GigaVUE V Series Applications Guide

GigaVUE Cloud Suite

Product Version: 6.5
Document Version: 1.0
Last Updated: Friday, February 9, 2024

(See Change Notes for document updates.)

Change Notes

When a document is updated, the document version number on the cover page will indicate a new version and will provide a link to this Change Notes table, which will describe the updates.

Product Version	Document Version	Date Updated	Change Notes
6.5.00	1.0	12/11/2023	The original release of this document with 6.5.00 GA.

Contents

GigaVUE V Series Application Guide

This guide describes the list of supported V Series Applications and how to add the V Series Applications to monitoring session and configure it.

- Supported V Series Applications
- Application Intelligence
- De-duplication
- GENEVE De-encapsulation
- Header Stripping
- Load Balancing
- Masking
- SSL Decrypt
- PCAPng Application
- 5G-Service Based Interface Application
- Slicing

Overview of GigaVUE V Series Applications

GigaVUE V Series Node is a virtual machine running in the customer's infrastructure which processes and distributes network traffic. It plays the same role as an H Series appliance in a physical deployment, running many of the same GigaSMART applications and feeding data to tools in a similar manner. Because GigaVUE V Series nodes reside in a virtual environment, inbound and outbound traffic is tunneled (because there are no physical device ports).

GigaVUE V Series Applications run on GigaVUE V Series Nodes. All these applications use Volume- Based License. Refer to Volume-Based License for more detailed information.

You can use these applications to optimize the traffic sent from your instances to the monitoring tools. GigaVUE Cloud Suite supports the following applications:

- Application Intelligence
- De-duplication
- GENEVE De-encapsulation
- Header Stripping
- Load Balancing
- Masking
- SSL Decrypt
- PCAPng Application
- 5G-Service Based Interface Application
- Slicing

Refer to the Supported V Series Applications table for more information on the platforms in which these applications will be supported.

Supported V Series Applications

GigaSMART Operation	GigaVUE Cloud Suite for AWS	GigaVUE Cloud Suite for Azure	GigaVUE Cloud Suite for OpenStack	GigaVUE Cloud Suite for VMware(ESXi)	GigaVUE Cloud Suite for VMware(NSX-T)	GigaVUE Cloud Suite for Third Party Orchestration	GigaVUE Cloud Suite for Nutanix
Masking	✓	✓	✓	✓	✓	✓	✓
Packet Slicing	✓	✓	✓	✓	✓	✓	✓
De-Duplication	✓	✓	✓	✓	✓	✓	✓
Application Metadata Exporter	✓	✓	✗	✓	✓	✓	✗
L2GRE Tunnel Encapsulation	✓	✗	✓	✓	✓	✓	✓
VXLAN Tunnel Encapsulation	✓	✓	✓	✓	✓	✓	✓
L2GRE Tunnel Decapsulation	✓	✗	✓	✓	✓	✓	✓
VXLAN Tunnel Decapsulation	✓	✓	✓	✓	✓	✓	✓
ERSPAN Tunnel Decapsulation	✓	✗	✓	✓	✓	✓	✓
UDPGRE Tunnel Decapsulation	✓	✗	✓	✓	✓	✓	✗
GENEVE Decap	✓	✗	✗	✗	✓ (NSX-T)	✗	✗

GigaSMART Operation	GigaVUE Cloud Suite for AWS	GigaVUE Cloud Suite for Azure	GigaVUE Cloud Suite for OpenStack	GigaVUE Cloud Suite for VMware(ESXi)	GigaVUE Cloud Suite for VMware(NSX-T)	GigaVUE Cloud Suite for Third Party Orchestration	GigaVUE Cloud Suite for Nutanix
Header Stripping	✓	✓	✓	✓	✓	✓	✓
Header Addition	✗	✗	✗	✗	✗	✗	✗
FlowVUE (IP-based)	✗	✗	✗	✗	✗	✗	✗
Adaptive Packet Filtering (APF) without RegEx	✓	✓	✗	✓	✓	✓	✓
Application Session Filtering (ASF)	✓	✓	✗	✓	✓	✓	✓
Application Filtering Intelligence (AFI)	✓	✓	✗	✓	✓	✓	✓
Application Metadata Intelligence (AMI)	✓	✓	✗	✓	✓	✓	✓
NetFlow	✓	✓	✗	✓	✓	✓	✓
Application Visualization	✓	✓	✗	✓	✓	✗	✓
Load Balancing (Stateless)	✓	✓	✓	✓	✓	✓	✓
Load Balancing (Stateful)	✗	✗	✗	✗	✗	✗	✗

GigaSMART Operation	GigaVUE Cloud Suite for AWS	GigaVUE Cloud Suite for Azure	GigaVUE Cloud Suite for OpenStack	GigaVUE Cloud Suite for VMware(ESXi)	GigaVUE Cloud Suite for VMware(NSX-T)	GigaVUE Cloud Suite for Third Party Orchestration	GigaVUE Cloud Suite for Nutanix
SSL Decryption for Out-of-Band Tools (Passive SSL)	✓	✓	✓	✓	✗	✓	✓
SSL Decryption for Inline Tools	✗	✗	✗	✗	✗	✗	✗
5G-Service Based Interface Application (5G-SBI)	✗	✗	✓	✓	✓	✓	✗

Application Intelligence

Application Intelligence provides a comprehensive solution that:

- identifies the applications contributing to the network traffic.
- isolates preferred application-specific traffic and directs it to the appropriate tools.
- exports relevant application metadata for further analytics and analysis.

Application Intelligence provides the following capabilities for virtual nodes:

- Application Visualization
- Application Filtering Intelligence
- Application Metadata Intelligence
- Application Metadata Exporter

Points to Note for Application Intelligence

Point to note when configuring Application Intelligence:

1. For a monitoring domain, the following application can be configured only once, and all these applications must be configured in a single monitoring session.
   a. Application Visualization
   b. Application Filtering
   c. Application Metadata
2. For GigaVUE V Series Node version lesser than 6.3.00, Application Visualization, Application Filtering, Application Metadata, and Application Metadata Exporter (AMX) applications are not supported in the Monitoring Session.

3. When undeploying and redeploying the Monitoring session which has the Application Intelligence application, ensure to follow the steps given below:

    a. Go to **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. The **Monitoring Sessions** page appears. Select the Monitoring Session for which you enabled Secure Tunnels. Click **Actions > Undeploy**. The monitoring session is undeployed.

    b. Select the Monitoring Session for which you enabled Secure Tunnels. Click **Actions > Edit**. The **Edit Monitoring Session** Canvas page appears.

    c. Add the Application Intelligence applications.

    d. Modify the Number of Flows as per the below table:

Cloud Platform	Instance Size	Maximum Number of Flows
VMware	Large (8 vCPU and 16 GB RAM)	200k
AWS	Large (c5n.2xlarge)	300k
	Medium (t3a.xlarge)	100k
Azure	Large (Standard_D8s_V4)	500k
	Medium (Standard_D4s_v4)	100k
Nutanix	Large (8 vCPU and 16 GB RAM)	200k

> **NOTE:** Medium Form Factor is supported for VMware ESXi only when secure tunnels option is disabled. The maximum Number of Flows for VMware ESXi when using a medium Form Factor is 50k.

    e. Click **Deploy**.

4. After adding the above-listed applications and deploying the Monitoring Session, you cannot edit the Number of flows and Fast Mode. For more detailed information on Number of flows and Fast Mode, refer to Number of Flows and Fast Mode.

5. Once the Number of flows is added in any of the above-listed applications, the same value is applied to all the above-listed applications configured in that Monitoring Session. You cannot change it.

6. Once Fast Mode is enabled in any of the above-listed applications, then it is enabled for all the above-listed applications configured in that Monitoring Session. You cannot change it.

7. You can also configure Application Intelligence with precryption, prefiltering, and secure tunnels. Refer to Precryption, Prefiltering, and Secure Tunnels topics in the respective cloud deployment guides for more detailed information on how to configure these features.

8. Small Form Factor for VMware ESXi is not supported when using applications like Application Visualization, Application Metadata, Application Filtering. Refer to Configure GigaVUE V Series Nodes for VMware ESXi more detailed information on how to deploy GigaVUE V Series Node, where you select the Form Factor.

Application Visualization

Application Visualization identifies and monitors all applications contributing to the network traffic and reports on the total applications and the total bandwidth they consume over a select period. Application Visualization allows you to identify more than 3,200 applications. It displays the traffic statistics in bytes and packets.

Refer to the following topics for more detailed information on how to configure the application and view the statistics:

- Configure Application Visualization for Virtual Environment
- View Application Statistics for Application Visualization
- Configure Filtering and Metadata Export for Selected Applications in Application Visualization

Configure Application Visualization for Virtual Environment

Application Visualization can be configured in the **Edit Monitoring Session** Canvas Page. To add an Application Visualization application to the canvas, follow the steps given below:

1. Drag and drop **Application Visualization** from **APPLICATIONS** to the graphical workspace.
2. Click the Application Visualization application and select **Details**. The Application quick

view appears.

3. In the Application quick view, enter or select the following details:

Parameter	Description
Name	Enter a name for the application.
Description	Enter the description.
Export Interval	The time interval in seconds at which the export must be done. The export interval is set to 300 seconds. It cannot be modified.
Advanced Settings	
Number of Flows	The number of flows supported by the application. Refer to the following table for the maximum number of flows supported for VMware, AWS, Nutanix, and Azure platforms.
Monitoring	You can use this option, enable or disable the Application Visualization application functionality.
Fast Mode	Enable the **Fast Mode** option for performance (less CPU cycles and less memory utilization) improvement. When the **Fast Mode** is enabled, some or all of the attributes of the applications will be disabled. If all the attributes of the application are disabled then the application itself is disabled. Refer to Fast Mode section for more information on the benefits and limitations of the Fast Mode. **NOTE:** This option is disabled for NetVUE Base Bundle License.

Table under Number of Flows:

Cloud Platform	Instance Size	Maximum Number of Flows
VMware	Large (8 vCPU and 16 GB RAM)	200k
AWS	Large (c5n.2xlarge)	300k
	Medium (t3a.xlarge)	100k
Azure	Large (Standard_D8s_V4)	500k
	Medium (Standard_D4s_v4)	100k
Nutanix	Large (8 vCPU and 16 GB RAM)	200k

NOTE: Medium Form Factor is supported for VMware ESXi only when secure tunnels option is disabled. The maximum Number of Flows for VMware ESXi when using a medium Form Factor is 50k.

4. Click **Save**.

View Application Statistics for Application Visualization

To view the application Statistics for the Application Visualization application, follow the steps given below:

1. Click **Traffic > Virtual > Orchestrated Flows > Select your cloud platform**.
2. Select a monitoring session from the list view, click **Actions > Edit**. The Edit Monitoring Session page appears.
3. Click the application and select **Details**. The Application quick view appears.
4. Click on **STATISTICS** tab.
5. You can view the following in the statistics page:
   a. **Total Traffic**: Displays the total traffic of the network. Use the drop-down menus to change the parameters.
   b. **Top Applications**: Displays the Top 10 applications running in the network based on the metrics.
   c. **All Applications** : Click on the drop-down menu that displays **Top 10** and select the **All** . You can view all the applications and their bandwidth in the network. You can also perform filtering and exporting metadata for selected applications. Refer to Configure Filtering and Metadata Export for Selected Applications in Application Visualization for more detailed information on how to perform filtering and exporting metadata for selected applications.

   You can view the statistics for past hour, past 24 hours, or past 7 days. GigaVUE-FM also allows you to view statistics for a particular period by selecting the date and time. The selected data and time must be with in the past 7 days.

   GigaVUE-FM takes more than five minutes to display the application statistics since the export interval is fixed at five minutes. For the first fifteen minutes after creating the solution, if GigaVUE-FM receives traffic, it will show real-time data. If there is no traffic during this time, it will take at least eleven minutes to display the statistics once traffic is received.

Configure Filtering and Metadata Export for Selected Applications in Application Visualization

This section describes how to perform filtering and exporting metadata for selected applications when configuring Application Visualization. Refer to the following steps for more detailed information:

- Filter Traffic for Selected Applications
- Export Metadata for Selected Applications

Filter Traffic for Selected Applications

1. Click the Application Visualization application in the Monitoring Session Canvas page and select **Details**. The Application quick view appears.
2. Click on **STATISTICS** tab.
3. Click on the drop-down menu that displays **Top 10** and select the **All** .

4. Select the applications for which you want to filter traffic.

> **NOTE:** Select the applications and their attributes for traffic filtering by layer seven applications. You can select a maximum of 64 attributes for each application.

5. Click **Actions > Filter Selected Applications**. The **Filter Selected Applications** dialog box opens.

6. In the **Filter Selected Applications** dialog box, Select the existing Application Filtering map or New Map from the **Send to Map** drop-down menu.

   - **New Map:**Select this option if you wish to create a new application filtering map, to filter the traffic from the applications.

   - **Existing map:** Select this option if you have already configured an application filtering map and you wish to send the traffic for filtering to that map.

7. Under the **Applications** section, choose the traffic as pass or drop for the selected applications.

8. Click **Send to Map**.

> **NOTE:** If the **New Map** option is selected from the **Send to Map** drop-down menu. Then, the map quick view appears. Refer to step 3, 4, 5, 6, and 7 in Configure Application Filtering Intelligence for Virtual Environmentsection for more detailed instructions on how to configure Application Filtering.

Export Metadata for Selected Applications

1. Click the Application Visualization application and select **Details**. The Application quick view appears.

2. Click on **STATISTICS** tab.

3. Click on the drop-down menu that displays **Top 10** and select the **All** .

4. Select the applications for which you want to export metadata.

> **NOTE:** Select the applications and their attributes for traffic filtering by layer seven applications. You can select a maximum of 64 attributes for each application.

5. Click **Actions > Export Metadata for Selected Applications**. The **Export Metadata for Selected Applications** dialog box opens.

6. In the **Export Metadata for Selected Applications** dialog box, Select the existing Application Metadata application or New Exporter from the **Send to Exporter** drop-down menu.

   - **New Application Metadata:**Select this option if you wish to create a new application metadata, to export metadata from the applications.

   - **Existing Application Metadata Application:** Select this option if you have already configured an Application Metadata Intelligence application and you wish to send the traffic for exporting metadata from the applications.

7. Click **Export**.

> **NOTE:** If the **New Application Metadata** option is selected from the **Send to Exporters** drop-down menu. Then, the application quick view appears. Refer to steps 3 and 4 in Configure Application Metadata Intelligence for Virtual Environment sectionConfigure Application Filtering Intelligence for Virtual Environmentfor more detailed instructions on how to configure Application Metadata application.

User Defined Application

This feature allows you to identify unclassified TCP, UDP, HTTP, and HTTPS applications and extract their application name and ID.

Refer to the following topic for more detailed information:

- Supported Protocols and Attributes
- Mindata
- Supported RegExp Syntax
- Limitations
- Create Rules for User Defined Application

Supported Protocols and Attributes

The DPI engine will match the rules defined based on the following protocols and attributes within the first 500 bytes of a packet payload.

For supported Regex patterns, refer Supported RegExp Syntax

Protocol	Attributes	Attribute Labels	Description	Direction	Supported Data Type	Example Value
http	cts-uri	Request URI	Partially Normalized URL (path + request)	Client to Server Only	REGEXP	\/fupload\/(create_file|new_slice|upload_slice)\?.*upload_token=.*
	cts-server	Server Name	Web Server Name from URI or Host	Client to Server Only	REGEXP	(.*\.)?gigamon\.com

	mime_type	MIME Type	Content type of Request or the Web page	Both, Client to Server or Server to Client	REGEXP	http
	cts-user_agent	User Agent	Software / Browser used for request	Client to Server Only	REGEXP	mozilla
	cts-referer	Referer URI	Source address where client got the URI	Client to Server Only	REGEXP	http:\/\/gigamon.com\/
	stc-server_agent	Server Agent	Software used for the server	Server to Client Only	REGEXP	NWS_TCloud_PX
	stc-location	Redirect Location	Destination address where the client is redirected to	Server to Client Only	REGEXP	.*\/football\/.*
	cts-cookie	Cookie (Raw)	Raw value of the HTTP Cookie header line	Client to Server Only	REGEXP	.*tEstCoOkie.*
	content	Content	Message body content	Both, Client to Server or	REGEXP	.*GIGAMON.* mindata = 206 Refer Mindata

				Server to Client		
http2	cts-uri	Reque st URI	Partially Normaliz ed URL (path + request)	Client to Server Only	REGEXP	\/fupload\/(create_file|new_ slice|upload_slice)\?.*upload_ token=.*
	cts-server	Server Name	Web Server Name from URI or Host	Client to Server Only	REGEXP	(.*\.)?gigamon\.com
	cts-user_ agent	User Agent	Software / Browser used for request	Client to Server Only	REGEXP	mozilla
	cts-referer	Referer URI	Source address where client got the URI	Client to Server Only	REGEXP	http:\/\/gigamon.com\/
ssl	commo n_name	Domai n Name	Domain name from Client Hello message or the certificat e		REGEXP	(.*\.)?gigamon\.com
	stc-subject_ alt_ name	Subjec t Alt Name (s)	List of host names which belong to the same certificat e	Server to Client Only	REGEXP	(.*\.)?gigamon\.com

rtmp	cts-page_url	Page URL	URL of the webpage where the audio/video content is streamed	Client to Server Only	REGEXP	http:\/\/www.music.tv\/recorded\/1234567
tcp	stream	Payload Data	Data payload for a packet, excluding the header.		REGEXP	.*GIGAMON.* mindata = 70 Refer Mindata
	port	Server Port	Server (listen) port number		UINT16 RANGE as REGEXP String	80-4350
udp	stream	Payload Data	Data payload for a packet, excluding the header		REGEXP	.*GIGAMON.* mindata = 100 Refer Mindata
	port	Server Port	Server (listen) port number		UINT16 RANGE as REGEXP String	80-4350
sip	user_agent	User Agent	Software used	Both, Client to Server or	REGEXP	GVUE-release 6.2.0

				Server to Client		
icmp	code	Messa ge Code	Code of the ICMP message	Both, Client to Server or Server to Client	UINT8 as REGEXP String	200
	typeval	Messa ge Type	Type of ICMP message	Both, Client to Server or Server to Client	UINT8 as REGEXP String	10
ip	address	Server IP Addres s	IP address of the server		IPV4 as REGEXP String	62.132.12.30√24
	dscp	DSCP Value	DSCP from Different ia ted Service (DS) Field in IP header		UINT8 as REGEXP String	33

	resolv_name	DNS Name	Server's DNS name		REGEXP	gigamon.com
ipv6	address	Server IP Address	IP address of the server		IPV6 as REGEXP String	2001:0:9d38:6ab8:307b:16a 4:9c66:5f4 2001:0:9d38::9c66:5f4/64
	dscp	DSCP Value	DSCP from Differentia ted Service (DS) Field in IP header		UINT8 as REGEXP String	43

Mindata

The mindata value is the number of payload bytes to buffer and match a given pattern. You can configure mindata value for HTTP content, TCP stream, and UDP stream. The buffer size is calculated from the start of the payload and the default buffer size is different for each protocol (HTTP - 206, TCP - 67, and UDP - 48.)

For example, for pattern ".*TEST.*" that may be present within the first 67 bytes of TCP payload, you can specify the mindata value as 4 (which is the length of the input string) or as 67 (which is the default buffer size of TCP payload). In case, the pattern is present in between 65 to 68 bytes of the payload and the mindata is specified as 4 or 67, it will not match. For this case, you must specify the mindata value as 68.

Supported RegExp Syntax

Pattern	Description
.	Matches any symbol
*	Searches for 0 or more occurrences of the symbol or character set that precedes it
+	Searches for 1 or more occurrences of the symbol or character set that precedes it
?	Searches for 0 or 1 occurrence of the symbol or character set that precedes it
( )	Groups a series of expressions together

[ ]	Matches any value included within the bracket at its current position Example: [Dd]ay matches Day and day
| [<start>-<end>]	Separates values contained in ( ). Searches for any one of the values that it separates. Example: The following expression matches dog or cat: (dog | cat). Matches any value contained within the defined range (a hyphen indicates the range). You can mix character class and a hexadecimal range Example: [AaBbCcDdEeFf0-9]
\0 <octal_ number>	Matches for a direct binary with octal input
\x<hexadecimal-number>\x	Matches for a direct binary with hexadecimal input
\[<character-set>\]	Matches a character set while ignoring case. WARNING: Not performance friendly

Limitations

- The maximum number of user defined application that can be configured is 120 per FM. These applications can be spread across one or more application intelligence sessions.
- The maximum number of rules that can be created per application is 8.
- The maximum number of protocols that can be configured per rule is 3.

Create Rules for User Defined Application

To create a new application:

1. Click **Traffic > Virtual > Orchestrated Flows > Select your cloud platform**.
2. Select a monitoring session from the list view, click **Actions > Edit**. The Edit Monitoring Session page appears.
3. In the Edit Monitoring Session page, click **Options**. The **Options** page appears.
4. Select the **USER-DEFINED APPS** tab.
5. Enable the **User-defined Applications** toggle button.
6. Click **New Application**. The New Application page appears.
7. Enter the **User-Defined Application Name**.
8. Enter **Priority**. The value must be between 1 and 120.

> **NOTE:** The lowest value has the highest priority.

9. In the Rules dialog box, select the following details:
    a. Choose the **Protocol** from the list of protocols.
    b. Choose the **Attributes** from the list of attributes.
    c. Choose the **Values** from the list of values.

    Using the **Actions** Button, you can perform the following actions:

10. Click **Save**.

To add the created applications to the monitoring session:

1. In the **USER-DEFINED APPS** tab, click Add Application button.
2. Select the applications that must be added.
3. Click **Done**.

After creating rules for User defined Applications, you can add it to Application Filtering when configuring the applications. Refer to Add Application section for more detailed information on how to add User defined Application when configuring Application Filtering.

Application Filtering Intelligence

Application Filtering Intelligence allows filtering of traffic based on the application (such as YouTube, Netflix, Sophos, or Facebook) or application family (such as antivirus, web, erp, or instant-messaging). Enables traffic filtering by layer 7 applications, which means you can filter out high-volume, low-risk traffic from reaching the tools and distribute high-risk network traffic of interest to the right tool at the right time.

Refer to the following topics for more detailed information and step-by-step instructions on how to configure Application Filtering Intelligence application and view the staistics:

- Configure Application Filtering Intelligence for Virtual Environment
- View Application Statistics for Application Filtering

Configure Application Filtering Intelligence for Virtual Environment

Application Filtering Intelligence (AFI) can be configured in the Monitoring Session Canvas. To add Application Filtering application to the canvas, follow the steps given below:

1. Drag and drop **New Map** from **New** to the graphical workspace.
2. Click the application and select **Details**. The Application quick view appears.
3. Enable **Application Filtering** in the **GENERAL** tab.

4. In the Application quick view, enter or select the following details in the **GENERAL** tab:

Parameter	Description
Name	Enter a name for the application.
Description	Enter the description.
Application Filtering Settings	
Bidirectional	Enable or Disable Bi-Directional Flow behavior. Bi-Directional is enabled by default. Disable this option for Uni-Directional Flow behavior.
Timeout	Specify the traffic flow inactivity timeout, in seconds. The session will be removed due to inactivity when no packets match.
Buffer	This option is enabled by default.
Buffer Count Before	Number of packets that should be buffered until the flow is identified. If the flow is not identified even after reaching the maximum number of packets buffered, then all the subsequent packets of this session will be dropped.
Protocol	Select the Protocol. The packet matching the selected protocol will be filtered. The default value is TCP-UDP.
Packet Count	Enable or Disable Packet Count. Packet Count is disabled by default.
Number of packets **NOTE:** This field appears only when Packet Count field is enabled.	Specifies the number of packets to forward to the tool port for each session match. After the packet count is reached, subsequent packets for the session are dropped. The packet count includes the packet that triggered the creation of the session. The default is disable, which means that all packets will be forwarded to the tool port. The range is from 2 to 100.
Session Fields	
Session Field	The Packet fields to be considered for creating the Session / traffic flow (Session key fields)
Action	Add or Remove 'VlanId' Packet field for creating the session / traffic flow.

Parameter	Description
Advanced Settings	
Number of Flows	The number of flows supported by the application. Refer to the following table for the maximum number of flows supported for VMware, AWS, and Azure platforms. **NOTE:** Medium Form Factor is supported for VMware ESXi only when secure tunnels option is disabled. The maximum Number of Flows for VMware ESXi when using a medium Form Factor is 50k.
Fast Mode	Enable the **Fast Mode** option for performance (less CPU cycles and less memory utilization) improvement. When the **Fast Mode** is enabled, some or all of the attributes of the applications will be disabled. You can view the list of attributes/applications available in the fast mode by navigating to the app editor under AMI feature in the FM. If all the attributes of the application are disabled then the application itself is disabled. Refer to Fast Mode section for more information on the benefits and Limitations of the Fast Mode.

Cloud Platform	Instance Size	Maximum Number of Flows
VMware	Large (8 vCPU and 16 GB RAM)	200k
AWS	Large (c5n.2xlarge)	300k
	Medium (t3a.xlarge)	100k
Azure	Large (Standard_D8s_V4)	500k
	Medium (Standard_D4s_v4)	100k
Nutanix	Large (8 vCPU and 16 GB RAM)	200k

5. Click the **RULESETS** tab. Through the map, packets can be dropped or passed based on the highest to lowest rule priority. You can add 5 rule sets on a map. Each rule set can have only 25 rules per map and each rule can have a maximum of 4 conditions.

Enter the following details for each of the Rule Set created:

Parameter	Description
Priority	A priority determines the order in which the rules are executed. The priority value can range from 1 to 5, with 1 being the highest and 5 is the lowest priority.
AE ID	Application Endpoint ID will be used as source or destination object for creating or connecting links
Actions	Using this option, you can perform the following functions: • **New Ruleset**- Use to add a new Rule Set. > **NOTE:** A maximum of 5 Rule Sets can be created. • **New Rule**- Use to add a New Rule > **NOTE:** A maximum of 25 Rules can be created per rule set. • **Delete this Ruleset**- Use to delete the Ruleset
RULES	
Rule	Use the toggle button to **Pass** or **Drop** the traffic through the map.

Parameter	Description
Condition	Select any one of the conditions from the drop-down menu and search or select the attributes. Use the + and - buttons to add or remove a condition with a Rule. Click [...] and select **Add Condition** to add more conditions. > **NOTE:** A maximum of 4 conditions can be created per Rule.
APPLICATION FILTERING Select the applications and their attributes for traffic filtering by layer seven applications. You can select a maximum of 64 attributes for each application.	
Add Application	Click on the **Add Application** button. The **Add Application** dialog box opens. Select an **Application Family** and the **Applications** that needs to be filtered from the traffic. In the Traffic Action column, select **Pass** or **Drop** to pass or drop the traffic. You can also use **Pass All** or **Drop All** to allow or drop the traffic for all the applications. **User Defined Applications**: To configure User Defined Applications for AFI, follow the steps given below. 1. Enable **User Defined Applications** toggle button in the **Options** page. Refer to User Defined Application topic for more detailed information on what is user defined applications and how to configure it. 2. In this **Add Application** dialog box, select **User Defined Applications** from the **Application Family** list.

6. To pass or drop any remaining traffic in the network, enter the priority and AE ID in the default rule set available. Select **Pass** or **Drop** option for **Any Remaining Traffic** field.

7. Click the **THRESHOLDS** tab. For more details on how to create and apply threshold template, refer to Traffic Health Monitoring section in the respective cloud deployment guides.

8. To reuse the configuration, click **Add to Library**. Save the application filtering configurations using one of the following ways:

    a. Select an existing group from the **Select Group** list or create a **New Group** with a name.

    b. Enter a description in the **Description** field, and click **Save**.

    c. The saved map can be found in the **Map Library** in the **Edit Monitoring Session** Canvas Page.

9. Click **Save**.

To edit a map, select the map and click **Details**, or click **Delete** to delete the map.

When using Application Filtering application, you can either use a single tunnel, to tunnel all the filtered traffic from the application or use a separate tunnel for each rule configured.

View Application Statistics for Application Filtering

To view the application Statistics for the Application filtering application, follow the steps given below:

1. Click **Traffic > Virtual > Orchestrated Flows > Select your cloud platform**.
2. Select a monitoring session from the list view, click **Actions > Edit**. The Edit Monitoring Session page appears.
3. Click the application and select **Details**. The Application quick view appears.
4. Click on **STATISTICS** tab.
5. You can view the following in the Application Filtering application statistics page:
   a. Rules - Displays the rules created in this application.
   b. Pass App (Bytes) - Displays the packet that pass through the applications selected.
   c. Drop App (Bytes) - Displays the packets that are dropped by the applications selected.
   d. Pass Rule (Bytes) - Displays the packet that pass through the rule sets configured.
   e. Drop Rule (Bytes) - Displays the packets that are dropped by the rule sets configured.

Application Metadata Intelligence

Application Metadata Intelligence allows you to export metadata from applications that are detected in the network traffic. The records can be exported to a collector either in IPFIX or CEF format through the IP interface or the management interface. You can also use the application metadata attributes for purposes other than security, such as to determine the network or application health, to track the long-lived sessions seen in the network, and so on.

Application Metadata Intelligence generates more than 5000 attributes for more than 3200 applications without impacting the users, devices, applications, or the network appliances. The feature identifies applications even when the traffic is encrypted.

Application Metadata Intelligence (AMI) is enabled to multi-collect protocols with more than one metadata attribute of the same type. The multi-collect feature supports additional protocols such as DNS, GTP,GTPV2, DHCP, HTTP, HTTPS, SSL, HTTP_PROXY, HTTP2, KERBEROS5, and DHCP6.

The generated metadata is exported in IPFIX (IP Flow Information Export) format and CEF (Common Even Format) to security analytics and forensics tools thereby providing greater visibility to enforce corporate compliance.

The output from the Application Metadata Intelligence in CEF format can also be converted to JSON format using Application Metadata Exporter (AMX) application. To learn more about AMX application refer to Application Intelligence—Application Metadata Exporter

Refer to following topics for more detailed information and step-by-step instructions on how to configure Application Metadata Intelligence and view the statistics:

- Configure Application Metadata Intelligence for Virtual Environment
- View Application Statistics for Application Metadata

You can convert the output from the Application Metadata Intelligence (AMI) which is in CEF format into JSON format and send it to the cloud tools and Kafka. Refer toApplication Metadata Exporter for detailed information on AMX and how to configure it..

Configure Application Metadata Intelligence for Virtual Environment

Application Metadata Intelligence (AMI) can be configured in the Monitoring Session Canvas. To add Application Metadata Intelligence application to the canvas, follow the steps given below:

1. Drag and drop **Application Metadata** from **APPLICATIONS** to the graphical workspace.
2. Click the Application Metadata application and select **Details**. The Application quick view appears.

3. In the Application quick view, enter or select the following details in the **General** tab:

Parameter	Description
Name	Enter a name for the application.
Description	Enter the description.
Application Metadata Settings	
Flow Direction	Enable or Disable Bi-Directional Flow behavior. Bi-Directional is enabled by default. Disable this option for Uni-Directional Flow behavior.
Timeout	Specify the traffic flow inactivity timeout, in seconds. The session will be removed due to inactivity when no packets match.
Multi Collect	• **Enable**: Enables the multi-collect of attributes within a given Metadata Store cache which means that if a configured attributes is seen in multiple packets within the same flow, each of these information is collected. Multi Collect is enabled by default, when a new cache is created. Multi Collect is enabled, when upgraded from an older release. • **Disable**: Disables the multi-collect of attributes within a given Metadata Store cache. **NOTE:** Do not enable this option if you are going to export the Application Metadata using the AMX application. There can be only one attribute in a JSON object, therefore Multi-collect is not supported when configuring the AMX application.
Data Link	If you want to include the VLAN ID along with the 5-tuple to identify the traffic flow, select the **Data Link** and enable the **VLAN** option.
Observation ID	Enter a value to identify the source from where the metadata is collected. The range is from 0 to 255. The calculated value of Observation Domain Id in Hexadecimal is **00 01 02 05**, and in Decimal is **66053**.
Advanced Settings	

Parameter	Description
Number of Flows	The number of flows supported by the application. Refer to the following table for the maximum number of flows supported for VMware, AWS, and Azure platforms.
Fast Mode	Enable the **Fast Mode** option for performance (less CPU cycles and less memory utilization) improvement. When the **Fast Mode** is enabled, some or all of the attributes of the applications will be disabled. If all the attributes of the application are disabled then the application itself is disabled. Refer to Fast Mode section for more information on the benefits and Limitations of the Fast Mode.
Aggregate Round-trip Time	Enable this option to export the minimum, maximum, and mean of RTT values for the following list of supported protocols and attributes and also the aggregate of TCP Lost byte values collected per export time interval.

Within "Number of Flows":

Cloud Platform	Instance Size	Maximum Number of Flows
VMware	Large (8 vCPU and 16 GB RAM)	200k
AWS	Large (c5n.2xlarge)	300k
	Medium (t3a.xlarge)	100k
Azure	Large (Standard_D8s_V4)	500k
	Medium (Standard_D4s_v4)	100k
Nutanix	Large (8 vCPU and 16 GB RAM)	200k

NOTE: Medium Form Factor is supported for VMware ESXi only when secure tunnels option is disabled. The maximum Number of Flows for VMware ESXi when using a medium Form Factor is 50k.

Within "Aggregate Round-trip Time":

Protocol	Arrtibute
http	rtt
icmp	rtt
icmp6	rtt
ssh	rtt
tcp	rtt
tcp	rtt_app
telnet	rtt
wsp	connect_rtt
wsp	query_rtt

4. In the Application quick view, enter or select the following details in the **Exporters** tab:

Parameter	Description
Exporter Name	Enter a name for the Exporter.
Actions	Using this option, you can perform the following functions: • **Add Exporter** - Use to add a new Exporter to this Application Metadata Intelligence Application. A maximum of 5 exporters can be added. • **Apply Template** - Use to select the tool template. Refer to Tool Templates for more information on tool templates and how to create custom tool templates. • **Save as New Template** - Use to save the current configuration as a new custom tool template. • **Delete this Exporter** - Use to delete the Exporter.
APPLICATION ID	Enable to export the data with Application Id.
Format	Select NetFlow or CEF
NetFlow: Select this option to use NetFlow	
Record / Template type	• Segregated - The application-specific attributes and the generic attributes will be exported as individual records to the tool. • Cohesive- The application-specific attributes and the generic attributes will be combined as a single record and exported to the tool.
Active Timeout	Enter the active flow timeout value in seconds.
Inactive Timeout	Enter the inactive flow timeout in seconds.
Version	Select the NetFlow version. The supported versions are V5, V9, IPFIX (V10).
Template Refresh Interval	Enter the time interval at which the template must be refreshed in seconds
CEF: Select this option to use CEF	
Record / Template type	• Segregated - The application-specific attributes and the generic attributes will be exported as individual records to the tool. • Cohesive- The application-specific attributes and the generic attributes will be combined as a single record and exported to the tool.
Active Timeout	Enter the active flow timeout value in seconds.
Inactive Timeout	Enter the inactive flow timeout in seconds.
APPLICATION & ATTRIBUTES: Select the applications and their attributes for traffic filtering by layer seven applications. You can select a maximum of 64 attributes for each of the application. (Not applicable when using NetFlow V5 Template in the above **Template** drop-down menu.)	
Add Application	Click on the **Add Application** button. The **Add Application** dialog box opens. Select an **Application Family** and the **Applications** that needs to be

Parameter	Description
	filtered from the traffic.
NETWORK & TRANSPORT PARAMETERS: Select the Network and the transport packet attributes with the respective parameters	
Data Link	Select any one of the parameters such as Source MAC address, Destination MAC Address and VLAN.
Interface	Select any one of the parameter such as Input Physical, Output Physical and Input Name.
IP	Select the parameter as Version if required.
IPv4	Select the required attributes. By default, Source Address, Destination Address, and Protocol are enabled.
IPv6	Select the required attributes. By default, Source Address, Destination Address, and Next Header are enabled.
Transport	Select the required attributes. By default, Source Port, Destination Port are enabled.
Counter	Select the Bytes, and Packets.
Timestamp	Select the required timestamp such as System Uptime First, Flow Start, System Uptime Last, and Flow End.
Flow	Select the parameter as End Reason if required.
GTP-U	Select the required parameters such as QFI and TEID.
Outer IPv4	Select any one of the parameter such as Source or Destination.
Outer IPv6	Select any one of the parameter such as Source or Destination.

5. Click **Save** to deploy the Application Metadata application.

After adding the Application Metadata application and deploying Monitoring Session, you cannot change the **Aggregate Round Trip time** option.

When using Application Metadata, if you create a tunnel to tunnel the output to the tools, then select the tunnel type as UDP.

When using Application Metadata application, you can either use a single tunnel to export all the metadata from the application or use a separate tunnel for each exporter configured.

View Application Statistics for Application Metadata

To view the application Statistics for the Application Metadata application, follow the steps given below:

1. Click **Traffic > Virtual > Orchestrated Flows > Select your cloud platform**.
2. Select a monitoring session from the list view, click **Actions > Edit**. The Edit Monitoring Session page appears.
3. Click the application and select **Details**. The Application quick view appears.

4. Click on **STATISTICS** tab.
5. You can view the following in the Application Metadata application statistics page:
   a. Exporter Name - Displays the exporters created for this application.
   b. Format - Displays the format as NetFlow or CEF, for the individual exporters.
   c. Packet Sent/ Sec - Displays the count of packets sent per second for each exporter.

Application Metadata Exporter

Refer to the following topics for more detailed information on the various ways to configure AMX:

- Export AMI output by AMX
- Export of 3G/4G/5G Control Plane Metadata by AMX

Export AMI output by AMX

Application Metadata Exporter(AMX) application converts the output from the Application Metadata Intelligence (AMI) in CEF format into JSON format and sends it to the cloud tools and Kafka.
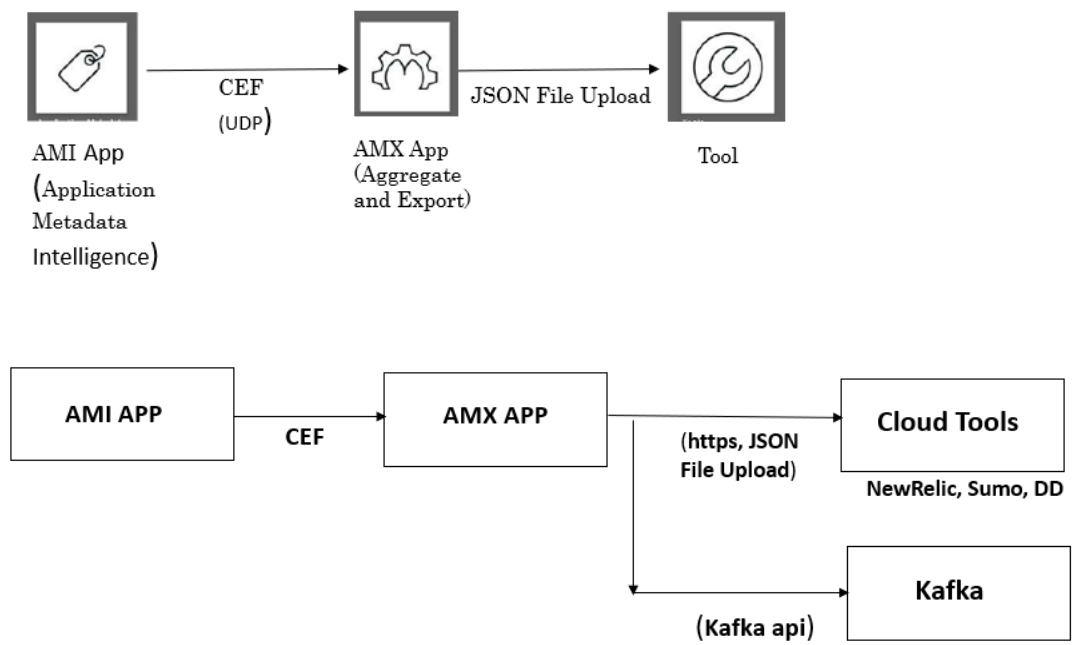
The AMX application can be deployed only on a GigaVUE V Series Node and can be connected to Application Metadata Intelligence running on a physical node or a virtual machine. The AMX application and the AMI are managed by GigaVUE-FM.

Export of 3G/4G/5G Control Plane Metadata by AMX

The AMX application can also export the 3G/4G control plane metadata received from the GTP Correlation engine and 5G control plane metadata received from the 5G CPN engine in either Flat or Hierarchical JSON format to the cloud tools and Kafka in Flat JSON format.

The AMX application can be deployed only on a GigaVUE V Series node and can be connected to a GTP Correlation / 5G CPN engine running on a physical node.
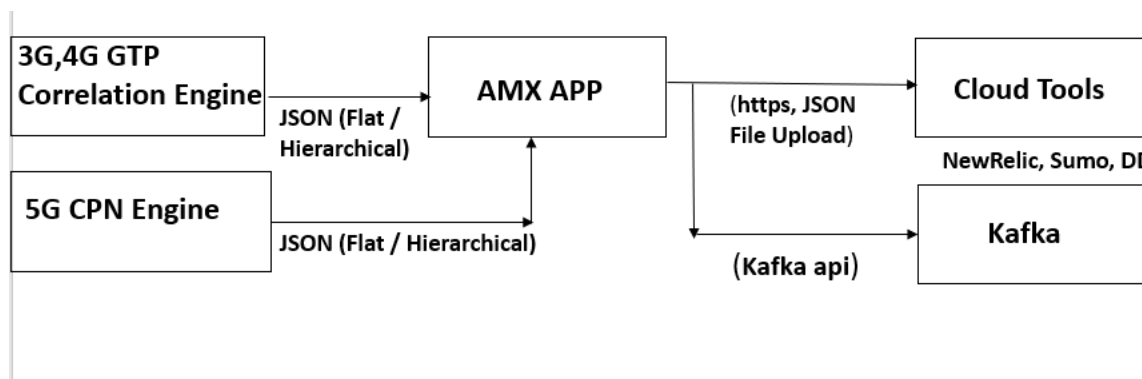
Refer to the following topics for more detailed information and configuration:

- AMX Application Deployment Options
- Prerequisites for Application Metadata Exporter
- Rules for Configuring Application Metadata Exporter
- Configure Application Metadata Exporter Application

AMX Application Deployment Options

AMX application can be deployed on:

- On-Premises
    - Hardware (AMI)
    - Hardware (Control Plane Metadata)
    - Virtual (VMware)

- Public Cloud

On-Premises

Hardware (AMI)

In hardware deployments, the Application Metadata Intelligence (AMI) runs on a physical node/cluster, and the AMX application is deployed on a GigaVUE V Series Node running on VMware ESXi. The output from the AMI in CEF format is sent to the AMX application in V Series Node. The performance of the device and the application is managed by GigaVUE-FM. The following devices support the integration of AMX application:

- GigaVUE-HC1
- GigaVUE-HC2
- GigaVUE-HC3
- GigaVUE-HC1-Plus
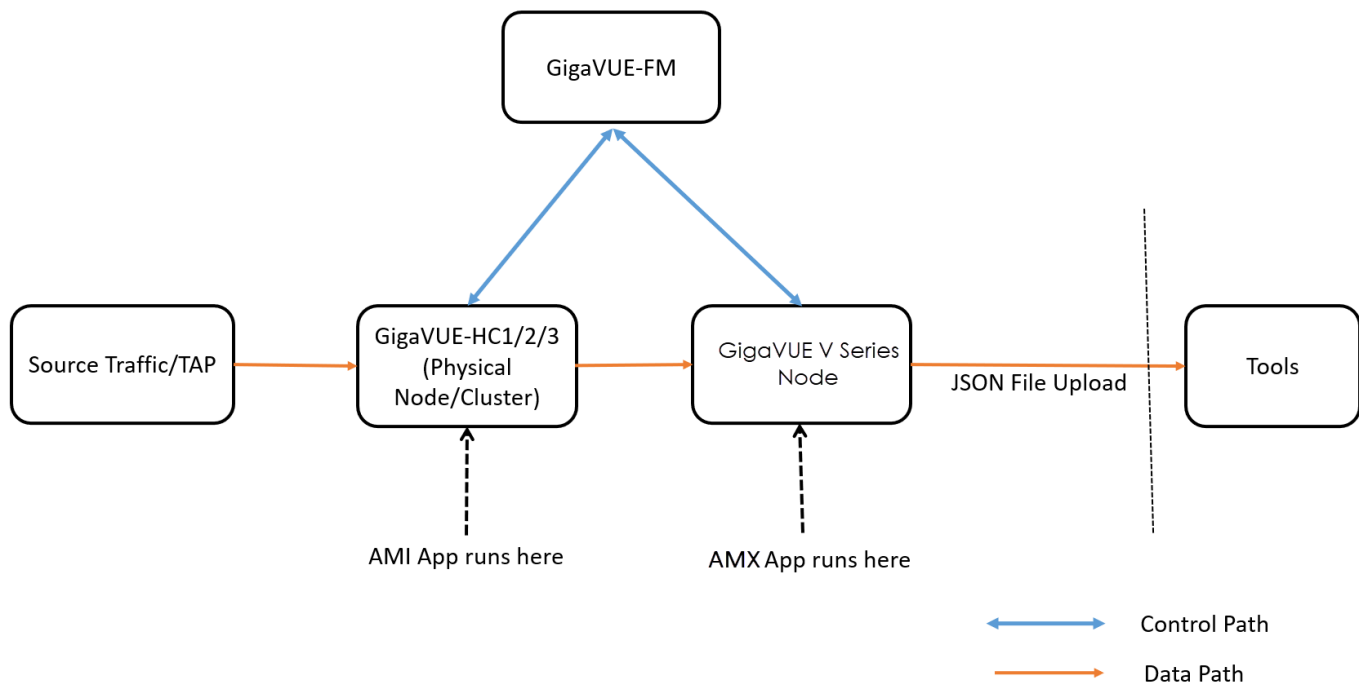
Hardware (Control Plane Metadata)

In hardware deployments, the GTP Correlation Engine runs on a physical node/cluster, and the AMX application is deployed on a GigaVUE V Series Node running on VMware ESXi. The output from the GTP Correlation Engine in Flat or Hierarchical JSON format is sent to the AMX application in V Series Node. The performance of the device and the application is managed by GigaVUE-FM. The GigaVUE-HC3 Gen3 devices support the integration of AMX application.
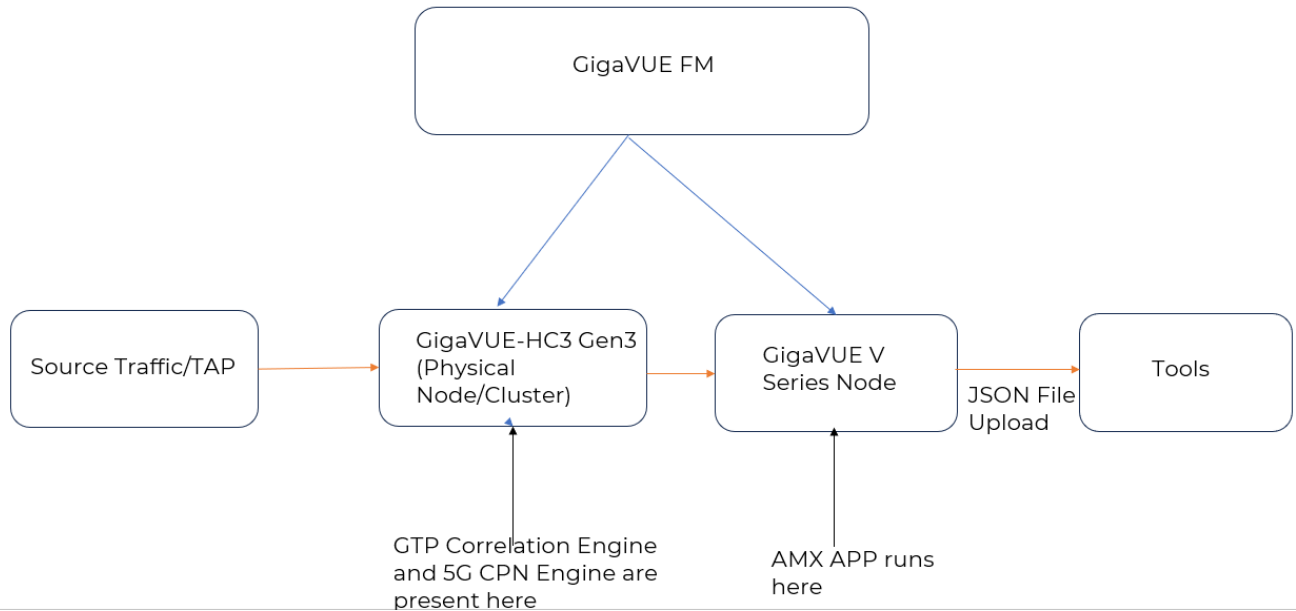
Private Cloud (VMware)

In the Private Cloud environment, the application is supported only on VMware and can be deployed in the VMware as shown in the diagram.
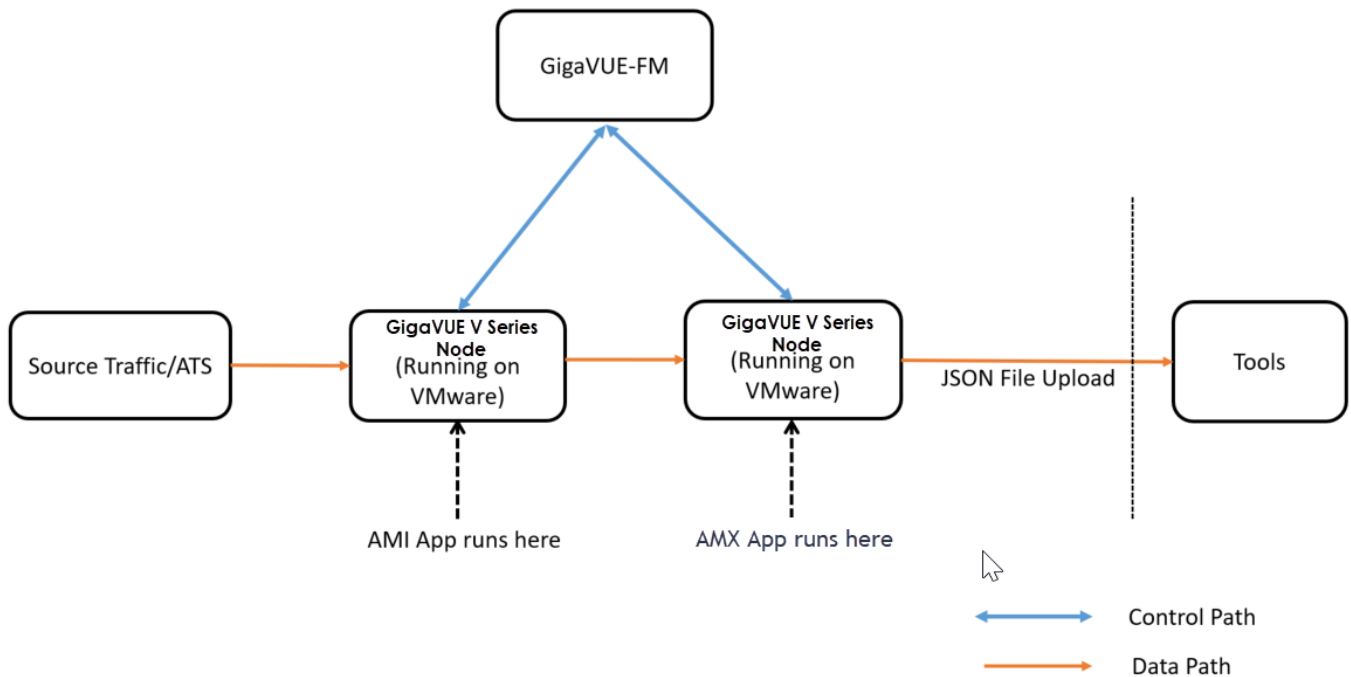
Public Cloud

In the Public Cloud environment, the application is supported on AWS and Azure platforms, and can be deployed as shown in the diagram:
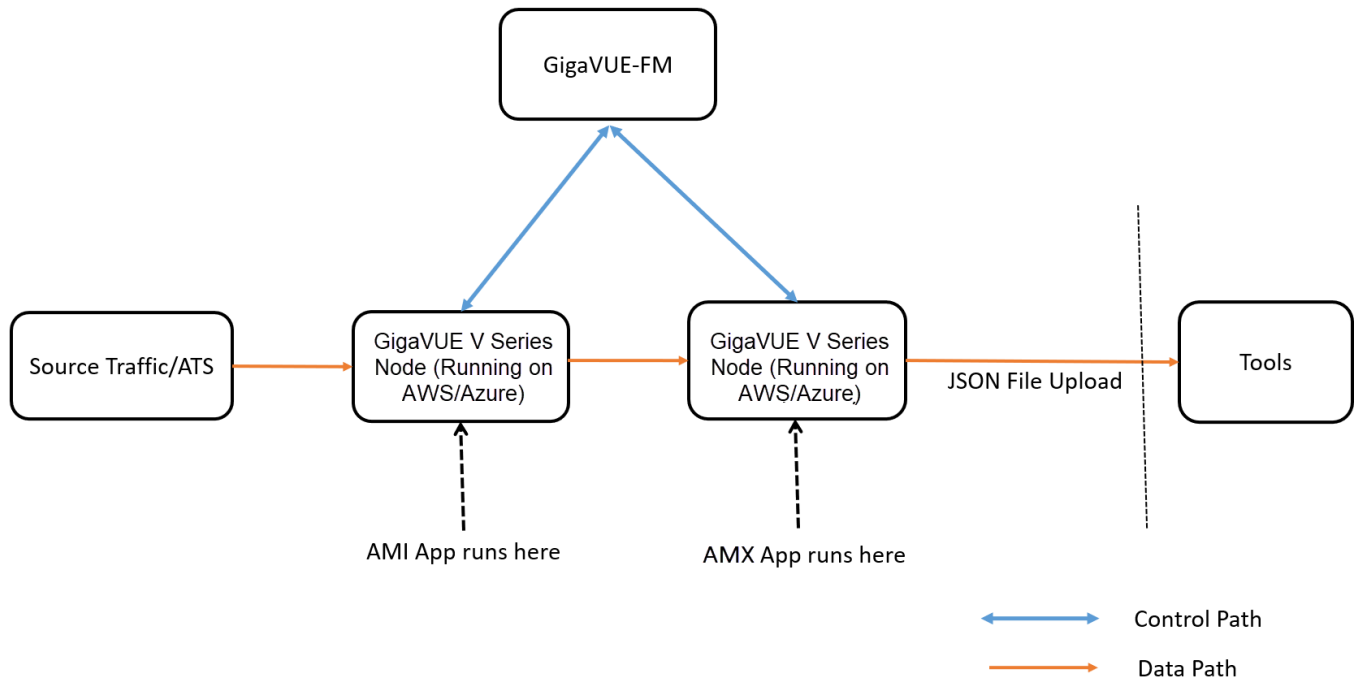
Prerequisites for Application Metadata Exporter

Prerequisites for AWS

Prerequisites to follow when creating a monitoring domain and deploying a V Series node in AWS:

- Select **Traffic Acquisition Method** as Customer Orchestrated Source. Refer Create a Monitoring Domain for more detailed information on how to create a monitoring domain.
- Select **Instance type** with three or more NICs. Refer Configure GigaVUE Fabric Components in GigaVUE-FM for more detailed information on how to deploy a GigaVUE V Series Node.
- When the **Traffic Acquisition Method** is selected as Customer Orchestrated Source, the Volume Size field appears on the **AWS Fabric Launch Configuration** page. Enter the Volume Size as 80GB.

  > **NOTE:** Check on the disk space run every 30 minutes and when the disk space reaches 50%, purge starts.

Prerequisites for Azure

Prerequisites to follow when creating a monitoring domain and deploying V Series node in Azure:

- Select **Traffic Acquisition Method** as Customer Orchestrated Source. Refer Create Monitoring Domain for more detailed information on how to create a monitoring domain.
- Select **Size** with three or more NICs. Refer Configure GigaVUE Fabric Components in GigaVUE-FM for more detailed information on how to deploy a GigaVUE V Series Node.
- When the **Traffic Acquisition Method** is selected as Customer Orchestrated Source, the **Disk Size** field appears on the **Azure Fabric Launch Configuration** page. Enter the Disk Size as 80GB.

  > **NOTE:** Check on the disk space run every 30 minutes and when the disk space reaches 50%, purge starts.

Prerequisites for VMware

Prerequisites to follow when creating a monitoring domain and deploying V Series node in VMware:

- Select **Traffic Acquisition Method** as Customer Orchestrated Source. Refer Create Monitoring Domain for VMware ESXi section in *GigaVUE Cloud Suite Deployment Guide - VMware (ESXi)* for more detailed information on how to create a monitoring domain and deploy GigaVUE V Series Nodes.
- .When deploying this application in VMware NSX-T, create a monitoring domain in the ESXi Monitoring domain. Even if your GigaVUE V Series Node is a part of VMware NSX-T host, you can still deploy it in VMware ESXi monitoring domain. Refer to the Same Host across Different Monitoring Domains topic in the *GigaVUE Cloud Suite Deployment Guide - VMware* for more detailed information*.*

Rules for Configuring Application Metadata Exporter

- The GigaVUE V Series Node deployed must be entirely dedicated to the AMX application, it cannot have other applications in it.
- The monitoring session can only have Raw End Point (REP), it cannot have other applications, maps, or tunnels when using the AMX application. Refer Create Raw Endpoint for more detailed information on how to add a REP to the monitoring session and how to configure it.
- When using this application for production usage, it is recommended to use large size Virtual Machines.

Configure Application Metadata Exporter Application

To add AMX application:

1. Drag and drop **Application Metadata Exporter** from **APPLICATIONS** to the graphical workspace. The Application quick view appears.

2. Enter the Alias for the application. Enter a port number for the **Cloud Tool Ingestor Port**. Then, click the **Add** button for **Cloud Tool Exports** or **Kafka**.

3. Drag and drop **Application Metadata Exporter** from **APPLICATIONS** to the graphical workspace. The Application quick view appears.

4. Enter the Alias for the application.

5. In the **Ingestor** section, enter a port number for the **Port**.field and select **ami** or **gtpc** or **gtpc_hier** for the **Type** field.
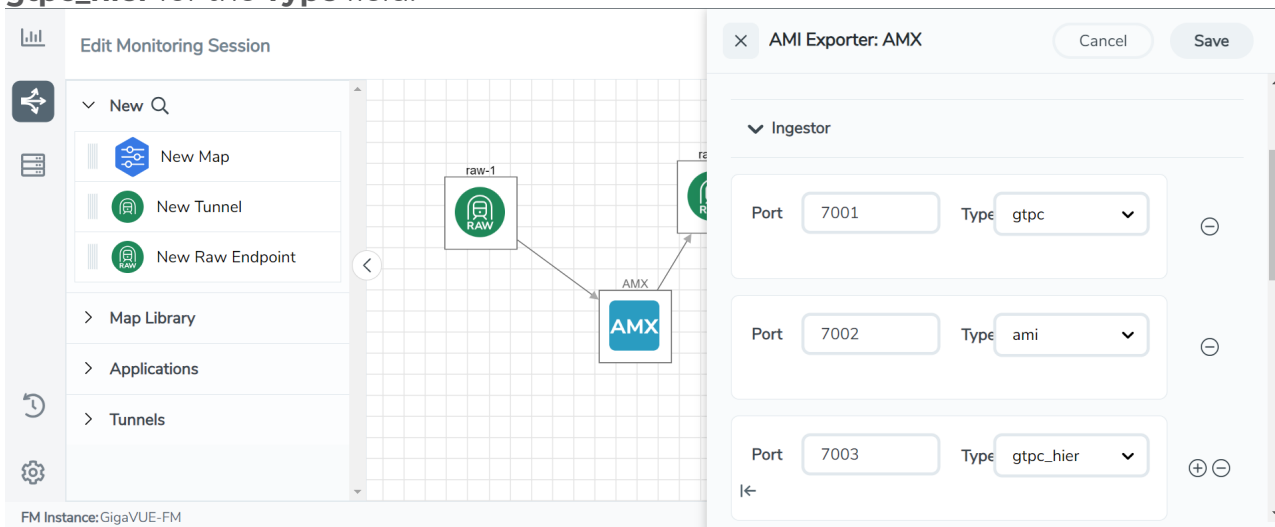
6. You can export your Application Metadata Intelligence output or control plane metadata to either cloud tools or Kafka. Enter the following details for the Cloud tool export in the Application quick view:

Fields	Description
Alias	Enter the alias name for the cloud tool export.
Cloud Tool	Select the Cloud tool from the drop-down menu.
Type	Select ami for exporting AMI or gtpc for exporting control plane metadata.
Account ID	Enter the account ID number of the selected Cloud Tool.
API Key	Enter the API key of the Cloud Tool.
Enable Export	Enable the box to export the Application Metadata Intelligence output in JSON format.
Zip	Enable the box to compress the output file. **NOTE:** Enable this field when using New Relic as the cloud tool.
Interval	The time interval (in seconds) in which the data should be uploaded periodically. The recommended minimum time interval is 10 seconds and the maximum time interval is 1800 seconds.
Parallel Writer	Specifies the number of simultaneous JSON exports done.
Export Retries	The number of times the application tries to export the entries to Cloud Tool. The recommended minimum value is 4 and the maximum is 10.
Maximum Entries	The number of JSON entries in a file. The maximum number of allowed entries is 5000 and the minimum is 10, however 1000 is the default value.
Labels	Click **Add**. Enter the following details: o Enter the **Key** . o Enter the **Value**. **NOTE:** When New Relic is selected as the cloud tool, the key is automatically set as is **eventType** and the Value can only have alphanumeric characters, colons (:), periods (.), and underscores (_).
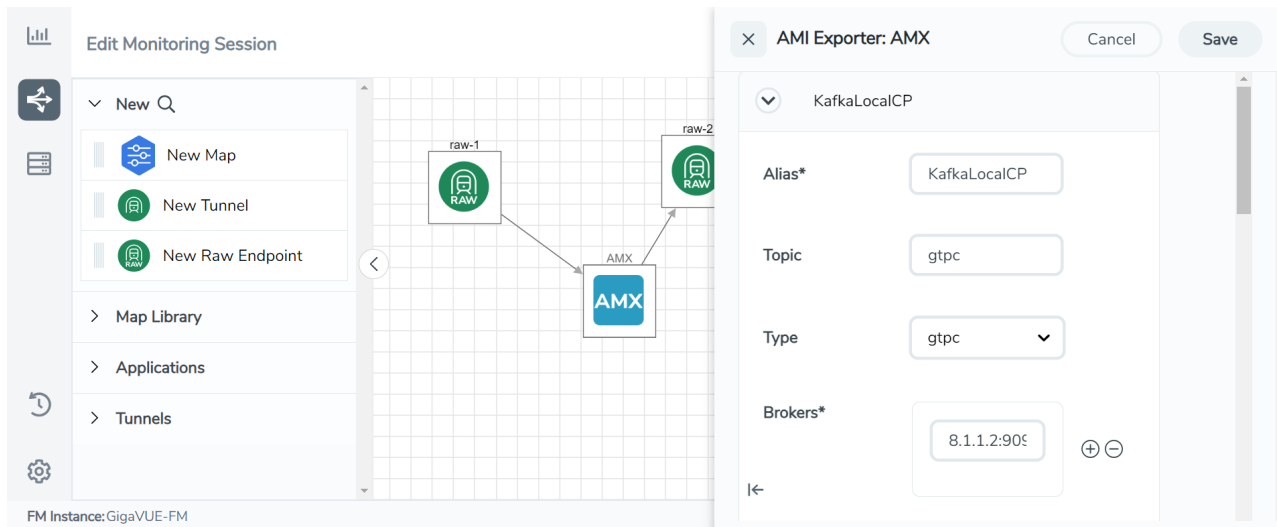
Enter the following details for Kafka export in the Application quick view:

Fields	Description
Alias	Enter the alias name for the Kafka Export.
Topic	The topic name to push JSON streams to, which is generally given to users part of the Kafka administration.
Type	Select ami for exporting AMI or gtpc for exporting control plane metadata.
Brokers	The URL that contains the Kafka cluster endpoints. Click ➕ to add another broker and click ⛔ to remove an existing broker.
Enable Export	Enable the box to export the Application Metadata Intelligence output in JSON format.
Zip	Enable the box to compress the output file.
Interval	The time interval (in seconds) in which the data should be uploaded periodically. The recommended minimum time interval is 10 seconds and the maximum time interval is 1800 secoonds. The default time interval is 30 seconds.
Parallel Writer	Specifies the number of simultaneous JSON exports done.
Export Retries	The number of times the application tries to export the entries to Kafka. The recommended minimum value is 4 and the maximum is 10.

Fields	Description
Maximum Entries	The number of JSON entries in a file. The maximum number of allowed entries is 5000 and the minimum is 10, however 1000 is the default value.

Labels	Click **Add**. Enter the following details:
	   o Enter the **Key**.
	   o Enter the **Value**.

Producer Configurations	Click **Add** to enter the authentication details if a Kafka broker needs authentication. For Example: • security.protocol=SASL_SSL • sasl.mechanism=PLAIN • sasl.username=username • sasl.password=password

7. Click **Deploy** to deploy the monitoring session. The **Select nodes to deploy the Monitoring Session** dialog box appears. Select the GigaVUE V Series Node for which you wish to deploy the monitoring session.

8. After selecting the V Series Node, select the interfaces for the REPs deployed in the monitoring session from the drop-down menu. Then, click **Deploy**.

> **NOTE:** If you reload the GigaVUE V Series Node after configuring the AMX application, then the Ingestor in the AMX application fails.

The monitoring session configuration health can be viewed on the Monitoring Session page. Refer Cloud Health Monitoring for more detailed information on how to view cloud configuration health.

To view the application statistics on the Monitoring Session Statistics page, click **View Monitoring Session Diagram** and click on the AMX application. The Statistics appear as a quick view page. To view the exporter related statistics, select **Exporter** from the top navigation button on the quick view page.

NetFlow

NetFlow Generation is a simple and effective way to increase visibility into traffic flows and usage patterns across systems. The flow-generated data can be used to build relationships and usage patterns between nodes on the network.

Refer to the following topics for step-by-step instructions on how to configure NetFlow:

• Configure Application Metadata Intelligence for Virtual Environment- For SecureVUE Plus Base Bundle

- Create NetFlow Session for Virtual Environment - For NetVUE Base Bundle

Create NetFlow Session for Virtual Environment

Note: This configuration is applicable only when using NetVUE Base Bundle.

To create an NetFlow session, follow these steps:

1. Drag and drop **Application Metadata** from **APPLICATIONS** to the graphical workspace.
2. Click the Application Metadata application and select **Details**. The Application quick view appears.

3. In the Application quick view, enter or select the following details in the **General** tab:

Parameter	Description
Name	Enter a name for the application.
Description	Enter the description.
Application Metadata Settings	
Flow Direction	Enable or Disable Bi-Directional Flow behavior. Bi-Directional is enabled by default. Disable this option for Uni-Directional Flow behavior.
Timeout	Specify the traffic flow inactivity timeout, in seconds. The session will be removed due to inactivity when no packets match.
Data Link	If you want to include the VLAN ID along with the 5-tuple to identify the traffic flow, select the **Data Link** and enable the **VLAN** option.
Observation ID	Enter a value to identify the source from where the metadata is collected. The range is from 0 to 255. The calculated value of Observation Domain Id in Hexadecimal is **00 01 02 05**, and in Decimal is **66053**.
Advanced Settings	
Number of Flows	The number of flows supported by the application. Refer to the following table for the maximum number of flows supported for VMware, AWS, and Azure platforms.

Cloud Platform	Instance Size	Maximum Number of Flows
VMware	Large (8 vCPU and 16 GB RAM)	200k
AWS	Large (c5n.2xlarge)	300k
	Medium (t3a.xlarge)	100k
Azure	Large (Standard_D8s_V4)	500k
	Medium (Standard_D4s_v4)	100k
Nutanix	Large (8 vCPU and 16 GB RAM)	200k

> **NOTE:** Medium Form Factor is supported for VMware ESXi only when secure tunnels option is disabled. The maximum Number of Flows for VMware ESXi when using a medium Form Factor is 50k.

> **NOTE:** When using NetVUE Base Bundle, Multi-Collect, Fast Mode, and Aggregate round-trip time fields are disabled.

4. In the Application quick view, enter or select the following details in the **Exporters** tab:

Parameter	Description
Exporter Name	Enter a name for the Exporter.
Actions	Using this option, you can perform the following functions: • **Add Exporter** - Use to add a new Exporter to this Application Metadata Intelligence Application • **Apply Template** - Use to select the tool template. Refer to Tool Templates for more details on what are tool templates and to create custom tool templates. • **Save as New Template** - Use to save the current configuration as a new custom tool template. • **Delete this Exporter** - Use to delete the Exporter.
APPLICATION ID	Enable to export the data with Application Id.
Format	Select NetFlow
NetFlow: Select this option to use NetFlow	
Record / Template type	• Segregated - The application-specific attributes and the generic attributes will be exported as individual records to the tool. • Cohesive- The application-specific attributes and the generic attributes will be combined as a single record and exported to the tool.
Active Timeout	Enter the active flow timeout value in seconds.
Inactive Timeout	Enter the inactive flow timeout in seconds.
Version	Select the NetFlow version.
Template Refresh Interval	Enter the time interval at which the template must be refreshed in seconds
APPLICATION & ATTRIBUTES: Select the applications and their attributes for traffic filtering by layer seven applications. You can select a maximum of 64 attributes for each application. (Not applicable when using Netflow V5, V9, Netflow IPFIX(V10), or CEF when the flow direction is Uni-Directional in the above **Template** drop-down menu.)	
Add Application	Click on the **Add Application** button. The **Add Application** dialog box opens. Select an **Application Family** and the **Applications** that needs to be filtered from the traffic.
NETWORK & TRANSPORT PARAMETERS: Select the Network and the transport packet attributes with the respective parameters	
Data Link	Select any one of the parameters such as Source MAC Address, Destination MAC Address and VLAN.
Interface	Select any one of the parameter such as Input Physical, Output Physical and Input Name.
IP	Select the parameter as Version if required.
IPv4	Select the required attributes. By default, Source Address, Destination

Parameter	Description
	Address, and Protocol are enabled.
IPv6	Select the required attributes. By default, Source Address, Destination Address, and Next Header are enabled.
Transport	Select the required attributes. By default, Source Port, Destination Port are enabled.
Counter	Select the Bytes, and Packets.
Timestamp	Select the required timestamp such as System Uptime First, Flow Start, System Uptime Last, and Flow End.
Flow	Select the parameter as End Reason if required.
GTP-U	Select the required parameters such as QFI and TEID.
Outer IPv4	Select any one of the parameter such as Source or Destination.
Outer IPv6	Select any one of the parameter such as Source or Destination.

5. Click **Save**.

Examples- Configuring Application Intelligence Solution with Other Applications

This sections provides information on how applications like Application Filtering Intelligence, Application Metadata Intelligence and Application Metadata Exporter can be used with other applications in the monitoring session.

Refer to the following topics for more detailed information:

- Slicing and Masking with Application Filtering Intelligence
- De-duplication with Application Metadata Intelligence

Slicing and Masking with Application Filtering Intelligence

When the traffic passes through the Application Filtering Intelligence, application metadata is created. You can use the slicing and masking application along with Application Filtering application slice, mask, or slice and mask the filtered packets before sending them to the destination tunnel endpoint.

> **NOTE:** When combining slicing and masking operations, the offset range of the masking must be lesser than the offset value entered for the slicing operation, as the slicing operation is performed first.

Follow the steps below to configure Application Filtering Intelligence with Masking and Slicing:

1. Drag and drop **New Map / Application Filtering** from **New** to the graphical workspace.
2. Click the map and select **Details**. The Application quick view appears.
3. Configure Application Filtering Intelligence using the steps given inConfigure Application Filtering Intelligence for Virtual Environment
4. Drag and drop **Slicing** from **Applications** to the graphical workspace.
5. Click the application and select **Details**. The Application quick view appears.
6. Configure slicing application using the steps given in Slicing
7. Drag and drop **Masking** from **Applications** to the graphical workspace.
8. Click the application and select **Details**. The Application quick view appears.
9. Configure masking application using the steps given in Masking.
10. Drag and drop **New Tunnel** from **New** to the graphical workspace.
11. Click the tunnel and select **Details**. The Application quick view appears.
12. Select the **Type** as L2GRE/VXLAN. Select the Traffic Direction as **Out**. Refer to Create Ingress and Egress Tunnel section in the respective Cloud Deployment guides for step-by-step instructions on how to configure Tunnels.
13. Enter Source L4 Port and Destination L4 Port.
14. After placing the required items in the canvas, hover your mouse on the applications, click the red dot, and drag the arrow over to another item (map, application, or tunnel).

The filtered traffic will be sent to the slicing application, the sliced traffic will be sent to masking application and then to the destination tunnel Endpoint.

De-duplication with Application Metadata Intelligence

Duplicate packets are common in network analysis environments where both the ingress and egress data paths are sent to a single output. Using de-duplication with Application Metadata Intelligence lets you eliminate the duplicate packets in the Application Metadata output, only forwarding a packet once and thus reducing the processing load on your tools.

Follow the steps below to configure Application Metadata Intelligence with De-duplication:

1. Drag and drop **Application Metadata** from **Applications** to the graphical workspace.
2. Click the application and select **Details**. The Application quick view appears.
3. Configure Application Metadata Intelligence using the steps given in Configure Application Metadata Intelligence for Virtual Environment.
4. Drag and drop **dedup** from **Applications** to the graphical workspace.
5. Click the application and select **Details**. The Application quick view appears.
6. Configure de-duplication application using the steps given in De-duplication.
7. Drag and drop **New Tunnel** from **New** to the graphical workspace.
8. Click the tunnel and select **Details**. The Application quick view appears.

9. Select the **Type** as UDP.
10. Enter Source L4 Port, Destination L4 Port, and Destination IP. Refer to Create Ingress and Egress Tunnel section in the respective Cloud Deployment guides for step-by-step instructions on how to configure Tunnels.
11. After placing the required items in the canvas, hover your mouse on the map, click the red dot, and drag the arrow over to another item (map, application, or tunnel).

The duplicate packets are removed before sending the traffic to AMI. This will reduce the load on Application Metadata application which in turn can avoid exporting the duplicated Metadata to the tool.

De-duplication

De-duplication application targets, identifies, and eliminates duplicate packets, blocking unnecessary duplication and sending optimized flows to your security and network monitoring tools. De-duplication lets you detect and choose the duplicate packets to count or drop in a network analysis environment.

Duplicate packets are common in network analysis environments where both the ingress and egress data paths are sent to a single output. They can also appear when packets are gathered from multiple collection points along a path. The de-duplication application lets you eliminate these packets, only forwarding a packet once and thus reducing the processing load on your tools.

Feature Overview

There are two actions that can be specified for handling the duplicate packets detected:

- drop, which drops the duplicate packets
- count, which counts the duplicate packets, but does not drop them

A time interval can be configured within which an identical packet will be considered a duplicate. The greater the interval over which traffic can be checked for duplicates, the higher the accuracy of the de-duplication detection and subsequent elimination.

For example, if two of the same packets are seen in the specified time interval, the packets will be detected as duplicates. If one packet is seen in the time interval and another packet is seen in a later time interval, the packets will not be detected as duplicates.

For IPv4 and IPv6 packets, to determine if a packet is considered to be a duplicate, parts of the IP headers (Layer 3 and Layer 4), as well as part of the payload are compared.

For non-IP packets, a packet is considered to be a duplicate if it is identical.

Configure De-duplication Application

To add a de-duplication application:

1. Drag and drop **Dedup** from **APPLICATIONS** to the graphical workspace.
2. Click the Dedup application and select **Details**. The Application quick view appears.
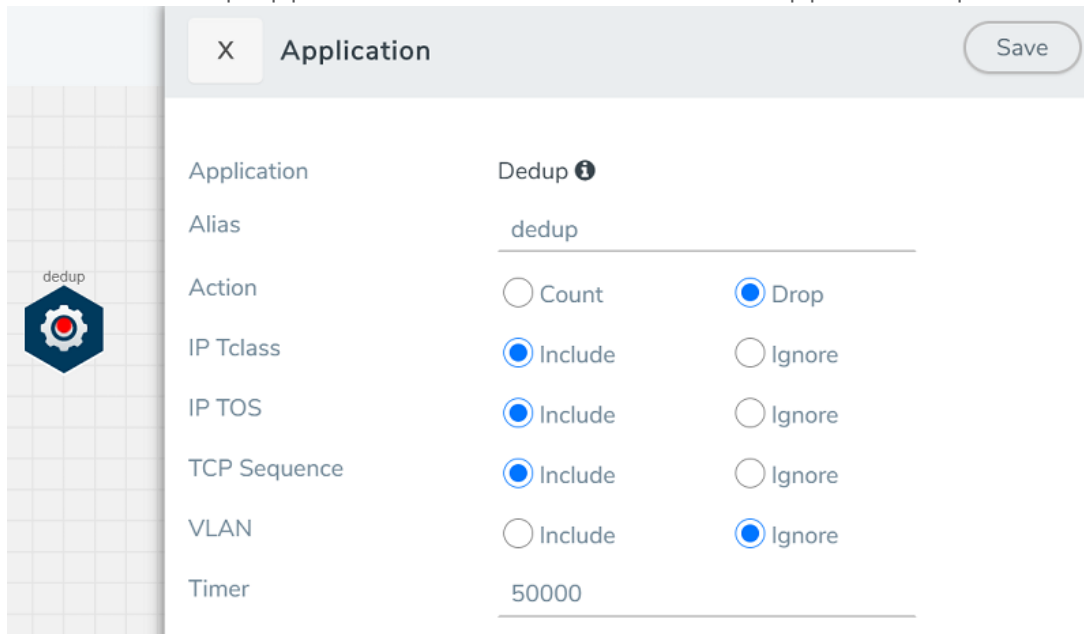
3. In the **DETAILS** tab of the Application quick view, enter the information as follows:

Parameter	Description
Alias	Enter a name for the masking application.
Action	Specifies whether duplicate packets are to be counted or dropped as follows: o **Count**– The de-duplication application counts the duplicate packets, but does not drop them. o **Drop**– The de-duplication application drops the duplicate packets. The default is drop.
IP Tclass IP TOS TCP Sequence VLAN	These options are useful when applying de-duplication operations to packets in a NAT environment. Different NAT implementations can change certain packet header fields (for example, the TCP sequence number). If you want to be able to detect duplicates without requiring that these fields match (ToS field, TCP sequence number, VLAN ID), you can disable the corresponding option. o **IP Tclass** – Ignore or include IPv6 traffic class. Use for IPv6. The default is include. o **IP TOS** – Ignore or include the IP ToS bits when detecting duplicates. Use for IPv4. The default is include. o **TCP Sequence** – Ignore or include the TCP Sequence number when detecting duplicates. The default is include. o **VLAN** – Ignore or include the VLAN ID when detecting duplicates. The default is ignore. Include means the field will be included when the application compares packets. Ignore means the field will be ignored when the application compares packets.
Timer <Value: 10-500000 µs>	Configures the time interval within which an identical packet will be considered a duplicate. The greater the interval over which traffic can be checked for duplicates, the higher the accuracy of the de-duplication detection and subsequent elimination. The default is 50,000µs. For example, if two same packets are seen in the specified time interval, the packets will be detected as duplicates. If one packet is seen in the time interval and another packet is seen in a later time interval, the packets will not be detected as duplicates. **NOTE:** Retransmissions are not counted as duplicates.

4. Click **Save**.

De-duplication application is successfully configured.

What's Next

You can configure the traffic health monitoring for this application in the **THRESHOLDS** tab. You can select an existing template from the Threshold Templates drop-down menu or provide the threshold values. For more details on Traffic health monitoring and how to

create threshold template, refer to Traffic Health Monitoring section in the respective cloud deployment guides.

You can view the configuration health status and the traffic health status of the application in the **HEALTH STATUS** tab. For more details on configuration health and traffic health, refer to Monitor Cloud Health section in the respective cloud deployment guides.

You can view the statistics of the application in the **STATISTICS** tab.

Distributed De-duplication

In distributed de-duplication, when you set up a monitoring session with a de-duplication app, the traffic is first sent to a component which distributes the traffic based on a consistent mechanism to ensure that packets from a particular traffic go to the same de-duplication instance. The packets are shared across the GigaVUE V Series Nodes. The distributed de-duplication more efficient that the existing de-duplication.

From version 6.5, distributed de-duplication is supported on Azure, AWS and, GCP. An enhanced configuration profile for the load balancer will be set by default with no option for modification. The default profile will use source and destination IP addresses, source and destination ports as the configuration for calculating the hash value for traffic distribution.

Important:

1. False traffic health alarms could be raised due to distribution of traffic across GigaVUE V Series Nodes.

2. Statistics are displayed for all the applications. Distributed De-duplication requires additional entities which will be listed in statistics page.

GENEVE De-encapsulation

The GENEVE De-encapsulation application is used to acquire and strip GENEVE headers. To route the traffic through the third-party network appliances seamlessly, the AWS gateway load balancer with a VPC adds GENEVE header to packets as they are forwarded to a third-party network appliance. Each appliance is expected to terminate the GENEVE tunnel and process the GENEVE encapsulated traffic traffic. When the GigaVUE-FM directs the acquisition of the customer traffic, the packets are encapsulated and forwarded as GENEVE tunnels that are terminated in GigaVUE V Series nodes.

To add a GENEVE application:

1. Drag and drop **GENEVE** from **APPLICATIONS** to the graphical workspace.
2. Click the GENEVE application and select **Details**. The Application quick view appears.
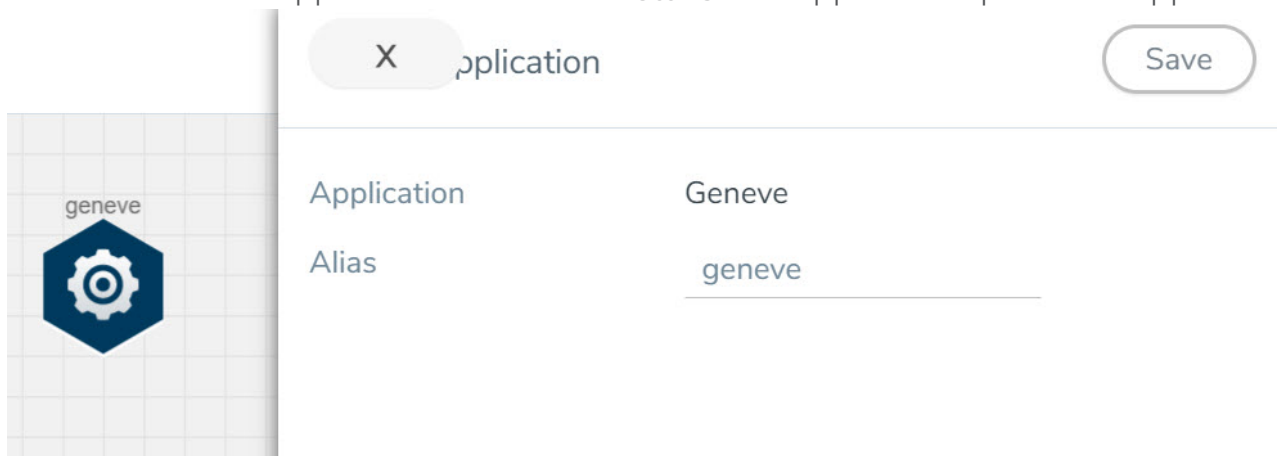
3. Enter an alias for the GENEVE application.
4. Click **Save**.

Header Stripping

Header Stripping application efficiently examines the packets for specified headers like GTP, ISL, ERSPAN, MPLS, MPLS+VLAN, VLAN, VN-Tag, VXLAN, FM6000Ts, and generic and removes them before sending the packet to the appropriate security and analysis tools. Each packet is examined for the packet forwarding addition and it also ensured that the headers are removed from the packet before sending the packet to the tools. This application is useful when working with tools that either cannot recognize these headers or have to engage in additional processing to adjust for them.

Furthermore, the presence of the protocols like GTP, ISL, ERSPAN, MPLS, MPLS+VLAN, VLAN, VN-Tag, VXLAN, and FM6000Ts in the packet can restrict or limit the ability to apply filtering and flow-based load balancing to the traffic as it is forwarded to specific tools. To address each of these challenges, header stripping of these protocols is required.

List of Protocols that are supported for stripping:

- GTP
- ISL
- ESPRAN
- MPLS
- MPLS+VLAN
- VLAN
- VN-Tag
- VXLAN
- FM6000Ts,
- Generic

Configure Header Stripping Application

To configure the header stripping application, follow the steps given below:

1. Drag and drop **Header Stripping** from **APPLICATIONS** to the graphical workspace.
2. Click the Header Stripping application and select **Details**. The Application quick view appears.

3. In the application quick view enter the following details:

Field	Description
Alias	Enter the alias name for the application
Protocol	Select the type protocol
VLAN: Use this option to strip VLAN header form the packets. You can strip only the outer VLAN header or the entire VLAN header. When choosing VLAN as your protocol for stripping, enter the following details	
VLAN Header	The VLAN Header that should be stripped. The supported minimum value is 0 and the maximum value is 16777215. The default value is 0.
VXLAN: Use this option to strip VXLAN (Virtual eXtensible Local Area Network) headers. You can strip either matching VXLAN headers or all VXLAN headers. When choosing VXLAN as your protocol for stripping, enter the following details	
VXLAN ID	The VXLAN ID that should be stripped. the default value is outer.
FM6000Ts: Use this option to strip FM6000Ts time stamp headers. Packets entering the application from other devices may contain FM6000 timestamps. FM6000 is an Intel chip used for timestamping. FM6000 has a hardware timestamp in the packet. When choosing FM6000Ts as your protocol for stripping, enter the following details.	
Time Stamp Format	The format of the time stamp you wish to be strip. Only the **None** format is supported.
ESPRAN: Use this option to strip ERSPAN Type II and Type III headers. When choosing ESPRAN as your protocol for stripping, enter the following details	
ESPRAN FlowID	Specify an ERSPAN flow ID, from 0 to 1023. A flow ID of zero is a wildcard value that matches all flow IDs.

Generic: Using this option to strip any header without having to worry about at which level header would occur. When choosing generic as your protocol for stripping, enter the following details	
Ah1	The anchor header (AH1) after which the header to be stripped is occurred.
Offset	Based on the offset selected the enter the following details:
	1. **Offset Range**: If you wish to use offset range as your offset then enter the following details:
	a. Offset Range Value: Offset of the header occurrence from the above anchor header. The minimum supported value is 1 and the maximum supported value is 1500.
	b. Header Count: Specifies how many headers from the offset, the application should remove. The minimum supported value is 1 and the maximum is 32.
	c. Custom Len: The length (in bytes) of the header that should be stripped.
	d. Ah2: The next possible standard header that occurs immediately after the header
	2. **Start / End**: If you wish to use start or end as your offset then enter the following details:
	a. Header Count: Specifies how many headers from the offset, the application should remove. The minimum supported value is 1 and the maximum is 32.
	b. Custom Len: The length (in bytes) of the header that should be stripped. The minimum supported value is 1 and the maximum supported value is 1500.
	c. Ah2: The next possible standard header that occurs immediately after the header

4. Click **Save**.

Header Stripping application is successfully configured.

What's Next

You can configure the traffic health monitoring for this application in the **THRESHOLDS** tab. You can select an existing template from the Threshold Templates drop-down menu or provide the threshold values. For more details on Traffic health monitoring and how to create threshold template, refer to Traffic Health Monitoring section in the respective cloud deployment guides.

You can view the configuration health status and the traffic health status of the application in the **HEALTH STATUS** tab. For more details on configuration health and traffic health, refer to Monitor Cloud Health section in the respective cloud deployment guides.

You can view the statistics of the application in the **STATISTICS** tab.

Load Balancing

Load balancing application performs stateless distribution or Enhanced Load Balacing of the packets between different endpoints. Stateless load balancing distributes the processed traffic to multiple tool ports or tunnel endpoints based on hash values generated from predefined protocol fields in the packet.

When Enhanced Load Balancing is enabled and an endpoint fails, the traffic is redistributed for the failed endpoint. When the failed endpoint recovers, the redistributed traffic is restored to the recovered endpoint. The traffic across other endpoints remain undisturbed during this process.

To add a load balancing application:

1. Drag and drop **Load Balancing** from **APPLICATIONS** to the graphical workspace.
2. Click the load balancing application and select **Details**. The Application quick view appears.

3. In the Application quick view, enter the information as follows:

Metric	Description
Alias	Enter a name for the load balancing application
Stateless	Select this option to enable Stateless Load Balancing
Enhanced Load Balancing	Select this option to enable Enhanced Load Balancing and select the ELB profile.
Hash Field	• **ipOnly** : The source IP and destination IP addresses. • **ipAndPort**: The source IP and destination IP addresses, and Layer 4 source port and destination port numbers. • **fiveTupl**e: The source IP and destination IP addresses, source port and destination port numbers, and protocol field in the IP header. • **gtpuTeid**: The GTP-u tunnel identifier (ID). **NOTE:** There is no inner or outer field location for `GTPU-TEID`.
Field Location	• **Outer**: The first occurrence of header or field. For example, **IP Only outer** is the first IP header in the packet, which could be IPv4 or IPv6. • **Inner**: The second occurrence of header or field. The supported IP encapsulation types are: IP-in-IP, VXLAN, GTP, GRE, and ERSPAN.
Load balancing groups	Add or remove an application with the Endpoint ID and Weight value (1-100). A load balancing group can have minimum of two endpoints.

4. Click **Save**.

> **NOTE:** When you configure the Load Balancing Application in enhanced mode, you can associate it with only a single enhanced load balancing profile. However, you have the flexibility of changing the association to different profile as needed.

Load Balancing application is successfully configured.

What's Next

You can configure the traffic health monitoring for this application in the **THRESHOLDS** tab. You can select an existing template from the Threshold Templates drop-down menu or provide the threshold values. For more details on Traffic health monitoring and how to create threshold template, refer to Traffic Health Monitoring section in the respective cloud deployment guides.

You can view the configuration health status and the traffic health status of the application in the **HEALTH STATUS** tab. For more details on configuration health and traffic health, refer to Monitor Cloud Health section in the respective cloud deployment guides.

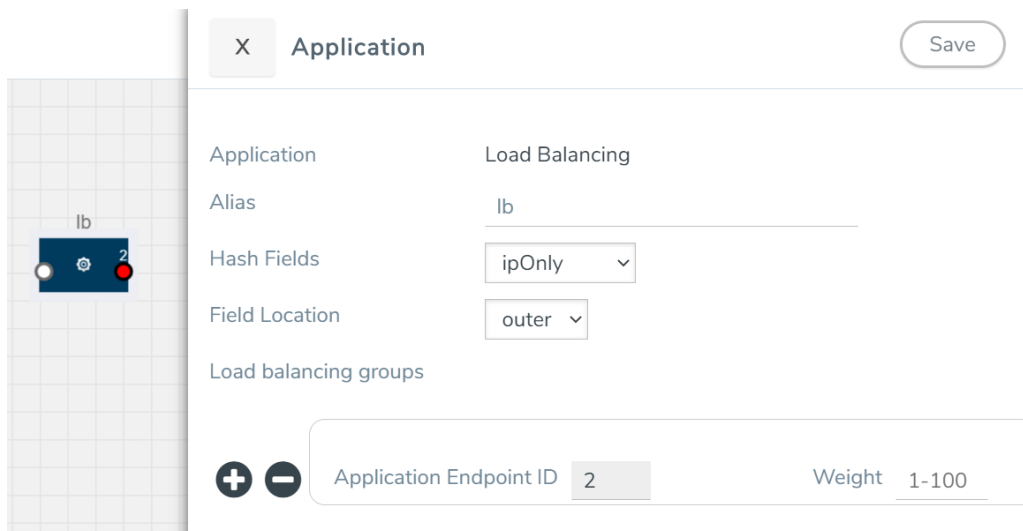You can view the statistics of the application in the **STATISTICS** tab.

Enhanced Load Balancing

Enhanced Load Balancing redistributes the traffic from a failed endpoint to another endpoint which is a part of the ELB group. When the failed endpoint recovers, the redistributed traffic is restored to the recovered endpoint. The traffic across other endpoints remain undisturbed during this process. Hashing is performed on the packets based on outer and/or inner headers.

To enable to enhanced load balancing application:

1. Create an Enhanced Load Balancing Profile.

    a. In the Monitoring domain page, click Settings, then click **Enhanced Load Balancing**

    b. Click **New** and then create a profile.

Fields	Values
Hash fields	The various hash options are
	ip
	ip-src
	ip-dst
	l4-port
	l4-portsrc
	l4-portdst
	gtputeid
Position	Select either inner/outer location of the hash field to be matched with the incoming packet..
Hash-mask	When the hash-fields ip-src/ip-dst are defined along with the IP, then ip-src/ip-dst hash-mask will overwrite the IP hash mask. For load balancing, you must apply this mask before hashing the IP.
	The default options and their default values are:
	IPv4 : 255.255.255.255
	IPv6 :FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF

2. Go to monitoring session page and

   a. Drag and drop **Load Balancing** from **APPLICATIONS** to the graphical workspace.

   b. Click the load balancing application and select **Details**. The Application quick view appears.

c. In the Application quick view, enter the information as follows:

Metric	Description
Alias	Enter a name for the load balancing application
Enhanced Load Balancing	Select this option to enable Enhanced Load Balancing and select the ELB profile.
Load balancing groups	Add or remove an application with the Endpoint ID and Weight value (1-100). A load balancing group can have minimum of two endpoints.

3. Click **Save**.

> **NOTE:** When you configure the Load Balancing Application in enhanced mode, you can associate it with only a single enhanced load balancing profile. However, you have the flexibility of changing the association to different profile as needed.

Masking

Masking lets you overwrite specific packet fields with a specified pattern so that sensitive information is protected during network analysis. Masking operations consist of an **offset**, **length**, and **pattern**.

To add a masking application:

1. Drag and drop **Masking** from **APPLICATIONS** to the graphical workspace.
2. Click the Masking application and select **Details**. The Application quick view appears.

3. In the Application quick view, enter the information as follows:

Component	Description
Alias	Enter a name for the masking application.
Protocol	The following are the protocols that you can select from the protocol drop-down list: o **None** – Mask starting a specified number of bytes from the start of the packet. o **IPV4** – Mask starting a specified number of bytes after the IPv4 header. o **IPV6** – Mask starting a specified number of bytes after the IPv6 header. o **UDP** – Mask starting a specified number of bytes after the UDP header. o **TCP** – Mask starting a specified number of bytes after the TCP header. o **ftp-data**– Identify using TCP port 20. Mask payloads using offset from the TCP header. o **HTTPS** – Identify using TCP port 443. Mask payloads using offset from the TCP header. o **SSH** – Identify using TCP port 22. Mask payloads using offset from the TCP header. o **GTP** – Mask starting a specified number of bytes after the outer GTP header. o **GTP-IPV4** – Mask starting a specified number of bytes after the IPv4 header inside the encapsulating GTP packet. o **GTP-UDP** – Mask starting a specified number of bytes after the UDP header inside the encapsulating GTP packet. o **GTP-TCP** – Mask starting a specified number of bytes after the TCP header inside the encapsulating GTP packet.
Offset	Specifies **where** the application should start masking data with the supplied pattern. You can specify this in terms of either a static offset from the start of the packet or a relative offset from a particular protocol layer. This lets you automatically compensate for variable length headers, specifying a mask target in terms of a particular packet header.
Length	Specifies **how much** of the packet should be masked. The specified one-byte pattern can be repeated to mask from 1-9600 bytes.
Pattern	Specifies **what** pattern the application should use to mask the specified portion of the packet. You can specify a one-byte hex pattern (for example, 0xFF).

4. Click **Save**.

Masking application is successfully configured.

What's Next

You can configure the traffic health monitoring for this application in the **THRESHOLDS** tab. You can select an existing template from the Threshold Templates drop-down menu or provide the threshold values. For more details on Traffic health monitoring and how to create threshold template, refer to Traffic Health Monitoring section in the respective cloud deployment guides.

You can view the configuration health status and the traffic health status of the application in the **HEALTH STATUS** tab. For more details on configuration health and traffic health, refer to Monitor Cloud Health section in the respective cloud deployment guides.

You can view the statistics of the application in the **STATISTICS** tab.

SSL Decrypt

License: For information on licensing, refer to the Volume Based License (VBL) section.

SSL Decrypt application delivers decrypted traffic to out-of-band tools that can then detect threats entering the network. Secure Socket Layer (SSL) is a cryptographic protocol that adds security to TCP/IP communications such as Web browsing and email. The protocol allows the transmission of secure data between a server and client who both have the keys to decode the transmission and the certificates to verify trust between them.

SSL encryption secures traffic between a client and a server, such as a Web server. SSL decryption uses keys to decode the traffic between the client and server.

SSL and Transport Layer Security (TLS) protocols consist of a set of messages exchanged between a client and server to set up and tear down the SSL connection between them. To set up the connection, the client and server use the Public Key Infrastructure (PKI) to exchange the bulk encryption keys needed for data transfer.

> **IMPORTANT:** To use SSL Decrypt application in GigaVUE-FM 6.3.00, install new GigaVUE-FM 6.3.00 image. Refer to *GigaVUE-FM Installation and Upgrade Guide* for step-by-step instructions on how to install GigaVUE-FM. SSL Decrypt application does not work if you upgrade from any previous GigaVUE-FM version to GigaVUE-FM 6.3.00.

Keep in mind the following when using SSL Decrypt application:

1. On updating the keys, service, or key maps which are already used in a monitoring session, the monitoring session is dynamically updated, and you need not re-deploy the monitoring session. You can also see if the updated keys, services, or key maps were successfully updated to the monitoring session and the respective GigaVUE V Series Nodes on the **All Events** page. Refer to Overview of Events section in the *GigaVUE Administration Guide* for detailed information on Events.

2. When deleting a key that is part of a Key Map and that Key Map is used in a monitoring session which is already deployed, then the key will be removed from the Key Map. If that key is the only available entry in the Key Map, then it will not be removed.

3. When deleting a key that is part of a Key Map and that Key Map is used in a monitoring session that is not deployed, then the key will be removed from the Key Map and if that key is the only available entry in the Key Map, the whole key map will be removed from the monitoring session.

4. When deleting a service that is part of a Key Map and that Key Map is used in a monitoring session which is already deployed, then the service will be removed from the Key Map. If that service is the only available entry in the Key Map, then it will not be removed.

5. When deleting a service that is part of a Key Map and that Key Map is used in a monitoring session which is not deployed, then the service will be removed from the Key Map and if that service is the only available entry in the Key Map, the whole key map will be removed from the monitoring session.

6. In VMware NSX-T platform, the throughput of SSL Decrypt application is improved to 480 Mbps.

Refer to the following topics for more detailed information:

- Supported Protocols, Algorithms, and Ciphers for SSL Decrypt
- Configure SSL Decrypt

Supported Protocols, Algorithms, and Ciphers for SSL Decrypt

The supported protocols are as follows:

- SSL 3.0
- TLS 1.0
- TLS 1.1
- TLS 1.2

The supported authentication (Au) is as follows:

- RSA

The supported key exchange (Kx) is as follows:

- RSA

The supported encryption algorithms (Enc) are as follows:

- NULL
- RC4
- DES
- 3DES
- AES (including GCM mode)
- CAMELLIA
- SEED
- IDEA

The supported compression algorithm is as follows:

- NULL

The supported digest algorithms are as follows:

- MD5

- SHA1
- SHA2

The supported key sizes are 128, 256, 512, 1024, 2048, and 4096.

The supported TLS extensions are as follows:

- Extended Master Secret, RFC 7627
- Encrypt-then-MAC, RFC 7366

The following table lists the supported ciphers:

Table 1: Supported Ciphers forSSL Decrypt

Cipher Name	Kx	Au	Enc	Bits	Mac
TLS_RSA_WITH_NULL_MD5	RSA	RSA	NULL	0	MD5
TLS_RSA_WITH_NULL_SHA	RSA	RSA	NULL	0	SHA
TLS_RSA_EXPORT_WITH_RC4_40_MD5	RSA_EXPORT	RSA_EXPORT	RC4_40	40	MD5
TLS_RSA_WITH_RC4_128_MD5	RSA	RSA	RC4_128	128	MD5
TLS_RSA_WITH_RC4_128_SHA	RSA	RSA	RC4_128	128	SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5	RSA_EXPORT	RSA_EXPORT	RC2_CBC_40	40	MD5
TLS_RSA_WITH_IDEA_CBC_SHA	RSA	RSA	IDEA_CBC	128	SHA
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA	RSA_EXPORT	RSA_EXPORT	DES40_CBC	40	SHA
TLS_RSA_WITH_DES_CBC_SHA	RSA	RSA	DES_CBC	56	SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA	RSA	RSA	3DES_EDE_CBC	168	SHA
TLS_RSA_WITH_AES_128_CBC_SHA	RSA	RSA	AES_128_CBC	128	SHA
TLS_RSA_WITH_AES_256_CBC_SHA	RSA	RSA	AES_256_CBC	256	SHA
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	RSA	RSA	CAMELLIA_128_CBC	128	SHA
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	RSA	RSA	CAMELLIA_256_CBC	256	SHA
TLS_RSA_WITH_SEED_CBC_SHA	RSA	RSA	SEED_CBC	128	SHA
TLS_RSA_WITH_NULL_SHA256	RSA	RSA	NULL	0	SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256	RSA	RSA	AES_128_CBC	128	SHA256

Cipher Name	Kx	Au	Enc	Bits	Mac
TLS_RSA_WITH_AES_256_CBC_SHA256	RSA	RSA	AES_256_CBC	256	SHA256
TLS_RSA_WITH_AES_128_GCM_SHA256	RSA	RSA	AES_128_GCM	128	SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384	RSA	RSA	AES_256_GCM	256	SHA384

All algorithms used for SSL Decrypt application are FIPS 140-2 compliant.

All key URLs must point to an RSA private key stored in the PEM or PKCS12 format, as follows:

- http://keyserver.domain.com/path/keyfile.pem
- https://keyserver.domain.com/path/keyfile.pem
- ftp://keyserver.domain.com/path/keyfile.pem
- tftp://keyserver.domain.com/path/keyfile.pem
- scp://username[:password]@keyserver.domain.com/path/keyfile.pem

The supported applications are as follows:

- HTTPS
- FTPS
- SMTP, IMAP, and POP3 with StartTLS

Configure SSL Decrypt

To configure SSL Decrypt Application using GigaVUE-FM follow the steps given below:

- Upload SSL Keys
- Create SSL Service
- Key Mapping
- SSL Key Store
- Add SSL Decrypt to Monitoring Session

Upload SSL Keys

To upload an SSL private key, do the following:

1. Go to **Inventory > Resources > Security > SSL Keys**.
2. Click **Add**. The **Create SSL Key** page appears.
3. Enter the following details:

Field	Description
Key Alias	Enter a name for the key.
Comment	Enter a description
Key Type	Select the either of the key type:
PEM	
PassPhrase (optional)	SSH passphrases allows you to protect your private key from being used with out the passphrase. Enter the passphrase created with the private key.
SSL Key Store	Enter the SSL Key Store in which the Key is stored.
Private key	Enter the Private Key using any of the following options: • Copy and Paste • Install from URL • Install from Local Directory
Certificate	Enter the Certificate using any of the following options: • Copy and Paste • Install from URL • Install from Local Directory
PKCS12	
PassPhrase	SSH passphrases allows you to protect your private key from being used with out the passphrase. Enter the passphrase created with the private key.
SSL Key Store	Enter the SSL Key Store in which the Key is stored.

4. Click **Save**.

> **NOTE:** SSL Decrypt application does not support HSM.

The following actions can also be performed from the SSL Keys Page:

Field	Description
Edit	To edit a SSL Key, select the key from the list in the SSL Keys page and click the **Edit** button.
Delete	To delete a SSL Key, select the key from the list in the SSL Keys page and click the **Delete** button.
Delete all	Use this button to delete all the SSL Keys in the SSL Keys page.
View certificate	To view the certificate associated with the particular SSL Key, select the key from the list in the SSL Keys page and click the **View Certificate** button.

Create SSL Service

After uploading a private key, you can add a service. A service maps to a physical server, such as an HTTP server. One server can run multiple services. A service is a combination of an IP address and a server port number.

Prerequisite

Before creating a service, upload a private key as described in Upload SSL Keys

To create a SSL service, do the following:

1. Go to **Inventory > Resources > Security > SSL Service**. The SSL Services page appears.
2. Click **Add**. The **Create SSL Service** page appears.
3. On the Create SSL Service page, enter the following details:

Field	Description
Alias	Enter a name for the SSL Service.
Default Service	Enable this to use default service.
Server IP Address	Enter the IP address of the server in which the service runs.
Server Port	Enter the port number of the server.

4. Click **Save**.

The following actions can also be performed from the SSL Service Page:

Field	Description
Edit	To edit a SSL Service, select the service from the list in the SSL Service page and click the **Edit** button.
Delete	To delete a SSL Service, select the service from the list in the SSL Service page and click the **Delete** button.
Delete all	Use this button to delete all the SSL Service in the SSL Service page.

Key Mapping

After adding the SSL Service, now you map the private key with the service using Key Mapping.

To map a key with the service, follow the steps given below,

1. Go to **Inventory > Resources > Security > SSL Key Mapping**. The SSL Key Mapping page appears.
2. Click **Add**.

3. Enter the Key Mapping Alias.
4. Select the SSL Service and Key Alias from the drop-down.
5. Click **Save**.

The following actions can also be performed from the SSL Keys Page:

Field	Description
Edit	To edit a SSL Service, select the service from the list in the SSL Service page and click the **Edit** button.
Delete	To delete a SSL Service, select the service from the list in the SSL Service page and click the **Delete** button.
Delete all	Use this button to delete all the SSL Service in the SSL Service page.

SSL Key Store

SSL Key Store is a repository, that allows you to save all the key under a single location. You can create multiple key stores and in each key store you can store multiple keys.

1. Go to **Inventory > Resources > Security > SSL Key Store**. The SSL Key Store page appears.
2. Click **Add**.
3. Enter the **Key Store Alias** and **Comment**.
4. Click **Save**.

The following actions can also be performed from the SSL Key Store Page:

Field	Description
Edit	To edit a SSL Key Store, select the Key Store from the list in the SSL Key Store page and click the **Edit** button.
Delete	To delete a SSL SSL Key Store, select the SSL Key Store from the list in the SSL Key Store page and click the **Delete** button.
Delete all	Use this button to delete all the SSL Key Store in the SSL Key Store page.

Add SSL Decrypt to Monitoring Session

After mapping your keys with service, to add GigaSMART applications to GigaVUE V Series Node, follow the steps given below,

1. Drag and drop **SSL Decrypt** from APPLICATIONS to the graphical workspace.
2. Click the SSL Decrypt application and select **Details**.

X	...pplication

Application	SSL Decrypt
Alias	ssl-decrypt
Enable	☑
Key Map	⌄
In Port ⓘ	0
Out Port ⓘ	0
Session Timeout (sec)	300
Pending Session Timeout (sec)	60
Tcp Syn Timeout (sec)	20
Decrypt Fail Action	○ Pass ● Drop
Key Cache Timeout (sec)	10800
Ticket Cache Timeout (sec)	10800
Non-ssl Traffic	○ Pass ● Drop

ssl-decrypt

Save
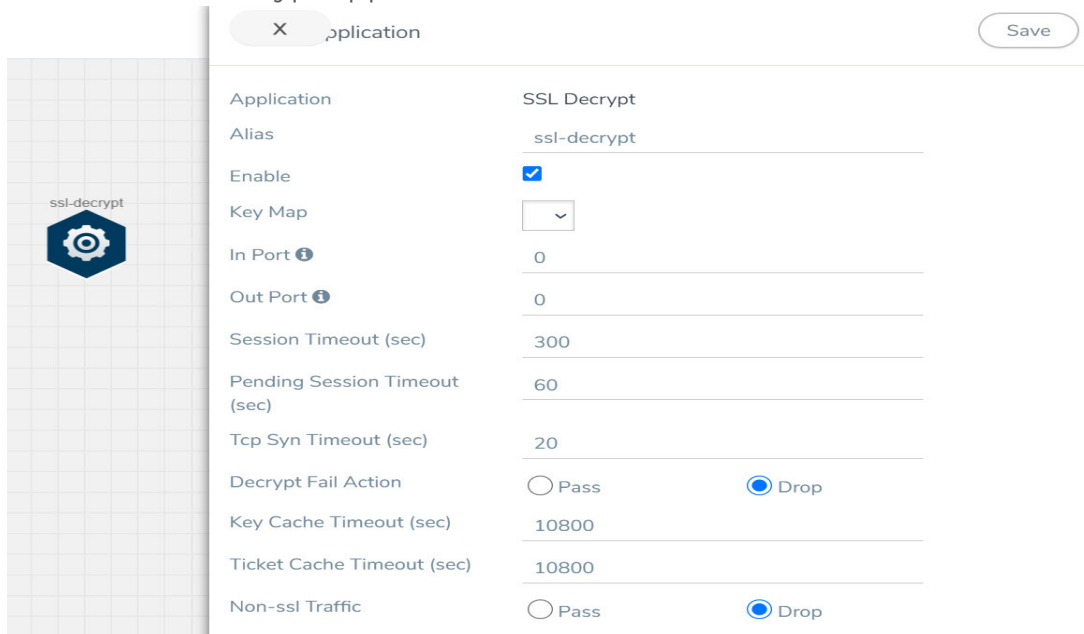
3. Enter the following details in the Application quick view:

Fields	Description
Alias	Enter the alias name for the application.
Enable	Enable the box to enable SSL Decryption.
Key Map	Select the Key Map from the list of available Key Maps. Refer to Key Mapping for more details on how to map the key to SSL Service.
In Port	Enter the source port number from which the traffic should be fetched.
Out Port	Enter the destination port number to which the decrypted traffic should be delivered.
Session Timeout	Enter the value in seconds after which the session should be timeout. The default value is 300 seconds.
Pending Session Timeout	Enter the value in seconds after which the session must timeout if the session is in pending state
Tcp Syn Timeout	Enter the value in seconds after which the session must timeout when the session does not synchronize TCP.
Decrypt Fail Action	Select **Pass** to allow the traffic to pass through the application when the decryption fails and select **Drop** to drop the traffic before passing through the application when the decryption fails.
Key Cache Timeout (sec)	Enter the value in seconds until which the key cache information can be reused for resumption.
Ticket Cache Timeout (sec)	Enter the value in seconds until which the ticket cache information can be reused for resumption.
Non-ssl Traffic	Select **Pass** to allow the non-SSL traffic to pass through the application and select **Drop** to drop the non- SSL traffic before passing through the application.

4. Click **Save**.
5. Click **Deploy**. The Select nodes to deploy the monitoring session page appears.
6. Select the GigaVUE V Series Nodes you want to deploy and select an interface for each GigaVUE V Series Node. Then, click **Deploy**.

The SSL Decrypt application is successfully configured.

What's Next

You can configure the traffic health monitoring for this application in the **THRESHOLDS** tab. You can select an existing template from the Threshold Templates drop-down menu or provide the threshold values. For more details on Traffic health monitoring and how to create threshold template, refer to Traffic Health Monitoring section in the respective cloud deployment guides.

You can view the configuration health status and the traffic health status of the application in the **HEALTH STATUS** tab. For more details on configuration health and traffic health, refer to Monitor Cloud Health section in the respective cloud deployment guides.

You can view the statistics of the application in the **STATISTICS** tab.

You can view the session summary and session details of the SSL Decryption application in the the **SESSIONS** tab. Select the **V Series Node IP** and enter the **Server Name**, **Client/ Server IP address**, and **Subnet Mask**. Then, click **Apply** to view the session summary and session details.

You can view the server certificate statistics in the **SERVER CERTIFICATES** tab. Select the **V Series Node IP** from the drop-down and enter the **Key Alias**. Then, click **Apply**.

All the service related details are displayed in the **SERVICES** tab. Select the **V Series Node IP** and **Service Alias** from the drop-down. Then, enter the **IP Address** and **Port**. Click **Apply**.

All the error codes and respective description are displayed in the **ERROR CODES** tab. To view the error code, select the **V Series Node IP** and **Service Alias** from the drop-down. Then, enter the **IP Address** and **Port**. Click **Apply**.

PCAPng Application

The PCAPng application reads the various blocks in the received PCAPng files and validates the blocks to be sent to the destination application or to the tools. The PCAPng file contains the following blocks:

- Mandatory Blocks
    - Section Header Block (SHB)

- Optional Blocks
    - Interface Description Block (IDB)
    - Enhanced Packet Block (EPB)
    - Simple Packet Block
    - Name Resolution Block
    - Interface Statistics Block

> **NOTE:** The PCAPng application is only applicable for the Ericsson 5G Core vTAP architecture. for detailed information.

The actual packets are present in the Enhanced Packet Block. The block data is parsed to find the start and end offset of the valid packets and the packet is sent out to the next application.

> **NOTE:** Only one EPB in a PCAPng file is supported.

The PCAPng application processes the data depending on the packet type that contains a combination of the blocks mentioned above:

Block Combination	Process
SHB+IDB+EPB+data	Packets are parsed, validated, and the data packet is sent out.
SHB+IDB	Packets are dropped.
EPB+Data	Packets are parsed, validated, and the data packet is sent out.

The PCAPng application validates if the incoming data matches any of the above three formats in the same order, and processes the packets accordingly.

The following figure shows a sample PCAPng file format that contains one section header block:
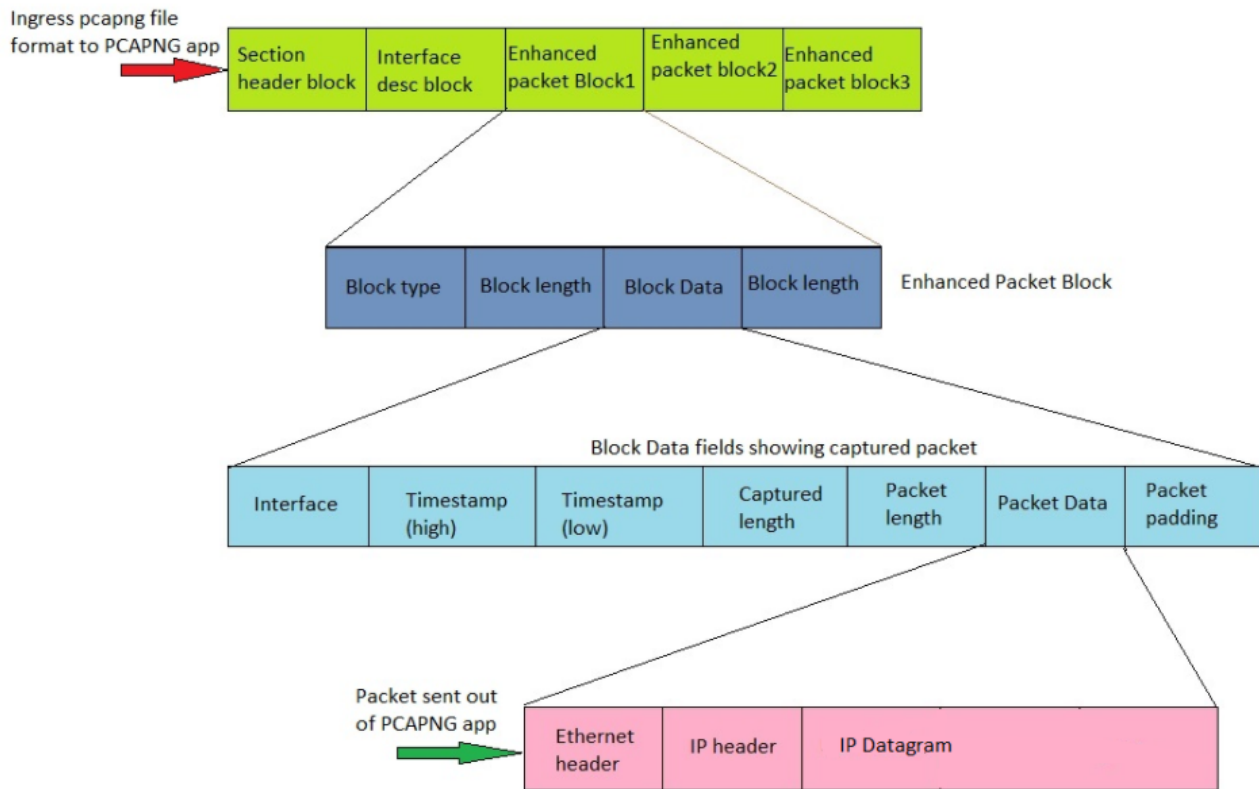
Create Link Between UDP-in-GRE Tunnel and PCAPng Application

To create a link with source as UDP-in-GRE tunnel and destination as PCAPng application:

1. In the GigaVUE-FM canvas, select **New > New Tunnel**, drag and drop a new tunnel template to the workspace. The **Add Tunnel Spec** quick view appears.
2. On the New Tunnel quick view, enter or select the required information as described in the following table.

Field	Description
Alias	The name of the tunnel endpoint **NOTE:** Do not enter spaces in the alias name.
Description	The description of the tunnel endpoint
Type	Select **UDPGRE** as the tunnel type
Traffic Direction	The direction of the traffic flowing through the V Series node • Choose **In** (Decapsulation) for creating an Ingress tunnel, traffic from the source to the V Series node
IP Version	The version of the Internet Protocol. Select IPv4 or IPv6
Remote Tunnel IP	The IP address of the tunnel source
Key	GRE key value
Source L4 Port	Layer 4 source port number
Destination L4 Port	Layer 4 destination port number. You can configure only 4754 or 4755 as the destination UDP ports

3. Click **Save**.
4. Click and drag the PCAPng application into the canvas. Configure the alias for the application.
5. Establish a link between the UDP-GRE TEP configured above and the PCAPng application.

Create Link Between PCAPng Application and Other Destinations

Create a link with source as PCAPng application and destination as one of the following:

- Other GigaSMART applications such as Slicing, Masking, etc.
- Other encapsulation TEPs.
- REP/MAP

Refer to the following image for a sample configuration.

What's Next

You can configure the traffic health monitoring for this application in the **THRESHOLDS** tab. You can select an existing template from the Threshold Templates drop-down menu or provide the threshold values. For more details on Traffic health monitoring and how to create threshold template, refer to Traffic Health Monitoring section in the respective cloud deployment guides.

You can view the configuration health status and the traffic health status of the application in the **HEALTH STATUS** tab. For more details on configuration health and traffic health, refer to Monitor Cloud Health section in the respective cloud deployment guides.

You can view the statistics of the application in the **STATISTICS** tab.

5G-Service Based Interface Application

5G-Core is a service-based architecture, in which many control plane network functions are available and communication across these network functions happens through HTTP2 protocol. These HTTP2 transactions are mirrored using some specific network functions, which are in JSON encoded format.

5G-Service Based Interface (SBI) Application synthesizes the HTTP2 transactions with proper L2, L3, and L4 headers from the JSON encoded data that it receives from the UDP-GRE or VXLAN ingress TEPs (Tunnel End Point). Once the headers are synthesized and a complete HTTP2 transaction is formed, the packets are sent to the egress TEP and then sent to the physical or virtual probes.

In Nokia 5G core network, the traffic is mirrored between control functions using HTTP2 protocol, which is mirrored from a service called SCP (Service Control Proxy) a centralised point through which all the communications between all the control plane functions pass. Hence, it becomes the right place to mirror the traffic.

Traffic mirrored here doesn't have enough information about the entire TCP flow information between them. It only has information about request and response details between the control functions. Since the tools cannot infer much with this request and response information alone, it is required to have the entire flow information from TCP handshake to TCP connection close to form a complete TCP flow information that can be sent to the tools.

In Ericsson 5G core, there is a software probe that is used for monitoring the traffic. It captures the traffic, encapsulates it in UDP-GRE, and forwards it to V Series nodes. Here it converts the HTTP2 transactions into JSON data and a set of TCP messages are captured as PCAPng file, which is encapsulated into UDP-GRE with proto ID 0x8047 and is sent to V Series.

In either case, these are not raw packets that any tools can understand. In the case of Nokia, it doesn't have TCP session information, whereas Ericsson has the session information, but they are in a JSON encoded format. In both cases, it can't be forwarded to tools directly. Hence, we need to synthesize those packets, by adding additional information, such as TCP 3-way handshake, L2 headers and form a TCP flow information that could be forwarded to the tools.

In some versions of Nokia or Ericsson 5G Cores, the IP addresses present in the encoded message is not reliable and the SBI application converts the strings in the form of instance ID (in case of Ericsson) or producer ID (in case of Nokia) to an IP address from the string-IP mapping table.

The instance ID or producer ID must be provided in the form of CSV file. You can upload the CSV file through GigaVUE-FM.
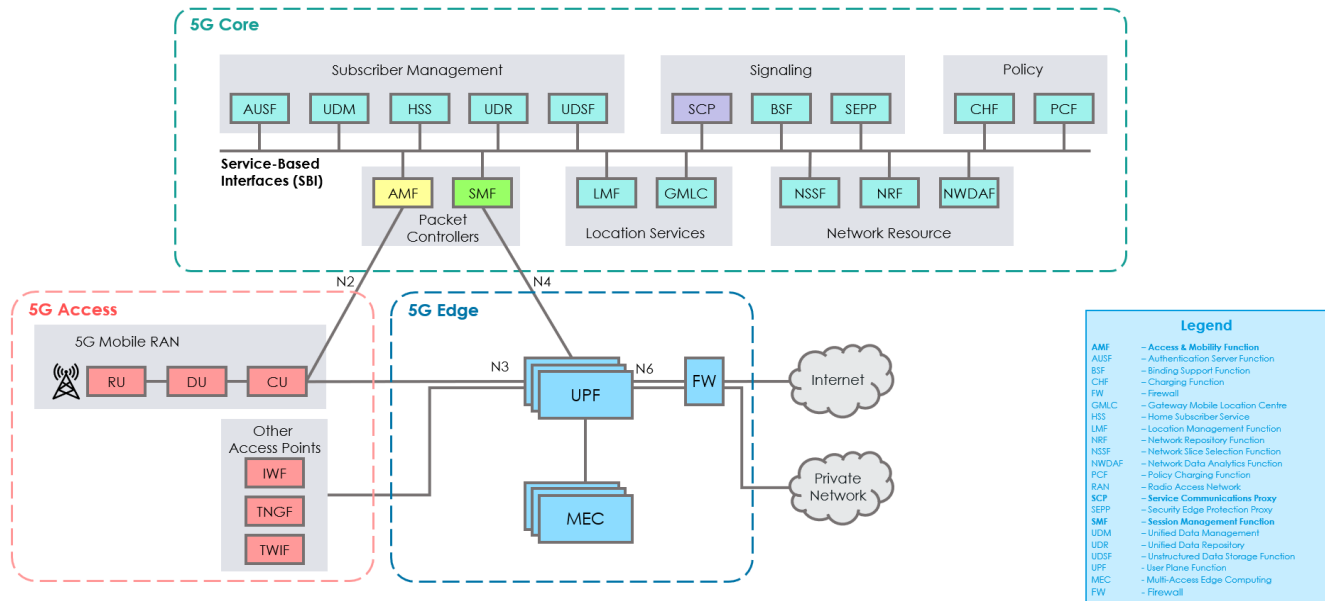
How SBI Application works

In the V series, the SBI application receives the HTTP2 transaction messages as JSON encoded data from any of the following sources:

- VxLAN TEP – In 5G-Nokia, the application receives the JSON encoded data from the VXLAN ingress TEPs
- PCAPng application - In 5G-Ericson, the application receives the JSON encoded data from the PCAPng application, whereas the PCAPng application receives the data from the UDP-GRE TEP.

In the SBI application, JSON encoded data traffic is further parsed to extract the source-destination information and is used to synthesize the complete HTTP2 transaction with proper L2, L3, and L4 headers and HTTP2 headers and HTTP2 body of the original HTTP2 transactions. Once the headers are synthesized and a complete HTTP2 transaction is formed, the packets are then given to the egress TEP to send it to the physical/virtual probes.

The following figure shows the block diagram of the data flow in the V Series containing the SBI application.
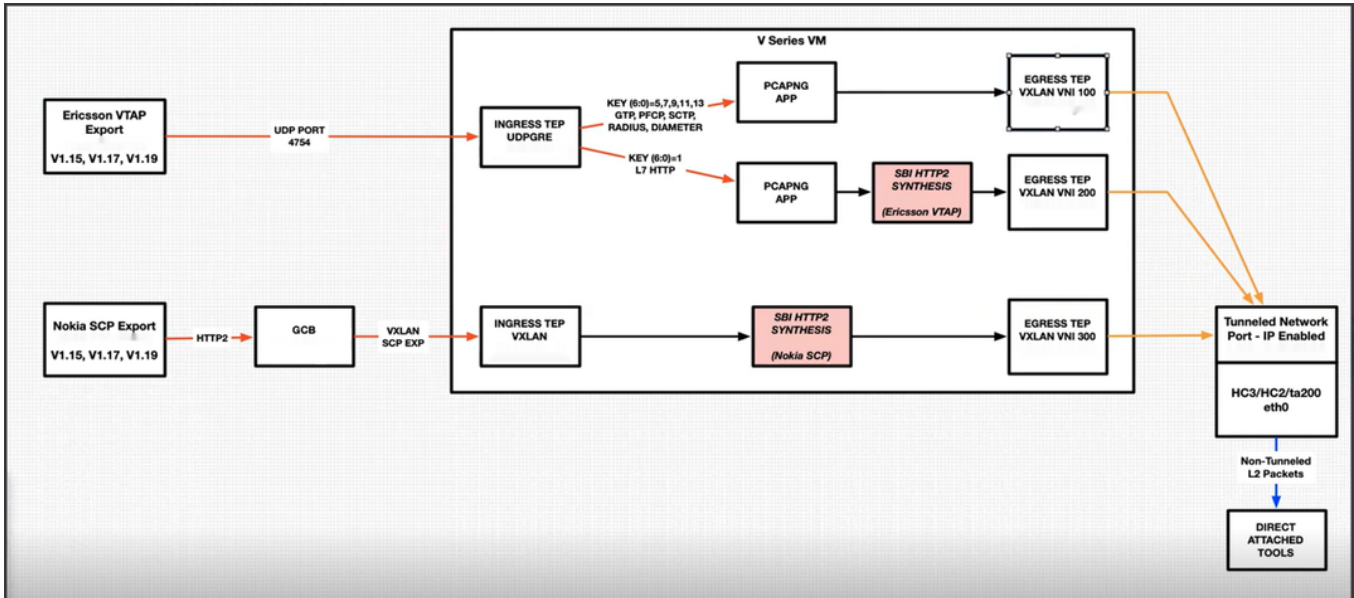
In 5G-SBI application, the V Series node can log the following details to CSV files:

- **Transaction details** - Represents the transaction or flow of request and response packets into the application. The details of the flow or transaction are recorded in the CSV file for 5 minutes or 60 minutes based on the configuration.

- **Flow statistics details** - Represents the packet and flow statistics in 60 seconds time interval.

These files help you to understand the records or traffic efficiently. The files are named as per the date and time in which the files were created. When the number of files and its size grows, the application automatically detects the old files and delete them.

Supported Platforms:

The application is supported on the following platforms:

- VMware
- OpenStack

Rules and Notes

- The maximum number of HTTP2 headers (in the synthesized HTTP2 transactions) that is supported is 64.

- The PCAPng application that is linked to 5G-SBI application (on the right side) should only be linked to UDP-GRE TEP with key value 1 on the left side. If it is linked to other UDP-GRE TEPs(key values other than 1), then the behavior cannot be defined and leads to unexpected result.
- The maximum number of NF entries supported is 4K.

Configuration of 5G-SBI Application

In V Series, 5G-SBI application receives all the mirrored traffic from any of the following sources:

- 5G-Nokia SCP
- 5G-Ericsson

In GigaVUE-FM, the application has a field **type**, which determines whether the data is collected from 5G-Nokia or 5G-Ericsson. Based on the **type** configured, the packets received are processed.

For example, in the case of 5G-Nokia this application reads the headers (source ip/port, destination ip/port), packet type (request or response) information from the HTTP2 message. Based on the retrieved information it synthesises a TCP flow.

In the case of 5G-Ericsson, after receiving the packets from the TEP, the packets are forwarded to PCAPng application for parsing. After parsing, the JSON type data from PCAPng has the information such as source ip/port, destination ip/port, message type. Using this information HTTP2 transaction can be synthesised.

In GigaVUE-FM, to configure the 5G-SBI application refer to any of the following sections based on the source type:

- Configuration of 5G-SBI Application for 5G-Nokia
- Configuration of 5G-SBI Application for 5G-Ericsson

Configuration of 5G-SBI Application for 5G-Nokia

In GigaVUE-FM, for 5G-Nokia, you must do the following to add the 5G-SBI application in the monitoring session of a monitoring domain in the V Series:

S.No	Steps	Refer to
1	Create VXLAN Ingress TEP to receive the HTTP2 post messages from GCB/UCT in a monitoring session.	Create Tunnel Endpoints
2	Add 5G-SBI Application (HTTP2 header synthesis) in the monitoring session.	

3	Create a link between VXLAN ingress TEP and 5G-SBI Application.	
4	Create egress TEP.	Create Tunnel Endpoints
5	Create a link between 5G-SBI Application (HTTP2 header synthesis) and Egress TEP.	
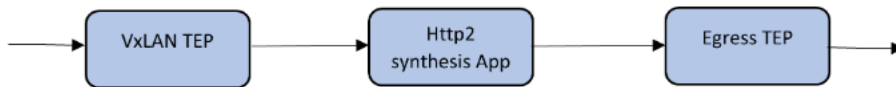
Adding 5G-SBI Application in 5G-Nokia

Prerequisites

The pre-requisite to add a 5G-SBI application in 5G-Nokia is:

- You must upload CSV file containing a valid FQDN name and a valid IPv4/IPv6 address. To upload the CSV file refer Adding CSV file for IP Mapping.

You can add a 5G-SBI application for:

- New monitoring session - You can add the 5G-SBI application after creating a new monitoring session and when the canvas appears.
- Existing session - Click **Edit** on existing monitoring session, the GigaVUE-FM canvas appears.

To add a 5G-SBI application:

1. In the canvas, Drag and drop 5G-SBI application and select **Details**. The Application quick view appears.

2. On the Application quick view, enter or select the required information as described in the following table:

Field	Description
Application	The name **5g-sbi** appears by default.
Alias	The name **sbi5gAppTemplate** appears by default.
Transaction log	Enable the check box to collect the log of transaction or flow of request and response packets into the application. **Note**: The transaction log cannot be enabled when the numTCPflows and numStreamsPerFlow parameters are configured with maximum values.
Transaction log interval	Specify the time to collect the transaction log. You can collect the transaction log for 5 minutes or 60 minutes.
MTU Packet Size	The MTU packet size range is 1200 to 9200 bytes. You can select the **MTU Size** option and specify a value between 1200 to 9200 bytes.
Stats log	Enable the check box to collect packet and flow statistics.
Log Folder Size	Specify the folder size to save the CSV files.
Log Folder Location	Specify the location of the folder in which the CSV files are saved.
Type	Select the option **SCPviaGCB** from the drop-down list .
Indexed Headers	Enable the check box to index the headers.
Compressed Headers	Enable the check box to compress the headers.
Ip Mapping	Select the required CSV file from the drop-down list with FQDN name. Refer to Adding CSV file for IP Mapping to get the required CSV file in the drop-down list. In case of inadequate information (i.e., NF lookup failure), the appropriate counter is incremented and the synthesized packet is sent out with inappropriate IP address.
Mode	Nokia SCP is selected by default

Number of SCP Flows	Specify the range of SCP flow (The request ID and producer ID forms a SCP flow). The mininum value is 128. The maximum value is 16000. The default vaule is 2000.
Request Timeout	Specify the time for the request packet to wait for the response packet in the flow. The minimum value is 1 second and the maximum value is 300 seconds. The default value is 10 seconds.
Response Timeout	Specify the time for the response packet to wait for the request packet in a stream. The minimum value is 1 second and the maximum value is 300 seconds. The default value is 2 seconds. **NOTE:** When you receive a message indicating that an HTTP2 Response for a HTTP2 Stream ID is indicated and you do not receive a HTTP2 Request for the same HTTP2 Stream ID within the Response Timeout timer value, the Stream gets timed out and the ResponseTimedOut error counter gets incremented. Currently the RequestTimedOut error counter gets incremented erroneously.
Nokia Use 3Gpp Target API Root	When detecting Producer IP/FQDN, treat the 3GPP Target API Root to be predictive of the Producer IP if the value is non-zero. The default value is 1.
Thresholds	Specify the threshold value to configure the packet-drop settings.
Threshold Templates	Select the threshold template.
Time Interval	Select the time interval in seconds.

Rules and Notes

- The following configuration parameters are non-editable and it can be configured only during the initial configuration:
  - type
  - mode
  - eevtapVersion
  - numTCPFlows
  - numStreamsPerFlow
  - numSCPFlows

Configuration of 5G-SBI Application for 5G-Ericsson

In GigaVUE-FM, for 5G-Ericsson, you must do the following to configure the 5G-SBI application in the monitoring session of a monitoring domain in the V Series:

S.No	Steps	Refer to
1	Configure UDP-GRE Ingress TEP to receive the HTTP2/L7-JSON messages.	Create Tunnel Endpoints

2	Configure multiple other TEPs for other control protocol PDUs.	
3	Configure two instances of PCAPng application and link ingress TEPs and PCAPng application instances.	
4	Add 5G-SBI Application (HTTP2 header synthesis) in the monitoring session.	
5	Create a link between TEP and 5G-SBI Application.	
6	Create egress TEP.	Create Tunnel Endpoints
7	Create a link between PCAPng and egress TEPs or SBI and egress TEPs.	
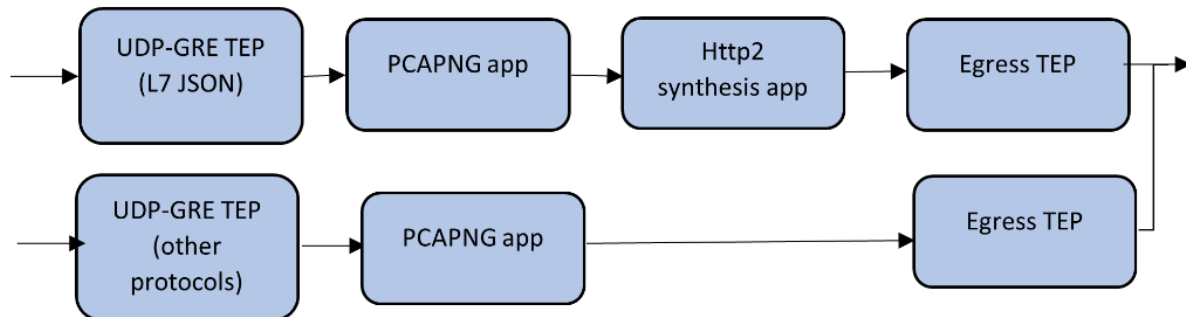
Adding 5G-SBI Application in 5G-Ericsson

Prerequisites

The pre-requisite to add a 5G-SBI application in Ericsson is:

- You must upload a CSV file containing a valid Network Function Instance ID (NFID) and a valid IPv4/IPv6 address. To upload the CSV file.

You can add a 5G-SBI application for:

- New monitoring session - You can add the 5G-SBI application after creating a new monitoring session and when the canvas appears.
- Existing session - Click **Edit** on existing monitoring session, the GigaVUE-FM canvas appears.

To add a 5G-SBI application:

1. In the canvas, Drag and drop 5G-SBI application and select **Details**. The Application quick view appears.

2. On the Application quick view, enter or select the required information as described in the following table:

Field	Description
Application	The name **5g-sbi** appears by default.
Alias	The name **sbi5gAppTemplate** appears by default.
Type	Select the option **ericssonVTap** from the drop-down list.
Indexed Headers	Enable the checkbox to index the HTTP2 headers in the 5G-SBI application.
Compressed Headers	Enable the checkbox to compress the HTTP2 headers in the 5G-SBI application.
Ip Mapping	Select the required CSV file from the drop-down list with required Network Function Instance ID (NFID) instance mapping. Refer to Adding CSV file for IP Mapping to get the required CSV file in the drop-down list.
Mode	L7json is selected by default. L7native is not supported in 6.1
EEV Tap Version	Select 1 or 2 from the drop-down list box.
TCP Flows	Specify the concurrent TCP flow range. The minimum value is 128 seconds, and the maximum value is 16000 seconds. The default value is 1000 seconds.
TCP Flow Timeout	Specify the flow range for which the TCP flow should remain valid in the application. The minimum value is 0 and the maximum value is 7200 seconds. The default value is 1800 seconds
Number of Streams per Flow	Specify the Number of Streams per flow. The minimum value is 1. The maximum value is 1024. The default value is 256.
Request Timeout	Specify the time for the request packet to wait for the response packet

	in a stream. The minimum value is 1 second and the maximum value is 300 seconds. The default value is 10 seconds.
Response Timeout	Specify the time for the response packet to wait for the request packet in a stream. The minimum value is 1 second and the maximum value is 300 seconds. The default value is 2 seconds.
Threshold Templates	Select the threshold template.
Time Interval	Select the time interval in seconds.

Adding CSV file for IP Mapping

To add the CSV file for IP mapping:

1. Go to **Inventory > VIRTUAL >** select your cloud platform, and then click **Settings > 5G-SBI**. The Proxy Server Configuration page appears.

2. Select any of the following from the **Type** as per the requirement:

   o **SCPviaGCP** - Adding the CSV file containing a valid FQDN name and a valid IPv4/IPv6 address for IP mapping in 5G-Nokia.

   o **ericcsonVTap** - Adding the CSV file containing a valid NF-instance ID and a valid IPv4/IPv6 address for IP mapping in 5G-Ericsson.

3. Enter the name for the CSV file in the **Alias** field.

4. Click **Choose File** in **FileName** field to upload the CSV file into GigaVUE-FM.

5. Click **Save** to add the CSV file.

What's Next

You can configure the traffic health monitoring for this application in the **THRESHOLDS** tab. You can select an existing template from the Threshold Templates drop-down menu or provide the threshold values. For more details on Traffic health monitoring and how to create threshold template, refer to Traffic Health Monitoring section in the respective cloud deployment guides.

You can view the configuration health status and the traffic health status of the application in the **HEALTH STATUS** tab. For more details on configuration health and traffic health, refer to Monitor Cloud Health section in the respective cloud deployment guides.

You can view the statistics of the application in the **STATISTICS** tab.

Slicing

Packet slicing allows you to truncate packets after a specified header and slice length, preserving the portion of the packet required for monitoring purposes. Slicing operations are typically configured to preserve specific packet header information, allowing effective network analysis without the overhead of storing full packet data.

Packets can have multiple variable-length headers, depending on where they are captured, the different devices that have attached their own headers along the way, and the protocols in use (for example, IPv4 versus IPv6). Because of this, slicing operations with a hard-coded offset will not typically provide consistent results.

To address this, the slicing application lets you configure packet slicing using protocols that allow you to start slicing from a particular number of bytes after a specific packet header (IPv4, IPv6, UDP, and so on). The slicing application parses through Layer 4 (TCP/UDP) to identify the headers in use, slicing based on the variable offset identified for a particular header instead of a hard-coded number of bytes.

To add a slicing application:

1. Drag and drop **Slicing** from **APPLICATIONS** to the graphical workspace.
2. Click the Slicing application and select **Details**. The Application quick view appears.

3. In the Application quick view, enter the information as follows:

Component	Description
Alias	Enter a name for the application.
Protocol	The following are the protocols that you can select for from the protocol drop-down list: o **None** –Slice starting a specific number of bytes from the start of the packet. o **IPV4** – Slice starting a specified number of bytes after the IPv4 header. o **IPV6** – Slice starting a specified number of bytes after the IPv6 header. o **UDP** – Slice starting a specified number of bytes after the UDP header. o **TCP** – Slice starting a specified number of bytes after the TCP header. o **FTP** – Identify using TCP port 20 and slice payloads using offset from the TCP header. o **HTTPS** – Identify using TCP port 443. Slice encrypted payloads using offset from the TCP header. o **SSH** – Identify using TCP port 22. Slice encrypted payloads using offset from the TCP header. The slicing application can provide slicing for GTP tunnels, provided the user payloads are unencrypted. Both GTPv1 and GTPv2 are supported – GTP' (GTP prime) is not supported. Keep in mind that only GTP-u (user plane packets) are sliced. Control plane packets (GTP-c) are left unmodified because of their importance for analysis. o **GTP** – Slice starting a specified number of bytes after the outer GTP header. o **GTP-IPV4** – Slice starting a specified number of bytes after the IPv4 header inside the encapsulating GTP packet. o **GTP-UDP** – Slice starting a specified number of bytes after the UDP header inside the encapsulating GTP packet. o **GTP-TCP** – Slice starting a specified number of bytes after the TCP header inside the encapsulating GTP packet.
Offset	Specify the length of the packet that must be sliced.

4. Click **Save**.

Slicing application is successfully configured.

What's Next

You can configure the traffic health monitoring for this application in the **THRESHOLDS** tab. You can select an existing template from the Threshold Templates drop-down menu or provide the threshold values. For more details on Traffic health monitoring and how to create threshold template, refer to Traffic Health Monitoring section in the respective cloud deployment guides.

You can view the configuration health status and the traffic health status of the application in the **HEALTH STATUS** tab. For more details on configuration health and traffic health, refer to Monitor Cloud Health section in the respective cloud deployment guides.

You can view the statistics of the application in the **STATISTICS** tab.

View Dashboard

Dashboard is a central location to display the statistics of all the applications, maps, Tunnel end points and Raw End Points configured for a particular monitoring session.

To view dashboard, follow the steps given below:

1. Go to **Traffic > Virtual > Orchestrated Flows > Select your cloud platform**.
2. Select a monitoring session from the list view, click **Actions > Edit**. The Edit Monitoring Session page appears.
3. Click **Dashboard**. The **Dashboard** dialog box opens.
4. Click on each tab to display the statistics of the respective entity configured in the Monitoring Session Canvas page.

Additional Sources of Information

This appendix provides additional sources of information. Refer to the following sections for details:

- Documentation
- Documentation Feedback
- Contact Technical Support
- Contact Sales
- The VÜE Community

Documentation

This table lists all the guides provided for GigaVUE Cloud Suite software and hardware. The first row provides an All-Documents Zip file that contains all the guides in the set for the release.

> **NOTE:** In the online documentation, view What's New to access quick links to topics for each of the new features in this Release; view Documentation Downloads to download all PDFs.

Table 1: Documentation Set for Gigamon Products

GigaVUE Cloud Suite 6.5 Hardware and Software Guides
DID YOU KNOW? If you keep all PDFs for a release in common folder, you can easily search across the doc set by opening one of the files in Acrobat and choosing **Edit > Advanced Search** from the menu. This opens an interface that allows you to select a directory and search across all PDFs in a folder.
Hardware   how to unpack, assemble, rack-mount, connect, and initially configure ports the respective GigaVUE Cloud Suite devices; reference information and specifications for the respective GigaVUE Cloud Suite devices
GigaVUE-HC1 Hardware Installation Guide
GigaVUE-HC2 Hardware Installation Guide
GigaVUE-HC3 Hardware Installation Guide
GigaVUE-HC1-Plus Hardware Installation Guide
GigaVUE-HCT Hardware Installation Guide
GigaVUE-TA25 Hardware Installation Guide
GigaVUE-TA25E Hardware Installation Guide

GigaVUE Cloud Suite 6.5 Hardware and Software Guides
GigaVUE-TA100 Hardware Installation Guide
GigaVUE-TA200 Hardware Installation Guide
GigaVUE-TA200E Hardware Installation Guide
GigaVUE-TA400 Hardware Installation Guide
GigaVUE-OS Installation Guide for DELL S4112F-ON
G-TAP A Series 2 Installation Guide
GigaVUE M Series Hardware Installation Guide
GigaVUE-FM Hardware Appliance Guide for GFM-HW1-FM010 and and GFM-HW1-FM001-HW
Software Installation and Upgrade Guides
GigaVUE-FM Installation, Migration, and Upgrade Guide
GigaVUE-OS Upgrade Guide
GigaVUE V Series Migration Guide
Fabric Management and Administration Guides
GigaVUE Administration Guide covers both GigaVUE-OS and GigaVUE-FM
GigaVUE Fabric Management Guide how to install, deploy, and operate GigaVUE-FM; how to configure GigaSMART operations; covers both GigaVUE-FM and GigaVUE-OS features
Cloud Guides how to configure the GigaVUE Cloud Suite components and set up traffic monitoring sessions for the cloud platforms
GigaVUE V Series Applications Guide
GigaVUE V Series Quick Start Guide
GigaVUE Cloud Suite Deployment Guide - AWS
GigaVUE Cloud Suite Deployment Guide - Azure
GigaVUE Cloud Suite Deployment Guide - OpenStack
GigaVUE Cloud Suite Deployment Guide - Nutanix
GigaVUE Cloud Suite Deployment Guide - VMware (ESXi)
GigaVUE Cloud Suite Deployment Guide - VMware (NSX-T)
GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration

GigaVUE Cloud Suite 6.5 Hardware and Software Guides
Universal Cloud Tap - Container Deployment Guide
Gigamon Containerized Broker Deployment Guide
GigaVUE Cloud Suite for Nutanix Guide—GigaVUE-VM Guide
GigaVUE Cloud Suite Deployment Guide - AWS Secret Regions
Reference Guides
GigaVUE-OS CLI Reference Guide library of GigaVUE-OS CLI (Command Line Interface) commands used to configure and operate GigaVUE HC Series and TA Series devices
GigaVUE-OS Security Hardening Guide
GigaVUE Firewall and Security Guide
GigaVUE Licensing Guide
GigaVUE-OS Cabling Quick Reference Guide guidelines for the different types of cables used to connect Gigamon devices
GigaVUE-OS Compatibility and Interoperability Matrix compatibility information and interoperability requirements for Gigamon devices
GigaVUE-FM REST API Reference in GigaVUE-FM User's Guide samples uses of the GigaVUE-FM Application Program Interfaces (APIs)
Release Notes
GigaVUE-OS, GigaVUE-FM, GigaVUE-VM, G-TAP A Series, and GigaVUE Cloud Suite Release Notes new features, resolved issues, and known issues in this release ; important notes regarding installing and upgrading to this release **NOTE:** Release Notes are not included in the online documentation. **NOTE:** Registered Customers can log in to My Gigamon to download the Software and Release Notes from the Software & Docs page on to My Gigamon. Refer to How to Download Software and Release Notes from My Gigamon.
In-Product Help
GigaVUE-FM Online Help how to install, deploy, and operate GigaVUE-FM.

How to Download Software and Release Notes from My Gigamon

Registered Customers can download software and corresponding Release Notes documents from the **Software & Release Notes** page on to My Gigamon. Use the My Gigamon Software & Docs page to download:

- Gigamon Software installation and upgrade images,
- Release Notes for Gigamon Software, or
- Older versions of PDFs (pre-v5.7).

To download release-specific software, release notes, or older PDFs:

1. Log in to My Gigamon
2. Click on the **Software & Release Notes** link.
3. Use the **Product** and **Release** filters to find documentation for the current release. For example, select Product: "GigaVUE-FM" and Release: "5.6," enter "pdf" in the search box, and then click **GO** to view all PDF documentation for GigaVUE-FM 5.6.xx.

> **NOTE:** My Gigamon is available to registered customers only. Newer documentation PDFs, with the exception of release notes, are all available through the publicly available online documentation.

Documentation Feedback

We are continuously improving our documentation to make it more accessible while maintaining accuracy and ease of use. Your feedback helps us to improve. To provide feedback and report issues in our documentation, send an email to:
documentationfeedback@gigamon.com

Please provide the following information in the email to help us identify and resolve the issue. Copy and paste this form into your email, complete it as able, and send. We will respond as soon as possible.

Documentation Feedback Form		
About You	**Your Name**	
	Your Role	
	Your Company	

For Online Topics	Online doc link	*(URL for where the issue is)*
	Topic Heading	*(if it's a long topic, please provide the heading of the section where the issue is)*
For PDF Topics	Document Title	*(shown on the cover page or in page header)*
	Product Version	*(shown on the cover page)*
	Document Version	*(shown on the cover page)*
	Chapter Heading	*(shown in footer)*
	PDF page #	*(shown in footer)*
How can we improve?	Describe the issue	*Describe the error or issue in the documentation.* *(If it helps, attach an image to show the issue.)*
	How can we improve the content? Be as specific as possible.	
	Any other comments?	

Contact Technical Support

For information about Technical Support: Go to **Settings** ⚙ **> Support > Contact Support** in GigaVUE-FM.

You can also refer to https://www.gigamon.com/support-and-services/contact-support for Technical Support hours and contact information.

Email Technical Support at support@gigamon.com.

Contact Sales

Use the following information to contact Gigamon channel partner or Gigamon sales representatives:

Telephone: +1.408.831.4025

Sales: inside.sales@gigamon.com

Partners: www.gigamon.com/partners.html

Premium Support

Email Gigamon at inside.sales@gigamon.com for information on purchasing 24x7 Premium Support. Premium Support entitles you to round-the-clock phone support with a dedicated Support Engineer every day of the week.

The VÜE Community

The VÜE Community is a technical site where Gigamon users, partners, security and network professionals and Gigamon employees come together to share knowledge and expertise, ask questions, build their network and learn about best practices for Gigamon products.

Visit the VÜE site to:

- Find knowledge base articles and documentation
- Ask and answer questions and learn best practices from other members.
- Join special-interest groups to have focused collaboration around a technology, use-case, vertical market or beta release
- Take online learning lessons and tutorials to broaden your knowledge of Gigamon products.
- Open support tickets (Customers only)
- Download the latest product updates and documentation (Customers only)

The VÜE Community is a great way to get answers fast, learn from experts and collaborate directly with other members around your areas of interest.

Register today at community.gigamon.com

Questions? Contact our Community team at community@gigamon.com.

Glossary

D

decrypt list

need to decrypt (formerly blacklist)

decryptlist

need to decrypt - CLI Command (formerly blacklist)

drop list

selective forwarding - drop (formerly blacklist)

F

forward list

selective forwarding - forward (formerly whitelist)

L

leader

leader in clustering node relationship (formerly master)

M

member node

follower in clustering node relationship (formerly slave or non-master)

N

no-decrypt list

no need to decrypt (formerly whitelist)

nodecryptlist

no need to decrypt- CLI Command (formerly whitelist)

P

primary source

root timing; transmits sync info to clocks in its network segment (formerly grandmaster)

R

receiver

follower in a bidirectional clock relationship (formerly slave)

S

source

leader in a bidirectional clock relationship (formerly master)