

Gigamon Dynatrace Integration

Referring to Figure 1 below, Gigamon leverages deep packet inspection to identify over 5,000 common and proprietary applications. Relevant application, application family, protocols, and attributes can be filtered within Gigamon and streamed to Dynatrace’s Log Management and Analytics solution.

Powered by Dynatrace’s purpose-built observability data lake house Grail, users can analyze Gigamon network data in context of traces, user sessions, and topology with intuitive visual diagnostics and powerful queries.

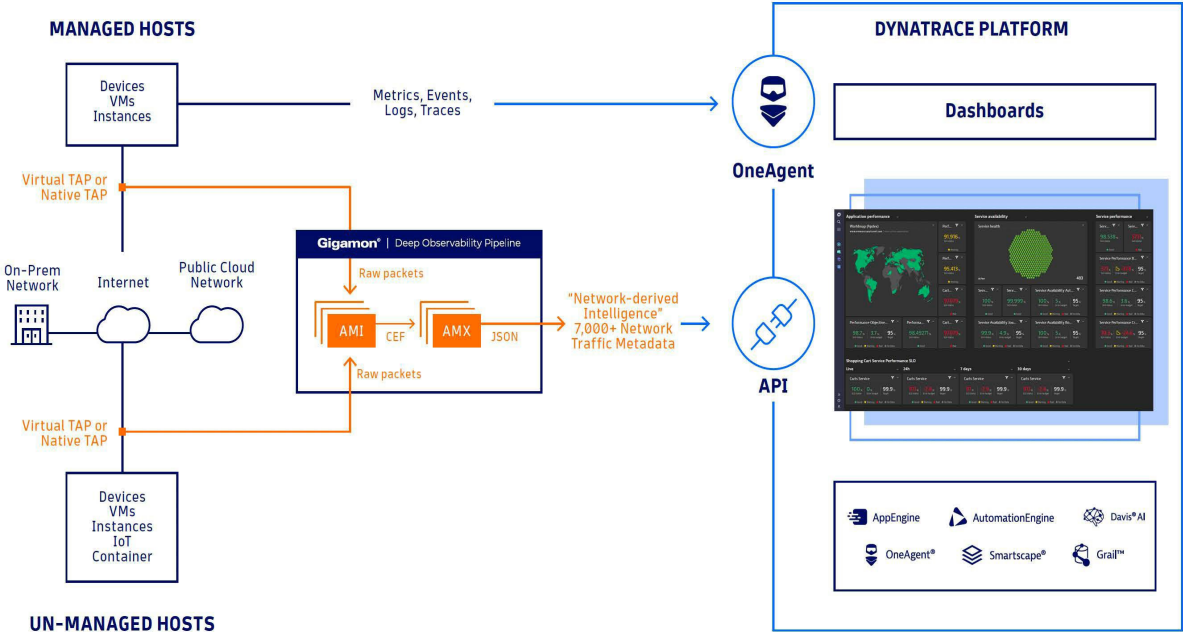


Figure 1. Gigamon accesses network traffic from all sources, extracts network-derived attributes, and sends this traffic as logs to Dynatrace.

Deployment Model

- Dynatrace
 - SaaS enabled with Grail
 - API token with log ingest scope for use by Gigamon Application Metadata Exporter
- Gigamon Cloud
 - Gigamon Cloud Suite
 - Gigamon Application Metadata Intelligence (AMI)
 - Gigamon Application Metadata Exporter (AMX)
- Gigamon On-Prem / Private Cloud
 - Physical appliance or vSeries appliance (VMware, Nutanix, etc.)
 - Gigamon Fabric manager
 - Gigamon Application Metadata Exporter (AMX)

To more details or questions about this integration please reach out sales@gigamon.com.
For technical questions, reach out to tme@gigamon.com.

Dynatrace Setup

STEP 1 of 1: Create Dynatrace API Access Token

The Gigamon Application Exporter uses a [Dynatrace Log Monitoring ingest logs API](#) and requires a [Dynatrace API access token](#).

To generate an access token:

1. In Dynatrace, open the **Access Token** page
1. Select Generate new token.
2. Enter a name for your token. *NOTE: Dynatrace doesn't enforce unique token names. You can create multiple tokens with the same name. Be sure to provide a meaningful name for each token you generate. Proper naming helps you to efficiently manage your tokens and perhaps delete them when they're no longer needed.*
3. Select the required scope of: **Ingest logs(logs.ingest)**
4. Select Generate.
5. Copy the generated token to the clipboard. Store the token in your password manager for future use.
NOTE: You can only access your token once upon creation. You can't reveal it afterwards.

Below is an example view of the Dynatrace generate access token page.

Access tokens > Generate access token

Generate access token

Give your new token a name and select only those scopes that you need. To generate an access token for PaaS or a Dynatrace module, select a token template. For details, go to [Token permissions documentation](#).

Token name
Gigamon Application Metadata Exporter

Expiration date
Optional, select expiration date

Template
None

Select scopes from the table below

ingest logs

Scope name	Scope type	Permission summary
<input checked="" type="checkbox"/> Ingest logs logs.ingest	API v2	Grants access to the POST ingest logs request of the Log Monitoring API v2.

Selected scopes

Ingest logs x Clear all

Gigamon Setup

STEP 1 of 3: Configure Application Metadata Intelligence (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
<input type="text"/>	<input type="text"/>	Virtual

Environment Info

Environment Name	Connection Name
<input type="text"/>	<input type="text"/>

Configurations

Export Interval	<input checked="" type="checkbox"/> Management Interface
<input type="text" value="60"/> secs	

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

Name	Filter Id	Filters	Operator	Values	Expand All Collapse All
▼ test_x	1	VmName_Src	startswith	ubuntu	⊕

4. Select Application Metadata

- Tool Ip Address should be AMX ingress IP Address.
- L4 Src & Dest port.

Application Filtering Deduplication **Application Metadata**

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

EXPORTER 1

Tool Name* tool_vmwareEsxi Tool IP Address* 172.16.102.151 Template L4 Source Port* 23384 L4 Destination Port* 514 Save...

Application List App Editor

> 11 Applications

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

> Advanced Settings

Save...

- Using Advanced settings, select any specific applications and its attribute to be exported. The example below shows SSL attributes available to be exported.

Application Intelligence

App Editor

- > smb 61 of 134 attributes Export
- > smtp 20 of 102 attributes Export
- > ssh 23 of 26 attributes Export
- > **ssl 61 of 72 attributes Export**

Filter Attributes

Select All Selected Attributes

<input checked="" type="checkbox"/> Cert-ext-authority-key-...	<input checked="" type="checkbox"/> Certificate-issuer-cn	<input checked="" type="checkbox"/> Certificate-subject-key...	<input checked="" type="checkbox"/> Certificate-subject-street	<input checked="" type="checkbox"/> Compression-method	<input checked="" type="checkbox"/> Ext-sig-algorithm-sig	<input checked="" type="checkbox"/> Parent-common-name	<input checked="" type="checkbox"/> Server-su...
<input checked="" type="checkbox"/> Cert-ext-subject-key-id	<input checked="" type="checkbox"/> Certificate-issuer-l	<input type="checkbox"/> Certificate-subject-key...	<input checked="" type="checkbox"/> Cipher-suite-id	<input checked="" type="checkbox"/> Content-type	<input checked="" type="checkbox"/> Ext-sig-algorithms-len	<input checked="" type="checkbox"/> Protocol-version	<input checked="" type="checkbox"/> Session-ic...
<input checked="" type="checkbox"/> Cert-extension-oid	<input checked="" type="checkbox"/> Certificate-issuer-o	<input type="checkbox"/> Certificate-subject-key...	<input checked="" type="checkbox"/> Cipher-suite-list	<input checked="" type="checkbox"/> Declassify-override	<input type="checkbox"/> Fingerprint-ja3	<input checked="" type="checkbox"/> Request-size	<input type="checkbox"/> Session-ti...
<input checked="" type="checkbox"/> Cert-extension-oid-raw	<input checked="" type="checkbox"/> Certificate-issuer-ou	<input checked="" type="checkbox"/> Certificate-subject-key...	<input checked="" type="checkbox"/> Client-hello-extension-L...	<input checked="" type="checkbox"/> Ext-ec-point-formats-nb	<input type="checkbox"/> Fingerprint-ja3s	<input checked="" type="checkbox"/> Serial-number	<input checked="" type="checkbox"/> Signalizat...
<input checked="" type="checkbox"/> Certif-md5	<input checked="" type="checkbox"/> Certificate-issuer-st	<input type="checkbox"/> Certificate-subject-key...	<input checked="" type="checkbox"/> Client-hello-extension...	<input checked="" type="checkbox"/> Ext-ec-point-formats-L...	<input checked="" type="checkbox"/> Handshake-type	<input checked="" type="checkbox"/> Server-hello-extension...	<input checked="" type="checkbox"/> Subject-al...
<input checked="" type="checkbox"/> Certif-sha1	<input checked="" type="checkbox"/> Certificate-issuer-street	<input checked="" type="checkbox"/> Certificate-subject-l	<input type="checkbox"/> Client-hello-version	<input checked="" type="checkbox"/> Ext-ec-supported-grou...	<input checked="" type="checkbox"/> Index	<input checked="" type="checkbox"/> Server-hello-extension...	<input checked="" type="checkbox"/> Supported...
<input checked="" type="checkbox"/> Certificate-dn-issuer	<input type="checkbox"/> Certificate-raw	<input checked="" type="checkbox"/> Certificate-subject-o	<input checked="" type="checkbox"/> Client-supported-version	<input checked="" type="checkbox"/> Ext-ec-supported-grou...	<input checked="" type="checkbox"/> Issuer	<input type="checkbox"/> Server-hello-version	<input checked="" type="checkbox"/> Validity-n...
<input checked="" type="checkbox"/> Certificate-dn-subject	<input checked="" type="checkbox"/> Certificate-subject-c	<input checked="" type="checkbox"/> Certificate-subject-ou	<input checked="" type="checkbox"/> Common-name	<input checked="" type="checkbox"/> Ext-sig-algorithm-haah	<input checked="" type="checkbox"/> Nb-compression-meth...	<input checked="" type="checkbox"/> Server-name	<input checked="" type="checkbox"/> Validity-n...

Cancel Add

5. Click Save and then Deploy

STEP 2 of 3: Configure Gigamon Application Metadata Exporter (AMX) to integrate with Dynatrace.

To bring up AMX from FM (Fabric Manager)

1. Create Monitoring Domain:

Inventory -> Virtual -> Select the Environment -> Create Monitoring Domain

Monitoring Domain	Connections	Name	Management IP	Type	Version	
Test						
		Test				
		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 Dynatrace (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 Dynatrace IP Address
- **As shown in below snapshot pick Dynatrace tool from cloud tool drop down**
- **Enter the Dynatrace Access Token**

The screenshot displays the configuration for an AMI Exporter named 'ogw'. On the left, a network diagram shows two 'RAW' endpoints (labeled 'raw-1' and 'raw-2') connected to a central 'ogw' endpoint. On the right, the configuration details are shown:

- Application: AMI Exporter
- Alias*: ogw
- Cloud Tool Ingestor Port: 514
- Cloud Tool Exports: dynatrace
- Alias*: dynatrace
- Cloud Tool*: Dyna Trace
- API Key*: dt0c01.MCDF3HXF5OUQYCGYUE3YV2DLV5462V2B
- MORE OPTIONS:
 - Enable Export:
 - Format: JSON
 - Zip:
 - Interval (sec): 30
 - Parallel Writers: 4
 - Export Retries: 10
 - Max Entries: 1000

3. Deploy the Solution.

- raw1 -> Interface connecting AMI
- raw2 -> Interface connecting Dynatrace

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

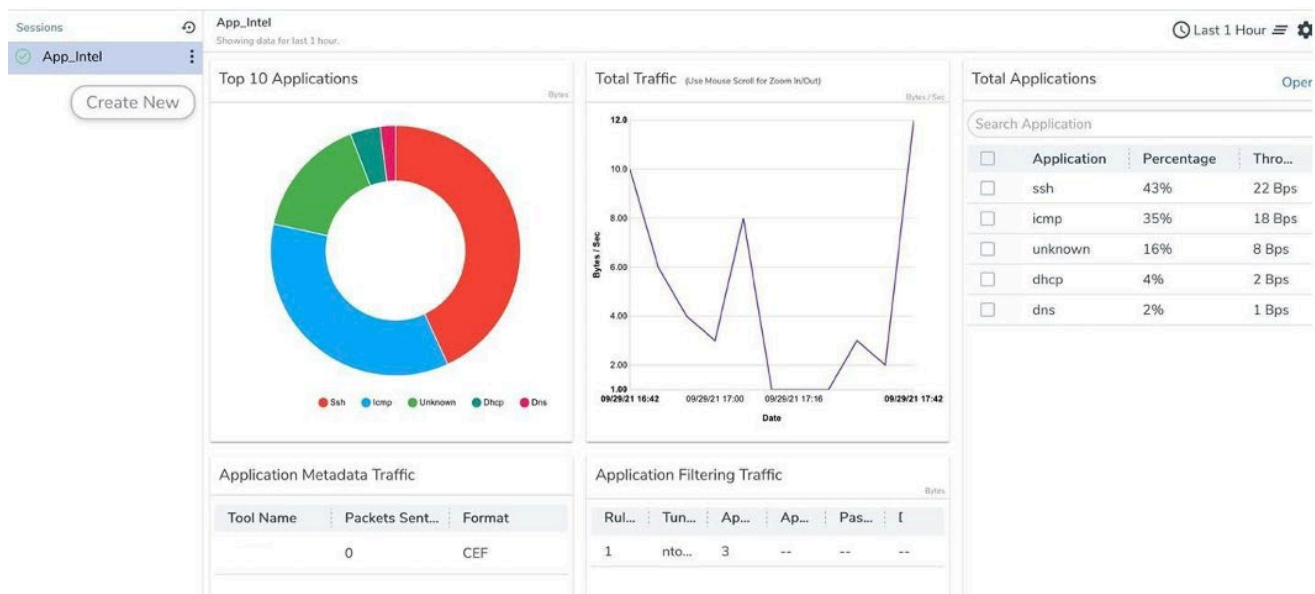
▼ VSeries-OGW10-115-81-119-toELK

raw-1	<input type="text" value="Select an interface"/>
raw-2	<input type="text" value="Select an interface"/>

STEP 3 of 3: Verify data is being sent to Dynatrace

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

Below the picture below snapshot from FM. Note that production environments will display hundreds of applications.



To verify log ingest within Dynatrace:

1. In Dynatrace, open the **Logs** page
2. Switch to **Advanced Mode**
3. Execute the following Dynatrace Query Language (DQL) statement to view ingested logs for the last 24 hours

```
fetch logs, from: - 24h
| filter vendor == "Gigamon"
| summarize count(), by:{Hour=formatTimestamp(bin(timestamp, 1h), format:"HH")}, alias: logCount
| fields Hour, logCount
| sort Hour
```


Example output

Search results | Visualization type: Table Single value Bar

Hour	logCount
00	10495
01	1312
02	20558
03	4751
04	5207
05	346

4. Execute the following DQL to view ingested logs broken out by **app_name** attribute for the last day.

```
fetch logs, from:now()-1d
| filter vendor == "Gigamon"
| summarize count(), by:{app_name}, alias: logCount
| sort logCount desc
```

Example output

Search results | Visualization type: Table Single value Bar

app_name	logCount
Classification-unknown	30726
http	24898
snmp	19152
modbus	16854
dns	15733

See the Dynatrace documentation for more details:

- Dynatrace Query Language
 - <https://www.dynatrace.com/support/help/observe-and-explore/query-data/dynatrace-query-language>
- Dynatrace dashboards
 - <https://www.dynatrace.com/support/help/observe-and-explore/dashboards>
- Access tokens
 - <https://www.dynatrace.com/support/help/manage/access-control/access-tokens>