

New Relic Integration

About The Integration

Gigamon GigaVUE Cloud Suite enables collection of network traffic from every instance across the entire cloud solution. Customers can then choose to either centralize the traffic for network metadata generation for New Relic or choose to do so in a distributed fashion.

This integration provides a way to collect metadata of over 7,000 network traffic-related attributes and export that to New Relic dashboard for holistic overview of cloud environment, and a much deeper level of security-related inspection.

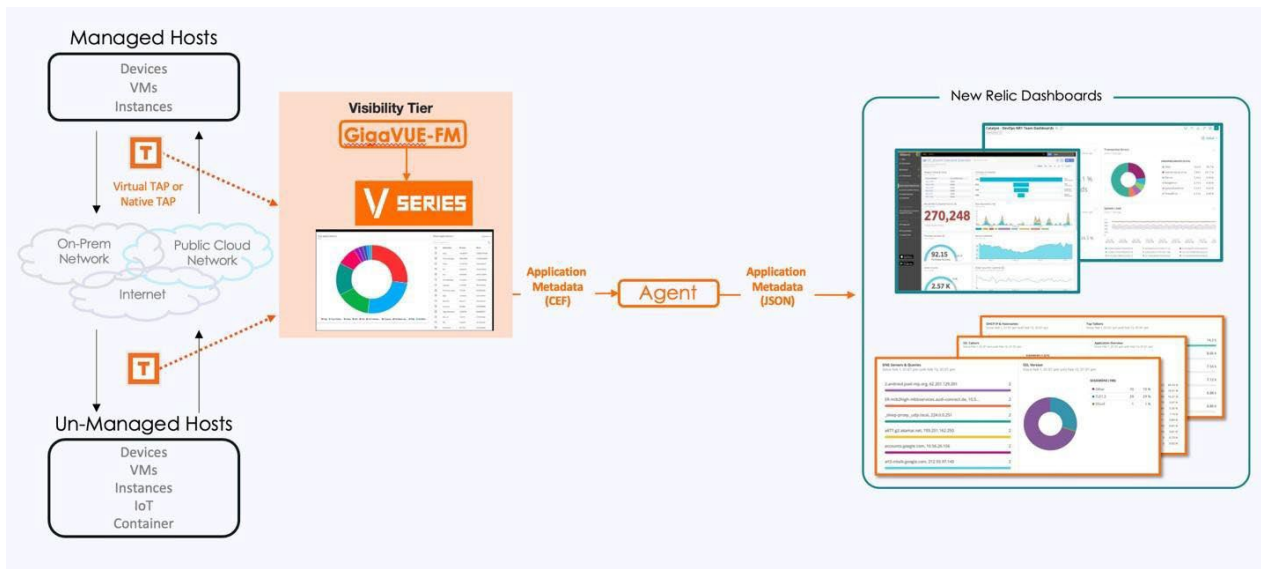


Figure 1. GigaVUE Cloud Suite: Capture all traffic and export metadata of interest to New Relic.

Components Involved

- Gigamon GigaVUE Cloud Suite
- Gigamon Application Metadata Intelligence (AMI)
- Gigamon Application Metadata Exporter (AMX)
- New Relic account

How to configure AMI

1. Go to Traffic -> Solutions -> Application Intelligence
2. Click on Create New -> Select the Environment

Create Application Intelligence Session

Basic Info

Name _____ Description (optional) _____ Environment **Virtual**

0 / 128

Environment Info

Environment Name _____ Connection Name _____

Configurations

Export Interval **60** secs Management Interface

Must be between 60-900

3. Select the source from where the traffic has to be tapped.

Source Traffic

Source Selector Tunnel Specification Raw Endpoint

Splunk-test x

Expand All Collapse All

Name	Filter Id	Filters	Operator	Values	
▼ Splunk-test	1	VmName_Src	startswith	ubuntu	⊕

4. Select Application Metadata

- Tool IP Address should be AMX ingress IP Address.
- L4 Src & Dest port.
- Using Advanced settings, you can also select any specific applications and its attribute to be exported.

Application Filtering **Deduplication** **Application Metadata**

Destination Traffic

Choose the existing tools to receive application-specific traffic or add new tool.

▼ EXPORTER 1 Save

Tool Name*	Tool IP Address*	L4 Source Port*	L4 Destination Port*
ELK-tool_vmwareEsxi	172.16.102.151	Template	23384
			514

Application List App Editor

> 11 Applications

FORMAT	RECORD/TEMPLATE TYPE	ACTIVE TIMEOUT*	INACTIVE TIMEOUT*
CEF	Cohesive	60 SECS	15 SECS

[Advanced Settings](#) Save

5. Click Save and then Deploy.

How to configure AMX and integrate with New Relic

How to Bring up AMX from FM

1. Create Monitoring Domain:

Inventory > Virtual > Select the Environment > Create Monitoring Domain

Monitoring Domain	Connections	Name	Management IP	Type	Version	
ELK-Test						
		ELKTest				
		VSeries-OGW10-115-81-	10.115.86.55	V Series Node	6.2.00	

2. Create Monitoring Session:

Traffic > Orchestrated Flows (select the right environment) > Create Monitoring Session

- Create REP from AMI to AMX(OGW) and AMX(OGW) to New Relic (REP-Raw End Point which is an IP Address)
- Ingress to AMX(OGW) will be from AMI
- Egress from AMX(OGW) should be pointing to New Relic IP Address
- **As shown in below snapshot select the cloud tool as New Relic with the right Account ID and API Key.**

The screenshot displays the configuration for an AMI Exporter named 'ogw'. The configuration is split into two tabs: 'Details' and 'Thresholds'. The 'Details' tab is active, showing the following settings:

- Application:** AMI Exporter
- Alias*:** ogw
- Cloud Tool Ingestor Port:** 514
- Cloud Tool Exports:**
 - ogwforNewRelic:**
 - Alias*:** ogwforNewRelic
 - Cloud Tool*:** New Relic
 - Account Id*:** Enter ID used with New Relic account
 - API Key*:** Enter API key
- MORE OPTIONS:**
 - Enable Export:**
 - Format:** JSON
 - Zip:**
 - Interval (sec):** 30
 - Parallel Writers:** 4
 - Export Retries:** 4
 - Max Entries:** 1000
 - Labels:** Add

A small dialog box is open at the bottom right, showing a 'Key' field with the value 'eventType' and a 'Value' field with the placeholder 'Enter value...'.

3. Deploy the Solution.

raw1 > Interface connecting AMI

raw2 > Interface connecting New Relic

Select nodes to deploy the Monitoring Session: forELKOGW

<input type="checkbox"/>	V Series Node Name	Status
<input checked="" type="checkbox"/>	VSeries-OGW10-115-81-119-toELK	OK

Go to page: 1 of 1 Total Records: 1

▼ VSeries-OGW10-115-81-119-toELK

raw-1

raw-2

Deploy Cancel

How to create an API Key From New Relic page

1. Reference Link: To Generate API Key
2. Click User ID > API Keys > Create a Key

The screenshot shows the New Relic Administration interface. On the left is a navigation sidebar with 'API Keys' highlighted. The main content area is titled 'Administration' and contains a table of API keys. A user menu is open over the table, with 'API Keys' selected. The table lists various keys with columns for Account, Type, Name, Value, Notes, and User.

Accou...	Type	Name	Value	Notes	User
Accou...	INGEST - LICENSE	engsol...	6a6d1683*****	This is
Accou...	USER	User K...	NRAK-GYV*****		...
Accou...	INGEST - LICENSE	OA_NR...	89718352*****		...
Accou...	INGEST - LICENSE	Syslog...	e4284b50*****	Autom...	...
Accou...	INGEST - LICENSE	Syslog...	27e99402*****	Autom...	...
Accou...	INGEST - LICENSE	Syslog...	cc43e106*****	Autom...	...
Accou...	INGEST - LICENSE	Syslog...	9468d7ed*****	Autom...	...

Create an API key

Ingest keys are for getting data into New Relic:

- **License** keys for agent configuration and metric, event, log and trace APIs
- **Browser** keys for browser applications
- **Mobile** keys for mobile applications. To learn how to manage mobile keys, [see our docs](#) ↗

User keys are for querying data and managing configurations (Alerts, Synthetics, dashboards, etc.)
To learn more about API keys, [see our docs](#) ↗

Account

Account: 1578679 - Demo ▼

Key type

Ingest - License ▼

Name

Gigamon AMI Integration

Notes

What do you want people to know about this key?

Figure 2. Details about types of Keys and account information

Once GigaVUE Cloud Suite is deployed in the environment it provides New Relic the ability to see all available applications communicating across the environment and collect metadata from that traffic.

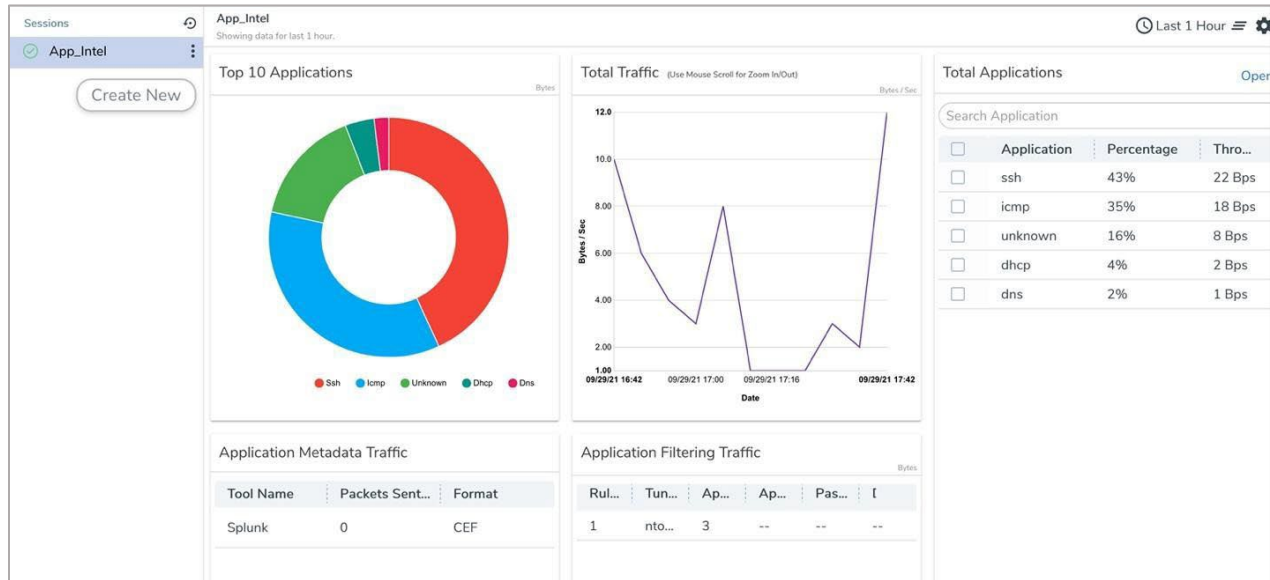


Figure 3. Screenshot of demo data in GigaVUE-FM.
 Note: Production environments will display hundreds of applications.

Different metadata elements can be selected based on an application, or a family of applications, and exported to Gigamon AMI Agent.

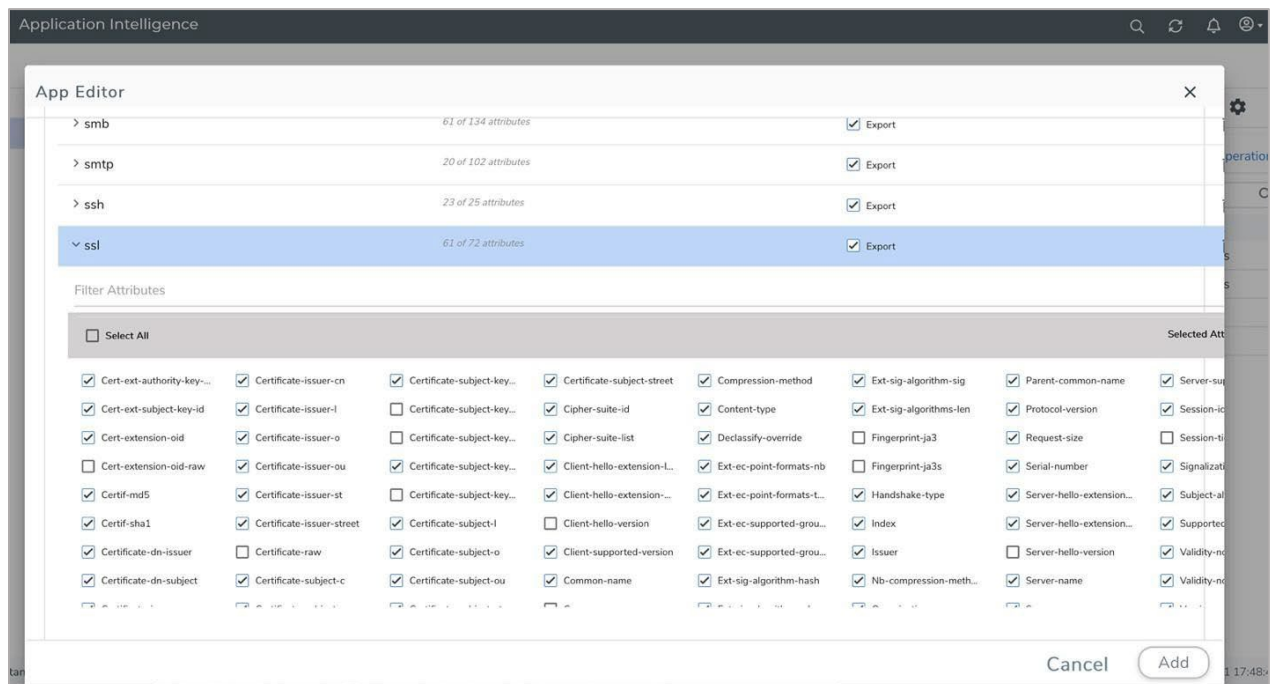


Figure 4. The example shows SSL attributes available to be exported.

Gigamon AMX collects metadata elements from Gigamon Cloud Suite and forwards them to New Relic Dashboard, where reporting and visualization can be performed in any number of ways. Here is a snapshot from New Relic dashboard page.

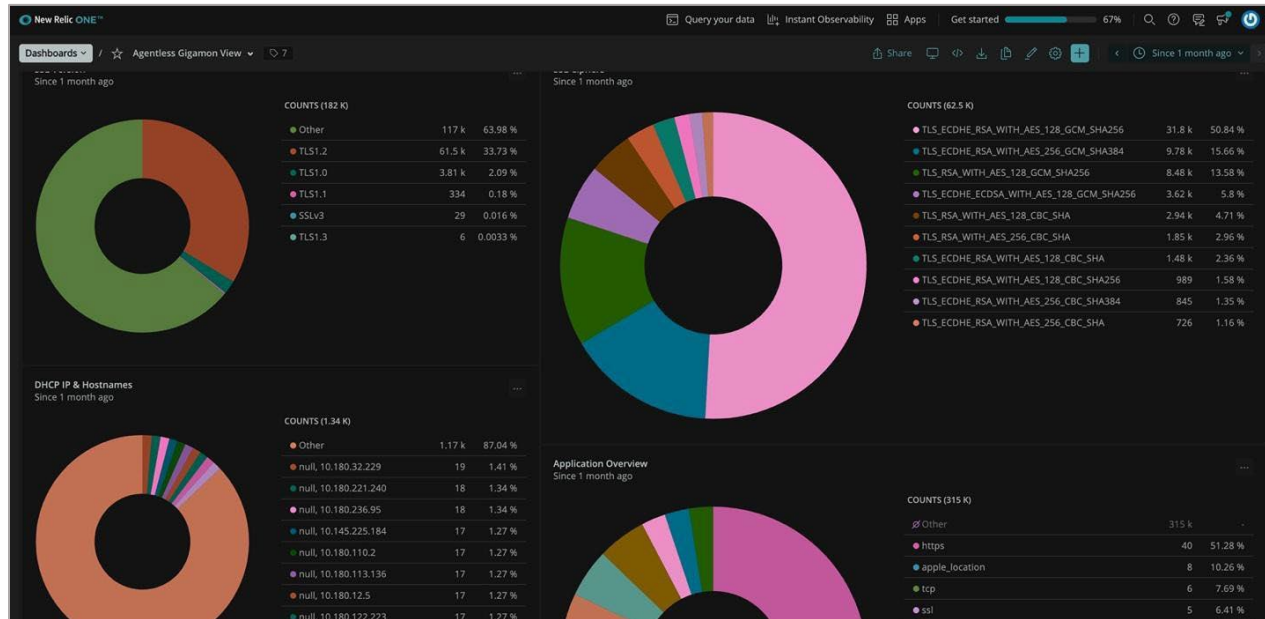


Figure 5. A sample dashboard created using AMI attributes from Gigamon.

Some of the sample queries are shown here used to build this dashboard, these can get as granular as needed.

```
FROM Gigamon SELECT count(*) FACET version where event_type ='ssl' FROM Gigamon
SELECT count(*) FACET cipher
FROM Gigamon SELECT count(*) FACET hostname,src_ip where event_type ='dhcp' FROM Gigamon
SELECT count(*) FACET application
```

Note: This integration will become more automated in the future where you will only need to provide the API key and endpoint to export data to New Relic.

To try this integration in your environment please reach out to tme@gigamon.com. If you would like to learn more about GigaVUE Cloud Suite, contact us at gigamon.com/contact-sales.