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.

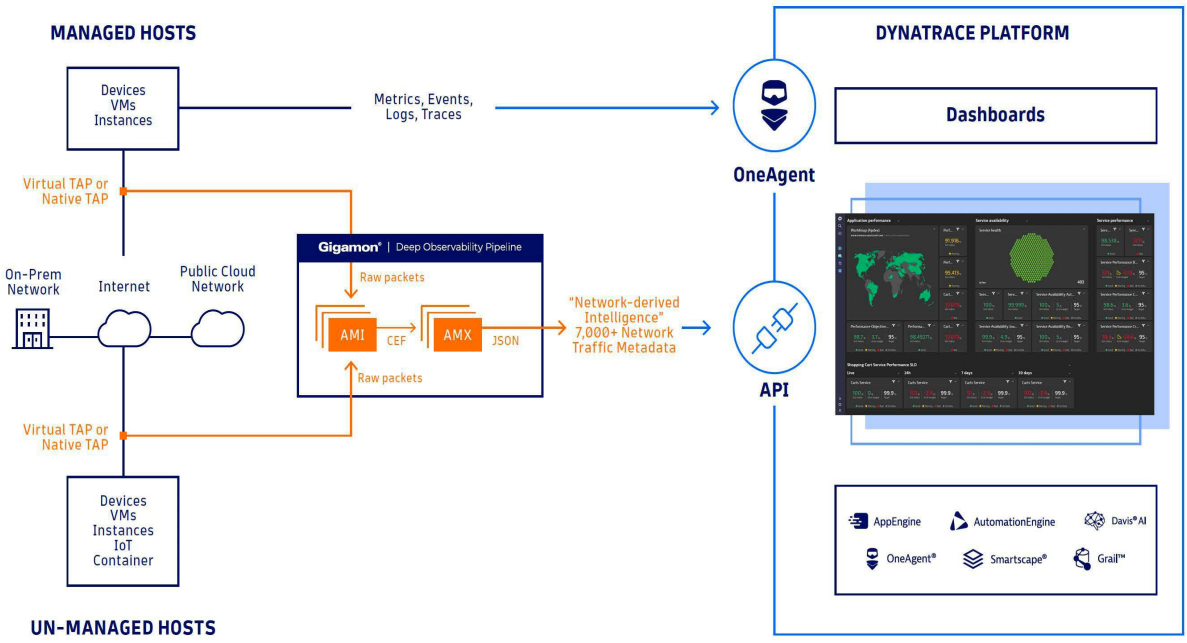


Figure 1. Gigamon accesses network traffic from all sources, extracts network-derived attributes, and sends this traffic as logs to Dynatrace.

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

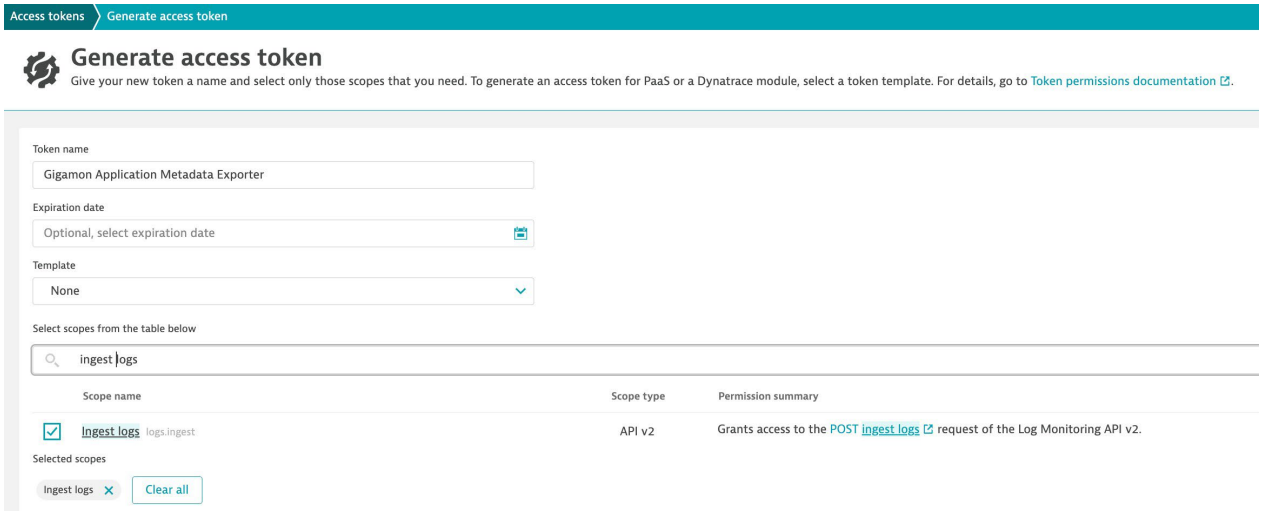
STEP 1 of 1: Create Dynatrace API Access Token

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.

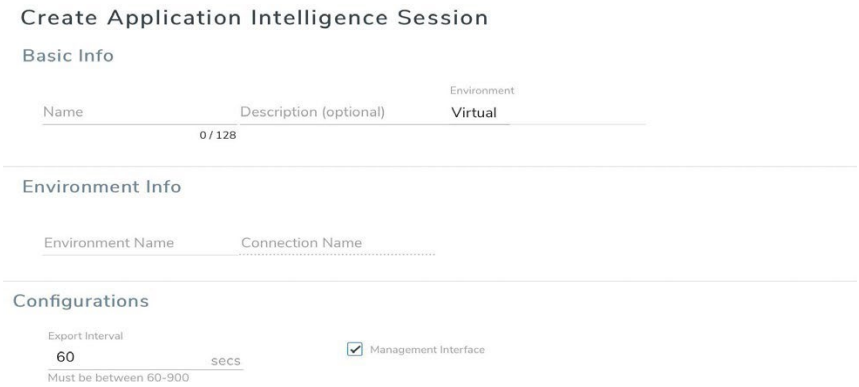
Below is an example view of the Dynatrace generate access token page.



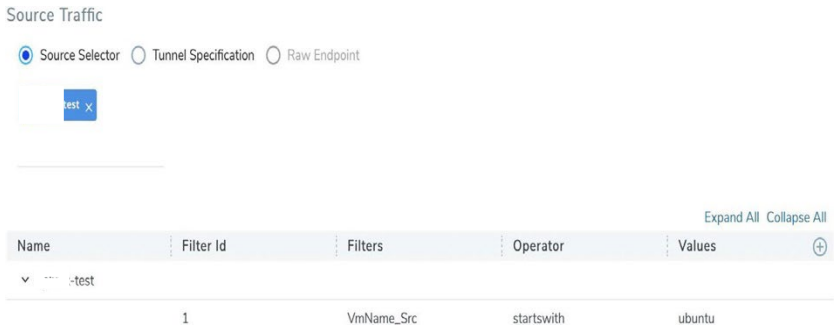
Gigamon Setup

STEP 1 of 3: Configure Application Metadata Intelligence (AMI)

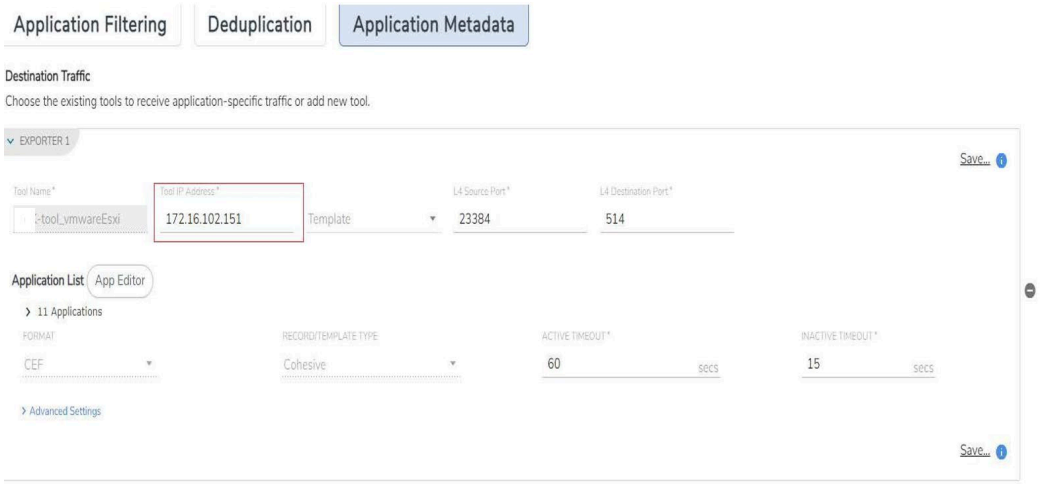
1. Go to Traffic -> Solutions -> Application Intelligence
2. Click on Create New -> Select the Environment



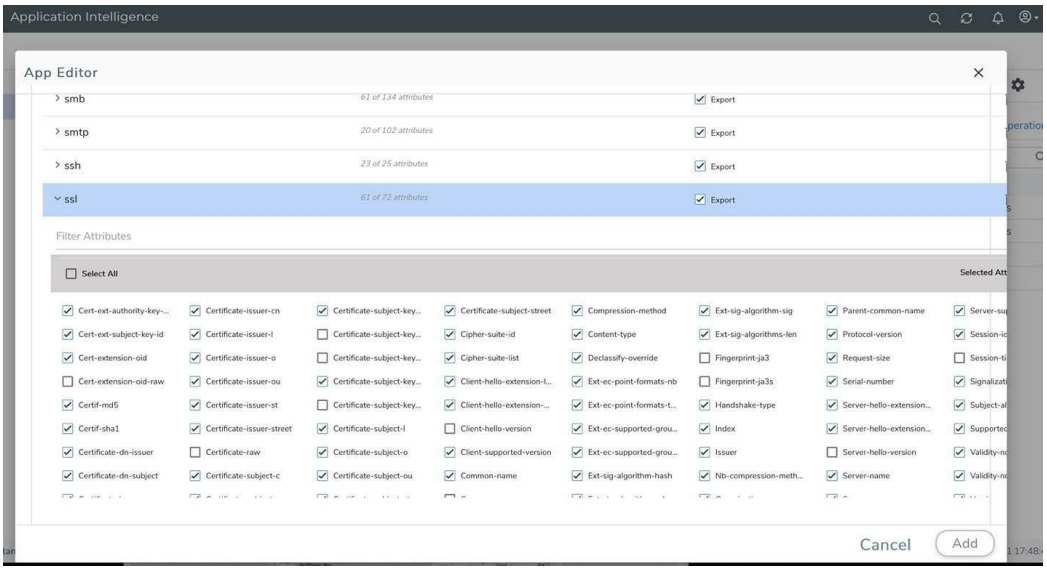
3. Select the source from where the traffic has to be tapped.



4. Select Application Metadata
   - Tool Ip Address should be AMX ingress IP Address.
   - L4 Src & Dest port.



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



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)

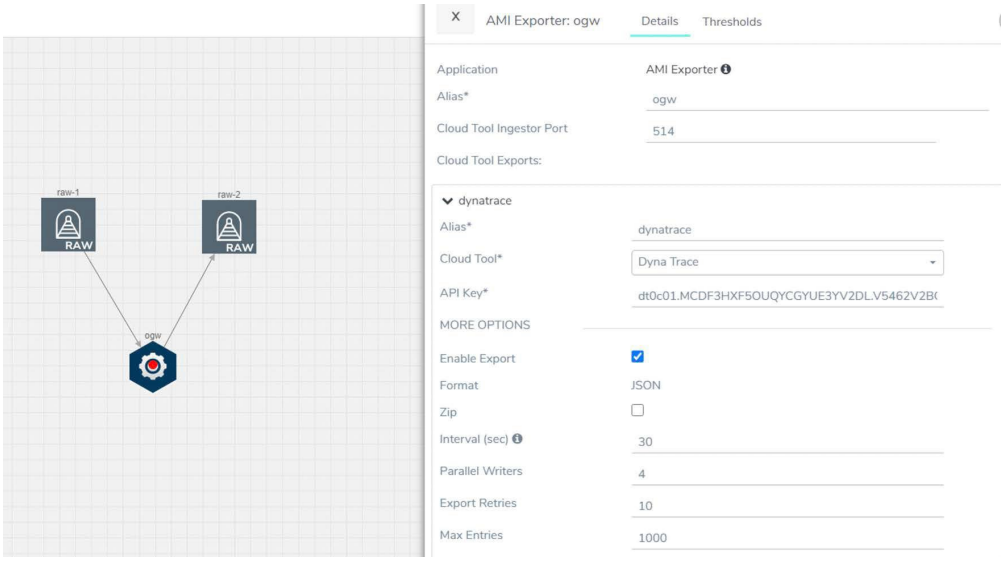
1. Create Monitoring Domain:

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

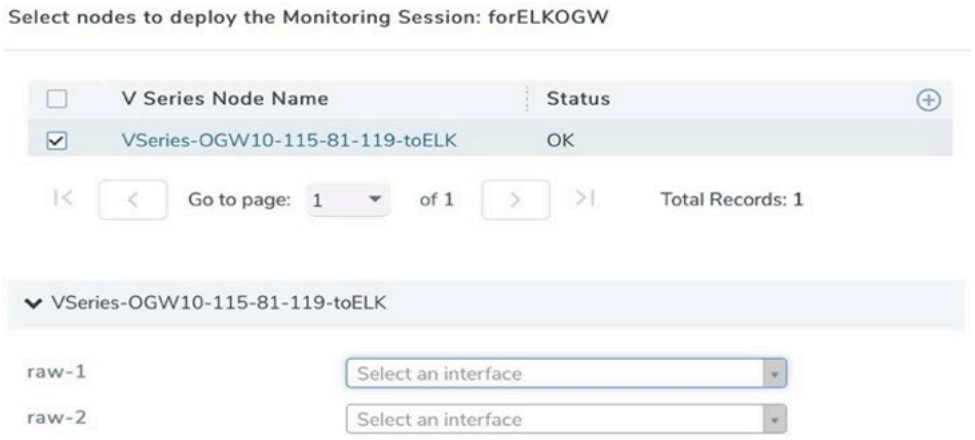
2. Create Monitoring Session:

   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**



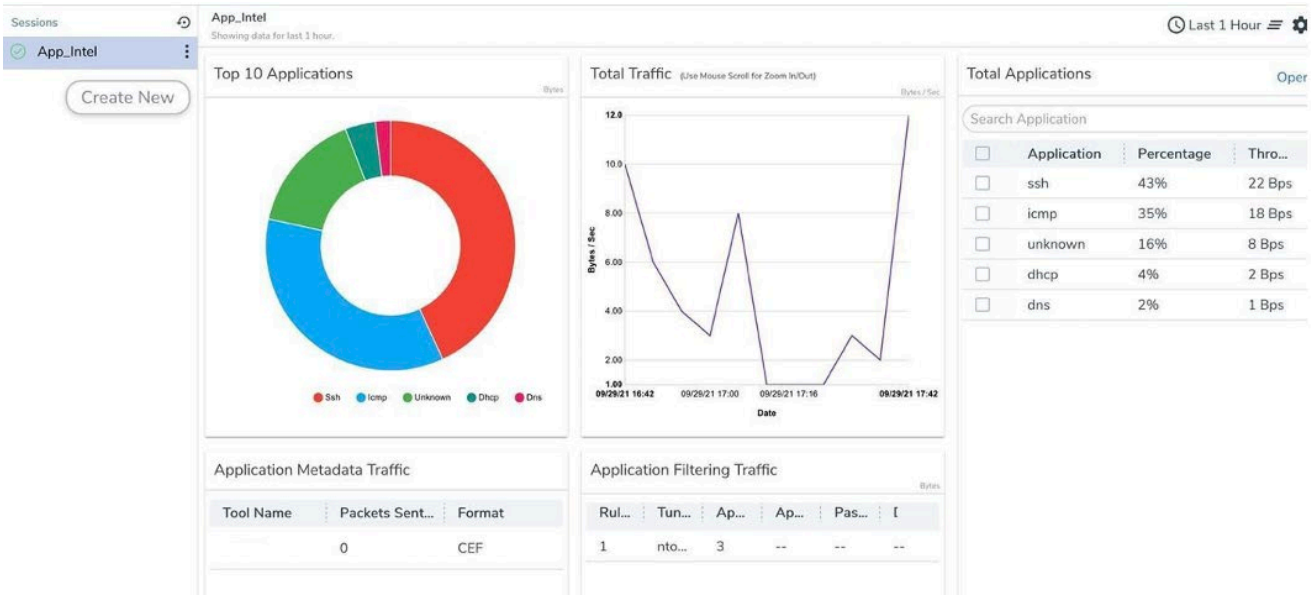
3. Deploy the Solution.
   - raw1 -> Interface connecting AMI
   - raw2 -> Interface connecting Dynatrace



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

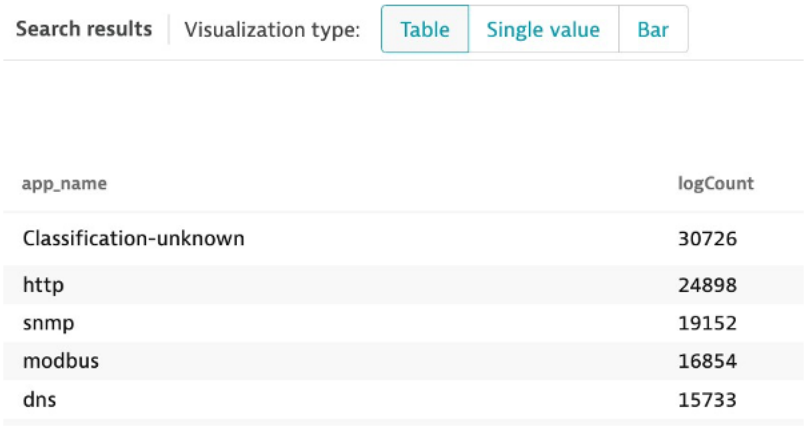
```
fetch logs, from: - 24h
| filter vendor == "Gigamon"
| summarize count(), by:{Hour=formatTimestamp(bin(timestamp, 1h), format:"HH")}, alias: logCount
| fields Hour, logCount
| sort Hour
```

Example output

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



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