



GigaVUE Cloud Suite for Azure Secret Regions - Deployment Guide

GigaVUE Cloud Suite

Product Version: 6.14.xx

Document Version: 2.0

(See Change Notes for document updates.)

Copyright © 2026 Gigamon Inc. All rights reserved.

Information in this document is subject to change without notice. The software described in this document is furnished under a license agreement or nondisclosure agreement. No part of this publication may be reproduced, transcribed, translated into any language, stored in a retrieval system, or transmitted in any form or any means without the written permission of Gigamon Inc.

Trademark Attributions

Gigamon and the Gigamon logo are trademarks of Gigamon in the United States and/or other countries. Gigamon trademarks can be found at www.gigamon.com/legal-trademarks. All other trademarks are the trademarks of their respective owners.

Gigamon Inc.
3300 Olcott Street
Santa Clara, CA 95054
408.831.4000

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
6.14.01/6.14.02	2.0	09/07/2026	This release incorporates changes in the following topics for the listed features: • Port Optimization ◦ Network Firewall Requirement
6.14.00	1.0	07/10/2026	The original release of this document with 6.14.00 GA.

Contents

GigaVUE Cloud Suite for Azure Secret Regions - Deployment Guide	1
Change Notes	3
Contents	4
GV-Cloud-Azure-Secret-Region	7
Get_Started	7
GigaVUE Cloud Suite for Azure Secret and Top Secret Regions	8
Prerequisites	9
Network Firewall Requirement	9
Reduced Control-Plane Ports	9
GigaVUE-FM	11
UCT-V Controller	11
UCT-V	12
GigaVUE V Series Node	12
GigaVUE V Series Proxy (Optional)	12
UCT-V OVS Controller	13
UCT-V OVS Module	13
GigaVUE FM	13
UCT-V Controller	14
UCT-V	15
GigaVUE V Series Node	16
GigaVUE V Series Proxy (Optional)	17
UCT-V OVS Controller	18
UCT-V OVS Module	18
Legacy Control-Plane Ports	19
GigaVUE FM	19
GigaVUE V Series Node	21
Giga VUE V Series Proxy(Optional)	22
GigaVUE V Series Node	23
GigaVUE V Series Proxy(Optional)	24
Inline V Series (Azure)	24
Inline V Series Deployment Types	24
Architecture of Inline V Series Solution in Azure	25
Limitation	26
Configure Custom Settings for Azure Secret and Top Secret Regions	26
Configure Service Endpoints	27

Configure Custom Regions	27
Import CA Certificate for Service Endpoints	28
Get_Started	29
Deploy GigaVUE Cloud Suite for Azure Secret or Top Secret Regions ..	29
Create Azure Credentials	30
Prerequisite	30
Integrate Private CA	31
Rules and Notes	31
Generate CSR	31
Upload CA Certificate	32
Adding Certificate Authority	32
Create Monitoring Domain	33
Prerequisite	33
Check Permissions while Creating a Monitoring Domain	36
Configure GigaVUE Fabric Components	39
Configure GigaVUE V Series Node and GigaVUE V Series Proxy	39
Deploy Inline V Series Solution in Azure	40
Prerequisite	40
Create a Resource Group	41
Create Virtual Networks	42
Create a Virtual Network Peering	42
Create a Network Security Group	42
Create a Load Balancer	42
Install GigaVUE-FM on Azure	46
Enable System Assigned Managed Identity	48
Create Gigamon Custom Role	48
Assign Role to Resource Group	49
Assign Role to GigaVUE-FM Instance	50
Create a GigaVUE-FM Token	50
Modify Virtual Machine Scale Set (VMSS) Cloud Initialization Template	51
Create a Virtual Machine Scale Set for Inline GigaVUE V Series Node (Tier 1)	51
Assign VMSS to GWLB Backend Pools	55
Create Monitoring Domain	55
Deploy GigaVUE V Series Nodes for Inline V Series Solution	56
(Optional) Create a Virtual Machine Scale Set for Out-of-Band GigaVUE V Series Node (Tier 2)	57
Configure Monitoring session	59
Configure	63
Configure Monitoring Session	63
Create a Monitoring Session (Azure)	64
Enable Prefiltering	67
Enable Precryption	67

Validate Precryption connection	69
Limitations	69
Apply Threshold Template	70
Enable User Defined Applications	70
Enable Distributed De-duplication	71
Tool Exclusion	71
Create Ingress and Egress Tunnels (Azure)	72
Create Raw Endpoint (Azure)	82
Create a New Map (Azure)	83
Add Applications to Monitoring Session (Azure)	88
What's Next	95
What's Next	97
Limitations	102
What's Next	102
Configure Application Visualization for Virtual Environment	105
Configure Filtering and Metadata Export for Selected Applications in	
Application Visualization	107
Filter Traffic for Selected Applications	107
Export Metadata for Selected Applications	108
View Application Statistics for Application Visualization	108
Supported Protocols and Attributes	109
Metadata	114
Supported RegExp Syntax	114
Limitations	115
Create Rules for User Defined Application	115
Configure Application Filtering Intelligence for Virtual Environment	117
View Application Statistics for Application Filtering	122
Configure Application Metadata Intelligence for Virtual Environment	123
Extend Your AMI and AMX Deployment	132
View Application Statistics for Application Metadata	133
What's Next	138
Upload SSL Key Pairs	153
Create SSL Service	155
Prerequisite	155
Key Mapping	155
SSL Key Pair Store	156
Add SSL Decrypt to Monitoring Session	156
Interface Mapping (Azure)	158
Deploy Monitoring Session (Azure)	159
Monitor and Troubleshoot	161
View Monitoring Session Statistics (Azure)	162
Visualize the Network Topology (Azure)	163
AdditionalInfoAppx	165

- Additional Sources of Information 165
 - Documentation 165
 - Documentation Feedback 168
 - Contact Technical Support 169
 - Contact Sales 169
 - The VÜE Community 170

GV-Cloud-Azure-Secret-Region

Get_Started

Delete this text and replace it with your own content.

GigaVUE Cloud Suite for Azure Secret and Top Secret Regions

The GigaVUE Cloud Suite for Azure Secret and Top Secret Regions option consists of the following components:

- **GigaVUE-FM fabric manager** - GigaVUE-FM is a web-based fabric management and orchestration interface that provides a single pane of glass visibility, management, and orchestration of both the physical and virtual traffic that form the GigaVUE Cloud Suite Cloud.
- **GigaVUE V Series Proxy (Optional)** - GigaVUE® V Series Proxy manages multiple GigaVUE V Series Nodes and orchestrates the flow of traffic from GigaVUE V Series Nodes to the monitoring tools
- **GigaVUE V Series Nodes** - GigaVUE® V Series Node is a visibility node that aggregates mirrored traffic. It applies filters, manipulates the packets using GigaSMART applications, and distributes the optimized traffic to cloud-based tools or backhaul to GigaVUE Cloud Suite Cloud using GRE or VXLAN tunnels, provided the cloud platform supports.

The images of all the fabric components are available in the [Gigamon Customer Portal](#). For information about installing GigaVUE-FM in your enterprise data center, refer to the *GigaVUE-FM Installation, Migration, and Upgrade Guide*.

Prerequisites

This section lists the minimum requirements that are required for deploying the fabric components:

1. GigaVUE V Series Node requires a minimum of two network interfaces (NIC). Both can be on the same subnet or different subnets.
2. GigaVUE V Series Node requires a minimum of one Management interface (MGMT). Management interface is used for communicating between GigaVUE-FM and V Series Node.
3. GigaVUE V Series Node requires a minimum of one Data/Tunnel interface.
4. The minimum system requirements for V Series Proxy is 1CPU/1GB RAM.

Network Firewall Requirement

Reduced Control-Plane Ports

Starting in release 6.14.02, the number of ports required for control-plane communication is reduced from 12 ports to 3 ports (443, 5671, and 9902). The reduced control-plane ports decrease the number of ports you must open between GigaVUE-FM and other fabric components while preserving management, registration, certificate exchange, and operational communication.

This change applies to control-plane traffic only. It does not change any data-path ports.

Use the minimum versions required for the reduced three-port configuration.

Component	Version
GigaVUE-FM	6.14.02
GigaVUE V Series Node	6.14.01
GigaVUE V Series Proxy	6.14.01
UCT-V	6.14.01
UCT-V Controller	6.14.01



Important

- Do not upgrade fabric components to version 6.14.01 unless GigaVUE-FM is running version 6.14.02 or later.
- Fabric components version 6.14.01 are incompatible with GigaVUE-FM 6.14.00 and 6.14.01.
- Deployments that use this unsupported version combination will not support reduced control-plane port communication and may not function correctly.

Choose the section that applies to your deployment scenario:

- [New Deployments](#) – Use this section if you are deploying a new environment with GigaVUE-FM 6.14.02 or later and all supported fabric components running version 6.14.01 or later. These deployments use only the reduced control-plane ports.
- [Existing Deployments](#) – Use this section if you are upgrading an existing deployment and want to migrate from legacy control-plane ports to the reduced control-plane ports. This section identifies the ports to add and remove for each component during migration.
- [Legacy Control-Plane Ports](#) – Use this section if GigaVUE-FM is running a version earlier than 6.14.02, if any fabric component is running a version earlier than 6.14.01, or if your deployment requires backward compatibility during a mixed-version upgrade.

New Deployments

For new deployments, configure only the reduced control-plane ports. You do not need to open any legacy control-plane ports. Use the firewall requirements in this section when deploying a new GigaVUE Cloud Suite environment.

The reduced configuration uses only the three ports listed below:

Direction	Port	Purpose
Inbound/Outbound	443	HTTPS/REST management and control-plane communication, including GigaVUE-FM UI/API access, component registration, and certificate-related requests.
Inbound/Outbound	5671	RMQ/RA control-plane messaging and statistics or health updates between GigaVUE-FM and fabric components.
Inbound/Outbound	9902	RPC and control-plane communication, especially between UCT-V Controllers and UCT-V agent.

Existing Deployments

Existing deployments continue to operate without any firewall changes after upgrading GigaVUE-FM and fabric components. Legacy control-plane ports remain supported for backward compatibility. You can continue to use the legacy control-plane ports or migrate to the reduced control-plane ports. For information about the legacy ports, refer to [Legacy Control-Plane Ports](#)

To migrate to the reduced control-plane ports, refer to [Migration to Reduced Control-Plane Ports](#)

Migration to Reduced Control-Plane Ports

If you are migrating your existing deployment from legacy control-plane ports to reduced control-plane ports, complete the following steps:

- Upgrade the deployment while keeping the legacy ports open.
- Verify that all upgraded components are in the supported versions.

- Open the required reduced control-plane ports for GigaVUE-FM, other fabric components, and the UCT-V Agent. Use the port requirements listed in [Firewall Rule Changes for Migrating to Reduced Control-Plane Ports](#).
- Use the **Reset** option to force the monitoring domain to reconnect by using the new ports. For more information, refer to the [Manage a Monitoring Domain](#).
- Verify that all applicable components are communicating over ports 443, 5671, and 9902.
- Remove the legacy ports from your firewall or security group rules after verification is complete.

NOTE: Do not close all legacy ports and enable only the new ports before upgrading. Doing so can disrupt existing connections and is not recommended.

Firewall Rule Changes for Migrating to Reduced Control-Plane Ports

The following tables summarize the firewall changes to make when migrating an existing deployment:

GigaVUE-FM

Action	Direction	Port
Remove	Inbound	9600
Remove	Outbound	8890
Remove	Outbound	8889
Remove	Outbound	80
Remove	Outbound	9990
Add	Inbound	443
Add	Inbound	5671
Add	Outbound	443
Add	Outbound	443

UCT-V Controller

Action	Direction	Port
Remove	Inbound	9900
Remove	Inbound	80
Remove	Inbound	8300
Remove	Inbound	8892
Remove	Outbound	9600
Remove	Outbound	8301
Add	Inbound	443

Add	Outbound	443
Add	Outbound	5671
Add	Outbound	9902

UCT-V

Action	Direction	Port
Remove	Inbound	8301
Remove	Outbound	8892
Remove	Outbound	9900
Remove	Outbound	8300
Add	Inbound	9902
Add	Outbound	5671
Add	Outbound	443

GigaVUE V Series Node

Action	Direction	Port
Remove	Inbound	8889
Remove	Inbound	80
Remove	Outbound	8891
Remove	Outbound	8892
Remove	Outbound	9600
Remove	Outbound	8300
Add	Inbound	443
Add	Outbound	443
Add	Outbound	5671

GigaVUE V Series Proxy (Optional)

Action	Direction	Port
Remove	Inbound	8890
Remove	Inbound	80
Remove	Inbound	8300
Remove	Inbound	8891
Remove	Inbound	8892
Remove	Outbound	8889
Remove	Outbound	9600
Remove	Outbound	80

Add	Inbound	5671
Add	Inbound	443
Add	Outbound	443

UCT-V OVS Controller

Action	Direction	Port
Remove	Inbound	9900
Add	Inbound	443
Add	Outbound	9901

UCT-V OVS Module

Action	Direction	Port
Add	Inbound	9901

The following tables identify the firewall changes required to migrate from the legacy control-plane ports to the optimized control-plane ports:

GigaVUE FM

The following table lists the reduced control-plane ports required for communication with GigaVUE-FM.

Direction	Protocol	Port	Replaces Legacy Port	Source CIDR2	Purpose
Inbound	TCP	443	9600	GigaVUE V Series Node IP	Allows GigaVUE-FM to receive certificate requests from GigaVUE V Series Node.
Inbound	TCP	443	9600	GigaVUE V Series Proxy IP	Allows GigaVUE-FM to receive certificate requests from GigaVUE V Series Proxy.
Direction	Protocol	Port	Replaces Legacy Port	Destination CIDR	Purpose
Outbound	TCP	443	8889	GigaVUE V Series Node IP	Allows GigaVUE-FM to communicate control and management plane traffic to GigaVUE V Series Node.

Outbound	TCP	443	8890	GigaVUE V Series Proxy IP	Allows GigaVUE-FM to communicate control and management plane traffic to GigaVUE V Series Proxy.
Outbound	TCP	443	9900	UCT-V Controller IP	Allows GigaVUE-FM to communicate control and management plane traffic with UCT-V Controller.
Outbound	TCP	443	9900	OVS Controller	Controller management communication.



Removed: Outbound TCP 80 (ACME challenge) is no longer required. Certificate issuance and renewal for fabric nodes (6.14.01 or later) use JWK-based authentication instead of the ACME HTTP challenge.

UCT-V Controller

The following table lists the reduced control-plane ports required for communication with UCT-V Controller.

Direction	Protocol	Port	Replaces Legacy Port	Source CIDR	Purpose
Inbound	TCP	443	9900	GigaVUE-FM IP	Allows UCT-V Controller to communicate control and management plane traffic with GigaVUE-FM.
Inbound	TCP	443	8300	UCT-VSubnet	Allows UCT-V Controller to receive the certificate requests from the UCT-V.
Inbound	TCP	443	8892	UCT-V Subnet	Allows UCT-V Controller to receive the registration requests and heartbeat from UCT-V.
Inbound	TCP	443	9900	UCT-V or Subnet IP	Allows UCT-V Controller to receive traffic health updates from UCT-V.

Direction	Protocol	Port	Replaces Legacy Port	Destination CIDR	Purpose
Outbound	TCP	5671	NA	UCT-V Subnet	Allows the UCT-V Controller to communicate control and management plane traffic with UCT-Vs for monitoring domains created in 6.14.01 and later.
Outbound	TCP	9902	NA	UCT-V Subnet	Allows UCT-V Controller to communicate control and management plane traffic with UCT-Vs for UCT-Vs with version earlier than 6.14.01.



Removed: Inbound TCP 80 (ACME challenge from GigaVUE-FM), Outbound TCP 9600 (certificate request to GigaVUE-FM), and Outbound TCP 8301 (ACME validation to UCT-V) are no longer required for 6.14.01+ deployments.

NOTE: For UCT-V Controller-to-UCT-V traffic, the controller uses 5671 for monitoring domains created in 6.14.01 and later, and 9902 for monitoring domains created in earlier releases. The UCT-V RPC port is configurable at the monitoring-domain level.

UCT-V

The following table lists the reduced control-plane ports required for communication with UCT-V.

Direction	Protocol	Port	Replaces Legacy Port	Source CIDR	Purpose
Inbound	TCP	5671	NA	UCT-V Controller IP	Allows UCT-V to receive control and management plane traffic from UCT-V Controller for monitoring domains created in 6.14.01 and later.
Inbound	TCP	9902	NA	UCT-V Controller IP	Allows UCT-V to receive control and management plane traffic from UCT-V Controller for existing monitoring domains created with version

					earlier than 6.14.01.
Direction	Protocol	Port	Replaces Legacy Port	Destination CIDR	Purpose
Outbound	TCP	443	9900	UCT-V Controller IP	Allows UCT-V to send traffic health updates to UCT-V Controller.
Outbound (This is the port used for Third Party Orchestration)	TCP	443	8892	UCT-V Controller IP	Allows UCT-V to receive the registration requests and heartbeat to UCT-V Controller.
Outbound	TCP	443	8300	UCT-V Controller IP	Allows UCT-V to receive the certificate requests from the UCT-V Controller.



Removed: Inbound TCP 8301 (ACME challenge) is no longer required for 6.14.01 or later.

NOTE: A 6.14.01 UCT-V listens on both 5671 and 9902 during discovery. The default listening port is 5671 for monitoring domains created in 6.14.01; monitoring domains migrated from earlier releases default to 9902. This port is configurable at the monitoring-domain level.

GigaVUE V Series Node

The following table lists the reduced control-plane ports required for communication with GigaVUE V Series Node.

Direction	Protocol	Port	Replaces Legacy Port	Source CIDR	Purpose
Inbound	TCP	443	8889	GigaVUE-FM IP	Allows GigaVUE V Series Node to communicate control and management plane traffic with GigaVUE-FM.
Direction	Protocol	Port	Replaces Legacy Port	Destination CIDR	Purpose
Outbound	TCP	5671	8300	GigaVUE V Series Proxy	Allows GigaVUE V Series Node to send certificate request to GigaVUE V Series Proxy IP.
Outbound	TCP	443	8891	GigaVUE V Series Proxy	Allows GigaVUE V Series Proxy to receive PKI requests from the

					GigaVUE V Series Node.
Outbound	TCP	443	8892	GigaVUE V Series Proxy	Allows GigaVUE V Series Proxy to receive registration requests and heartbeat messages from GigaVUE V Series Node.
Outbound	TCP	443	9600	GigaVUE-FM IP	Allows GigaVUE-FM to receive certificate requests from GigaVUE V Series Node.



Removed: Inbound TCP 80 (ACME challenge) is no longer required for 6.14.01 or later.

NOTE: Cross-version deployments between GigaVUE V Series Nodes and GigaVUE V Series Proxy are not supported. Ensure that the GigaVUE V Series Node and GigaVUE V Series Proxy are running the same software version. For example, a 6.13 GigaVUE V Series Node cannot communicate with a 6.14 GigaVUE V Series Proxy.

GigaVUE V Series Proxy (Optional)

The following table lists the reduced control-plane ports required for communication with GigaVUE V Series Proxy.

Direction	Protocol	Port	Replaces Legacy Port	Source CIDR	Purpose
Inbound	TCP	443	8890	GigaVUE-FM IP	Allows GigaVUE-FM to communicate control and management plane traffic with GigaVUE V Series Proxy.
Inbound	TCP	443	8891	GigaVUE V Series Node	Allows GigaVUE V Series Proxy to receive PKI requests from GigaVUE V Series Node.
Inbound	TCP	443	8892	GigaVUE V Series Node	Allows GigaVUE V Series Proxy to receive registration requests and heartbeat messages from GigaVUE V Series Node.

Inbound	TCP	5671	8300	GigaVUE V Series Node	Allows GigaVUE V Series Proxy to receive certificate requests from GigaVUE V Series Node for the configured params and provides the certificate using those parameters.
Direction	Protocol	Port	Replaces Legacy Port	Destination CIDR	Purpose
Outbound	TCP	443	9600	GigaVUE-FM IP	Allows GigaVUE-FM to receive certificate requests from GigaVUE V Series Proxy.



Removed: Inbound and outbound TCP 80 (ACME challenge) is no longer required for 6.14.01 or later.

UCT-V OVS Controller

The following table lists the reduced control-plane ports required for communication with UCT-V OVS Controller.

Direction	Protocol	Port	Replaces Legacy Port	Source CIDR	Purpose
Inbound	TCP	443	9900	GigaVUE-FM IP	Allows GigaVUE-FM to communicate control and management plane traffic. The controller supports both ports for compatibility and falls back to 9900 when required.
Direction	Protocol	Port	Replaces Legacy Port	Destination CIDR	Purpose
Outbound	TCP	9901	NA	UCT-V OVS Module IP	Allows to communicate with UCT-V OVS Modules (RPC).

UCT-V OVS Module

The following table lists the reduced control-plane ports required for communication with UCT-V OVS Module.

Direction	Protocol	Port	Replaces Legacy Port	Source CIDR	Purpose
Inbound	TCP	9901	NA	UCT-V OVS Controller IP	Allows to receive control communication from UCT-V OVS Controller. The module listens on 9901 for backward compatibility.

Legacy Control-Plane Ports

Legacy control-plane ports remain supported for backward compatibility with earlier versions and mixed-version deployments.

When to Use Legacy Ports

- GigaVUE-FM is running version 6.10 or later but earlier than 6.14.02.
- One or more fabric components (such as UCT-V Controller, UCT-V, GigaVUE V Series Node, GigaVUE V Series Proxy, or OVS components) are running a version earlier than 6.14.01.
- This includes mixed-version deployments where GigaVUE-FM 6.14.02 or later communicates with fabric components running N-1 or N-2 releases.
- The deployment has not yet been migrated to the reduced control-plane port architecture.

The following table lists the Network Firewall / Security Group requirements for GigaVUE Cloud Suite:

NOTE: When using dual stack network, open the below mentioned ports for both IPv4 and IPv6.

GigaVUE FM

The following table specifies the inbound and outbound communication parameters—protocols, ports, and CIDRs—required for GigaVUE-FM to support secure access, registration, certificate exchange, and control-plane communication with associated components.

Direction	Protocol	Port	Source CIDR	Purpose
Inbound	TCP	443	Administrator Subnet	Allows GigaVUE-FM to accept Management connection using REST API. Allows users to access GigaVUE-FM UI securely through an HTTPS connection.

Inbound	TCP	22	Administrator Subnet	Allows CLI access to user-initiated management and diagnostics.
Inbound (This is the port used for Third Party Orchestration)	TCP	443	GigaVUE V Series Node IP	Allows GigaVUE-FM to receive registration requests from GigaVUE V Series Node using REST API when GigaVUE V Series Proxy is not used.
Inbound (This is the port used for Third Party Orchestration)	TCP	443	GigaVUE V Series Proxy IP	Allows GigaVUE-FM to receive registration requests from GigaVUE V Series Proxy using REST API.
Inbound	TCP	5671	GigaVUE V Series Node IP	Allows GigaVUE-FM to receive traffic health updates from GigaVUE V Series Nodes.
Inbound	TCP	9600	GigaVUE V Series Proxy	Allows GigaVUE-FM to receive certificate requests from GigaVUE V Series Proxy.
Inbound	TCP	9600	GigaVUE V Series Node	Allows GigaVUE-FM to receive certificate requests from GigaVUE V Series Node.
Inbound	UDP	2056	GigaVUE V Series Node IP	Allows GigaVUE-FM to receive Application Intelligence and Application Visualization reports from GigaVUE V Series Node.
Direction	Protocol	Port	Destination CIDR	Purpose
Outbound (optional)	TCP	8890	GigaVUE V Series Proxy IP	Allows GigaVUE-FM to communicate control and management plane traffic to GigaVUE V Series Proxy.
Outbound	TCP	8889	GigaVUE V Series Node IP	Allows GigaVUE-FM to communicate control and management plane traffic to GigaVUE V Series Node.
Outbound	TCP	80	GigaVUE V Series Node	Allows GigaVUE-FM to send ACME challenge requests to GigaVUE V

				Series Node.
Outbound	TCP	80	GigaVUE V Series Proxy	Allows GigaVUE-FM to send ACME challenge requests to GigaVUE V Series Proxy.
Outbound	TCP	443	Any IP Address	Allows GigaVUE-FM to reach the Public Cloud Platform APIs.

GigaVUE V Series Node

The following table outlines GigaVUE V Series Node's network communication requirements, detailing protocols, ports, and CIDRs necessary for tunneling, management, diagnostics, and secure data transfer across connected components

Direction	Protocol	Port	Source CIDR	Purpose
Inbound	TCP	8889	GigaVUE-FM IP	Allows GigaVUE V Series Node to communicate control and management plane traffic with GigaVUE-FM.
Inbound	TCP	8889	GigaVUE V Series Proxy IP	Allows GigaVUE V Series Node to communicate control and management plane traffic with GigaVUE V Series Proxy.
Inbound	UDPGRE	4754	Ingress Tunnel	Allows GigaVUE V Series Node to receive tunnel traffic from UDPGRE Tunnel.
Inbound	TCP	22	Administrator Subnet	Allows CLI access for user-initiated management and diagnostics, specifically when using third party orchestration.
Inbound	TCP	80	GigaVUE-FM	Allows GigaVUE V Series Node to receive the ACME challenge requests from GigaVUE-FM.
Inbound	TCP	80	GigaVUE V Series Proxy IP	Allows UCT-V to receive the ACME challenge requests from the GigaVUE V Series Proxy.
Inbound (Optional - This port is used only for configuring AWS Gateway Load Balancer)	UDP (GENEVE)	6081	Ingress Tunnel	Allows GigaVUE V Series Node to receive tunnel traffic from AWS Gateway Load Balancer.
Direction	Protocol	Port	Destination CIDR	Purpose
Outbound	TCP	5671	GigaVUE-FM IP	Allows GigaVUE V Series Node to

				send traffic health updates to GigaVUE-FM.
Outbound	UDP (VXLAN)	VXLAN (default 4789)	Tool IP	Allows GigaVUE V Series Node to tunnel output to the tool.
Outbound	IP Protocol (L2GRE)	L2GRE (IP 47)	Tool IP	Allows GigaVUE V Series Node to tunnel output to the tool.
Outbound	UDP	2056	GigaVUE-FM IP	Allows GigaVUE V Series Node to send Application Intelligence and Application Visualization reports to GigaVUE-FM.
Outbound	UDP	2055	Tool IP	Allows GigaVUE V Series Node to send NetFlow Generation traffic to an external tool.
Outbound	UDP	8892	GigaVUE V Series Proxy	Allows GigaVUE V Series Node to send certificate request to GigaVUE V Series Proxy IP.
Outbound	TCP	514	Tool IP	Allows GigaVUE V Series Node to send Application Metadata Intelligence log messages to external tools.
Bidirectional (optional)	ICMP	- echo request - echo reply	Tool IP	Allows GigaVUE V Series Node to send health check tunnel destination traffic.
Outbound (This is the port used for Third Party Orchestration)	TCP	443	GigaVUE-FM IP	Allows GigaVUE V Series Node to send registration requests and heartbeat messages to GigaVUE-FM when GigaVUE V Series Proxy is not used.
Outbound (Optional - This port is used only for Secure Tunnels)	TCP	11443	Tool IP	Allows to securely transfer the traffic to an external tool.

Giga VUE V Series Proxy(Optional)

The following table defines GigaVUE V Series Proxy's network communication parameters, listing essential protocols, ports, and CIDRs for registration, certificate exchange, diagnostics, and control-plane traffic with GigaVUE-FM and V Series Nodes.

Direction	Protocol	Port	Source CIDR	Purpose
Inbound	TCP	8890	GigaVUE-FM IP	Allows GigaVUE-FM to communicate control and management plane traffic with GigaVUE V Series Proxy.
Inbound	TCP	22	Administrator Subnet	Allows CLI access for user-initiated management and diagnostics,

				specifically when using third party orchestration.
Inbound	TCP	80	GigaVUE-FM	Allows GigaVUE V Series Proxy to receive the ACME challenge requests from the GigaVUE-FM.
Inbound	TCP	8300	GigaVUE V Series Node	Allows GigaVUE V Series Proxy to receive certificate requests from GigaVUE V Series Node for the configured params and provides the certificate using those parameters.
Inbound	TCP	8892	GigaVUE V Series Node IP	Allows GigaVUE V Series Proxy to receive registration requests and heartbeat messages from GigaVUE V Series Node.
Direction	Protocol	Port	Destination CIDR	Purpose
Outbound	TCP	443	GigaVUE-FM IP	Allows GigaVUE V Series Proxy to communicate the registration requests to GigaVUE-FM.
Outbound	TCP	8889	GigaVUE V Series Node IP	Allows GigaVUE V Series Proxy to communicate control and management plane traffic with GigaVUE V Series Node.

Ports for Backward Compatibility

Ensure to open these ports for backward compatibility when GigaVUE-FM is running version 6.10 or later, and the fabric components are on (n-1) or (n-2) versions.

GigaVUE V Series Node

The following table specifies the outbound communication requirement for GigaVUE V Series Node, detailing the protocol, port, and source CIDR used to send registration and heartbeat messages to the GigaVUE V Series Proxy during third-party orchestration.

Direction	Protocol	Port	Source CIDR	Purpose
Outbound (This is the port used for Third Party Orchestration)	TCP	8891	GigaVUE V Series Proxy IP	Allows GigaVUE V Series Node to send registration requests and heartbeat messages to GigaVUE V Series Proxy when GigaVUE V Series Proxy is used.

GigaVUE V Series Proxy(Optional)

The following table specifies the optional inbound communication parameter for GigaVUE V Series Proxy, detailing the protocol, port, and source CIDR required to receive security parameter requests from GigaVUE V Series Node during third-party orchestration.

Direction	Protocol	Port	Source CIDR	Purpose
Inbound (This is the port used for Third Party Orchestration)	TCP	8891	GigaVUE V Series Node IP	Allows GigaVUE V Series Proxy to receive security parameter requests from GigaVUE V Series Node.

Inline V Series (Azure)

The Inline V Series solution provides an advanced, scalable, agentless traffic acquisition mechanism that integrates seamlessly into your network. By deploying V Series Nodes in inline mode, you can mirror and process traffic efficiently while ensuring the reinjection of production traffic without disruption.

In AWS and Azure environments, the Inline V Series solution leverages Gateway Load Balancers (GWLb) to enable efficient traffic handling and visibility. This feature ensures low-latency performance, making it ideal for continuous traffic inspection and monitoring. Designed for simplicity and operational efficiency, the Inline V Series allows you to gain deep insights into network activity while maintaining high performance in demanding network environments.

You can use this solution for forwarding inline traffic and traffic processing. When traffic reaches the Inline V Series Node, a copy of the packet is taken as out-of-band traffic. You can forward the copied traffic to a GigaVUE V Series Node for additional processing or directly to monitoring tools. During boot-up, the Inline V Series Node initializes with the default Inline application.

A Monitoring Session is required to:

- Tap the inline traffic
- Create a copy for out-of-band forwarding
- Send the traffic to the desired tools.

Inline V Series Deployment Types

Single Tier Deployment

You can use this deployment model when traffic has to be tapped, filtered, and directly sent to tools without any processing.

Multi-Tier Deployment

Use this model when you need to process traffic through GigaVUE V Series applications before forwarding it to the tools. The first tier taps the traffic, and the second tier processes it using the GigaVUE V Series applications and forwards it to the tools.

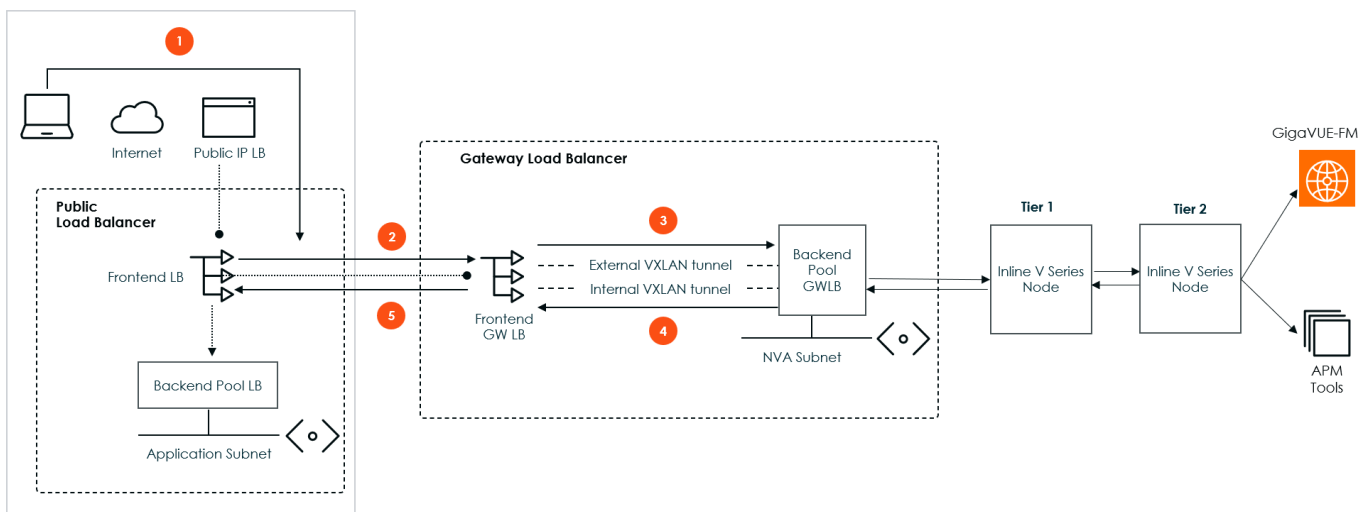
Architecture of Inline V Series Solution in Azure

Components required for configuring Inline V Series Solution in Azure:

- Application VNet
- Appliance VNet
- Public Load balancer
- Gateway Load balancer
- Inline V Series Node

Application VNet consists of multiple workload VMs, Public Load Balancer, Public IP Load Balancer, and Application Server in the Backend pool. The appliance VNet consists of Gateway Load Balancer, Inline V Series Node. Any traffic reaching the Gateway Load Balancer will be routed to the Inline V Series Node.

The below architecture diagram explains how the Inline V Series solution works:



Traffic from the internet to the application server:

1. The traffic from the internet is sent to the Public Load Balancer configured in Application VNet using an Public IP LB configuration.
2. This traffic is routed the Gateway Load balancer.
3. The Gateway Load Balancer in the Appliance VNet forwards the traffic to the Inline V Series Nodes. The following actions are performed in the Inline V Series Node:
 - Once the traffic reaches the Inline V Series Nodes, a copy of the packet is taken as out of band traffic.
 - The Out of Band traffic is forwarded to the GigaVUE V Series Node for further processing or it can be forwarded to the tools.
 - The Inline V Series swaps the IP address and the Mac of the packets, where the source and destination are interchanged. As a result the Inline V Series Node becomes the source and Gateway Load Balancer becomes the destination.

NOTE: Packets sent from the Gateway Load Balancer will be VXLAN encapsulated and forwarded to the Inline V Series Nodes.

4. The inline traffic is sent back to the Gateway Load Balancer.
5. The Gateway Load Balancer forwards the inline traffic to the application servers in the Application VNet.

For a detailed workflow on acquiring traffic through the Inline V Series, refer to [Deploy Inline V Series Solution in Azure](#).

Limitation

This solution can be implemented only to tap the North-South traffic.

Configure Custom Settings for Azure Secret and Top Secret Regions

This section explains how to configure GigaVUE Cloud Suite for Azure in Secret and Top Secret regions. These settings apply to users running Azure services in isolated environments where endpoints and regions are not publicly exposed.

GigaVUE-FM requires configuration options for service endpoint URLs, region settings, and CA certificates to connect to these isolated Azure environments.

NOTE: This feature has been tested and validated only in IPv4-only environments.

Refer to the following sections for more details.

Configure Service Endpoints

This section provides steps to configure custom service endpoint URLs in GigaVUE-FM to enable connectivity with Azure Secret and Top Secret regions. These regions use isolated service endpoints that differ from those in Azure Commercial or Azure Government clouds.

To configure Service Endpoints:

1. Go to **Inventory > VIRTUAL > Azure**.
2. Select **Settings > Custom Configuration**. The **Custom Configurations** page appears.
3. Select the **Custom Environment** tab and click **Create**.
4. On the **Configure Custom Environment** page, enter an **Environment Name** and the required service endpoint URLs:
 - a. **resourceManagerEndpointUrl** - Base HTTPS endpoint that GigaVUE-FM can use to reach the Azure management/control plane APIs for your environment.
 - b. **activeDirectoryEndpointUrl** - Base HTTPS endpoint for Azure Resource Manager (ARM) in your IL6 environment. All ARM API calls from GigaVUE-FM use this base URL.
 - c. **managementEndpointUrl** - Base HTTPS endpoint for Azure Active Directory in your IL6 environment. GigaVUE-FM will use this to obtain access tokens.



Notes:

- GigaVUE-FM does not provide or auto-discover the required endpoint URLs. You must obtain the correct URLs from official Microsoft documentation or your Azure administrator.
- Ensure that the URLs are valid HTTPS URLs.

5. Click **Save** to apply the custom environment configuration.

When creating or editing an Azure Credential in GigaVUE-FM, you can now select a custom environment that you have configured. Previously, only “**Azure**” and “**Azure US Government**” options were available. By choosing your custom environment, GigaVUE-FM will use the endpoints you specify, ensuring all connections align with your configuration. Refer to [Create Azure Credentials](#) for details.

Configure Custom Regions

This section explains how to define region entries that are not included in the SDK's predefined list. Secret and Top Secret regions require manual addition so GigaVUE-FM can recognize and interact with them during Monitoring Domain setup.

To configure Custom Regions:

1. Go to **Inventory > VIRTUAL > Azure**.
2. Select **Settings > Custom Configuration**. The **Custom Configurations** page appears.
3. Select the **Custom Region** tab and click **Create**.
4. On the **Configure Custom Region** page, enter the **Region Alias** and the exact **Region Name**. The Region Name can be user-defined (for example, East US or West US).
5. Click **Save**. The configured custom region will now be available for selection in the Monitoring Domain creation page. Refer to [Create Monitoring Domain](#) for details.

Import CA Certificate for Service Endpoints

Service endpoints in the secure regions may use TLS certificates signed by a Root CA that differs from the default trusted CAs in GigaVUE-FM. To establish secure HTTPS connections and validate server certificates, GigaVUE-FM must have the Root CA in its trust store. Importing the Root CA certificate ensures GigaVUE-FM can securely connect to the endpoints without certificate errors.

To Import Root CA into GigaVUE-FM Java Trust Store:

1. Obtain the required Root CA certificate file that signed the TLS certificate for your Azure Secret/Top Secret service endpoints.
2. Enter "**sudo keytool -keystore /usr/lib/jvm/java-17-openjdk-17.0.17.0.10-1.el8.x86_64/lib/security/cacerts -list**" in GigaVUE-FM. If prompted for a password, press Enter. The command lists the trusted Root CAs in the JDK trust store. Note the number of entries. The output includes a line such as: Your key store contains 146 entries. Here, the trust store contains 146 entries.
3. To import the Root CA into GigaVUE-FM, follow the steps listed below:
 - a. Copy the Root CA into GigaVUE-FM, for example, to "/home/admin" or "/home/azureuser".

```
[admin@GigaVUE-FM-6800 ~]$ ll
total 580
-rw----- 1 azureuser azureuser 4201 Nov 13 03:58 ca-chain.crt
```

- b. Import the certificate into JDK trust store:
 - I. Run: "sudo keytool -import -alias <RootCAalias> -keystore /usr/lib/jvm/java-17-openjdk-17.0.16.0.8-2.el8.x86_64/lib/security/cacerts -file <RootCA.crt file>".
 - II. When prompted for a password, enter the default trust store password: **"changeit"**.

- III. The command displays certificate details (fingerprints, extensions) and prompts: Trust this certificate? [no]: Type **yes** and press Enter.
- IV. After successful import, it will display "Certificate was added to keystore".
- V. Repeat Step I to verify the Root CA is in the trust store. The entry count increases by one, and the Root CA appears in the list with the alias you specified, for example:

.....

Your keystore contains 147 entries

.....

userca, Nov 13, 2025, trustedCertEntry

Certificate fingerprint (SHA-256):

BO:0C:D7:F1:0B:A2:12:4D:BB:AB:70:90:61:4C:6C:5A:9A:69:D8:49:94:E2:2B:E5:CE:62:72
:E1:8B:49:D1:62

.....

4. Restart the CMS process to apply the certificate import:

```
sudo systemctl restart tomcat@cms.service
```

NOTE: You must repeat the import steps when upgrading GigaVUE-FM.

Get_Started

Delete this text and replace it with your own content.

Deploy GigaVUE Cloud Suite for Azure Secret or Top Secret Regions

This chapter describes how to connect, launch, and deploy the fabric components of GigaVUE Cloud Suite for Azure Secret or Top Secret Regions.

Refer to the following topics for details:

- [Create Azure Credentials](#)
- [Integrate Private CA](#)
- [Adding Certificate Authority](#)
- [Create Monitoring Domain](#)
- [Configure GigaVUE Fabric Components](#)

Create Azure Credentials

You can monitor workloads across multiple Azure subscriptions within one monitoring domain. All the deployed GigaVUE fabric components are shared among many Azure subscriptions to reduce the cost. Earlier, each Azure subscription carried a set of GigaVUE fabric components.



- After launching GigaVUE-FM in Azure, the **Managed Identity** authentication credential is automatically added to the Azure Credential page as the default credential.
- You can only add the **Application ID with Client Secret** authentication credentials to the Azure Credential page.

Prerequisite

You can configure a custom environment in Azure. For detailed instructions, refer to [Configure Custom Settings for Azure Secret and Top Secret Regions](#).

To create Azure credentials,

1. Go to **Inventory > VIRTUAL > Azure**.
2. Select **Settings > Credential**.
3. In the Azure Credential page, select **Add**.

The **Configure Credential** wizard appears.

4. Enter or select the appropriate information for the Azure credential:

a. **Name:** An alias used to identify the Azure credential.

b. **Authentication Type:**

Application ID with Client Secret: Connection with Azure with a service principal. Enter the values for the following fields.

- **Tenant ID:** A unique identifier of the Azure Active Directory instance.
- **Application ID:** A unique identifier of an application in Azure platform.
- **Application Secret:** a password or key to request tokens.

For details on how to create service principal and assign custom roles, refer to [Application ID with client secret](#).

c. **Azure Environment:** Select an Azure environment where your workloads are located. For example, Azure_US_Government.

5. Select **Save**.

You can view the list of available credentials in the Azure Credential page.

Integrate Private CA

You can integrate your own PKI infrastructure with GigaVUE-FM.

Rules and Notes

- Always place the root CA in a separate file.
- When using multiple intermediate CAs, consider the following:
 - Include all intermediate CAs in a single file in the correct order.
 - Place the last intermediate CA in the chain at the top.
 - Place the preceding CAs in descending order.

To integrate private CA

- Generate a Certificate Signing Request (CSR).
- Get a signature of the Certificate Authority (CA) on the CSR.
- Upload CA Certificate to GigaVUE-FM.

Generate CSR

To create an intermediate CA certificate:

1. Go to  > **System > Certificates**.
2. In the top navigation bar, from the **PKI** drop-down list, select **CSR**. The **Generate Intermediate CA Certificate** page appears.
3. Enter details in the following fields:
 - **Country:** Enter the name of your country.
 - **Organization:** Enter the name of your organization.
 - **Organization Unit:** Enter the name of the department or unit.
 - **Common Name:** Enter the common name associated with the certificate.
4. From the **Algorithm** drop-down list, select the desired encryption algorithm used to encrypt your private key.
5. Select **Generate CSR**.

The CSR is downloaded successfully.

Upload CA Certificate

Get the CSR signed from your Enterprise PKI or any public PKI and upload the signed intermediate CA certificate to GigaVUE-FM.

To upload the signed CA certificate to GigaVUE-FM:

1. Go to  > **System > Certificates**.
2. In the top navigation bar, from the **PKI** drop-down list, select **CA**. The **CA Certificate** page appears.
3. From the **Actions** drop-down list, select **Upload CA**. The **Upload CA** pop-up appears.
4. Next to **Intermediate CA**, select **Choose File** to upload the signed intermediate CA certificate.
5. Next to **Root CA**, select **Choose File** to upload the corresponding root or intermediate CA.

The **CA Certificate** page displays the uploaded CA certificate.

Adding Certificate Authority

This section describes how to add CA Certificate chain Authority in GigaVUE-FM.

The CA Certificate chain List page allows you to add the root CA for the devices.

To upload the CA Certificate chain using GigaVUE-FM, follow these steps:

1. Go to **Inventory > Resources > Security > CA List**.
2. Select **Add**, to add a new Custom Authority.
The **Add Certificate Authority** page appears.

3. In the **Alias** field, enter the alias name of the CA Certificate chain Authority
4. Use one of the following options to enter the CA Certificate chain Authority:
 - **Copy and Paste:** In the **Certificate** field, enter the certificate.
 - **Install from URL:** In the **Path** field, enter the URL in the format: <protocol>://<username>@<hostname/IP address>/<file path>/<file name>. In the **Password** field, enter the password.
 - **Install from Local Directory:** Select **Choose File** to browse and select a certificate from the local directory.
5. Select **Save**.

Create Monitoring Domain

A Monitoring Domain in GigaVUE-FM allows you to define and manage this connection. Once established, GigaVUE-FM can deploy and manage GigaVUE V Series Proxy, and GigaVUE V Series Nodes within your specified VNets and Resource Groups.

GigaVUE-FM connects to Azure using either an Application ID and Client Secret (Service Principal) or the Managed Service Identity (MSI) authentication method.

Prerequisite

- Before configuring, you must establish a connection between GigaVUE-FM and your Azure environment.
- You configure a custom Region in Azure before creating a Monitoring Domain. For detailed instructions, refer to [Configure Custom Settings for Azure Secret and Top Secret Regions](#).

To create an Azure monitoring domain in GigaVUE-FM,

1. Go to **Inventory > VIRTUAL > Azure**
2. Select **Monitoring Domain**.

The **Monitoring Domain** page appears.

3. In the Monitoring Domain page, select **New**.

The **Azure Monitoring Domain Configuration** wizard appears.

4. Enter or select the appropriate information for the Monitoring Domain:

- **Monitoring Domain:** An alias used to identify the monitoring domain.
- **Traffic Acquisition Method:** Select Inline as the Tapping method:
 - **Inline:** You can directly capture the inline traffic from the instances.
- **Use FM to Launch Fabric:** Select **Yes** to [Configure GigaVUE Fabric Components in GigaVUE-FM](#) or select **No** to [Configure GigaVUE Fabric Components](#).
- **Connections:**

Connections

- A Monitoring Domain can have multiple connections, however only one connection can have **Managed Service Identity** as the **Credential**.
- The connections in a monitoring domain can be a combination of multiple **Application ID with Client Secret** (Service Principal) accounts, or one **Managed Service Identity** and multiple **Application ID with Client Secret** (Service Principal) accounts.
- Each connection can have only one **Subscription ID**.
- **Name:** An alias used to identify the connection.
- **Credential:** Select an Azure credential. For details, refer to [Create Azure Credentials](#).
- **Subscription ID:** A unique alphanumeric string that identifies your Azure subscription.
- **Region:** Azure region for the monitoring domain. For example, West India.

- **Resource Groups:** Select the Resource Groups of the corresponding VMs to monitor.

**Notes:**

- This field is not applicable if you select **Customer Orchestrated Source** as the **Traffic Acquisition Method**.
- When you remove and re-add a resource group in IAM, it won't appear in GigaVUE-FM automatically. To refresh the list and make the resource group selectable, reselect the Subscription ID from the drop down. This action triggers the UI to reload the resource groups associated with the selected subscription.

5. Select **Save**.

The **Azure Fabric Launch Configuration** wizard appears.

**Notes:**

- Ensure that all V Series Nodes within a single Monitoring Domain are running the same version. Mixing different versions in the same Monitoring Domain may lead to inconsistencies when configuring Monitoring Session traffic elements.
- Similarly, when upgrading a V Series Node, ensure that the GigaVUE-FM version is the same or higher than the V Series Node version.
- You can only view and delete the existing configuration for GigaVUE V Series Node 1. You cannot perform any other actions on the existing configuration for GigaVUE V Series Node 1 as the features are deprecated from GigaVUE-FM.

Check Permissions while Creating a Monitoring Domain

NOTE: The Check Permissions feature is not available when the **Traffic Acquisition Method** is **vTAP**.

To check the permissions while creating a monitoring domain, follow these steps:

1. Go to **Inventory > VIRTUAL > Azure**.
2. Select **Monitoring Domain**. The **Monitoring Domain** page appears.
3. Select **New**. The **Monitoring Domain Configuration** page appears.
4. Enter the details as mentioned in the Create Monitoring Domain section.
5. Select **Check Permission**. The **Check Permissions** widget opens.
6. Select the connection for which you wish to check the required permissions and then click **Next**.
7. Select the **Permission Status** tab to view the missing permissions. The **PERMISSIONS** tab lists the permissions required to run GigaVUE Cloud Suite for Azure.
8. Make sure to include all the permissions with Access Status as 'Denied' in the IAM policy.

The **IAM POLICY** tab lists the sample policy containing the required permissions for deploying the GigaVUE Cloud Suite for Azure. You must update the Azure IAM policy with the missing permissions that are highlighted in the JSON. To recheck the IAM policy, go to the **PERMISSIONS** tab and select the **Recheck** button.

Check Permissions



Connection Selection



Permissions

Click on the permission status to view the missing permissions for the selected connection.

CONNECTION	PERMISSION STATUS	CREDENTIAL	REGION
C	 Success	sriram-cred	West US

Go to page: 1 of 1
1 permissions total

PERMISSIONS
IAM POLICY

Below is the sample policy containing the required permissions for deploying the GigaVUE Cloud Suite.

Copy
Download

i You must update the AZURE IAM Policy with the missing permissions that are highlighted in the JSON. To recheck the IAM Policy, go to the Permissions tab and click the Recheck button.

```

{
  "properties": {
    "roleName": "GigaVUE-FM-Service-Role",
    "description": "The minimum required permissions for FM to deploy GigaVUE Cloud Suite",
    "assignableScopes": [
      "6447eb55-9d09-481b-89bc-52e96bb52823",
      "d719fcb1-0d1a-43a8-bf8e-7844e293ce1a"
    ],
    "permissions": [
      {
        "actions": [
          "Microsoft.Authorization/roleAssignments/read",
          "Microsoft.Compute/disks/delete",
          "Microsoft.Compute/images/read",
          "Microsoft.Compute/virtualMachines/delete",
          "Microsoft.Compute/virtualMachines/powerOff/action",
          "Microsoft.Compute/virtualMachines/read",
          "Microsoft.Compute/virtualMachines/restart/action",
          "Microsoft.Compute/virtualMachines/start/action",
          "Microsoft.Compute/virtualMachines/vmSizes/read",
          "Microsoft.Compute/virtualMachines/write",
          "Microsoft.Network/networkInterfaces/delete",
          "Microsoft.Network/networkInterfaces/join/action",
          "Microsoft.Network/networkInterfaces/read",
          "Microsoft.Network/networkInterfaces/write",
          "Microsoft.Network/networkSecurityGroups/join/action",
          "Microsoft.Network/networkSecurityGroups/read",
          "Microsoft.Network/publicIPAddresses/delete",
          "Microsoft.Network/publicIPAddresses/join/action",
          "Microsoft.Network/publicIPAddresses/read",
          "Microsoft.Network/publicIPAddresses/write",
          "Microsoft.Network/virtualNetworks/read",
          "Microsoft.Network/virtualNetworks/subnets/join/action",
          "Microsoft.Resources/subscriptions/read",
          "Microsoft.Resources/subscriptions/resourceGroups/read"
        ],
        "notActions": [],
        "dataActions": [],
        "notDataActions": []
      }
    ]
  }
}

```

Back
Close

You can use the **Copy** button to copy the permissions to the clipboard. Also, you can use the **Download** button to download the permission in JSON format.

NOTE: After updating the IAM Policy, it takes around 5 minutes for the changes to reflect on the Check Permissions screen.

Configure GigaVUE Fabric Components

You can use your own orchestration system to deploy the GigaVUE fabric components instead of using GigaVUE-FM to deploy the fabric components.

The GigaVUE fabric components register themselves with GigaVUE-FM using the information provided by you. Once the nodes are registered with GigaVUE-FM, you can configure monitoring sessions and related services in GigaVUE-FM. After launching the fabric component images in your orchestration system use the registration data provided in the sections below to deploy your fabric components to GigaVUE-FM. Health status of the registered nodes is determined by the heartbeat messages sent from the respective nodes.

This section provides step-by-step information on how to register GigaVUE fabric components using your own orchestration system or a configuration file.

Configure GigaVUE V Series Node and GigaVUE V Series Proxy

NOTE: It is not mandatory to register GigaVUE V Series Nodes via V Series proxy however, if there are a large number of nodes connected to GigaVUE-FM or if you do not wish to reveal the IP addresses of the nodes, then you can register your nodes using GigaVUE V Series Proxy. In this case, GigaVUE-FM communicates with GigaVUE V Series Proxy to manage the GigaVUE V Series Nodes.

To register GigaVUE V Series Proxy or node after launching the instance using a configuration file, follow the steps given below:

1. Log in to the GigaVUE V Series Proxy or Node.
2. Create a local configuration file (**/etc/gigamon-cloud.conf**) and enter the following custom data.

Registration:

```
groupName: <Monitoring Domain Name>
subGroupName: <VPC ID>
token: <Token>
remoteIP: <IP address of the GigaVUE-FM> or
          <IP address of the Proxy>
remotePort: 443
```



- You can register your GigaVUE V Series Node directly with GigaVUE-FM or you can use V Series proxy to register your GigaVUE V Series node with GigaVUE-FM. If you wish to register GigaVUE V Series Node directly, enter the **remotePort** value as 443 and the **remoteIP** as *<IP address of the GigaVUE-FM>* or if you wish to deploy GigaVUE V Series node using GigaVUE V Series proxy then, enter the **remotePort** value as 8891 and **remoteIP** as *<IP address of the Proxy>*.
- Use only the default **user** and **password** details given in the custom data.

3. Restart the GigaVUE V Series proxy or node service.

- GigaVUE V Series node:
`$ sudo service vseries-node restart`
- GigaVUE V Series proxy:
`$ sudo service vps restart`

The deployed GigaVUE V Series proxy or node registers with the GigaVUE-FM.

After successful registration, the fabric components send heartbeat messages to GigaVUE-FM every 30 seconds. If one heartbeat is missing, the visibility node status appears as 'Unhealthy'. If more than five heartbeats fail to reach GigaVUE-FM, GigaVUE-FM tries to reach the fabric components and if that fails GigaVUE-FM unregisters the fabric component and it will be removed from GigaVUE-FM.

Deploy Inline V Series Solution in Azure

NOTE: Click the following prompt to generate a quick deployment checklist for this topic.

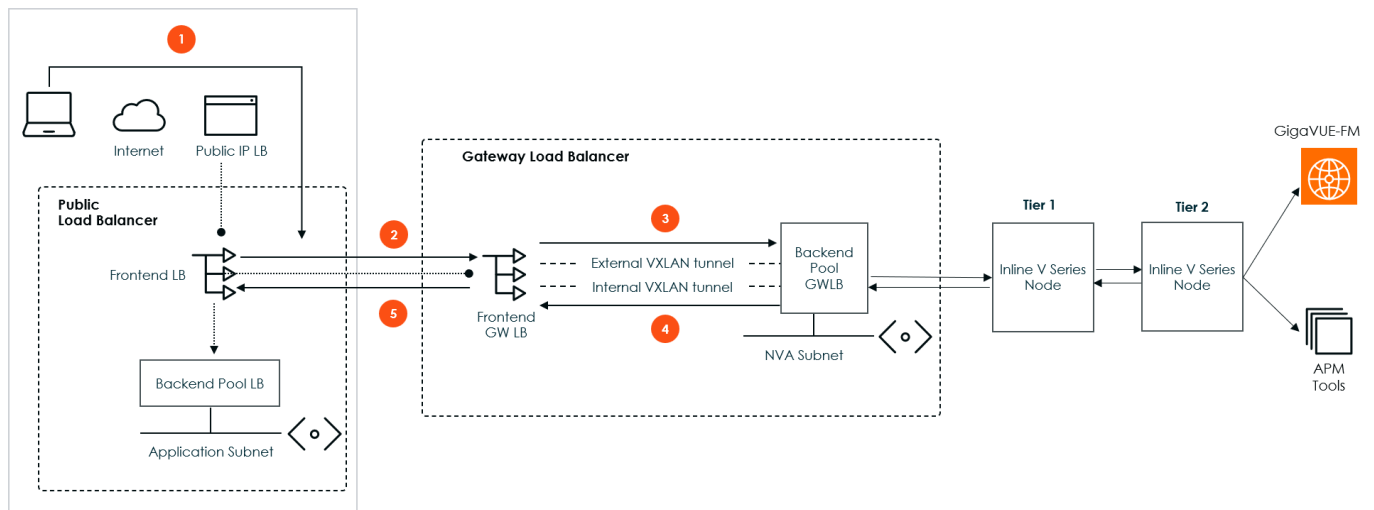
Create a comprehensive checklist based on the deployment steps outlined in the Deploy Inline V Series Solution in Azure topic.

This section outlines the work flow for acquiring traffic using Inline V Series Node and deploying GigaVUE Fabric Components using Third Party Orchestration. It provides instructions to configure traffic acquisition, processing, and forwarding to your desired destination.

Prerequisite

Ensure that you configure a custom environment and a custom region in Azure before creating a Monitoring Domain. For detailed instructions, refer to [Configure Custom Settings for Azure Secret and Top Secret Regions](#).

Note: The work flow described in this section is based on the topology shown below. The approach for acquiring traffic depends on your specific requirements. Additionally, you can decide whether to route traffic through public load balancer based on your topology.



Refer to the following topics to deploy Inline V Series in Azure:

- [Create a Resource Group](#)
- [Create Virtual Networks](#)
- [Create a Virtual Network Peering](#)
- [Create a Network Security Group](#)
- [Create a Load Balancer](#)
- [Install GigaVUE-FM on Azure](#)
- [Enable System Assigned Managed Identity](#)
- [Create Gigamon Custom Role](#)
- [Assign Role to Resource Group](#)
- [Assign Role to GigaVUE-FM Instance](#)
- [Create a GigaVUE-FM Token](#)
- [Modify Virtual Machine Scale Set \(VMSS\) Cloud Initialization Template](#)
- [Create a Virtual Machine Scale Set for Inline GigaVUE V Series Node \(Tier 1\)](#)
- [Assign VMSS to GWLB Backend Pools](#)
- [Create Monitoring Domain](#)
- [Deploy GigaVUE V Series Nodes for Inline V Series Solution](#)
- [\(Optional\) Create a Virtual Machine Scale Set for Out-of-Band GigaVUE V Series Node \(Tier 2\)](#)
- [Configure Monitoring session](#)

Create a Resource Group

The resource group is a container that holds all the resources for a solution. Select an existing resource group or create a new resource group. For navigation steps and detailed instructions, refer to [Create a resource group](#) topic in the Azure Documentation.

NOTE: We recommend creating a dedicated Resource Group for GigaVUE Visibility Fabric components such as GigaVUE-FM, V Series Nodes, Gateway Load Balancer, and others.

Create Virtual Networks

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. You can choose to:

- Select an existing VNet: When you choose an existing VNet, Azure automatically populates the Subnet and Public IP fields.
- Create a new VNet: To create a new VNet, follow the steps in the [Create a virtual network](#) topic in the Azure Documentation

NOTE: We recommend setting up two separate virtual networks to support the GigaVUE Visibility Fabric. The first VNet (Viz_VNet) will host the GigaVUE visibility components such as GigaVUE-FM and V Series Nodes. The second VNet (App_VNet) will contain the virtual machines responsible for generating traffic.

Create a Virtual Network Peering

When workload virtual machines are distributed across multiple virtual networks, you must enable Virtual Network Peering between each workload VNet and the VNet hosting the GigaVUE V Series Node. This peering setup allows seamless communication between VNets within Azure.

To set up peering between the two VNets you created, refer to [Manage a virtual network peering](#) topic in Azure documentation.

Create a Network Security Group

Network Security Groups (NSGs) filter inbound and outbound traffic to subnets and network interfaces using security rules. You should configure the Network Security Group to allow GigaVUE-FM to communicate with the rest of the components. Select an existing network security group or create a new network security group. For navigation steps and detailed instructions, refer to [Create a network security group](#) topic in the Azure Documentation.

Create a Load Balancer

Gigamon deploys its solution as a Network Virtual Appliance positioned behind a Gateway Load Balancer. To ensure traffic flows through the V Series, it must be routed to the GWLB. You can achieve this routing either via a Standard Load Balancer or directly from a virtual machine's public interface. Microsoft recommends using a Standard Load Balancer for optimal integration.

Refer to the following sections for information on creating a Gateway Load Balancer and Standard Load Balancer:

Create a Gateway Load Balancer

Set up a Gateway Load Balancer (GWLB), which will later forward traffic to the Tier 1 V Series Node. Once deployed, the Tier 1 V Series Node will mirror packets from the workload virtual machines, enabling traffic visibility.

The following table lists the specific options you must select when creating a Gateway Load Balancer for an inline V Series deployment. For navigation steps and detailed instructions, refer to [Create a Gateway Load Balancer](#) topic in Azure documentation.

Parameters	Description	Mandatory field
Basics		
Subscription	Select your subscription	Yes
Resource Group	Select the Inline V Series Resource Group that you created	Yes
Name	Enter a valid name	Yes
Region	Select the region	Yes
SKU	Select Gateway	Yes
Type	Select Internal	Yes
Tier	Select Regional (default)	Yes
FrontEnd IP Configuration - Add a frontend IP configuration		
Name	Enter a valid name	Yes
IP Version	Select based on the requirement	Yes
Virtual Network	Select your virtual network	Yes
Subnet and IP Assignment	Select your subnet and choose Dynamic for assignment	Yes
Backend Pools - Add a backend pool		
Name	Enter a valid name	Yes
Virtual Network	Default	Yes
Backend Pool Configuration	Select NIC	Yes
Gateway load balancer configuration		
Type	Choose Internal and External .	Yes
Internal and External Ports	Use default values Note: If you change the port values here, update the same ports in the Custom data and cloud-init field when creating the Virtual Machine Scale Set	Yes

Parameters	Description	Mandatory field
NOTE: Add backend pool without IP Configuration (you will attach NICs later in this step Assign VMSS to GWLB Backend Pools).		
Inbound Rules - Add a load balancing rule		Yes
Name	Enter a valid name	Yes
IP Version	Select IPv4 or IPv6	Yes
Frontend IP Address	Select an existing Frontend IP from the drop-down list	Yes
Backend Pool	Select an existing Backend pool from the drop-down list	Yes
Session Persistence	Select None	Yes
Health Probe	Select Create New and enter the following details: - Protocol - Select HTTP as the protocol - Port - Enter 8888 as the port - Path: /health - Interval - Enter 5 seconds as the approximate amount of time, in seconds	Yes
Idle timeout (minutes)	Leave default or adjust as required	Yes

(Optional) Create a Standard Load Balancer

NOTE: Routing traffic through a public load balancer is optional and applies only to the topology shown at the beginning of this document. Alternatively, you can route traffic to the Gateway Load Balancer from a VM that has an interface with a public IP.

The following table lists the specific options you must select when creating a Standard Load Balancer for an inline V Series deployment. For navigation steps and detailed instructions, refer to [Create a Public Gateway Load Balancer](#) topic in Azure documentation.

For details regarding traffic flow from Gateway Load Balancer to Standard Load Balancer, refer to [Gateway Load Balancer](#) topic in Azure documentation.

Parameters	Description	Mandatory field
Basics		
Subscription	Select your subscription	Yes
Resource Group	Select the Inline V Series Resource Group that you created	Yes
Name	Enter a valid name	Yes
Region	Select the region	Yes
SKU	Select Standard	Yes
Type	Select Public (validated type)	Yes

Parameters	Description	Mandatory field
Tier	Select Regional	Yes
FrontEnd IP Configuration - Add a frontend IP configuration		
Name	Enter a valid name	Yes
IP Version	Select IPv4	Yes
IP Type	Select IP Address as the IP type	Yes
Public IP address	Select the public IP address from the drop-down list. If required, you can create a new IP address	Yes
Gateway Load Balancer	Select the Gateway Load Balancer you created in the previous step to associate it with the frontend IP configuration	Yes
Backend Pools - Add a backend pool		
Name	Enter a valid name	Yes
Virtual Network	Select the same virtual network as the Standard Load Balancer —typically the App VNet—to ensure communication with the workloads.	Yes
Backend Pool Configuration	Select IP Address	Yes
IP Address	Specify the private IP address of the source/customer VM	
Inbound Rules - Add a load balancing rule		Yes
Name	Enter a valid name	Yes
IP Version	Select IPv4	Yes
Frontend IP Address	Select an existing Frontend IP from the drop-down list	Yes
Backend Pool	Select an existing Backend pool from the drop-down list	Yes
Protocol	Select TCP as the protocol	Yes
Port	Enter 80 as the port	Yes
Backend Port	You can configure the backend port to match the frontend port. Enter a value based on your traffic requirements	Yes
Health Probe	Select Create new and create a new Health Probe with TCP Protocol, Port 80, and 5-second attempt interval	Yes
Session Persistence	Select None	Yes
Idle timeout (minutes)	Enter or select 4	Yes
Outbound Rules -		
Name	Enter a valid name	Yes
IP Version	Select IPv4	Yes
Frontend IP Address	Select an existing Frontend IP from the drop-down list.	Yes
Protocol	All	Yes
Idle timeout (minutes)	Enter or select 4	Yes

Parameters	Description	Mandatory field
TCP Reset	Enabled	Yes
Backend Pool	Select an existing Backend pool from the drop-down list.	Yes
Port Allocation	Use the default number of outbound ports	Yes

Install GigaVUE-FM on Azure

To install GigaVUE-FM using the Azure Marketplace:

1. Go to Azure Marketplace and search for Gigamon. The latest version of Gigamon GigaVUE Cloud Suite for Azure appears. Click **Get it Now**.
2. In the pop-up window, select the **GigaVUE-FM (Fabric Manager) vX.XX - BYOL** option and click Continue.
3. Select the "**Want to deploy programmatically? Get started**" link.
4. Review the terms of service and the subscription name, and then select Enable. Click **Save**.
5. Verify the selected **Subscription** and **Plan**, then click **Create**.

6. Configure the GigaVUE-FM VM details. Most fields are pre-populated, but some require manual input. Enter the details as mentioned in [Table 1: GigaVUE-FM Installation Steps](#). For detailed instructions, refer to [Create a Linux virtual machine in the Azure](#) in Azure Documentation.

Table 1: GigaVUE-FM Installation Steps

Field	Description
Basics	
Subscription	Select your subscription.
Resource Group	Select the Inline V Series Resource Group that you created.
System-assigned managed identity	Use a system-assigned managed identity when a resource needs to authenticate to other services, and you want the identity to be created and deleted with the resource. Note: If you update any role it would take more than an hour to reflect in GigaVUE-FM, however, if you use APP registration it would take between 5-10 minutes to update in GigaVUE-FM.
Virtual machine name	Enter a name for the VM.
Region	Select a region for Azure VM.
Availability Zone	Choose your availability zone
Security Type	To enable UEFI secure boot, select Trusted launch virtual machines from the drop-down list. Click Configure security features and ensure that the Enable secure boot check box is enabled.
Image	Select the latest GigaVUE-FM images. NOTE: You cannot select multiple images for a VM.
Size	Select the recommended instance type: GigaVUE-FM - Standard_D4s_v3
Authentication Type	We support only SSH public key authentication type - SSH public key - Enter the administrator username for the VM. - Enter the SSH public key pair name. - Password - Enter the administrator username for the VM. - Enter the administrator password. NOTE: The username "gigamon" is reserved for internal usage. Do not create a user with the name "gigamon"
Disks	

Field	Description
Disk Size	The required disk size for GigaVUE-FM is 2 x 40GB .
Networking	
Virtual Network	Select the virtual network that you created.
Configure network security group	Select the network security group that you created.

NOTE: Verify the summary before proceeding to create. It will take several minutes for the VM to initialize. After the initialization is completed, you can verify the VM through the Web interface.

After the deployment, navigate to the VM overview page, copy the **Public IP address**, and paste it in a new web browser tab.

If GigaVUE-FM is deployed in Azure, use **admin123A!!** as the password for the **admin** user to login to GigaVUE-FM. You must change the default password after logging in to GigaVUE-FM.

Enable System Assigned Managed Identity

Managed Identity (MSI) is a feature of Azure Active Directory. When you enable MSI on an Azure service, Azure automatically creates an identity for the service VM in the Azure AD tenant used by your Azure subscription.

To enable MSI on the VM running in GigaVUE-FM using the Azure portal, refer to [Configure managed identities using the Azure portal](#) in the Azure documentation.

Create Gigamon Custom Role

When you first connect GigaVUE-FM to Azure, you need the appropriate authentication for Azure to verify your identity and check if you have permission to access the resources that you are requesting. This is used for GigaVUE-FM to integrate with Azure APIs and to automate the fabric deployment and management.

IMPORTANT: "Microsoft.Authorization/roleAssignments/read" permission is required for validating the required permissions. Ensure to include "Microsoft.Authorization/roleAssignments/read" permission in your IAM policy.

The 'built-in' roles provided by Microsoft are open to all resources. Refer to [Create or update Azure custom roles](#) topic in the Azure documentation to update the policy with the relevant IAM service.

After completing the configuration in the Basics, Permissions, and Assignable Scopes sections, copy the permissions listed below and paste them into the JSON code to create a custom role.

NOTE: Ensure to assign the roles for the permissions listed below at the subscription level.

```
{
  "Name": "CustomRoleForInline",
  "description": "Minimum requirements for FM in inline tapping",
  "assignableScopes": [
    "/subscriptions/<Subscription ID>"
  ],
  "permissions": [
    {
      "actions": [
        "Microsoft.Resources/subscriptions/read",
        "Microsoft.Resources/subscriptions/resourceGroups/read",
        "Microsoft.Network/virtualNetworks/read",
        "Microsoft.Network/loadBalancers/read",
        "Microsoft.Network/loadBalancers/backendAddressPools/read",
        "Microsoft.Network/loadBalancers/backendAddressPools/backendPoolAddresses/read",
        "Microsoft.Compute/virtualMachineScaleSets/read",
        "Microsoft.Compute/virtualMachineScaleSets/virtualMachines/read",
        "Microsoft.Compute/virtualMachineScaleSets/virtualMachines/networkInterfaces/read",
        "Microsoft.Compute/virtualMachineScaleSets/virtualMachines/networkInterfaces/ipConfigurations/read",
        "Microsoft.Compute/virtualMachines/read"
      ],
      "notActions": [],
      "dataActions": [],
      "notDataActions": []
    }
  ]
}
```

NOTE: Ensure you maintain the exact indentation and order shown in the code snippet when copying and pasting it. Any changes in formatting or order may cause errors or prevent the code from working correctly. We recommend copying the indentation from the online documentation for complete accuracy.

Assign Role to Resource Group

You can specify where the custom role is available for assignment such as a management group, subscription, or resource group and assign the created role to the resource group you created. In Azure, locate your newly created Role by navigating to "Management Groups"

and selecting your subscription Id.

For further navigation and instructions to assign a role to your resource group, refer to the steps listed in **Update a custom role** and **Assignable scopes** sections of the [Create or update Azure custom roles](#) topic in the Azure documentation.

Assign Role to GigaVUE-FM Instance

You can assign the custom role you have created to GigaVUE-FM instance in Azure. For navigation path and detailed instructions, follow the steps listed in **Open the Add role assignment page**, **Select the appropriate role**, and **Select who needs access** sections of the [Assign Azure roles using the Azure portal](#) topic in the Azure documentation.

Create a GigaVUE-FM Token

GigaVUE-FM allows you to generate a token only if you are an authenticated user and based on your privileges in accessing the GigaVUE-FM. You can create multiple tokens if required.

To create a token in GigaVUE-FM, follow these steps:

1. Go to , select **Authentication > GigaVUE-FM User Management**. The **User Management** page appears.
2. In the **User Management** page, select **Tokens**.

NOTE: If you are a user with write access, then you can view a drop- down list under **Tokens**. Select **Current User Tokens** to create a token.

3. Select **New Token**.
4. Enter a name for the new token in the **Name** field.
5. Enter the days until the token is valid in the **Expiry** field.
6. Select the user group for which you are privileged to access GigaVUE-FM from the **User Group** drop-down list.
7. Select **OK** to generate a new token. The generated token appears on the **Tokens** page.
8. Select the token to copy and use it to authenticate the GigaVUE-FM REST APIs.
 - a. Go to **Actions > Copy Token**.
 - b. Paste the copied token in the required fields to complete authentication.

NOTE: You cannot view the generated token. You can only copy and paste the generated token.

Modify Virtual Machine Scale Set (VMSS) Cloud Initialization Template

The script given below will be essential for creating the VMSS, which uses this data to deploy the V Series node. This information is also required when configuring the Monitoring Domain in GigaVUE-FM.

Ensure you save these values in a secure location for reference in the upcoming steps. You can modify only the following parameters in the template:

- groupName
- subGroupName
- remoteIP
- Token

Custom Template:

NOTE: Ensure you maintain the exact indentation and order shown in the code snippet when copying and pasting it. Any changes in formatting or order may cause errors or prevent the code from working correctly. We recommend copying the indentation from the online documentation for complete accuracy.

```
#cloud-config
write_files:
- path: /etc/gigamon-cloud.conf
  owner: root:root
  permissions: '0644'
  content: |
    Registration:
      groupName: <Monitoring Domain Name>
      subGroupName: <Connection Name>
      remoteIP: <IP address of the GigaVUE-FM>
      remotePort: 443
      token: <token>

- path: /etc/vseries-inline.conf
  owner: root:root
  permissions: '0644'
  content: ""
```

Create a Virtual Machine Scale Set for Inline GigaVUE V Series Node (Tier 1)

V Series Nodes are created as part of a Virtual Machine Scale Set (VMSS) to allow scaling based on demand. This setup enables you to scale out or scale in the number of V Series Nodes as needed for each tier. Therefore, each tier will have a dedicated VMSS. The inline V Series solution does not support standalone V Series Nodes that are not part of a scale set.

The following table lists the specific options you must select when creating a Virtual Machine Scale Set for an inline V Series deployment. For navigation steps and detailed instructions, refer to [Create a Virtual Machine Scale Set](#) topic in Azure documentation.

Parameters	Description	Mandatory field
Subscription	Select your subscription	Yes
Resource Group	Select the Inline V Series Resource Group	Yes
Virtual Machine Scale Set Name	Enter a valid name	
Region	Select a desired region	
Availability Zones	Choose if you want to use zones for high availability.	No
Orchestration		
Orchestration Mode	Select Uniform as the orchestration mode.	Yes
Security Type	Select Standard mode.	Yes
Scaling		
Scaling Mode	Choose Autoscaling .	Yes
Scaling Configuration	Click Configure to edit the scaling conditions.	Yes
Default Condition	Enter the Initial Instance Count as 0. NOTE: Once the Monitoring Domain and connection is configured, edit this value to the number of GigaVUE V Series Node that you need to deploy in this Monitoring Domain.	Yes
Condition	Choose a metric-based scaling condition (For example, CPU usage, network traffic).	Yes
Metric Source	Select the metric (For example, Average CPU Percentage).	Yes
Scale out	Set conditions like greater than 70% for scaling up.	Yes
Scale in	Set conditions like less than 20%.	
Cooldown Period	Set a cooldown period to prevent rapid scaling.	Yes
Instance Details		
Instance Type	Choose Standard_D4S_v4 as the VM size.	
Image	Select the GigaVUE V Series Node image.	
Authentication Type	Choose SSH public key.	
Username	Enter a user name. Do not use admin or gigamon.	
Networking		
Virtual Network	Select the required VNet.	Yes
Subnet Selection	Choose the appropriate subnet for Inline V Series Node.	Yes
NIC Configuration	GigaVUE V Series Node requires two NICs—one for management and one for mirrored data traffic. To configure the Data NIC, add a second network interface, select	Yes

Parameters	Description	Mandatory field
	the appropriate subnet and network security group (NSG), and enable Accelerated Networking.	
Management		

Parameters	Description	Mandatory field
Upgrade Mode	Choose Automatic .	Yes
Advanced		
Custom data and cloud init	Enter the Custom Template modified in step Modify Virtual Machine Scale Set (VMSS) Cloud Initialization Template as text in the following format and deploy the instance. The GigaVUE V Series Nodes uses this user data to generate config files (/etc/gigamon-cloud.conf and /etc/vseries-inline.conf) and register with GigaVUE-FM using Third Party Orchestration. NOTE: Ensure you maintain the exact indentation and order shown in the code snippet when copying and pasting it. Any changes in formatting or order may cause errors or prevent the code from working correctly. We recommend copying the indentation from the online documentation for complete accuracy. <pre>#cloud-config write_files: - path: /etc/gigamon-cloud.conf owner: root:root permissions: '0644' content: Registration: groupName: <Monitoring Domain Name> subGroupName: <Connection Name> remoteIP: <IP address of the GigaVUE-FM> remotePort: 443 token: <token> - path: /etc/vseries-inline.conf owner: root:root permissions: '0644' content: ""</pre> Custom Data with Internal and External Ports If you have modified the internal and external port values in the Gateway Load Balancer, use the following custom data: <pre>#cloud-config write_files: - path: /etc/gigamon-cloud.conf owner: root:root permissions: '0644' content: Registration:</pre>	Yes

Parameters	Description	Mandatory field
	<pre> groupName: <Monitoring Domain Name> subGroupName: <Connection Name> remoteIP: <IP address of the GigaVUE-FM> remotePort: 443 token: <token> - path: /etc/vseries-inline.conf owner: root:root permissions: '0644' content: tunnel: vxlan external_port : <Enter the port value> external_vni : <Enter the port value> internal_port : <Enter the port value> internal_vni : <Enter the port value> </pre>	

Assign VMSS to GWLB Backend Pools

Identify the Gateway Load Balancer you created in [Create a Load Balancer](#) step. To attach the Data NIC of the VMSS to the Gateway Load Balancer:

1. In the Azure portal, navigate to the Gateway Load Balancer you created earlier.
2. From the main page, go to **Settings** and select **Backend Pool**.
3. Locate the Virtual Network (VNet) where your VMSS is deployed.
4. Click **+ Add** under **IP Configuration**.
5. In the pop-up window, search for the Data NIC associated with your VMSS.
6. Select the NIC and click **Add**.
7. Click Save to apply the changes.

Create Monitoring Domain

Azure Load Balancer launches and manages GigaVUE V Series Node that is registered with GigaVUE-FM.

To deploy GigaVUE V Series Node with Gateway Load Balancing in GigaVUE-FM:

1. Go to **Inventory > VIRTUAL > Azure**.
2. Select **Monitoring Domain**.
3. On the Monitoring Domain page, select **New**.
4. On the **Monitoring Domain Configuration** page, select **Inline** as the Traffic Acquisition method.

5. Enter the **Monitoring Domain** Name and the **Connection** Name as mentioned in the user data provided during the template launch in Azure. Refer to Advanced section in [Create a Virtual Machine Scale Set for Inline GigaVUE V Series Node \(Tier 1\)](#).
6. (Optional) Turn on the **Use FM to launch Proxy** toggle to launch the GigaVUE V Series Proxy using GigaVUE-FM.

NOTE: You can use GigaVUE V Series proxy if GigaVUE-FM cannot directly reach the GigaVUE V Series Nodes (management interface) directly over the network. GigaVUE V Series Proxy is an optional component.

- a. From the **Image** drop-down list, select the required image.
 - b. From the **Size** drop-down list, select the instance size.
 - c. For **Number of Instances**, specify the required number of instances.
 - d. For **Management Subnet**:
 - a. Select the **IP Address Type** as Private or Public.
 - b. From the **Subnet** drop-down list, select the management subnet.
 - c. Select **Add Subnet** under **Additional Subnets** to add additional subnets.
 - e. Select **Add** under **Tags** to assign tags for resource identification.
7. Select **Save**.

Deploy GigaVUE V Series Nodes for Inline V Series Solution

When the Monitoring Domain is created successfully you will be navigated to the **Azure Fabric Launch Configuration** page in GigaVUE-FM automatically.

1. From the **Connections** drop-down list, select the required connection that you have configured.



Note:

After configuring the Monitoring Domain and establishing the connection, update the **Default Condition** count in the following steps based on the number of GigaVUE V Series Nodes you want to deploy within the Monitoring Domain:

- [Create a Virtual Machine Scale Set for Inline GigaVUE V Series Node \(Tier 1\)](#)
- (Optional) [Create a Virtual Machine Scale Set for Out-of-Band GigaVUE V Series Node \(Tier 2\)](#)

Adjust the instance count in the scale set to match the required number of nodes for your deployment.

2. Select the required resource group from the **Resource Group** drop-down list.
3. From the **Gateway Load Balancer** drop-down list, select the Load Balancer configured in Azure.

4. Under **Node Groups**, you can configure multiple node groups based on the deployment use case.
 - o **Inline Node Group:** This node group is used for the Inline V Series Node that is used for traffic acquisition.
 - a. In the **Inline Node Group Name** field, enter a name for the node group.
 - b. From the **Inline Auto Scaling Group** drop-down list, select the auto scaling group where you deploy the Inline V Series Node.
 - o **(Optional) Node Group:** You can configure this section if you wish to process the traffic using GigaVUE V Series Node. You can add or delete node groups using the + and - buttons.
 - a. In the **Node Group Name** field, enter a name for the node group.
 - b. From the **Auto Scaling Group** drop-down list, select the VMSS created in Azure.
5. Select **Save**.

NOTE: You can configure a maximum of eight Node groups.

(Optional) Create a Virtual Machine Scale Set for Out-of-Band GigaVUE V Series Node (Tier 2)

The Tier 2 V Series Node (Out-of-Band) processes mirrored traffic using GigaSMART operations to enrich and optimize data before forwarding it to the tool set. If only filtering is required, the Tier 1 V Series Node can handle it and send the traffic directly to the tool—eliminating the need for a Tier 2 node.

The following table lists the specific options you must select when creating a Virtual Machine Scale Set for Out-of-Band for an inline V Series deployment. For navigation steps and detailed instructions, refer to [Create a Virtual Machine Scale Set](#) topic in Azure documentation.

Parameters	Description	Mandatory field
Availability Zones	Choose if you want to use zones for high availability.	No
Orchestration		
Orchestration Mode	Select Uniform as the orchestration mode.	Yes
Security Type	Select Standard mode.	Yes
Scaling		
Scaling Mode	Choose Autoscaling .	Yes

Parameters	Description	Mandatory field
Scaling Configuration	Click Configure to edit the scaling conditions.	Yes
Default Condition	Enter the Initial Instance Count as 0. NOTE: Once the Monitoring Domain and connection is configured, edit this value to the number of GigaVUE V Series Node that you need to deploy in this Monitoring Domain.	Yes
Condition	Choose a metric-based scaling condition (For example, CPU usage, network traffic).	Yes
Metric Source	Select the metric (For example, Average CPU Percentage).	Yes
Scale out	Set conditions like greater than 70% for scaling up.	Yes
Scale in	Set conditions like less than 20%.	
Cooldown Period	Set a cooldown period to prevent rapid scaling.	Yes
Instance Details		
Instance Type	Choose Standard_D4S_v4 as the VM size.	Yes
Image	Select the GigaVUE V Series Node image.	Yes
Authentication Type	Choose SSH public key.	Yes
Username	Enter a user name. Do not use admin or gigamon.	Yes
Networking		
Virtual Network	Select the required VNet.	Yes
Subnet Selection	Choose the appropriate subnet for V Series Node.	Yes
NIC Configuration	GigaVUE V Series Node requires two NICs—one for management and one for mirrored data traffic. To configure the Data NIC, add a second network interface, select the appropriate subnet and network security group (NSG), and enable Accelerated Networking.	Yes
Management		

Parameters	Description	Mandatory field
Upgrade Mode	Choose Automatic .	
Advanced		
Custom data and cloud init	Enter the Custom data as text in the following format and deploy the instance. The GigaVUE V Series Nodes uses this user data to generate config files (/etc/gigamon-cloud.conf) and register with GigaVUE-FM using Third Party Orchestration. NOTE: Ensure you maintain the exact indentation and order shown in the code snippet when copying and pasting it. Any changes in formatting or order may cause errors or prevent the code from working correctly. We recommend copying the indentation from the online documentation for complete accuracy. <pre>#cloud-config write_files: - path: /etc/gigamon-cloud.conf owner: root:root permissions: '0644' content: Registration: groupName: <Monitoring Domain Name> subGroupName: <Connection Name> remoteIP: <IP address of the GigaVUE-FM> remotePort: 443 token: <token></pre>	Yes

Configure Monitoring session

When the **Traffic Acquisition Method** is **Inline**, the **UCT-I** application is available on the canvas by default. You can configure up to three tiers in a Monitoring Session and define multiple Sub Policies. Each Sub Policy can have its own ingress and egress tunnels and traffic processing applications.



Notes:

- You can configure a maximum of three tiers in a Monitoring Session.
- Tier 1 supports only Maps. Inline traffic is disabled and reserved for future use.
- You can configure a maximum of 8 Sub Policies in a Monitoring Session.
- Each Sub Policy can have its own Ingress Tunnels, Egress Tunnels, and Applications.
- Traffic from an out-of-band endpoint can either:
 - Pass through a Map and send to a tool using an Egress Tunnel.



- (Optional) Send to the GigaVUE V Series Node of the next tier for further processing.

To configure the Monitoring Session for Inline V Series Solution:

Tier 1 Monitoring Session:

1. Perform one of the following options:
 - Create a new Monitoring Session. Refer to [Create a Monitoring Session \(Azure\)](#) for details.
 - On an existing Monitoring Session, navigate to the **TRAFFIC PROCESSING** tab.

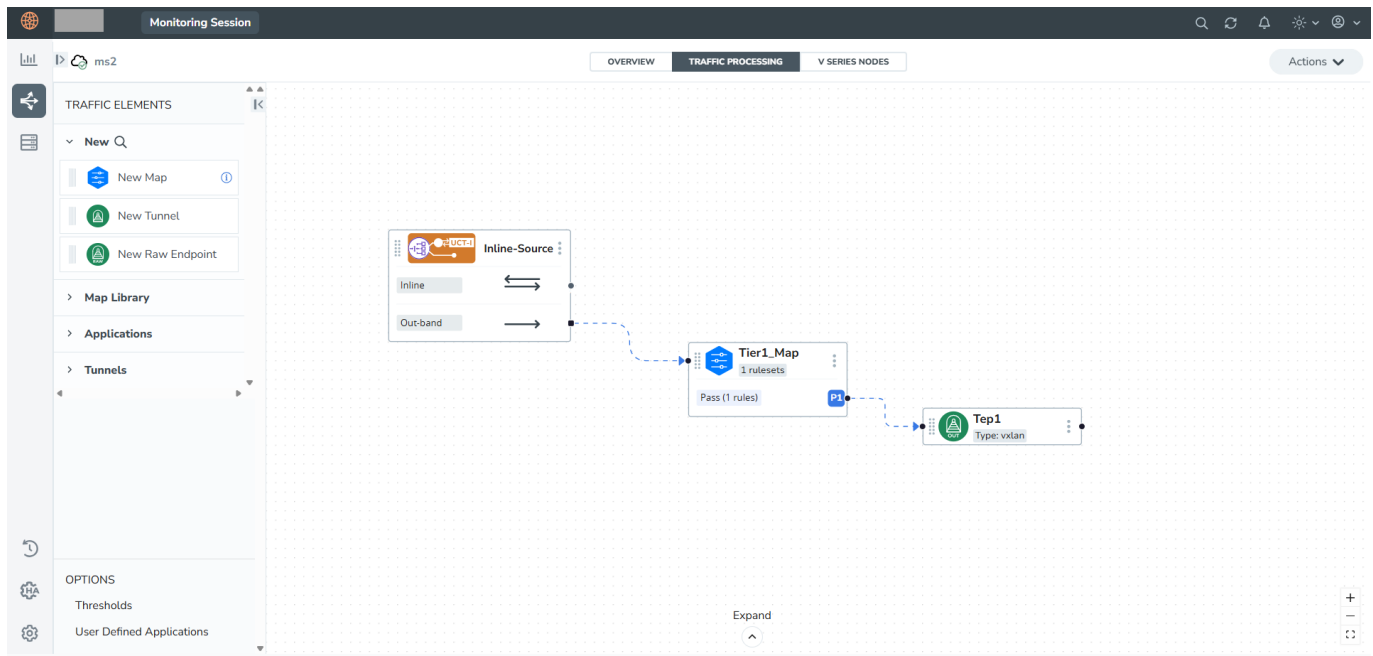
The GigaVUE-FM Monitoring Session canvas page appears.

When the **Traffic Acquisition Method** is **Inline**, the **UCT-I** application is available on the canvas by default.

2. Drag and drop the following items to the canvas as required for Tier 1 or Sub Policy 1:
 - Maps from the **new map** section. Refer to [Create a New Map \(Azure\)](#) for details.
 - Egress tunnels from the **new tunnel** section. When configuring Egress Tunnel, configure the **Remote Tunnel IP** if you intend to send the traffic directly from Tier 1 to the tool. Refer to [Create Ingress and Egress Tunnels \(Azure\)](#) for details.

NOTE: If sending traffic to Tier 2, Remote IP is optional. GigaVUE-FM will automatically add the remote IPs internally.

3. Now create a connection between the three tiles by dragging a line from the Inline-Source tile labeled “Out-Band” to the newly created Map and from Map to Egress tunnel.



Deploy Monitoring Session (Tier 1)

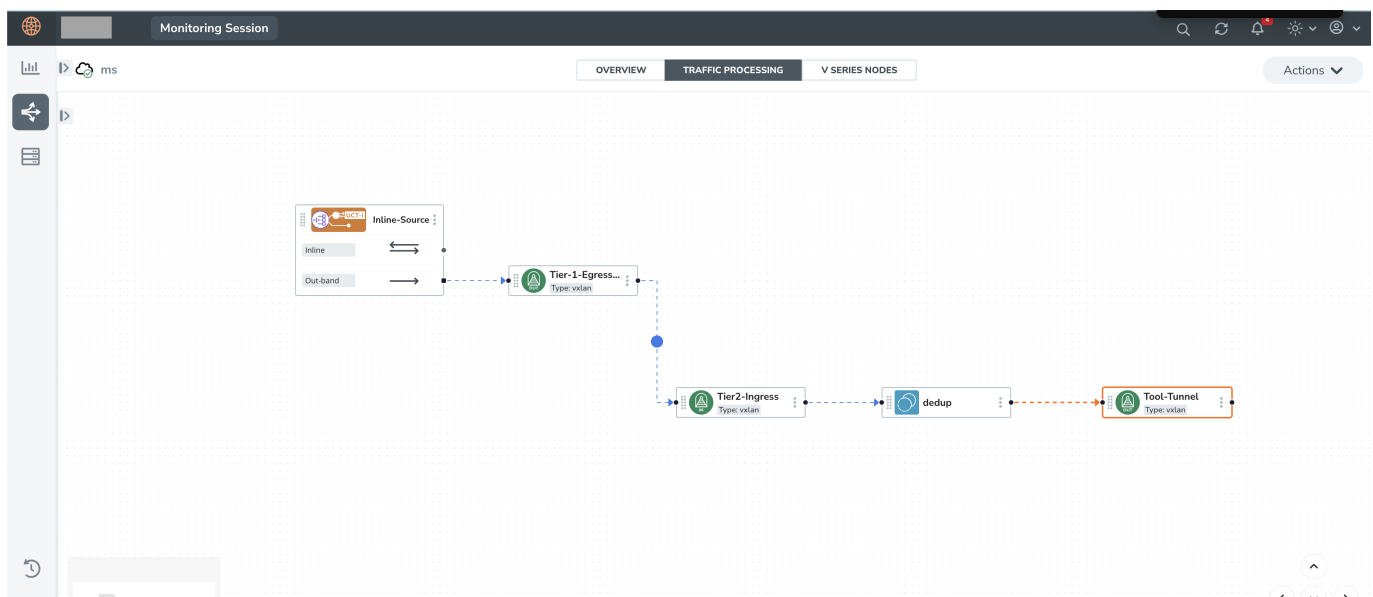
1. From the Actions drop-down list, select **Deploy**. The Deploy Monitoring Session pop-up appears.
2. Enter the following details:
 - In the **Policy Name** field, verify the auto-generated policy name or enter a custom name.
 - From the **Node Group** drop-down list, select the appropriate node group associated with this policy.
 - Under **Interface Mapping**, configure the interfaces:
 - i. From the **Ingress - <Tunnel>** drop-down list, select the input interface.
 - ii. From the **Egress - <Tunnel>** drop-down list, select the output interface.
3. Select **Deploy** the Monitoring Session.

To view the GigaVUE V Series Node associated with each Sub Policy, navigate to the **V SERIES NODES** tab and select a policy from the **Select a Sub policy** drop-down menu.

Tier 2 Monitoring Session (Optional):

You can send the filtered traffic to a Tier 2 V Series node, where GigaVUE-FM enriches and optimizes the data further.

1. In the same Monitoring Session canvas, drag and drop the following items to the canvas as required for Tier 2 or Sub Policy 2:
 - Ingress tunnel (as a source) from the **New** section. Refer to [Create Ingress and Egress Tunnels \(Azure\)](#) for details.
 - Maps from the **New Map** section. Refer to [Create a New Map \(Azure\)](#) for details.
 - GigaSMART apps from the Applications section. Refer to [Add Applications to Monitoring Session \(Azure\)](#).
 - Egress tunnels from the **new tunnel** section. Enter the **Remote Tunnel IP** address.
2. Create a link from the Ingress Tunnel to the Map or Application, and then connect it to the Egress Tunnel.
3. Create a direct link between the Egress Tunnel of Tier 1 and the Ingress Tunnel of Tier 2. The Blue Dot serves as an identifier to differentiate between tiers.
4. Repeat the above steps to configure a third tier, if required.



Deploy Monitoring Session Tier 1 to Tier 2

1. From the Actions drop-down list, select **Deploy**.

The Deploy Monitoring Session pop-up appears.

2. For each Policy (Tier) configured in the Monitoring Session, enter the following details:
 - In the **Policy Name** field, verify the auto-generated policy name or enter a custom name.
 - From the **Node Group** drop-down list, select the appropriate node group associated with this policy.
 - Under **Interface Mapping**, configure the interfaces:
 - i. From the **Ingress - <Tunnel>** drop-down list, select the input interface.
 - ii. From the **Egress - <Tunnel>** drop-down list, select the output interface.
3. Select **Deploy** the Monitoring Session.

To view the GigaVUE V Series Node associated with each Sub Policy, navigate to the **V SERIES NODES** tab and select a policy from the **Select a Sub policy** drop-down menu.

What to do Next:

To view Monitoring Session Statistics and Dashboards for Inline V Series Solution, refer to:

- [View Monitoring Session Statistics \(Azure\)](#)
- [Analytics for Inline V Series Solution \(Azure\)](#)

Configure

Delete this text and replace it with your own content.

Configure Monitoring Session

This chapter describes how to setup ingress and egress tunnels, maps, and applications in a Monitoring Session to receive and send traffic to the GigaVUE Cloud Suite V Series node. It also describes how to filter, manipulate, and send the traffic from the V Series node to monitoring tools.

Refer to the following sections for details:

- [Create a Monitoring Session \(Azure\)](#)
- [Configure Monitoring Session for Inline V Series](#)

- [Create Ingress and Egress Tunnels \(Azure\)](#)
- [Create Raw Endpoint \(Azure\)](#)
- [Create a New Map \(Azure\)](#)
- [Add Applications to Monitoring Session \(Azure\)](#)
- [Interface Mapping \(Azure\)](#)
- [Deploy Monitoring Session \(Azure\)](#)
- [View Monitoring Session Statistics \(Azure\)](#)
- [Visualize the Network Topology \(Azure\)](#)

Create a Monitoring Session (Azure)

You must create a Monitoring Domain before creating a Monitoring Session. Refer to [Create Monitoring Domain](#).

GigaVUE-FM automatically collects inventory data on all target instances in your cloud environment. You can design your Monitoring Session to:

- Include or exclude the instances that you want to monitor.
- Monitor egress, ingress, or all traffic.

Target Instance

- When a new target instance is added to your cloud environment, GigaVUE-FM automatically detects and adds it to your Monitoring Session based on your selection criteria. Similarly, when an instance is removed, it updates the Monitoring Sessions.

You can create multiple Monitoring Sessions within one Monitoring Domain.

To create a new Monitoring Session:

1. Go to **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. The **Monitoring Session** page appears.
2. Select **New Monitoring Session** to open the New Monitoring Session configuration page.

3. In the configuration page, perform the following:

- In the **Alias** field, enter the name of the Monitoring Session.
- From the **Monitoring Domain** drop-down list, select the desired Monitoring Domain or select **Create New** to create a Monitoring Domain.
For details, refer to the Create a Monitoring Domain section in the respective cloud guides.
- From the **Connections** drop-down list, select the required connections to include as part of the Monitoring Domain.
- From the **VPC** drop-down list, select the required VPCs to include as part of the Monitoring Domain.
- Enable the **Distributed Deduplication** option to identify duplicate packets across different GigaVUE V Series Nodes when traffic from various targets is routed to these instances for monitoring. Distributed Deduplication is only supported on GigaVUE V Series Node version 6.5.00 and later.

4. Select **Save**.

The Monitoring Session Overview page appears.

Monitoring Session Page (Azure)

The following table outlines the functional tabs available on the Azure Monitoring Session page, each designed to support specific aspects of network monitoring and session management:

Tab	Description
Overview	You can view the high level information of the selected Monitoring Session such as, connections, tunnel details, health status, deployment status, and information related to Application Intelligence statistics. You can also view the statistics of the incoming and outgoing traffic on an hourly, daily, weekly, and monthly basis. You can filter the statistics based on the elements associated with the Monitoring Session. For more information, refer to View Monitoring Session Statistics (Azure) .
Sources	Displays the sources and target details monitored by the Monitoring Session. You can view and filter the connection details of the Monitoring Session. You can view the deployment status, number of targets, and targets source health. In the Selection Status section, you can view the VM status. The status indicates whether the VM is supported, not supported, selected, or not selected. When you hover over the status, a tooltip displays the reason for that status. NOTE: In the case of OVS Mirroring, the Sources tab also displays the Hypervisor details along with the Instances.
Traffic Acquisition	You can enable or disable Prefiltering, Precryption, and Secure Tunnel here. You can also create a Prefiltering and Precryption templates and apply them to the Monitoring Session. Refer to Enable Prefiltering. Note: Traffic Acquisition is only applicable for Monitoring Domain created with UCT-V as

Tab	Description
	Acquisition method.
Traffic Processing	You can view, add, and configure applications, tunnel endpoints, raw endpoints, and maps. You can view the statistical data for individual applications and also apply threshold templates, enable user defined applications, and enable or disable distributed De-duplication. Refer to Enable Prefiltering .
V Series Nodes	You can view the V Series nodes associated with the Monitoring Session. In the split view, you can view details such as Node name, Health status (Configuration health + Traffic health), Host VPC, Management IP and Deployment Failure Message (if applicable). You can also change the interfaces mapped to an individual GigaVUE V Series Node. Refer to Interface Mapping (Azure) .
Topology	Displays the fabric and monitored instances based on the connections configured in your network. You can select a specific connection to explore its associated subnets and instances in the topology view, offering a clear visualization of the monitored network elements. Refer to Visualize the Network Topology (Azure) .

NOTE: Ensure that the GigaVUE V Series Node and GigaVUE-FM are time synchronized or configure NTP time synchronization.

The Monitoring Session page **Actions** button has the following options. The Actions menu is placed common in all the tabs explained above.

Button	Description
Delete	Deletes the selected Monitoring Session.
Clone	Duplicates the selected Monitoring Session.
Deploy	Deploys the selected Monitoring Session.
Undeploy	Undeploys the selected Monitoring Session.

You can use the  icon on the left side of the Monitoring Session page to view the Monitoring Sessions list. Click  to filter the Monitoring Sessions list. In the side bar, you can:

- Create a new Monitoring Session
- Rename a Monitoring Session
- Hover over, click the check box of the required Monitoring Session(s) and perform bulk actions (Delete, Deploy, or Undeploy).

Configure Monitoring Session Options (Azure)

In the Monitoring Session page, you can perform the following actions in the **TRAFFIC ACQUISITION** and **TRAFFIC PROCESSING** tabs:

- Enable Prefiltering
- Enable Precryption
- Apply Threshold Template
- Enable User-defined applications
- Enable Distributed De-duplication

TRAFFIC ACQUISITION

To navigate to **TRAFFIC ACQUISITION** tab,

1. Go to **Traffic > Virtual > Orchestrated Flows > Select your cloud platform**.
2. Select the required Monitoring Session from the list view on the left pane and select the **TRAFFIC ACQUISITION** tab.

You can perform the following actions in the **TRAFFIC ACQUISITION** page:

- [Enable Prefiltering](#)
- [Enable Precryption](#)

Enable Prefiltering

To enable Prefiltering:

1. In the **TRAFFIC ACQUISITION** page, go to **Mirroring > Edit Mirroring**.
2. Enable the **Mirroring** toggle button.
3. Enable **Secure Tunnel** option if you wish to use Secure Tunnels. Refer to the *Configure Secure Tunnel* section in the respective GigaVUE Cloud Suite Deployment Guide.
4. Select an existing Prefiltering template from the **Template** drop-down menu, or create a new template using **Add Rule** option and apply it. For details, refer to .
5. Select the **Save as Template** to save the newly created template.
6. Select **Save** to apply the template to the Monitoring Session.

Enable Precryption

Consideration before you enable Precryption:

- To avoid packet fragmentation, change the option `precryption-path-mtu` in UCT-V configuration file (**/etc/uctv/uctv.conf**) within the range 1400-9000 based on the platform path MTU.
- Protocol version IPv4 and IPv6 are supported.
- If you wish to use IPv6 tunnels, ensure that the versions of GigaVUE-FM and the fabric components are 6.6.00 or above.

NOTE: We recommend to enable the secure tunnel feature whenever the Precryption feature is enabled. Secure tunnel helps to securely transfer the cloud captured packets or Precryption data to a GigaVUE V Series Node. For more information, refer to *Secure Tunnels* in the respective GigaVUE Cloud Suite Deployment Guide.

To enable Precryption:

1. In the **TRAFFIC ACQUISITION** page, select **Precryption** tab and click **Edit Precryption**.
2. Enable the **Precryption** toggle button. Refer to Precryption™ topic in the respective cloud guides for details.

3. Apply Precryption to a few selective components based on the traffic:

NOTE: If you wish to use Selective Precryption, ensure that the versions of GigaVUE-FM and the fabric components are 6.8.00 or above.

Applications:

- a. Select the **APPLICATIONS** tab.
The **Pass All Applications** is enabled by default. If you wish to use selective Precryption, disable this option.
- b. Select any one of the following options from **Actions**:
 - i. Include: Select to include the traffic from the selected applications for Precryption.
 - ii. Exclude: Select to exclude the traffic from the selected applications for Precryption.
- c. Select **Add**. The **Add Application** widget opens.
- d. Select **csv** as the **Type**, if you wish to add the applications using a .csv file.
- e. Select **Choose File** and upload the file.
- f. Select **Manual** as the **Type**, if you wish to add the applications manually.
- g. Enter the **Application Name** and select + icon to add more applications.
- h. Select **Save**.

L3-L4

You can select an existing Precryption template from the **Template** drop-down list, or you can create a new template and apply it. For details, refer to [Create Precryption Template for UCT-V](#).

4. Enable the **Secure Tunnel** option if you wish to use Secure Tunnels. Refer to the *Configure Secure Tunnel* section in the respective GigaVUE Cloud Suite Deployment Guide.

Validate Precryption connection

To validate the Precryption connection, follow the steps:

- To confirm it is active, navigate to the Monitoring Session **Overview** tab and check the Traffic Acquisition Options.
- Select **Precryption**, to view the rules configured.

Limitations

During Precryption, UCT-V generates a TCP message with the payload being captured in clear text. Capturing the L3/L4 details of this TCP packet by probing the SSL connect/accept APIs. The default gateway's MAC address is the destination MAC address for the TCP packet

when SSL data is received on a specific interface. If the gateway is incorrectly configured, the destination MAC address is all Zeros.

TRAFFIC PROCESSING

To navigate to **TRAFFIC PROCESSING** tab:

1. Go to **Traffic > Virtual > Orchestrated Flows > Select your cloud platform**.
2. Select the required Monitoring Session from the list view on the left side of the screen and click **TRAFFIC PROCESSING** tab.

You can perform the following actions in the **TRAFFIC PROCESSING** page:

- [Apply Threshold Template](#)
- [Enable User Defined Applications](#)
- [Enable Distributed De-duplication](#)
- [Tool Exclusion](#)

Apply Threshold Template

To apply threshold:

1. In the **TRAFFIC PROCESSING** page, select **Thresholds** under **Options** menu.
2. You can select an existing threshold template from the **Select Template** drop-down list, or you can create a new template using **New Threshold Template** option and apply it.
For more details on Threshold Template, refer to the [Traffic Health Monitoring](#) section.
3. Select **Save** to save the newly created template.
4. Select **Apply** to apply the template to the Monitoring Session.

NOTE: You can apply the Threshold configuration to a Monitoring Session before it is deployed. Furthermore, undeploying the Monitoring Session does not remove the applied Thresholds.

You can also view the related details of the applied thresholds, such as Traffic Element, Metric, Type, Trigger Values, and Time Interval in the **Threshold** window. Select **Clear Thresholds** to clear the applied thresholds across the selected Monitoring Session.

Enable User Defined Applications

To enable user defined application:

1. In the **TRAFFIC PROCESSING** page, click **User Defined Applications** under **Options** menu.
2. Enable the **User-defined Applications** toggle button.
3. Add from the existing applications or create new User-Defined Application from the **Actions** drop-down. Refer to [Supported Protocols and Attributes](#).

Enable Distributed De-duplication

In the TRAFFIC PROCESSING page, click **Distributed De-duplication** under **Options** menu. Enabling the Distributed De-duplication option identifies duplicate packets across different GigaVUE V Series Nodes when traffic from various targets is routed to these instances for monitoring. Refer to [Distributed De-duplication](#).



Notes:

- Distributed De-duplication is only supported on V Series version 6.5.00 and later.
- From version 6.9.00, Traffic Distribution option is renamed to Distributed De-duplication.

Tool Exclusion

Tool Exclusion helps prevent traffic loops by ensuring monitoring tools are not mistakenly selected as traffic targets during Automatic Target Selection (ATS). This feature is available only when the traffic acquisition method is VPC Traffic Mirroring.

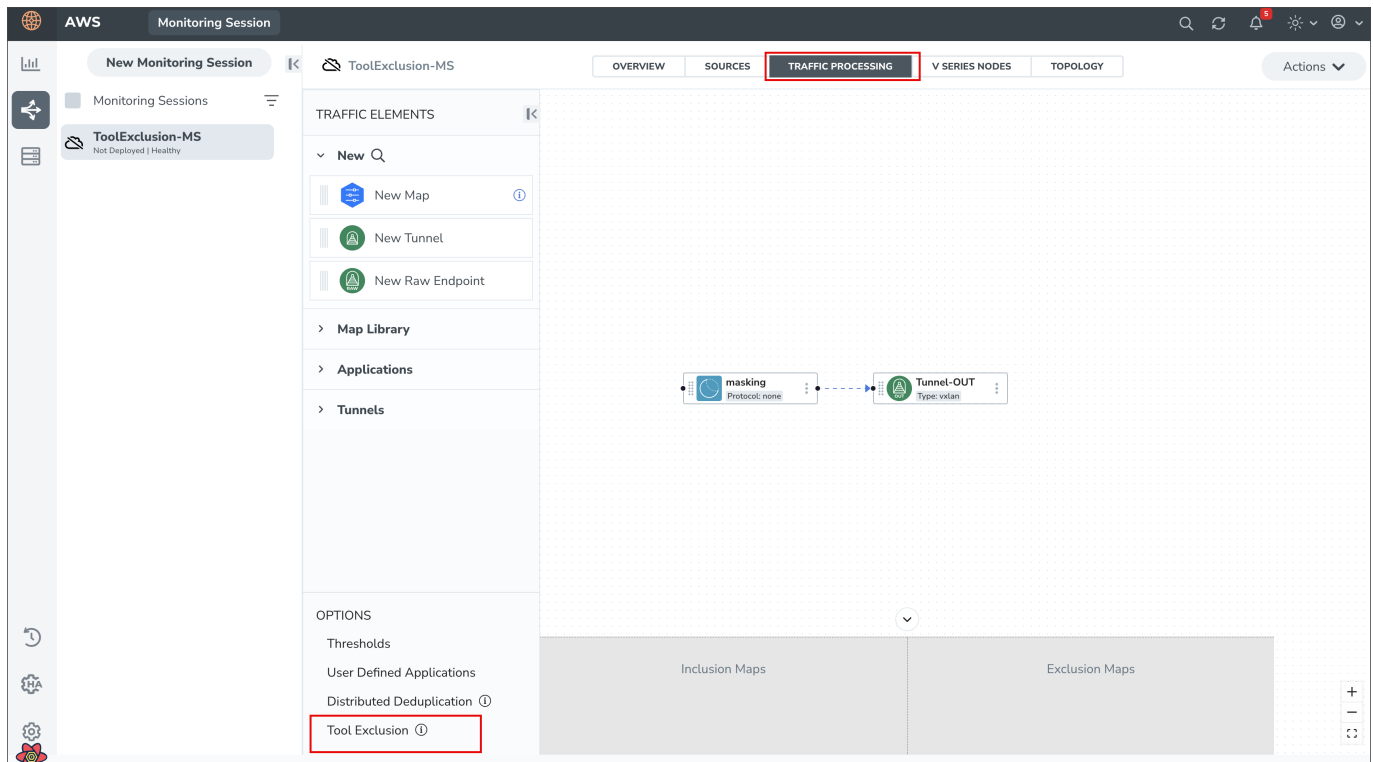
You can exclude tool instances using either of the following methods:

1. Using AWS Tag Key

During deployment, apply the AWS tag key **GigamonExclude:Value** (Any Value) to any instance that acts as a monitoring tool. This tag ensures the system automatically excludes these instances from ATS.

2. Using the Tool Exclusion Feature in UI

During deployment, if the same instance IP is configured as both source (ingress) and tool (egress), the system prompts you to manually identify and exclude tools. Also, you can use the **Tool Exclusion** option to include or exclude tools and targets manually.



Create Ingress and Egress Tunnels (Azure)

Traffic from the GigaVUE V Series Node is distributed to tunnel endpoints in a Monitoring Session. A tunnel endpoint can be created using a standard L2GRE, VXLAN, UDPGRE, UDP, or ERSPAN tunnel.

Create a new tunnel endpoint

To create,

1. Perform one of the following and navigate to the **TRAFFIC PROCESSING** tab:
 - Create a new monitoring session
 - Select **Actions > Edit** on an existing monitoring session.

The GigaVUE-FM Monitoring Session canvas page appears.

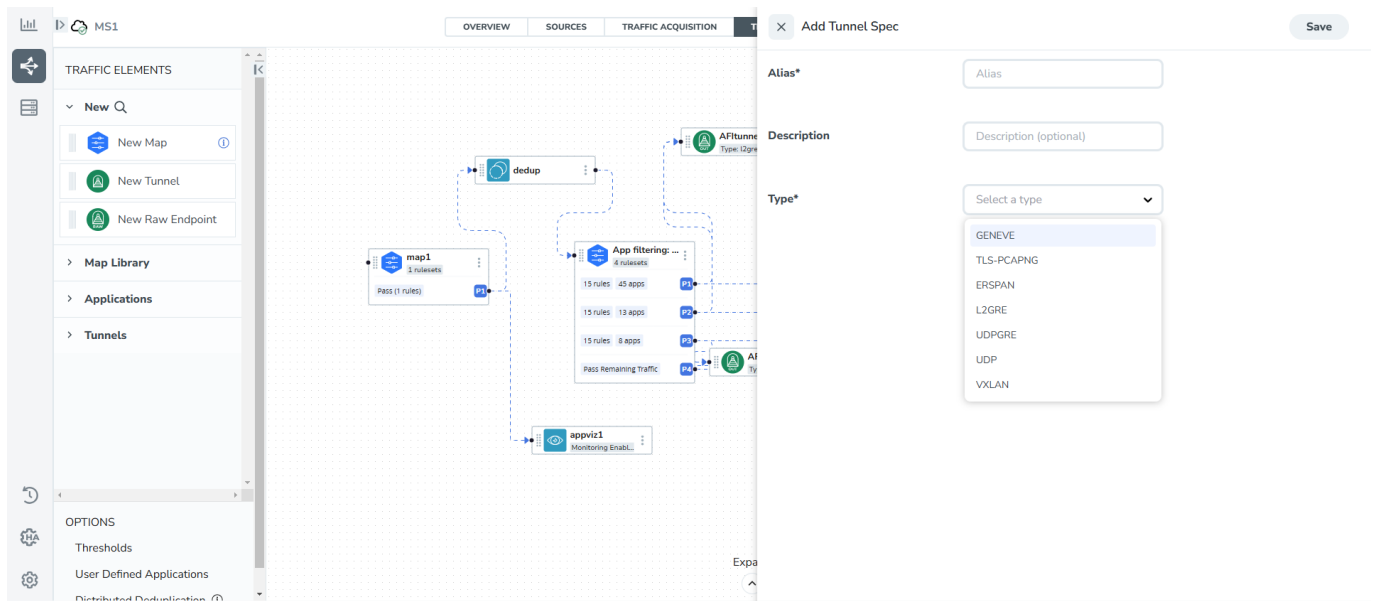
2. On the left pane of the canvas, select the  icon to view the traffic processing elements.
3. Select **New > New Tunnel**, drag and drop a new tunnel template to the workspace.

The **Add Tunnel Spec** quick view appears.

4. Enter the **Alias**, **Description**, and **Type** details.

For details, refer to [Details - Add Tunnel Specifications](#) table.

5. Select **Save**.



To delete a tunnel, select the menu button of the required tunnel and select **Delete**.

Apply a threshold template to Tunnel End Points

1. Select the menu button of the required tunnel endpoint on the canvas and click **Details**.
2. In the quick view, go to the **Threshold** tab.

For details on creating or applying a threshold template, refer to the Monitor Cloud Health topic in the respective Cloud guides.

You can use the configured Tunnel End Points to send or receive traffic from GigaVUE HC Series and GigaVUE TA Series. Provide the IP address of the GigaVUE HC Series and GigaVUE TA Series as the Source or the Destination IP address as required when configuring Tunnel End Points.

After configuring the tunnels and deploying the Monitoring Session, you can view the number of ingress and egress tunnels configured for a Monitoring Session. Select the numbers of tunnels displayed in the **OVERVIEW** tab to view the tunnel names and their respective **ADMIN STATUS** and **HEALTH STATUS**.

Table 1: Details - Add Tunnel Specifications

Field	Description	
Alias	The name of the tunnel endpoint.	
Description	The description of the tunnel endpoint.	
Admin State Note: This option appears only after the Monitoring session deployment.	Use this option to send or stop the traffic from GigaVUE-FM to the egress tunnel endpoint. Admin State is enabled by default. You can use this option to stop sending traffic to unreachable or down tools. Each egress tunnel configured on the GigaVUE V SeriesNode has an administrative state that enables GigaVUE-FM to halt the tunnel's traffic flow. GigaVUE-FM only disable the tunnels when it receives a notification via REST API indicating that a tool or group of tools is down. Note: This option is not supported for TLS-PCAPNG tunnels.	
Type	The type of the tunnel. Select from the options below to create a tunnel. ERSPAN, L2GRE, VXLAN, TLS-PCAPNG, UDP, or UDPGRE.	
VXLAN		
Traffic Direction		
The direction of the traffic flowing through the GigaVUE V Series Node.		
Note: In the scenario where secure tunnels need to be established between a GigaVUE V Series Node and a GigaVUE HC Series, you can utilize the Configure Physical Tunnel option provided in the GigaVUE V Series Secure Tunnel page. This allows you to configure secure tunnels on your physical device conveniently. For details, refer to Secure Tunnels .		
In	Choose In (Decapsulation) for creating an ingress tunnel to carry traffic from the source to the GigaVUE V Series Node.	
	IP Version	The version of the Internet Protocol. Select IPv4 or IPv6.
	Remote Tunnel IP/FQDN	For egress tunnels, specify the destination endpoint by using an IPv4 address, IPv6 address, or fully qualified domain name (FQDN). FQDN support applies only to VXLAN and L2GRE egress tunnels. By using an FQDN, you can keep the same tunnel configuration even when the destination IP address changes. If the FQDN resolves to both IPv4 and IPv6 addresses, the system selects the address based on the preferred IP stack configured for the monitoring domain.
	VXLAN Network Identifier	Unique value that is used to identify the VXLAN. The value ranges from 1 to 16777215.
	Source L4 Port	The port used to establish the connection to the target. For example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	The port used to establish the connection will be established from the source. For example, if A is the source and B is the destination, this port value belongs to B.
Out	Choose Out (Encapsulation) for creating an egress tunnel from the GigaVUE V Series Node	

Field	Description
	to the destination endpoint.

Field	Description	
	Remote Tunnel IP	For egress tunnel, the Remote Tunnel IP is the IP address of the tunnel destination endpoint.
	MTU	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry. The default value is 1500.
	Time to Live	Enter the value of the time interval for which the session needs to be available. The value ranges from 1 to 255. The default value is 64.
	DSCP	Differentiated Services Code Point (DSCP) is a value that network devices use to identify traffic to be handled with higher or lower priority. The values ranges from 0 to 63 with 0 being the highest priority and 63 being the lowest priority.
	Flow Label	Unique value, which is used to identify packets that belong to the same flow. A flow is a sequence of packets that need to be treated as a single entity that may require special handling. The accepted value is between 0 and 1048575.
	VXLAN Network Identifier	Unique value which is used to identify the VXLAN. The value ranges from 1 to 16777215.
	Multi Tunnel	Enable the multi-tunnel flag to create multiple tunnels for flow distribution to the 5G-Cloud application. Refer to 5G-Cloud Ericson SCP Support. Applicable Platforms: OpenStack, Third Party Orchestration, VMware ESXi  Notes: - You can configure either a single-tap or multi-tap setup for the egress tunnel. Switching between these configurations is not allowed; to make changes, you must undeploy and redeploy the Monitoring Session. - When you enable Multi-Tunnel on a VXLAN tunnel and set the number of tunnels, GigaVUE-FM automatically creates the additional VXLAN tunnel endpoints. Any later changes to the original VXLAN tunnel, such as disabling Multi-Tunnel or modifying Domain Tagging do not update these auto created endpoints. They continue to retain the configuration that existed at the time they were created. To apply updated settings, you must delete the VXLAN TEP and the associated LB application, then recreate the LB and VXLAN TEP with the new configuration, and re-establish the link between them.
	Source L4 Port	The port from which the connection is established to the target.

Field	Description	
		For example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	The port to which the connection is established from the source. For example, if A is the source and B is the destination, this port value belongs to B.
	Domain Tagging	Enable this option to tag packets on the egress tunnel with the Ericsson domain-specific VLAN IDs derived from the PCAPng Domain VLAN Mapping. NOTE: This setting is available only when Domain Classification is enabled in the associated PCAPng application. Refer to PCAPng Application for details.
UDPGRE		
Traffic Direction The direction of the traffic flowing through the GigaVUE V Series Node.		
In	Choose In (Decapsulation) for creating an ingress tunnel to carry traffic from the source to the GigaVUE V Series Node.	
	IP Version	The version of the Internet Protocol. Select IPv4 or IPv6.
	Remote Tunnel IP	For ingress tunnel, the Remote Tunnel IP is the IP address of the tunnel source.
	Key	Identifier used to differentiate different UDPGRE/L2GRE tunnels. It routes the encapsulated frames to the appropriate tunnel on the remote endpoint. Enter a value between 0 and 4294967295.
	Source L4 Port	The port from which the connection is established to the target. For example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	The port to which the connection is established from the source. For example, if A is the source and B is the destination, this port value belongs to B.
L2GRE		
Traffic Direction The direction of the traffic flowing through the GigaVUE V Series Node. Note: In the scenario where secure tunnels need to be established between a GigaVUE V Series and a GigaVUE HC Series, you can utilize the Configure Physical Tunnel option provided in the GigaVUE V Series Secure Tunnel page. This allows you to conveniently configure secure tunnels on your physical device . For details, refer to the Secure Tunnels .		
In	Choose In (decapsulation) to create an ingress tunnel, which will carry traffic from the source to the GigaVUE V Series Node.	

Field	Description	
	IP Version	The version of the Internet Protocol. Select IPv4 or IPv6.
	Remote Tunnel IP	For ingress tunnel, the Remote Tunnel IP is the IP address of the tunnel source.
	Key	Identifier used to differentiate different UPDGRE/L2GRE tunnels. It is used to route the encapsulated frames to the appropriate tunnel on the remote endpoint. Enter a value between 0 and 4294967295.
Out	Choose Out (Encapsulation) for creating an egress tunnel from the V Series Node to the destination endpoint.	
	Remote Tunnel IP/FQDN	For egress tunnels, specify the destination endpoint by using an IPv4 address, IPv6 address, or fully qualified domain name (FQDN). FQDN support applies only to VXLAN and L2GRE egress tunnels. By using an FQDN, you can keep the same tunnel configuration even when the destination IP address changes. If the FQDN resolves to both IPv4 and IPv6 addresses, the system selects the address based on the preferred IP stack configured for the monitoring domain.
	MTU	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry. The default value is 1500.
	Time to Live	Enter the value of the time interval for which the session needs to be available. The value ranges from 1 to 255. The default value is 64.
	DSCP	Differentiated Services Code Point (DSCP) is a value that network devices use to identify traffic to be handled with higher or lower priority. The values ranges from 0 to 63 with 0 being the highest priority and 63 being the lowest priority.
	Flow Label	Unique value, which is used to identify packets that belong to the same flow. A flow is a sequence of packets that need to be treated as a single entity that may require special handling. The accepted value is between 0 and 1048575.
	Key	Identifier used to differentiate different UPDGRE/L2GRE tunnels. It is used to route the encapsulated frames to the appropriate tunnel on the remote endpoint. Enter a value between 0 and 4294967295.
	Domain Tagging	Enable this option to tag packets on the egress tunnel with the Ericsson domain-specific VLAN IDs derived from the PCAPng Domain VLAN Mapping. NOTE: This setting is available only when Domain Classification is enabled in the associated PCAPng application. Refer to PCAPng Application for details.

Field		Description
ERSPAN		
Traffic Direction The direction of the traffic flowing through the GigaVUE V Series Node.		
In	IP Version	The version of the Internet Protocol. Select IPv4 or IPv6.
	Remote Tunnel IP	For ingress tunnel, the Remote Tunnel IP is the IP address of the tunnel source.
	Flow ID	The ERSPAN flow ID is a numerical identifier that distinguishes different ERSPAN sessions or flows. The value ranges from 1 to 1023.
TLS-PCAPNG		
Traffic Direction The direction of the traffic flowing through the GigaVUE V Series Node. Note: In the scenario where secure tunnels need to be established between a GigaVUE V Series and a GigaVUE HC Series, you can utilize the Configure Physical Tunnel option provided in the GigaVUE V Series Secure Tunnel page. This allows you to conveniently configure secure tunnels on your physical device . For details, refer to Secure Tunnels section.		

Field	Description	
In	IP Version	The version of the Internet Protocol. Only IPv4 is supported.
	Remote Tunnel IP	For ingress tunnel, the Remote Tunnel IP is the IP address of the tunnel source.
	MTU	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry. The default value is 1500.
	Source L4 Port	The port from which the connection is established to the target. For example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	The port to which the connection is established from the source. For example, if A is the source and B is the destination, this port value belongs to B.
	Key Alias	Select the Key Alias from the drop-down.
	Cipher	Only SHA 256 is supported.
	TLS Version	Only TLS Version 1.3.
	Selective Acknowledgments	Enable to receive the acknowledgments.
	Sync Retries	Enter the number of times the sync has to be tried. The value ranges from 1 to 6.
	Delay Acknowledgments	Enable to receive the acknowledgments for a delay.

Field	Description	
Out	IP Version	The version of the Internet Protocol. Only IPv4 is supported.
	Remote Tunnel IP	For ingress tunnel, the Remote Tunnel IP is the IP address of the tunnel source.
	MTU	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry. The default value is 1500.
	Time to Live	Enter the value of the time interval for which the session needs to be available. The value ranges from 1 to 255. The default value is 64.
	DSCP	Differentiated Services Code Point (DSCP) is a value that helps network devices identify the higher or lower priority to handle traffic. The values ranges from 0 to 63 with 0 being the highest priority and 63 being the lowest priority.
	Flow Label	Unique value which is used to identify packets that belong to the same flow. A flow is a sequence of packets that need to be treated as a single entity that may require special handling. The accepted value is between 0 and 1048575.
	Source L4 Port	The port from which the connection is established to the target. For example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	The port to which the connection is established from the source. For example, if A is the source and B is the destination, this port value belongs to B.
	Cipher	Only SHA 256 is supported.
	TLS Version	Only TLS Version 1.3.
	Selective Acknowledgments	Enable the receipt of acknowledgments.
	Sync Retries	Enter the number of times you can try the sync. The value ranges from 1 to 6.
	Delay Acknowledgments	Enable the receipt of acknowledgments when there is a delay.
UDP:		

Field	Description	
Out	L4 Destination IP Address	Enter the IP address of the tool port or when using Application Metadata Exporter (AMX), enter the IP address of the AMX application. For details, refer to Application Metadata Exporter .
	Source L4 Port	The port from which the connection is established to the target. For example, if A is the source and B is the destination, this port value belongs to A.
	Destination L4 Port	The port to which the connection is established from the source. For example, if A is the source and B is the destination, this port value belongs to B.

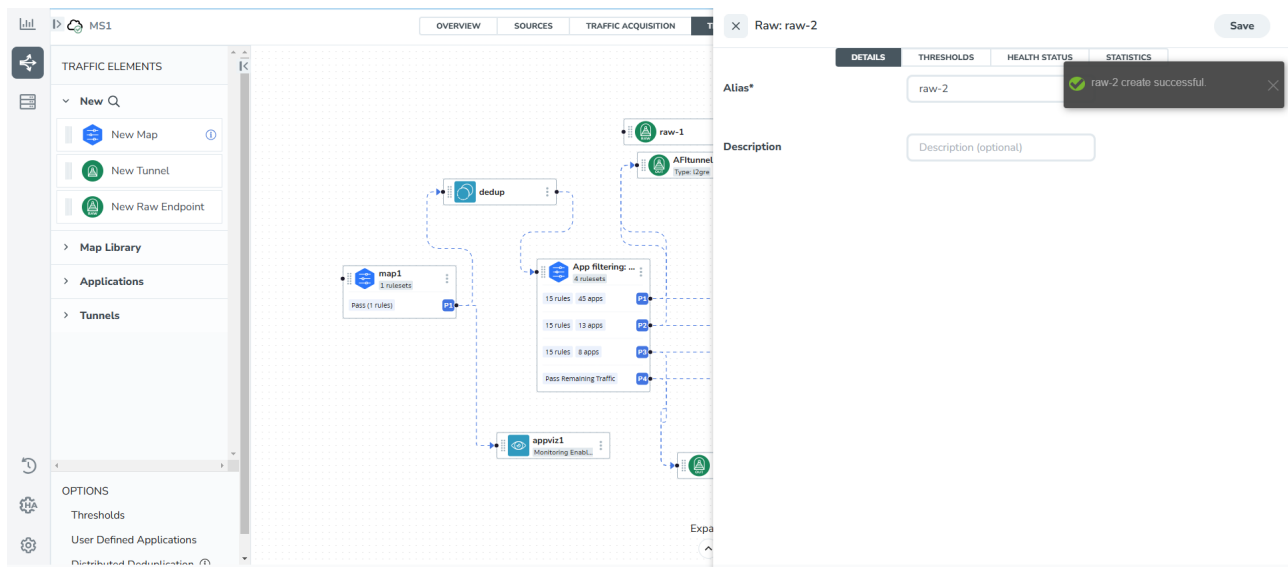
Create Raw Endpoint (Azure)

Raw End Point (REP) is used to pass traffic from an interface. REP is used to ingress data from a physical interface attached to GigaVUE V Series Nodes. You can optionally use this end point to send traffic to the applications deployed in the Monitoring Session.

NOTE: The maximum number of links that can egress from any endpoint in V Series is four.

To add Raw Endpoint to the Monitoring Session:

1. Drag and drop **New Raw Endpoint** from the **New** expand menu to the graphical workspace.
2. On the new raw endpoint icon, click the  menu button and select **Details**. The **Raw** quick view page appears.
3. Enter the Alias and Description details for the Raw End Point and click **Save**.



4. To deploy the Monitoring Session after adding the Raw Endpoint:
 - a. Select **Deploy** from the **Actions** drop-down list on the **TRAFFIC PROCESSING** page. The **Deploy Monitoring Session** dialog box appears.
 - b. Select the V Series Nodes for which you wish to deploy the Monitoring Session.
 - c. Select the interfaces for each of the REPs and the TEPs deployed in the Monitoring Session from the drop-down menu for the selected individual V Series Nodes.
 - d. Select **Deploy**.
5. Select **Export** to download all or selected V Series Nodes in CSV and XLSX formats.

Create a New Map (Azure)

Terms to know before creating a map:

Parameter	Description
Rules	A rule (R) contains specific filtering criteria that the packets must match. The filtering criteria lets you determine the targets and the (egress or ingress) direction of tapping the network traffic.
Priority	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.
Pass	The traffic from the virtual machine is passed to the destination.
Drop	The traffic from the virtual machine is dropped when passing through the map.
Traffic Filter Maps	A set of maps that are used to match traffic and perform various actions on the matched traffic.
Inclusion Map	An inclusion map determines the instances to be included for monitoring. This map is used only for target selection.

Exclusion Map	An exclusion map determines the instances to be excluded from monitoring. This map is used only for target selection.
Automatic Target Selection (ATS)	A built-in feature that automatically selects the cloud instances based on the rules defined in the traffic filter maps, inclusion maps, and exclusion maps in the Monitoring Session. The below formula describes how ATS works: Selected Targets = Traffic Filter Maps $\cap$ Inclusion Maps - Exclusion Maps Below are the filter rule types that work in ATS: • mac Source • mac Destination • ipv4 Source • ipv4 Destination • ipv6 Source • ipv6 Destination • VM Name Destination • VM Name Source • VM Tag Destination • VM Tag Source • VM Category Source • VM Category Destination • Host Name The traffic direction is as follows: • For any rule type as Source - the traffic direction is egress. • For Destination rule type - the traffic direction is ingress. • For Hostname - As it doesn't have Source or Destination rule type, the traffic direction is Ingress and Egress. Note: • If no ATS rule filters listed above are used, all VMs and vNICs are selected as targets. When any ATS rule results in a null set, no target is selected and V Series Node does not receive traffic from any VM or vNIC. • Use the GigamonNode Tag to exclude any Gigamon devices from the target. • When using VM Name filter for selecting the Virtual Machines using Inclusion and Exclusion Maps, wild- cards in VM names are not supported. You must use the prefix of the Virtual Machine name.
Group	A group is a collection of maps that are pre-defined and saved in the map library for reuse.

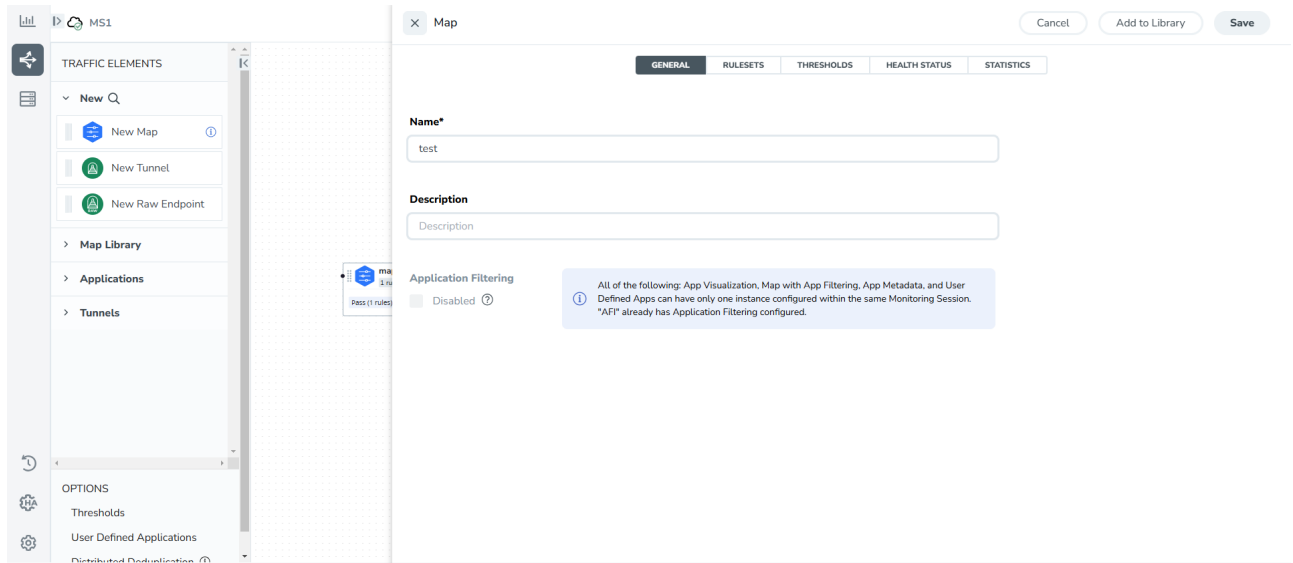
Rules and Notes:

- Directional rules do not work on single NIC VMs that are running a Windows UCT-V.
- Loopback captures bidirectional traffic from both ingress and egress. To prevent duplicate tapping, only egress tapping is permitted.

- If a packet is fragmented then all the fragments are destined to the same application end point. You can find the stats of mapped fragmented traffic in GigaVUE-FM.

To create a new map:

1. Drag and drop **New Map** from the **New** expand menu to the graphical workspace. The **Map** quick view appears.



2. On the new Map quick view, select the **General** tab and enter the required information as described below.

- a. Enter the **Name** and **Description** of the new map.
- b. Enable the **Application Filtering** option if you wish to use Application Filtering Intelligence.

Enabling this option allows you to filter traffic based on Application name or family. Refer to [Application Filtering Intelligence](#).

NOTE: Pass and Drop rule selection with Automatic Target Selection (ATS) differ with the Map type as follows:

- Traffic Map—Only Pass rules for ATS
- Inclusion Map—Only Pass rules for ATS
- Exclusion Map—Only Drop rules for ATS

3. Select the **Rule Sets** tab.
 - a. **To create a new rule set:**
 - i. Select **Actions > New Ruleset**.
 - ii. Enter a **Priority** value from 1 to 5 for the rule with 1 being the highest and 5 is the lowest priority.
 - iii. Enter the Application Endpoint in the Application EndPoint ID field.
 - iv. Select a required condition from the drop-down list.
 - v. Select the rule to **Pass** or **Drop** through the map.
 - b. **To create a new rule:**
 - i. Select **Actions > New Rule**.
 - ii. Select a required condition from the drop-down list. Click  and select **Add Condition** to add more conditions.
 - iii. Select the rule to **Pass** or **Drop** through the map.
4. Select **Save**.

Through the map, you can drop or pass packets based on the highest to lowest rule priority. You can add 5 rule sets on a map. Use the + and - buttons to add or remove a rule set in the map. Each rule set can have only 25 rules per map and each rule can have a maximum of 4 conditions. To add ATS rules for an Inclusion/Exclusion map, you must select at least one rule condition. For details, refer to [Example- Create a New Map using Inclusion and Exclusion Maps](#).

You can also perform the following action in the Monitoring session canvas.

- To edit a map, select the  menu button of the required map on the canvas and click **Details**, or select **Delete** to delete the map.
- To apply threshold template to maps, select the required map on the canvas and click **Details**. The quick view appears, select on the Thresholds tab. For more details on how to create or apply threshold templates, refer to [Monitor Cloud Health](#).
- Hover over the rules and apps buttons on the map to view the rule and applications configured for the selected map. Select the rules and apps buttons to open the quick view menu for RULESETS.

Example- Create a New Map using Inclusion and Exclusion Maps

Consider a Monitoring Session with 5 cloud instances. Namely target-1-1, target-1-2, target-1-3, target-2-1, target-2-2.

1. Drag and drop a new map template to the workspace. The New map quick view appears.
2. In the **GENERAL** tab, enter the name as Map 1 and enter the description. In the **RULESETS** tab, enter the priority and Application Endpoint ID.

3. Select the condition as VM Name and enter the **target**. This includes the instances target-1-1, target-1-2, target-1-3, target-2-1, and target-2-2.
4. Select the Expand icon at the bottom of the Monitoring session canvas. The Inclusion Maps and Exclusion Maps section appears.
5. Drag and drop a new map template to the Inclusion Maps region. The New Map quick view appears. Enter the Name and Description of the map.
 - a. In the **GENERAL** tab, enter the name as Inclusionmap1 and enter the description. In the **RULESETS**, enter the priority and Application Endpoint ID.
 - b. Select the condition as VM Name and enter the VM Name as **target-1**. Then, the instance with VM name **target-1-1**, **target-1-2**, and **target-1-3** is included.
6. Drag and drop a new map template to the Exclusion Maps region. The New Map quick view appears. Enter the details as mentioned in the above section.
 - a. In the **GENERAL** tab, enter the name as Exclusionmap1 and enter the description. In the **RULESETS** tab, enter the priority and Application Endpoint ID.
 - b. Select the condition as VM Name and enter the VM Name as **target-1-3**. Then, the instance **target-1-3** is excluded.

Based on this configuration, the Automatic Target Selection selects the instances target-1-1 and target-1-2 as target.

Map Library

Map Library is available in the **TRAFFIC PROCESSING** canvas page. You can add and use the maps from the Monitoring Session.

To add a map,

1. From the **Monitoring Session** screen, select **TRAFFIC PROCESSING**.

The GigaVUE-FM Canvas page appears.

2. From the page, select the desired map and save it as a template.
3. Select **Details**.

The Application quick view appears.

4. Select **Add to Library** and perform one of the following:
 - From the **Select Group** list, select an existing group.
 - Select **New Group** to create a new one.
5. In the **Description** field, add details, and select **Save**.

The map is added to Map Library. You can use the added map for all the monitoring sessions.

Reusing a map

From the **Map Library**, drag and drop the saved map.

Add Applications to Monitoring Session (Azure)

GigaVUE Cloud Suite with GigaVUE V Series Node supports the following GigaSMART applications in the GigaVUE-FM canvas:

The following table summarizes GigaSMART feature support across GigaVUE Cloud Suite platforms, covering packet operations, tunnel handling, application intelligence, and 5G capabilities.

GigaSMART Operation	GigaVUE Cloud Suite for AWS	GigaVUE Cloud Suite for Azure	GigaVUE Cloud Suite for OpenStack	GigaVUE Cloud Suite for VMware (VMware vCenter)	GigaVUE Cloud Suite for VMware (NSX-T)	GigaVUE Cloud Suite for Third Party Orchestration	GigaVUE Cloud Suite for Nutanix
Application Filtering Intelligence (APF without RegEx+ASF)	✓	✓	✓	✓	✓	✓	✓
Application Metadata Exporter	✓	✓	✓	✓	✓ (Only when deploying GigaVUE V Series Node using Third party Orchestration)	✓	✓
Application Metadata Intelligence	✓	✓	✓	✓	✓	✓	✓
Application Visualization	✓	✓	✓	✓	✓	✓	✓

GigaSMA RT Operation	GigaVUE Cloud Suite for AWS	GigaVUE Cloud Suite for Azure	GigaVUE Cloud Suite for OpenStack	GigaVUE Cloud Suite for VMware (VMware vCenter)	GigaVUE Cloud Suite for VMware (NSX-T)	GigaVUE Cloud Suite for Third Party Orchestration	GigaVUE Cloud Suite for Nutanix
De-duplication	✓	✓	✓	✓	✓	✓	✓
L2GRE Tunnel Encapsulation Refer to <i>Create Ingress and Egress Tunnels</i> section on the retrospective GigaVUE Cloud Suite Deployment Guide.	✓	✗	✓	✓	✓	✓	✓
VXLAN Tunnel Encapsulation Refer to <i>Create Ingress and Egress Tunnels</i> section on the retrospective GigaVUE Cloud Suite Deployment Guide.	✓	✓	✓	✓	✓	✓	✓
L2GRE Tunnel Decapsulation	✓	✗	✓	✓	✓	✓	✓

GigaSMA RT Operation	GigaVUE Cloud Suite for AWS	GigaVUE Cloud Suite for Azure	GigaVUE Cloud Suite for OpenStack	GigaVUE Cloud Suite for VMware (VMware vCenter)	GigaVUE Cloud Suite for VMware (NSX-T)	GigaVUE Cloud Suite for Third Party Orchestration	GigaVUE Cloud Suite for Nutanix
on Refer to <i>Create Ingress and Egress Tunnels</i> section on the retrospective GigaVUE Cloud Suite Deployment Guide.							
VXLAN Tunnel Decapsulation Refer to <i>Create Ingress and Egress Tunnels</i> section on the retrospective GigaVUE Cloud Suite Deployment Guide.	✓	✓	✓	✓	✓	✓	✓
ERSPAN Tunnel Decapsulation Refer to <i>Create Ingress and Egress</i>	✓	x	✓	✓	✓	✓	✓

GigaSMART Operation	GigaVUE Cloud Suite for AWS	GigaVUE Cloud Suite for Azure	GigaVUE Cloud Suite for OpenStack	GigaVUE Cloud Suite for VMware (VMware vCenter)	GigaVUE Cloud Suite for VMware (NSX-T)	GigaVUE Cloud Suite for Third Party Orchestration	GigaVUE Cloud Suite for Nutanix
Tunnels section on the retrospective GigaVUE Cloud Suite Deployment Guide.							
UDPGRE Tunnel Decapsulation Refer to <i>Create Ingress and Egress Tunnels</i> section on the retrospective GigaVUE Cloud Suite Deployment Guide.	✓	✗	✓	✓	✓	✓	✗
GigaSMART NetFlow Generation	✓	✓	✓	✓	✓	✓	✓
GRE-In-UDP Tunnel Decapsulation	✗	✗	✓	✓	✗	✓	✗
GENEVE Decapsulation	✓	✗	✗	✗	✓	✗	✗
Header Stripping	✓	✓	✓	✓	✓	✓	✓

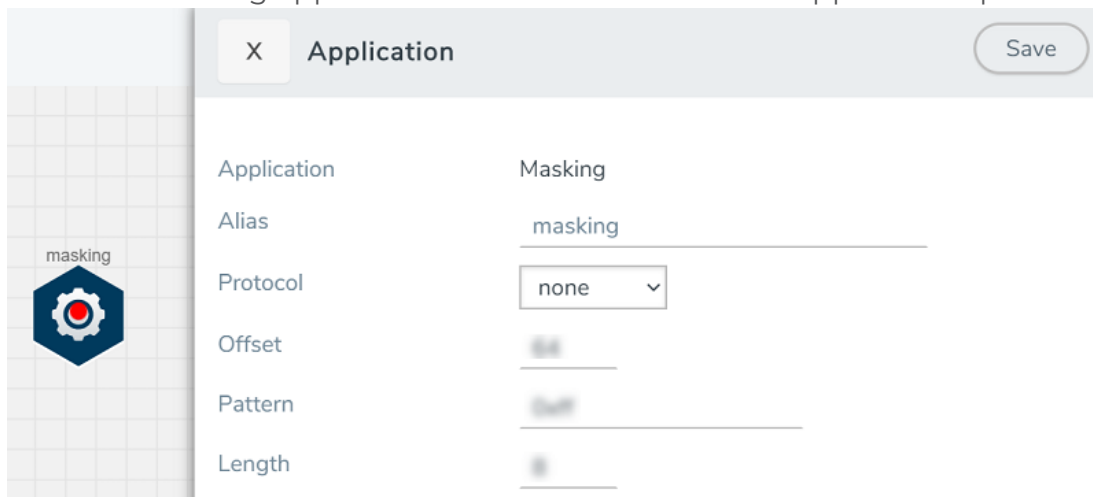
GigaSMA RT Operation	GigaVUE Cloud Suite for AWS	GigaVUE Cloud Suite for Azure	GigaVUE Cloud Suite for OpenStack	GigaVUE Cloud Suite for VMware (VMware vCenter)	GigaVUE Cloud Suite for VMware (NSX-T)	GigaVUE Cloud Suite for Third Party Orchestration	GigaVUE Cloud Suite for Nutanix
Load Balancing	✓	✓	✓	✓	✓	✓	✓
Masking	✓	✓	✓	✓	✓	✓	✓
SSL Decrypt	✓	✓	✓	✓	✗	✓	✓
Secure Tunnels Encapsulation	✗	✓	✗	✓	✓	✓	✓
Secure Tunnels Decapsulation	✗	✓	✗	✓	✓	✓	✓
Slicing	✓	✓	✓	✓	✓	✓	✓
5G-Cloud Application	✗	✗	✓	✓	✗	✓	✗
5G-Service Based Interface Application	✗	✗	✓	✓	✓	✓	✗

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.



The screenshot shows the 'Masking' application configuration window. On the left is a sidebar with a grid of application icons; the 'masking' icon, which is a blue hexagon with a red gear, is selected. The main area is titled 'Application' and contains the following fields:

Field	Value
Application	Masking
Alias	masking
Protocol	none
Offset	0
Pattern	0x00
Length	1

At the top right of the configuration area is a 'Save' button.

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 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**.

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

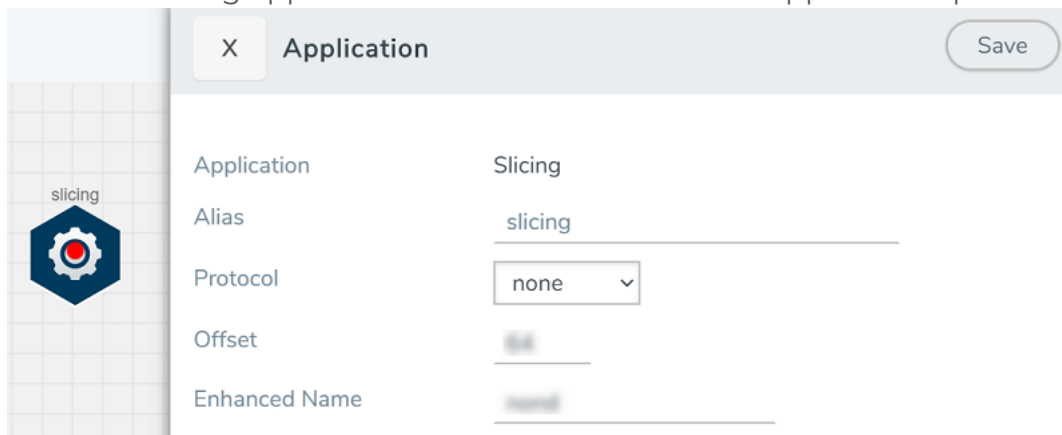
Packet Slicing allows you to truncate packets after a specified header and slice length, preserving the portion of the packet required for monitoring purposes. Slicing operations are typically configured to preserve specific packet header information, allowing effective network analysis without the overhead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



Application	
Application	Slicing
Alias	slicing
Protocol	none
Offset	64
Enhanced Name	none

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**.

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.

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.

Refer to the following topics:

- [Feature Overview](#)
- [Configure De-duplication Application](#)
- [Distributed De-duplication](#)

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.

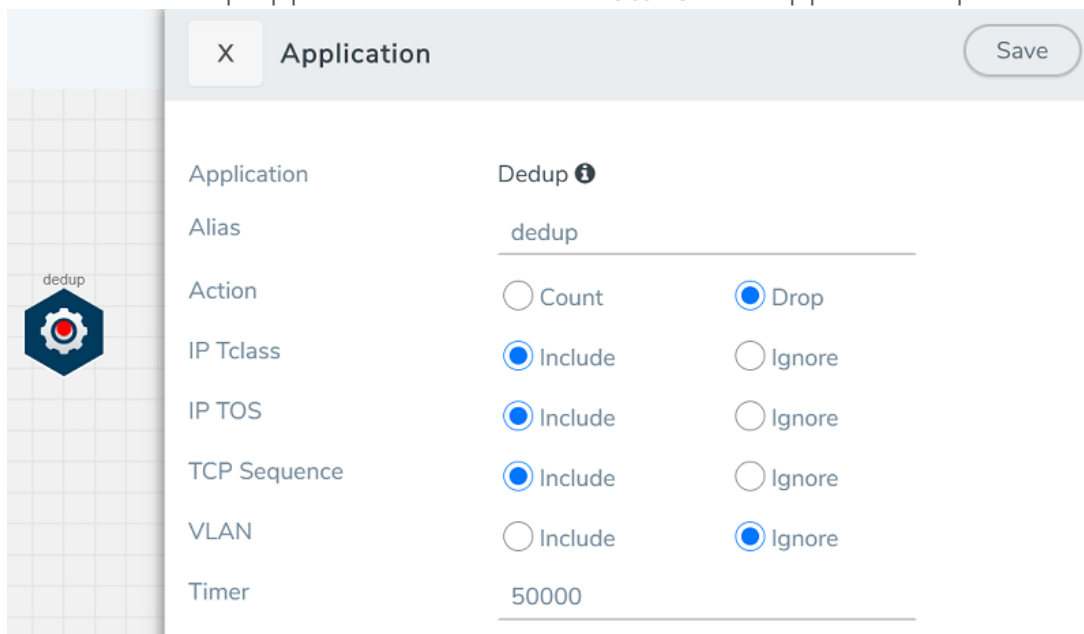
For IPv4 and IPv6 packets, to determine if a packet is considered to be a duplicate, parts of the IP headers (Layer 3 and Layer 4), as well as part of the payload are compared.

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.



Application	Dedup ⓘ
Alias	dedup
Action	☐ Count ☒ Drop
IP Tclass	☒ Include ☐ Ignore
IP TOS	☒ Include ☐ Ignore
TCP Sequence	☒ Include ☐ Ignore
VLAN	☐ Include ☒ Ignore
Timer	50000

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

Parameter	Description
Alias	Enter a name for the 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**.

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.

NOTE: From version 6.9, Traffic Distribution option is renamed to Distributed De-duplication.

From version 6.5, distributed de-duplication is supported on Azure, AWS, GCP, Nutanix, VMware NSX-T, VMware ESXi, and OpenStack. 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.

Limitations

- When using distributed de-duplication application, if **Prefer IPv6** option is enabled when configuring GigaVUE V Series Node using GigaVUE-FM, IPv6 tunnel will be created only between GigaVUE V Series Node and UCT-V and the rest of the tunnels created are IPv4 tunnels. Refer to Configure GigaVUE Fabric Components section in the respective cloud deployment guide for more detailed information on how to deploy GigaVUE V Series Node with IPv6 tunnels.
- When using distributed de-duplication application, if **Enable IPv6 Preference** option is enabled when configuring GigaVUE V Series Node using Third Party Orchestration, IPv6 tunnel will be created only between GigaVUE V Series Node and UCT-V and the rest of the tunnels created are IPv4 tunnels. Refer to *Create Monitoring Domain* section in GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration Guide for more detailed information on how to create a monitoring domain to register GigaVUE fabric components with IPv6 tunnels.

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.

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:

- [Configure Application Visualization for Virtual Environment](#)
- [Configure Application Filtering Intelligence for Virtual Environment](#)
- [Configure Application Metadata Intelligence for Virtual Environment](#)
- [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 16GB RAM)	200k
AWS	AMD - Large (c5n.2xlarge)	300k
	AMD - Medium (t3a.xlarge)	100k
	ARM - Large (c7gn.2xlarge)	100k
	ARM - Medium (m7g.xlarge)	200k
Azure	Large (Standard_D8s_V4)	500k
	Medium (Standard_D4s_v4)	100k
Nutanix	Large (8 vCPU and 16GB RAM)	200k

- 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..
 - If the rate of unique UDP sessions per second exceeds the threshold—calculated as maximum number of flows per second divided by the UDP timeout value—the system may fail to classify applications correctly. In such cases, AFI may not filter packets accurately, resulting in incorrect packet passes or drops. However, this limitation does not apply to DNS flows.
- 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* section in GigaVUE Cloud Suite Deployment Guide - VMware (ESXi) for 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](#)
- [Configure Filtering and Metadata Export for Selected Applications in Application Visualization](#)
- [View Application Statistics for 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. <table border="1"> <thead> <tr> <th>Cloud Platform</th><th>Instance Size</th><th>Maximum Number of Flows</th></tr> </thead> <tbody> <tr> <td>VMware</td><td>Large (8 vCPU and 16GB RAM)</td><td>200k</td></tr> <tr> <td rowspan="4">AWS</td><td>AMD - Large (c5n.2xlarge)</td><td>300k</td></tr> <tr> <td>AMD - Medium (t3a.xlarge)</td><td>100k</td></tr> <tr> <td>ARM - Large (c7gn.2xlarge)</td><td>100k</td></tr> <tr> <td>ARM - Medium (m7g.xlarge)</td><td>200k</td></tr> <tr> <td rowspan="2">Azure</td><td>Large (Standard_D8s_v4)</td><td>500k</td></tr> <tr> <td>Medium (Standard_D4s_v4)</td><td>100k</td></tr> <tr> <td>Nutanix</td><td>Large (8 vCPU and 16GB RAM)</td><td>200k</td></tr> </tbody> </table> ▪ 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.. ▪ If the rate of unique UDP sessions per second exceeds the threshold—calculated as maximum number of flows per second divided by the UDP timeout value—the system may fail to classify applications correctly. In such cases, AFI may not filter packets accurately, resulting in incorrect packet passes or drops. However, this limitation does not apply to DNS flows.	Cloud Platform	Instance Size	Maximum Number of Flows	VMware	Large (8 vCPU and 16GB RAM)	200k	AWS	AMD - Large (c5n.2xlarge)	300k	AMD - Medium (t3a.xlarge)	100k	ARM - Large (c7gn.2xlarge)	100k	ARM - Medium (m7g.xlarge)	200k	Azure	Large (Standard_D8s_v4)	500k	Medium (Standard_D4s_v4)	100k	Nutanix	Large (8 vCPU and 16GB RAM)	200k
Cloud Platform	Instance Size	Maximum Number of Flows																						
VMware	Large (8 vCPU and 16GB RAM)	200k																						
AWS	AMD - Large (c5n.2xlarge)	300k																						
	AMD - Medium (t3a.xlarge)	100k																						
	ARM - Large (c7gn.2xlarge)	100k																						
	ARM - Medium (m7g.xlarge)	200k																						
Azure	Large (Standard_D8s_v4)	500k																						
	Medium (Standard_D4s_v4)	100k																						
Nutanix	Large (8 vCPU and 16GB RAM)	200k																						
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. Note: This option is disabled for NetVUE Base Bundle License.																							

4. Click **Save**.

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 Environment](#) section 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](#) section for more detailed instructions on how to configure Application Metadata application.

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. You can use the **Select Tags** filter option to filter the traffic related to the selected application tags.
 - b. **Total Applications :** 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.
 - c. **Top 10 Applications:** Click on the drop-down menu that displays **All** and select the **Top 10** . Displays the Top 10 applications running in the network based on the metrics.
 - d. **Top 10 Application Families:** You can view a graphical representation of top 10 applications running in the network based on the metrics. When you hover over the Pie-chart, GigaVUE-FM shows the application families in the network.

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 within 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.

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	Server to Client Only	REGEXP	.*\football\.*

			is redirecte d to			
	cts- cookie	Cookie (Raw)	Raw value of the HTTP Cookie header line	Client to Server Only	REGEXP	.*tEstCoOkie.*
	content	Conten t	Message body content	Both, Client to Server or Server to Client	REGEXP	.*GIGAMON.* mindata = 206 Refer Mindata
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		REGEXP	(.*\.)?gigamon\.com

			Hello message or the certificate			
	stc-subject_alt_name	Subject Alt Name(s)	List of host names which belong to the same certificate	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		REGEXP	.*GIGAMON.* mindata = 100

			packet, excluding the header			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 Server to Client	REGEXP	GVUE-release 6.2.0
icmp	code	Message Code	Code of the ICMP message	Both, Client to Server or Server to Client	UINT8 as REGEXP String	200
	typeval	Message Type	Type of ICMP message	Both, Client to Server or Server to Client	UINT8 as REGEXP String	10
ip	address	Server IP Addresses	IP address of the server		IPV4 as REGEXP String	62.132.12.30\24
	dscp	DSCP Value	DSCP from Different		UINT8 as REGEXP	33

			ia ted Service (DS) Field in IP header		String	
	resolv_ name	DNS Name	Server's DNS name		REGEXP	gigamon.com
ipv6	address	Server IP Addres s	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 Different ia 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 GigaVUE-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:

You can create rules for User Defined Application in two ways:

1. Go to **Inventory > Resources > User-defined Applications**. Refer to User Defined Applications section in GigaVUEGigaVUE Fabric Management Guide for details.
2. Go to **Traffic > Virtual > Orchestrated Flows > Select your cloud platform**. Follow the steps listed below:
 - a. Select a Monitoring Session from the list view. Navigate to **TRAFFIC PROCESSING** tab. The GigaVUE-FM canvas page appears.
 - b. In the canvas, click on the  icon on the left side of the page to view the traffic processing elements.
 - c. Select **User Defined Applications** under **Options** menu.
 - d. Enable the **User-defined Applications** toggle button.
 - e. Click **New Application**. The New Application page appears.
 - f. Enter the **User-Defined Application Name**.
 - g. Enter **Priority**. The value must be between 1 and 120.

NOTE: The lowest value has the highest priority.

- h. In the Rules dialog box, select the following details:
 - Choose the **Protocol** from the list of protocols.
 - Choose the **Attributes** from the list of attributes.
 - Choose the **Values** from the list of values.

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

- i. Click **Save**.

To add the created applications to the Monitoring Session:

1. In the **User Defined Applications** 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) or application tags. 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 statistics:

- [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.																							
	<table><tr><th>Cloud Platform</th><th>Instance Size</th><th>Maximum Number of Flows</th></tr><tr><td>VMware</td><td>Large (8 vCPU and 16GB RAM)</td><td>200k</td></tr><tr><td rowspan="4">AWS</td><td>AMD - Large (c5n.2xlarge)</td><td>300k</td></tr><tr><td>AMD - Medium (t3a.xlarge)</td><td>100k</td></tr><tr><td>ARM - Large (c7gn.2xlarge)</td><td>100k</td></tr><tr><td>ARM - Medium (m7g.xlarge)</td><td>200k</td></tr><tr><td rowspan="2">Azure</td><td>Large (Standard_D8s_V4)</td><td>500k</td></tr><tr><td>Medium (Standard_D4s_v4)</td><td>100k</td></tr><tr><td>Nutanix</td><td>Large (8 vCPU and 16GB RAM)</td><td>200k</td></tr></table>	Cloud Platform	Instance Size	Maximum Number of Flows	VMware	Large (8 vCPU and 16GB RAM)	200k	AWS	AMD - Large (c5n.2xlarge)	300k	AMD - Medium (t3a.xlarge)	100k	ARM - Large (c7gn.2xlarge)	100k	ARM - Medium (m7g.xlarge)	200k	Azure	Large (Standard_D8s_V4)	500k	Medium (Standard_D4s_v4)	100k	Nutanix	Large (8 vCPU and 16GB RAM)	200k
	Cloud Platform	Instance Size	Maximum Number of Flows																					
	VMware	Large (8 vCPU and 16GB RAM)	200k																					
	AWS	AMD - Large (c5n.2xlarge)	300k																					
		AMD - Medium (t3a.xlarge)	100k																					
		ARM - Large (c7gn.2xlarge)	100k																					
		ARM - Medium (m7g.xlarge)	200k																					
	Azure	Large (Standard_D8s_V4)	500k																					
		Medium (Standard_D4s_v4)	100k																					
Nutanix	Large (8 vCPU and 16GB RAM)	200k																						
- 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.. - If the rate of unique UDP sessions per second exceeds the threshold—calculated as maximum number of flows per second divided by the UDP timeout value—the system may fail to classify applications correctly. In such cases, AFI may not filter packets accurately, resulting in incorrect packet passes or drops. However, this limitation does not apply to DNS flows.																								
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 GigaVUE-FM. If all the attributes of the application are disabled then the application itself is disabled.																							

- 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 a Type. The available options are: • Application Family: Each application is mapped only mapped to one Application Family ▪ 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. • Application Tag: Each application can be mapped to one or more Application Tags. ▪ Select an Application Tag 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. - Enable User Defined Applications toggle button in the Options page. Refer to Supported Protocols and Attributes topic for more detailed information on what is user defined applications and how to configure it. - In this Add Application dialog box, select User Defined Applications from the Application Family list.

- 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.
- 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 the 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 6000 attributes for more than 4000 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 to [Application 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:



Notes:

- Ensure to create separate Monitoring Domains and Monitoring Sessions for Application Metadata Exporter (AMX) and Application Metadata Intelligence (AMI). Even when AMI is deployed virtually, it operates independently and requires its own Monitoring Session.
- Flow Direction/Behaviour under Application Metadata Settings must be configured as **Bidirectional** for exporting application Metadata. Each exporter can be configured to export application metadata for up to 256 applications, and up to 64 attributes can be exported for each application. GigaVUE-FM allows selecting metadata for applications



that support exporting metadata. Applications which do not support exporting metadata are not listed in the GigaVUE-FM. By default, application name is exported for all such applications.

1. In GigaVUE-FM, go to **Traffic > Virtual > Orchestrated Flows**. Select the required cloud platform.
2. After creating a new Monitoring Session or on an existing Monitoring Session, navigate to the **TRAFFIC PROCESSING** tab. The GigaVUE-FM Monitoring Session canvas page appears.
3. Drag and drop **Application Metadata** from **APPLICATIONS** to the graphical workspace.
4. Click the Application Metadata application and select **Details**. The Application quick

view appears.

5. 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. This option is disabled by default. 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 .
Enable DPI Packet limit	This field is used to restrict the number of packets in a particular session to be sent to the DPI engine instead of sending all the packets in order to improve the AMI performance. The value must range between 20 - 50 as the first 20 to 50 packets contains the most significant attributes.
Recurring attributes (SNI)	When enabled, it keeps the TLS SNI (SSL server name) for the full lifetime of each SSL/TLS flow. This means every active or inactive timeout export record will include the hostname, giving consistent visibility for long-lived flows. When disabled, SNI is exported only in the first record of a session. Later records for the same flow may not contain the hostname. This feature is supported only on GigaVUE HC Series Gen3 and GigaVUE V Series. It requires a bidirectional cache and exporter templates that already export SNI. The setting applies only to new flows after it is enabled.
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.

Parameter	Description		
	Cloud Platform	Instance Size	Maximum Number of Flows
	VMware	Large (8 vCPU and 16GB RAM)	200k
	AWS	AMD - Large (c5n.2xlarge)	300k
		AMD - Medium (t3a.xlarge)	100k
		ARM - Large (c7gn.2xlarge)	100k
		ARM - Medium (m7g.xlarge)	200k
	Azure	Large (Standard_D8s_V4)	500k
		Medium (Standard_D4s_v4)	100k
	Nutanix	Large (8 vCPU and 16GB RAM)	200k
	- 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.. - If the rate of unique UDP sessions per second exceeds the threshold—calculated as maximum number of flows per second divided by the UDP timeout value—the system may fail to classify applications correctly. In such cases, AFI may not filter packets accurately, resulting in incorrect packet passes or drops. However, this limitation does not apply to DNS flows.		
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.		
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.		
Protocol		Attribute	
http		rtt	
icmp		rtt	
icmp6		rtt	
ssh		rtt	
tcp		rtt	
tcp		rtt_app	

Parameter	Description	
	telnet	rtt
	wsp	connect_rtt
	wsp	query_rtt

6. 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. • Save as New Template - Use to save the current configuration as a new custom tool template. • Delete this Exporter - Use to delete the Exporter.
Template	Use to select the tool template. Refer to <i>Tool Templates</i> section in GigaVUE Fabric Management Guide for more information on tool templates and how to create custom tool templates.
Export Params	Select any one of the following options: • Application Name - Exports Application Name Attribute in AMI records. Enable this option to export Application Name attribute with network attributes • Application Family - Exports Application Family Attribute in AMI records. Enable this option to export Application Family attribute with network attributes • Application Tags - Exports Application Tag Attribute in AMI records. Enable this option to export Application Tag attribute with network attributes
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. Note: It is recommended to select Cohesive from the drop-down menu, as NetFlow exports network and transport parameters only.
Enable Maximum Packet Length	Enable this option to edit the interface MTU value.
Maximum Packet Length (This option appears only when Enable Maximum Packet Length option is enabled)	Using this field, you can configure the maximum length of the packet that can be exported. Enter this value less than or equal to egress interface MTU value to avoid fragmentation. The value can range between 1280 and 9001.
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

Parameter	Description
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, V9, NetFlow IPFIX(V10), or CEF when the flow direction is Uni-Directional in the above Template drop-down menu.)	
NOTE: When you edit application attributes during an AMI deployment with background traffic, you may experience minor data loss until the update completes.	
Add Application	Click on the Add Application button. The Add Application dialog box opens. Select a Type. The available options are: Application Family: Each application is mapped only mapped to one Application Family - Select an Application Family and the Applications that needs to be filtered from the traffic. - Attributes for the selected application is displayed in the Attribute column. You can select the required attributes. Application Tag: Each application can be mapped to one or more Application Tags. - Select an Application Tag and the Applications that needs to be filtered from the traffic. - Attributes for the selected application is displayed in the Attribute column. You can select the required attributes. NOTE: The AMI exporter exports application metadata for the selected applications but exports the packet attributes for all applications. To export packet attributes only for the selected applications, filter the required traffic by using a flow map or AFI.
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.

Parameter	Description
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.

NOTE: In the exporter record, the generator ID represents the hostname of the GigaVUE V Series Node. Any changes to the hostname after deploying the Monitoring Domain with the AMI application will not be reflected in the exporter record.

7. Click **Save**.

After configuring the Application Metadata application, follow the below steps to create an egress tunnel:

1. In the canvas page, select **New > New Tunnel**, drag and drop a new tunnel template to the workspace. The **Add Tunnel Spec** quick view appears.
2. Enter the **Alias**, **Description** and select **UDP** as **Type**.

NOTE: When using Application Metadata, if you create a tunnel to send the output to the tools, select UDP as the tunnel type.
You can either use a single tunnel to export all metadata from the application or configure separate tunnels for each exporter.

3. Enter the **MTU** value.
4. **L4 Destination IP Address** - Enter the IP address of the tool port. If using Application Metadata Exporter (AMX), enter the data subnet IP address of the V Series Node where AMX application is deployed. Refer to [Application Metadata Exporter](#) for details.
5. **Source L4 Port** - The port from which the connection will be established to the target. For example, if A is the source and B is the destination, this port value belongs to A.

6. **Destination L4 Port** - The port to which the connection will be established from the source. For example, if A is the source and B is the destination, this port value belongs to B. The destination port must match the AMX ingestor port number to ensure seamless data forwarding from AMI to AMX.

NOTE: If the export format is CEF, the default value for L4 destination port is 514. If the export format is NetFlow, the default value for L4 destination port is 2055.

To deploy the configured Application Metadata Intelligence application, follow the below steps:

1. On the Monitoring Session canvas page, click **Deploy** from the **Actions** menu to deploy the Monitoring Session. The status is displayed as **Success** in the Monitoring Sessions page. The session is successfully deployed on the V Series Node.
2. You can view the Monitoring Session Deployment Report in the **SOURCES** and **V SERIES NODES** tab. When you click on the Status link, the Deployment Report is displayed. If the Monitoring Session is not deployed properly, then one of the following errors is displayed in the Status column.
 - Success—The session is not deployed on one or more instances due to V Series Node failure.
 - Failure—The session is not deployed on any of the V Series Nodes or Instances.

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

NOTE: To configure Application Metadata Intelligence in physical environment, refer to [Create an Application Intelligence Session in Physical Environment](#).

Extend Your AMI and AMX Deployment

Your AMI and AMX deployment is the foundation of deep network observability. Once it is up and running, you can:

- **Integrate with Third-Party Tools:** AMI and AMX support seamless integration with popular monitoring, analytics, security, and visualization platforms such as Splunk, Elastic, CrowdStrike, Dynatrace, Datadog, and Grafana. For step-by-step integration guides, refer to [Integrate Application Metadata Intelligence and Application Metadata Exporter with Tools](#).
- **Analyze Metadata with Gigamon Insights:** Use [Gigamon Insights](#) to query your AMI and AMX metadata using plain-language prompts and get immediate, AI-powered answers — no dashboards or manual queries needed.

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.

Header Stripping

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

Furthermore, the presence of protocols like GTP, ISL, ERSPAN, MPLS, MPLS+VLAN, VLAN, VN-tag, VXLAN, GENEVE, 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
- GENEVE
- Generic



Note:

Header Stripping for the GENEVE protocol is currently supported for the following platforms:

- VMware vCenter
- VMware NSX-T
- Nutanix

Limitation

The GENEVE protocols currently supported for header stripping are the Transparent Ethernet Bridge (0x6558), IPv4 (0x0800), and IPv6 (0x86DD).

Configure Header Stripping Application

To configure the Header Stripping application in GigaVUE-FM, 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 or select the required information as described in the following table:

Field	Description
Alias	Enter the alias name for the application.
Protocol	Select the type of protocol.
VLAN: Use this option to strip the VLAN header from the packets. You can either strip 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 time stamping. 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 strip. The only supported format for the time stamp is None .
ESPRAN: Use this option to strip ESPRAN Type II and Type III headers. When choosing ESPRAN as your protocol for stripping, enter the following details:	
ESPRAN FlowID	Specify an ESPRAN flow ID between 0 to 1023. A flow ID of zero is a wildcard value that matches all flow IDs.
GENEVE: Use this option to strip the GENEVE header from the packets. The default L4 Destination Port value is 6081. To change the default L4 destination port value, follow the steps given below:	
1. Expand the Custom Port section. 2. You can either select an existing template with the port details or provide them directly in the pop-up window. - o Using Template - If you wish to use an existing template, select the template from the Template drop-down menu. To create a new template, refer to Create Custom Port Template. Note: You cannot modify an existing template by editing the values directly in the Monitoring Session. However, you can modify the values in the Monitoring Session and save it as a new template. - o Without Template - You can directly enter your port details in the L4 Destination Port field. Click the Save as New Template button to save this existing configuration as a template. You can view the newly created template in the Custom Port Template page.	

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

4. Click **Save**.

Create Custom Port Template

GigaVUE-FM enables you to specify custom L4 destination port values when using the Header Stripping application. You can create a template and utilize it to define custom port values when configuring the Header Stripping application.

To create a custom port template for the Header Stripping application:

1. Go to **Inventory > Resources > Custom Port Template**. The **Custom Port Template** page appears.
2. Click **New** to create a new template. The **New Custom Port Template** dialog box appears.
3. Enter a name for the template.
4. Enter valid port numbers between the range 1025 to 65535 in the **L4 Destination Port** field. Enter only comma separated integer values. You can provide a maximum of 10 ports. For example: 1034,1098,1039
5. Click **Save**.

You can view the created template on the **Custom Port Template** page. If a template is associated with a Monitoring Session, you can view the name of the Monitoring Session to which the template is associated in the Affected Entity column.

You can use the **Actions** buttons to perform the following:

- **Edit:** You can use this option to edit a template. If a template is associated with a Monitoring Session, editing it will be reflected in all the Monitoring Sessions associated with that template.
- **Delete:** You can use this option to delete a template. You cannot delete a template associated to a Monitoring Session.

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 a threshold template, refer to *Traffic Health Monitoring* section in the respective GigaVUE Cloud Suite 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 GigaVUE Cloud Suite deployment guides.

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

GigaSMART NetFlow Generation

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 topic for step-by-step instructions on how to configure NetFlow for Virtual Environment:

- [Configure Application Metadata Intelligence for Virtual Environment](#)- For SecureVUE Plus Base Bundle
- [Create NetFlow Session for Virtual Environment](#) - ForNetVUE 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. <table border="1"> <thead> <tr> <th>Cloud Platform</th><th>Instance Size</th><th>Maximum Number of Flows</th></tr> </thead> <tbody> <tr> <td>VMware</td><td>Large (8 vCPU and 16GB RAM)</td><td>200k</td></tr> <tr> <td rowspan="4">AWS</td><td>AMD - Large (c5n.2xlarge)</td><td>300k</td></tr> <tr> <td>AMD - Medium (t3a.xlarge)</td><td>100k</td></tr> <tr> <td>ARM - Large (c7gn.2xlarge)</td><td>100k</td></tr> <tr> <td>ARM - Medium (m7g.xlarge)</td><td>200k</td></tr> <tr> <td rowspan="2">Azure</td><td>Large (Standard_D8s_v4)</td><td>500k</td></tr> <tr> <td>Medium (Standard_D4s_v4)</td><td>100k</td></tr> <tr> <td>Nutanix</td><td>Large (8 vCPU and 16GB RAM)</td><td>200k</td></tr> </tbody> </table> - 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.. - If the rate of unique UDP sessions per second exceeds the threshold—calculated as maximum number of flows per second divided by the UDP timeout value—the system may fail to classify applications correctly. In such cases, AFI may not filter packets accurately, resulting in incorrect packet passes or drops. However, this limitation does not apply to DNS flows.	Cloud Platform	Instance Size	Maximum Number of Flows	VMware	Large (8 vCPU and 16GB RAM)	200k	AWS	AMD - Large (c5n.2xlarge)	300k	AMD - Medium (t3a.xlarge)	100k	ARM - Large (c7gn.2xlarge)	100k	ARM - Medium (m7g.xlarge)	200k	Azure	Large (Standard_D8s_v4)	500k	Medium (Standard_D4s_v4)	100k	Nutanix	Large (8 vCPU and 16GB RAM)	200k
Cloud Platform	Instance Size	Maximum Number of Flows																						
VMware	Large (8 vCPU and 16GB RAM)	200k																						
AWS	AMD - Large (c5n.2xlarge)	300k																						
	AMD - Medium (t3a.xlarge)	100k																						
	ARM - Large (c7gn.2xlarge)	100k																						
	ARM - Medium (m7g.xlarge)	200k																						
Azure	Large (Standard_D8s_v4)	500k																						
	Medium (Standard_D4s_v4)	100k																						
Nutanix	Large (8 vCPU and 16GB RAM)	200k																						

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 Create Custom 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 a Type. The available options are: • Application Family: Each application is mapped only mapped to one Application Family ▪ Select an Application Family and the Applications that needs to be filtered from the traffic. ▪ Attributes for the selected application is displayed in the Attribute column. You can select the required attributes. • Application Tag: Each application can be mapped to one or more Application Tags. ▪ Select an Application Tag and the Applications that needs to be filtered from the traffic. ▪ Attributes for the selected application is displayed in the

Parameter	Description
	Attribute column. You can select the required attributes.
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**.

Load Balancing

Load balancing application performs stateless distribution or Enhanced Load Balancing 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. fiveTuple: 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. greFlowid: The flow identifier location. NOTE: The default field location value is outer. When configuring 5G-Cloud Ericsson SCP Transparent, greFlowid hash field should be selected. Refer to 5G-Cloud Ericsson SCP Support.
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. Endpoint with higher weight receives more traffic.

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.

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 - gtpuportid
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.

× Load Balancing: lb
 Save

DETAILS

THRESHOLDS

HEALTH STATUS

STATISTICS

Application Load Balancing

Alias* lb

☐ Stateless
 ☒ Enhanced Load balancing

ELB profiles* Select... ▼

Load balancing groups

Application Endpoint ID	2	Weight	1	⊕ ⊖
Application Endpoint ID	3	Weight	1	⊕ ⊖

⏪

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.

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 GigaVUE Cloud Suite 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 GigaVUE Cloud Suite deployment guides.

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

SSL Decrypt

License: For information on licensing, refer to the) section of respective GigaVUE Cloud Suite Deployment Guide.

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 for SSL 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
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 140-3 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](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 Key Pairs](#)
- [Create SSL Service](#)
- [Key Mapping](#)
- [SSL Key Pair Store](#)
- [Add SSL Decrypt to Monitoring Session](#)

Upload SSL Key Pairs

To upload an SSL private key, do the following:

1. Go to **Inventory > Resources > Security > SSL Keys**.
2. Click **Add**. The **Create SSL Key Pair** 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 Pair 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 Pair 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 Key Pairs Page:

Field	Description
Edit	To edit a SSL Key pair, select the key from the list in the SSL Key Pairs page and click the Edit button.
Delete	To delete a SSL Key pair, select the key from the list in the SSL Key pairs page and click the Delete button.
Delete all	Use this button to delete all the SSL Key pairs in the SSL Key pairs page.
View certificate	To view the certificate associated with the particular SSL Key Pair, select the key from the list in the SSL Key Pairs 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 Key Pairs](#)

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 Pair 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 Key Pairs 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 Pair Store

SSL Key Pair 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 Pair 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 Pair Store Page:

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



XApplicationSave

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

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**.

Interface Mapping (Azure)

You can remap interfaces for individual GigaVUE V Series Nodes within a Monitoring Session.

Note: When using Raw and Tunnel In, Interface Mapping is mandatory before you deploy the Monitoring Session.

To perform interface mapping,

1. Go to **Traffic > Virtual > Orchestrated Flows** and select your cloud platform.

The **Monitoring Sessions** landing page appears.

2. Navigate to the **V SERIES NODES** tab and select **Interface Mapping**.

The **Deploy Monitoring Session** dialog box appears.

3. Select the GigaVUE V Series Nodes to which you wish to map the interface.
4. From the drop-down menu of the GigaVUE V Series Nodes, select the interfaces for the following deployed in the Monitoring Session:
 - REPs (Raw Endpoints)
 - TEPs (Tunnel Endpoints)
5. Select **Deploy**.

NOTE: The updated mappings take effect when deployed.

Deploy Monitoring Session (Azure)

You can deploy the Monitoring Session on all the nodes and view the report.

To deploy the Monitoring Session,

1. **Add components to the canvas**

Drag and drop the following items to the canvas as required:

- **Ingress tunnel** (as a source): From the **New** section.
- **Maps:** From the **Map Library** section.
- **Inclusion and Exclusion maps:** From the Map Library to their respective section at the bottom of the workspace.
- GigaSMART **apps:** From the **Applications** section.
- **Egress tunnels:** From the **Tunnels** section.

2. **Connect components**

Perform the following steps after placing the required items in the canvas.

- a. Hover your mouse on the map
- b. Select the dotted lines
- c. Drag the arrow over to another item (map, application, or tunnel).

You can drag multiple arrows from a single map and connect them to different maps.

3. **(Optional) Review Sources**

Select the **SOURCES** tab to view details about the subnets and monitored instances.

The monitored instances and the subnets are visible in orange.

Not applicable for NSX-T solution and Customer Orchestrated Source as Traffic Acquisition Method.

4. **Deploy the Monitoring Session**

From the **Actions** menu, select **Deploy**.

After successful deployment on all the V Series Nodes, the status appears as **Success** on the **Monitoring Sessions** page.

View the Deployment Report

You can view the Monitoring Session Deployment Report in the **SOURCES** and **V SERIES NODES** tab.

- When you select the **Status** link, the Deployment Report is displayed.
- When the deployment is incorrect, the Status column displays one of the following errors:
 - **Success:** Not deployed on one or more instances due to V Series Node failure.
 - **Failure:** Not deployed on all V Series Nodes or Instances.

The **Monitoring Session Deployment Report** displays the errors that appeared during deployment.

The Monitoring Session Deployment includes two key configuration:

- [Interface Mapping](#)
- [Tool Exclusion](#)

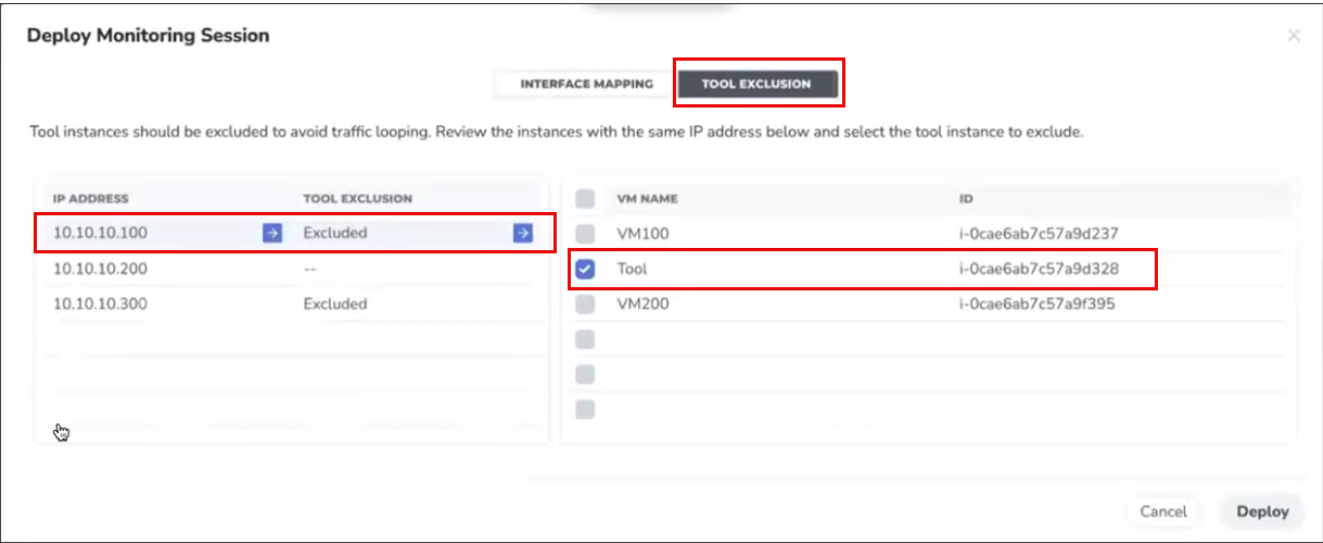
Interface Mapping

It allows to associate specific network interfaces (from monitored instances) with monitoring tools. This ensures that traffic from selected sources is accurately mirrored and routed for analysis. You can:

- Select interfaces from available instances.
- Map each interface to one or more monitoring tools.
- Apply filters or conditions to refine traffic selection.

Tool Exclusion

It excludes specific monitoring tools from receiving mirrored traffic during a monitoring session. This option is available only when the Traffic Acquisition method is set to **VPC Traffic Mirroring**.



- Review the list of available monitoring tools.
- Select the tools to exclude from traffic flow.
- Confirm the exclusion before deploying the session.

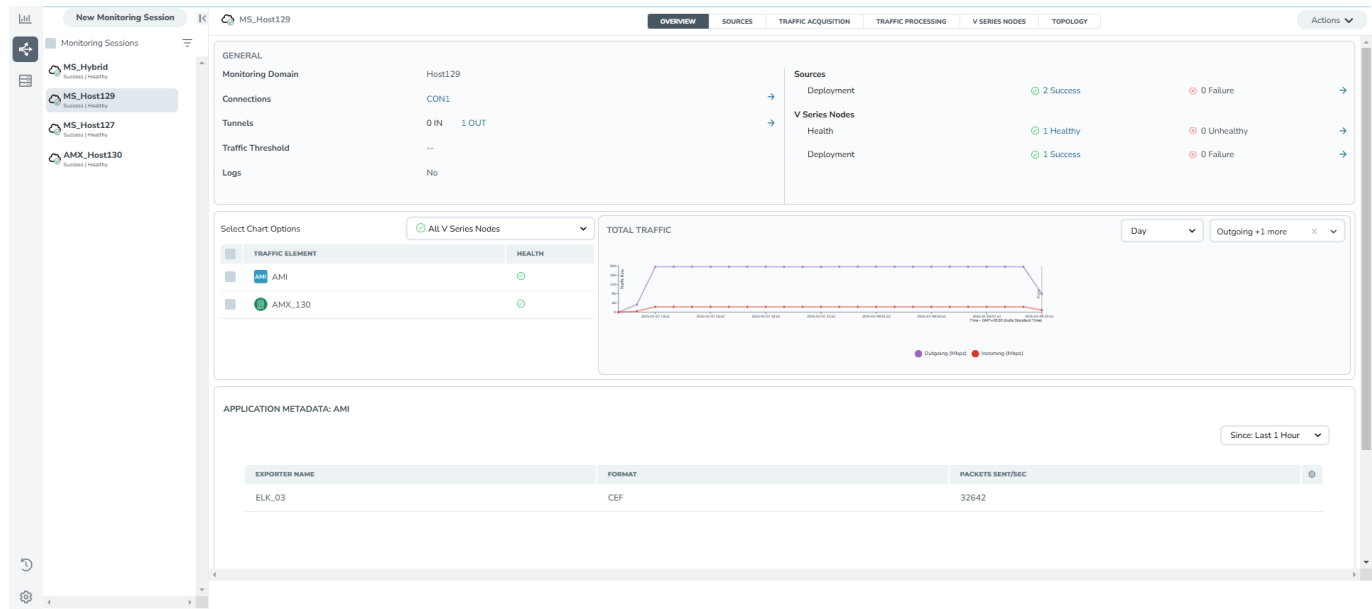
Monitor and Troubleshoot

Delete this text and replace it with your own content.

View Monitoring Session Statistics (Azure)

The Monitoring Session **OVERVIEW** page lets you analyze the incoming and outgoing traffic on an hourly, daily, weekly, and monthly basis.

You can view the high level information of the selected Monitoring Session such as, connections, tunnel details, health status, deployment status, and information related to Application Intelligence statistics. You can view the detailed statistics of an individual traffic processing element in the **TRAFFIC PROCESSING** tab.



You can view the statistics by applying different filters as per the requirements of analyzing the data. GigaVUE-FM allows you to perform the following actions on the Monitoring Session Statistics page:

- You can view the incoming and outgoing traffic on an hourly, daily, weekly, and monthly basis.
- You can filter the traffic and view the statistics based on factors such as **Incoming**, **Outgoing**, **Ratio (Out/In)**, **Incoming Packets**, **Outgoing Packets**, **Ratio (Out/In) Packets**. You can select the options from the drop-down list box in the **TOTAL TRAFFIC** section of the **OVERVIEW** page.
- You can also view the statistics of the Monitoring Session deployed in the individual V Series Nodes. To view the statistics of the individual GigaVUE V Series Node, select the name of the **V Series Node** for which you want to view the statistics from the GigaVUE V Series Node drop-down list on the bottom left corner of the **OVERVIEW** page.

View FQDN resolution details

Use the **FQDN tab** under the **V SERIES NODES tab** to view the FQDNs configured for supported egress tunnel destinations in the monitoring session. This tab displays the configured FQDN, the current resolution status, and the IP address to which the FQDN currently resolves.

- Use this tab to verify that the system resolved the configured FQDN and to identify DNS resolution issues.
- If the system resolves the FQDN successfully, the status shows OK and the Resolve IP field displays the mapped IP address.
- If the system cannot resolve the FQDN, the status shows Failed and the Resolve IP field displays 0.0.0.0.

The screenshot shows the GigaVUE Cloud Suite interface. The top navigation bar includes tabs for OVERVIEW, SOURCES, TRAFFIC PROCESSING, **V SERIES NODES** (highlighted with a red box), and TOPOLOGY. The left sidebar shows a sidebar menu with 'Monitoring Sessions' and 'MS1' (Success | Healthy). The main content area displays a message: 'Following is the list of V Series Nodes where MS1 is deployed.' Below this is a table with the following data:

V SERIES NODE	IP ADDRESS	VPC	HEALTH STATUS	DEPLOYMENT STATUS
Gigamon-VSeriesNode-	54.189.50.107	devtest_FQA-de7c	Healthy	Success

Below the table is a pagination control: 'Go to page: 1 of 1' and '1 v series nodes total'. A modal window titled 'V Series Node: Gigamon-VS...' is open, showing the 'FQDN' tab (highlighted with a red box). The modal contains a table with the following data:

FQDN	STATUS	RESOLVE IP	NOTE
sslqa1.com	Resolved	22.0.3.110	—
sslqa2.com	Resolved	2600:1f14:388a:9c01:b477:c431...	—
sslqa3.com	Resolved	22.0.3.250	—

Visualize the Network Topology (Azure)

You can have multiple connections in GigaVUE-FM. Each connection can have multiple Monitoring Sessions configured within it. The Topology tab provides a visual representation of the monitored elements within a selected connection and Monitoring Session.

To view the topology in GigaVUE-FM:

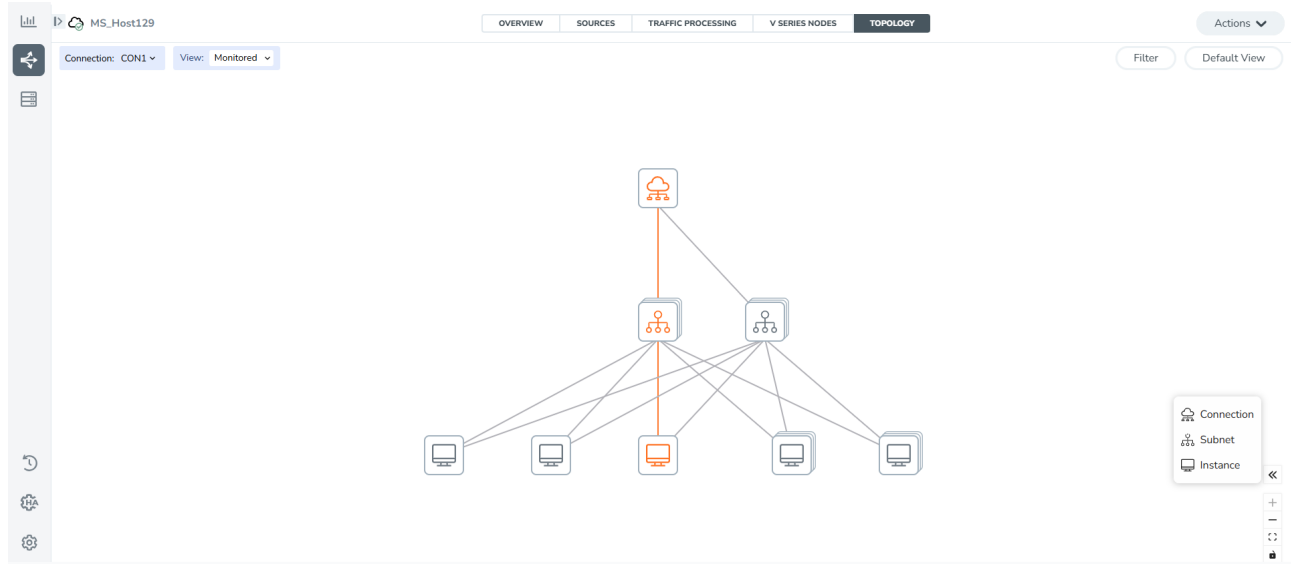
1. Go to **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. The **Monitoring Sessions** landing page appears.
2. Create a Monitoring Session or select an existing Monitoring Session,
3. Open the **TOPOLOGY** tab.

- From the **Connection** list on the Topology page, select a connection.

The topology view of the monitored subnets and instances in the selected session is displayed.

- From **View**, select one of the following instance types:

- Fabric
- Monitored



- (Optional) Hover over the subnet or VM group icons to view details such as the subnet ID, subnet range, and the total number of subnets and instances.
- Select the subnet or VM group icons to explore the subnets or instances within the group.

In the Topology page, you can also perform the following:

- Use the **Filter** button to filter the instances based on the VM name, VM IP, OS Type, Subnet ID, or Subnet IP, and view the topology based on the search results.
- Use the **Default View** button to view the topology diagram based on the source interfaces of the monitored instances.
- Apply Navigation controls, such as:
 - Use the arrows at the bottom-right corner to move the topology page up, down, left, or right.
 - Use **+** or **-** icons to zoom in and zoom out of the topology view.
 - Select the **Fit View** icon to fit the topology diagram according to the width of the page.

AdditionalInfoAppx

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 VUE 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 6.14.02 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, rackmount, 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-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-TA100 Hardware Installation Guide	

GigaVUE Cloud Suite 6.14.02 Hardware and Software Guides
GigaVUE-TA200 Hardware Installation Guide
GigaVUE-TA200E Hardware Installation Guide
GigaVUE-TA400 Hardware Installation Guide
GigaVUE-TA400E 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 Appliances Guide
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
GigaVUE Application Intelligence Solutions Guide
GigaVUE Inline Solutions Guide(NEW) (previously included in the GigaVUE Fabric Management Guide)
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 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 6.14.02 Hardware and Software Guides	
GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration	
Universal Cloud TAP - Container Deployment Guide	
Gigamon Containerized Broker Deployment Guide	
GigaVUE Cloud Suite Deployment Guide - AWS Secret Regions	
GigaVUE Cloud Suite Deployment Guide - Azure 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 GigaVUE 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)
Factory Reset Guidelines for GigaVUE-FM and GigaVUE-OS Devices	Sanitization guidelines for GigaVUE Fabric Management Guide and GigaVUE-OS devices.
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 and 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	<i>(shown on the cover page or in page header)</i>
	Product Version	<i>(shown on the cover page)</i>
	Document Version	<i>(shown on the cover page)</i>
	Chapter Heading	<i>(shown in footer)</i>
	PDF page #	<i>(shown in footer)</i>
How can we improve?	Describe the issue	<i>Describe the error or issue in the documentation. (If it helps, attach an image to show the issue.)</i>
	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 Community 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.