reflected in the CloudLens Manager portal once they are launched with the correct project key.



8.2. If not done previously, use Cloudlens tags to group instances as source groups. For instance, I will create 2 different source groups.



☑ db
□ web_srv
□ tcpdump

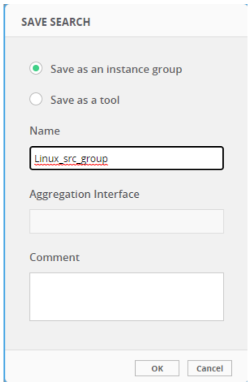
Tag: Options

□ WEEK

Tag: Name

□ Windows_S1
□ gamadornieto-Cloudlens-6.0-db0
□ gamadornieto-Cloudlens-6.0-web-srv0

#	TAG: NAME	TAG: TYPE	TAG: NAME	TAG: LOCATION	TAP ID
1	n/a	db	gamadornieto-Cloudlens-6.0-db0	n/a	a805e9f7b1


SAVE SEARCH

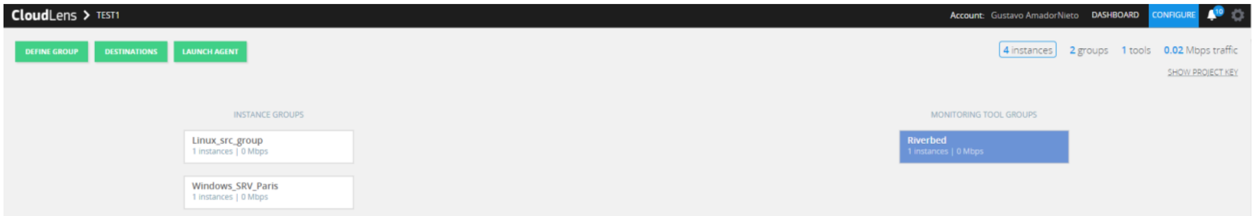
● Save as an instance group

○ Save as a tool

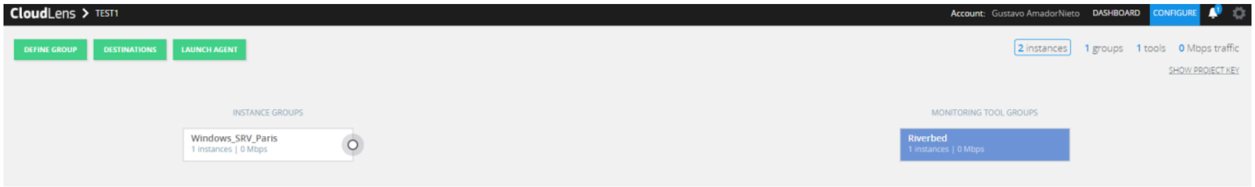
Name: Linux_src_group

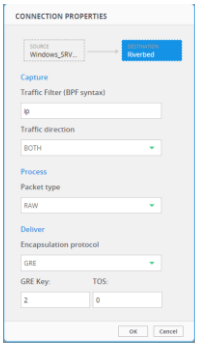
Aggregation Interface:

Comment:



8.3. Drag a secure visibility paths between the source groups and the tool group (Riverbed). Choose Encapsulation Protocol GREG, and set a value for the GRE key





CONNECTION PROPERTIES

SOURCE Windows_SRV... → DESTINATION Riverbed

Capture

Traffic Filter (BPF syntax): ip

Traffic direction: BOTH

Process

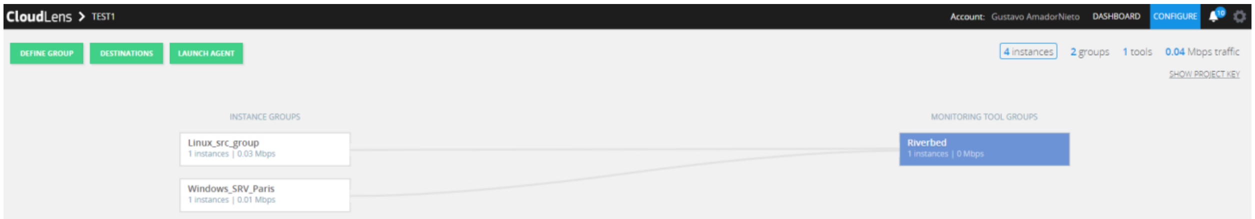
Packet type: RAW

Deliver

Encapsulation protocol: GRE

GRE Key: 2   TOS: 0

8.4. Repeat for all the source groups



4 instances   2 groups   1 tools   0.04 Mbps traffic

INSTANCE GROUPS

Linux_src_group
1 instances | 0.03 Mbps

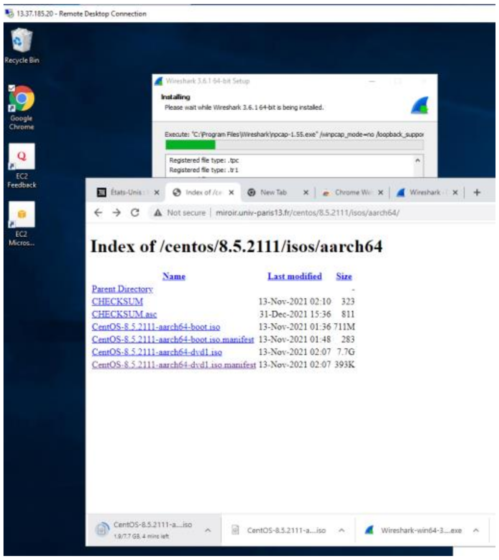
Windows_SRV_Paris
1 instances | 0.01 Mbps

MONITORING TOOL GROUPS

Riverbed
1 instances | 0 Mbps

8.5. Generate traffic from the sources.

For example, from one of my Windows instances I download the following image:



Installing

Please wait while Wireshark 3.6.1 64-bit is being installed.

Execute: "C:\Program Files\Wireshark\npcap-1.55.exe" /winpcap_mode=no /loopback_suppor

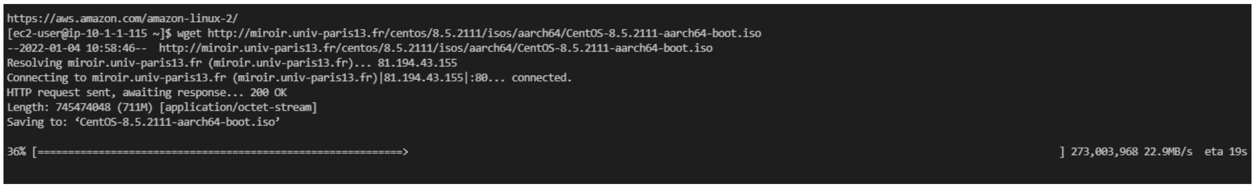
Registered file type: .tpc
Registered file type: .tr1

Not secure | miroir.univ-paris13.fr/centos/8.5.2111/isos/aarch64/

Index of /centos/8.5.2111/isos/aarch64

Name	Last modified	Size
Parent Directory		-
CHECKSUM	13-Nov-2021 02:10	323
CHECKSUM.asc	31-Dec-2021 15:36	811
CentOS-8.5.2111-aarch64-boot.iso	13-Nov-2021 01:36	711M
CentOS-8.5.2111-aarch64-boot.iso.manifest	13-Nov-2021 01:48	283
CentOS-8.5.2111-aarch64-dvd1.iso	13-Nov-2021 02:07	7.7G
CentOS-8.5.2111-aarch64-dvd1.iso.manifest	13-Nov-2021 02:07	393K

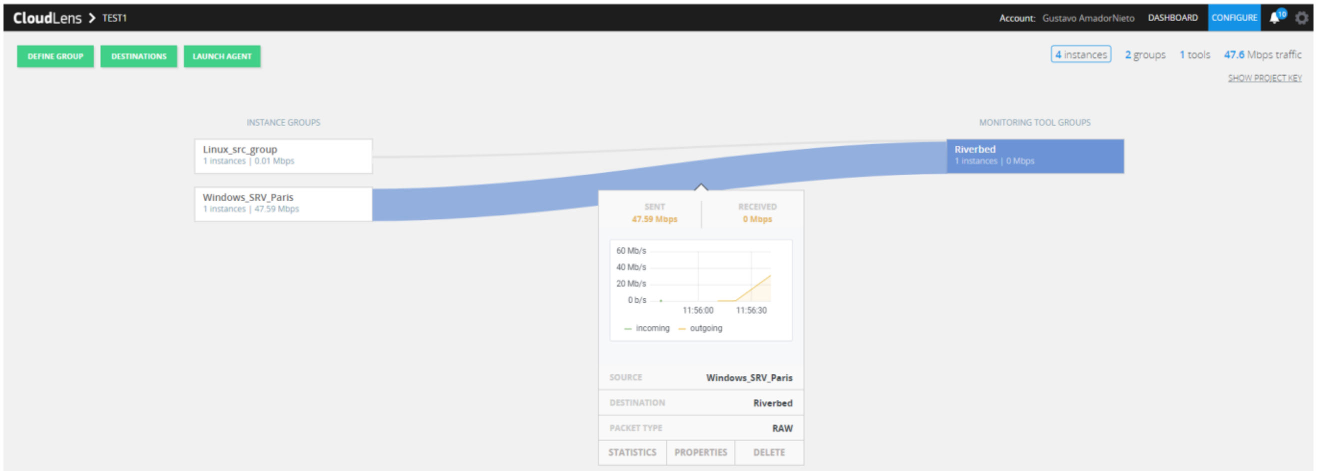
For example, from one of my Linux db instances I download the following image:



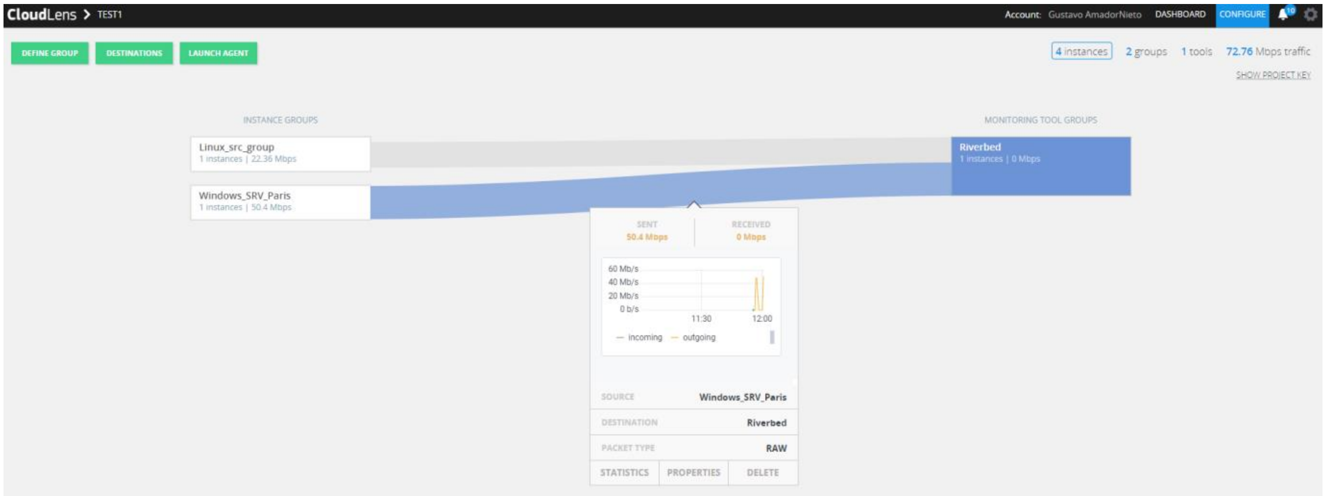
```
https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-1-1-115 ~]$ wget http://miroir.univ-paris13.fr/centos/8.5.2111/isos/aarch64/CentOS-8.5.2111-aarch64-boot.iso
--2022-01-04 10:58:46--  http://miroir.univ-paris13.fr/centos/8.5.2111/isos/aarch64/CentOS-8.5.2111-aarch64-boot.iso
Resolving miroir.univ-paris13.fr (miroir.univ-paris13.fr)... 81.194.43.155
Connecting to miroir.univ-paris13.fr (miroir.univ-paris13.fr)|81.194.43.155|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 745474048 (711M) [application/octet-stream]
Saving to: ‘CentOS-8.5.2111-aarch64-boot.iso’

36% [==============================================================>                                                ] 273,003,968 22.9MB/s  eta 19s
```

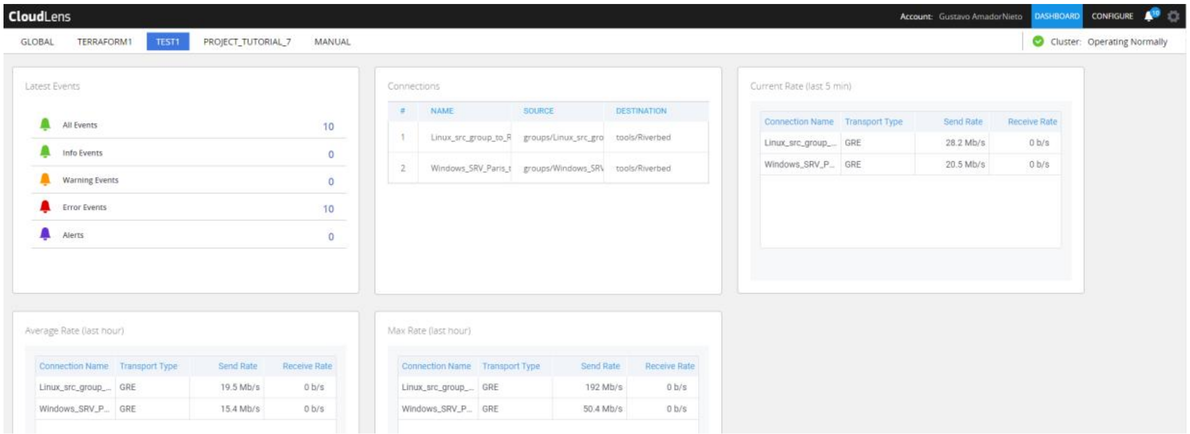
8.6. You can check the statistics of mirrored traffic in the Cloudlens Manager



SOURCE Windows_SRV_Paris
DESTINATION Riverbed
PACKET TYPE RAW



SOURCE Windows_SRV_Paris
DESTINATION Riverbed
PACKET TYPE RAW



Latest Events

All Events	10
Info Events	0
Warning Events	0
Error Events	10
Alerts	0

Connections

#	NAME	SOURCE	DESTINATION
1	Linux_src_group_to_R	groups/Linux_src_gro	tools/Riverbed
2	Windows_SRV_Paris_t	groups/Windows_SRV	tools/Riverbed

Current Rate (last 5 min)

Connection Name	Transport Type	Send Rate	Receive Rate
Linux_src_group_...	GRE	28.2 Mb/s	0 b/s
Windows_SRV_P...	GRE	20.5 Mb/s	0 b/s

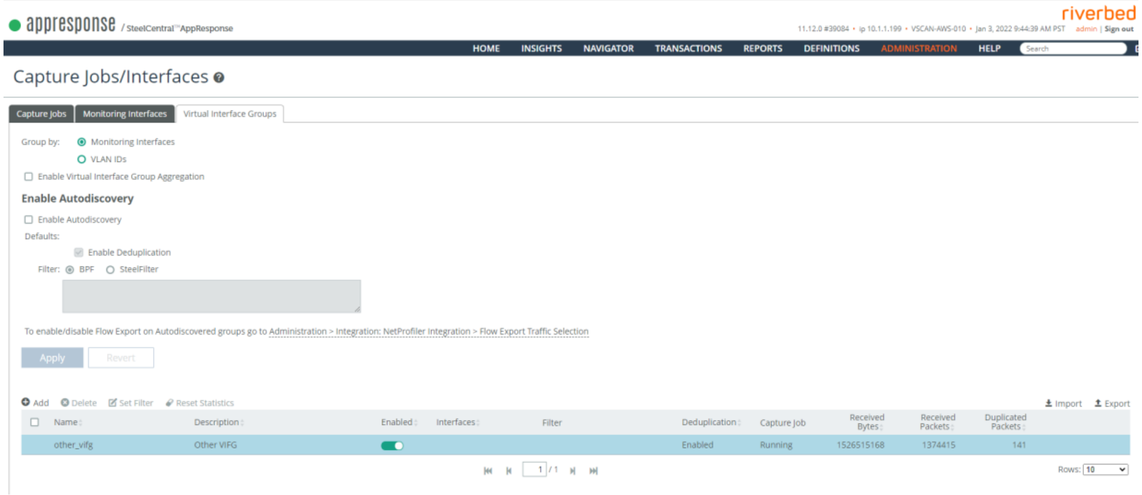
Average Rate (last hour)

Connection Name	Transport Type	Send Rate	Receive Rate
Linux_src_group_...	GRE	19.5 Mb/s	0 b/s
Windows_SRV_P...	GRE	15.4 Mb/s	0 b/s

Max Rate (last hour)

Connection Name	Transport Type	Send Rate	Receive Rate
Linux_src_group_...	GRE	192 Mb/s	0 b/s
Windows_SRV_P...	GRE	50.4 Mb/s	0 b/s

8.7. And check that traffic is received by Riverbed AppResponse



appresponse / SteelCentral™AppResponse
riverbed
11.12.0 #39084 • ip 10.1.1.199 • VSCAN-AWS-010 • Jan 3, 2022 9:44:39 AM PST admin | Sign out
HOME
INSIGHTS
NAVIGATOR
TRANSACTIONS
REPORTS
DEFINITIONS
ADMINISTRATION
HELP
Search

Capture Jobs/Interfaces

Group by: ● Monitoring Interfaces
○ VLAN IDs

☐ Enable Virtual Interface Group Aggregation

Enable Autodiscovery

☐ Enable Autodiscovery

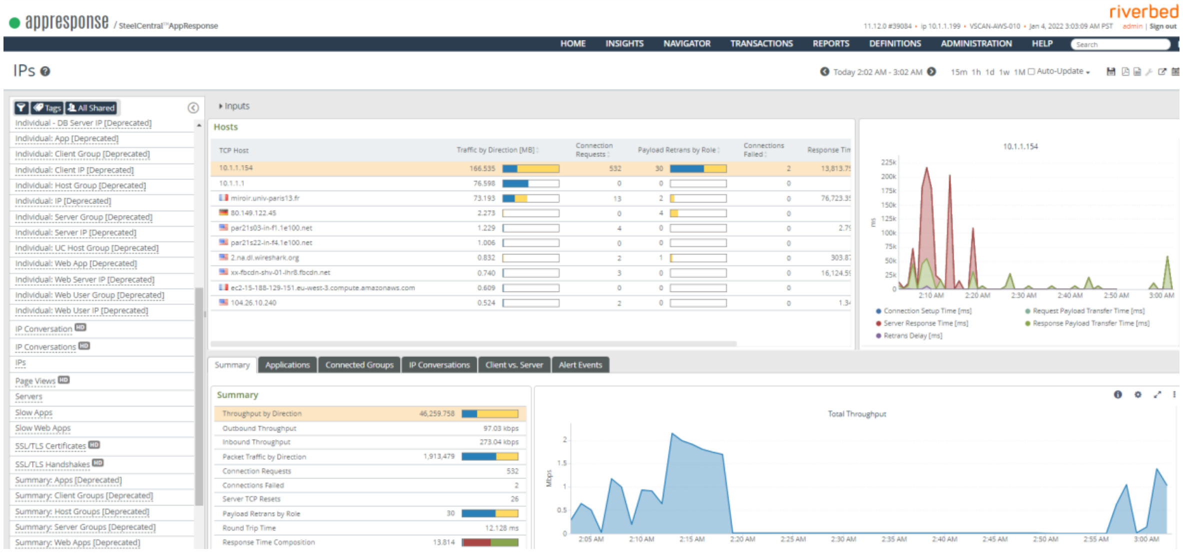
Defaults:

☑ Enable Deduplication

Filter: ● BPF ○ SteelFilter

To enable/disable Flow Export on Autodiscovered groups go to Administration > Integration: NetProfiler Integration > Flow Export Traffic Selection

Name	Description	Enabled	Interfaces	Filter	Deduplication	Capture Job	Received Bytes	Received Packets	Duplicated Packets
other_vifg	Other VIFG	●			Enabled	Running	1526515168	1374415	141



appresponse / SteelCentral™AppResponse
riverbed
11.12.0 #39084 • ip 10.1.1.199 • VSCAN-AWS-010 • Jan 4, 2022 3:03:09 AM PST admin | Sign out
HOME
INSIGHTS
NAVIGATOR
TRANSACTIONS
REPORTS
DEFINITIONS
ADMINISTRATION
HELP
Search

IPs

Today 2:02 AM - 3:02 AM
15m 1h 1d 1w 1M
☐ Auto-Update
Tags
All Shared
Individual - DB Server IP [Deprecated]
Individual: App [Deprecated]
Individual: Client Group [Deprecated]
Individual: Client IP [Deprecated]
Individual: Host Group [Deprecated]
Individual: IP [Deprecated]
Individual: Server Group [Deprecated]
Individual: Server IP [Deprecated]
Individual: UC Host Group [Deprecated]
Individual: Web App [Deprecated]
Individual: Web Server IP [Deprecated]
Individual: Web User Group [Deprecated]
Individual: Web User IP [Deprecated]
IP Conversation HD
IP Conversations HD
IPs
Page Views HD
Servers
Slow Apps
Slow Web Apps
SSL/TLS Certificates HD
SSL/TLS Handshakes HD
Summary: Apps [Deprecated]
Summary: Client Groups [Deprecated]
Summary: Host Groups [Deprecated]
Summary: Server Groups [Deprecated]
Summary: Web Apps [Deprecated]
Inputs

Hosts

TCP Host	Traffic by Direction [MB]	Connection Requests	Payload Retrans by Role	Connections Failed	Response Tim
10.1.1.154	166.535	532	30	2	13,813.7
10.1.1.1	76.598	0	0	0	
miroir.univ-paris13.fr	73.193	13	2	0	76,723.3
80.149.122.45	2.273	0	4	0	
par21s03-in-f1.1e100.net	1.229	4	0	0	2.7
par21s22-in-f4.1e100.net	1.006	0	0	0	
2.na.dl.wireshark.org	0.832	2	1	0	303.8
xx-fbcdn-shv-01-lhr8.fbcdn.net	0.740	3	0	0	16,124.5
ec2-15-188-129-151.eu-west-3.compute.amazonaws.com	0.609	0	0	0	
104.26.10.240	0.524	2	0	0	1.3

Summary

Throughput by Direction	46,259.758
Outbound Throughput	97.03 kbps
Inbound Throughput	273.04 kbps
Packet Traffic by Direction	1,913,479
Connection Requests	532
Connections Failed	2
Server TCP Resets	26
Payload Retrans by Role	30
Round Trip Time	12.128 ms
Response Time Composition	13.814

9. Firewall ports to open for Cloudlens

Note: *default Security Group 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 :

- TCP 22 ** for SSH if Linux instance
- TCP 3389 ** for RDP if Windows instance
- HTTPS 443 open from IP address of CloudLens Manager

CloudLens Manager:

- HTTPS 443 **

Riverbed AppResponse Instance:

- GRE Protocol 47 *
- ICMP Protocol * required with Cloudlens 6.1.0 ***
- TCP 22 **
- TCP 443 **

* Leave open all IP of Traffic Sources Addreses

** Specify IP addresses of customer administrators

*** Linux Source Instances don't require ICMP protocol allowed in AppResponse if the "out_interface" parameter is specified when invoking the Docker container.

WHERE TO GET HELP

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