Gigamon®

GigaVUE Cloud Suite for AWS - 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	The original release of this document with 6.14.02 GA. This release incorporates changes in the following topics for the listed features: • Port Optimization o 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 AWS - Deployment Guide **1**
Change Notes 3
Contents 4
GV-Cloud-AWS **14**
Get Started 14
GigaVUE Cloud Suite for AWS 14
Overview of GigaVUE Cloud Suite for AWS 15
Architecture 17
GigaVUE Fabric Components and Deployment Options 19
GigaVUE-FM Orchestrated Fabric Deployment 20
Third Party Orchestrated Fabric Deployment 20
GigaVUE-FM Orchestrated Fabric Deployment 22
Third Party Orchestrated Fabric Deployment 26
Key Concepts 28
Monitoring Domain 29
Monitoring Session 32
Traffic Acquisition 34
Deploying Fabric Components using GigaVUE-FM 35
Deploy Fabric Components using Third Party Orchestration 36
Ingress Tunneled Traffic 37
Precryption Technology on Single Node 42
Precryption Technology on Multi-Node 43
Supported Kernel Version 45
Traffic Processing 49
Traffic Forwarding 52
Egress Tunneled Traffic 53
Elastic Load Balancing 54
Inline V Series (AWS) 57
Secure Tunneling to GigaVUE V Series Nodes 60
Deployment Overview 61
Deployment Planning 62
Identify the Deployment Method 62
Identify the AWS Regions 63
Define GigaVUE-FM Deployment Location 63
Identify the Traffic Acquisition Method 63
Identify the Deployment Model 64

Identify the AWS Accounts Involved ... 66
Identify the Subnets Involved ... 66
Identify the Required IAM Roles, Policies, and Permissions ... 67
Identify or Create the Necessary Keypairs ... 68
Identify the UCT-V Deployment Details ... 68
Identify the UCT-C Deployment Details ... 68
Deployment Prerequisites ... 68
Points to Note for GigaVUE Cloud Suite for AWS ... 69
Subscribe to GigaVUE Products ... 69
Supported Operating Systems for UCT-V ... 70
Network Firewall Requirement ... 71
GigaVUE FM ... 80
UCT-V Controller ... 83
UCT-V ... 84
GigaVUE V Series Node ... 85
Giga VUE V Series Proxy(Optional) ... 87
UCT-C Controller - deployed in Kubernetes worker mode ... 87
UCT-V Controller ... 88
GigaVUE V Series Node ... 88
GigaVUE V Series Proxy(Optional) ... 89
Licensing for GigaVUE Cloud Suite for AWS ... 89
Bundle Replacement Policy ... 92
View active Volume-Based License ... 94
View Inactive Volume-Based License ... 95
Activate Volume-Based Licenses ... 96
AWS Security Credentials ... 97
AWS Key Pair ... 98
AWS Service Regions ... 98
Subnet and Security Group for Amazon VPC ... 99
GigaVUE FM ... 109
UCT-V Controller ... 111
UCT-V ... 112
GigaVUE V Series Node ... 113
Giga VUE V Series Proxy(Optional) ... 115
UCT-C Controller - deployed in Kubernetes worker mode ... 116
UCT-V Controller ... 116
GigaVUE V Series Node ... 117
GigaVUE V Series Proxy(Optional) ... 117
Recommended and Supported Instance Types for AWS ... 117
Configure Tokens ... 119
GigaVUE-FM Version Compatibility ... 121
Default Login Credentials for GigaVUE Fabric Components ... 121
Permissions and Privileges (AWS) ... 122
Prerequisites ... 122

Procedure ... 123
Install GigaVUE-FM on AWS ... 126
Subscribe to GigaVUE-FM ... 126
Initial Configuration ... 127
Upgrade GigaVUE-FM in AWS ... 128
Upgrade GigaVUE-FM ... 129
Upgrade GigaVUE-FM using Snapshot in AWS ... 132
Upgrade GigaVUE Fabric Components in GigaVUE-FM for AWS ... 135
Prerequisite ... 135
Upgrade UCT-V Controller ... 136
Upgrade GigaVUE V Series Nodes and GigaVUE V Series Proxy ... 137
Upgrade GigaVUE Fabric Components using Third Party Orchestration ... 140
Deploy ... 140
Deploy GigaVUE Cloud Suite for AWS using GigaVUE-FM Orchestration ... 141
Acquire Traffic using UCT-V - GigaVUE-FM Orchestration ... 141
Post Deployment Check: ... 151
Prerequisite ... 161
Rules and Notes: ... 168
Upload the UCT-V Images ... 168
Upgrade the UCT-V ... 169
Acquire Traffic using Traffic Mirroring – GigaVUE-FM Orchestration ... 171
Prerequisite ... 176
Acquire Traffic using Traffic Mirroring with Network Load Balancer 181
Prerequisites ... 184
Acquire Traffic using Traffic Mirroring with Gateway Load Balancing ... 188
Prerequisites ... 190
Points to Note: ... 191
Acquire Traffic using Customer Orchestrated Source - GigaVUE-FM Orchestration ... 194
Prerequisite ... 199
Acquire Traffic using Customer Orchestrated Source with Network Load Balancer ... 204
Prerequisites ... 209
Acquire Traffic using Customer Orchestrated Source with Gateway Load Balancing ... 215
Prerequisites ... 217
Points to Note: ... 218
Acquire Traffic using Inline V Series Solution ... 223
Deploy GigaVUE Cloud Suite for AWS using Third Party Orchestration 245
Generic Mode ... 245

Integrated Mode 245
Deployment Options for GigaVUE Cloud Suite for AWS - Generic Mode 245
Create a Custom User 246
Create a Custom Role and Assign the User 247
Create a Custom User Group and Assign the Custom Role and the User 247
Linux UCT-V Installation 248
Linux UCT-V Installation Scenarios 252
Post Deployment Check: 256
Windows UCT-V Installation 257
Rules and Notes: 257
Windows UCT-V Installation Scenarios 260
Recommended Instance Type 263
Configure UCT-V Controller in AWS 264
Register UCT-V Controller during Instance Launch 265
Register UCT-V Controller after Instance Launch 265
Assign Static IP address for UCT-V Controller 266
Configure UCT-V in AWS 267
Configure GigaVUE V Series Nodes and V Series Proxy in AWS 268
Register GigaVUE V Series Node and GigaVUE V Series Proxy during Instance Launch 269
Register GigaVUE V Series Node and GigaVUE V Series Proxy after Instance Launch 269
Assign Static IP address for GigaVUE V Series 270
What to do Next 272
Create a Custom User 273
Create a Custom Role and Assign the User 273
Create a Custom User Group and Assign the Custom Role and the User 274
Recommended Instance Type 274
Configure UCT-V Controller in AWS 276
Register UCT-V Controller during Instance Launch 276
Register UCT-V Controller after Instance Launch 277
Assign Static IP address for UCT-V Controller 277
Configure UCT-V in AWS 278
Configure GigaVUE V Series Nodes and V Series Proxy in AWS 280
Register GigaVUE V Series Node and GigaVUE V Series Proxy during Instance Launch 280
Register GigaVUE V Series Node and GigaVUE V Series Proxy after Instance Launch 281
Assign Static IP address for GigaVUE V Series 282
What to do Next 284

Create a Custom User 284
Create a Custom Role and Assign the User 285
Create a Custom User Group and Assign the Custom Role and the User 285
Linux UCT-V Installation 286
Linux UCT-V Installation Scenarios 290
Post Deployment Check: 294
Windows UCT-V Installation 295
Rules and Notes: 295
Windows UCT-V Installation Scenarios 298
Recommended Instance Type 305
Configure UCT-V Controller in AWS 306
Register UCT-V Controller during Instance Launch 306
Register UCT-V Controller after Instance Launch 307
Assign Static IP address for UCT-V Controller 308
Configure UCT-V in AWS 309
Configure GigaVUE V Series Nodes and V Series Proxy in AWS 310
Register GigaVUE V Series Node and GigaVUE V Series Proxy during Instance Launch 311
Register GigaVUE V Series Node and GigaVUE V Series Proxy after Instance Launch 311
Assign Static IP address for GigaVUE V Series 312
What to do Next 314
Create a Custom User 315
Create a Custom Role and Assign the User 316
Create a Custom User Group and Assign the Custom Role and the User 316
Recommended Instance Type 320
Configure UCT-V Controller in AWS 321
Register UCT-V Controller during Instance Launch 321
Register UCT-V Controller after Instance Launch 322
Assign Static IP address for UCT-V Controller 323
Configure UCT-V in AWS 324
Configure GigaVUE V Series Nodes and V Series Proxy in AWS 325
Register GigaVUE V Series Node and GigaVUE V Series Proxy during Instance Launch 326
Register GigaVUE V Series Node and GigaVUE V Series Proxy after Instance Launch 326
Assign Static IP address for GigaVUE V Series 327
What to do Next 329
Deployment Options for GigaVUE Cloud Suite for AWS - Integrated Mode 329
Create a Custom User 333

Create a Custom Role and Assign the User 334
Create a Custom User Group and Assign the Custom Role and the User 334
Register UCT-V Controller using User Data 337
Register UCT-V Controller using a Configuration File 338
Register GigaVUE V Series Node and GigaVUE V Series Proxy using User Data 341
Register GigaVUE V Series Nodes without GigaVUE V Series Proxy using User Data 341
Register GigaVUE V Series Nodes with GigaVUE V Series Proxy using User Data 342
Register GigaVUE V Series Proxy using User Data 342
Register GigaVUE V Series Node when using GigaVUE V Series Proxy using User Data 342
Register GigaVUE V Series Node and Proxy using a Configuration File 343
Register GigaVUE V Series Nodes without GigaVUE V Series Proxy using a Configuration file 343
Register GigaVUE V Series Nodes with GigaVUE V Series Proxy using a Configuration file 344
Register GigaVUE V Series Proxy using Configuration file: 344
Register GigaVUE V Series Node when using GigaVUE V Series Proxy using Configuration File 344
Linux UCT-V Installation 345
Linux UCT-V Installation Scenarios 349
Post Deployment Check: 353
Windows UCT-V Installation 354
Rules and Notes: 354
Windows UCT-V Installation Scenarios 357
What to do Next 361
Upgrade UCT-V through GigaVUE-FM (Recommended Method) 362
Rules and Notes: 362
Upload the UCT-V Images 362
Upgrade the UCT-V 363
Upgrade UCT-V Manually 364
Create a Custom User 368
Create a Custom Role and Assign the User 368
Create a Custom User Group and Assign the Custom Role and the User 369
Register UCT-V Controller using User Data 372
Register UCT-V Controller using a Configuration File 373
Register GigaVUE V Series Node and GigaVUE V Series Proxy using User Data 376
Register GigaVUE V Series Nodes without GigaVUE V Series Proxy using User Data 377

Register GigaVUE V Series Nodes with GigaVUE V Series Proxy using User Data ... 377
Register GigaVUE V Series Proxy using User Data ... 377
Register GigaVUE V Series Node when using GigaVUE V Series Proxy using User Data ... 378
Register GigaVUE V Series Node and Proxy using a Configuration File 379
Register GigaVUE V Series Nodes without GigaVUE V Series Proxy using a Configuration file ... 379
Register GigaVUE V Series Nodes with GigaVUE V Series Proxy using a Configuration file ... 380
Register GigaVUE V Series Proxy using Configuration file: ... 380
Register GigaVUE V Series Node when using GigaVUE V Series Proxy using Configuration File ... 380
What to do Next ... 382
Create a Custom User ... 384
Create a Custom Role and Assign the User ... 385
Create a Custom User Group and Assign the Custom Role and the User ... 385
Register UCT-V Controller using User Data ... 388
Register UCT-V Controller using a Configuration File ... 389
Register GigaVUE V Series Node and GigaVUE V Series Proxy using User Data ... 392
Register GigaVUE V Series Nodes without GigaVUE V Series Proxy using User Data ... 392
Register GigaVUE V Series Nodes with GigaVUE V Series Proxy using User Data ... 393
Register GigaVUE V Series Proxy using User Data ... 393
Register GigaVUE V Series Node when using GigaVUE V Series Proxy using User Data ... 393
Register GigaVUE V Series Node and Proxy using a Configuration File 394
Register GigaVUE V Series Nodes without GigaVUE V Series Proxy using a Configuration file ... 394
Register GigaVUE V Series Nodes with GigaVUE V Series Proxy using a Configuration file ... 395
Register GigaVUE V Series Proxy using Configuration file: ... 395
Register GigaVUE V Series Node when using GigaVUE V Series Proxy using Configuration File ... 395
What to do Next ... 397
Deploy GigaVUE Cloud Suite for VMware ESXi using Terraform ... 397
License ... 397
Supportability ... 397
Rules and notes ... 398
Prerequisites ... 399
Get Started ... 399

Deployment Using Terraform 400
Install the Gigamon Terraform Provider Without Internet Access 402
Single-file configuration 403
Module-based configuration 405
Run the Terraform Deployment File 406
Best Practices 410
Verification and Troubleshooting 411
Configure 413
Configure UCT-V Features 413
Configure Prefiltering 413
Create Precryption Template for UCT-V 415
Configure Secure Tunnel (AWS) 420
Configure Monitoring Session 428
Create a Monitoring Session (AWS) 429
Enable Prefiltering 432
Enable Precryption 432
Validate Precryption connection 433
Limitations 433
Apply Threshold Template 434
Enable User Defined Applications 434
Enable Distributed De-duplication 435
Tool Exclusion 435
Configure Monitoring Session for Inline V Series 437
What to do Next: 440
Create Ingress and Egress Tunnels (AWS) 440
Create Raw Endpoint (AWS) 449
Create a New Map (AWS) 450
Add Applications to Monitoring Session (AWS) 455
Configure Application Visualization for Virtual Environment 462
Configure Filtering and Metadata Export for Selected Applications in Application Visualization 464
Filter Traffic for Selected Applications 464
Export Metadata for Selected Applications 465
View Application Statistics for Application Visualization 465
Supported Protocols and Attributes 466
Mindata 471
Supported RegExp Syntax 471
Limitations 472
Create Rules for User Defined Application 472
Configure Application Filtering Intelligence for Virtual Environment 474
View Application Statistics for Application Filtering 479
Configure Application Metadata Intelligence for Virtual Environment 480
Extend Your AMI and AMX Deployment 488

View Application Statistics for Application Metadata 489
On-Premises 490
Hardware (AMI) 490
Hardware (Control Plane Metadata) 491
Private Cloud (VMware) 492
Public Cloud 493
Export Application Metadata in JSON format over HTTPS/Kafka 493
Transform NetFlow/IPFIX records to JSON format and export over HTTPS/Kafka 494
Supported Platforms 495
Important Notes 495
Export of 3G/4G/5G Control Plane Metadata by AMX 496
Export GigaVUE Enriched Metadata for Mobile Networks and Export over HTTPS/Kafka 497
Export GigaVUE Enriched Metadata for Cloud Workloads and Export over HTTPS/Kafka 498
Export of GigaVUE Enriched Metadata for Cloud Workloads (Virtual Machines) 498
Export of GigaVUE Enriched Metadata for Cloud Workloads Kubernetes containers - Azure Kubernetes Service (AKS) 499
Switching to outer_ip for Mobility Enrichment 509
Application Monitoring Options 510
Predeployment Checklist: 510
(Optional) Install GigaVUE-FM on AWS 513
Subscribe to GigaVUE-FM 513
Initial Configuration 514
What to do Next: 515
(Optional) Configure Metadata Export Filter for AMX 515
(Optional) Configure Role-Based Access for Third Party Orchestration 515
Create a Custom User 515
Create a Custom Role and Assign the User 516
Create a Custom User Group and Assign the Custom Role and the User 516
Create Monitoring Domain to Acquire Traffic from Customer Orchestrated Source 517
Create Tokens to Secure REST API and Third Party Orchestration Access to GigaVUE-FM 517
Deploy V Series Node and Register with GigaVUE-FM 518
Verify GigaVUE V Series Node Registration 520
Create a Monitoring Session to Configure Application Metadata Exporter 521
Configure Ingestor in AMX to Process Traffic 522
Scenario 1 - Export Application Metadata in JSON format over HTTPS/Kafka 522

Scenario 2 - Export GigaVUE Enriched Metadata for Mobile Networks and Export over HTTPS/Kafka ... 523
Scenario 3 - Export GigaVUE Enriched Metadata for Cloud Workloads and Export over HTTPS/Kafka ... 523
Scenario 4 - Transform NetFlow/IPFIX records to JSON format and export over HTTPS/Kafka ... 524
Scenario 5 - Configure Identity Enrichment Metadata using Zscaler Private Access (ZPA) ... 525
Prerequisites ... 525
Integrate ZPA with Gigamon AMX ... 526
Configure Ingestor for AMX ... 527
Integrate AMX with Third Party Tool ... 528
Set up the Third Party Tool for AMX Integration ... 528
Configure Exporter to Export Attributes to Third Party tools ... 528
Configure Cloud Tool Exporter ... 528
Deploy the Monitoring Session ... 529
Cloud Tool Exporter - Field References ... 529
Configure Kafka Exporter ... 530
Deploy the Monitoring Session ... 530
Kafka Exporter - Field References ... 530
Verify Your Deployment ... 532
Control Plane Attributes ... 536
User Plane Attributes ... 538
AWS ... 542
Azure ... 543
VMware vCenter ... 544
Azure Kubernetes Service (AKS) ... 545
Zscaler Private Access (ZPA) Attributes ... 547
Post Migration Notes for Application Intelligence ... 553
Limitations ... 559
What's Next ... 559
What's Next ... 569
What's Next ... 578
What's Next ... 580
Upload SSL Key Pairs ... 585
Create SSL Service ... 587
Prerequisite ... 587
Key Mapping ... 587
SSL Key Pair Store ... 588
Add SSL Decrypt to Monitoring Session ... 588
Deploy Monitoring Session (AWS) ... 590
Monitor and Troubleshoot ... 593
Monitor Cloud Health ... 593

Configuration Health Monitoring 593
Traffic Health Monitoring 594
Apply Threshold Template to Monitoring Session 598
Apply Threshold Template to Applications 599
Clear Thresholds for Applications 599
Clear Thresholds across the Monitoring Session 599
View Health Status 600
View Monitoring Session Statistics (AWS) 603
Visualize the Network Topology (AWS) 605
Administer GigaVUE Cloud Suite for AWS 606
Manage a Monitoring Domain 607
Check Permissions while Creating a Monitoring Domain 612
Check Permissions while Configuring GigaVUE Fabric Components using GigaVUE-FM 615
Configure AWS Settings 615
Interface Mapping (AWS) 619
Configure Proxy Server 620
Configure Certificate Settings 621
About Events 621
About Audit Logs 623
High Availability for Cloud Infrastructure 625
Analytics for Virtual Resources 646
Virtual Inventory Statistics and Cloud Applications Dashboard 646
Analytics for Inline V Series Solution (AWS) 650
Debuggability and Troubleshooting 653
Sysdumps 653
FAQs - Secure Communication between GigaVUE Fabric Components (AWS) 654

GV-Cloud-AWS

Get Started

GigaVUE Cloud Suite for AWS

This guide describes how to configure GigaVUE Cloud Suite for AWS using the GigaVUE-FM interface. This guide also describes the procedure for setting up the traffic monitoring sessions for AWS using the GigaVUE-FM.

Topics:

- Overview of GigaVUE Cloud Suite for AWS
- Architecture
- GigaVUE Fabric Components and Deployment Options
- Key Concepts
- Deployment Overview
- Deployment Planning
- Deployment Prerequisites
- Install GigaVUE-FM on AWS
- Deploy GigaVUE Cloud Suite for AWS using GigaVUE-FM Orchestration
- Deploy GigaVUE Cloud Suite for AWS using Third Party Orchestration
- Configure UCT-V Features
- Configure Monitoring Session
- Monitor Cloud Health
- Administer GigaVUE Cloud Suite for AWS
- Analytics for Virtual Resources
- Analytics for Inline V Series Solution (AWS)
- Upgrade GigaVUE-FM in AWS
- Upgrade GigaVUE Fabric Components in GigaVUE-FM for AWS
- Upgrade GigaVUE Fabric Components using Third Party Orchestration
- Migrate Application Intelligence Session to Monitoring Session
- Debuggability and Troubleshooting
- FAQs - Secure Communication between GigaVUE Fabric Components (AWS)

Overview of GigaVUE Cloud Suite for AWS

GigaVUE Cloud Suite for AWS delivers a cloud-native visibility and analytics solution for Amazon Web Services (AWS). It enables full network observability so you can:

- Migrate workloads to the cloud
- Optimize your existing cloud environment

The suite removes network blind spots. It reduces security and compliance risks and helps you resolve performance issues quickly.

Traffic Acquisition

GigaVUE Cloud Suite for AWS captures network traffic from workloads running in AWS.

It uses a simple and efficient process:

- Copies and mirrors traffic through tunnels.

- Sends the traffic to GigaVUE V Series Nodes.
- These nodes filter and process the packets.
- The processed traffic goes to your security and monitoring tools.

The suite supports several traffic acquisition methods, including:

- GigaVUE Universal Cloud Tap (UCT)
- AWS Traffic Mirroring

Unified Data Visibility

The suite gives you a single, clear view of all data in motion. It works across single, hybrid, and multi-cloud networks.

GigaVUE Cloud Suite for AWS:

- Collects traffic from any source
- Optimizes it automatically
- Delivers it to any destination

This end-to-end visibility helps your tools analyze raw packet data, application-layer information, and enriched metadata. You can detect threats, improve performance, and make better decisions faster.

Enriched Metadata

GigaVUE Enriched Metadata (GEM) turns raw packet data into actionable insights.

GEM:

- Extracts and enriches metadata
- Sends enriched data to security and analytics tools
- Speeds up threat detection and performance monitoring
- Links platform metadata with real packet data

Key Capabilities

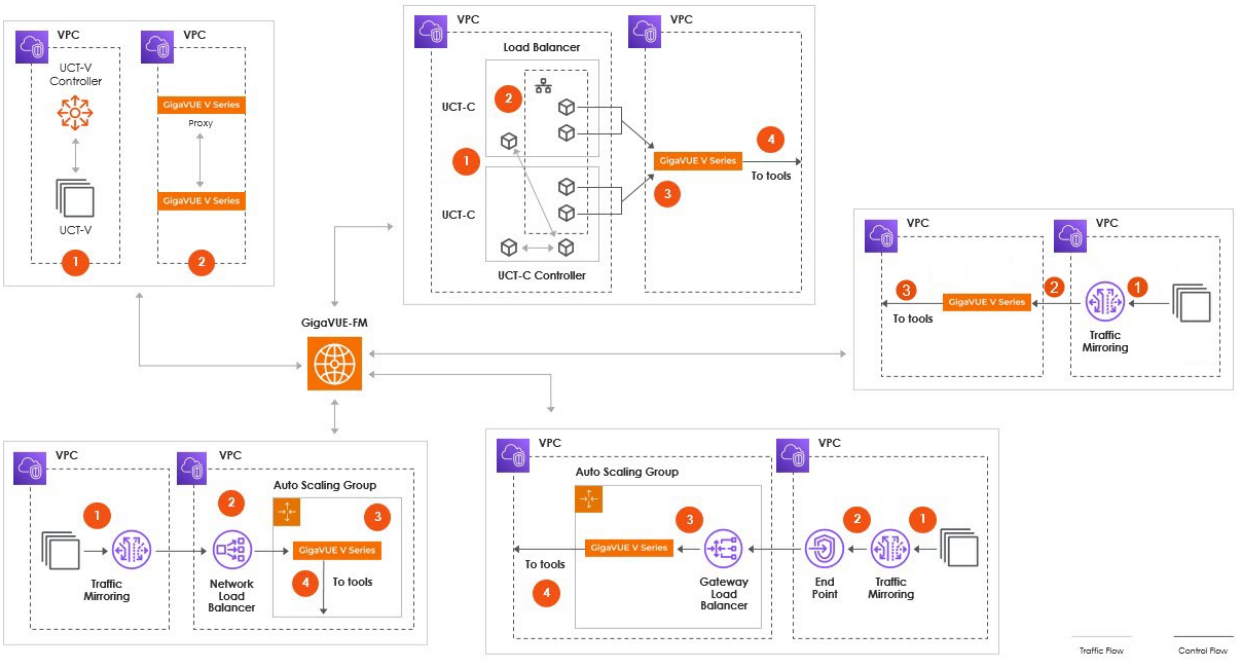
GigaVUE Cloud Suite for AWS offers powerful features, including

- Automatic discovery and deployment of visibility nodes in the platform.
- Application of advanced traffic intelligence to optimize tool performance.
- Support for both public cloud and hybrid cloud architectures.

- Integration with AWS APIs for rapid detection of changes in the workloads.
- Ability to extend on-premises security and monitoring tools to AWS environments.

Architecture

The following diagram provides a high level overview of how GigaVUE Cloud Suite for AWS acquires and processes traffic from workloads running in your AWS accounts and VPCs.



This architecture diagram illustrates different deployment options for acquiring and processing network traffic using GigaVUE fabric components. Each box represents a distinct deployment model, optimized for specific scenarios:

Acquire Traffic from Container Environment

This segment illustrates how you can use GigaVUE V Series Nodes to process traffic from a container environment.

1. UCT-C deployed within the Kubernetes environment captures traffic
2. UCT-C forwards it to the UCT-C Controller for aggregation.
3. The UCT-C Controller then sends the traffic to GigaVUE V Series Nodes for advanced processing, such as filtering or slicing
4. The processed traffic is forwarded to the tools.

GigaVUE-FM manages the entire deployment, handling configuration and orchestration, ensuring scalable and efficient traffic monitoring. Control flows manage configuration between components, while traffic flows indicate data capture and processing, enabling efficient and scalable monitoring container environments.

Regardless of how the traffic is acquired from the workload VMs or pods, GigaVUE V Series Nodes help you to process the traffic and efficiently distribute it to the analysis tools.

Acquire Traffic using UCT-V

This segment shows how UCT-V components can be used for traffic monitoring in virtualized environments.

1. The UCT-V captures traffic from virtual workloads and forwards it to the UCT-V Controller.
2. The UCT-V Controller aggregates the traffic and sends it to GigaVUE V Series Nodes for processing.
3. A GigaVUE V Series Proxy can optionally be used for communicating between the GigaVUE-FM and GigaVUE V Series Nodes.
4. The processed traffic is forwarded to the tools.

GigaVUE-FM manages the entire deployment, handling configuration and orchestration, ensuring scalable and efficient traffic monitoring. Control flows manage configuration between components, while traffic flows indicate data capture and processing, enabling efficient and scalable monitoring container environments.

Acquire Traffic using Traffic Mirroring

The segment explains how the traffic is acquired when your traffic acquisition method is Traffic Mirroring.

1. The traffic from the workload VMs is acquired using Traffic Mirroring.
2. The traffic mirroring forwards the traffic to the GigaVUE V Series Nodes. GigaVUE V Series Nodes are deployed centrally within a VPC or region, handling the processing, filtering, and forwarding of traffic acquired from the workload VMs through tunneling protocols like L2GRE, UDPGRE, or VXLAN.
3. The filtered traffic is then forwarded to monitoring tools for analysis.

With Network Load Balancer

This segment explains how to uniformly distribute the traffic from AWS target VMs to GigaVUE V Series Nodes using a Network Load balancer.

1. The traffic is acquired from the workloads VMs using Traffic Mirroring or Customer Orchestrated Source and is passed to the Network Load balancer.
2. The Network load balancer evenly distributes the filtered traffic across GigaVUE V Series Nodes,
3. The GigaVUE V Series Nodes are deployed in an auto-scaling group to handle variable traffic loads and it processes the traffic.
4. The processed traffic is forwarded to monitoring tools.

GigaVUE-FM centrally manages the entire deployment, ensuring efficient traffic processing, load balancing, and scalability.

With Gateway load Balancer

This segment explains how to uniformly distribute the traffic from AWS target VMs to GigaVUE V Series Nodes using the Gateway Load balancer.

1. The traffic is acquired from the workloads VMs using Traffic Mirroring or Customer Orchestrated Source
2. The traffic is passed via the endpoints to the gateway load balancer.
3. The gateway load balancer evenly distributes the filtered traffic across GigaVUE V Series Nodes, which are deployed in an auto-scaling group to handle variable traffic loads.
4. The GigaVUE V Series Nodes process the traffic and forward it to monitoring tools.

GigaVUE-FM centrally manages the entire deployment, ensuring efficient traffic processing, load balancing, and scalability.

GigaVUE Fabric Components and Deployment Options

You can deploy GigaVUE Fabric Components in your AWS cloud environment and configure to support the visibility policies you have defined.

GigaVUE Cloud Suite for AWS includes the following fabric components:

- GigaVUE-FM
- UCT-V
- UCT-V Controller
- GigaVUE V Series Node
- GigaVUE V Series Proxy

You can use one of the following two different approaches to deploy GigaVUE Fabric Components:

- GigaVUE-FM Orchestrated Fabric Deployment
- Third Party Orchestrated Fabric Deployment

GigaVUE-FM Orchestrated Fabric Deployment

Using the GigaVUE-FM GUI, like

- UCT-V Controllers
- GigaVUE V Series Nodes
- GigaVUE V Series Proxy

You can define Monitoring Domains and then use the UI to deploy the fabric components into your AWS environment. Refer to GigaVUE-FM Orchestrated Fabric Deployment topic for more details about fabric components.

Third Party Orchestrated Fabric Deployment

GigaVUE fabric components support flexible deployment options beyond the standard GigaVUE-FM deployment method. You can use third-party orchestration tools, such as Terraform or custom scripts, to deploy these components, enabling seamless integration with existing infrastructure management workflows.

When deploying fabric components through an external orchestration system,

- You can provide the necessary parameters for self-registration with GigaVUE-FM.
- Once registered, GigaVUE-FM serves as the central point for configuring Monitoring Sessions and associated services
- It ensuring unified management and control of the deployed fabric.

Benefits

- Leverage existing orchestration workflows for automated deployment.
- Ensure seamless integration with infrastructure management tools.
- Maintain centralized monitoring and service configuration through GigaVUE-FM.
- Enhances flexibility while maintaining control over network monitoring infrastructure.

Deployment Methods with Third Party Orchestration

- User Driven Fabric Deployment
- Automated Fabric Deployment

User Driven Fabric Deployment

This method uses a combination of the cloud platform's UI or CLI.

To use user-driven fabric deployment method,

1. Deploy GigaVUE-FM

   Deploy the GigaVUE-FM in to your AWS cloud environment using the AWS Marketplace or AWS EC2 console.
2. Create a Monitoring Domain

   Log in to GigaVUE-FM and create a Monitoring domain to define the boundaries for your fabric components.
3. Deploy the Fabric Components

   Use AWS UI to deploy the following components into a VPC within the Monitoring Domain:
   a. UCT-V Controller: Deploy this if you are using UCT-V to acquire traffic.
   b. GigaVUE V Series Nodes: Deploy these for traffic processing.
   c. GigaVUE V Series Proxy: Deploy this if required for your environment.
4. Monitor Workloads in EKS Clusters (if applicable)

   For monitoring workloads in EKS clusters, launch the UCT-C and UCT-C Controller services using the EKS console or AWS CLI.
5. Configure AWS Load Balancers (if applicable)

   If you are using AWS load balancers, launch these resources from the AWS console with any associated resources, such as an auto-scaling group.

With these steps, you can efficiently deploy and configure the fabric components in your AWS environment.

Automated Fabric Deployment

When using Infrastructure as Code (IaC) methodology, you can automate the deployment of a fabric component using scripts written in tools such as Terraform, Ansible, or CloudFormation.

To use the automated fabric deployment method,

1. Deploy GigaVUE-FM

   Launch GigaVUE-FM in your chosen environment, such as an AWS cloud environment or your private cloud.
2. Deploy Workload VMs with UCT-V
   - Pre-install UCT-V.
   - Use your scripts to install UCT-V after launch.
3. Register UCT-VGigaVUE-FM
   Each UCT-V is configured with the IP address of FM . Once initialized, each UCT-V sends a REST API call to GigaVUE-FM to register itself.

4. Deploy UCT-V Controller and GigaVUE V Series Nodes
   - Launch UCT-V Controller and GigaVUE V Series Nodes as dedicated VMs in your AWS environment.
   - Configure each controller and node with the IP address of GigaVUE-FM and any other relevant information needed to register with FM after initialization.
5. Deploy UCT-C and UCT-C Controllers (if applicable)
   - For monitoring workloads in EKS clusters, deploy UCT-C and UCT-C Controllers in the required clusters.
   - Configure these components so they automatically register with GigaVUE-FM once initialized.

With these steps, you can efficiently deploy and configure the fabric components. Refer to Third Party Orchestrated Fabric Deployment topic for more details about fabric components.

GigaVUE-FM Orchestrated Fabric Deployment

GigaVUE Fabric Components are the set of resources used to acquire, transport, process and distribute traffic to support your monitoring goals.

Using the GigaVUE-FM GUI, like UCT-V Controllers, GigaVUE V Series Nodes, and GigaVUE V Series Proxy, you can define Monitoring Domains and then use the UI to deploy the fabric components into your AWS environment.

GigaVUE Cloud Suite for AWS includes the following fabric components:

- GigaVUE-FM
- UCT-V
- UCT-V Controller
- GigaVUE V Series Node
- GigaVUE V Series Proxy

GigaVUE-FM

GigaVUE-FM gives you unified access, centralized control, and full visibility into all GigaVUE traffic nodes across your enterprise or data center. It offers a global view that individual nodes cannot provide.

Along with management and monitoring, GigaVUE-FM lets you create and manage traffic policies for your visibility fabric. This helps direct network traffic to your monitoring and analytics tools.

You can install GigaVUE-FM on a range of supported platforms. It also works in any supported cloud environment, as long as there is IP connectivity.

You can deploy GigaVUE-FM on-premises as a physical or virtual appliance, or launch it from an Amazon Machine Image (AMI) in the AWS Marketplace.

GigaVUE-FM in AWS

GigaVUE-FM manages the setup of key components in your Amazon Virtual Private Cloud (VPC), including:

- UCT-V Controller (Only if you are using UCT-V as the traffic acquisition method)
- GigaVUE V Series® Node
- GigaVUE V Series® Proxy (Optional)

GigaVUE-FM Orchestration Capabilities

GigaVUE-FM controls the GigaVUE Cloud Suite for AWS.

It helps you:

- Define monitoring areas in your network where workloads run.
- Provide credentials so GigaVUE-FM can discover workloads and related resources.
- Create and deploy visibility policies (Monitoring Sessions) that collect traffic using your chosen method and send it to GigaVUE V Series Nodes.
- Configure V Series Nodes to process and forward traffic to tools based on your policy rules.
- Monitor network areas continuously and automatically apply visibility policies to new workloads if they meet the criteria.
- Gain full visibility into your AWS environment, optimize tool traffic, and keep security consistent across hybrid and multi-cloud setups.

UCT-V

UCT-V (earlier known as G-vTAP Agent) is a module installed in the VM instance. It provides packet-level visibility from inside the workload VMs without informing the cloud provider or requiring any assistance from the cloud provider. You can install UCT-V on both Linux and Windows environments. The installed UCT-V mirrors packets from workload virtual interfaces and sends to GigaVUE V Series nodes for filtering, mapping, and transformation.

How UCT-V Works

- UCT-V mirrors the selected traffic from a source interface to a destination mirror interface.

- The mirrored traffic is encapsulated using GRE or VXLAN tunneling.
- Then, sent to the GigaVUE Cloud Suite® V Series Node.

A UCT-V can consist of multiple source interfaces and a single destination interface. It mirrors network packets collected from the source interface to destination interface. From the destination interface, packets traverse via L2GRE, VXLAN tunnel, or Secure Tunnels to the GigaVUE V Series Node.

Single Network Interface Configuration

You can configure a single network interface card (NIC to act as both the source and the destination. This setup allows you to monitor ingress and egress traffic using the same interface.

Example scenario:

If the VM has only one interface (For example, eth0), UCT-V configuration, can mirror ingress and egress traffic through eth0.

> **NOTE:** Using a single network interface card as the source and the destination interface can introduce higher latency.

Linux Configuration Example for a single NIC configuration:

Grant permission to monitor ingress and egress traffic at iface

```
# eth0 mirror-src-ingress mirror-src-egress mirror-dst
```

Multiple Network Interface Configuration

UCT-V supports using two separate interfaces, one for capturing traffic and other for sending mirrored packets.

Example scenario:

- Use eth0 as the source to monitor traffic
- Use eth1 as the destination to send mirrored packets

So, the mirrored traffic from eth0 is sent to eth1. From eth1, the traffic is sent to the GigaVUE V Series Node.

Linux UCT-V configuration Example for a dual NIC configuration:

Grant permission to monitor ingress and egress traffic at iface

```
# 'eth0' to monitor and 'eth1' to transmit the mirrored packets
# eth0 mirror-src-ingress mirror-src-egress
# eth1 mirror-dst
```

Loopback Network Interface Configuration

> **NOTE:** Windows environment does not support the Loop Back Interface configuration.

UCT-V supports the ability to tap and mirror the loopback interface. You can tap the loopback interfaces on the workload that carries application-level traffic inside the Virtual Machine. The loopback interface is always configured as bidirectional traffic, regardless of the configurations provided in the configuration file.

The UCT-V is offered as a Debian (.deb), Redhat Package Manager (.rpm) package for Linux workloads and a ZIP or MSI for Windows Server workloads. For more information on installing UCT-V on your virtual machines, refer to Configure UCT-V.

UCT-V Controller

UCT-V Controller (earlier known as G-vTAP Controller) manages multiple UCT-Vs and, proxied through GigaVUE-FM, orchestrates the flow of mirrored traffic to GigaVUE V Series Nodes.

GigaVUE-FM uses one or more UCT-V Controllers to communicate with the UCT-Vs. A single UCT-V Controller can only manage UCT-Vs that run the same version. For example, the UCT-V Controller6.14.00 can only manage UCT-Vs 6.14.00.

If you still have the older version of UCT-V deployed in the EC2 instances, you must configure both the previous version and 6.14.00. While configuring the UCT-V Controllers, you can specify the tunnel type used to carry the mirrored traffic from the UCT-Vs to the GigaVUE V Series Nodes.

> **NOTE:** You must enable the basic authentication to launch the GigaVUE fabric components for version 6.9 and lower. For more instructions on the steps to enable the basic authentication, refer to Authentication Type.

Supported UCT-V Instances

This table lists the number of UCT-V's supported for each instance type:

UCT-V Controller	No of UCT-V's
t2.large	>1001
t2.medium	1001
t2.small	480
t2.micro	200

GigaVUE V Series Node

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 on-premise devices or tools. GigaVUE Cloud Suite for AWS uses the TLS- PCAPng, L2GRE, UDPGRE, and VXLAN tunnels to deliver traffic to tool endpoints.

NOTE: You must enable the basic authentication to launch the GigaVUE fabric components for version 6.9 and lower. For more instructions on the steps to enable the basic authentication, refer to Authentication Type.

For more information on installing and configuring GigaVUE V Series Node, refer to Deploy GigaVUE Cloud Suite for AWS using GigaVUE-FM Orchestration.

GigaVUE V Series Proxy

The GigaVUE V Series Proxy is an optional component. GigaVUE-FM uses one or more GigaVUE V Series Proxies to communicate with the GigaVUE V Series Nodes.

You can use a proxy,

- If GigaVUE-FM cannot directly reach the GigaVUE V Series Nodes (management interface) over the network.
- If GigaVUE-FM connects to a large number of nodes.
- If you wish to keep the IP addresses of the nodes private.

You can launch a single GigaVUE V Series Proxy to provide the GigaVUE-FM network communication to hundreds of GigaVUE V Series Nodes present in private networks behind the Proxy.

NOTE: You must enable the basic authentication to launch the GigaVUE fabric components for version 6.9 and lower. For more instructions on the steps to enable the basic authentication, refer to Authentication Type.

For detailed information about configuring and deploying fabric components using different traffic acquisition methods, refer to Deploy GigaVUE Cloud Suite for AWS using GigaVUE-FM Orchestration.

Third Party Orchestrated Fabric Deployment

You can use your orchestration system, instead of GigaVUE-FM to deploy GigaVUE fabric components. The Third Party orchestration feature allows you to register these fabric components, after deployment, with GigaVUE-FM using the information you provide. After registering, you can set up monitoring sessions and other services in GigaVUE-FM.

Components in Third Party Orchestration

The GigaVUE Cloud Suite for Third Party Orchestration consists of the following components:

- GigaVUE-FM
- UCT-Vs
- UCT-V Controllers
- GigaVUE V Series Proxy
- GigaVUE V Series Nodes

GigaVUE-FM is a key component of the GigaVUE Cloud Suite Cloud solution. GigaVUE-FM is a web-based fabric management interface that provides a single-pane-of-glass to manage and view both physical and virtual network traffic.

What You Need to Do

If you prefer to use the Third Party orchestration deployment option, you need to:

- Install and start GigaVUE-FM on a supported cloud or enterprise platform.
- Launch the fabric components in your environment.
- Register the fabric components with GigaVUE-FM.
- Delete the fabric components from the platform when you no longer need them.

Getting the Images of Components

- Download the component images from the Gigamon Customer Portal
- Get public cloud images from the respective marketplace.

> **NOTE:** Contact Gigamon Technical Support team if your platform doesn't support the available Gigamon images.

For information about installing GigaVUE-FM in your enterprise data center, refer to the *GigaVUE-FM Installation and Upgrade Guide*.

Components for Third Party Orchestration

The following table provides a brief description of the components that you can deploy using the Third Party orchestration:

Component	Description
GigaVUE-FM fabric manager (GigaVUE-FM)	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. You are responsible for launching GigaVUE-FM from your end on the supported cloud or enterprise platforms.
UCT-V(earlier known as G-vTAP Agent)	UCT-V is a standalone service installed in your Virtual Machine (VM). This service mirrors the selected traffic from the VMs to the GigaVUE® V Series node. The UCT-V is offered as a Debian (.deb), Red Hat Package Manager (.rpm), or Windows package. For details, refer to Install UCT-Vs.
Next generation UCT-V(earlier known as Next Generation G-vTAP Agent)	**Next generation UCT-V** is a lightweight solution that: • Acquires traffic from VMs and improves UCT-V mirroring capability with a lightweight solution. • Reduces the traffic flow from the UCT-V to the V Series node with tap-level prefiltering, lowering the V Series load. • Activates UCT-V on Linux systems with a Kernel version above 5.4. • Allows you to prefilter traffic at UCT-Vs before sending it to V Series nodes. • Allows you to create a prefiltering policy template to apply on a monitoring session.
UCT-V Controller (earlier known as G-vTAP Controller)	• Manages multiple UCT-Vs and orchestrates the mirrored traffic flow to GigaVUE V Series nodes. • GigaVUE-FM uses one or more UCT-V Controllers to communicate with the UCT-Vs.
GigaVUE® V Series Proxy (optional)	• Manages multiple V Series nodes and orchestrates the traffic flow from GigaVUE V Series nodes to the monitoring tools. • GigaVUE-FM uses one or more GigaVUE V Series Proxies to communicate with the GigaVUE V Series nodes.
GigaVUE® V Series Node	GigaVUE® V Series Node is a visibility node that: • Aggregates mirrored traffic from multiple UCT-Vs. • Applies filters and manipulates the packets using GigaSMART applications. • Distributes the optimized traffic to cloud-based tools or backhauls it to GigaVUE Cloud Suite Cloud using GRE or VXLAN tunnels, when the platform supports.

For detailed information about configuring and deploying fabric components using different traffic acquisition methods, refer to Deploy GigaVUE Cloud Suite for AWS using Third Party Orchestration.

Key Concepts

This section provides the key concepts required to understand GigaVUE Cloud Suite for AWS.

For details, refer to the following section:

- Monitoring Domain
- Monitoring Session
- Traffic Acquisition
- Traffic Processing
- Traffic Forwarding
- Egress Tunneled Traffic
- Elastic Load Balancing
- Inline V Series (AWS)
- Secure Tunneling to GigaVUE V Series Nodes

Monitoring Domain

Your AWS cloud infrastructure may encompass numerous resources spread across multiple AWS accounts and Virtual Private Clouds (VPCs). When implementing GigaVUE Cloud Suite for AWS to monitor specific workloads, it's crucial to limit access to only the necessary parts of your cloud environment.

To clearly define the scope of deployment, GigaVUE Cloud Suite for AWS follows the concept of Monitoring Domain. This domain establishes a boundary within your AWS cloud environment where you implement the visibility solution.

Monitoring Domain

You can create a Monitoring Domain in AWS using:

- AWS accounts
- Regions
- VPCs

GigaVUE Cloud Suite for AWS interacts only with resources within the specified accounts and VPCs listed in a Monitoring Domain.

Connection

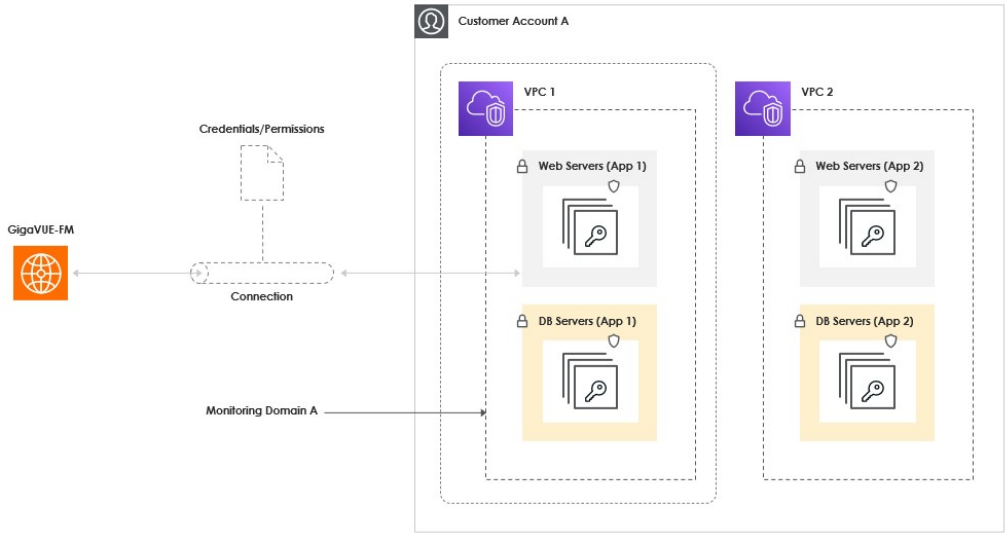
To control access better, GigaVUE Cloud Suite for AWS uses a Connection.

A connection,

- Includes a set of credentials and permissions that precisely limit what GigaVUE Cloud Suite for AWS can access.
- Helps you deploy GigaVUE Cloud Suite for AWS to the appropriate resources with minimal credentials and permissions, enhancing security and control.

Monitoring Domains and Connections work together to provide secure, targeted monitoring. You define what GigaVUE Cloud Suite for AWS can see and do.

The following diagram provides more details about the concepts of Monitoring Domain and Connection:



© 2017-2025 Gigamon Inc. All rights reserved.

In the above diagram:

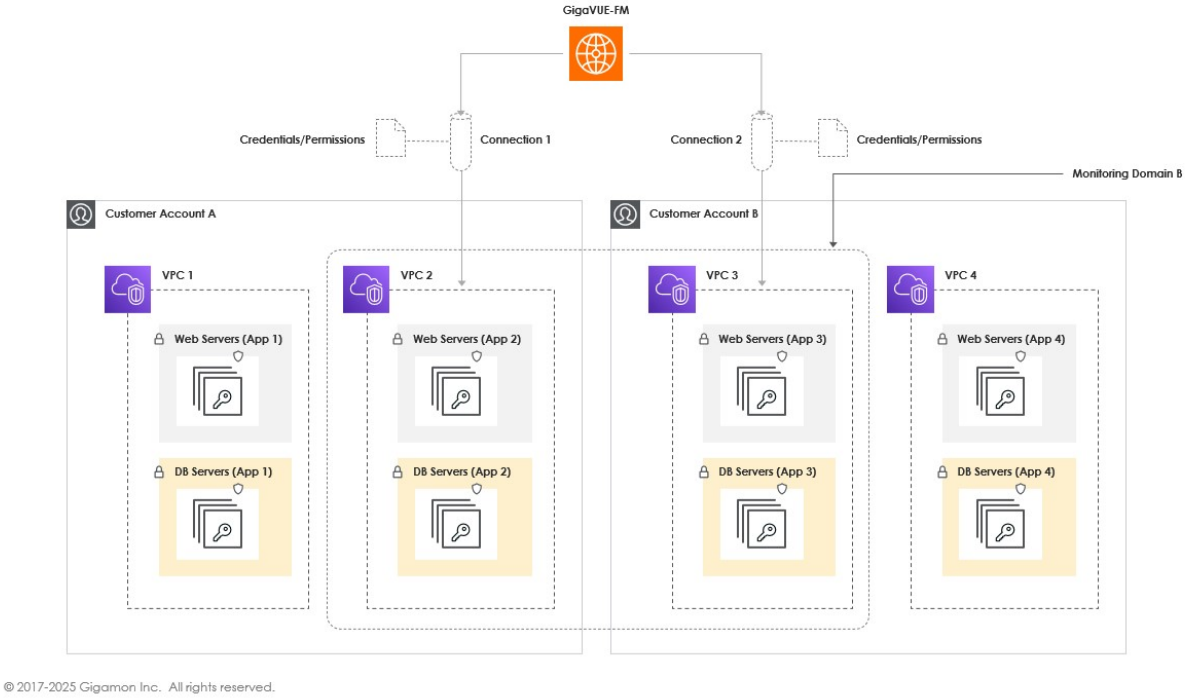
- You create Monitoring Domain A for VPC 1 in Account A
- You assign a Connection that grants access to only VPC 1
- GigaVUE-FM uses this connection to find and monitor resources like:
    - Workload VMs
    - Subnets
    - Security groups
    - Key pairs

It then deploys GigaVUE components to collect and process traffic. The data is forwarded to your monitoring tools. GigaVUE-FM operates only within VPC 1, following the rules of the Monitoring Domain and its associated connection.

The Monitoring Domain defines a clear boundary within which GigaVUE-FM operates. This ensures both security and performance goals are achieved. In this case, you do not want GigaVUE-FM to access any VPCs other than VPC 1,GigaVUE-FM complies with your intent. It restricts its operations strictly to the boundary defined by the Monitoring Domain. Additionally, the credentials and permissions you provide through the connection associated with the Monitoring Domain further restrict the actions of GigaVUE-FM.

The Monitoring Domain is a logical concept. Its definition is based on concepts defined by the underlying cloud platform. On AWS, you can define any boundary using accounts and VPCs.

The following diagram illustrates a Monitoring Domain encompassing resources in VPCs in two different AWS accounts:



© 2017-2025 Gigamon Inc. All rights reserved.

In this diagram:

- Monitoring Domain B includes VPC 2 in Account A and VPC 3 in Account B
- You assign Connection 1 to access VPC 2 and Connection 2 to access VPC 3

GigaVUE-FM accesses only VPC 2 and VPC 3. It does not see or touch VPC 1 or VPC 4. The domain and connections define strict access limits.

Monitoring Session

GigaVUE Cloud Suite for AWS offers a sophisticated approach to network visibility through customizable Monitoring Sessions. These sessions allow you to tailor your visibility strategy with precision, focusing on specific aspects of your AWS environment:

Workload Selection

You can select target workloads to define the scope of your monitoring:

- Select VMs or pods based on various criteria
- Utilize filters such as VPC name, subnet, IP address, VM tags, or pod labels
- Align selections with your predefined Monitoring Domain boundaries

Traffic Acquisition

You can specify the types of traffic to capture from selected sources:

- Options vary depending on the chosen acquisition technology
- Customize traffic selection to match your monitoring requirements

Traffic Processing

You can leverage a comprehensive suite of traffic processing features:

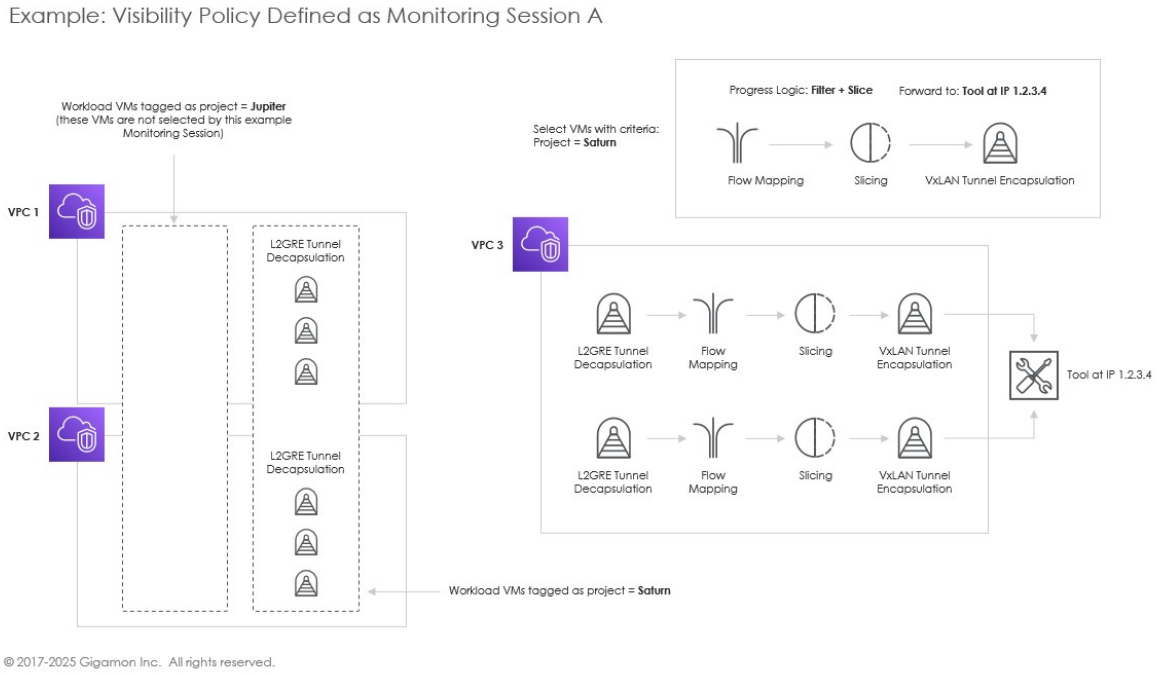
- Apply various GigaSMART Applications to refine and optimize captured traffic.
- Enhance security and efficiency of your monitoring solutions
- Tailor the data sent to analysis tools for maximum relevance

Configuring these elements within a Monitoring Session allows you to create a finely-tuned visibility policy that aligns perfectly with your specific monitoring objectives in AWS environments.

After you define a Monitoring Session, GigaVUE-FM

- Automatically configures the required traffic acquisition points
- Processes the traffic.
- Sends the captured traffic to GigaVUE V Series Nodes.
- Forwards the process data to to your analysis tools.

The following diagram provides a high-level overview of an example Monitoring Session:



The above diagram display an example to monitor VMs tagged with project = "Saturn". For this, you

- Define a Monitoring Session with this tag filter
- Choose UCT-V to acquire traffic
- Apply packet slicing in the V Series Nodes
- Forward traffic to your analysis tool at IP 1.2.3.4

When deployed, GigaVUE-FM:

- Discovers all matching VMs in your Monitoring Domain
- Configures UCT-V on these VMs
- Starts forwarding sliced packets to your tool

If new Saturn-tagged VMs are launched, GigaVUE-FM detects them automatically. It applies the same monitoring policy without manual action.

Benefits

- Focus monitoring on only the workloads you need
- Control how traffic is captured and processed

- Automatically update monitoring as your environment changes

For more information, see Configure Monitoring Session.

Traffic Acquisition

You can acquire traffic from multiple virtual machines and container pod instances using one of the following options:

- UCT-V
- UCT-C(for containers)
- AWS infrastructure sources such as Traffic Mirroring.

The acquired traffic is forwarded to the GigaVUE V Series Node to conduct core intelligence and additional GigaSMART processing.

For details, refer to the following topics:

- Deploying Fabric Components using GigaVUE-FM
- Container Based Workloads
- Packet Mirroring
- Precryption Technology on Single Node
- Secure Communication between GigaVUE Fabric Components

Virtual Machine Based Workloads

You can acquire traffic for Virtual Machines using the following ways:

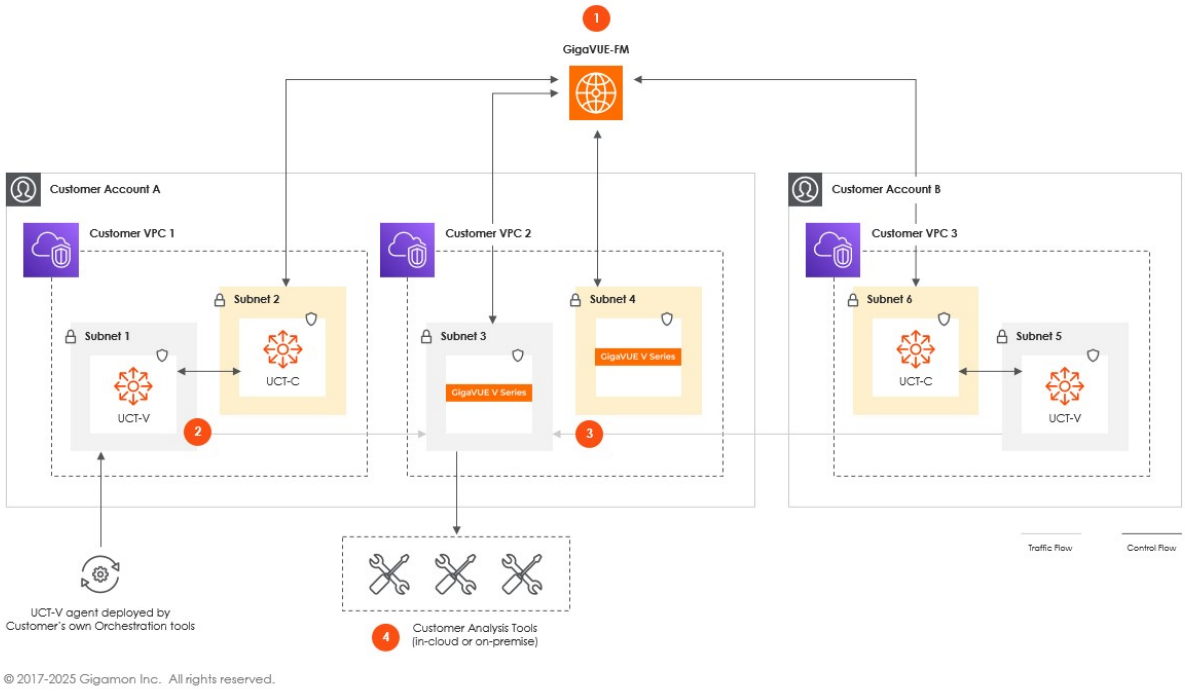
- Traffic Acquisition Method using UCT-V
- Traffic Acquisition Method using Traffic Mirroring
- Traffic Acquisition Method using Customer Orchestrated Source

Traffic Acquisition Method using UCT-V

You can

- Deploy UCT-V in various compute instances to mirror production traffic.
- Send to GigaVUE V Series Nodes for further processing and distribution to monitoring and observability tools.

Deploying Fabric Components using GigaVUE-FM

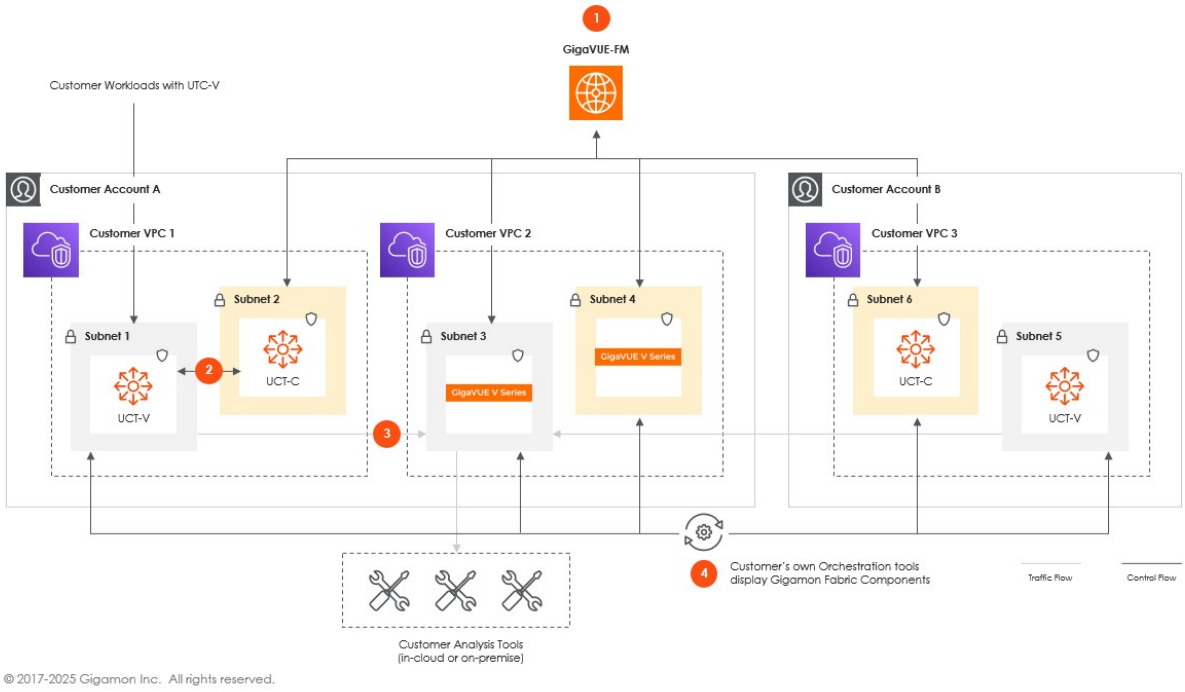


This diagram illustrates the deployment of fabric components across multiple AWS accounts, enabling traffic acquisition, processing, and forwarding to your analysis tools. GigaVUE-FM establishes control flows across accounts and VPCs, ensuring seamless integration and centralized management.

GigaVUE-FM communicaties with deployed components, including UCT-Vs, UCT-V Controllers, GigaVUE V Series Nodes, and Proxies to orchestrate traffic acquisition and processing

UCT-V Controller orchestrates the communication between installed workload VMs, captures the traffic, and forwards the traffic to GigaVUE V Series Nodes. GigaVUE V Series processes this traffic before forwards to analysis tools in the cloud or on-premises.

Deploy Fabric Components using Third Party Orchestration



Traffic Acquisition Method using Traffic Mirroring

With VPC Traffic Mirroring, the mirrored traffic from your workloads is directed directly to the GigaVUE V Series Nodes, and you need not configure the UCT-Vs and UCT-V Controller.

VPC Peering is required to send mirrored traffic from other VPCs into a centralized GigaVUE V Series deployment.

- UCT-V Controller configuration is not applicable to VPC Traffic Mirroring.
- Traffic Mirroring does not support cross-account solutions without a load balancer.
- VPC Traffic Mirroring option requires additional permissions. For details, refer to Permissions and Privileges (AWS).
- After deploying the Monitoring Session, a traffic mirror session is created in your AWS VPC consisting of a session, a filter, sources, and targets. For more details, refer to Traffic Mirroring in AWS Documentation.

For details on how to use Application Filtering Intelligence and Slicing with Traffic Mirroring, see AWS Traffic Mirroring with Application Filter Intelligence and Slicing (6.3).

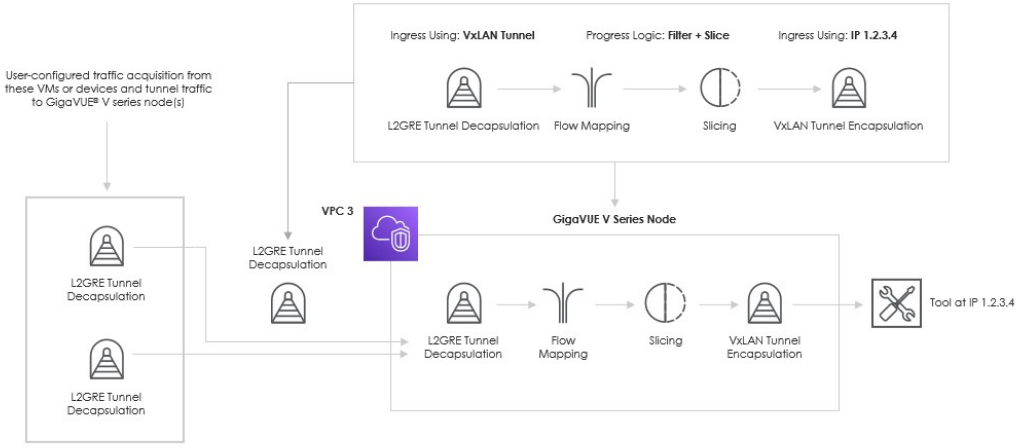
Traffic Acquisition Method using Customer Orchestrated Source

Customer Orchestrated Source is a traffic acquisition method that allows you to tunnel traffic directly to the GigaVUE V Series Nodes. In cases where you cannot configure UCT-V or Traffic Mirroring due to firewall or other restrictions, you can still leverage GigaVUE Cloud Suite features to efficiently process and distribute acquired traffic to the tools.

When using Customer Orchestrated Source, you can directly configure tunnels or raw endpoints in the monitoring session. You can use other applications, such as, Slicing, Masking, Application Metadata, and Application Filtering to process the tunneled traffic. For details on how to configure Tunnels and Raw End Points in the Monitoring Session, refer to Create Ingress and Egress Tunnels (AWS) and Create Raw Endpoint (AWS).

The following diagram provides more details on how customer orchestrated source works:

Example: Monitoring Session for User-Configured Sources



© 2017-2025 Gigamon Inc. All rights reserved.

Ingress Tunneled Traffic

With user configured traffic acquisition, several tunnel types are available for user to ingress traffic into V Series nodes for processing: VXLAN, L2GRE or ERSPAN. User chooses the type and detailed configuration of ingress tunnel endpoint that works best in their environment.

Select **Customer Orchestrated Source** as the tapping method. You can use the Customer Orchestrated Source as a source option in the monitoring session, where the traffic is directly tunneled to the GigaVUE V Series nodes without deploying UCT-Vs and UCT-V Controller. You must create this tunnel feed and point it to the GigaVUE V Series Node(s).

You can configure an Ingress tunnel in the Monitoring Session with the GigaVUE V Series Node IP address as the destination IP address. Then, the traffic is directly tunneled to that GigaVUE V Series Node.

For details on how to select **Traffic Acquisition Method** as **Customer Orchestrated Source**, refer to Acquire Traffic using Customer Orchestrated Source - GigaVUE-FM Orchestration.

Container Based Workloads

You can use GigaVUE V Series Nodes to process traffic from a container environment. For container-based workloads, UCT-C deployed within the Kubernetes environment captures traffic. Then, it forwards to the GigaVUE V Series Nodes deployed in VMs.

The V Series Nodes apply advanced processing, such as filtering or slicing, before forwarding it to analysis tools. For instructions on UCT-C deployment, refer to Universal Cloud TAP - Container Deployment Guide.

Packet Mirroring

Packet Mirroring is one of the fundamental ways to acquire traffic from the workloads (VMs or pods) for monitoring. It clones network packets directly from network interfaces of selected workloads and sends them to a destination for processing and analysis.

You can,

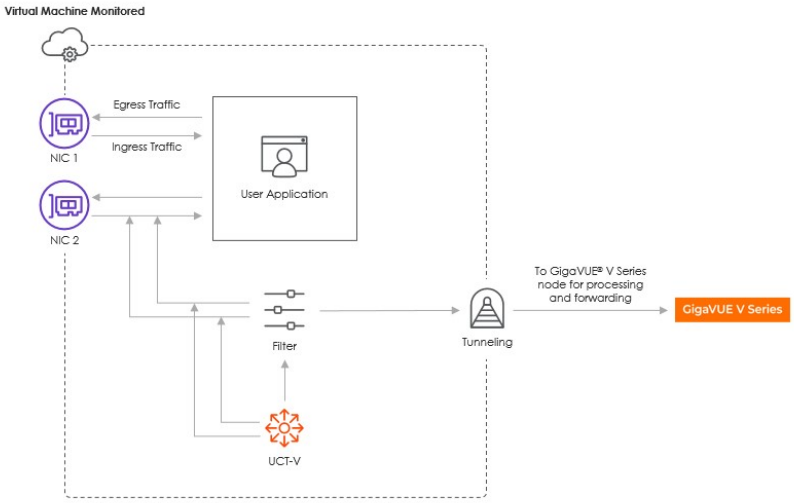
- Mirror Packets from some or all the network interfaces of the workloads.
- Configure to mirror packets only for ingress or egress traffic or both.

GigaVUE Cloud Suite for AWS supports packet mirroring through:

- UCT-V-based packet mirroring
- Cloud platform native packet mirroring capabilities such as Traffic Mirroring

How Packet Mirroring Works

The following diagram illustrates how packet mirroring works using UCT-V.



© 2017-2025 Gigamon Inc. All rights reserved.

To acquire traffic from a Virtual Machine using UCT-V, install UCT-V into the VMs you want to monitor. After creating and deploying a Monitoring Session in a Monitoring Domain using UCT-V as traffic acquisition method, GigaVUE-FM sends proper configuration details to all UCT-Vs instances. You can filter the Mirrored packets according to the defined criteria and tunneled out to GigaVUE V Series Nodes for processing and forwarding.

Prefilter Mirrored Traffic

> **NOTE:** UCT-V supports Prefiltering on Windows systems and Linux systems running Kernel version 4.18 or later.

Using a filtering criteria in the Monitoring Session, you can filter the mirrored traffic from the packet mirroring before tunneling it to the GigaVUE V Series Nodes. This helps reduce the volume of mirrored traffic sent to the analysis tool. UCT-V supports a range of criteria to acquire and forward the traffic most relevant to your monitoring needs:

- Layer 3 filters: IPv4 source IP, IPv4 destination IP, IPv6 source IP, IPv6 destination IP and protocol
- Layer 4 filters: source port, destination port

For details, refer to Configure Prefiltering.

Precryption

License: Precryption requires a **SecureVUE Plus** license.

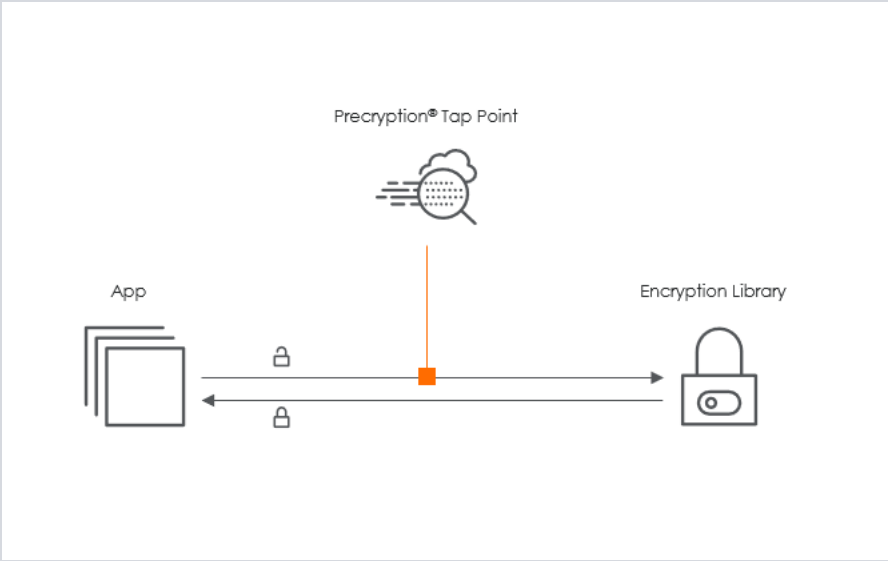
Gigamon Precryption™ technology[1] provides you clear-text visibility into encrypted network traffic without the need for traditional decryption. It works across virtual, cloud, and container environments, helping you get the full security stack without added complexity

In this section:

- How Gigamon Precryption Technology Works
- Why Gigamon Precryption
- Key Features
- Key Benefits
- Precryption Technology on Single Node
- Precryption Technology on Multi-Node
- Supported Platforms
- Prerequisites

How Gigamon Precryption Technology Works

Precryption technology leverages built-in Linux functionality to copy communications between the application and the encryption library, such as OpenSSL.



Key Highlights

[1]**Disclaimer**: The Precryption feature allows you to capture decrypted traffic from both virtual machine (VM) and container-based environments. After capturing the traffic using (via UCT-C or UCT-V), you can send to the V Series product for further processing. You can choose to secure this traffic using encrypted tunnels between the capture point and the V Series. This option helps protect sensitive data during transit. If you don't enable encrypted tunnels, the captured (decrypted) traffic remains in plain text while moving between the source and the V Series—introducing potential exposure risks. Please note that the feature behavior and security options may change over time. Stay informed about updates to ensure you use the latest protections. By using this feature, you acknowledge and accept the current limitations and potential risks associated with the transmission of decrypted traffic.

- Captures network traffic in plain text, either before the system encrypts it or after it decrypts it.
- Does not change how encryption or transmission works.
- Avoids proxies, retransmissions, and “break-and-inspect” steps. Instead, it sends the plaintext copy to the Gigamon Deep Observability Pipeline, where tools can optimize, transform, and forward the traffic as needed.
- Runs on GigaVUE® Universal Cloud Tap (UCT) and supports hybrid and multi-cloud environments, including on-prem and virtual platforms.
- Runs independently of your applications, so you don’t need to change your development lifecycle.

Why Gigamon Precryption

GigaVUE Universal Cloud Tap with Precryption technology is a lightweight, friction-free solution that eliminates blind spots present in modern hybrid cloud infrastructure.

Precryption helps you:

- Improve visibility for East-West traffic into virtual, cloud, and container platforms
- Delivers unobscured visibility into all encryption types, including TLS 1.3, without managing and maintaining decryption keys.
- Manages compliance with IT organizations, keeps communications private, architects a Zero Trust foundation, and boosts security-tool effectiveness by a factor of 5x or more.

Key Features

The following are the key features of this technology:

- Plain text visibility into communications with modern encryption (TLS 1.3, mTLS, and TLS 1.2 with Perfect Forward Secrecy).
- Plain text visibility into communications with legacy encryption (TLS 1.2 and earlier).
- Non-intrusive traffic access without agents running inside container workloads.
- Elimination of expensive resource consumption associated with traditional traffic decryption.
- Elimination of key management required by traditional traffic decryption.
- Zero performance impact based on cipher type, strength, or version.
- Support across hybrid and multi-cloud environments, including on-prem, virtual, and container platforms.
- Keep private communications private across the network with plaintext threat activity delivered to security tools.
- Integration with Gigamon Deep Observability Pipeline for the full suite of optimization, transformation, and brokering capabilities.

Key Benefits

The following are the key benefits of this technology:

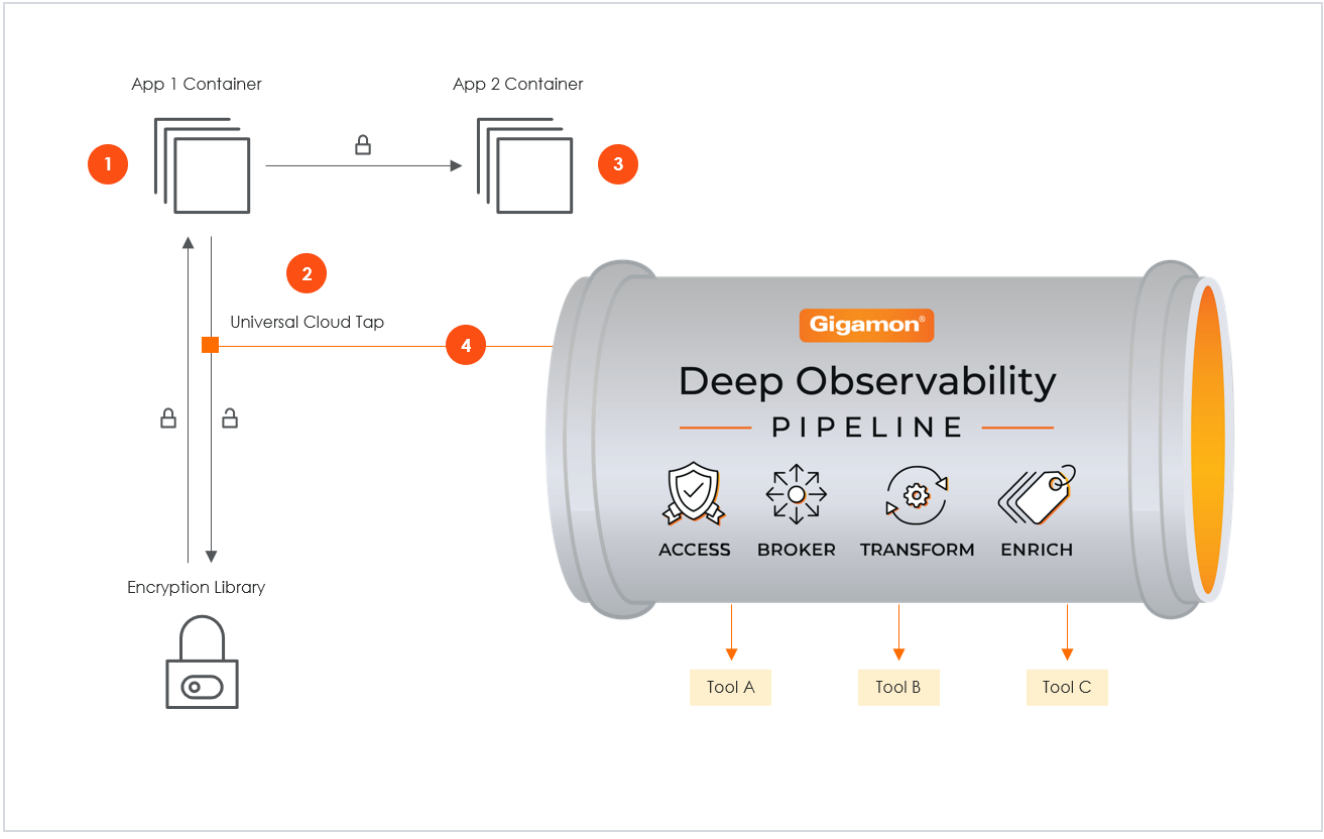
- Eliminates blind spots for encrypted East-West (lateral) and North-South communications, including traffic that may not cross firewalls.
- Monitors application communications with an independent approach that enhances development team velocity.
- Extends security tools' visibility to all communications, regardless of encryption type.
- Achieves maximum traffic tapping efficiency across virtual environments.
- Leverages a 5–7x performance boost for security tools by consuming unencrypted data.
- Supports a Zero Trust architecture founded on deep observability.
- Maintains privacy and compliance adherence associated with decrypted traffic management.

How Gigamon Precryption Technology Works

This section explains how Precryption technology works on single nodes and multiple nodes in the following sections:

- Precryption Technology on Single Node
- Precryption Technology on Multi-Node

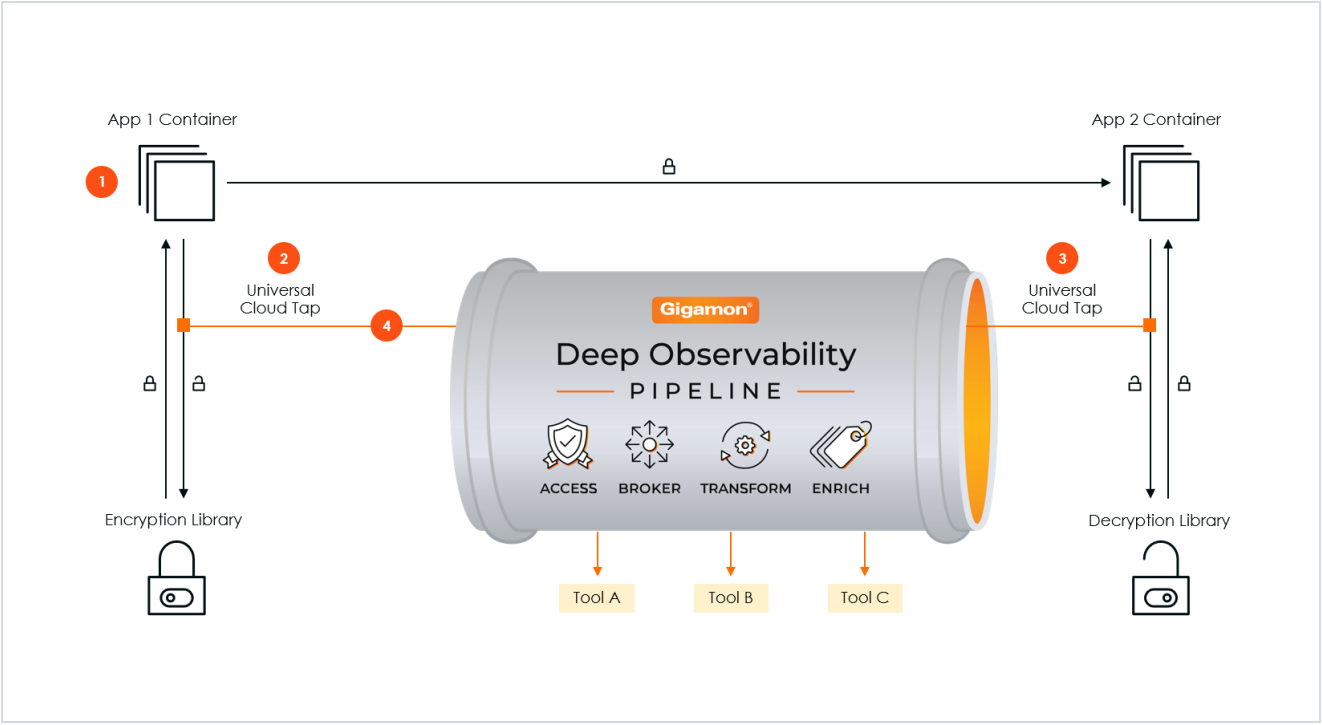
Precryption Technology on Single Node



1. An application uses an encryption library, such as OpenSSL, to encrypt a message.

2. GigaVUE Universal Cloud Tap (UCT), enabled with Precryption technology, gets a copy of this message before it is encrypted on the network.
3. The encrypted message is sent to the receiving application with unmodified encryption—no proxy, no re-encryption, no retransmissions.
4. GigaVUE UCT creates packet headers as needed, encapsulates them in a tunnel, and forwards them to GigaVUE V Series in the deep observability pipeline.
5. Gigamon optimizes, transforms, and delivers data to tools without further decryption.

Precryption Technology on Multi-Node



1. An application uses an encryption library, such as OpenSSL, to encrypt a message.
2. GigaVUE Universal Cloud Tap (UCT), enabled with Precryption technology, gets a copy of this message before it is encrypted on the network
3. Optionally, GigaVUE UCT enabled with Precryption can also acquire a copy of the message from the server end after the decryption.
4. GigaVUE UCT creates packet headers as needed, encapsulates them in a tunnel, and forwards them to GigaVUE V Series in the deep observability pipeline.
5. Gigamon optimizes, transforms, and delivers data to tools without further decryption.

Supported Platforms

VM environments: Precryption™ is supported on the following VM platforms that support UCT-V:

Platform Type	Platform
Public Cloud	• AWS • Azure • GCP (via Third Party Orchestration)
Private Cloud	• OpenStack • VMware ESXi (via Third Party Orchestration only) • VMware NSX-T (via Third Party Orchestration only) • Nutanix (via Third Party Orchestration only)

Container environments: Precryption™ is supported on the following container platforms that support UCT-C:

Platform Type	Platform
Public Cloud	• EKS • AKS • GKE
Private Cloud	• OpenShift • Native Kubernetes (VMware)

Prerequisites

Points to Note

- OpenSSL version 1.0.2, version 1.1.0, version 1.1.1, and version 3.x.
- For UCT-C, worker pods should always have libssl installed to ensure that UCT-C Tap can tap the Precryption packets from the worker pods whenever libssl calls are made from the worker pods.
- For GigaVUE-FM, add port 5671 in the security group to capture the statistics.
- In security group settings on the UCT-V Controller, enable Port 9900 to receive the statistics information from UCT-V.
- For UCT-C, add port 42042 and port 5671 to the security group.
- Precryption works only on Linux systems running Kernel version 4.18 or later.

License Prerequisite

- Precryption™ requires a SecureVUE Plus license.

Supported Kernel Version

Precryption is supported on kernel versions 4.18 and above, including 5.4+ kernels, across all Linux and Ubuntu operating systems. For the Kernel versions below 5.4, refer to the following table:

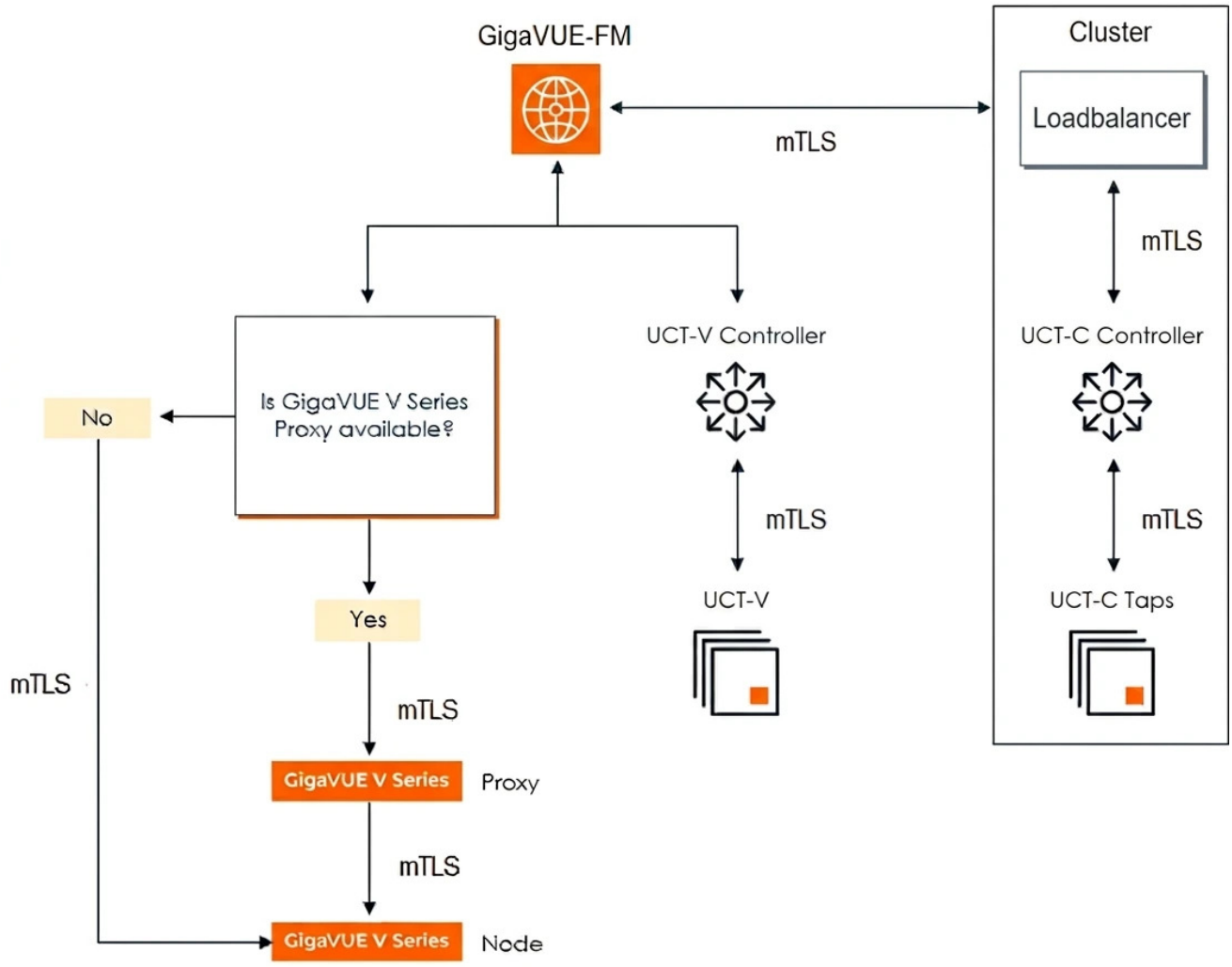
Kernel-Version	Operating System
4.18.0-193.el8.x86_64	RHEL release 8.2 (Ootpa)
4.18.0-240.el8.x86_64	RHEL release 8.3 (Ootpa)
4.18.0-305.76.1.el8_4.x86_64	RHEL release 8.4 (Ootpa)
4.18.0-348.12.2.el8_5.x86_64	RHEL release 8.5 (Ootpa)
4.18.0-372.9.1.el8.x86_64	RHEL release 8.6 (Ootpa)
4.18.0-423.el8.x86_64	RHEL release 8.7 Beta (Ootpa)
4.18.0-477.15.1.el8_8.x86_64	RHEL release 8.8 (Ootpa)
5.3.0-1024-kvm	Ubuntu 19.10
4.18.0-305.3.1	Rocky Linux 8.4
4.18.0-348	Rocky Linux 8.5
4.18.0-372.9.1	Rocky Linux 8.6
4.18.0-425.10.1	Rocky Linux 8.7
4.18.0-477.10.1	Rocky Linux 8.8
4.18.0-80.el8.x86_64	CentOS 8.2
4.18.0-240.1.1.el8_3.x86_64	CentOS 8.3
4.18.0-305.3.1.el8_4.x86_64	CentOS 8.4
4.18.0-408.el8.x86_64	CentOS 8.5

For more details, refer to Gigamon TV.

Secure Communication between GigaVUE Fabric Components

The Secure Communication feature in GigaVUE-VM uses mutual TLS (mTLS) authentication to improve network security. It ensures all GigaVUE Fabric Components communicate over encrypted, verified connections using certificates issued by a Certificate Authority (CA), without relying on static credentials.

How it Works!



In this setup:

- GigaVUE-FM establishes an mTLS connection and checks for GigaVUE V Series Proxy availability.
- If GigaVUE V Series Proxy is unavailable, it directly connects to the GigaVUE V Series Node through mTLS.
- If a GigaVUE V Series is available, GigaVUE-FM first connects to the GigaVUE V Series Proxy and establishes an mTLS connection with the GigaVUE V Series Node.
- GigaVUE-FM also initiates an mTLS connection to theUCT-V Controller, establishing an mTLS connection with UCT-V.

  This structured flow ensures secure communication using mTLS-based authentication across all the fabric components.

GigaVUE-FM acts as the PKI

GigaVUE-FM manages all certificates for fabric components. It acts as a private PKI and uses Step-CA with the ACME protocol to issue and renew certificates. This automated process reduces the need for manual certificate handling and avoids external dependencies.

Bring Your Own CA

If your organization already uses a corporate CA, you can import those certificates into GigaVUE-FM. This allows your existing PKI infrastructure to work with Gigamon's secure communication system.

For more details on how to integrate your PKI infrastructure with GigaVUE-FM, refer to Integrate Private CA

- The active GigaVUE-FM instance shares intermediate CA files with all standby nodes.
- Only the active instance handles certificate requests. In case of a failover, a standby node takes over.
- The root and intermediate CAs are copied to all nodes to ensure continuity.
- If an instance is removed, it generates a new self-signed CA on restart.

Supported Platforms

- AWS
- Azure
- OpenStack
- Nutanix
- GCP
- OCI
- Openshift(UCT-C)
- VMware ESXi
- VMware NSX-T

Supported Components

- GigaVUE V Series Node
- GigaVUE V Series Proxy
- UCT-V
- UCT-V Controller
- UCT-C Controller and Tap

Rules and Notes

- If a public IP is revoked in public cloud platforms, you can issue a new certificate to remove the old IP.
- This feature is optional.
- Ensure NTP (Network Time Protocol) runs if GigaVUE-FM and components are on different hosts.
- Applying a certificate may temporarily cause a component to show as Down, but it recovers automatically.
- In AWS, disable the Source/Destination Check on network interfaces for GigaVUE V Series Proxy.

  Note: Enabling this check may block traffic if the IP address does not match the associated interface.

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.

Traffic Processing

GigaVUE Cloud Suite for AWS provides a comprehensive set of applications that allows you to build efficient and effective visibility solutions. These applications:

- **Reduce the traffic volume:** Apply user-defined filtering criteria, remove duplicate copies of packets, or remove a significant portion of each packet to reduce. The ability to focus on the right information carried in network packets helps increase the efficiency of analysis tools.
- **Protect Sensitive Data:** Mask sensitive information to meet regulatory compliance requirements.
- **Extract metadata:** Extract information such as NetFlow Generation and a vast array of other types of metadata.
- **Simplify Packet structure:** Remove different layers of headers in nested packets so that analysis tools can easily access the real payload.

This section provides detailed information on the following topics:

- Supported Applications
- Flexible Application Chaining

Supported Applications

The following table provides an overview of the applications included in GigaVUE Cloud Suite for AWS:

Parameter	Description
Application Filtering Intelligence	Filters traffic based on Layer 7 applications like YouTube, Netflix, or Facebook. Helps prioritize critical traffic and exclude low-value flows.
Adaptive Packet Filtering (Part of Application Filtering Intelligence)	Inspects any part of a packet—including within encapsulations and applies actions like drop, mask, or forward based on RegEx or string matches. This feature supports filtering across complex encapsulation headers, such as VXLAN, ERSPAN, GRE, Nested VLANs, MPLS, VN-Tag, and more.
Application Session Filtering (Part of Application Filtering Intelligence)	Uses RegEx to detect session patterns and forwards all packets in a matched session for analysis.
Application Metadata Intelligence	Exports metadata (For example, IPFIX or CEF) about detected applications to external collectors.
Application Metadata Exporter	Converts CEF metadata into JSON and sends it to cloud tools or Kafka.
Application Visualization	Identifies over 3,500 applications and shows their bandwidth usage over time.
De-Duplication	Detects and removes duplicate packets to prevent tool overload.
ERSPAN Tunnel Decapsulation	Strips ERSPAN headers to reveal the original packet.
Map	A collection of rules used to filter traffic in a V Series node.
GENEVE Decapsulation	Removes GENEVE tunnel headers.
Header Stripping	Removes headers like MPLS, VLAN, VXLAN, and GRE for cleaner analysis.
L2GRE Tunnel Decapsulation	Removes the protocol header added by the L2GRE tunnel to extract the original user data packet.
L2GRE Tunnel Encapsulation	Adds L2GRE headers to send packets to next-hop destinations.
Load Balancing	Distributes traffic to multiple tools while keeping flows consistent.
Masking	Overwrite specific packet fields to hide sensitive data during network analysis.
Packet Slicing	Truncates packets after a chosen point to reduce size and focus on relevant data.
Out of Band SSL/TLS Decryption	Decrypts SSL/TLS traffic for offline threat analysis.
UDPGRE Tunnel Decapsulation	Removes the protocol header added by the UDPGRE tunnel to extract the original user data packet.
VXLAN Tunnel Decapsulation	Removes the protocol header added by the VXLAN tunnel to extract the original user data packet.
VXLAN Tunnel Encapsulation	Adds VXLAN headers to send packets for further processing..

For details on how to configure these applications in the Monitoring Session canvas, refer to Add Applications to Monitoring Session (AWS).

Flexible Application Chaining

You can chain multiple applications in a Monitoring Session to control how traffic is received, processed, and forwarded. This chaining follows a Directed Acyclic Graph (DAG) model for maximum flexibility.

Example 1: The following diagram explains application chaining with two applications, Map and Slicing between Ingress and Egress Tunnels.

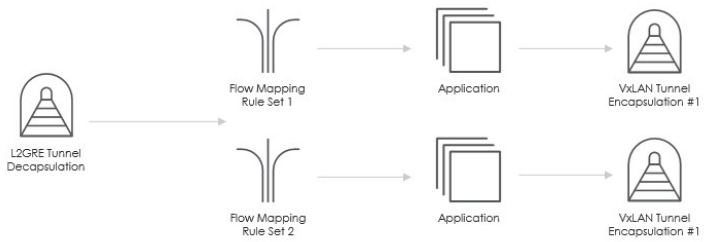
© 2017-2025 Gigamon Inc. All rights reserved.

The application chain in this example specifies the following:

- **Traffic Reception**: The V Series nodes receives acquired traffic through an L2GRE tunnel. It removes the L2GRE protocol header before sending packets to the FlowMap for filtering.
- **Traffic Filtering**: Packets are filtered based on user-defined rules in the FlowMap. Only packets matching the criteria are forwarded to the Slicing application.
- **Traffic Slicing**: The Slicing application removes specific parts of each packet as per user-defined parameters.
- **Traffic Forwarding**: The system adds a VXLAN header and sends the packet to your analysis tools based on the VXLAN Tunnel Encap configuration.

This Directed Acyclic Graph (DAG) model used in Monitoring Sessions provides the flexibility to customize how traffic is processed and forwarded.

Example 2: Here's another simple example of an application chain defined as part of a Monitoring Session:



© 2017-2025 Gigamon Inc. All rights reserved.

Traffic is received via an L2GRE tunnel with the L2GRE header removed before being sent to the FlowMap for filtering. The FlowMap application applies two sets of user-defined filtering rules:

- Set 1 sends packets to App1 for further processing.
- Set 2 sends matching packets matching to App2 for separate processing.

This flexible application chaining allows you to treat different types of traffic uniquely and send each to the most suitable tool—improving both efficiency and insight.

Traffic Forwarding

GigaVUE Cloud Suite for AWS provides useful features to forward processed traffic efficiently:

- Use tunnel encapsulation to forward traffic directly to your monitoring tools.
- Replicate traffic easily to send it to multiple tools at the same time..
- Load balances the traffic forwarded to multiple tools.
- Secure tunneling for added security.

Egress Tunneled Traffic

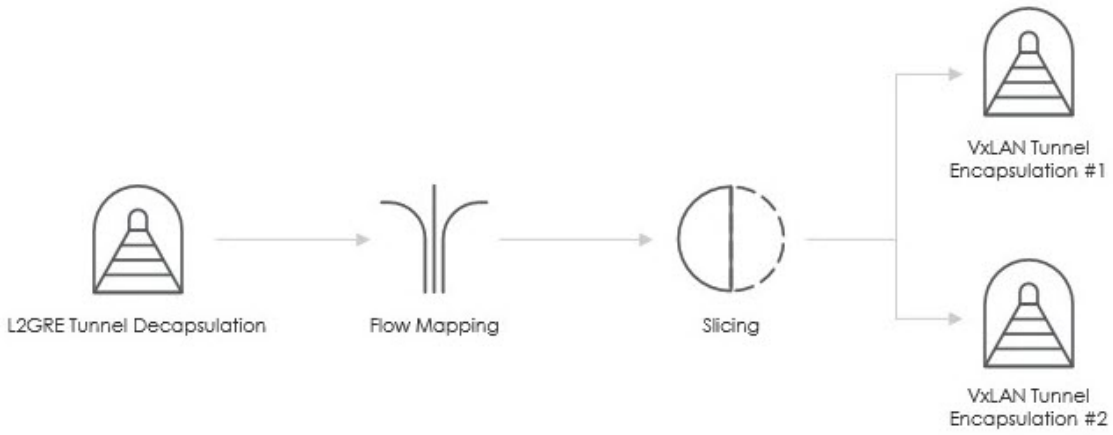
To route processed traffic, add tunnel endpoints to the Monitoring Session canvas. Configure each endpoint with a destination IP address, tunnel type, and other protocol-specific details. GigaVUE Cloud Suite for AWS supports four protocols for sending traffic to tools:

- L2GRE
- VXLAN
- TLS-PCAPNG (For secure tunnels)
- UDP

You can improve traffic analysis and tool efficiency by either replicating egress traffic to multiple tools or distributing high-volume traffic across several tool instances using the load balancer application.

Replicate Egress Traffic

You can easily replicate the processed traffic in the Monitoring Session canvas page. You can analyze the same traffic using different types of tools to catch different types of problems (For example,, network performance versus cyber security). The following example of a Monitoring Session configuration shows how the traffic is replicated and sent to different tools:



In the above diagram, all packets coming out from the Slicing application are replicated and tunneled to two different tools using the VXLAN protocol.

Load Balance Egress Traffic

In scenarios where the processed traffic volume exceeds the capacity of a single tool, you can deploy multiple tool instances to share the load. To simplify this, GigaVUE Cloud Suite for AWS provides a load balancer application that runs directly on GigaVUE V Series Nodes to distribute and balance traffic across multiple tools. To use this feature, simply add the load balancer application to your Monitoring Session canvas and connect its egress endpoint to all the egress tunnel endpoints. This ensures efficient traffic distribution and optimal tool utilization.

Elastic Load Balancing

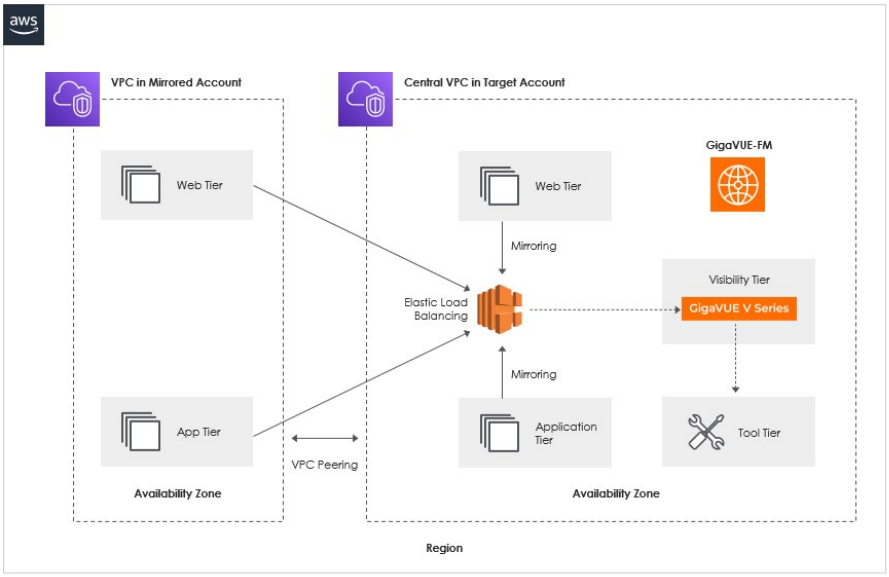
You can use a load balancer to uniformly distribute the traffic from AWS target VMs to GigaVUE V Series Nodes. The load balancer distributes the traffic to the GigaVUE V Series Nodes and the auto-scaling group deploys the GigaVUE V Series Nodes based on the traffic.

The following load balancers are supported:

- Network Load Balancer
- Gateway Load Balancer

Network Load Balancer

The AWS Network Load Balancer (NLB) uses NLB targets to distribute traffic across multiple resources such as EC2 instances, containers, or IP addresses within a VPC. It operates at the transport layer (Layer 4) and supports protocols like TCP, UDP, and TLS for low-latency, high-throughput applications. With the NLB, you can forward traffic from any subnet to targets across multiple Availability Zones for better fault tolerance and scalability. It allows you to monitor and manage network traffic across your VPC, ensuring high availability and performance.



© 2017-2025 Gigamon Inc. All rights reserved.

In this diagram, GigaVUE Cloud Suite deploys fabric components in a centralized VPC. External AWS accounts send mirrored traffic from their target VMs to an external Network Load Balancer. GigaVUE-FM configures traffic mirroring on these targets and forwards the mirrored traffic to the NLB. The load balancer then distributes the traffic to the GigaVUE V Series Nodes.

An Auto Scaling group monitors traffic levels and, through RESTful API integration with GigaVUE-FM, automatically adds or removes V Series Nodes based on pre-defined thresholds.

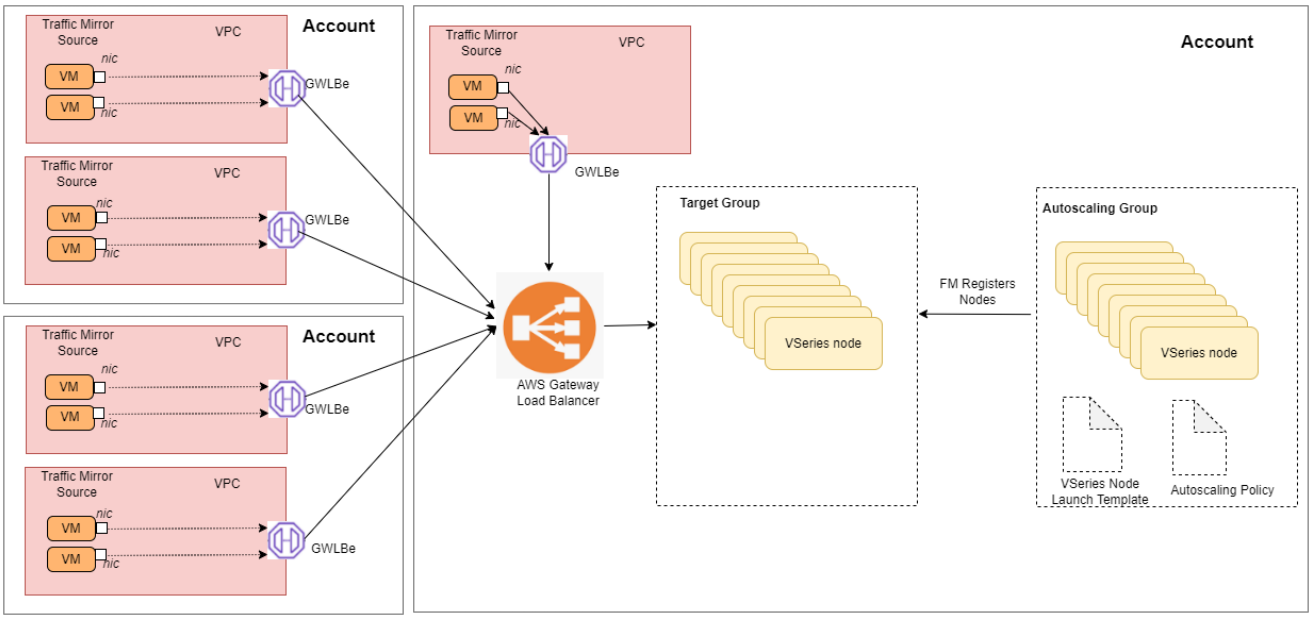
Components Required:

- GigaVUE-FM (Fabric Manager)
- GigaVUE V Series Nodes
- AWS Network Load Balancer (uniformly distributes traffic from AWS target VMs to GigaVUE V Series Nodes)

For detailed setup instructions, refer to Acquire Traffic using Traffic Mirroring with Network Load Balancer.

Gateway Load Balancer

The gateway load balancer (GWLB) uses the gateway load balancer endpoints to distribute the traffic across the endpoints. It is a VPC endpoint that provides connectivity between virtual machines. With GWLB Endpoint as a target, you can forward mirrored traffic from any subnet. You can monitor network traffic across multiple VPCs and accounts, with centralized traffic inspection in a single VPC across the entire organization.



In the architecture, you can see the deployment of GigaVUE Cloud Suite for AWS environments that have GWLB implementation for security appliances, such as firewalls. In such deployments, the applications and your appliances are in different VPCs. The workload VPC is configured with the Gateway load balancer endpoint while the service VPC is configured with the Gateway load balancer. Gigamon deployed VPC has the solution components, such asNodes, and the OOB tools, which consume the mirrored and decapsulated data.

In this deployment model, your workloads reside in one VPC, and the security appliances (such as firewalls) reside in another (called a service VPC). The workload VPC includes a GWLB Endpoint, while the service VPC hosts the actual GWLB and the GigaVUE Cloud Suite components, including:

- GigaVUE-FM
- GigaVUE V Series Nodes
- Out-of-band (OOB) tools that analyze mirrored and decapsulated traffic

This design allows scalable, centralized inspection across your cloud environment.

For more details, refer to Acquire Traffic using Traffic Mirroring with Gateway Load Balancing.

Inline V Series (AWS)

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.

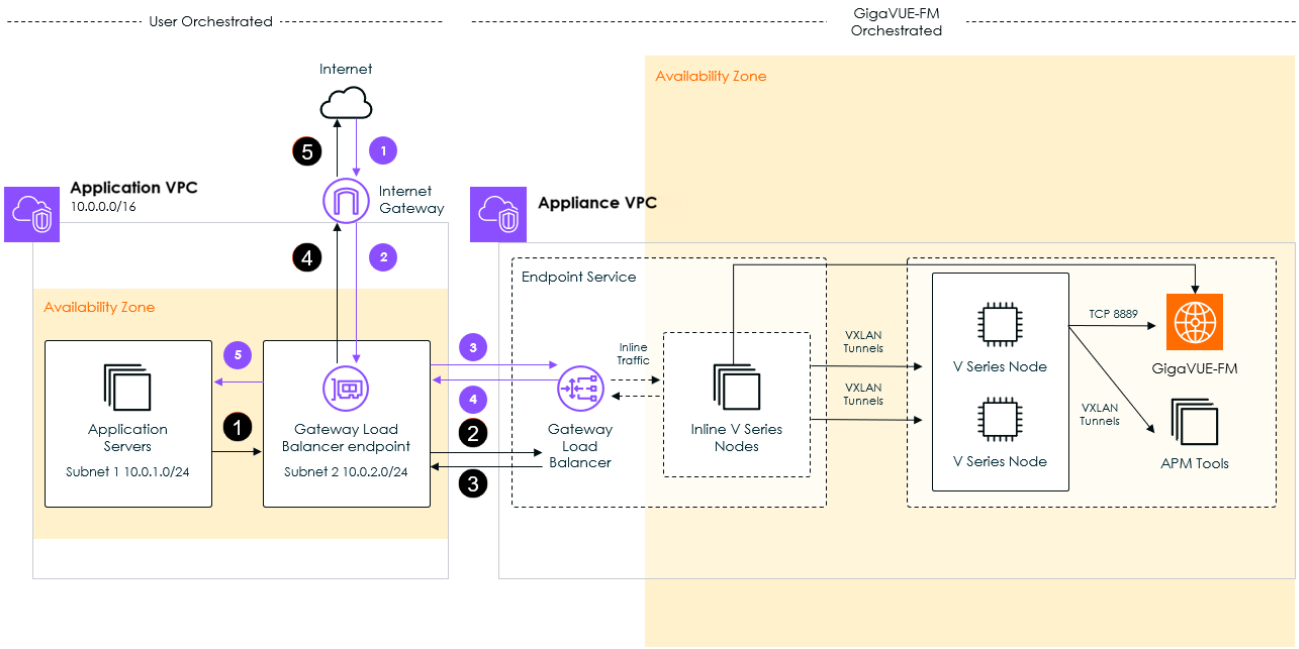
Architecture of Inline V Series Solution in AWS

Components required for configuring Inline V Series Solution in AWS:

- Application VPC
- Appliance VPC
- Internet Gateway
- Gateway Load Balancer endpoint
- Gateway Load balancer
- Inline V Series Node

Application VPC consists of multiple workload VMs, Gateway Load Balancer endpoint, Internet Gateway, availability zone, and Application Server with the availability zone. The appliance VPC consists of Gateway Load Balancer, Gateway Load Balancer service, Inline V Series Node (Target Listeners). Any traffic reaching the Gateway Load Balancer will be routed to the Target Listeners.

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



Traffic from the internet to the application server (Violet arrows):

1. The traffic from the internet is sent to the Application VPC using an Internet gateway.
2. This traffic is routed to the Gateway Load Balancer endpoint, as a result of ingress routing.

3. The Gateway Load Balancer endpoint sends the traffic to the Gateway Load Balancer in the Appliance VPC using a PrivateLink (for details refer to AWS PrivateLink) that is created between Gateway Load Balancer endpoint and the Gateway Load Balancer. The Gateway Load balancer 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 application 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 GENEVE encapsulated and forwarded to the Inline V Series Nodes.
4. The inline traffic is sent back to the Gateway Load Balancer endpoint in the application VPC.
5. Based on the look up in the routing table configured in the Gateway Load Balancer endpoint, the traffic is sent to the application servers (destination subnet).

Traffic from the application server to the internet (Black arrows):

1. Traffic from the application server is sent to the Gateway Load Balancer endpoint as a result of the default route configured on the application server subnet.
2. The Gateway Load Balancer endpoint forwards the traffic to the Gateway Load Balancer in the Appliance VPC over the private link between the endpoint and the Gateway Load Balancer. The Gateway Load balancer 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 application 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.
3. The inline traffic is sent back from the V Series Nodes to the Gateway Load Balancer in the Application VPC for egress handling.
4. Based on the Gateway Load Balancer associated route table, the processed traffic is forwarded to the Internet Gateway.
5. The traffic from the Application VPC is sent to internet.

Refer to the Acquire Traffic using Inline V Series Solution section for a detailed workflow on acquiring traffic through the Inline V Series.

Secure Tunneling to GigaVUE V Series Nodes

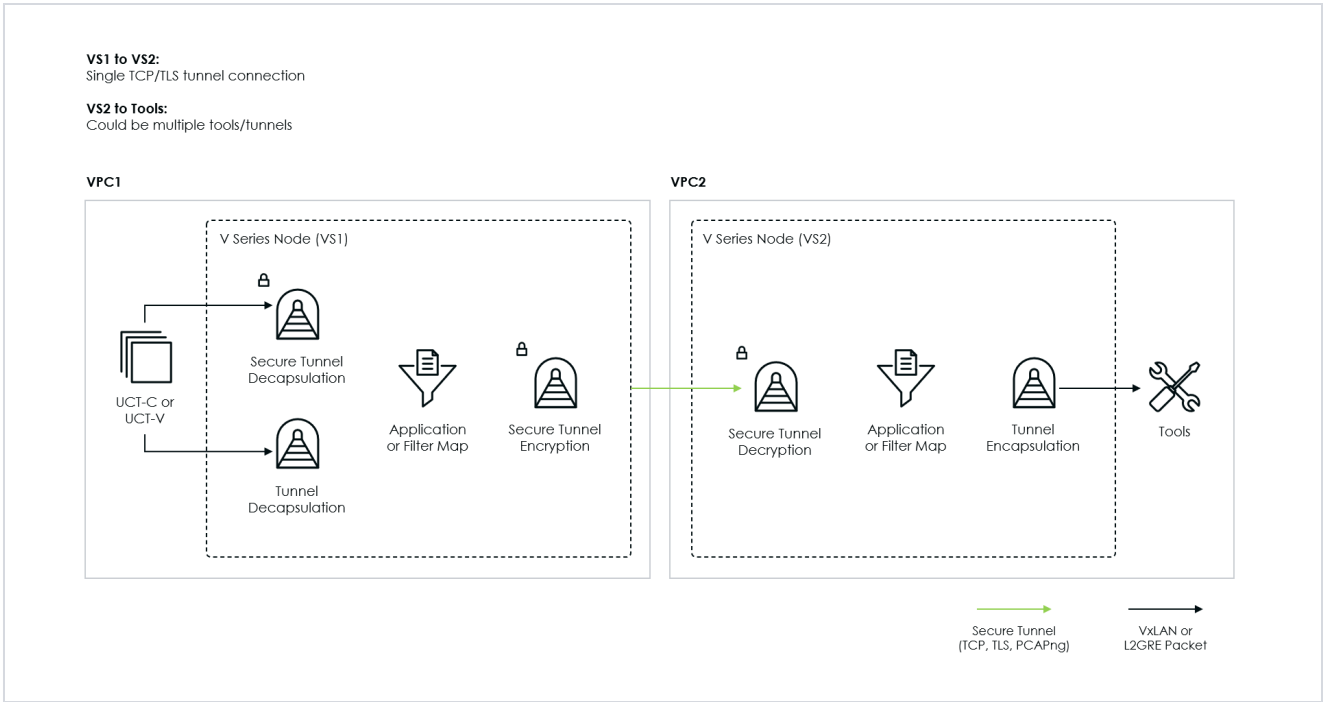
Secure Tunnel transfers the cloud captured packets from one GigaVUE V Series Node to another.

When sending traffic between two V Series Nodes, the source node captures and encapsulates the packets in PCAPng format. It then sends them to the destination V Series Node that decapsulates and processes the traffic based on your configuration.

How Does it Work!

- The source V Series forwards packets to the destination V series for further analysis.
- The destinatin node applies processing features such as de-duplication, application intelligence, or load balancing.
- The built-in load balancer distributes traffic across multiple V Series Nodes.
- If the load balancer sends packets to another node, it can re-encapsulate them and send them over another secure tunnel.

For more information, refer to PCAPng Application.



Supported Platforms

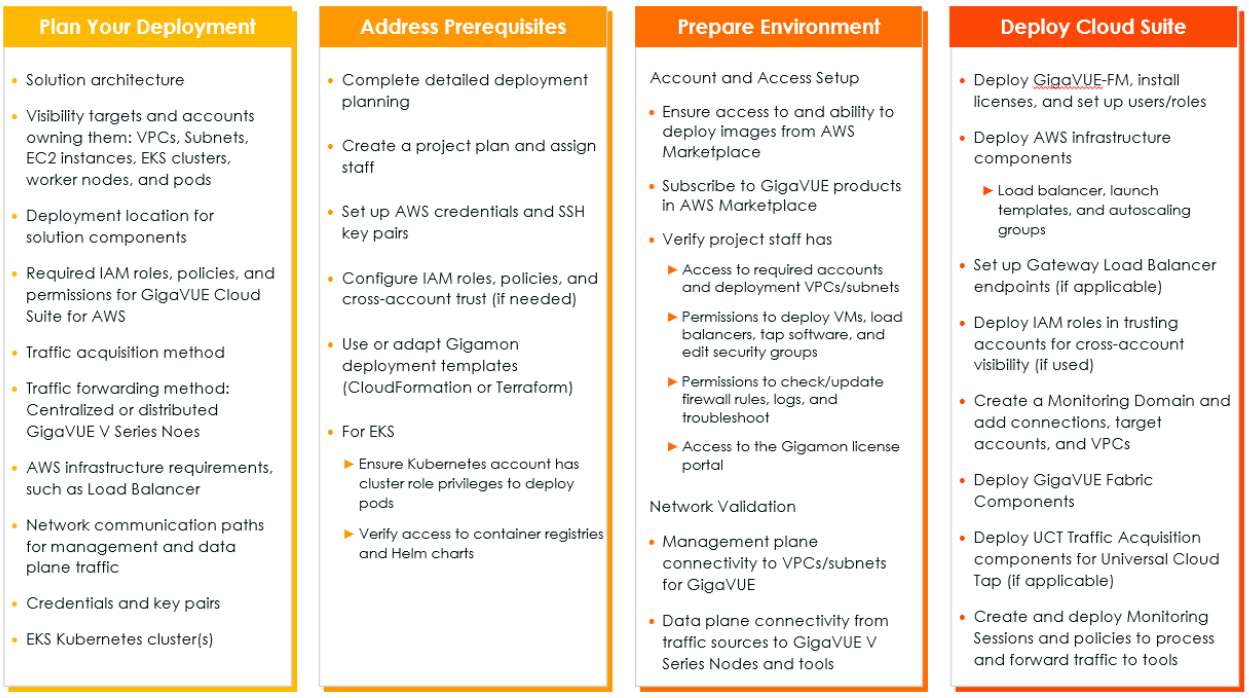
Secure Tunnels are supported on:

- OpenStack
- Azure
- AWS
- VMware NSX-T (only for Third Party Orchestration)
- VMware ESXi (only for Third Party Orchestration)
- Nutanix (only for Third Party Orchestration)
- Google Cloud Platform (only for Third Party Orchestration)

Refer to Configure Secure Tunnel (AWS) for instructions on how to configure Secure tunnels.

Deployment Overview

GigaVUE Cloud Suite for AWS deployment follows a set of steps that include planning and preparation before the actual solution deployment. This section provides an overview of the activities associated with GigaVUE Cloud Suite for AWS deployment. The top-level deployment activities are:



Deployment Planning

This section focuses on the different decisions and information that you need to know before deploying GigaVUE Cloud Suite for AWS. It assumes you have read the previous chapters and have a good understanding of the Cloud Suite components and concepts, along with AWS components, services, and architectures.

Identify the Deployment Method

GigaVUE Cloud Suite for AWS supports two options for deploying the Fabric Components:

- GigaVUE-FM Orchestration
- Third Party Orchestration

In either scenario, you need to first launch GigaVUE-FM and run. You can deploy GigaVUE-FM from the AWS Marketplace via a template or using script-based approach such as Cloud Formation, Terraform, or other.

GigaVUE-FM Orchestration

In this method, you can use the GigaVUE-FM user interface to delpoy the GigaVUE Fabric Components. After launching GigaVUE-FM, and applying the required license, you can deploy GigaVUE V Series Node, GigaVUE V Series Proxy, and UCT-V Controller using the GigaVUE-FM interface. Once deployed, GigaVUE-FM monitors the state of the deployed fabric components, and automatically replaces or relaunches them if any error conditions occur.

The GigaVUE-FM Orchestrated option simplifies the GigaVUE Cloud Suite for AWS deployment in AWS but requires AWS API access and permissions to deploy and manage visibility fabric VMs.

Third Party Orchestration

In this method, you need to use an external process to deploy the GigaVUE Fabric Components. It is typically a combination of Ansible and Terraform products or similar products. You can also use AWS as your Orchestrator. All of the GigaVUE fabric component images are accessible in AWS to support this method.

The Third Party Orchestration method provides an automated method to deploy fabric components in AWS. In this case, GigaVUE-FM can operate with a reduced set of permissions, or with no AWS API access at all (depending on solution architecture). For details, refer to Architecture.

This method requires an additional configuration file for GigaVUE V Series Node, GigaVUE V Series Proxy, UCT-V Controller, and UCT-V to register with the Monitoring Domain created in GigaVUE-FM. However, you can use the GigaVUE-FM to monitor the fabric components health. But you cannot use GigaVUE-FM to replace or relaunch the externally deployed fabric components.

Identify the AWS Regions

You can deploy GigaVUE Cloud Suite for AWS such that a single GigaVUE-FM instance manages and orchestrates the solution across multiple AWS regions.

- Each region requires its own Monitoring Domain
- Deployment of a separate fabric components is required.
- As a best practice to avoid inter-region data transfers and associated costs, deploy the fabric components (and tools) in each region.

Define GigaVUE-FM Deployment Location

You can deploy GigaVUE-FM inside or outside of AWS, such as an existing GigaVUE-FM instance on-premises.

Benefits of deploying a new instance of GigaVUE-FM in AWS:

1. Eliminates any upgrade requirements for existing on-premises GigaVUE-FM instance and GigaVUE appliances.
2. Enables AWS Instance Role-based credentials.
3. Eliminates the need to create or configure AWS credentials in GigaVUE-FM, especially in multi-account deployments.
4. As an alternative, you can use AWS access keys for credentials if GigaVUE-FM is external to AWS.

Points to Note:

- If GigaVUE-FM is deployed inside AWS, use IAM Role Based credentials.
- If GigaVUE-FM is deployed outside AWS, use Access Keys.

Identify the Traffic Acquisition Method

GigaVUE Cloud Suite for AWS supports traffic acquisition that includes AWS VPC Traffic Mirroring (TM), Gigamon Universal Cloud Tap, and customer orchestrated sources.

The traffic acquisition variations supported are:

- Direct VPC Traffic Mirroring
- VPC Traffic Mirroring with Network Load Balancer
- VPC Traffic Mirroring with Gateway Load Balancer
- UCT-V for VMs
- UCT-C for Containers
- Customer Orchestrated Source
- Customer Orchestrated Source with Gateway Load Balancer
- Customer Orchestrated Source with Network Load Balancer
- Inline V Series Solution

When creating a Monitoring Domain in GigaVUE-FM, you can choose any of the following Traffic Acquisition Methods:

- VPC Traffic Mirroring
- UCT-V
- Customer Orchestrated Source
- Inline

You can only choose one traffic acquisition method per Monitoring Domain. To use different traffic acquisition methods, you can create multiple Monitoring Domains.

> **NOTE:** GigaVUE Cloud Suite for AWS does not support VPC Traffic Mirroring and UCT-V in the same Monitoring Domain.

GigaVUE Cloud Suite for AWS requires deployment of each Monitoring Domain and its fabric components in a separate VPC.

Each Monitoring Domain supports one primary traffic acquisition type. But, you can add tunnel-based traffic sources as overlays using tunnels in a Monitoring Session. This allows traffic aggregation from containers and third-party tunnel sources into the same Monitoring Domain, regardless of its primary acquisition type.

Identify the Deployment Model

GigaVUE Cloud Suite for AWS provides flexibility in terms of the deployment model and the deployment location of fabric components. The deployment model can be of three types:

- Centralized
- Distributed
- Hybrid

Deployment Model for GigaVUE V Series Node

Centralized

In this model, the acquired traffic is forwarded or aggregated to a central location (central VPC), typically called the Tools VPC, where the GigaVUE V Series Node, load balancers (if used), and analysis tools are all colocated. This setup optimizes resource usage by centralizing traffic processing, enabling efficient scaling and simplified management. However, AWS costs may apply for traffic transfer via Transit Gateway (TGW) or Gateway Load Balancer (GWLB). Proper resource planning ensures the central VPC can handle the aggregated traffic effectively.

Distributed

In this model, GigaVUE V Series Nodes, UCT components (if used), and analysis tools are deployed directly into each VPC to process mirrored traffic locally. This approach minimizes data transfer costs by reducing reliance on Transit Gateway (TGW) or Gateway Load Balancer (GWLB) for traffic forwarding. While this requires additional EC2 resources in each VPC, it optimizes performance, lowers AWS costs, and ensures efficient local traffic processing and analysis.

Hybrid

In this model, a combination of both centralized and distributed deployment models is used. This hybrid approach allows for flexibility, where the design is optimized based on traffic volume, cost considerations, and performance needs. By considering factors like compute costs for GigaVUE V Series Nodes and GigaVUE V Series Proxy and the data transfer costs between VPCs, you can design a solution that balances efficiency and budget. For local traffic, a distributed model reduces transfer costs, while centralizing processing may simplify management but incur higher data transfer fees. The key is to tailor the design based on your specific needs.

Deployment Model for UCT-V Controller

For UCT-V traffic acquisition, deploy at least one UCT-V Controller to act as a communication proxy between GigaVUE-FM and the UCT-Vs. The UCT-V Controller connects to each UCT-V and maintains a single connection to GigaVUE-FM. You can optimize its placement to localize traffic and simplify security groups or network firewall rules.

Centralized

The centralized UCT-V Controller model simplifies deployment but requires additional network connections between the UCT-V Controller and distributed UCT-V instances.

Distributed

The distributed UCT-V Controller model minimizes security group and firewall requirements between GigaVUE-FM to enhance communication efficiency, while localizing connections to UCT-V instances. Its small VM footprint enables the cost-effective deployment of multiple controllers.

Hybrid

In this model, a combination of both centralized and distributed deployment models is used. It is common to combine centralized and distributed deployment models based on traffic, costs, and desired traffic types to optimize for cost and performance. Considerations should include computing costs for the controller VMs vs. the traffic crossing any VPC barrier.

Identify the AWS Accounts Involved

Most GigaVUE Cloud Suite for AWS deployments enable network visibility across multiple AWS accounts using AWS Secure Token Service (STS), Assumed Roles, and trust relationships. This eliminates the need to store credentials for different accounts in GigaVUE-FM.

Centralized vs Decentralized Account Deployment

When planning, identify all AWS accounts involved in the deployment:

Centralized Model

- A single central account hosts the visibility fabric components, including GigaVUE-FM, UCT-V Controller, GigaVUE V Series Nodes, and tools.
- Traffic sources reside in multiple VPCs across other AWS accounts.

Distributed Model

- The GigaVUE fabric components are deployed across all involved accounts.
- Clearly define the locations of deployed modules within each account.

Planning Action:

- For the centralized model, define the central account and list all other accounts requiring traffic visibility.
- For the distributed model, identify all accounts and specify where the modules will be deployed.

Identify the Subnets Involved

For each AWS Region, based on the chosen traffic acquisition method, identify the subnets involved.

For Traffic Mirroring and Customer Orchestrated Source

- For Centralized GigaVUE V Series Node deployment model or if load balancer used:
  - Define the central VPC and subnet where GigaVUE V Series Nodes and load balancer (if used) are deployed.
- For the Distributed GigaVUE V Series Node deployment model:
  - Define the list of all VPCs and associated subnets where GigaVUE V Series Nodes are deployed.
- Make a note if each VPC or subnet is pre-existing or you need to create.

For UCT-V

- For the Centralized UCT-V Controller deployment model:
  - Define the central VPC and subnet where the UCT-V Controller are deployed.
- For the Distributed UCT-V Controller deployment model:
  - Define the list of all VPCs and associated subnets where UCT-V Controller instancesare deployed.
- Make a note if each VPC or subnet is pre-existing or you need to create.

For UCT-C

Define a list of EKS clusters that contain EC2 worker nodes where UCT-C components are deployed. For details, refer to Universal Cloud TAP - Container Deployment Guide.

Identify the Required IAM Roles, Policies, and Permissions

GigaVUE-FM uses the AWS API to perform various tasks depending on the solution architecture. The IAM policy attached to the role used by GigaVUE-FM must contain the necessary permissions to perform those tasks. For the minimum required permission, refer to Permissions and Privileges (AWS).

During the actual deployment, GigaVUE-FM provides a Permission Check tool that allows you to verify:

- access to public cloud endpoints,
- if the required permissions are in place.

> **NOTE:** This tool is not a replacement for pre-deployment planning and permissions establishment.

Identify or Create the Necessary Keypairs

GigaVUE Fabric Components support administrative SSH access via SSH key pairs. When deploying these components the name of an AWS stored SSH Key must be provided to provision the public key on each component. You can use the associated private key for administrative access to these components. For details, refer to AWS Key Pair.

Identify the UCT-V Deployment Details

The UCT-V is provided as a Debian (.deb), RedHat Package Manager (.rpm), and Microsoft Installer (msi) package files. The UCT-V deployment configuration requires knowledge of the OS network interface naming conventions such as eth0, ens5, ad enX0,

Before deploying UCT-V:

- Identify the VMs where UCT-V deployment is required.
- Familiarize yourself with OS Network interface naming conventions.
- Identify the deployment method.

Identify the UCT-C Deployment Details

GigaVUE Cloud Suite for AWS supports hybrid deployments where traffic visibility for VMs (EC2 instances) and Kubernetes cluster is simultaneously supported from the same GigaVUE-FM, Monitoring Domain and GigaVUE V Series Node. The UCT-C Tap and Controller pod components are deployed to provide traffic acquisition in Kubernetes clusters. This is currently supported only for EKS clusters with EC2 worker nodes. For the specific planning and requirements for UCT-C based deployments for Kubernetes, refer to Universal Cloud TAP - Container Deployment Guide.

Deployment Prerequisites

The following sections explain the prerequisites for successful GigaVUE Cloud Suite for AWS deployment:

- Points to Note for GigaVUE Cloud Suite for AWS
- Subscribe to GigaVUE Products
- Supported Operating Systems for UCT-V
- Network Firewall Requirement
- Licensing for GigaVUE Cloud Suite for AWS
- AWS Security Credentials
- AWS Key Pair
- AWS Service Regions
- Subnet and Security Group for Amazon VPC

- Recommended and Supported Instance Types for AWS
- Configure Tokens
- GigaVUE-FM Version Compatibility
- Default Login Credentials for GigaVUE Fabric Components
- Permissions and Privileges (AWS)

Points to Note for GigaVUE Cloud Suite for AWS

Keep in mind the following notes and rules when deploying GigaVUE Cloud Suite:

- Deploy the GigaVUE-FM in AWS.
- If you already have GigaVUE-FM running outside of your AWS environment, connect that existing GigaVUE-FM to your AWS using Basic Credentials (access keys).
- If you have deployed the GigaVUE-FM outside of AWS, the GigaVUE-FM encrypts and stores the access key and the secret key in its database.
- Always attach an IAM role to the instance running GigaVUE-FM in AWS to connect it to your AWS account.
- Support is available for deploying GigaVUE fabric components through a third-party orchestrator.
- Set appropriate MTU for the interfaces to avoid fragmentation from UCT-V to GigaVUE V Series Node and from GigaVUE V Series Node to the tool. If the tool VM MTU is less than that of the GigaVUE V Series Node, the GigaVUE V Series Node fragments the packets. This results in packet loss because the Elastic Network Adapter (ENA) of AWS drops all fragments exceeding 200 packets per second.

  If you deploy GigaVUE-FM and GigaVUE V Series Nodes in different cloud platforms, add the GigaVUE-FM public IP address to the Data Notification Interface as the Target Address in the Event Notifications page. For information on configuration details, refer to the
  Configuration Setting section GigaVUE Administration Guide.
- If GigaVUE-FM and the workload VMs that require monitoring are in different AWS accounts (cross-account) and AWS Traffic Mirroring is the traffic acquisition method, you must configure either a Network Load Balancer or a Gateway Load Balancer. For more information, refer to Configure AWS Elastic Load Balancing.

Subscribe to GigaVUE Products

To deploy the GigaVUE Cloud Suite for AWS from the AWS Marketplace, you can subscribe to the following GigaVUE Cloud Suite components.

- GigaVUE V Series Node
- GigaVUE V Series Proxy

- GigaVUE V Series Controller
- GigaVUE Cloud Suite BYOL

NOTE:

- Subscribing to these components does not incur fee.
- To subscribe to GigaVUE Products, you must add "aws-marketplace:ViewSubscriptions" permission to the IAM policy.

To subscribe to the GigaVUE components, perform the following steps:

1. On your browser, log in to your AWS account.
2. On the AWS page, go to https://aws.amazon.com/marketplace/.
3. In the **Search** field, type Gigamon and select **Search**.
4. Select the latest version of the fabric component.
5. Select **View Purchase Options**. The terms and condition page is displayed.
6. Review the Terms and Conditions and select **Accept Terms**.

Supported Operating Systems for UCT-V

Supported Operating System for UCT-V[1] is 6.5.00, 6.6.00, 6.7.00, 6.8.00, 6.9.00, 6.10.00, 6.11.00, 6.12.00, 6.13.00

The table below lists the validated and supported versions of the Operating Systems for UCT-V.

Operating System	Supported Versions
Ubuntu/Debian	Versions 16.04 through 22.04
CentOS	Versions 7.5 through 9.0
RHEL	Versions 7.5 through 9.4
Windows Server	Versions 2012 through 2022 **Note**: Ensure the **send buffer size** of the network adapters is set to 128 MB for optimal performance and to minimize traffic disruption.
Rocky OS	Versions 8.4 through 8.8

GigaVUE-FM version 6.14.02 supports UCT-V version 6.14.02 as well as (n-2) versions. We recommend to use the latest version of UCT-V with GigaVUE-FM for better compatibility.

[1]From Software version 6.4.00, G-vTAP is renamed to UCT-V.

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

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.

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) 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	UCT-V Controller IP	Allows GigaVUE-FM to receive registration requests from UCT-V Controller using REST API.
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	443	UCT-V Controller IP	Allows GigaVUE-FM to receive registration requests from UCT-C Controller 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	5671	UCT-V Controller IP	Allows GigaVUE-FM to receive statistics from UCT-V Controllers.
Inbound	TCP	9600	UCT-V Controller	Allows GigaVUE-FM to receive certificate requests from UCT-V Controller.
Inbound	TCP	9600	GigaVUE V Series	Allows GigaVUE-FM to

			Proxy	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	TCP	5671	UCT-V Controller IP	Allows GigaVUE-FM to receive statistics from UCT-C Controllers.
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	TCP	9900	UCT-V Controller IP	Allows GigaVUE-FM to communicate control and management plane traffic with UCT-V Controller.
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	8443	UCT-C Controller IP	Allows GigaVUE-FM to communicate control and management plane traffic to UCT-C Controller.
Outbound	TCP	80	UCT-V Controller IP	Allows GigaVUE-FM to send ACME challenge requests to UCT-V Controller.

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.

UCT-V Controller

The following table defines the network communication parameters—protocols, ports, and CIDRs—required for UCT-V Controller to interact with GigaVUE-FM and UCT-V components, supporting registration, diagnostics, certificate exchange, and control-plane operations including third-party orchestration..

Direction	Protocol	Port	Source CIDR	Purpose
Inbound	TCP	9900	GigaVUE-FM IP	Allows UCT-V Controller to communicate control and management plane traffic with GigaVUE-FM.
Inbound	TCP	9900	UCT-V or Subnet IP	Allows UCT-V Controller to receive traffic health updates from UCT-V.
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 UCT-V Controller to receive the ACME challenge requests from GigaVUE-FM.
Inbound	TCP	8300	UCT-VSubnet	Allows UCT-V Controller to receive the certificate requests from the UCT-V.
Inbound (This is the port used for Third Party Orchestration)	TCP	8892	UCT-V Subnet	Allows UCT-V Controller to receive the registration requests and heartbeat from UCT-V.
Direction	**Protocol**	**Port**	**Destination CIDR**	**Purpose**
Outbound (This is the port used for Third Party Orchestration)	TCP	443	GigaVUE-FM IP	Allows UCT-V Controller to send the registration requests to GigaVUE-FM using REST API.

Outbound	TCP	5671	GigaVUE-FM IP	Allows UCT-V Controller to send traffic health updates to GigaVUE-FM.
Outbound (This is the port used for Third Party Orchestration)	TCP	9600	GigaVUE-FM IP	Allows GigaVUE-FM to receive certificate requests from the UCT-V Controller.
Outbound	TCP	9902	UCT-V Subnet	Allows UCT-V Controller to communicate control and management plane traffic with UCT-Vs for UCT-Vs with version greater than 6.10.00.
Outbound	TCP	8301	UCT-V Subnet	Allows ACME validation flow from UCT-V Controller to UCT-V.

UCT-V

The following table outlines UCT-V Controller's network communication requirements with GigaVUE-FM, detailing essential ports, protocols, and CIDRs for registration, diagnostics, certificate exchange, and orchestration traffic.

Direction	Protocol	Port	Source CIDR	Purpose
Inbound	TCP	9902	UCT-V Controller IP	Allows UCT-V to receive control and management plane traffic from UCT-V Controller.
Inbound	TCP	8301	UCT-V Controller IP	Allows UCT-V to receive the ACME challenge requests from the UCT-V Controller.
Direction	**Protocol**	**Port**	**Destination CIDR**	**Purpose**
Outbound	UDP (VXLAN)	VXLAN (default 4789)	GigaVUE V Series Node IP	Allows UCT-V to tunnel VXLAN traffic to GigaVUE V Series Nodes.
Outbound	IP Protocol (L2GRE)	L2GRE (IP 47)	GigaVUE V Series Node IP	Allows UCT-V to tunnel L2GRE traffic to GigaVUE V Series Nodes.
Outbound (Optional - This port is used only for Secure Tunnels)	TCP	11443	GigaVUE V Series Node IP	Allows UCT-V to securely transfer the traffic to the GigaVUE V Series Node.

Outbound	TCP	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	8892	UCT-V Controller IP	Allows UCT-V to receive the registration requests and heartbeat to UCT-V Controller.
Outbound	TCP	8300	UCT-V Controller IP	Allows UCT-V to receive ACME validation flow from UCT-V Controller.

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	UDP (VXLAN)	VXLAN (default 4789)	UCT-V Subnet IP	Allows GigaVUE V Series Nodes to receive VXLAN tunnel traffic to UCT-V.
Inbound	IP Protocol (L2GRE)	L2GRE	UCT-V Subnet IP	Allows GigaVUE V Series Nodes to receive L2GRE tunnel traffic to UCT-V.
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 Secure Tunnels)	TCP	11443	UCT-V subnet	Allows to securely transfer the traffic to GigaVUE V Series Nodes.
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.

UCT-C Controller - deployed in Kubernetes worker mode

The following table outlines UCT-C Controller's network communication parameters in Kubernetes worker mode, specifying TCP ports and CIDRs required for management, statistics exchange, and secure connectivity with GigaVUE-FM.

UCT-C Controller deployed inside Kubernetes worker node				
Direction	**Protocol**	**Port**	**Source CIDR**	**Purpose**

Inbound	TCP	8443 (configurable)	GigaVUE-FM IP	Allows GigaVUE-FM to communicate with UCT-C Controller.
Direction	**Protocol**	**Port**	**Destination CIDR**	**Purpose**
Outbound	TCP	5671	Any IP address	Allows UCT-C Controller to send statistics to GigaVUE-FM.
Outbound	TCP	443	GigaVUE-FM IP	Allows UCT-C Controller to communicate with GigaVUE-FM.

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.

UCT-V Controller

The following table specifies the communication parameters required for third-party orchestration, detailing the TCP ports and CIDRs used by UCT-V Controller to manage registration and control-plane traffic with UCT-V components.

Direction	Protocol	Port	Source CIDR	Purpose
Inbound (This is the port used for Third Party Orchestration)	TCP	8891	UCT-V or Subnet IP	Allows UCT-V Controller to receive the registration requests from UCT-V.
Direction	**Protocol**	**Port**	**Destination CIDR**	**Purpose**
Outbound	TCP	9901	UCT-V Controller IP	Allows UCT-V Controller to communicate control and management plane traffic with UCT-Vs.

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	TCP	8891	GigaVUE V Series Proxy IP	Allows GigaVUE V Series Node to send registration requests and

for Third Party Orchestration)				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.

Licensing for GigaVUE Cloud Suite for AWS

You can license the GigaVUE Cloud Suite for AWS using one of the following methods:

- Purchase GigaVUE Cloud Suite using CPPO
- Bundle Replacement Policy

Upon installing GigaVUE-FM, you receive a complimentary 30-day SecureVUE Plus trial Volume-Based License (VBL) with a 1TB capacity, valid from the installation date. For details, refer to Default Trial Licenses.

For purchasing licenses with the Volume-Based License (VBL) option, contact our Sales. Refer to Contact Sales. For instructions on how to generate and apply license refer to the *GigaVUE Administration Guide* and the *GigaVUE Licensing Guide*.

Default Trial Licenses

After installing GigaVUE-FM, you receive a one-time, free 1TB SecureVUE Plus trial Volume-Based License (VBL) for 60 days, starting from the installation date.

This license includes the following applications:

- ERSPAN
- GENEVE
- Slicing
- Masking
- Trailer

- Tunneling
- Load Balancing
- Enhanced Load Balancing
- Flow map
- Header Stripping
- Header Addition
- De-duplication
- NetFlow
- Application Packet Filtering
- Application Filtering Intelligence
- Application Metadata Intelligence
- Application Metadata Exporter
- Inline SSL
- SSL Decrypt
- Precryption

> **NOTE:** If you do not have any other volume-based licenses installed, the deployed monitoring sessions are undeployed from the existing GigaVUE V Series Nodes after 60 days at the expiration of the trial license.

When you install a new Volume-Based License (VBL), the existing trial license remains active alongside the new VBL. When the trial license period expires, it is automatically deactivated. After deactivation, the trial license moves to the Inactive tab on the VBL page.

License Requirements for Monitoring Sessions

You must use one of the following GigaVUE Cloud Suite™ licenses to deploy any supported application in a Monitoring Session:

- CoreVUE Base Bundle (minimum required)
- NetVUE
- SecureVUE Plus

The default GigaVUE-FM licenses do not provide entitlement for deploying Monitoring Session applications.

The default trial VBL license (SecureVUE Plus) will support deploying applications in Monitoring Sessions only for the duration of the trial license.

Purchase GigaVUE Cloud Suite using CPPO

GigaVUE Cloud Suite is available as an Amazon Machine Image (AMI) product within the AWS Marketplace. GigaVUE Cloud Suite purchased through the AWS Marketplace with Channel Partner Private Offers (CPPO) comes with a Volume-Based License.

The list of SKUs[1]. is available on the AWS Marketplace through the Channel Partner Private Offers (CPPO):

- VBL-250T-BN-SVP
- VBL-50T-BN-SVP
- VBL-2500T-BN-NV

For detailed information on VBL and the available add-on packages, refer to Bundle Replacement Policy.

For purchasing Volume-Based License (VBL), Contact Sales.

Volume Based License (VBL)

All the GigaVUE V Series Nodes connected to GigaVUE-FM periodically report statistics on the amount of traffic that flows through the V Series Nodes. The statistics reflect the data volume flowing through the V Series Nodes, with the usage statistics of all licensed applications that run on these nodes.

GigaVUE Cloud Suite uses volume-based licensing (VBL), available as monthly subscription licenses. In the Volume-based Licensing (VBL) scheme, specific applications on the V Series Nodes are entitled to a specified amount of total data volume over the term of the license.

Distributing the license to individual nodes becomes irrelevant for Gigamon accounting purposes. GigaVUE-FM monitors overall consumption across all nodes and tracks individual application usage and overages.

Related Information

- Contact Sales: For purchasing licenses with the Volume-Based License (VBL) option.
- For more information, refer to the Data Sheet for the required GigaVUE Cloud Suite.

Base Bundles

In volume-based licensing scheme, licenses are offered as bundles. The following three base bundle types are available:

[1]Stock Keeping Unit. Refer to the *What is a License SKU?* section in the FAQs for License.

- CoreVUE
- NetVUE
- SecureVUE Plus

The bundles are available as SKUs [1]. The SKUs are named such that the number indicates the total volume allowance of the SKU for that base bundle. For example, VBL-250T-BN-CORE indicates a daily volume allowance of 250 Terabytes (250T) for the CoreVUE bundle.

The features supported for base bundle licenses are given in the following table:

Feature	CoreVUE	NetVUE	SecureVUE Plus
Slicing	√	√	√
Masking	√	√	√
Advanced Load Balancing	√	√	√
Advanced Tunneling	√	√	√
Deduplication	-	√	√
NetFlow Generation	-	√	√
Adaptive Packet Filtering (APF)	-	-	√
Application Filtering Intelligence (AFI)	-	-	√
Application Metadata Intelligence (AMI)	-	-	√
Application Metadata Exporter (AMX)	-	-	√
Inline Decryption	-	-	√
OOB Decryption	-	-	√
Precryption	-	-	√
Gigamon Enriched Metadata	-	-	√

Bundle Replacement Policy

Refer to the following notes:

[1]Stock Keeping Unit. Refer to the What is a License SKU? section in the FAQs for Licenses chapter.

- You can only upgrade to a higher bundle.
- You cannot have two different base bundles at the same time. However, you can have multiple base bundles of the same type.
- As soon as you upgrade to a higher bundle, the existing lower bundles are automatically deactivated.

Add-on Packages

GigaVUE-FM allows you to add add-on packages to the base bundles. These add-on packages allow you to add additional applications to your base bundles. Add-on packages have their own start/end date and volume specifications.

The following add-on SKUs are available:

- VBL-50T-ADD-5GC
- VBL-250T-ADD-5GC
- VBL-2500T-ADD-5GC
- VBL-25KT-ADD-5GC

Rules for add-on packages:

- An active base bundle is required to use an Add-on package.
- Your base bundle limits the total volume usage of the add-on package in the following ways:
  - If the volume allowance of your add-on package is less than the base bundle, then your add-on package can only handle the volume allocated for the add-on package.
  - When the life term of an add-on package extends beyond the base bundle, and the base bundle expires, the add-on package's volume allowance is reduced to zero until you add a new base bundle.
  - The total volume is cumulative when multiple base bundles of the same type are active within the same time interval.

For more information about SKUs, refer to the respective Data Sheets as follows:

- GigaVUE Cloud Suite for VMware Data Sheet
- GigaVUE Cloud Suite for AWS Data Sheet
- GigaVUE Cloud Suite for Azure Data Sheet
- GigaVUE Cloud Suite for OpenStack
- GigaVUE Cloud Suite for Nutanix

How GigaVUE-FM Tracks Volume-Based License Usage

GigaVUE-FM applies the following methods to track the license usage for each GigaVUE V Series Node:

- When you create and deploy a monitoring session, GigaVUE-FM allows you to use only applications with active licenses.
- When a license expires, you are notified with an audit log. For more information, refer to the *About Audit Logs* section in the respective GigaVUE Cloud Suite Deployment Guide.
- When a license expires (and has not been renewed yet), the monitoring sessions using the corresponding license are not undeployed.
- For releases prior to 6.4:
  - The Monitoring Sessions using the corresponding license are undeployed, but not deleted from the database.
  - Any undeployed monitoring sessions are redeployed when you renew a license or newly import the same.

NOTE: GigaVUE-FM displays a notification on the screen when the license expires.

Activate Volume-Based Licenses

To activate Volume-Based Licenses,

1. On the left navigation pane, select .
2. Go to **System > Licenses**.
3. From the top navigation bar, select the **VBL** from the **Activation** drop-down.
4. Select **Activate Licenses**. The **Activate License** page appears.
5. Select **IP Address** or **Hostname** to include this information. If you exclude the IP Address or Hostname, identify the chassis or GigaSMART card by its ID when activating.
6. Download the fabric inventory file that contains information about GigaVUE-FM.
7. Select **Next**. For details, refer to the What is a Fabric Inventory File?What is a Fabric Inventory File section in *GigaVUE Licensing Guide*
8. Select **Gigamon License Portal**.
9. On the portal, upload the Fabric Inventory file.
10. Select the required license and select **Activate**. A license key is provided.
11. Record the license key or keys.
12. Return to GigaVUE-FM and select **Choose File to** upload the file.

Manage Volume-Based Licenses

This section provides information on how to manage active and inactive Volume-Based Licenses in GigaVUE-FM.

View active Volume-Based License

To view active Volume-Based License (VBL):

1. On the left navigation pane, click .
2. Go to **System > Licenses**.
3. From the top navigation bar, select the **VBL** from the **Activation** drop-down list and click **Active**.

   This page lists the following information about the active Volume-Based Licenses.

Field	Description
SKU	Unique identifier associated with the license.
Bundle	Bundle to which the license belongs to.
Volume	Total daily allowance volume.
Starts	License start date.
Ends	License end date.
Type	Type of license (Commercial, Trial, Lab, and other license types).
Activation ID	Activation ID.
Entitlement ID	Entitlement ID. Entitlement ID is the permission with which the acquired license can be activated online.
Reference ID	Reference ID.
Status	License status.

NOTE: The License Type and Activation ID are displayed by default in the Active tab in the VBL page.

To display the Entitlement ID field, select the column setting configuration option to enable the Entitlement ID field.

View Inactive Volume-Based License

To view inactive Volume-Based License (VBL):

1. On the left navigation pane, click .
2. Go to **System > Licenses**.
3. From the top navigation bar, select the **VBL** from the **Activation** drop-down and click **Inactive**.

   This page lists the following information about the inactive Volume-Based Licenses.

Field	Description
SKU	Unique identifier associated with the license.
Bundle	Bundle to which the license belongs to.
Ends	License end date.
Deactivation Date	Date the license got deactivated.
Revocation Code	License revocation code.
Status	License status.

NOTE: The License Type, Activation ID and Entitlement ID fields are not displayed by default in the Inactive tab of VBL page. To display these fields, select the column setting configuration option and enable these fields.

Activate Volume-Based Licenses

To activate Volume-Based Licenses,

1. On the left navigation pane, select .
2. Go to **System > Licenses**.
3. From the top navigation bar, select the **VBL** from the **Activation** drop-down.
4. Select **Activate Licenses**. The **Activate License** page appears.
5. Select **IP Address** or **Hostname** to include this information. If you exclude the IP Address or Hostname, identify the chassis or GigaSMART card by its ID when activating.
6. Download the fabric inventory file that contains information about GigaVUE-FM.
7. Select **Next**. For details, refer to the What is a Fabric Inventory File section in *GigaVUE Licensing Guide*
8. Select **Gigamon License Portal**.
9. On the portal, upload the Fabric Inventory file.
10. Select the required license and select **Activate**. A license key is provided.
11. Record the license key or keys.
12. Return to GigaVUE-FM and select **Choose File to** upload the file.

NOTE: If a VBL is deactivated after a bundle upgrade, you cannot create or edit Monitoring Sessions that include applications from the deactivated VBL during the grace period. You should manually deactivate the upgraded license during the grace period to move the inactive lower bundle license back to active status.

For detailed information on dashboards and report generation for Volume-Based Licensing refer to the following table:

For details about:	Reference section	Guide
How to generate Volume-Based License reports	Generate VBL Usage Reports	GigaVUE Administration Guide
Volume-Based License report details	Volume Based License Usage Report	GigaVUE Administration Guide
Fabric Health Analytics dashboards for Volume-Based Licenses usage	Dashboards for Volume Based Licenses Usage	GigaVUE-FM User Guide

AWS Security Credentials

You need valid security credentials for AWS to establish the initial connection between GigaVUE-FM and AWS. These credentials verify your identity and determine whether you have authorization to access the resources you are requesting. AWS employs these security credentials to authenticate and authorize your requests.

You need one of the following security credentials:

- **Identity and Access Management (IAM) role**: If GigaVUE-FM is running within AWS, it is recommended to use an IAM role. Using an IAM role helps you securely make API requests from the instances.
  - Create an IAM role according to the permissions and policies listed in Permissions and Privileges (AWS).
  - Ensure that you are using Customer Managed Policies or Inline Policies.
- **Access Keys**: If GigaVUE-FM is configured in the enterprise data center, then you must use the access keys or basic credentials to connect to the VPC. Basic credentials allow full access to all the resources in your AWS account. An access key consists of an access key ID and a secret access key. For detailed instructions on creating access keys, refer to the AWS documentation on Managing Access Keys for Your AWS Account.

NOTE: To obtain the IAM role or access keys, contact your AWS administrator.

For details on how to configure AWS Credentials in GigaVUE-FM, refer to Deployment Options for GigaVUE Cloud Suite for AWS using GigaVUE-FM Orchestration.

AWS Key Pair

When configuring GigaVUE-FM and GigaVUE fabric components in AWS, you need to specify the defined key pair. A key pair, consisting of a public key and a private key, is a set of security credentials that you use to prove your identity when connecting to an Amazon EC2 instance.

When you define the specifications for the UCT-V Controllers, GigaVUE V Series Nodes, and GigaVUE V Series Proxy in your VPC, you must create a key pair and specify the name of this key pair.

Important considerations

- The key pair is crucial for securely accessing your Gigamon instances in AWS.
- Keep the private key file safe, as it is required to connect to the instances.
- You cannot recover a key pair. If lost, you need to create a new key pair.
- Key pairs are region-specific in AWS.

To create a key pair in AWS, refer to the Create a key pair for your Amazon EC2 instance section in AWS Documentation.

AWS Service Regions

GigaVUE-FM connects to the AWS platform through public API endpoints using HTTPS, the default protocol for communication. Ensure that GigaVUE-FM has access to the following service endpoints:

- iam.amazonaws.com
- ec2.<region>.amazonaws.com
- kms.<region>.amazonaws.com
- sts.<region>.amazonaws.com
- autoscaling.<region>.amazonaws.com
- ram.<region>.amazonaws.com
- elasticloadbalancing.<region>.amazonaws.com

For more information about the endpoints and the protocols used, refer to AWS service endpoints.

Subnet and Security Group for Amazon VPC

Your VPC must have the following elements to configure the GigaVUE Cloud Suite for AWS:

- Subnet for VPC
- Security Group

Subnet for VPC

VPC must have a subnet to configure the GigaVUE Cloud Suite for AWS components. You can either have the components deployed in a single subnet or in multiple subnets.

- **Management Subnet** that GigaVUE-FM uses to communicate with the GigaVUE V Series Nodes and UCT-V Controllers.
- **Data Subnet** that can accept incoming mirrored traffic from UCT-V or be used to egress traffic to a tool.

If a single subnet is used, then the Management subnet is also used as a Data Subnet.

Security Group

When you launch GigaVUE-FM, GigaVUE V Series Proxies, GigaVUE V Series Nodes, and UCT-V Controllers, a security group is utilized to define virtual firewall rules for your instance, which in turn regulates inbound and outbound traffic. You can add rules to manage inbound traffic to instances, and a distinct set of rules to control outbound traffic.

To create a security group, refer to Create a security group topic in the AWS Documentation.

We recommend to create a separate security group for each component using the rules and port numbers listed in the following table.

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

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.

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	Allows UCT-V Controller

				IP	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	Allows GigaVUE V Series

				Proxy	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) 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	UCT-V Controller IP	Allows GigaVUE-FM to receive registration requests from UCT-V Controller using REST API.
Inbound	TCP	443	GigaVUE V Series	Allows GigaVUE-FM to

(This is the port used for Third Party Orchestration)			Node IP	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	443	UCT-V Controller IP	Allows GigaVUE-FM to receive registration requests from UCT-C Controller 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	5671	UCT-V Controller IP	Allows GigaVUE-FM to receive statistics from UCT-V Controllers.
Inbound	TCP	9600	UCT-V Controller	Allows GigaVUE-FM to receive certificate requests from UCT-V Controller.
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	TCP	5671	UCT-V Controller IP	Allows GigaVUE-FM to receive statistics from UCT-C Controllers.
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	TCP	9900	UCT-V Controller IP	Allows GigaVUE-FM to communicate control

				and management plane traffic with UCT-V Controller.
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	8443	UCT-C Controller IP	Allows GigaVUE-FM to communicate control and management plane traffic to UCT-C Controller.
Outbound	TCP	80	UCT-V Controller IP	Allows GigaVUE-FM to send ACME challenge requests to UCT-V Controller.
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.

UCT-V Controller

The following table defines the network communication parameters—protocols, ports, and CIDRs—required for UCT-V Controller to interact with GigaVUE-FM and UCT-V components, supporting registration, diagnostics, certificate exchange, and control-plane operations including third-party orchestration..

Direction	Protocol	Port	Source CIDR	Purpose
Inbound	TCP	9900	GigaVUE-FM IP	Allows UCT-V Controller to communicate control and management plane traffic with GigaVUE-FM.
Inbound	TCP	9900	UCT-V or Subnet IP	Allows UCT-V Controller to receive traffic health updates

				from UCT-V.
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 UCT-V Controller to receive the ACME challenge requests from GigaVUE-FM.
Inbound	TCP	8300	UCT-VSubnet	Allows UCT-V Controller to receive the certificate requests from the UCT-V.
Inbound (This is the port used for Third Party Orchestration)	TCP	8892	UCT-V Subnet	Allows UCT-V Controller to receive the registration requests and heartbeat from UCT-V.

Direction	Protocol	Port	Destination CIDR	Purpose
Outbound (This is the port used for Third Party Orchestration)	TCP	443	GigaVUE-FM IP	Allows UCT-V Controller to send the registration requests to GigaVUE-FM using REST API.
Outbound	TCP	5671	GigaVUE-FM IP	Allows UCT-V Controller to send traffic health updates to GigaVUE-FM.
Outbound (This is the port used for Third Party Orchestration)	TCP	9600	GigaVUE-FM IP	Allows GigaVUE-FM to receive certificate requests from the UCT-V Controller.
Outbound	TCP	9902	UCT-V Subnet	Allows UCT-V Controller to communicate control and management plane traffic with UCT-Vs for UCT-Vs with version greater than 6.10.00.
Outbound	TCP	8301	UCT-V Subnet	Allows ACME validation flow from UCT-V Controller to UCT-V.

UCT-V

The following table outlines UCT-V Controller's network communication requirements with GigaVUE-FM, detailing essential ports, protocols, and CIDRs for registration, diagnostics, certificate exchange, and orchestration traffic.

Direction	Protocol	Port	Source CIDR	Purpose
Inbound	TCP	9902	UCT-V Controller IP	Allows UCT-V to receive control and management plane traffic from UCT-V Controller.

Inbound	TCP	8301	UCT-V Controller IP	Allows UCT-V to receive the ACME challenge requests from the UCT-V Controller.
Direction	**Protocol**	**Port**	**Destination CIDR**	**Purpose**
Outbound	UDP (VXLAN)	VXLAN (default 4789)	GigaVUE V Series Node IP	Allows UCT-V to tunnel VXLAN traffic to GigaVUE V Series Nodes.
Outbound	IP Protocol (L2GRE)	L2GRE (IP 47)	GigaVUE V Series Node IP	Allows UCT-V to tunnel L2GRE traffic to GigaVUE V Series Nodes.
Outbound (Optional - This port is used only for Secure Tunnels)	TCP	11443	GigaVUE V Series Node IP	Allows UCT-V to securely transfer the traffic to the GigaVUE V Series Node.
Outbound	TCP	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	8892	UCT-V Controller IP	Allows UCT-V to receive the registration requests and heartbeat to UCT-V Controller.
Outbound	TCP	8300	UCT-V Controller IP	Allows UCT-V to receive ACME validation flow from UCT-V Controller.

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	UDP (VXLAN)	VXLAN (default 4789)	UCT-V Subnet IP	Allows GigaVUE V Series Nodes to receive VXLAN tunnel traffic to UCT-V.
Inbound	IP Protocol (L2GRE)	L2GRE	UCT-V Subnet IP	Allows GigaVUE V Series Nodes to receive L2GRE

				tunnel traffic to UCT-V.
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 Secure Tunnels)	TCP	11443	UCT-V subnet	Allows to securely transfer the traffic to GigaVUE V Series Nodes.
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.

UCT-C Controller - deployed in Kubernetes worker mode

The following table outlines UCT-C Controller's network communication parameters in Kubernetes worker mode, specifying TCP ports and CIDRs required for management, statistics exchange, and secure connectivity with GigaVUE-FM.

UCT-C Controller deployed inside Kubernetes worker node				
Direction	**Protocol**	**Port**	**Source CIDR**	**Purpose**
Inbound	TCP	8443 (configurable)	GigaVUE-FM IP	Allows GigaVUE-FM to communicate with UCT-C Controller.
Direction	**Protocol**	**Port**	**Destination CIDR**	**Purpose**
Outbound	TCP	5671	Any IP address	Allows UCT-C Controller to send statistics to GigaVUE-FM.
Outbound	TCP	443	GigaVUE-FM IP	Allows UCT-C Controller to communicate with GigaVUE-FM.

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.

UCT-V Controller

The following table specifies the communication parameters required for third-party orchestration, detailing the TCP ports and CIDRs used by UCT-V Controller to manage registration and control-plane traffic with UCT-V components.

Direction	Protocol	Port	Source CIDR	Purpose
Inbound (This is the port used	TCP	8891	UCT-V or Subnet IP	Allows UCT-V Controller to receive the registration requests

for Third Party Orchestration)				from UCT-V.
Direction	**Protocol**	**Port**	**Destination CIDR**	**Purpose**
Outbound	TCP	9901	UCT-V Controller IP	Allows UCT-V Controller to communicate control and management plane traffic with UCT-Vs.

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.

Recommended and Supported Instance Types for AWS

This section provides information on the recommended and supported instance types for AWS.

Product	Instance Type	vCPU	RAM
GigaVUE-FM	m5.xlarge	4 vCPU	16GB
GigaVUE V Series Node	c5n.xlarge (AMD)	4 vCPU	10.5GB
	c7gn.xlarge (ARM)	4 vCPU	8GB
GigaVUE V Series Proxy	t2.medium (AMD)	2 vCPU	4GB
	t4g.micro (ARM)	2 vCPU	1GB
UCT-V	t2.micro	1 vCPU	1GB
UCT-V Controller	t2.xlarge	4 vCPU	16GB

Notes:

- A single UCT-V Controller can manage up to 500 (t2.small) UCT-Vs. For more than 500 UCT-Vs, you must add an additional UCT-V Controller to scale up accordingly.
- For recommended instance types for the V Series Node, running Application Intelligence applications- such as Application Metadata, Application Visualization, and Application Filtering, refer to the following sections:
  - Configure Application Metadata Intelligence for Virtual Environment
  - Configure Application Filtering Intelligence for Virtual Environment
  - Configure Application Visualization for Virtual Environment

Supported Instance Types

GigaVUE-FM supports both nitro and non-nitro-based instances; the following sections list the supported nitro and non-nitro-based instances:

Supported Nitro Instance Types

VPC Traffic Mirroring is supported on the following EC2 instance types:

Purpose	Instance types
General purpose	M5, M5a, M5ad, M5d, M5dn, M5n, M6g, M6gd, T3, T3a
Compute optimized	C5, C5d, C5n, C6g, C6gd
Memory optimized	R5, R5a, R5ad, R5d, R5dn, R5n, R6g, R6gd, X1, X1e, z1d
Storage optimized	D3, D3en, I3, I3en
Accelerated computing	F1, G4, Inf1, P3, P3dn

Supported Non-Nitro Instance Types

VPC Traffic Mirroring is available on the following non-Nitro instance types:

Purpose	Instance types
General purpose	M4

Compute optimized	C4
Memory optimized	R4, X1, X1e
Storage optimized	D2, H1
Accelerated computing	G3. G3s, P2

Configure Tokens

You must configure tokens for registering GigaVUE Fabric Components using Third Party Orchestration and registering UCT-V with GigaVUE-FM.

This feature verifies the identity of a user for accessing the GigaVUE-FM REST APIs by generating tokens.

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 copy the generated tokens from the GUI, which can be used to access the REST APIs. Token inherits the Role-Based Access (RBAC) privilege (read or write) of the user groups assigned to a particular user.

GigaVUE-FM enables the generation of multiple tokens and associates them with the corresponding user groups. If you have GigaVUE-FM Security Management privileges with write access, you can revoke other users' tokens but not view the created tokens.

Prerequisite

You must create user groups in GigaVUE-FM. For details, refer to Configure Role-Based Access for Third Party Orchestration.

Rules and Notes

- Authentication using a token is an additional mechanism to access GigaVUE-FM REST APIs, and it does not replace the existing GigaVUE-FM authentication mechanism.
- Only authenticated users can create tokens.
- The token expires or becomes invalid under the following circumstances:
  - Based on the configured value for expiry:
    - Default value: 30 days
    - Maximum value: 105 days
  - Deleting a related user group that exists as part of the token leads to deletion of the corresponding token.
  - A password change for the user(local) deletes the corresponding token.
    - A change in the authentication type deletes all the tokens.
- During the back up and restoration of GigaVUE-FM, previously generated tokens are not available.
- In FMHA role changeover, active GigaVUE-FM tokens are active.

- For basic authentication, activities such as creating, revoking, and reviewing of Token APIs are restricted.
- For expired or invalid tokens, you notice the error code 401 on GigaVUE-FM REST API access.

This section explains about the following:

- Create Token
- Revoke Tokens
- Export Token
- Configure Tokens

Create Token

GigaVUE-FM allows you to create a token or multiple tokens if required.

To create a token, 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. You can copy and use the generated token to authenticate the GigaVUE-FM REST APIs.

Copy and Paste a Token

1. Select the token that you want to copy.
2. Select **Actions>Copy Token.**

   The token is copied.
3. Paste the copied token in the required areas.

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

Revoke Tokens

You can revoke tokens that other users create.

Prerequisite: Write access in GigaVUE-FM Security Management.

To revoke tokens,

1. Go to , select **Authentication** > **GigaVUE-FM User Management**.
2. In the **User Management** page, select **Tokens**.
3. From the drop-down, select **Token Management**. You can view the created tokens.
4. Select the token that you want to revoke.
5. Select **Action> Revoke**.

Export Token

GigaVUE-FM allows you to export selected or all the tokens in CSV and XLSX format.

- To export a token, select the token, select the **Export Selected** drop-down list box, and then select the **CSV** or **XLSX** format as per requirement.
- To export all the tokens, select the token, select the **Export All** drop-down list box, and then select the **CSV** or **XLSX** format as per requirement.

GigaVUE-FM Version Compatibility

GigaVUE-FM version 6.14.00 supports the latest version (6.14.00) of GigaVUE V Series Node, GigaVUE V Series Proxy, UCT-V Controller, and UCT-V, as well as (n-2) versions. For better compatibility, we recommend to use the latest version of fabric components with GigaVUE-FM.

Default Login Credentials for GigaVUE Fabric Components

Using the default credentials, you can login to the GigaVUE V Series Node, GigaVUE V Series proxy, and UCT-V Controller.

Product	Login credentials
GigaVUE V Series Node	You can login to the GigaVUE V Series Node by using ssh. The default username and password are: • Username: gigamon • Password: Use the SSH key.
GigaVUE V Series proxy	You can log in to the GigaVUE V Series proxy by using ssh. The default username and password are:

Product	Login credentials
	• Username: gigamon • Password: Use the SSH key.
UCT-V Controller	You can log in to the GigaVUE V Series proxy by using ssh. The default username and password are: • Username: gigamon • Password: Use the SSH key.

Permissions and Privileges (AWS)

GigaVUE-FM requires access to AWS EC2 APIs to deploy the solution. IAM allows you to control the actions that GigaVUE-FM can take on your EC2 resources.

To configure the components,

1. Enable the permissions listed below and attach the policies to an IAM role.
2. Attach the IAM role to the GigaVUE-FM instance running in AWS.

   If the GigaVUE-FM is running outside the AWS, then you must use the access key id and secret access keys.

   For details, refer to IAM roles for Amazon EC2.

The following topics list the minimum permissions that are required for traffic acquisition:

- Prerequisites
- Minimum Permissions Required for Inline Policies and Basic Authentication
- Minimum Permissions Required for Acquiring Traffic using Inline V Series
- Check for Required IAM Permissions

Refer to Deployment Options for GigaVUE Cloud Suite for AWS using GigaVUE-FM Orchestration and Deployment Options for GigaVUE Cloud Suite for AWS - Integrated Mode topics for other required permission details based on the traffic Acquisition methods.

GigaVUE-FM Instance Multi Account Support Using Amazon STS

This topic provides instructions on how to set up your GigaVUE-FM instance to work with multiple accounts using Amazon Security Token Service (STS).

Prerequisites

You must complete the following prerequisites before configuring GigaVUE-FM for Amazon STS support.

- Include a policy in other accounts as well.
  - These policies must allow GigaVUE-FM to assume the role in that account.

Procedure

For the purposes of these instructions, the AWS account that runs the GigaVUE-FM instance is called the source account, and any other AWS account that runs monitored instances is called a target account.

To configure GigaVUE-FM for Amazon STS support:

1. In each target account, perform the following steps:
   a. Create an IAM role with the source account number as a trusted entity.
   b. Attach policies with permissions allowing GigaVUE-FM to perform its functions.
   c. Record the ARN of each role created.

   NOTE: This role must exist in all accounts to support the ability to create a single Monitoring Domain in GigaVUE-FM that includes multiple accounts.

2. In the source account, create a new IAM policy that allows GigaVUE-FM to retrieve IAM policies.
   Example:

   a. Use the following permissions if you are using the IAM instance role for authentication:

   ```
   "iam:ListAttachedRolePolicies",
   "iam:GetPolicy",
   "iam:GetPolicyVersion",
   "iam:ListRolePolicies",
   "iam:ListAccountAliases",
   ```

   If inline policies are linked to the role, then include the following permission:

   ```
   "iam:GetRolePolicy"
   ```

   b. Use the following permissions for basic authentication:

   ```
   "iam:ListGroupsForUser"
   "iam:ListAttachedUserPolicies"
   "iam:ListAttachedGroupPolicies"
   "iam:GetPolicy",
   "iam:GetPolicyVersion",
   "iam:ListUserPolicies"
   "iam:ListGroupPolicies"
   "iam:ListAccountAliases",
   ```

   If inline policies are attached to the user, then include the following permission:

   ```
   "iam:GetUserPolicy"
   ```

   If inline policies attached to the user group, then include the following permission:

   ```
   "iam:GetGroupPolicy"
   ```

3. In the source account, create a new IAM policy that allows the "sts:AssumeRole" action on all role ARNs created in Step 1.
   IMPORTANT: The following example is provided as an example:

   ```
   {    "Version": "2012-10-17",    "Statement": {        "Effect": "Allow",
   "Action": "sts:AssumeRole",      "Resource": [
   "arn:aws:iam::123456789012:role/FM-Role-target-account"         ]        }    }
   ```

   NOTE: In this example, 123456789012 is a target account and FM-Role-target-account is the role in the target account configured in step 1 with permissions required for GigaVUE-FM.

4. In the source account, attach the policies created in steps 2 and 3 to the IAM role that is attached to the GigaVUE-FM instance.

Minimum Permissions Required for Inline Policies and Basic Authentication

This section provides information on the permissions that are required to use IAM instance role for inline policies, authentication and basic authentication.

IAM instance role for authentication

Use the following permissions if you are using the IAM instance role for authentication:

```
"iam:ListAttachedRolePolicies",
"iam:GetPolicy",
"iam:GetPolicyVersion",
"iam:ListRolePolicies",
"iam:ListAccountAliases",
```

IAM permissions required for Basic Authentication

```
"iam:ListGroupsForUser"
"iam:ListAttachedUserPolicies"
"iam:ListAttachedGroupPolicies"
"iam:GetPolicy",
"iam:GetPolicyVersion",
"iam:ListUserPolicies"
"iam:ListGroupPolicies"
"iam:ListAccountAliases",
```

Check for Required IAM Permissions

GigaVUE-FM validates whether the policy attached to theGigaVUE-FM using EC2 Instance Role or Access Credential has the required IAM permissions and notifies users about missing permissions. While creating the Monitoring Domain and deploying GigaVUE Fabric Components using GigaVUE-FM, you can check permissions. To check, select the **Check Permissions** button on the **Monitoring Domain Configuration** page and **AWS Fabric Launch Configuration** page. The GigaVUE-FM displays the minimum required IAM permissions.

Prerequisites to deploy GigaVUE Cloud Suite for AWS

- **IAM permissions**: Check whether the GigaVUE-FM instance has the minimum required permissions. For details on how to configure the required permissions in AWS, refer to Permissions and Privileges (AWS).
- **Access to public cloud end points:** Check for access to the AWS cloud end point APIs.
- **Subscription to the GigaVUE Cloud Suite for AWS**: Before deploying the solution, subscribe to the GigaVUE Cloud Suite components from the AWS marketplace. It checks whether whether you have subscribed to the required components in the marketplace. For details, refer to Subscribe to GigaVUE Products.
- **Security Group**: Checks whether the required ports are configured in the security group. For more information, see Subnet and Security Group for Amazon VPC

> **NOTE:** Security group rules validation does not validate prefix List and user groups. For a successful validation, update the ports and CIDR range in the Security Group.

After you press the **Check Permissions** button, GigaVUE-FM verifies the minimum required permissions. Any missing permission is highlighted with the respective message against the permission in a dialog box. You can use the displayed IAM Policy JSON as a reference and update the policy that is attached to the GigaVUE-FM.

Refer to the following sections for more detailed information:

- Check Permissions while Creating a Monitoring Domain
- Check Permissions while Configuring GigaVUE Fabric Components using GigaVUE-FM

Install GigaVUE-FM on AWS

You can subscribe to GigaVUE-FM in the marketplace and launch in AWS.

Refer to the following topics for instruction on installing GigaVUE-FM in AWS:

- Subscribe to GigaVUE-FM
- Initial Configuration

Subscribe to GigaVUE-FM

You can deploy the GigaVUE Cloud Suite for AWS from the AWS Marketplace.

> **NOTE:** Only users with **aws-marketplace:ViewSubscriptions** permission in their IAM policy can subscribe to GigaVUE products.

To subscribe to the GigaVUE-FM, perform the following steps:

1. Log in to your AWS account.
2. Go to AWS Marketplace: https://aws.amazon.com/marketplace/.
3. In the **Search** field, type Gigamon and select **Search**.
4. Select the latest version GigaVUE Cloud Suite BYOL version. For details, refer to Licensing.
5. Select **View Purchase Options**. The terms and condition page is displayed.
6. Review the Terms and Conditions and select **"Accept Terms**".
7. Review the summary and then select **Continue to Configuration**.
8. In the **Configure this software** page, enter the following details for your deployment:
   a. Set **Fulfillment Option** to the default value.
   b. Select the latest version in the **Software Version** field.
   c. Choose your deployment **Region**.
   d. Select **Continue to Launch.**

9. In the **Configure this software** page, perform the following:
    a. In the **Choose Action** field, select the **Launch from Website** option.
    b. From the **EC2 Instance Type** drop-down list, select the instance type. Refer to Recommended and Supported Instance Types for AWS.
    c. From the **VPC Settings** drop-down list, select the VPC for deploying GigaVUE-FM.
    d. In the **Subnet Settings**, select your desired Subnet.
    e. In the **Security Group Settings**, configure the security group to match your access and permissions needs. For details, refer to Security Group.
    f. Select your preferred **Key Pair** for secure access to the instance.
    g. In the **Advanced details** section, select **V2 only (token required)** from the Metadata version drop-down list.
    h. Select **Launch**.

For details, refer to Launch an instance using defined parameters in AWS documentation.

GigaVUE-FM is launched in AWS. You must perform the initial configuration to view the GigaVUE-FM UI.

Initial Configuration

It may take several minutes for the GigaVUE-FM instance to start up. Once it is up and running, perform the following steps to verify:

1. In your EC2 Instances page, select the **Instance ID** of the launched GigaVUE-FM to view the instance information.
2. Copy and paste the **Public IP address** into a new browser window or tab. The GigaVUE-FM GUI appears.

NOTE:

- If GigaVUE-FM is deployed inside AWS, use **admin** as the username and the **Instance ID** as the default password for the admin user to login to GigaVUE-FM, (Ex: i-079173111e2d73753). You can get the **Instance ID** of GigaVUE-FM in the EC2 Instances page.
- If GigaVUE-FM is deployed outside the AWS, use admin123A!! as the default admin password.

When you first log in to GigaVUE-FM, you are asked to change your default password.

What to do Next:

Configure the required permission and privileges in AWS. For detailed instructions on configuring required AWS permissions and privileges for your chosen deployment option, refer to the following topics:

Deployment Options	Reference Topics
Acquire Traffic using UCT-V	Acquire Traffic using UCT-V - GigaVUE-FM Orchestration
Acquire Traffic using Customer Orchestrated Source	Acquire Traffic using Customer Orchestrated Source - GigaVUE-FM Orchestration
Acquire Traffic using Customer Orchestrated Source when configuring Gateway Load Balancer in AWS	Acquire Traffic using Customer Orchestrated Source with Gateway Load Balancing
Acquire Traffic using Customer Orchestrated Source when configuring Network Load Balancer in AWS	Acquire Traffic using Customer Orchestrated Source with Network Load Balancer
Acquire Traffic using Traffic Mirroring	Acquire Traffic using Traffic Mirroring – GigaVUE-FM Orchestration
Acquire Traffic using Traffic Mirroring when configuring Gateway Load Balancer in AWS	Acquire Traffic using Traffic Mirroring with Gateway Load Balancing
Acquire Traffic using Traffic Mirroring when configuring Network Load Balancer in AWS	Acquire Traffic using Traffic Mirroring with Network Load Balancer

Upgrade GigaVUE-FM in AWS

This chapter describes how to upgrade the GigaVUE-FM instance deployed in AWS. GigaVUE-FM deployed in AWS can be upgraded in two ways. Refer to the following sections for more detailed information:

- Upgrade GigaVUE-FM
- Upgrade GigaVUE-FM using Snapshot in AWS

IMPORTANT:

- When you are upgrading GigaVUE-FM to 6.13, you must upgrade all fabric components within **30** days of upgrading GigaVUE-FM to ensure version compatibility before the next UCT-V certificate renewal. Complete the following upgrades immediately after the GigaVUE-FM upgrade to ensure that UCT-V certificates renew only after all components are running compatible versions, reducing the risk of registration or communication failures:
  - UCT-V Controller
  - UCT-V's
  - GigaVUE V Series Node

- GigaVUE V Series Proxy

Upgrade GigaVUE-FM

This section describes the steps to upgrade GigaVUE-FM from the UI. You can upgrade by using an image that is located on an external image server, or you can use GigaVUE-FM as the image server.

Keep in mind the following rules and notes before you upgrade GigaVUE-FM from the UI:

- When using the GigaVUE-FM UI to upgrade GigaVUE-FM, you can only upgrade to the currently available version or to the next version. You cannot downgrade.
- When using the Firefox browser, clear the cache before upgrading to prevent issues with the browser.
- When upgrading GigaVUE-FM to the latest image file, the upgrade operation will fail if GigaVUE-FM already has three image files. Delete the unused image files before proceeding to download a new image file.

  NOTE: You can enable auto-purge of GigaVUE-FM images using an API. Contact Gigamon Technical Support for assistance.

- Starting from software version 5.15.00, subsequent GigaVUE-FM upgrade operation to higher versions deletes the upgraded GigaVUE-FM image file irrespective of the completion status. For example, when upgrading from 5.15.00 to 5.16.00, irrespective of whether the upgrade process fails or succeeds, GigaVUE-FM deletes the 5.16.00 image file at the end of the upgrade process.

Upgrade from External Image Server

This section provides the steps for upgrading the GigaVUE-FM from an image stored on an external server. The image can be transferred from the server to the GigaVUE-FM using SCP.

To upgrade with an image stored on an external image server, do the following:

1. Upload the image to the external image server to make it available to GigaVUE-FM.

   To obtain software images, register on the Gigamon Customer Portal and download the software.

2. Add the image server to GigaVUE-FM. This stores the credentials, image file name, and IP address of the server on GigaVUE-FM.

   To add the image server:

   a. Go to **Settings**.

   b. Select **System** on the left navigation panel and go to **Images > External Servers**. The External Servers page appears.

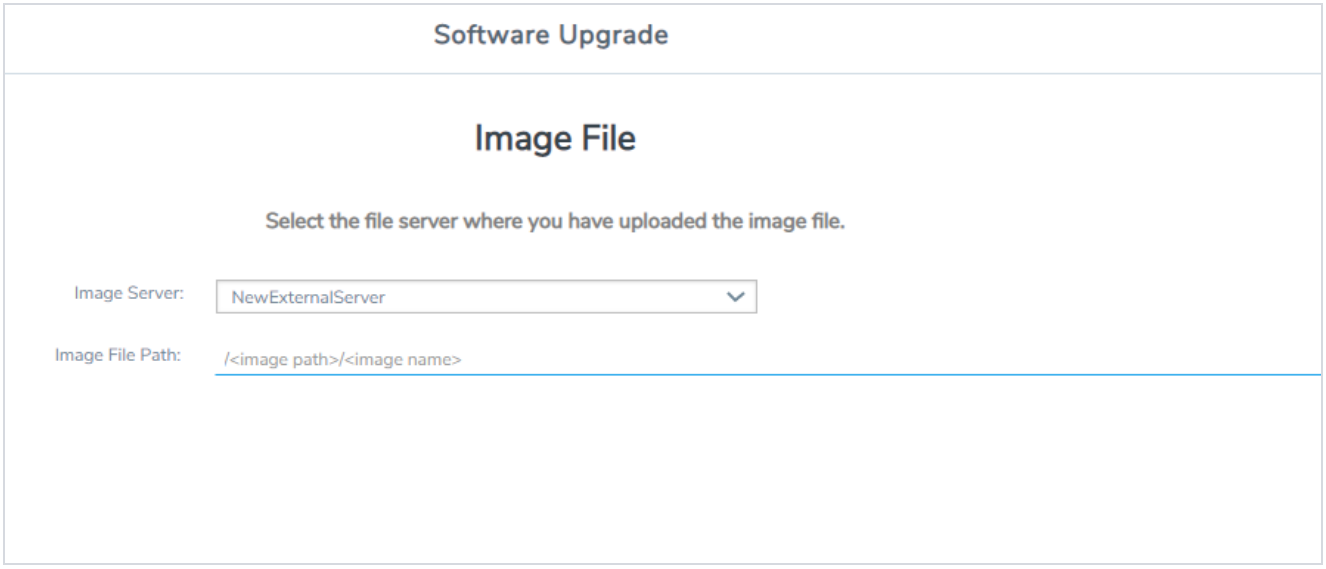
   c. Click **Add**. The Add External Server page appears.

d. On the Images Server page, specify the following:

- An alias to help identify the image server.
- The host IP address of the server.
- The protocol to use for the download: SCP
- The user name and password.

e. Click **Save**.

The External Server page displays the newly added external server. From the **Admin** drop-down list in the top right corner of the window, select **Upgrade** to open the GigaVUE-FM Image Upgrade page as shown in the following figure.



To monitor the progress and status of the upgrade, click "GigaVUE Administration Guide".

3. On the GigaVUE-FM Image Upgrade page, click on the Image Server field and select the server added in Step 2.
4. In the Image File Path, enter the image path and filename on the external file server.
5. Upgrade any deployed GigaVUE Cloud Suite-VMs.

   After upgrading GigaVUE-FM, you must also upgrade any deployed GigaVUE Cloud Suite-VMs. Otherwise, maps may not work and the GigaVUE Cloud Suite-VMs will be unreachable. For information about upgrading GigaVUE Cloud Suite-VM, refer to the *"Bulk Upgrading GigaVUE-VM Nodes"* section in the *GigaVUE Cloud Suite Deployment Guide - VMware*.

Upgrade with GigaVUE-FM as the Image Server

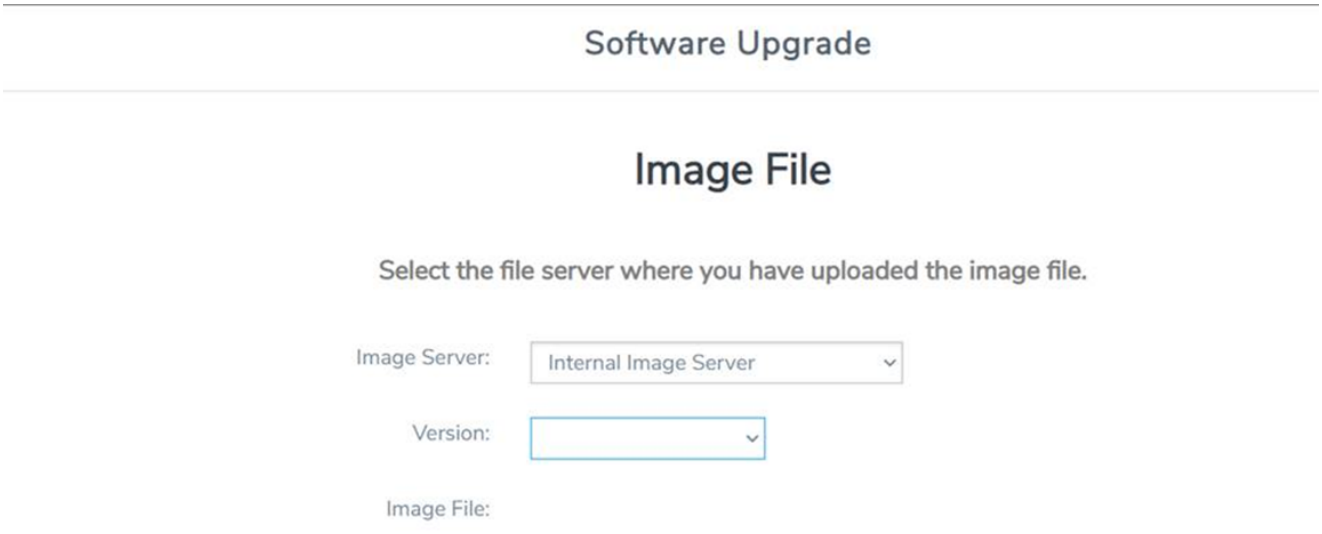
This section provides the steps for upgrading GigaVUE-FM when GigaVUE-FM is used as the file server.

To upgrade a GigaVUE-FM using internal image files, perform the following:

1. Download the images from the Gigamon website and store them in the instance where GigaVUE-FM is installed.

   To obtain software images, register on the Gigamon Customer Portal and download the software.
2. Upload the images file to GigaVUE-FM.
   a. Go to **Settings** and select to **System > Images > Internal Image Files**.
   b. On the Internal Image File page, click **Upload**.
   c. Click **Browse** to locate the image file.
   d. Click **OK** to upload the file. The page displays the progress of the upload.

   After the upload completes, you can see the GigaVUE-FM image to use for the upgrade on the Internal Images Files page.
3. Click the **Admin** drop-down list on the top right of the window and select **Upgrade**.
4. On the GigaVUE-FM Image Upgrade page, click in the **Image Server** field and select **Internal Image Server**.



5. From the **Version** drop-down list, select the version to which you are upgrading.

> **NOTE:** You can only upgrade to another instance of the current version or the immediate next version. Downgrading to a lower version is not supported through the UI.

6. Click **Upgrade**.

   > **NOTE:** When you change the IP address of the GigaVUE-FM instance using the jump-start configuration, the internal database and the in-memory caches of the GigaVUE-FM instance are not updated. The Database continues to have the IP address of the old GigaVUE-FM, and the image upgrade using the internal server option does not work. To fix this, you must restart the GigaVUE-FM instance after upgrade.

   After upgrading GigaVUE-FM, you must also upgrade any deployed GigaVUE-VMs. Otherwise, maps may not work and the GigaVUE-VMs will be unreachable. For information about upgrading GigaVUE-VM, refer to the "*Bulk Upgrading GigaVUE-VM Nodes*" section in the *GigaVUE Cloud Suite Deployment Guide - VMware*.

> **NOTE:** If you are using FireFox, clear the cache before upgrading to prevent issues with the browser.

Upgrade GigaVUE-FM using Snapshot in AWS

This chapter describes how to upgrade the GigaVUE-FM instance deployed on AWS using snapshot:

- At a Glance
- Stop GigaVUE-FM Instance
- Create Snapshot of the GigaVUE-FM Instance
- Upgrade GigaVUE-FM Instance

At a Glance

To upgrade the GigaVUE-FM instance successfully, you must perform the following steps:

Step 1: Stop the existing version of the GigaVUE-FM instance.

Step 2: Create a snapshot of the second disk (dev/sdb) of the GigaVUE-FM instance.

Step 3: Make a note of the snapshot ID.

Step 4: Launch the latest version of the GigaVUE-FM instance. While launching the latest version, enter the snapshot ID of the old version of the GigaVUE-FM instance in **Add Storage** > **Add New Volume**.

Step 5: Complete the launch.

Step 6: Verify if the data from the previous GigaVUE-FM instance is restored in the new instance.

Step 7: Terminate the old GigaVUE-FM instance.

Stop GigaVUE-FM Instance

Before upgrading the GigaVUE-FM instance, the existing version of the GigaVUE-FM instance must be stopped.

> **NOTE:** Do not terminate the GigaVUE-FM instance.

To stop the GigaVUE-FM instance:

1. Login to the AWS account and select **Services > EC2**.
2. In the left navigation pane, select **Instances**.
3. In the search field, enter the name of the existing GigaVUE-FM instance and select the Instance ID.

> **NOTE:** If the instance ID is the password for logging in to the existing GigaVUE-FM, make note of this instance ID. This instance ID will be used as the password for logging in to the upgraded GigaVUE-FM as well. If the password is changed, use the changed password to login to the upgraded GigaVUE-FM.

4. Go to **Actions** > **Instance State** > **Stop**.

Create Snapshot of the GigaVUE-FM Instance

You must create a snapshot of the volume of the existing version (dev/sdb) of the GigaVUE-FM instance. Snapshots capture data that are written to your Amazon EBS volume at the time the snapshot is taken. This excludes any data that are cached by any applications or the operating system.

To create a snapshot:

1. Select the GigaVUE-FM instance and click the **Description** tab.
2. Scroll down and locate Block Devices.
3. Click the **/dev/sdb** link. The Block Device dialog box is displayed with the volume ID link.
4. In the Block Device dialog box, click the volume ID link. The Volumes page is displayed.
5. Click **Actions** and select **Create Snapshot.**

   The Create Snapshot dialog box is displayed.
6. In the Create Snapshot dialog box, enter the following information:

Table 1: Fields for Creating a Snapshot

Field	Description
Name	The name of the snapshot.
Description	The description of the snapshot.

7. Click **Create**. It will take several minutes for the snapshot to be created.

NOTE: Make a note of the snapshot ID. This snapshot ID will be used to find the snapshot and add the volume while upgrading the GigaVUE-FM instance.

Upgrade GigaVUE-FM Instance

While upgrading the GigaVUE-FM instance, the Amazon EBS volume must be restored with the data from the snapshot that is created in Create Snapshot of the GigaVUE-FM Instance.

To upgrade the GigaVUE-FM instance:

1. Select **Services > EC2**.
2. Click **LaunchInstance** and go to **AWS Marketplace** or **Community AMIs**.
3. Search for **Gigamon**, locate the latest version of the GigaVUE-FM AMI, and click **Select**.
4. Choose the Instance Type. The recommended instance type is **m4.xlarge**.

NOTE: Do not select the t2 instance types as they are not supported.

5. Click **Next:Configure Instance Details.**
6. Enter the following information.
   - **Network**— Select the VPC where you want to launch the AMI.
   - **Subnet**— Select the management subnet that the instance will use after launch. (Required)
   - **Auto-assign Public IP**— Select **Enable**.
   - **IAM role**—Select an existing IAM role to associate with the instance. Refer to the *GigaVUE Cloud Suite for AWS Quick Start Guide*.
7. Click **Configure storage** and then click **Advanced**.
8. Select **Volume 2** and then select the Snapshot that you created in Create Snapshot of the GigaVUE-FM Instance.
9. Click **Next: Tag Instance,** and then add a key-value pair to identify the instance.

10. Click **Next: Add Security Group**. Click the **Select an existing security group** check box if the security group is already created. Otherwise, select the **Create a new security group** check box and click **Add Rule**. For more information on creating a security group, refer to the *Security Group* section in GigaVUE Cloud Suite Deployment Guide - AWS.
11. Click **Review and Launch**. Review the instance launch details and click **Launch**.
12. Select the SSH key pair, check the acknowledgment check box, and click **Launch Instances**.
13. It will take several minutes for the instance to initialize. After the initialization is completed, verify the instance through the Web interface as follows:
    a. Find the instance and expand the page in the **Descriptions** tab to view the instance information, if necessary.
    b. Copy the Public DNS value and paste the value into a new browser window or tab.
    c. Copy the Instance ID of the previous version of the GigaVUE-FM. If the password is changed, use the changed password to login to the upgraded GigaVUE-FM.

NOTE: Do not have multiple versions of GigaVUE-FM instances monitoring the same AWS connection.

Launch the new version of the GigaVUE-FM instance. Verify if the data from the previous GigaVUE-FM instance is restored in the new instance. Once the data is verified, terminate the old version of the GigaVUE-FM instance.

Upgrade GigaVUE Fabric Components in GigaVUE-FM for AWS

This chapter describes how to upgrade UCT-V Controller, GigaVUE V Series Proxy and GigaVUE V Series Nodes.

Refer to the following topic for more information:

- Prerequisite
- Upgrade UCT-V Controller
- Upgrade GigaVUE V Series Nodes and GigaVUE V Series Proxy

Prerequisite

Before you upgrade the GigaVUE V Series Proxy and GigaVUE V Series Nodes, you must upgrade GigaVUE-FM to software version 5.13 or above.

Upgrade UCT-V Controller

NOTE: UCT-V Controllers cannot be upgraded. Only a new version that is compatible with the UCT-V's version can be added or replaced in the **AWS Fabric Launch Configuration** page.

UCT-V Controller version can be changed in the following two ways:

- Upgrade between Major Versions
- Upgrade within the Same Major Version

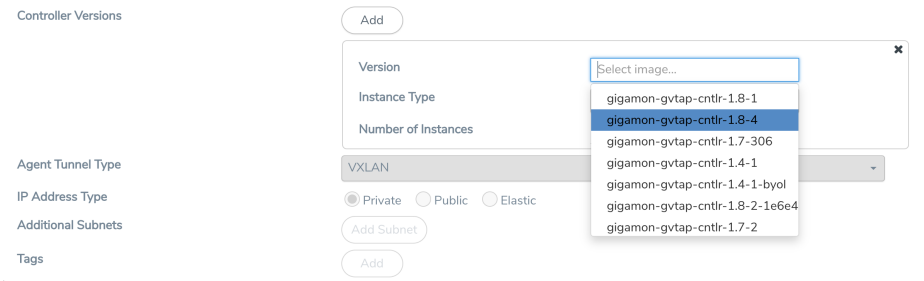
To change the UCT-V Controller version follow the steps given below:

Upgrade between Major Versions

To upgrade between the major versions of UCT-V Controller, you must add the new version of the UCT-V Controller and remove the existing version.

NOTE: You can only add UCT-V Controllers which has different major versions. For example, you can only add UCT-V Controller version 6.8.00 if your existing version is 6.9.00.

1. Go to **Inventory > VIRTUAL > AWS**.
2. Click **Actions > Edit Fabric**. The **AWS Fabric Launch Configuration** page appears.
3. Under **Controller Versions**, click **Add**.
4. From the **Version** drop-down list, select a UCT-V Controller image that matches with the version number of UCT-Vs installed in the instances.
5. From the **Instance Type** drop-down list, select a size for the UCT-V Controller.
6. In **Number of Instances**, specify the number of UCT-V Controllers to launch. The minimum number you can specify is 1.



You cannot modify the **IP Address Type** and the **Additional Subnets** details, provided at the time of UCT-V Controller configuration.

After installing the new version of UCT-V Controller, follow the steps given below:

1. Install UCT-V with the version same as the UCT-V Controller or upgrade the UCT-V to the same version as the UCT-V Controller. Refer to Configure UCT-V for more detailed information on how to install or upgrade UCT-V.
2. Delete the UCT-V Controller with older version.

Upgrade within the Same Major Version

This is only applicable if you wish to change your UCT-V Controller version from one minor version to another within the same major version. For example, from 6.10.00 to 6.10.01.

1. Go to **Inventory > VIRTUAL > AWS**.
2. Click **Actions > Edit Fabric**. The **AWS Fabric Launch Configuration** page appears.
3. Under **Controller Versions**, select a UCT-V Controller image within the same major version from the **Version** drop-down list.
4. Specify the **Number of Instances**. The minimum number you can specify is 1.
5. Select the **Subnet** from the drop-down.

You cannot modify the rest of the fields.

Upgrade GigaVUE V Series Nodes and GigaVUE V Series Proxy

GigaVUE-FM lets you upgrade GigaVUE V Series Proxy and GigaVUE V Series Nodes at a time.

There are two ways to upgrade the GigaVUE V Series Proxy and Nodes. You can:

- Launch and replace the complete set of nodes and proxy at a time.

  For example, if you have 1 GigaVUE V Series Proxy and 10 GigaVUE V Series Nodes in your VPC, you can upgrade all of them at once. First, the new version of GigaVUE V Series Proxy is launched. Next, the new version of GigaVUE V Series Nodes is launched. Then, the old version of V Series Proxy and Nodes are deleted from the VPC.

  NOTES:
  - When the new version of nodes and proxy are launched, the old version is not deleted by GigaVUE-FM until the new version of node and proxy is launched and the status is changed to **Ok**. Make sure that the instance type of the node and proxy selected during the configuration can accommodate the total number of new and old fabric components present in the VPC. If the instance type cannot support so many Virtual Machines, you can choose to upgrade the fabric components in multiple batches.
  - If there is an error while upgrading the complete set of proxy and nodes present in the VPC, the new version of the fabric is immediately deleted and the old version of the fabric is retained as before.

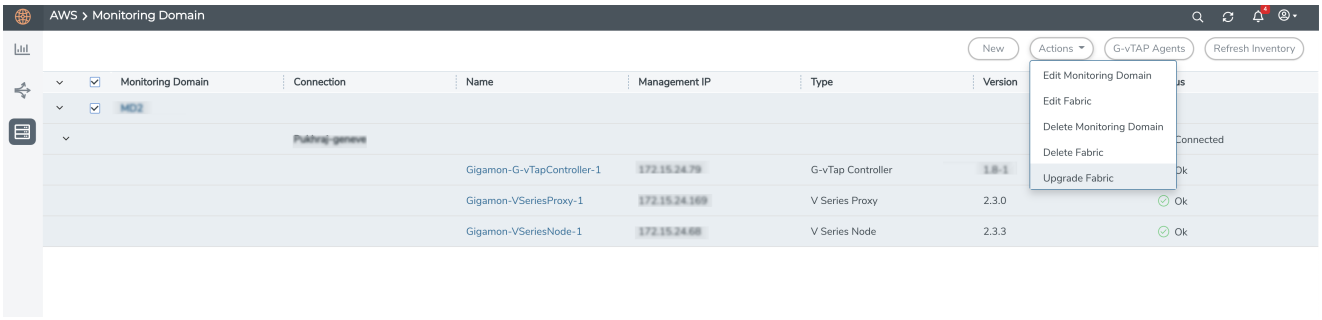
- Prior to upgrading the GigaVUE V Series Proxy and Nodes, you must ensure that the required number of free addresses are available in the respective subnets. Otherwise, the upgrade will fail.

- Launch and replace the nodes and proxy in multiple batches.

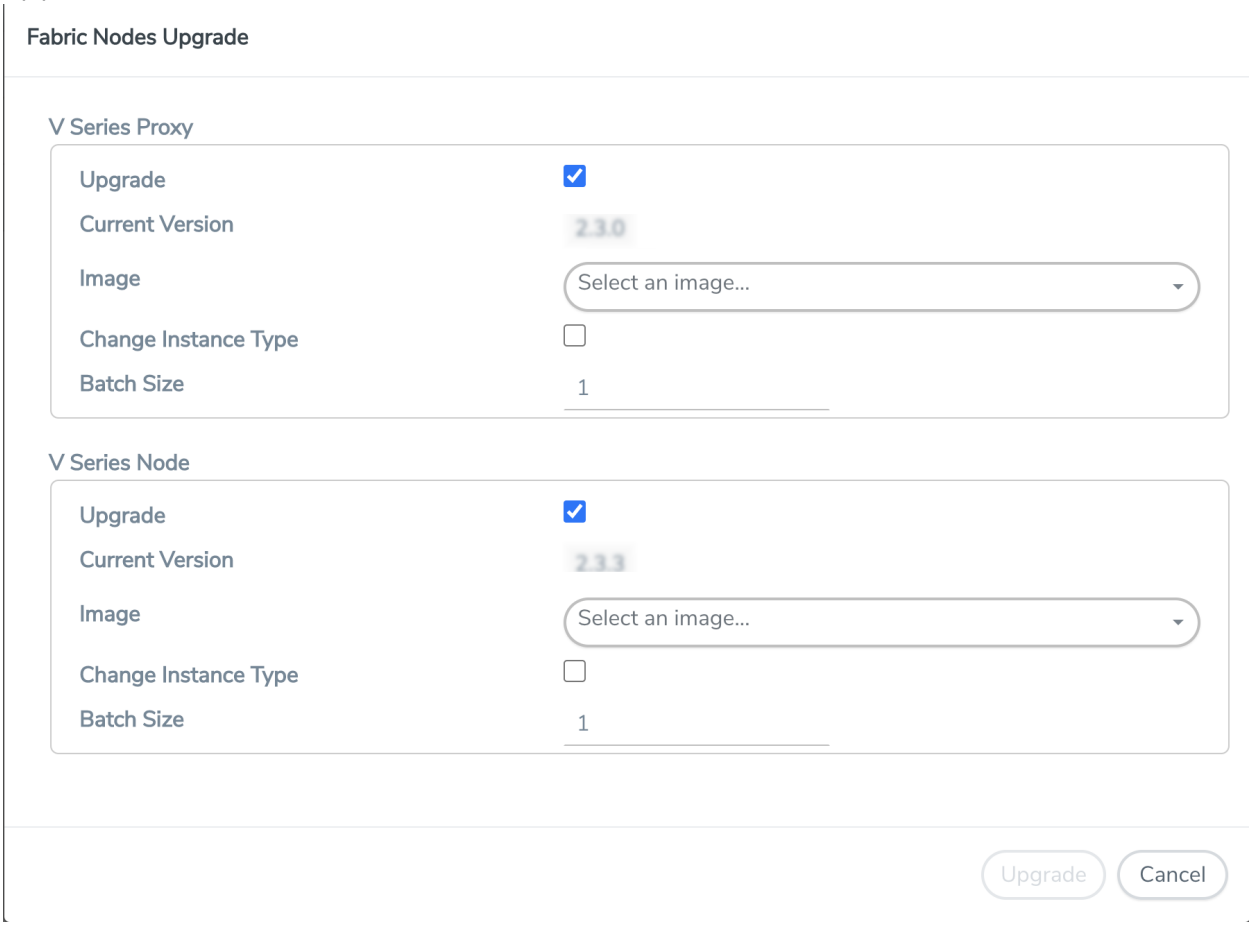
  For example, if there are 18 GigaVUE V Series Nodes to be upgraded, you can specify how many you want to upgrade per batch.

To upgrade the GigaVUE V Series Proxy and GigaVUE V Series Nodes:

1. Go to **Inventory > VIRTUAL > AWS** , and then click **Monitoring Domain**. The Monitoring Domain page appears.
2. On the Monitoring Domain page, select the connection name check box and click **Actions**



3. Select **Upgrade Fabric** from the drop-down list. The **Fabric Nodes Upgrade** page appears.



4. To upgrade the GigaVUE V Series Nodes or Proxy, select the **Upgrade** checkbox.
5. From the **Image** drop-down list, select the latest version of the GigaVUE V Series Proxy or Nodes.
6. Select the **Change Instance Type** checkbox to change the instance type of the nodes or proxy, only if required.
7. To upgrade the GigaVUE V Series Nodes or Proxy, specify the batch size in the **Batch Size** box.

   For example, if there are 7 GigaVUE V Series Nodes, you can specify 7 as the batch size and upgrade all of them at once. Alternatively, you can specify 3 as the batch size, and launch and replace 3 V Series Nodes in each batch. In the last batch, the remaining 1 V Series Node is launched.
8. Click **Upgrade**.

   The upgrade process takes a while depending on the number of GigaVUE V Series Proxy and Nodes upgrading in your AWS environment. First, the new version of the

GigaVUE V Series Proxy is launched. Next, the new version of GigaVUE V Series Nodes is launched. Then, the older version of both is deleted from the project. In the V Series Proxy page, click the link under Progress to view the upgrade status.

Once the nodes are upgraded successfully, the Monitoring Session is re-deployed automatically.

Upgrade GigaVUE Fabric Components using Third Party Orchestration

In a Third Party Orchestration deployment method, you cannot upgrade directly. To upgrade the fabric components, you must replace the existing version with the latest version. This process requires reinstallation and reconfiguration of the entire setup to ensure compatibility with the updated version.

We recommend backing up all necessary configurations and data before initiating this process to prevent any potential data loss.

Key Considerations for Upgrade

Consider the following when upgrading the GigaVUE-FM to 6.1.00 or higher version (when using third party orchestration to deploy fabric components):

When upgrading GigaVUE-FM to any version higher than 6.0.00, if the GigaVUE V Series Nodes version deployed in that GigaVUE-FM is lower than or equal to 6.0.00, then, for the seamless flow of traffic, GigaVUE-FM automatically creates **Users** and **Roles** in GigaVUE-FM with the required permission.

For the user created in GigaVUE-FM,

- Username: **orchestration**
- Password: **orchestration123A!**.

  Verify that the username **orchestration** does not belong to another user in GigaVUE-FM.

After the upgrade, we recommend changing the password on the Users page. For details, refer to Configure Role-Based Access for Third Party Orchestration.

Deploy

Deploy GigaVUE Cloud Suite for AWS using GigaVUE-FM Orchestration

This section describes various options to configure GigaVUE Cloud Suite for AWS to provide visibility for both physical and virtual traffic. You can configure GigaVUE Cloud Suite for AWS in ten different ways, based on the traffic acquisition method and your approach to deploying fabric components.

Different deployment options for GigaVUE Cloud Suite for AWS based on the Traffic Acquisition Method

Refer to the following topics for detailed information:

- Acquire Traffic using UCT-V - GigaVUE-FM Orchestration
- Acquire Traffic using Traffic Mirroring – GigaVUE-FM Orchestration
- Acquire Traffic using Traffic Mirroring with Network Load Balancer
- Acquire Traffic using Traffic Mirroring with Gateway Load Balancing
- Acquire Traffic using Customer Orchestrated Source - GigaVUE-FM Orchestration
- Acquire Traffic using Customer Orchestrated Source with Network Load Balancer
- Acquire Traffic using Customer Orchestrated Source with Gateway Load Balancing
- Acquire Traffic using Inline V Series Solution

Acquire Traffic using UCT-V - GigaVUE-FM Orchestration

This section outlines the workflow to acquire traffic with UCT-V and deploy GigaVUE Fabric Components using GigaVUE-FM. Refer to the following topics for instructions on configuring traffic acquisition, processing, and forwarding to your desired destination.

- Install GigaVUE-FM on AWS
- Configure the permissions required in AWS
- Create the AWS Credentials
- Install UCT-Vs
- Create a Monitoring Domain
- Deploy GigaVUE Fabric Components in GigaVUE-FM
- Configure and Deploy Monitoring Session

Install GigaVUE-FM on AWS

This step is optional and applies only when an existing GigaVUE-FM instance is not available.
Refer to Install GigaVUE-FM on AWS for steps to install GigaVUE-FM on AWS and the steps to start GigaVUE-FM instance and configure it.

Configure the permissions required in AWS

If you are using inline policy or basic authentication, then you must update the policy with the relevant IAM service. For details, see Minimum Permissions Required for Inline Policies and Basic Authentication.

These are the minimum permissions that are required to acquire traffic using the UCT-V and authenticate using an IAM instance role.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags",
                "ec2:DeleteTags",
                "ec2:RunInstances",
                "ec2:TerminateInstances",
                "ec2:AssociateAddress",
                "ec2:DisassociateAddress",
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeVolumes",
                "ec2:DescribeAddresses",
                "ec2:RebootInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedRolePolicies",
                "iam:ListAccountAliases",
                "iam:ListRolePolicies",
                "kms:ListAliases",
                "kms:GenerateDataKeyWithoutPlaintext"

            ],
            "Resource": "*"
        }
    ]
}
```

For more information regarding policies and permissions, refer to AWS Documentation.

Create the AWS Credentials

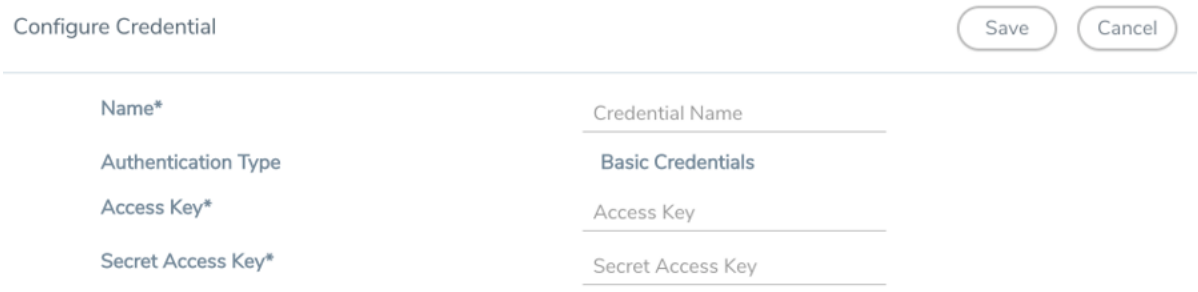
You can monitor workloads across multiple AWS accounts within one Monitoring Domain.

- After launching GigaVUE-FM in AWS, if the IAM is attached to the running instance of FM, then the **EC2 Instance Role** authentication credential is automatically added to the **Credential** page as the default credential. You must attach the IAM prior to creating a Monitoring Domain.
- If you use the **Basic Credentials** authentication credentials, you must add these to the GigaVUE-FM on the **AWS Settings** page, or on the Monitoring Domain creation page.

For details, refer to Create a Monitoring Domain.

To create AWS credentials:

1. Go to **Inventory > VIRTUAL > AWS**, and select **Settings > Credentials**
2. On the **Credential** page, select **Add**. The **Credential Configure** page appears.



3. Enter a name to identify the AWS Credential in the **Name** Field.
4. Basic Credentials is selected as the default **Authentication Type**. For more information, refer to AWS Security Credentials
5. Enter the credential of an IAM user or the AWS account root user in the **Access Key** field.
6. Enter the security password or key in the **Secret Access Key** field.
7. Select **Save**. You can view the list of available credentials on the AWS Credential page.

Install UCT-Vs

You can install UCT-V on both Linux and Windows environments. For details, refer to the following topics:

- Linux UCT-V Installation
- Windows UCT-V Installation

NOTE: If you want to avoid downloading and installing the UCT-Vs every time there is a new instance to be monitored, you can save the UCT-V running on an instance as a private AMI.
To save the UCT-V as an AMI from your EC2 console, right click on the instance and navigate to **Image and Templates** > **Create Image**.

Linux UCT-V Installation

You can install UCT-V on various Linux distributions using Debian or RPM packages.

You must have sudo/root access to edit the UCT-V configuration file. Establish an SSH connection to the virtual machine and ensure you have permission to execute the sudo command.

You may need to modify the network configuration files for dual or multiple network interface configurations to ensure that the extra NIC/Network interface initializes at boot time.

Refer to the following sections:

- Linux Network Firewall Requirements
- Install Linux UCT-Vs
- Register Linux UCT-V

Prerequisites

- UCT-V is a standalone service. By default, most modern Linux operating systems come pre-installed with all the necessary packages for the UCT-V to function without additional configuration.
- Before registering Linux UCT-V, you should generate a token and place it in the **/etc/gigamon-cloud.conf** configuration file. Refer to Configure Tokens.

Linux Network Firewall Requirements

If Network Firewall requirements or security groups are configured in your environment, you must open the following ports for the virtual machine.

Direction	Port	Protocol	CIDR	Purpose
Inbound	9902	TCP	UCT-V Controller IP	Allows UCT-V to receive control and management plane traffic from UCT-V Controller

You can use the following commands to add the Network Firewall rule.

```
sudo firewall-cmd --add-port=9902/tcp
sudo firewall-cmd --runtime-to-permanent
```

Install Linux UCT-Vs

You can install the UCT-Vs either from Debian or RPM packages using one of the following options:.

- Install Linux UCT-Vs using Installation Script

- Install Linux UCT-Vs using Manual Configuration

Refer to the following sections for more detailed information and step-by-step instructions.

Install Linux UCT-Vs using Installation Script

Using installation script, you can complete installation.

Perform the following steps:

1. **To install UCT-V from Ubuntu/Debian:**
    a. Download the UCT-V**6.14.00** Debian (.deb) package from the Gigamon Customer Portal. For assistance, contact Gigamon Technical Support.
    b. Copy this package to your instance and Install the package with root privileges. For example,

    ```
    $ ls gigamon-gigavue-uctv-6.14.00-amd64.deb
    $ sudo dpkg -i gigamon-gigavue-uctv-6.14.00-amd64.deb
    ```

2. **To install UCT-V from RPM, Red Hat Enterprise Linux, and CentOS:**
    a. Download the UCT-V**6.14.00** RPM (.rpm) package from the Gigamon Customer Portal. For assistance, contact Gigamon Technical Support.
    b. Copy this package to your instance and install the package with root privileges. For example,

    ```
    $ ls gigamon-gigavue-uctv-6.14.00-x86_64.rpm
    $ sudo rpm -i gigamon-gigavue-uctv-6.14.00-x86_64.rpm
    ```

3. Use the command given below to perform pre-check, installation, and configuration functionalities.

```
sudo uctv-wizard
```

> **NOTE:** The installation script is not provided with the Debian or RPM packages. You can use the script (installation_wizard.sh/uctv-wizard) only after the UCT-V is installed.

Refer to the table below to know more about **uctv-wizard** command usage options and functionalities:

Options	Use Command	Description
pre-check	sudo uctv-wizard pre-check	Checks the status of the required packages and firewall requirements. • If any package is missing, it displays an appropriate message with the missing package details. • If installation includes all the packages, it displays a success message indicating that UCT-V is ready for configuration.
pkg-install	sudo uctv-wizard pkg-install **NOTE:** The uctv-wizard install command requires access to a repository, either public (internet-based) or local, that hosts prerequisite packages for installation. If no repository is accessible, you must manually install the required packages.	Displays the missing package and version details. To proceed with the installation, you can choose between the following: If you wish to skip the prompts and proceed with the system update, enter your option as **y**. The console interface installs the missing packages and restarts the UCT-V service. Enter **N** if you wish to install it manually. For details, refer to Install Linux UCT-Vs using Manual Configuration.
configure	sudo uctv-wizard configure	First, it checks for any existing configured file in the tmp directory (file named gigamon-cloud.conf in the **C:\Users\<username>\AppData\Local** (Windows) or **/etc/uctv/uctv.conf** (Linux) location). If available, UCT-V uses that configuration. If unavailable, UCT-V automatically adds the interface configuration in uctv.conf file, excluding the loopback (lo) interface, with all permissions enabled (source ingress, source egress, and destination). You can add the required policy for the available port if a firewall is installed. If you wish to skip the prompts to add the

Options	Use Command	Description
		required firewall policy, enter your option as **y**. The console interface adds the firewall rules automatically. Enter **N** if you wish to configure manually. For details, refer to Install Linux UCT-Vs using Manual Configuration section.
uninstall	sudo uctv-wizard uninstall	Automatically stops the UCT-V service, removes the firewall rules, and uninstalls the UCT-V.

Notes:

- Use the command below to view all the log messages generated from uctv-wizard. These log messages are stored at /**var/log/uctv-installation.log**

  ```
  sudo vi /var/log/uctv-installation.log
  ```

- Use the command below to know the usage descriptions for the individual operations.

  ```
  sudo uctv-wizard help
  ```

Linux UCT-V Installation Scenarios

1. **Zero Touch Installation** - When using a cloud-integrated script to deploy UCT-V in a virtual machine, no interference is required as the script installs and configures everything automatically.
2. **One Touch Installation** - When using .deb or .rpm packages with all prerequisite packages in place, UCT-V determines that all dependencies are met. It performs auto-configuration and restarts the service.
3. **Two Touch Installation** - When using .deb or .rpm packages with missing prerequisite packages, the platform displays a warning message about the missing packages. You need to install the missing packages using the **sudo uctv-wizard pkg-install** command.

Install Linux UCT-Vs using Manual Configuration

- Install UCT-V from Ubuntu/Debian Package
- Install UCT-V from RPM, Red Hat Enterprise Linux, and CentOS

Install UCT-V from Ubuntu/Debian Package

To install from a Debian package:

1. Download the UCT-V`6.14.00` Debian (.deb) package from the Gigamon Customer Portal. For assistance contact Gigamon Technical Support.
2. Copy this package to your instance.

3. Install the package with root privileges. For example,

```
$ ls gigamon-gigavue-uctv-6.14.00-amd64.deb
$ sudo dpkg -i gigamon-gigavue-uctv-6.14.00-amd64.deb
```

4. Modify the file **/etc/uctv/uctv.conf** to configure and register the source and destination interfaces.
   The following examples registers eth0 as the mirror source for both ingress and egress traffic and eth1 as the destination for this traffic:

   NOTE: When you have an active, successful monitoring session deployed, any modification to the UCT-V config file made after the initial setup requires a UCT-V restart and an inventory refresh or sync from GigaVUE-FM to pick up the new changes and re-initiate the traffic mirroring. GigaVUE-FM does a periodic sync on its own every 15 minutes.

   Example 1—Configuration example to monitor ingress and egress traffic at interface eth0 and use the same interface to send out the mirrored packets

```
# eth0   mirror-src-ingress mirror-src-egress mirror-dst
```

   Example 2—Configuration example to monitor ingress and egress traffic at interface eth0 and use the interface eth1 to send out the mirrored packets

```
# eth0   mirror-src-ingress mirror-src-egress
# eth1   mirror-dst
```

   Example 3—Configuration example to monitor ingress and egress traffic at interface eth0 and eth 1; use the interface eth1 to send out the mirrored packets

```
# eth0   mirror-src-ingress mirror-src-egress
# eth1   mirror-src-ingress mirror-src-egress mirror-dst
```

   Example 4—Configuration example to monitor ingress traffic at iface 'eth0' and egress traffic at iface 'eth1' and use iface 'eth2' to transmit the mirrored packets.

```
# eth0   mirror-src-ingress
# eth1   mirror-src-egress
# eth2 mirror-dst
```

   Example 5—Configuration example to monitor traffic at iface 'lo' that is always registered as bidirectional traffic regardless of the config and use iface 'eth0' to transmit the mirrored packets.

```
# lo mirror-src-ingress mirror-src-egress
# eth0 mirror-dst
```

   NOTE: Ensure that the configuration for a single interface is provided on a single line.

5. Save the file.

6. Restart the UCT-V service.

```
$ systemctl restart uctv.service
```

The UCT-V status is displayed as running. Verify the status using the following command:

```
$ systemctl status uctv.service
```

Install UCT-V from RPM, Red Hat Enterprise Linux, and CentOS

To install from an RPM (.rpm) package on a RedHat, CentOS, or other RPM-based system:

1. Download the UCT-V**6.14.00** RPM (.rpm) package from the Gigamon Customer Portal.
   For assistance contact Gigamon Technical Support.
2. Copy this package to your instance.
3. Install the package with root privileges. For example,

```
$ ls gigamon-gigavue-uctv-6.14.00-x86_64.rpm
$ sudo rpm -i gigamon-gigavue-uctv-6.14.00-x86_64.rpm
```

4. Modify the **/etc/uctv/uctv.conf** file to configure and register the source and destination interfaces.
   The following example registers the eth0 as the mirror source for both ingress and egress traffic and registers eth1 as the destination for this traffic as follows:

   NOTE: When you have an active, successful monitoring session deployed, any changes to the UCT-V config file made after the initial setup require an UCT-V restart and an inventory refresh or sync from GigaVUE-FM to pick up the new changes and re-initiate the traffic mirroring. GigaVUE-FM does a periodic sync on its own every 15 minutes.

   Example 1—Configuration example to monitor ingress and egress traffic at interface eth0 and use the same interface to send out the mirrored packets

   ```
   # eth0   mirror-src-ingress mirror-src-egress mirror-dst
   ```

   Example 2—Configuration example to monitor ingress and egress traffic at interface eth0 and use the interface eth1 to send out the mirrored packets

   ```
   # eth0   mirror-src-ingress mirror-src-egress
   # eth1   mirror-dst
   ```

   Example 3—Configuration example to monitor ingress and egress traffic at interface eth0 and eth 1; use the interface eth1 to send out the mirrored packets

   ```
   # eth0   mirror-src-ingress mirror-src-egress
   # eth1   mirror-src-ingress mirror-src-egress mirror-dst
   ```

   Example 4—Configuration example to monitor ingress traffic at iface 'eth0' and egress traffic at iface 'eth1' and use iface 'eth2' to transmit the mirrored packets.

   ```
   # eth0   mirror-src-ingress
   # eth1   mirror-src-egress
   # eth2 mirror-dst
   ```

   Example 5—Configuration example to monitor traffic at iface 'lo' that is always registered as bidirectional traffic regardless of the config and use iface 'eth0' to transmit the mirrored packets.

   ```
   # lo mirror-src-ingress mirror-src-egress
   # eth0 mirror-dst
   ```

   NOTE: Ensure that the configuration for a single interface is provided on a single line.

5. Save the file.
6. Restart the UCT-V service.
   ```
   $ sudo service uctv restart
   ```

The UCT-V status is displayed as running. Verify the status with the following command:

```
$ sudo service uctv status
```

Notes:

- When UCT-V fails to start due to a "**start-limit-hit**" (caused by repeated restarts within 10 minutes), you should correct the underlying issue first. To clear the failure and allow UCT-V to restart, run the following command:

  ```
  sudo systemctl reset-failed uctv.service
  ```

Post Deployment Check:

After installing UCT-V, you can perform the following to verify the version of UCT-V:

1. Enter the command:

   ```
   sudo uctvl uctv-show
   ```

2. Manually execute the following command:

   ```
   export LD_LIBRARY_PATH=/usr/lib/uctv/ssl-lib64/
   ```

Register Linux UCT-V

It is mandatory to create a cloud configuration file and add the token to authenticate the UCT-V package with GigaVUE-FM. The token is required only for initial registration before generating the certificate. You can use the token only once and do not need to maintain.

You can register UCT-V in your virtual machine using:

- **GigaVUE-FM Orchestration**: Perform the following steps:

  a. Log in to the UCT-V.

  b. Create a local configuration file and enter the following user data. **/etc/gigamon-cloud.conf** is the local configuration file in the Linux platform.

  ```
  Registration:
      token: <Enter the token created in GigaVUE-FM>
  ```

  c. Restart the UCT-V service.

  Linux platform:

  ```
  $ sudo service uctv restart
  ```

  For more details on how to create tokens, refer to Configure Tokens.

NOTE: If you have already configured gigamon-cloud.conf file in the /tmp directory, you can directly use the **uctv-wizard configure** command (sudo uctv-wizard configure). This action automatically fetches the configuration file and completes the registration process.

Windows UCT-V Installation

Windows UCT-V allows you to select the network interfaces by subnet/CIDR and modify the corresponding monitoring permissions in the configuration file. This options helps you get granular control over the monitored and mirrored traffic.

Refer to the following sections for the Windows UCT-V installation:

- Windows Network Firewall Requirements
- Install Linux UCT-Vs
- Register Linux UCT-V

Windows Network Firewall Requirements

If your environment uses network firewall rules or security groups, you must open specific ports for the virtual machine.

Ensure to use UCT-V Wizard with the configure option to configure Windows local firewall rules. Refer to Install Linux UCT-Vs using Installation Script for more details.

Install Windows UCT-Vs

Rules and Notes:

- VXLAN is the only tunnel type supported for Windows UCT-V.
- Loopback Interface is not supported for Windows UCT-V.
- Before registering Windows UCT-V, generate a token and place it in the **C:\ProgramData\uctv\gigamon-cloud.conf** configuration file. Refer to Configure Tokens.
- Do not manually edit the UCT-V Windows service registry settings. Use the supported installation and upgrade workflows instead.

You can install the UCT-Vs with MSI package using one of the following options:

- Install Linux UCT-Vs using Installation Script
- Install Linux UCT-Vs using Manual Configuration

The Windows UCT-V MSI is a self-contained package that includes all necessary dependencies. However, during set up, it automatically installs the following components:

- **Visual C++ Redistributable 2019 (x86)**

- **Npcap (v1.81 OEM)**

  Before installing the Windows Agent, ensure that Npcap is not already present on the system. If an existing version of Npcap is present, uninstall it manually to avoid conflicts and ensure compatibility with the version bundled in the UCT-V.

Refer to the following sections for more detailed information and instructions.

Install Windows UCT-Vs using Installation Script

1. Download the Windows UCT-V **`6.14.00`** MSI package from the Gigamon Customer Portal. For assistance, contact Gigamon Technical Support.
2. Install the downloaded MSI package as **Administrator**.
   The UCT-V service starts automatically.

3. Use the command below to perform pre-check, adapter setup, adapter restore, and configuration functionalities.

   ```
   uctv-wizard
   ```

   Refer to the table below to know more about **uctv-wizard** command usage options and functionalities:

Options	Use Command	Description
pre-check	uctv-wizard pre-check	Checks the network adapter properties and firewall requirements. It notifies the user if the network adapter's send buffer size is smaller than the required size for the Windows UCT-V and if any firewall rules need to be added. **NOTE:** We recommend to Increase the send buffer size of network adapters to 128 MB during the UCT-V installation to optimize performance and minimize traffic disruption.
adapter-setup	uctv-wizard adapter-setup	Checks the compatible network adapters, increases the send buffer size and restarts the service. Before changing the buffer size, the existing configuration is saved as a backup. You can choose between the following: • If you wish to skip the prompts for changing the buffer size of compatible network adapters, enter the option as **y**. • Enter **N** if you wish to set it up manually. For details, refer to Install Linux UCT-Vs using Manual Configuration.
adapter-restore	uctv-wizard adapter-restore	Using this command, you can restore the backup copy of the network adapter buffer size configuration saved in the in the **uctv-wizard adapter-setup** step. **NOTE:** You need to manually restart the network adapters for changes to take effect immediately. You can choose between the following: • If you wish to skip the prompts for restoring the buffer size of the compatible network adapters, enter the option as **y**.

Options	Use Command	Description
		• Enter **N** if you wish to restore it manually. For details, refer to
configure	uctv-wizard configure	First, it checks for any existing configured file in the tmp directory (file named gigamon-cloud.conf in the **C:\Users\<username>\AppData\Local** location). If available, UCT-V will use that configuration. If unavailable, UCT-V automatically adds the interface configuration in uctv.conf file, excluding the loopback (lo) interface, with all permissions enabled (source ingress, source egress, and destination). You can add the required policy for the available port if a firewall is installed. • If you wish to skip the prompts to add the required firewall policy, enter your option as **y**. The console interface adds the firewall rules automatically. • Enter **N** if you wish to configure manually.
uninstall	uctv-wizard uninstall	Automatically stops the UCT-V service, removes the firewall rules, and uninstalls the UCT-V.

Notes:

- The log messages generated from uctv-wizard are stored at /**C:\ProgramData\uctv\uctv-installation.txt**
- Use the command below to know the usage descriptions for the individual operations.

```
uctv-wizard help
```

Windows UCT-V Installation Scenarios

1. **Zero Touch Installation**: When using a cloud integrated script to deploy UCT-V in a virtual machine, zero interference is required as the script installs and configures everything automatically.
2. **One Touch Installation**: When using a .msi package with all prerequisite packages in place, UCT-V determines that all dependencies are met. It performs auto-configuration and restarts the service.

Install Windows UCT-Vs using Manual Configuration

1. Download the Windows UCT-V**`6.14.00`** MSI package from the Gigamon Customer Portal. For assistance, contact Gigamon Technical Support.
2. Install the downloaded MSI package as **Administrator**. The UCT-V service starts automatically.

3. Modify the file **C:\ProgramData\Uct-v\uctv.conf** to configure and register the source and destination interfaces.

   NOTE: When you have an active, successful monitoring session deployed, any changes to the UCT-V config file made after the initial setup require a UCT-V restart and an inventory refresh or sync from GigaVUE-FM to pick up the new changes and re-initiate the traffic mirroring. GigaVUE-FM does a periodic sync on its own every 15 minutes.

   Following are the rules to modify the UCT-V configuration file:
   - Interface is selected by matching its CIDR address with config entries.
   - For the VMs with single interface *(.conf file modification is optional)*:
     - if neither mirror-src permissions is granted to the interface, both mirror-src-ingress and mirror-src-egress are granted to it.
     - mirror-dst is always granted implicitly to the interface.
   - For the VMs with multiple interfaces:
     - mirror-dst is granted explicitly in the config file. Only the first matched interface is selected for mirror-dst, all other matched interfaces are ignored.
     - if none interfaces is granted any mirror-src permission, all interfaces are granted mirror-src-ingress and mirror-src-egress.

   Example 1—Configuration example to monitor ingress and egress traffic at interface 192.168.1.0/24 and use the same interface to send out the mirrored packets.

   For IPv4:

   ```
   192.168.1.0/24  mirror-src-ingress mirror-src-egress mirror-dst
   ```

   For IPv6:

   ```
   2001:db8:abcd:ef01::/64 mirror-src-ingress mirror-src-egress mirror-dst
   ```

   Example 2—Configuration example to monitor ingress and egress traffic at interface 192.168.1.0/24 and use the interface 192.168.2.0/24 to send out the mirrored packets.

   For IPv4:

   ```
   192.168.1.0/24   mirror-src-ingress mirror-src-egress
   192.168.2.0/24   mirror-dst
   ```

   For IPv6:

   ```
   2001:db8:abcd:ef01::/64 mirror-src-ingress mirror-src-egress
    2001:db8:abcd:ef01::2/64 mirror-dst
   ```

4. Save the file.

5. Restart the Windows UCT-V using one of the following actions:
   - From the command prompt, run **sc stop uctv** and **sc start uctv**.
   - From the Windows Task Manager, restart the UCT-V.

You can verify the status of the UCT-V in the Service tab of the Windows Task Manager.

Register Windows UCT-V

It is mandatory to create a cloud configuration file and add the token to authenticate the UCT-V package with GigaVUE-FM. The token is required only for initial registration before generating the certificate. You can use the token only once and do not need to maintain.

You can register UCT-V in your virtual machine using:

- **GigaVUE-FM Orchestration**: Refer to the following steps:

  a. Log in to the UCT-V.

  b. Create a local configuration file and enter the following user data. **C:\ProgramData\uctv\gigamon-cloud.conf** is the local configuration file in Windows platform.

  ```
  Registration:
      token: <Enter the token created in GigaVUE-FM>
  ```

  c. Restart the UCT-V service.

  Windows platform: Restart from the Task Manager Service

  For more details on how to create tokens, refer to Configure Tokens.

- **Third Party Orchestration**: The third-party orchestration feature allows you to deploy UCT-V using your own orchestration system. UCT-V uses the information of user to register with GigaVUE-FM.
  UCT-V can register with GigaVUE-FM using Third Party Orchestration in one of the following two modes:

  a. Generic Mode - Deploy GigaVUE Fabric Components using Generic Mode section in GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration

  b. Integrated Mode - Deploy GigaVUE Fabric Components using Integrated Mode section in GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration

NOTE: If you have already configured gigamon-cloud.conf file in the directory (C:\Users\<username>\AppData\Local), you can directly use the **uctv-wizard configure** command (sudo uctv-wizard configure). This action automatically fetches the configuration file and complete the registration process.

Create a Monitoring Domain

GigaVUE-FM connects to the AWS Platform through the public API endpoint and uses HTTPS, the default protocol to communicate with API. For more information about the endpoint and the protocol used, refer to AWS service endpoints.

GigaVUE-FM provides you the flexibility to monitor multiple VPCs. You can choose the VPC ID and launch the GigaVUE fabric components in the desired VPCs.

NOTE: To configure the Monitoring Domain and launch the fabric components in AWS, you must have the **fm_super_admin** role or the write access to the **Infrastructure Management** category. For details, refer to Role Based Access Control.

To create a Monitoring Domain:

1. Go to **Inventory > VIRTUAL > AWS** , and select **Monitoring Domain**.
2. On the **Monitoring Domain** page, select **New**. The **Monitoring Domain Configuration** page appears.
3. Select **Check Permissions** and validate whether you have the required permissions.
4. In the **Monitoring Domain** field, enter an alias used to identify the Monitoring Domain.

5. From the **Traffic Acquisition Method** drop-down list, select one of the following tapping methods:
   - **UCT-V**: UCT-Vs are deployed on your VMs to acquire the traffic and forward the acquired traffic to the GigaVUE V Series Nodes. If you select UCT-V as the tapping method, you must configure the UCT-V Controller to communicate to the UCT-Vs from GigaVUE-FM.
     You can also configure the UCT-V Controller and UCT-Vs from your own orchestrator. For details, refer to Configure GigaVUE Fabric Components in AWS using Third Party Orchestration - Integrated Mode.
   - **VPC Traffic Mirroring**: If you select the Traffic Mirroring option, the mirrored traffic from your workloads is directed to the GigaVUE V Series nodes, and you need not configure the UCT-Vs and UCT-V Controllers.
     For more information on VPC Peering, refer to VPC peering connections in the AWS Documentation. Peering is required to send mirrored traffic from other VPCs into a centralized GigaVUE V Series deployment. You can choose to use an external load balancer for Traffic Mirroring. Select **Yes** to use load balancer. For details, refer to Configure AWS Elastic Load Balancing.

   NOTE:
   - UCT-V Controller configuration is not applicable for Traffic Mirroring.
   - Traffic Mirroring does not support cross-account solutions without a load balancer.
   - For VPC Traffic Mirroring option, additional permissions are required. For details, refer to the Permissions and Privileges (AWS).
   - After deploying the Monitoring Session, a traffic mirror session is created in your AWS VPC consisting of a session, a filter, sources, and targets. For more details, refer to Traffic Mirroring in AWS Documentation.

6. In the **Traffic Acquisition Tunnel MTU**, enter the MTU value. The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry from the UCT-V to the GigaVUE V Series Node. The default value is 8951.
   - When using IPv4 tunnels, the maximum MTU value is 8951. Ensure that the UCT-V tunnel MTU is 50 bytes less than the destination interface MTU size of the UCT-V.
   - When using IPv6 tunnels, the maximum MTU value is 8931. Ensure that UCT-V tunnel MTU is 70 bytes less than the destination interface MTU size of the UCT-V.
7. Enable the **Use FM to Launch Fabric** toggle, to deploy GigaVUE Fabric Components using GigaVUE-FM.
8. Disable the **Use FM to Launch Fabric** toggle, to deploy GigaVUE Fabric Components using Third Party Orchestration.

9. Turn on the **Enable IPv6 Preference** toggle to create IPv6 tunnels between UCT-V and the GigaVUE V Series Nodes.

   > **NOTE:** This appears only when **Use FM to Launch Fabric** is disabled and **Traffic Acquisition Method** is **UCT-V**.

10. Under Connections, in the **Name** field, enter an alias used to identify the connection.
11. From the **Credential** drop-down list, select an AWS credential. For details, refer to Create AWS Credentials.
12. From the **Region** drop-down list, select AWS region for the Monitoring Domain. For example, US West.

    > **NOTE:** China regions are not supported.

13. From the **Accounts** drop-down list, select the AWS accounts.
14. From the **VPCs** drop-down list, select the VPCs to monitor.
15. Click **Save**.

> **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 view the new Monitoring Domain in the **Monitoring Domain** page list view.

To edit a Monitoring Domain, select the deployed Monitoring Domain and select **Actions**. From the drop-down list, select **Edit** and the **Monitoring Domain Configuration** page appears.

For details regarding the Check permissions while creating a Monitoring Domain, refer to Manage a Monitoring Domain .

Deploy GigaVUE Fabric Components in GigaVUE-FM
You can configure the following fabric components:

- UCT-V Controller
- GigaVUE V Series Proxy
- GigaVUE V Series Node

Prerequisite

Before you begin, create a monitoring domain in GigaVUE-FM to establish connection between your AWS environment and GigaVUE-FM. For details, refer to Create a Monitoring Domain.

To configure,

1. Go to **Inventory > VIRTUAL > AWS**.
2. Select the required Monitoring Domain and select **Actions > Deploy Fabric**.

   The **AWS Fabric Launch Configuration** page appears.
3. From the **Centralized VPC** drop-down list, select the alias of the centralized VPC.
4. Centralized VPC refers to the launch location of UCT-V Controller, V Series Proxies, and the GigaVUE V Series Nodes.

   NOTE: Select **Check Permissions** to ensure you have the required permissions for inventory, security groups, fabric launch, and IAM policy. For details, refer to Acquire Traffic using UCT-V - GigaVUE-FM Orchestration.
5. From the EBS Volume Type drop-down list, select one of the following Elastic Block Store (EBS) volume that you can attach to the fabric components:
   - gp2 (General Purpose SSD)
   - gp3 (General Purpose SSD)
   - io1 (Provisioned IOPS SSD)
   - io2 (Provisioned IOPS SSD)
   - Standard (Magnetic)

   NOTE: The default EBS Volume Type is **gp3 (General Purpose SSD)**.
6. Turn on the **Enable Encryption** toggle to encrypt the EBS volume with AWS Key Management Service (KMS).
7. From the **KMS Key** drop-down list, select the required KMS key. For details, refer to the Create a KMS Key section in the AWS Documentation.
8. From the **SSH Key Pair** drop-down list, select the key pair that you created to launch the UCT-V Controller, GigaVUE V Series node, and GigaVUE V Series Proxy from GigaVUE-FM. For details, refer to the Create a key pair section in the AWS Documentation.
9. From the **Management Subnet** drop-down list, select the subnet you use for communication between the controllers and the nodes and with GigaVUE-FM.
10. From the **Security Groups** drop-down list, select one or more security groups you created for the GigaVUE fabric nodes. For details, refer to Security Group.
11. Turn on the **Enable Custom Certificates** toggle to validate the custom certificate during SSL Communication.

    GigaVUE-FM validates the Custom certificate with the Trust Store. If the certificate is unavailable in the Trust Store, communication does not happen, and a handshake error occurs.

> **NOTE:** If the certificate expires after the successful deployment of the fabric components, the fabric components move to the failed state.

12. From the **Custom SSL Certificate** drop-down list, select the custom certificate that you have already installed.

> **NOTE:** You can also select **Create New** to upload the custom certificate for GigaVUE V Series Nodes, GigaVUE V Series Proxy, and UCT-V Controllers. For details, refer to Install Custom Certificate on AWS.

13. Turn on the **Prefer IPv6** toggle to deploy all the fabric controllers and the tunnel between the hypervisor and GigaVUE V Series Nodes using an IPv6 address.

    If the IPv6 address is unavailable, it uses an IPv4 address.

> **NOTE:** You can enable this option only when deploying a new GigaVUE V Series Node. If you want to enable this option after deploying the GigaVUE V Series Node, you must delete the existing GigaVUE V Series Node and deploy it again with this option enabled.

14. Complete the required fields to configure the following GigaVUE Fabric Components:
    - **UCT-V Controller** – Configure UCT-V Controllers in the AWS cloud only if you want to capture traffic using UCT-Vs. A UCT-V Controller can manage only UCT-Vs that have the same version. If the version of UCT-V Controllers do not match the version of UCT-Vs, GigaVUE-FM cannot detect the UCT-Vs in the instances.
    - **GigaVUE V Series Proxy** – Turn on the **Configure a V Series Proxy** toggle, if GigaVUE-FM cannot directly reach the GigaVUE V Series Nodes (management interface) directly over the network.
    - **GigaVUE V Series Node** – Creating a GigaVUE V Series Node profile automatically launches the GigaVUE V Series Nodes.

> **NOTE:** Refer to GigaVUE Fabric Components Configuration – Field References.

15. Select **Save**.

GigaVUE Fabric Components Configuration – Field References

The following table lists and describes the fields you must complete to configure the UCT-V Controller, GigaVUE V Series Proxy, and GigaVUE V Series Node.

Field	Description
UCT-V Controller • Configure UCT-V Controllers in the AWS cloud only if you want to capture traffic using UCT-Vs. • A UCT-V Controller can manage only UCT-Vs that have the same version. If there is a version mismatch between the UCT-V Controllers and UCT-Vs, GigaVUE-FM cannot detect the UCT-Vs in the instances.	
Controller Version(s)	To add UCT-V Controllers: **c.** Under **Controller Versions**, click **Add**. **d.** From the **Version** drop-down list, select a UCT-V Controller image that matches with the version number of UCT-Vs installed in the instances. **e.** From the **Instance Type** drop-down list, select a size for the UCT-V Controller. Refer to Recommended Instance Types for AWS. **f.** In the **Number of Instances** field, enter the number of UCT-V Controllers to launch. The minimum number you can enter is 1.
Agent Tunnel Type	Select one of the following tunnel types to send the traffic from UCT-Vs to GigaVUE V Series Nodes: • GRE • VXLAN – Select this type if Windows UCT-Vs co-exist with Linux UCT-Vs. • Secure tunnels (TLS-PCAPNG)
Agent CA	Select the Certificate Authority (CA) you want to use to connect the tunnel. UCT-V uses this CA to verify the server-side certificate of the GigaVUE V Series Node. **NOTE:** Use this field only when configuring secure tunnels.
IP Address Type	Select one of the following IP address types: • Private – If you want to assign an IP address that is not reachable over Internet. You can use private IP address for communication between the UCT-V Controller and GigaVUE-FM. • Public – If you want the IP address to be assigned from Amazon's pool of public IP address. The public IP address changes every time the instance is stopped and restarted. • Elastic—If you want a static public IP address for your instance, ensure that you have the elastic IP address available in your VPC. The elastic IP address does not change when you stop or start the instance. o From the **Elastic IPs** drop-down list, select the required IP addresses.
Additional Subnets	[Optional] If UCT-Vs are available on networks that are not IP routable from the management network, you must specify additional networks or subnets so that the UCT-V Controller can communicate with all the UCT-Vs. Click **Add Subnet** to select additional networks (subnets) if needed. Make sure to select a list of security groups for each additional network.
Tags	[Optional] The key name and value that helps to identify the UCT-V Controller instances in your environment. For example, you might have deployed UCT-V Controller in many regions. To distinguish these UCT-V Controllers based on the regions, you can provide a name (also known as a tag) that is easy to identify such as us-west-2- uctvcontrollers. To add a tag, select **Add**, and enter a **Key** and **Value**. For example, enter Name as your **Key** and us-west-2-uctv-controllers as the **Value**.
GigaVUE V Series Proxy	

Field	Description
Version	GigaVUE V Series Proxy version.
Instance Type	Instance type for the GigaVUE V Series Proxy. The recommended minimum instance type is t2.micro. You can review and modify the number of instances for the nitro-based instance types in the Configure AWS Settings page.
Number of Instances	Number of GigaVUE V Series Proxy to deploy in the monitoring domain.
Set Management Subnet	Use the toggle button to select a management subnet. • **Yes** to use the management subnet that you selected previously. • **No** to use another management subnet.
Set Security Groups	Toggle option to **Yes** to set the security group that is created for the GigaVUE V Series Proxy. Refer to Security Group for more details.
IP Address Type	Select one of the following IP address types: ▪ Select **Private** if you want to assign an IP address that is not reachable over Internet. You can use private IP address for communication between the GigaVUE V Series Proxy and GigaVUE-FM instances in the same network. ▪ Select **Public** if you want the IP address to be assigned from Amazon's pool of public IP address. The public IP address gets changed every time the instance is stopped and restarted. ▪ Select **Elastic** if you want a static IP address for your instance. Ensure to have the available elastic IP address in your VPC. The elastic IP address does not change when you stop or start the instance.
Additional Subnets	(Optional) If there are GigaVUE V Series Nodes on subnets that are not IP routable from the management subnet, additional subnets must be specified so that the GigaVUE V Series Proxy can communicate with all the GigaVUE V Series Nodes. Select **Add** to specify additional subnets, if needed. Also, make sure that you specify a list of security groups for each additional subnet.
Tags	(Optional) The key name and value that help to identify the GigaVUE V Series Proxy instances in your AWS environment.
GigaVUE V Series Node	
SSL Key	Select the SSL key from the drop-down list.
Version	Enter the GigaVUE V Series Node version.
Instance Type	The instance type for the GigaVUE V Series Node. For details, refer to Recommended and Supported Instance Types for AWS. You can review and modify the number of instances for the nitro-based instance types in the Configure AWS Settings page.
Volume Size	The size of the storage disk. The default volume size is 8. The recommended volume size is 80. **NOTE:** When using Application Metadata Exporter, the minimum recommended Volume Size is 80GB.
IP Address Type	Select one of the following IP address types: ▪ Select **Private** if you want to assign an IP address that is not reachable over

Field	Description
	Internet. You can use private IP address for communication between the GigaVUE V Series Controller and GigaVUE-FM instances in the same network. ▪ Select **Elastic** if you want a static IP address for your instance. Ensure to have the available elastic IP address in your VPC. The elastic IP address does not change when you stop or start the instance.
Min Number of Instances	The minimum number of GigaVUE V Series Nodes in the Monitoring Domain. The minimum number of instances must be 1. **NOTE:** If the minimum number of instances is set as '0', then the GigaVUE V Series nodes launch only when GigaVUE-FM discovers some targets to monitor and deploys a monitoring session.
Max Number of Instances	The maximum number of GigaVUE V Series Nodes deployed in the Monitoring Domain.
Data Subnets	The subnet that receives the mirrored GRE or VXLAN tunnel traffic from the UCT-Vs. **NOTE:** Using the Tool Subnet check box, you can indicate the subnets the GigaVUE V Series uses to egress the aggregated/manipulated traffic to the tools.
Tags	(Optional) The key name and value that helps to identify the GigaVUE V Series Node instances in your AWS environment. For example, you might have GigaVUE V Series Node deployed in many regions. To distinguish these GigaVUE V Series Node based on the regions, you can provide a name that is easy to identify, such as us-west-2-vseries. To add a tag: a. Select **Add tag**. b. In the **Key** field, enter the key. For example, enter Name. c. In the **Value** field, enter the key value. For example, us-west-2-vseries.

For details regarding the Check permissions to validate IAM and security-group settings, refer to Check Permissions while Configuring GigaVUE Fabric Components using GigaVUE-FM.

Configure and Deploy Monitoring Session

In GigaVUE-FM, you must do the following to configure and deploy the Monitoring Session. Refer to Configure Monitoring Session section for more details.

1. **Access the Monitoring Session Page**:
   a. In GigaVUE-FM, go to **Traffic** > **Virtual** > **Orchestrated Flows > AWS**.
   b. 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.
2. **Add components to the canvas**:
   a. Drag and drop the required components to the canvas.

b. From the **Applications** expand menu, drag and drop the required applications to the graphical workspace.

3. **Deploy the Monitoring Session**:

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

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

What to do Next

You can view the detailed statistics of an individual traffic processing element in the **TRAFFIC PROCESSING** tab. For more details, refer to View Monitoring Session Statistics (AWS).

Uninstall UCT-V

This section describes how to uninstall Linux UCT-V and Windows UCT-V.

Uninstallation Method

- Linux:
  - Uninstall the UCT-V in Ubuntu/Debian, RPM, Red Hat Enterprise Linux, and CentOS packages
  - Use the following command: **`sudo uctv-wizard uninstall`**
- Windows
  - Uninstall the UCT-V in the MSI package.
  - Use the following command: **`CMD uctv-wizard uninstall`**

NOTE: Uninstall command automatically stops the UCT-V service, removes the firewall rules, and uninstalls the UCT-V.

Upgrade or Reinstall UCT-V

You can upgrade UCT-V in your virtual machine using the following options:

- Upgrade UCT-V through GigaVUE-FM (Recommended Method)
- Upgrade UCT-V Manually

Refer to the below sections for detailed information and instructions.

Upgrade UCT-V through GigaVUE-FM (Recommended Method)

Upgrading UCT-V manually involves a series of steps to uninstall, install, and restart the service again. This upgrade method is applicable to both GigaVUE-FM Orchestration and Third Party orchestration. For a list of supported platforms, refer to Install UCT-V.

NOTE: This method is complicated if you need to upgrade UCT-Vs for a large number of VMs. However, you can upgrade UCT-V in the workload VM without any hands-on involvement through GigaVUE-FM.

Refer to the sections below for details and instructions:

1. Upload the UCT-V Images
2. Upgrade the UCT-V

Rules and Notes:

- Upgrade is allowed only to versions 6.9.00 or later. Ensure that the UCT-V Controller version is compatible with the version to which you are upgrading.
- Do not trigger system upgrades or other upgrades at the same time as the UCT-V upgrade.
- You should have Infrastructure Management permission to upgrade the UCT-Vs.
- Currently, you can upgrade the UCT-Vs to n+2 versions and any number of patch releases through GigaVUE-FM.
- Before you proceed with the upgrade, ensure that the UCT-Vs are in a healthy state.
- Make sure that a UCT-V is performing only one active job at a time. If the selected UCT-V is part of another job, you cannot trigger the immediate job using the same UCT-V.
- You must upload a compatible image type to upgrade the UCT-V; otherwise, the UCT-V is rejected for the upgrade job.
- Upgrade through GigaVUE-FM is not applicable to OVS Modules. For OVS tapping, you should upgrade the UCT-Vs manually.

Upload the UCT-V Images

Perform the following steps to upload UCT-V image files in GigaVUE-FM:

1. Go to **Inventory > Virtual** and select your cloud platform.
   The **Monitoring Domain** page appears.
2. Select the **UCT-V Upgrade** drop-down menu and select **Images**.
3. In the **Images** page, click **Upload**. The **Upload Internal Image Files** wizard appears.

4. Select **Choose File**, upload the UCT-V files from your local, and select **Ok**.

   Notes:
   - You can download the UCT-V image files from Gigamon software portal.
   - You can upload a maximum of 15 UCT-V files at a time.
   - The supported file formats are **.deb**, **.rpm**, and **.msi**.
   - Ensure that you do not change the file names. GigaVUE-FM does not accept the image files with modified names.
   - When the upload is in process, GigaVUE-FM does not allow uploading a file with similar type and version.

5. Verify if the uploaded UCT-V images is listed in the **Images** page.

Delete the file

You can delete one or multiple images.

1. In the **Images** page, select **Filter** to find the images based on Image Name, Version, and Image Type.
2. Select the required images.
3. From the Actions drop-down menu, select **Delete** or **Delete All**.

You can only delete those image files that are not associated with any tasks created for the upgrade process.

Upgrade the UCT-V

Follow the steps below to upgrade UCT-V in GigaVUE-FM:

1. In the **UCT-V Upgrade** drop-down menu, select **Dashboard** to view the UCT-V upgrade landing page.
   In the Dashboard page, you can view the upgrade status of individual UCT-Vs and the stages of the upgrade process (Fetch, Install, Verify). The page also displays the overall progress of the upgrade.
2. Select the required UCT-Vs, and from the **Actions** drop-down menu, select **Upgrade**.
   The **UCT-V Upgrade task** page appears.
3. Enter the task name.
4. In the **Image Version** drop-down menu, select the required version you want to upgrade to from the list of available image versions. You can choose to upgrade immediately or schedule a time for the upgrade to happen.
5. Select the required option in the **Time Selection** field. If you prefer to schedule the upgrade, enter the choice of your date and time in the respective fields.
   Do not schedule the upgrade for a time in the past.

6. Select **Create**.
   The image upgrade task is now created.

   Note:
   - You cannot edit the upgrade task once it is created.
   - You can only reschedule the scheduled task but cannot edit the UCT-V selected for the particular task.
   - In the event of the errors listed below, GigaVUE-FM displays a pop-up message with the list of UCT-Vs that are not compatible for upgrade. Select **Proceed** to ignore the unsupported UCT-Vs and upgrade the compatible ones, or sekect "**Edit**" to modify your changes. The errors include:
     - Controller version is not compatible with the upgrade version.
     - Inconsistency between the uploaded image file type and the selected UCT-V.

You can view the created task details (both immediate and scheduled) in the **UCT-V Upgrade > Jobs** section.

Notes:
- For better progress monitoring, it is recommended to split the upgrade task to a limited number, such as 50 or 100 UCT-Vs.
- When you create a new upgrade task for the same UCT-V, the status of any existing UCT-V changes to 'In Progress' until the latest task is completed. Once the upgrade for the existing tasks is successfully finished, you can create another task for that same UCT-V.

You can view the different stages of the upgrade process in UCT-V Upgrade Dashboard page. Each stage is marked with if it is successful and in case of failure. If the upgrade is successful, GigaVUE-FM updates the upgrade status as **Success** for the selected UCT-V.

Notes:
- The default wait time for the **Upgrade Status** to get updated is 15 minutes.
- The default wait time for the **Image Version** to get updated is 5 minutes.
- In case of failure, you can upgrade the failed instance manually.

Upgrade UCT-V Manually

To upgrade UCT-V manually on a virtual machine, delete the existing UCT-V and install the new version of UCT-V.

NOTE: Before deleting the UCT-V, take a backup copy of the **/etc/uctv/uctv.conf** configuration file. This step avoids reconfiguring the source and destination interfaces.

1. Uninstall the existing UCT-V. Refer to the *Uninstall UCT-V* section in the respective GigaVUE Cloud Suite Deployment Guide.
2. Install the latest version of the new UCT-V. Refer to the Linux UCT-V Installation and the Windows UCT-V Installation topics in the respective GigaVUE Cloud Suite Deployment Guides.
3. Restart the UCT-V service.
   - Linux platform:
     ```
     $ sudo service uctv restart
     ```
   - Windows platform: Restart from the Task Manager.

Acquire Traffic using Traffic Mirroring – GigaVUE-FM Orchestration

This section outlines the workflow for acquiring traffic with Traffic Mirroring and deploying GigaVUE Fabric Components using GigaVUE-FM. Refer to the following topics for instruction on configuring traffic acquisition, processing, and forwarding to your desired destination.

NOTE: When GigaVUE-FM and the workload VMs requiring monitoring are in different AWS accounts, you must configure a load balancer. For steps to configure, refer to Acquire Traffic using Traffic Mirroring with Network Load Balancer or Acquire Traffic using Traffic Mirroring with Gateway Load Balancing for configuration steps.

- Install GigaVUE-FM on AWS
- Configure the permissions required in AWS
- Create the AWS Credentials
- Create a Monitoring Domain
- Configure and Deploy GigaVUE Fabric Components in GigaVUE-FM
- Configure and Deploy Monitoring Session

Install GigaVUE-FM on AWS

This step is optional and applies only when an existing GigaVUE-FM instance is not available.
Refer to Install GigaVUE-FM on AWS for steps to install GigaVUE-FM on AWS and the steps to start GigaVUE-FM instance and configure it.

Configure the permissions required in AWS

If you are using inline policy or basic authentication, then you must update the policy with the relevant IAM service. For more information, see Minimum Permissions Required for Inline Policies and Basic Authentication.

These are the minimum permissions that are required to acquire traffic using Traffic Mirroring and authenticate using an IAM instance role.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags",
                "ec2:DeleteTags",
                "ec2:AssociateAddress",
                "ec2:DisassociateAddress",
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeVolumes",
                "ec2:DescribeAddresses",
                "ec2:RunInstances",
                "ec2:TerminateInstances",
                "ec2:RebootInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:DescribeTrafficMirrorFilters",
                "ec2:DescribeTrafficMirrorSessions",
                "ec2:DescribeTrafficMirrorTargets",
                "ec2:CreateTrafficMirrorTarget",
                "ec2:CreateTrafficMirrorSession",
                "ec2:DeleteTrafficMirrorTarget",
                "ec2:DeleteTrafficMirrorSession",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedRolePolicies",
                "iam:ListRolePolicies",
                "iam:ListAccountAliases",
                "kms:ListAliases"
            ],
            "Resource": "*"
        }
    ]
}
```

For more information regarding policies and permissions, refer to AWS Documentation.

Create the AWS Credentials

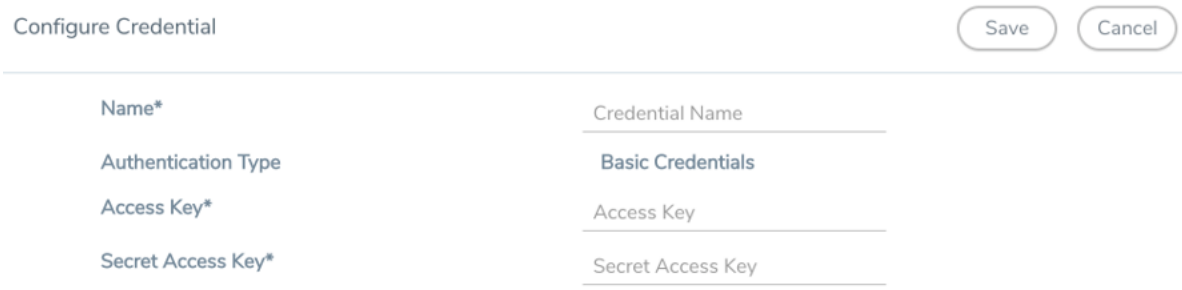
You can monitor workloads across multiple AWS accounts within one Monitoring Domain.

- After launching GigaVUE-FM in AWS, if the IAM is attached to the running instance of FM, then the **EC2 Instance Role** authentication credential is automatically added to the **Credential** page as the default credential. You must attach the IAM prior to creating a Monitoring Domain.
- If you use the **Basic Credentials** authentication credentials, you must add these to the GigaVUE-FM on the **AWS Settings** page, or on the Monitoring Domain creation page.

For details, refer to Create a Monitoring Domain.

To create AWS credentials:

1. Go to **Inventory > VIRTUAL > AWS**, and select **Settings > Credentials**
2. On the **Credential** page, select **Add**. The **Credential Configure** page appears.



3. Enter a name to identify the AWS Credential in the **Name** Field.
4. Basic Credentials is selected as the default **Authentication Type**. For more information, refer to AWS Security Credentials
5. Enter the credential of an IAM user or the AWS account root user in the **Access Key** field.
6. Enter the security password or key in the **Secret Access Key** field.
7. Select **Save**. You can view the list of available credentials on the AWS Credential page.

Create a Monitoring Domain

GigaVUE-FM connects to the AWS Platform through the public API endpoint and uses HTTPS, the default protocol to communicate with API. For more information about the endpoint and the protocol used, refer to AWS service endpoints.

GigaVUE-FM provides you the flexibility to monitor multiple VPCs. You can choose the VPC ID and launch the GigaVUE fabric components in the desired VPCs.

NOTE: To configure the Monitoring Domain and launch the fabric components in AWS, you must have the **fm_super_admin** role or the write access to the **Infrastructure Management** category. For details, refer to Role Based Access Control.

To create a Monitoring Domain:

1. Go to **Inventory > VIRTUAL > AWS** , and select **Monitoring Domain**.
2. On the **Monitoring Domain** page, select **New**. The **Monitoring Domain Configuration** page appears.
3. Select **Check Permissions** and validate whether you have the required permissions.
4. In the **Monitoring Domain** field, enter an alias used to identify the Monitoring Domain.
5. From the **Traffic Acquisition Method** drop-down list, select one of the following tapping methods:
   - **VPC Traffic Mirroring**: If you select the Traffic Mirroring option, the mirrored traffic from your workloads is directed to the GigaVUE V Series nodes, and you need not configure the UCT-Vs and UCT-V Controllers.
     For more information on VPC Peering, refer to VPC peering connections in the AWS Documentation. Peering is required to send mirrored traffic from other VPCs into a centralized GigaVUE V Series deployment. You can choose to use an external load balancer for Traffic Mirroring. Select **Yes** to use load balancer. For details, refer to Configure AWS Elastic Load Balancing.

     NOTE:
     - UCT-V Controller configuration is not applicable for Traffic Mirroring.
     - Traffic Mirroring does not support cross-account solutions without a load balancer.
     - For VPC Traffic Mirroring option, additional permissions are required. For details, refer to the Permissions and Privileges (AWS).
     - After deploying the Monitoring Session, a traffic mirror session is created in your AWS VPC consisting of a session, a filter, sources, and targets. For more details, refer to Traffic Mirroring in AWS Documentation.

6. In the **Traffic Acquisition Tunnel MTU**, enter the MTU value. The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry from the UCT-V to the GigaVUE V Series Node. The default value is 8951.
   - When using IPv4 tunnels, the maximum MTU value is 8951. Ensure that the UCT-V tunnel MTU is 50 bytes less than the destination interface MTU size of the UCT-V.
   - When using IPv6 tunnels, the maximum MTU value is 8931. Ensure that UCT-V tunnel MTU is 70 bytes less than the destination interface MTU size of the UCT-V.
7. Enable the **Use FM to Launch Fabric** toggle, to deploy GigaVUE Fabric Components using GigaVUE-FM.
8. Turn on the **Enable IPv6 Preference** toggle to create IPv6 tunnels between UCT-V and the GigaVUE V Series Nodes.

   NOTE: This appears only when **Use FM to Launch Fabric** is disabled and **Traffic Acquisition Method** is **UCT-V**.
9. Under Connections, in the **Name** field, enter an alias used to identify the connection.
10. From the **Credential** drop-down list, select an AWS credential. For details, refer to Create AWS Credentials.
11. From the **Region** drop-down list, select AWS region for the Monitoring Domain. For example, US West.

    NOTE: China regions are not supported.
12. From the **Accounts** drop-down list, select the AWS accounts.
13. From the **VPCs** drop-down list, select the VPCs to monitor.
14. Click **Save**.

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 view the new Monitoring Domain in the **Monitoring Domain** page list view.

To edit a Monitoring Domain, select the deployed Monitoring Domain and select **Actions**. From the drop-down list, select **Edit** and the **Monitoring Domain Configuration** page appears.

For details regarding the Check permissions while creating a Monitoring Domain, refer to Manage a Monitoring Domain .

Configure and Deploy GigaVUE Fabric Components in GigaVUE-FM

NOTE: You can configure a prefilter and determine the VPC endpoint traffic that is mirrored. For more information on prefiltering, see Configure a Traffic Pre-filter.

You can configure the following fabric components:

- UCT-V Controller
- GigaVUE V Series Proxy
- GigaVUE V Series Node

Prerequisite

Before you begin, create a monitoring domain in GigaVUE-FM to establish connection between your AWS environment and GigaVUE-FM. For details, refer to Create a Monitoring Domain.

To configure,

1. Go to **Inventory > VIRTUAL > AWS**.
2. Select the required Monitoring Domain and select **Actions > Deploy Fabric**.

   The **AWS Fabric Launch Configuration** page appears.
3. From the **Centralized VPC** drop-down list, select the alias of the centralized VPC.
4. Centralized VPC refers to the launch location of UCT-V Controller, V Series Proxies, and the GigaVUE V Series Nodes.

   NOTE: Select **Check Permissions** to ensure you have the required permissions for inventory, security groups, fabric launch, and IAM policy. For details, refer to Acquire Traffic using Traffic Mirroring – GigaVUE-FM Orchestration.
5. From the EBS Volume Type drop-down list, select one of the following Elastic Block Store (EBS) volume that you can attach to the fabric components:
   - gp2 (General Purpose SSD)
   - gp3 (General Purpose SSD)
   - io1 (Provisioned IOPS SSD)
   - io2 (Provisioned IOPS SSD)
   - Standard (Magnetic)

   NOTE: The default EBS Volume Type is **gp3 (General Purpose SSD)**.
6. Turn on the **Enable Encryption** toggle to encrypt the EBS volume with AWS Key Management Service (KMS).
7. From the **KMS Key** drop-down list, select the required KMS key. For details, refer to the Create a KMS Key section in the AWS Documentation.

8. From the **SSH Key Pair** drop-down list, select the key pair that you created to launch the UCT-V Controller, GigaVUE V Series node, and GigaVUE V Series Proxy from GigaVUE-FM. For details, refer to the Create a key pair section in the AWS Documentation.
9. From the **Management Subnet** drop-down list, select the subnet you use for communication between the controllers and the nodes and with GigaVUE-FM.
10. From the **Security Groups** drop-down list, select one or more security groups you created for the GigaVUE fabric nodes. For details, refer to Security Group.
11. Turn on the **Enable Custom Certificates** toggle to validate the custom certificate during SSL Communication.

    GigaVUE-FM validates the Custom certificate with the Trust Store. If the certificate is unavailable in the Trust Store, communication does not happen, and a handshake error occurs.

    NOTE: If the certificate expires after the successful deployment of the fabric components, the fabric components move to the failed state.
12. From the **Custom SSL Certificate** drop-down list, select the custom certificate that you have already installed.

    NOTE: You can also select **Create New** to upload the custom certificate for GigaVUE V Series Nodes, GigaVUE V Series Proxy, and UCT-V Controllers. For details, refer to Install Custom Certificate on AWS.
13. Turn on the **Prefer IPv6** toggle to deploy all the fabric controllers and the tunnel between the hypervisor and GigaVUE V Series Nodes using an IPv6 address.

    If the IPv6 address is unavailable, it uses an IPv4 address.

    NOTE: You can enable this option only when deploying a new GigaVUE V Series Node. If you want to enable this option after deploying the GigaVUE V Series Node, you must delete the existing GigaVUE V Series Node and deploy it again with this option enabled.
14. Complete the required fields to configure the following GigaVUE Fabric Components:
    - **UCT-V Controller** – Configure UCT-V Controllers in the AWS cloud only if you want to capture traffic using UCT-Vs. A UCT-V Controller can manage only UCT-Vs that have the same version. If the version of UCT-V Controllers do not match the version of UCT-Vs, GigaVUE-FM cannot detect the UCT-Vs in the instances.
    - **GigaVUE V Series Proxy** – Turn on the **Configure a V Series Proxy** toggle, if GigaVUE-FM cannot directly reach the GigaVUE V Series Nodes (management interface) directly over the network.
    - **GigaVUE V Series Node** – Creating a GigaVUE V Series Node profile automatically launches the GigaVUE V Series Nodes.

> **NOTE:** Refer to GigaVUE Fabric Components Configuration – Field References.

15. Select **Save**.

GigaVUE Fabric Components Configuration – Field References

The following table lists and describes the fields you must complete to configure the UCT-V Controller, GigaVUE V Series Proxy, and GigaVUE V Series Node.

Field	Description
UCT-V Controller • Configure UCT-V Controllers in the AWS cloud only if you want to capture traffic using UCT-Vs. • A UCT-V Controller can manage only UCT-Vs that have the same version. If there is a version mismatch between the UCT-V Controllers and UCT-Vs, GigaVUE-FM cannot detect the UCT-Vs in the instances.	
Controller Version(s)	To add UCT-V Controllers: **a.** Under **Controller Versions**, click **Add**. **b.** From the **Version** drop-down list, select a UCT-V Controller image that matches with the version number of UCT-Vs installed in the instances. **c.** From the **Instance Type** drop-down list, select a size for the UCT-V Controller. Refer to Recommended Instance Types for AWS. **d.** In the **Number of Instances** field, enter the number of UCT-V Controllers to launch. The minimum number you can enter is 1.
Agent Tunnel Type	Select one of the following tunnel types to send the traffic from UCT-Vs to GigaVUE V Series Nodes: • GRE • VXLAN – Select this type if Windows UCT-Vs co-exist with Linux UCT-Vs. • Secure tunnels (TLS-PCAPNG)
Agent CA	Select the Certificate Authority (CA) you want to use to connect the tunnel. UCT-V uses this CA to verify the server-side certificate of the GigaVUE V Series Node. **NOTE:** Use this field only when configuring secure tunnels.
IP Address Type	Select one of the following IP address types: • Private – If you want to assign an IP address that is not reachable over Internet. You can use private IP address for communication between the UCT-V Controller and GigaVUE-FM. • Public – If you want the IP address to be assigned from Amazon's pool of public IP address. The public IP address changes every time the instance is stopped and restarted. • Elastic—If you want a static public IP address for your instance, ensure that you have the elastic IP address available in your VPC. The elastic IP address does not change when you stop or start the instance. o From the **Elastic IPs** drop-down list, select the required IP addresses.
Additional Subnets	[Optional] If UCT-Vs are available on networks that are not IP routable from the management network, you must specify additional networks or subnets so that the UCT-V Controller can communicate with all the UCT-Vs. Click **Add Subnet** to select additional networks (subnets) if needed. Make sure to

Field	Description
	select a list of security groups for each additional network.
Tags	[Optional] The key name and value that helps to identify the UCT-V Controller instances in your environment. For example, you might have deployed UCT-V Controller in many regions. To distinguish these UCT-V Controllers based on the regions, you can provide a name (also known as a tag) that is easy to identify such as us-west-2- uctvcontrollers. To add a tag, select **Add**, and enter a **Key** and **Value**. For example, enter Name as your **Key** and us-west-2-uctv-controllers as the **Value**.
GigaVUE V Series Proxy	
Version	GigaVUE V Series Proxy version.
Instance Type	Instance type for the GigaVUE V Series Proxy. The recommended minimum instance type is t2.micro. You can review and modify the number of instances for the nitro-based instance types in the Configure AWS Settings page.
Number of Instances	Number of GigaVUE V Series Proxy to deploy in the monitoring domain.
Set Management Subnet	Use the toggle button to select a management subnet. • **Yes** to use the management subnet that you selected previously. • **No** to use another management subnet.
Set Security Groups	Toggle option to **Yes** to set the security group that is created for the GigaVUE V Series Proxy. Refer to Security Group for more details.
IP Address Type	Select one of the following IP address types: ▪ Select **Private** if you want to assign an IP address that is not reachable over Internet. You can use private IP address for communication between the GigaVUE V Series Proxy and GigaVUE-FM instances in the same network. ▪ Select **Public** if you want the IP address to be assigned from Amazon's pool of public IP address. The public IP address gets changed every time the instance is stopped and restarted. ▪ Select **Elastic** if you want a static IP address for your instance. Ensure to have the available elastic IP address in your VPC. The elastic IP address does not change when you stop or start the instance.
Additional Subnets	(Optional) If there are GigaVUE V Series Nodes on subnets that are not IP routable from the management subnet, additional subnets must be specified so that the GigaVUE V Series Proxy can communicate with all the GigaVUE V Series Nodes. Select **Add** to specify additional subnets, if needed. Also, make sure that you specify a list of security groups for each additional subnet.
Tags	(Optional) The key name and value that help to identify the GigaVUE V Series Proxy instances in your AWS environment.
GigaVUE V Series Node	
SSL Key	Select the SSL key from the drop-down list.
Version	Enter the GigaVUE V Series Node version.
Instance Type	The instance type for the GigaVUE V Series Node. For details, refer to Recommended and Supported Instance Types for AWS.

Field	Description
	You can review and modify the number of instances for the nitro-based instance types in the Configure AWS Settings page.
Volume Size	The size of the storage disk. The default volume size is 8. The recommended volume size is 80. **NOTE:** When using Application Metadata Exporter, the minimum recommended Volume Size is 80GB.
IP Address Type	Select one of the following IP address types: ▪ Select **Private** if you want to assign an IP address that is not reachable over Internet. You can use private IP address for communication between the GigaVUE V Series Controller and GigaVUE-FM instances in the same network. ▪ Select **Elastic** if you want a static IP address for your instance. Ensure to have the available elastic IP address in your VPC. The elastic IP address does not change when you stop or start the instance.
Min Number of Instances	The minimum number of GigaVUE V Series Nodes in the Monitoring Domain. The minimum number of instances must be 1. **NOTE:** If the minimum number of instances is set as '0', then the GigaVUE V Series nodes launch only when GigaVUE-FM discovers some targets to monitor and deploys a monitoring session.
Max Number of Instances	The maximum number of GigaVUE V Series Nodes deployed in the Monitoring Domain.
Data Subnets	The subnet that receives the mirrored GRE or VXLAN tunnel traffic from the UCT-Vs. **NOTE:** Using the Tool Subnet check box, you can indicate the subnets the GigaVUE V Series uses to egress the aggregated/manipulated traffic to the tools.
Tags	(Optional) The key name and value that helps to identify the GigaVUE V Series Node instances in your AWS environment. For example, you might have GigaVUE V Series Node deployed in many regions. To distinguish these GigaVUE V Series Node based on the regions, you can provide a name that is easy to identify, such as us-west-2-vseries. To add a tag: a. Select **Add tag**. b. In the **Key** field, enter the key. For example, enter Name. c. In the **Value** field, enter the key value. For example, us-west-2-vseries.

For details regarding the Check permissions to validate IAM and security-group settings, refer to Check Permissions while Configuring GigaVUE Fabric Components using GigaVUE-FM.

Configure and Deploy Monitoring Session

In GigaVUE-FM, you must do the following to configure and deploy the Monitoring Session. Refer to Configure Monitoring Session section for more details.

1. **Access the Monitoring Session Page**:

a. In GigaVUE-FM, go to **Traffic** > **Virtual** > **Orchestrated Flows > AWS**.

b. 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.

2. **Add components to the canvas**:

   a. Drag and drop the required components to the canvas.

   b. From the **Applications** expand menu, drag and drop the required applications to the graphical workspace.

3. **Deploy the Monitoring Session**:

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

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

What to do Next

You can view the detailed statistics of an individual traffic processing element in the **TRAFFIC PROCESSING** tab. For more details, refer to View Monitoring Session Statistics (AWS).

Acquire Traffic using Traffic Mirroring with Network Load Balancer

This section outlines the workflow for acquiring traffic using Traffic Mirroring with Network Load Balancer. Refer to the following topics for instruction on configuring traffic acquisition, processing, and forwarding to your desired destination.

> **NOTE:** When GigaVUE-FM and the workload VMs requiring monitoring are in different AWS accounts, you must configure a load balancer. For steps to configure, refer to Acquire Traffic using Traffic Mirroring with Network Load Balancer or Acquire Traffic using Traffic Mirroring with Gateway Load Balancing for configuration steps.

- Install GigaVUE-FM on AWS
- Configure the permissions required in AWS
- Create the AWS Credentials
- Configure Network Load Balancer and deploy GigaVUE V Series Nodes
- Configure and Deploy Monitoring Session

Install GigaVUE-FM on AWS

This step is optional and applies only when an existing GigaVUE-FM instance is not available.
Refer to Install GigaVUE-FM on AWS for steps to install GigaVUE-FM on AWS and the

steps to start GigaVUE-FM instance and configure it.

Configure the permissions required in AWS

If you are using inline policy or basic authentication, then you must update the policy with the relevant IAM service. For more information, see Minimum Permissions Required for Inline Policies and Basic Authentication.

These are the minimum permissions that are required to acquire traffic using Traffic Mirroring with Network Load Balancer and authenticate using an IAM instance role.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "autoscaling:DescribeAutoScalingGroups",
                "elasticloadbalancing:DescribeLoadBalancers",
                "elasticloadbalancing:DescribeTargetGroups",
                "elasticloadbalancing:RegisterTargets",
                "elasticloadbalancing:DeregisterTargets",
                "elasticloadbalancing:DescribeTargetHealth",
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeAddresses",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeSecurityGroups",
                "ec2:CreateTags",
                "ec2:DeleteTags",
                "ec2:DescribeImages",
                "ec2:DescribeVolumes",
                "ec2:CreateTrafficMirrorFilterRule",
                "ec2:CreateTrafficMirrorTarget",
                "ec2:CreateTrafficMirrorSession",
                "ec2:CreateTrafficMirrorFilter",
                "ec2:DeleteTrafficMirrorTarget",
                "ec2:DeleteTrafficMirrorSession",
                "ec2:DeleteTrafficMirrorFilter",
                "ec2:DescribeTrafficMirrorSessions",
                "ec2:DescribeTrafficMirrorTargets",
                "ec2:DescribeTrafficMirrorFilters",
                "ram:CreateResourceShare",
                "ram:DeleteResourceShare",
                "ram:GetResourceShareInvitations",
                "ram:AcceptResourceShareInvitation",
                "ram:DisassociateResourceShare",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedRolePolicies",
                "iam:ListRolePolicies",
                "iam:ListAccountAliases",
                "kms:GenerateDataKeyWithoutPlaintext",
                "kms:ListAliases",
```

```
            ],
            "Resource": "*"
        }
    ]
}
```

For more information regarding policies and permissions, refer to AWS Documentation.

If you are using inline policy or basic authentication, then you must update the policy with the relevant IAM service. For more information, see Prerequisites.

Create the AWS Credentials

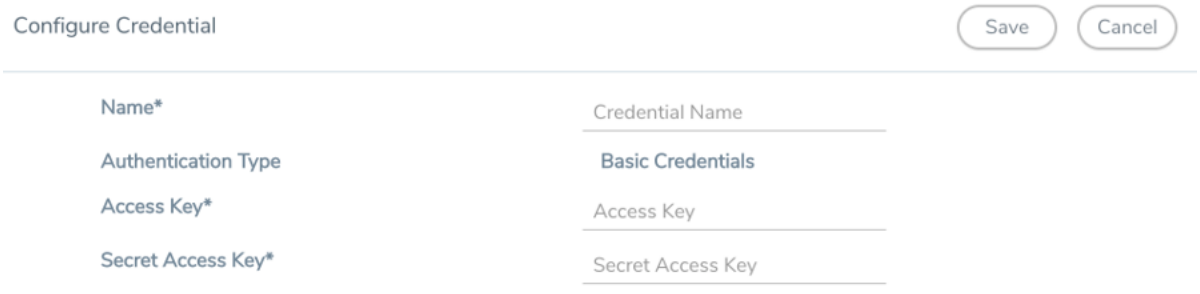
You can monitor workloads across multiple AWS accounts within one Monitoring Domain.

- After launching GigaVUE-FM in AWS, if the IAM is attached to the running instance of FM, then the **EC2 Instance Role** authentication credential is automatically added to the **Credential** page as the default credential. You must attach the IAM prior to creating a Monitoring Domain.
- If you use the **Basic Credentials** authentication credentials, you must add these to the GigaVUE-FM on the **AWS Settings** page, or on the Monitoring Domain creation page.

For details, refer to Create a Monitoring Domain.

To create AWS credentials:

1. Go to **Inventory > VIRTUAL > AWS**, and select **Settings > Credentials**
2. On the **Credential** page, select **Add**. The **Credential Configure** page appears.



3. Enter a name to identify the AWS Credential in the **Name** Field.
4. Basic Credentials is selected as the default **Authentication Type**. For more information, refer to AWS Security Credentials
5. Enter the credential of an IAM user or the AWS account root user in the **Access Key** field.

6. Enter the security password or key in the **Secret Access Key** field.
7. Select **Save**. You can view the list of available credentials on the AWS Credential page.

Configure Network Load Balancer and deploy GigaVUE V Series Nodes

You can configure an external Network Load Balancer (NLB) in AWS for GigaVUE Cloud Suite.

Prerequisites

- Create or update Security Group policies of GigaVUE Cloud Suite components. For details, refer to Security Group.
- Create or update routes in various VPCs across participating mirrored AWS accounts so that all mirrored account VPCs can connect to the target account VPC where the AWS Network Load Balancer is deployed.

  NOTE: GigaVUE-FM considers the target account VPC as the centralized VPC. Use the connections towards all other mirrored account VPCs either through 1 : 1 VPC peering or via 1 : M transit gateway (that connects all participating VPCs across mirrored AWS accounts). VPC peering has no bandwidth limitation and no additional cost within the same region (recommended). Transit gateway costs more and also has a limitation of 50 Gbps burst per VPC.
- Create or update existing IAM role for GigaVUE-FM in the centralized VPC. In addition, you need to create trust relationship between the mirrored and the target account for GigaVUE-FM to execute the above permissions at the IAM role level. For details, refer to Permissions and Privileges (AWS).
- When configuring Network Load Balancer, you need to deploy the GigaVUE V Series Nodes using Third Party Orchestration.
- You need to configure Token \in the **User Management** page. For details, refer to Configure Tokens.

Perform the following steps to configure an external network load balancer in AWS:

1. Create a Target Group
2. Create a Load Balancer
3. Create a Launch Template for Auto Scaling group
4. Create an Auto Scaling group using a Launch Template

Create a Target Group

Enter or select the following details to configure target groups in AWS.

Parameters	Description	Reference	Mandatory field
Basic Configuration			
Choose a target type	Select IP address as the target type	Create a target group for your Network Load Balancer	Yes
Protocol	Select UDP as the protocol from the drop-down list		Yes
Port	Enter 4789 as the port value		Yes
Health Checks			
HealthCheckProtocol	Select TCP as the protocol.	Health checks for Network Load Balancer target groups	Yes
HealthCheckPort	Enter 8888 as the port.		Yes
HealthCheckIntervalSeconds	Enter 10 seconds as the approximate amount of time, in seconds.		Yes

Create a Load Balancer

Enter or select the following details to configure a load balancer in AWS.

Parameters	Description	Reference	Mandatory field
Basic Configuration			
Scheme	Select Internal as the scheme for the load balancer	Create a Network Load Balancer	Yes
Network Mapping			
VPC	Select the VPC for your targets (GigaVUE V Series Node)	Create a Network Load Balancer	Yes
Listeners and routing			
Protocol	Select UDP as the protocol.	Create a Network Load Balancer	Yes
Port	Enter 4789 as the port.		Yes

Create a Launch Template for Auto Scaling group

Enter or select the following details to create a launch template for auto scaling groups in AWS.

Parameters	Description	Reference	Mandatory field
Launch Template contents			
Application and OS Images (Amazon Machine Image)	Select the AMI of the GigaVUE V Series Node.	Create a launch template for an Auto Scaling group	Yes
Instance type	Select **t3a.xlarge** as the instance type.		Yes
Key pair name	Select a Key pair for the instance.		Yes
Network Settings			
Device Index	Add 2 Network Interfaces for the GigaVUE V Series Node with device index as **0** and **1** (mgmt and data interface respectively) and for the interfaces,	Create a launch template for an Auto Scaling group	Yes
Firewall (security groups)	Keep this blank and configure one or more security groups as part of the network interface.		Yes
Advanced Settings			

Advanced details	Enter the User data as text in the following format and deploy the instance. The GigaVUE V Series Nodes uses this user data to generate config file (**/etc/gigamon-cloud.conf**) used to register with GigaVUE-FM using Third Party Orchestration.
	`#cloud-config`
	`write_files:`
	`- path: /etc/gigamon-cloud.conf`
	`owner: root:root`
	`permissions: '0644'`
	`content: |`
	`Registration:`
	`groupName: <Monitoring Domain Name>`
	`subGroupName: <VPC Name>`
	`token: <Token>`
	`remoteIP: <IP address of the GigaVUE-FM>`
	`remotePort: 443`
		Create a launch template using advanced settings	Yes

Create an Auto Scaling group using a Launch Template

Enter or select the following details to create an auto scaling group and launch the fabric components using the launch template in AWS.

Parameters	Description	Reference	Mandatory field
Configure group size and scaling policies			
Group Size	Enter the Desired capacity as 0. Ensure that the Desired capacity value is less that the Maximum Capacity value. **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.	Creating an Auto Scaling group using a launch template	Yes
Automatic Scaling	Select **Target tracking scaling policy** and enter the following details to define a policy: • Metric Type: 1000000000 (bytes) • Instance warmup: **300** seconds	Create a target tracking scaling policy	Yes
Add tag	Provide a tag key and value for each tag. • Tag key - GigamonNode • Value - VSeriesNode	Tag Auto Scaling groups and instances	Yes

In the Instances page, you can view the GigaVUE V Series Node instance that the load balancer deployed.

Configure and Deploy Monitoring Session

In GigaVUE-FM, you must do the following to configure and deploy the Monitoring Session. Refer to Configure Monitoring Session section for more details.

1. **Access the Monitoring Session Page**:
   a. In GigaVUE-FM, go to **Traffic** > **Virtual** > **Orchestrated Flows > AWS**.
   b. 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.
2. **Add components to the canvas**:
   a. Drag and drop the required components to the canvas.
   b. From the **Applications** expand menu, drag and drop the required applications to the graphical workspace.
3. **Deploy the Monitoring Session**:
   a. From the **Actions** menu, select **Deploy**.
   b. After successful deployment on all the V Series Nodes, the status appears as **Success** on the Monitoring Sessions **Sources** tab.

What to do Next

You can view the detailed statistics of an individual traffic processing element in the **TRAFFIC PROCESSING** tab. For more details, refer to View Monitoring Session Statistics (AWS).

Acquire Traffic using Traffic Mirroring with Gateway Load Balancing

This section outlines the workflow for acquiring traffic with Traffic Mirroring and deploying GigaVUE Fabric Components with a Gateway Load Balancer. Refer to the following topics for instructions on configuring traffic acquisition, processing, and forwarding to your desired destination.

- Install GigaVUE-FM on AWS
- Configure the permissions required in AWS
- Create the AWS Credentials
- Configure Gateway Load Balancer and deploy GigaVUE V Series Nodes
- Configure and Deploy Monitoring Session

Install GigaVUE-FM on AWS

This step is optional and applies only when an existing GigaVUE-FM instance is not available.
Refer to Install GigaVUE-FM on AWS for steps to install GigaVUE-FM on AWS and the steps to start GigaVUE-FM instance and configure it.

Configure the permissions required in AWS

If you are using inline policy or basic authentication, then you must update the policy with the relevant IAM service. For more information, see Minimum Permissions Required for Inline Policies and Basic Authentication.

This policy allows you to acquire traffic using Traffic Mirroring with Gateway Load Balancer and authenticate using an IAM instance role.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "autoscaling:DescribeAutoScalingGroups",
                "elasticloadbalancing:DescribeLoadBalancers",
                "elasticloadbalancing:DescribeTargetGroups",
                "elasticloadbalancing:RegisterTargets",
                "elasticloadbalancing:DeregisterTargets",
```

```
                "elasticloadbalancing:DescribeTargetHealth",
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeAddresses",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeSecurityGroups",
                "ec2:CreateTags",
                "ec2:DeleteTags",
                "ec2:DescribeImages",
                "ec2:DescribeVolumes",
                "ec2:CreateTrafficMirrorFilterRule",
                "ec2:CreateTrafficMirrorTarget",
                "ec2:CreateTrafficMirrorSession",
                "ec2:CreateTrafficMirrorFilter",
                "ec2:DeleteTrafficMirrorTarget",
                "ec2:DeleteTrafficMirrorSession",
                "ec2:DeleteTrafficMirrorFilter",
                "ec2:DescribeTrafficMirrorSessions",
                "ec2:DescribeTrafficMirrorTargets",
                "ec2:DescribeTrafficMirrorFilters",
                "ec2:DescribeVpcEndpointServiceConfigurations",
                "ec2:DescribeVpcEndpoints",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedRolePolicies",
                "iam:ListRolePolicies",
                "iam:ListAccountAliases",
                "kms:ListAliases",
                "kms:GenerateDataKeyWithoutPlaintext"
            ],
            "Resource": "*"
        }
    ]
}
```

For more information regarding policies and permissions, refer to AWS Documentation.

If you are using inline policy or basic authentication, then you must update the policy with the relevant IAM service. For more information, see Prerequisites.

Create the AWS Credentials

You can monitor workloads across multiple AWS accounts within one Monitoring Domain.

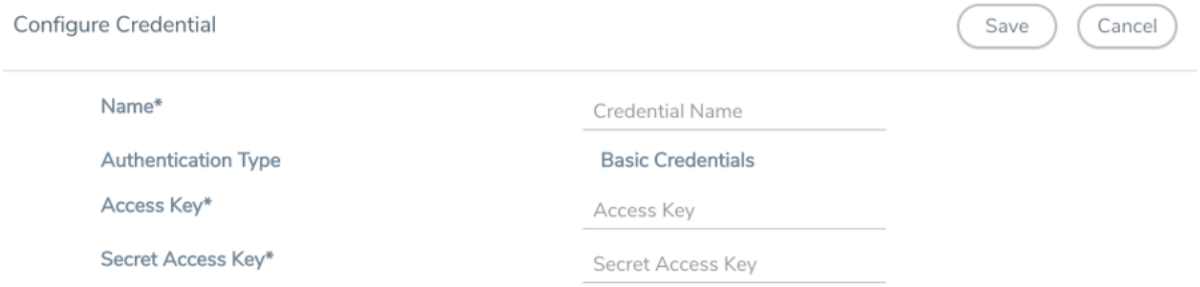
- After launching GigaVUE-FM in AWS, if the IAM is attached to the running instance of FM, then the **EC2 Instance Role** authentication credential is automatically added to the **Credential** page as the default credential. You must attach the IAM prior to creating a Monitoring Domain.

- If you use the **Basic Credentials** authentication credentials, you must add these to the GigaVUE-FM on the **AWS Settings** page, or on the Monitoring Domain creation page.

  For details, refer to Create a Monitoring Domain.

To create AWS credentials:

1. Go to **Inventory > VIRTUAL > AWS**, and select **Settings > Credentials**
2. On the **Credential** page, select **Add**. The **Credential Configure** page appears.



3. Enter a name to identify the AWS Credential in the **Name** Field.
4. Basic Credentials is selected as the default **Authentication Type**. For more information, refer to AWS Security Credentials
5. Enter the credential of an IAM user or the AWS account root user in the **Access Key** field.
6. Enter the security password or key in the **Secret Access Key** field.
7. Select **Save**. You can view the list of available credentials on the AWS Credential page.

Configure Gateway Load Balancer and deploy GigaVUE V Series Nodes

Prerequisites

- Create or update Security Group policies of GigaVUE Cloud Suite components. For details, refer to Security Group topic for detailed information.
- Create or update route tables in the VPCs across all mirrored AWS accounts. Ensure each mirrored account VPC can connect to the target account VPC where you deploy the Gateway Load Balancer. For details, refer to Subnet and Security Group for Amazon VPC.
- Create or update an IAM role for GigaVUE-FM in the centralized VPC. Establish a trust relationship between the mirrored and the target account for GigaVUE-FM to execute the above permissions at the IAM role level. For details, refer to Permissions and Privileges (AWS).
  For more information on AWS recommended design for Gateway Load Balancer implementation with inline services, such as firewall. see Getting started with Gateway Load Balancers - Elastic Load Balancing (amazon.com)

- Create a VPC endpoint and endpoint service. For more information, see Create endpoint service
- Create a routing table. For more information, see Amazon documentation.
- Configure a token in the **User Management** page. For details, refer to Configure Tokens.

Points to Note:

When configuring Gateway Load Balancer, you need to deploy the GigaVUE V Series Nodes using Third Party Orchestration.

Perform the following steps to configure an external load balancer in AWS:

1. Create a Target Group
2. Create a Load Balancer
3. Create a Launch Template for Auto Scaling group
4. Create an Auto Scaling group using a Launch Template

Create a Target Group

Enter or select the following details as mentioned in the table to configure target groups in AWS.

Parameters	Description	Reference	Mandatory field
Basic Configuration			
Choose a target type	Select IP address as the target type	Create a target group for your Gateway Load Balancer	Yes
Protocol	Verify that Protocol is GENEVE		Yes
Port	Verify that the port value is 6081		Yes
Health Checks			
HealthCheckProtocol	Select TCP as the protocol.	Health checks for Gateway Load Balancer target groups	Yes
HealthCheckPort	Enter 8888 as the port.		Yes
HealthCheckIntervalSeconds	Enter 10 seconds as the approximate amount of time, in seconds.		Yes

Create a Load Balancer

Enter or select the following details as mentioned in the table to configure a load balancer in AWS.

Parameters	Description	Reference	Mandatory field
Network Mapping			
VPC	Select the VPC for your targets (GigaVUE V Series Node)	Create a Gateway Load Balancer	Yes
IP Listener routing			
Default action	Select the target group to receive traffic. If you don't have a target group, choose Create target group.	Create a target group	Yes

Create a Launch Template for Auto Scaling group

Enter or select the following details to create a launch template for auto scaling groups in AWS.

Parameters	Description	Reference	Mandatory field
Launch Template contents			
Application and OS Images (Amazon Machine Image)	Select the AMI of the GigaVUE V Series Node.	Create a launch template for an Auto Scaling group	Yes
Instance type	Select **c5n.xlarge** as the instance type.		Yes
Key pair name	Select a Key pair for the instance.		Yes
Network Settings			
Device Index	Add 2 Network Interfaces for the GigaVUE V Series Node with device index as **0** and **1** (mgmt and data interface respectively) and for the interfaces,	Create a launch template for an Auto Scaling group	Yes

Parameters	Description	Reference	Mandatory field
Firewall (security groups)	Keep this blank and configure one or more security groups as part of the network interface.		Yes
Advanced Settings			

Advanced details	Enter the User data as text in the following format and deploy the instance. The GigaVUE V Series Nodes uses this user data to generate config file (**/etc/gigamon-cloud.conf**) used to register with GigaVUE-FM using Third Party Orchestration.
	`#cloud-config`
	`write_files:`
	`- path: /etc/gigamon-cloud.conf`
	`owner: root:root`
	`permissions: '0644'`
	`content: |`
	`Registration:`
	`groupName: <Monitoring Domain Name>`
	`subGroupName: <VPC Name>`
	`token: <Token>`
	`remoteIP: <IP address of the GigaVUE-FM>`
	`remotePort: 443`
		Create a launch template using advanced settings	Yes

Create an Auto Scaling group using a Launch Template

Enter or select the following details to create an auto scaling group and launch the fabric components using the launch template in AWS.

Parameters	Description	Reference	Mandatory field
Configure group size and scaling policies			
Group Size	Enter the Desired capacity as 0. The Desired capacity value must be less than the Maximum Capacity value. **Note**: Once the monitoring Domain and connection is configured, edit this value to the number of GigaVUE V Series Node.	Creating an Auto Scaling group using a launch template	Yes
Automatic Scaling	Select **Target tracking scaling policy** and enter the following details to define a policy: Metric Type: 1000000000 (bytes) Instance warmup: **300** seconds	Create a target tracking scaling policy	Yes
Add tag	Provide a tag key and value for each tag.	Tag Auto Scaling groups and instances	No

In the Instances page, you can view the GigaVUE V Series Node instance that the load balancer deploys.

Configure and Deploy Monitoring Session

In GigaVUE-FM, you must do the following to configure and deploy the Monitoring Session. Refer to Configure Monitoring Session section for more details.

1. **Access the Monitoring Session Page**:
   a. In GigaVUE-FM, go to **Traffic** > **Virtual** > **Orchestrated Flows > AWS**.
   b. 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.
2. **Add components to the canvas**:
   a. Drag and drop the required components to the canvas.
   b. From the **Applications** expand menu, drag and drop the required applications to the graphical workspace.
3. **Deploy the Monitoring Session**:
   a. From the **Actions** menu, select **Deploy**.
   b. After successful deployment on all the V Series Nodes, the status appears as **Success** on the Monitoring Sessions **Sources** tab.

What to do Next

You can view the detailed statistics of an individual traffic processing element in the **TRAFFIC PROCESSING** tab. For more details, refer to View Monitoring Session Statistics (AWS).

Acquire Traffic using Customer Orchestrated Source - GigaVUE-FM Orchestration

This section outlines the workflow for acquiring traffic with Customer Orchestrated Source and deploying GigaVUE Fabric Components using GigaVUE-FM.Refer to the following topics for instruction on configuring traffic acquisition, processing, and forwarding to your desired destination.

- Install GigaVUE-FM on AWS
- Configure the permissions required in AWS
- Create the AWS Credentials
- Create a Monitoring Domain

- Deploy GigaVUE Fabric Components in GigaVUE-FM
- Configure and Deploy Monitoring Session

Install GigaVUE-FM on AWS

This step is optional and applies only when an existing GigaVUE-FM instance is not available.
Refer to Install GigaVUE-FM on AWS for steps to install GigaVUE-FM on AWS and the steps to start GigaVUE-FM instance and configure it.

Configure the permissions required in AWS

If you are using inline policy or basic authentication, then you must update the policy with the relevant IAM service. For details, see Minimum Permissions Required for Inline Policies and Basic Authentication.

These are the minimum permissions that are required to acquire traffic using the customer orchestrated, use a GigaVUE V Series Proxy and authenticate using an IAM instance role.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags",
                "ec2:DeleteTags",
                "ec2:RunInstances",
                "ec2:TerminateInstances",
                "ec2:AssociateAddress",
                "ec2:DisassociateAddress",
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeVolumes",
                "ec2:DescribeAddresses",
                "ec2:RebootInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                “ec2:AssociateAddress”,
                “ec2:DisassociateAddress”,
                “ec2:RebootInstances”,
                “ec2:StartInstances”,
                “ec2:StopInstances”,
                “ec2:RunInstances”,
                “ec2:TerminateInstances”,
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
```

```
                "iam:ListAttachedRolePolicies",
                "iam:ListRolePolicies",
                "iam:ListAccountAliases",
                "kms:ListAliases",
                "kms:GenerateDataKeyWithoutPlaintext"
            ],
            "Resource": "*"
        }
    ]
}
```

For more information regarding policies and permissions, refer to AWS Documentation.

Create the AWS Credentials

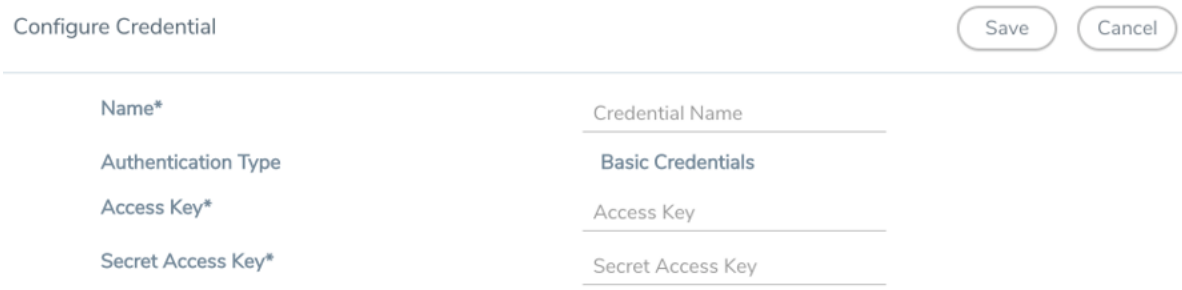
You can monitor workloads across multiple AWS accounts within one Monitoring Domain.

- After launching GigaVUE-FM in AWS, if the IAM is attached to the running instance of FM, then the **EC2 Instance Role** authentication credential is automatically added to the **Credential** page as the default credential. You must attach the IAM prior to creating a Monitoring Domain.
- If you use the **Basic Credentials** authentication credentials, you must add these to the GigaVUE-FM on the **AWS Settings** page, or on the Monitoring Domain creation page.

For details, refer to Create a Monitoring Domain.

To create AWS credentials:

1. Go to **Inventory > VIRTUAL > AWS**, and select **Settings > Credentials**
2. On the **Credential** page, select **Add**. The **Credential Configure** page appears.



3. Enter a name to identify the AWS Credential in the **Name** Field.
4. Basic Credentials is selected as the default **Authentication Type**. For more information, refer to AWS Security Credentials
5. Enter the credential of an IAM user or the AWS account root user in the **Access Key** field.

6. Enter the security password or key in the **Secret Access Key** field.
7. Select **Save**. You can view the list of available credentials on the AWS Credential page.

Create a Monitoring Domain

GigaVUE-FM connects to the AWS Platform through the public API endpoint and uses HTTPS, the default protocol to communicate with API. For more information about the endpoint and the protocol used, refer to AWS service endpoints.

GigaVUE-FM provides you the flexibility to monitor multiple VPCs. You can choose the VPC ID and launch the GigaVUE fabric components in the desired VPCs.

NOTE: To configure the Monitoring Domain and launch the fabric components in AWS, you must have the **fm_super_admin** role or the write access to the **Infrastructure Management** category. For details, refer to Role Based Access Control.

To create a Monitoring Domain:

1. Go to **Inventory > VIRTUAL > AWS** , and select **Monitoring Domain**.
2. On the **Monitoring Domain** page, select **New**. The **Monitoring Domain Configuration** page appears.
3. Select **Check Permissions** and validate whether you have the required permissions.
4. In the **Monitoring Domain** field, enter an alias used to identify the Monitoring Domain.
5. From the **Traffic Acquisition Method** drop-down list, select one of the following tapping methods:
   - **Customer Orchestrated Source**: If you select **Customer Orchestrated Source** as the tapping method, you can use the Customer Orchestrated Source as a source option in the Monitoring Session, where the traffic is directly tunneled to the GigaVUE V Series nodes without deploying UCT-Vs and UCT-V Controllers. The user is responsible for creating this tunnel feed and pointing it to the GigaVUE V Series Node(s).

     NOTE: When using Application Metadata Exporter (AMX) application, select the **Traffic Acquisition Method** as **Customer Orchestrated Source**.

6. In the **Traffic Acquisition Tunnel MTU**, enter the MTU value. The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry from the UCT-V to the GigaVUE V Series Node. The default value is 8951.
   - When using IPv4 tunnels, the maximum MTU value is 8951. Ensure that the UCT-V tunnel MTU is 50 bytes less than the destination interface MTU size of the UCT-V.
   - When using IPv6 tunnels, the maximum MTU value is 8931. Ensure that UCT-V tunnel MTU is 70 bytes less than the destination interface MTU size of the UCT-V.
7. Enable the **Use FM to Launch Fabric** toggle, to deploy GigaVUE Fabric Components using GigaVUE-FM.
8. Turn on the **Enable IPv6 Preference** toggle to create IPv6 tunnels between UCT-V and the GigaVUE V Series Nodes.

   NOTE: This appears only when **Use FM to Launch Fabric** is disabled and **Traffic Acquisition Method** is **UCT-V**.
9. Under Connections, in the **Name** field, enter an alias used to identify the connection.
10. From the **Credential** drop-down list, select an AWS credential. For details, refer to Create AWS Credentials.
11. From the **Region** drop-down list, select AWS region for the Monitoring Domain. For example, US West.

    NOTE: China regions are not supported.
12. From the **Accounts** drop-down list, select the AWS accounts.
13. From the **VPCs** drop-down list, select the VPCs to monitor.
14. Click **Save**.

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 view the new Monitoring Domain in the **Monitoring Domain** page list view.

To edit a Monitoring Domain, select the deployed Monitoring Domain and select **Actions**. From the drop-down list, select **Edit** and the **Monitoring Domain Configuration** page appears.

For details regarding the Check permissions while creating a Monitoring Domain, refer to Manage a Monitoring Domain .

Deploy GigaVUE Fabric Components in GigaVUE-FM
You can configure the following fabric components:

- UCT-V Controller
- GigaVUE V Series Proxy
- GigaVUE V Series Node

Prerequisite

Before you begin, create a monitoring domain in GigaVUE-FM to establish connection between your AWS environment and GigaVUE-FM. For details, refer to Create a Monitoring Domain.

To configure,

1. Go to **Inventory > VIRTUAL > AWS**.
2. Select the required Monitoring Domain and select **Actions > Deploy Fabric**.

   The **AWS Fabric Launch Configuration** page appears.
3. From the **Centralized VPC** drop-down list, select the alias of the centralized VPC.
4. Centralized VPC refers to the launch location of UCT-V Controller, V Series Proxies, and the GigaVUE V Series Nodes.

   NOTE: Select **Check Permissions** to ensure you have the required permissions for inventory, security groups, fabric launch, and IAM policy. For details, refer to Acquire Traffic using Customer Orchestrated Source - GigaVUE-FM Orchestration.
5. From the EBS Volume Type drop-down list, select one of the following Elastic Block Store (EBS) volume that you can attach to the fabric components:
   - gp2 (General Purpose SSD)
   - gp3 (General Purpose SSD)
   - io1 (Provisioned IOPS SSD)
   - io2 (Provisioned IOPS SSD)
   - Standard (Magnetic)

   NOTE: The default EBS Volume Type is **gp3 (General Purpose SSD)**.
6. Turn on the **Enable Encryption** toggle to encrypt the EBS volume with AWS Key Management Service (KMS).
7. From the **KMS Key** drop-down list, select the required KMS key. For details, refer to the Create a KMS Key section in the AWS Documentation.

8. From the **SSH Key Pair** drop-down list, select the key pair that you created to launch the UCT-V Controller, GigaVUE V Series node, and GigaVUE V Series Proxy from GigaVUE-FM. For details, refer to the Create a key pair section in the AWS Documentation.
9. From the **Management Subnet** drop-down list, select the subnet you use for communication between the controllers and the nodes and with GigaVUE-FM.
10. From the **Security Groups** drop-down list, select one or more security groups you created for the GigaVUE fabric nodes. For details, refer to Security Group.
11. Turn on the **Enable Custom Certificates** toggle to validate the custom certificate during SSL Communication.

    GigaVUE-FM validates the Custom certificate with the Trust Store. If the certificate is unavailable in the Trust Store, communication does not happen, and a handshake error occurs.

    NOTE: If the certificate expires after the successful deployment of the fabric components, the fabric components move to the failed state.
12. From the **Custom SSL Certificate** drop-down list, select the custom certificate that you have already installed.

    NOTE: You can also select **Create New** to upload the custom certificate for GigaVUE V Series Nodes, GigaVUE V Series Proxy, and UCT-V Controllers. For details, refer to Install Custom Certificate on AWS.
13. Turn on the **Prefer IPv6** toggle to deploy all the fabric controllers and the tunnel between the hypervisor and GigaVUE V Series Nodes using an IPv6 address.

    If the IPv6 address is unavailable, it uses an IPv4 address.

    NOTE: You can enable this option only when deploying a new GigaVUE V Series Node. If you want to enable this option after deploying the GigaVUE V Series Node, you must delete the existing GigaVUE V Series Node and deploy it again with this option enabled.
14. Complete the required fields to configure the following GigaVUE Fabric Components:
    - **UCT-V Controller** – Configure UCT-V Controllers in the AWS cloud only if you want to capture traffic using UCT-Vs. A UCT-V Controller can manage only UCT-Vs that have the same version. If the version of UCT-V Controllers do not match the version of UCT-Vs, GigaVUE-FM cannot detect the UCT-Vs in the instances.
    - **GigaVUE V Series Proxy** – Turn on the **Configure a V Series Proxy** toggle, if GigaVUE-FM cannot directly reach the GigaVUE V Series Nodes (management interface) directly over the network.
    - **GigaVUE V Series Node** – Creating a GigaVUE V Series Node profile automatically launches the GigaVUE V Series Nodes.

> **NOTE:** Refer to GigaVUE Fabric Components Configuration – Field References.

15. Select **Save**.

GigaVUE Fabric Components Configuration – Field References

The following table lists and describes the fields you must complete to configure the UCT-V Controller, GigaVUE V Series Proxy, and GigaVUE V Series Node.

Field	Description
UCT-V Controller • Configure UCT-V Controllers in the AWS cloud only if you want to capture traffic using UCT-Vs. • A UCT-V Controller can manage only UCT-Vs that have the same version. If there is a version mismatch between the UCT-V Controllers and UCT-Vs, GigaVUE-FM cannot detect the UCT-Vs in the instances.	
Controller Version(s)	To add UCT-V Controllers: **a.** Under **Controller Versions**, click **Add**. **b.** From the **Version** drop-down list, select a UCT-V Controller image that matches with the version number of UCT-Vs installed in the instances. **c.** From the **Instance Type** drop-down list, select a size for the UCT-V Controller. Refer to Recommended Instance Types for AWS. **d.** In the **Number of Instances** field, enter the number of UCT-V Controllers to launch. The minimum number you can enter is 1.
Agent Tunnel Type	Select one of the following tunnel types to send the traffic from UCT-Vs to GigaVUE V Series Nodes: • GRE • VXLAN – Select this type if Windows UCT-Vs co-exist with Linux UCT-Vs. • Secure tunnels (TLS-PCAPNG)
Agent CA	Select the Certificate Authority (CA) you want to use to connect the tunnel. UCT-V uses this CA to verify the server-side certificate of the GigaVUE V Series Node. **NOTE:** Use this field only when configuring secure tunnels.
IP Address Type	Select one of the following IP address types: • Private – If you want to assign an IP address that is not reachable over Internet. You can use private IP address for communication between the UCT-V Controller and GigaVUE-FM. • Public – If you want the IP address to be assigned from Amazon's pool of public IP address. The public IP address changes every time the instance is stopped and restarted. • Elastic—If you want a static public IP address for your instance, ensure that you have the elastic IP address available in your VPC. The elastic IP address does not change when you stop or start the instance. o From the **Elastic IPs** drop-down list, select the required IP addresses.
Additional Subnets	[Optional] If UCT-Vs are available on networks that are not IP routable from the management network, you must specify additional networks or subnets so that the UCT-V Controller can communicate with all the UCT-Vs. Click **Add Subnet** to select additional networks (subnets) if needed. Make sure to

Field	Description
	select a list of security groups for each additional network.
Tags	[Optional] The key name and value that helps to identify the UCT-V Controller instances in your environment. For example, you might have deployed UCT-V Controller in many regions. To distinguish these UCT-V Controllers based on the regions, you can provide a name (also known as a tag) that is easy to identify such as us-west-2- uctvcontrollers. To add a tag, select **Add**, and enter a **Key** and **Value**. For example, enter Name as your **Key** and us-west-2-uctv-controllers as the **Value**.
GigaVUE V Series Proxy	
Version	GigaVUE V Series Proxy version.
Instance Type	Instance type for the GigaVUE V Series Proxy. The recommended minimum instance type is t2.micro. You can review and modify the number of instances for the nitro-based instance types in the Configure AWS Settings page.
Number of Instances	Number of GigaVUE V Series Proxy to deploy in the monitoring domain.
Set Management Subnet	Use the toggle button to select a management subnet. • **Yes** to use the management subnet that you selected previously. • **No** to use another management subnet.
Set Security Groups	Toggle option to **Yes** to set the security group that is created for the GigaVUE V Series Proxy. Refer to Security Group for more details.
IP Address Type	Select one of the following IP address types: ▪ Select **Private** if you want to assign an IP address that is not reachable over Internet. You can use private IP address for communication between the GigaVUE V Series Proxy and GigaVUE-FM instances in the same network. ▪ Select **Public** if you want the IP address to be assigned from Amazon's pool of public IP address. The public IP address gets changed every time the instance is stopped and restarted. ▪ Select **Elastic** if you want a static IP address for your instance. Ensure to have the available elastic IP address in your VPC. The elastic IP address does not change when you stop or start the instance.
Additional Subnets	(Optional) If there are GigaVUE V Series Nodes on subnets that are not IP routable from the management subnet, additional subnets must be specified so that the GigaVUE V Series Proxy can communicate with all the GigaVUE V Series Nodes. Select **Add** to specify additional subnets, if needed. Also, make sure that you specify a list of security groups for each additional subnet.
Tags	(Optional) The key name and value that help to identify the GigaVUE V Series Proxy instances in your AWS environment.
GigaVUE V Series Node	
SSL Key	Select the SSL key from the drop-down list.
Version	Enter the GigaVUE V Series Node version.
Instance Type	The instance type for the GigaVUE V Series Node. For details, refer to Recommended and Supported Instance Types for AWS.

Field	Description
	You can review and modify the number of instances for the nitro-based instance types in the Configure AWS Settings page.
Volume Size	The size of the storage disk. The default volume size is 8. The recommended volume size is 80. **NOTE:** When using Application Metadata Exporter, the minimum recommended Volume Size is 80GB.
IP Address Type	Select one of the following IP address types: ▪ Select **Private** if you want to assign an IP address that is not reachable over Internet. You can use private IP address for communication between the GigaVUE V Series Controller and GigaVUE-FM instances in the same network. ▪ Select **Elastic** if you want a static IP address for your instance. Ensure to have the available elastic IP address in your VPC. The elastic IP address does not change when you stop or start the instance.
Min Number of Instances	The minimum number of GigaVUE V Series Nodes in the Monitoring Domain. The minimum number of instances must be 1. **NOTE:** If the minimum number of instances is set as '0', then the GigaVUE V Series nodes launch only when GigaVUE-FM discovers some targets to monitor and deploys a monitoring session.
Max Number of Instances	The maximum number of GigaVUE V Series Nodes deployed in the Monitoring Domain.
Data Subnets	The subnet that receives the mirrored GRE or VXLAN tunnel traffic from the UCT-Vs. **NOTE:** Using the Tool Subnet check box, you can indicate the subnets the GigaVUE V Series uses to egress the aggregated/manipulated traffic to the tools.
Tags	(Optional) The key name and value that helps to identify the GigaVUE V Series Node instances in your AWS environment. For example, you might have GigaVUE V Series Node deployed in many regions. To distinguish these GigaVUE V Series Node based on the regions, you can provide a name that is easy to identify, such as us-west-2-vseries. To add a tag: a. Select **Add tag**. b. In the **Key** field, enter the key. For example, enter Name. c. In the **Value** field, enter the key value. For example, us-west-2-vseries.

For details regarding the Check permissions to validate IAM and security-group settings, refer to Check Permissions while Configuring GigaVUE Fabric Components using GigaVUE-FM.

Configure and Deploy Monitoring Session

In GigaVUE-FM, you must do the following to configure and deploy the Monitoring Session. Refer to Configure Monitoring Session section for more details.

1. **Access the Monitoring Session Page**:

a. In GigaVUE-FM, go to **Traffic** > **Virtual** > **Orchestrated Flows > AWS**.

b. 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.

2. **Create an ingress REP**:

   a. In the canvas, from the **New** expand menu, drag and drop New Tunnel to the graphical workspace.

   b. On the new tunnel icon, select the ⋮ menu button and select **Details**. The **Add Tunnel Spec** quick view page appears.

   c. Enter the **Alias**, **Description**, and the **Type** details and click **Save**.

3. **Add components to the canvas**:

   a. Drag and drop the required components to the canvas.

   b. From the **Applications** expand menu, drag and drop the required applications to the graphical workspace.

4. **Deploy the Monitoring Session**:

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

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

What to do Next

You can view the detailed statistics of an individual traffic processing element in the **TRAFFIC PROCESSING** tab. For more details, refer to View Monitoring Session Statistics (AWS).

Acquire Traffic using Customer Orchestrated Source with Network Load Balancer

This section outlines the workflow for acquiring traffic using Customer Orchestrated Source with Network Load Balancer. Refer to the following topics for instruction on configuring traffic acquisition, processing, and forwarding to your desired destination.

- Install GigaVUE-FM on AWS
- Configure the permissions required in AWS
- Create the AWS Credentials
- Configure Role-Based Access for Third Party Orchestration
- Configure Tokens
- Configure Network Load Balancer and deploy GigaVUE V Series Nodes

- Deploy Visibility Fabric with Network Load Balancer
- Configure and Deploy Monitoring Session

Install GigaVUE-FM on AWS

This step is optional and applies only when an existing GigaVUE-FM instance is not available.
Refer to Install GigaVUE-FM on AWS for steps to install GigaVUE-FM on AWS and the steps to start GigaVUE-FM instance and configure it.

Configure the permissions required in AWS

If you are using inline policy or basic authentication, then you must update the policy with the relevant IAM service. For more information, see Minimum Permissions Required for Inline Policies and Basic Authentication.

These are the minimum permissions that are required to acquire traffic using Traffic Mirroring with Network Load Balancer and authenticate using an IAM instance role.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "autoscaling:DescribeAutoScalingGroups",
                "elasticloadbalancing:DescribeLoadBalancers",
                "elasticloadbalancing:DescribeTargetGroups",
                "elasticloadbalancing:RegisterTargets",
                "elasticloadbalancing:DeregisterTargets",
                "elasticloadbalancing:DescribeTargetHealth",
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeAddresses",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeSecurityGroups",
                "ec2:CreateTags",
                "ec2:DeleteTags",
                "ec2:DescribeImages",
                "ec2:DescribeVolumes",
                "ec2:CreateTrafficMirrorFilterRule",
                "ec2:CreateTrafficMirrorTarget",
                "ec2:CreateTrafficMirrorSession",
                "ec2:CreateTrafficMirrorFilter",
                "ec2:DeleteTrafficMirrorTarget",
                "ec2:DeleteTrafficMirrorSession",
                "ec2:DeleteTrafficMirrorFilter",
                "ec2:DescribeTrafficMirrorSessions",
                "ec2:DescribeTrafficMirrorTargets",
                "ec2:DescribeTrafficMirrorFilters",
                "ram:CreateResourceShare",
```

```
                "ram:DeleteResourceShare",
                "ram:GetResourceShareInvitations",
                "ram:AcceptResourceShareInvitation",
                "ram:DisassociateResourceShare",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedRolePolicies",
                "iam:ListRolePolicies",
                "iam:ListAccountAliases",
                "kms:GenerateDataKeyWithoutPlaintext",
                "kms:ListAliases",
            ],
            "Resource": "*"
        }
    ]
}
```

For more information regarding policies and permissions, refer to AWS Documentation.

If you are using inline policy or basic authentication, then you must update the policy with the relevant IAM service. For more information, see Prerequisites.

Create the AWS Credentials

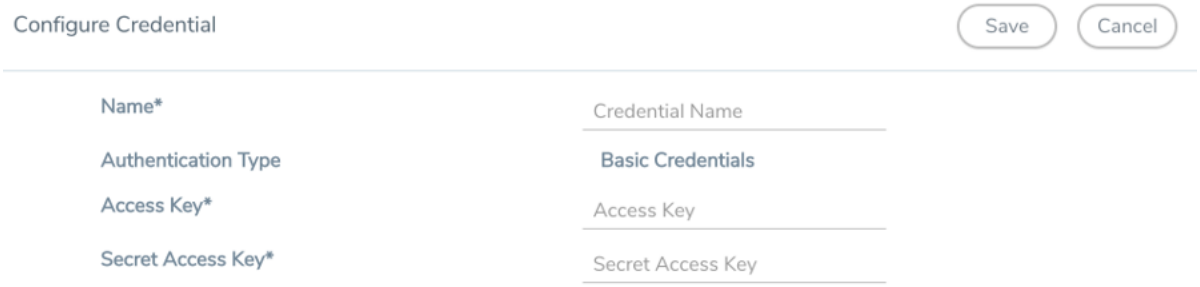
You can monitor workloads across multiple AWS accounts within one Monitoring Domain.

- After launching GigaVUE-FM in AWS, if the IAM is attached to the running instance of FM, then the **EC2 Instance Role** authentication credential is automatically added to the **Credential** page as the default credential. You must attach the IAM prior to creating a Monitoring Domain.
- If you use the **Basic Credentials** authentication credentials, you must add these to the GigaVUE-FM on the **AWS Settings** page, or on the Monitoring Domain creation page.

For details, refer to Create a Monitoring Domain.

To create AWS credentials:

1. Go to **Inventory > VIRTUAL > AWS**, and select **Settings > Credentials**
2. On the **Credential** page, select **Add**. The **Credential Configure** page appears.



3. Enter a name to identify the AWS Credential in the **Name** Field.
4. Basic Credentials is selected as the default **Authentication Type**. For more information, refer to AWS Security Credentials
5. Enter the credential of an IAM user or the AWS account root user in the **Access Key** field.
6. Enter the security password or key in the **Secret Access Key** field.
7. Select **Save**. You can view the list of available credentials on the AWS Credential page.

Configure Role-Based Access for Third Party Orchestration

If you do not want to use an **Admin Profile** to deploy GigaVUE V Series through a Third Party orchestrator, you can create the required users, roles, and user groups in GigaVUE-FM.

Create a Custom User

You can add users only if you are a user with **fm_super_admin role** or a user with either read or write access to the GigaVUE-FM security Management category.

To add users:

1. Go to **Settings** and select **Authentication** > **GigaVUE-FM User Management > Users**.
2. On the User page, select **New User**.
3. In the Add User page, enter the following details:
   - **Name:** Actual name of the user
   - **Username**: User name configured in GigaVUE-FM
   - **Email**: Email ID of the user
   - **Password/Confirm Password**: Password for the user. For more details, refer to Change Your Password.
   - **User Group:** Select the desired User Group to associate the user.

   GigaVUE-FM prompts for your password.
4. Click **Ok**. The new user is added.

Create a Custom Role and Assign the User

A user role defines permission for users to perform any task or operation in GigaVUE-FM or on the managed device. You can associate a role with user.

> **NOTE:** A user with read-only access cannot perform configurations on the screen. The menus and action buttons in the UI pages are disabled appropriately.

To create a role:

1. Go to **Settings** and select **Authentication> GigaVUE-FM User Management >Roles**.
2. Select **New Role**.
3. In the New Role page, select or enter the following details:
   - **Role Name**: Name of the role.
   - **Description**: Description of the role.
   - **Select Permission**: From the **Select Permissions** tab, select **Third Party Orchestration**, and provide write permissions.
4. Select **Apply** to save the configuration.

Create a Custom User Group and Assign the Custom Role and the User

A user group consists of a set of roles and set of tags associated with users in that group. You can associate the user to one or more groups.

To create a new user group:

1. Go to **Settings**, and then select **Authentication> GigaVUE-FMUser Management >User Groups**.
2. Select **New Group.**
3. In the New User Group page, select **Next** to progress forward and **Back** to navigate backward.
4. In the **Group Info** tab, enter the Group Name and Description details:
5. In the **Assign Roles** tab, select the role that you want to assign to the user group.
6. In the **Assign Tags** tab, select the required tag key and tag value.
7. In the **Assign Users** tab, select the required users.
8. Select **Apply** to save the configuration. The new user group is added.

Configure Tokens

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.

You can create tokens only if you are a user with fm_super_admin role or a user with write access to the GigaVUE-FM security Management category.

To create a token:

1. Go to **Settings > Authentication** > **GigaVUE-FM User Management**. The **User Management** page appears.
2. Select **Current User Tokens** from the **Tokens** drop-down list.
3. Click **New Token**. The **New Token** pop-up appears.
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 the GigaVUE-FM from the **User Group** drop-down list. The token inherits the read or write RBAC privileges of this group.
7. Select **OK** to generate a new token. You can copy and use the generated token to authenticate the GigaVUE-FM REST APIs.

Configure Network Load Balancer and deploy GigaVUE V Series Nodes

You can configure an external Network Load Balancer (NLB) in AWS for GigaVUE Cloud Suite.

Prerequisites

- Create or update Security Group policies of GigaVUE Cloud Suite components. For details, refer to Security Group.
- Create or update routes in various VPCs across participating mirrored AWS accounts so that all mirrored account VPCs can connect to the target account VPC where the AWS Network Load Balancer is deployed.

  NOTE: GigaVUE-FM considers the target account VPC as the centralized VPC. Use the connections towards all other mirrored account VPCs either through 1 : 1 VPC peering or via 1 : M transit gateway (that connects all participating VPCs across mirrored AWS accounts). VPC peering has no bandwidth limitation and no additional cost within the same region (recommended). Transit gateway costs more and also has a limitation of 50 Gbps burst per VPC.
- Create or update existing IAM role for GigaVUE-FM in the centralized VPC. In addition, you need to create trust relationship between the mirrored and the target account for GigaVUE-FM to execute the above permissions at the IAM role level. For details, refer to Permissions and Privileges (AWS).
- When configuring Network Load Balancer, you need to deploy the GigaVUE V Series Nodes using Third Party Orchestration.
- You need to configure Token \in the **User Management** page. For details, refer to Configure Tokens.

Perform the following steps to configure an external network load balancer in AWS:

1. Create a Target Group
2. Create a Load Balancer
3. Create a Launch Template for Auto Scaling group
4. Create an Auto Scaling group using a Launch Template

Create a Target Group

Enter or select the following details to configure target groups in AWS.

Parameters	Description	Reference	Mandatory field
Basic Configuration			
Choose a target type	Select IP address as the target type	Create a target group for your Network Load Balancer	Yes
Protocol	Select UDP as the protocol from the drop-down list		Yes
Port	Enter 4789 as the port value		Yes
Health Checks			
HealthCheckProtocol	Select TCP as the protocol.	Health checks for Network Load Balancer target groups	Yes
HealthCheckPort	Enter 8888 as the port.		Yes
HealthCheckIntervalSeconds	Enter 10 seconds as the approximate amount of time, in seconds.		Yes

Create a Load Balancer

Enter or select the following details to configure a load balancer in AWS.

Parameters	Description	Reference	Mandatory field
Basic Configuration			
Scheme	Select Internal as the scheme for the load balancer	Create a Network Load Balancer	Yes
Network Mapping			
VPC	Select the VPC for your targets (GigaVUE V Series Node)	Create a Network Load Balancer	Yes

Parameters	Description	Reference	Mandatory field
Listeners and routing			
Protocol	Select UDP as the protocol.	Create a Network Load Balancer	Yes
Port	Enter 4789 as the port.		Yes

Create a Launch Template for Auto Scaling group

Enter or select the following details to create a launch template for auto scaling groups in AWS.

Parameters	Description	Reference	Mandatory field
Launch Template contents			
Application and OS Images (Amazon Machine Image)	Select the AMI of the GigaVUE V Series Node.	Create a launch template for an Auto Scaling group	Yes
Instance type	Select **t3a.xlarge** as the instance type.		Yes
Key pair name	Select a Key pair for the instance.		Yes
Network Settings			
Device Index	Add 2 Network Interfaces for the GigaVUE V Series Node with device index as **0** and **1** (mgmt and data interface respectively) and for the interfaces,	Create a launch template for an Auto Scaling group	Yes

Parameters	Description	Reference	Mandatory field
Firewall (security groups)	Keep this blank and configure one or more security groups as part of the network interface.		Yes
Advanced Settings			

Advanced details	Enter the User data as text in the following format and deploy the instance. The GigaVUE V Series Nodes uses this user data to generate config file (**/etc/gigamon-cloud.conf**) used to register with GigaVUE-FM using Third Party Orchestration.
	`#cloud-config`
	`write_files:`
	`- path: /etc/gigamon-cloud.conf`
	`owner: root:root`
	`permissions: '0644'`
	`content: |`
	`Registration:`
	`groupName: <Monitoring Domain Name>`
	`subGroupName: <VPC Name>`
	`token: <Token>`
	`remoteIP: <IP address of the GigaVUE-FM>`
	`remotePort: 443`
		Create a launch template using advanced settings	Yes

Create an Auto Scaling group using a Launch Template

Enter or select the following details to create an auto scaling group and launch the fabric components using the launch template in AWS.

Parameters	Description	Reference	Mandatory field
Configure group size and scaling policies			
Group Size	Enter the Desired capacity as 0. Ensure that the Desired capacity value is less that the Maximum Capacity value. **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.	Creating an Auto Scaling group using a launch template	Yes

Parameters	Description	Reference	Mandatory field
Automatic Scaling	Select **Target tracking scaling policy** and enter the following details to define a policy: • Metric Type: 1000000000 (bytes) • Instance warmup: **300** seconds	Create a target tracking scaling policy	Yes
Add tag	Provide a tag key and value for each tag. • Tag key - GigamonNode • Value - VSeriesNode	Tag Auto Scaling groups and instances	Yes

In the Instances page, you can view the GigaVUE V Series Node instance that the load balancer deployed.

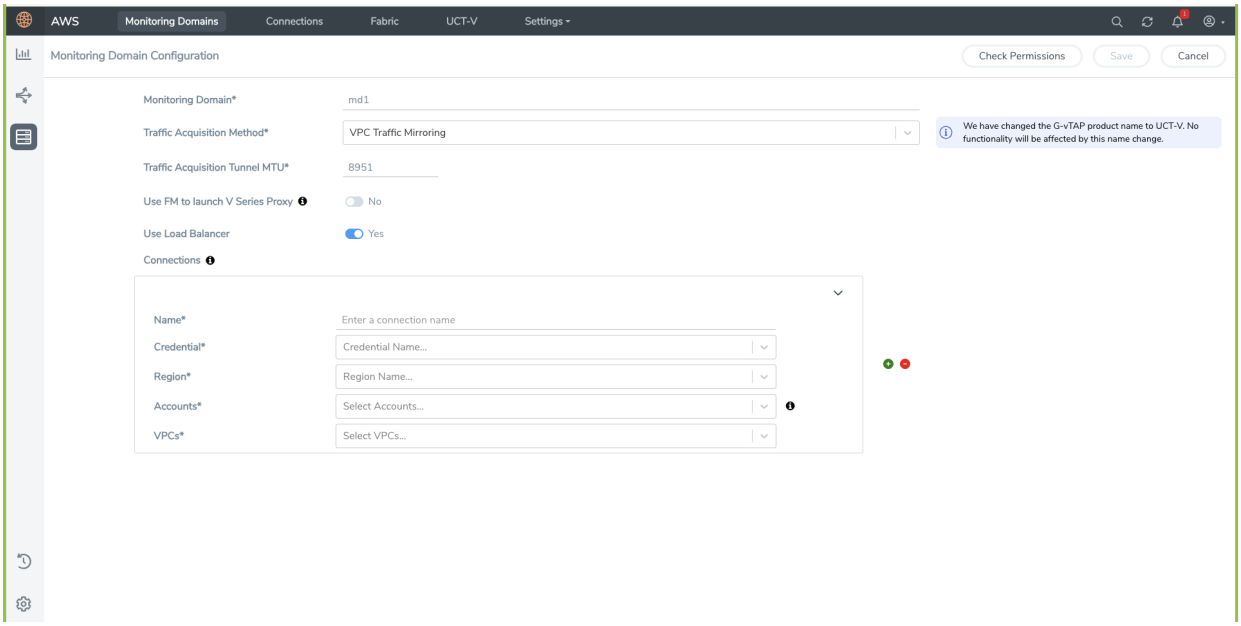
Deploy Visibility Fabric with Network Load Balancer

You can deploy GigaVUE V Series Node across the AWS accounts with Network Load Balancer in GigaVUE-FM.

To deploy,

1. Go to **Inventory > VIRTUAL > AWS** , and select **Monitoring Domain**.
2. On the **Monitoring Domain** page, select **New**. The **Monitoring Domain Configuration** page appears.
3. Select **Check Permissions** and validate whether you have the required permissions.
4. In the **Monitoring Domain** field, enter an alias used to identify the Monitoring Domain.
5. In the **Traffic Acquisition Method** drop-down list, select **VPC Traffic Mirroring** or **Customer Orchestrated Source** as the Traffic Acquisition method. For details, refer to Create a Monitoring Domain.
6. Enter the Monitoring Domain name and the Connection name as mentioned in the user data provided during the template launch in AWS. For details, refer to Configure Network Load Balancer in AWS.
7. For the **Use Load Balancer** field, select **Yes**.

8. For the **Use FM to Launch Fabric** option, select **No**. This allows you to deploy the fabric components using Third Party Orchestration.



9. Select **Save**. The Monitoring Domain is created successfully.
10. In the AWS Fabric Launch Configuration page, perform the following for the load balancer.
    - Select the **VPC** from the drop down list.
    - Select the **Load Balancer** configured in AWS.
    - Select the **Auto Scaling Group** configured in AWS.
11. Select **Save** to save the configuration.

Once the Monitoring Domain is successfully configured, edit the **Desired capacity** value for the Auto Scaling Group in AWS. For details, refer to the Create an Auto Scaling group using a launch template section in AWS.

Configure and Deploy Monitoring Session

In GigaVUE-FM, you must do the following to configure and deploy the Monitoring Session. Refer to Configure Monitoring Session section for more details.

1. **Access the Monitoring Session Page**:
    a. In GigaVUE-FM, go to **Traffic** > **Virtual** > **Orchestrated Flows > AWS**.
    b. 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.
2. **Add components to the canvas**:
    a. Drag and drop the required components to the canvas.

b. From the **Applications** expand menu, drag and drop the required applications to the graphical workspace.

3. **Deploy the Monitoring Session**:

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

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

What to do Next

You can view the detailed statistics of an individual traffic processing element in the **TRAFFIC PROCESSING** tab. For more details, refer to View Monitoring Session Statistics (AWS).

Acquire Traffic using Customer Orchestrated Source with Gateway Load Balancing

This section outlines the workflow for acquiring traffic with Customer Orchestrated Source and deploying GigaVUE Fabric Components with a Gateway Load Balancer. Refer to the following topics for instructions on configuring traffic acquisition, processing, and forwarding to your desired destination.

- Install GigaVUE-FM on AWS
- Configure the permissions required in AWS
- Create the AWS Credentials
- Configure Gateway Load Balancer and deploy GigaVUE V Series Nodes
- Deploy Visibility Fabric with Gateway Load Balancer
- Configure and Deploy Monitoring Session

Install GigaVUE-FM on AWS

This step is optional and applies only when an existing GigaVUE-FM instance is not available.
Refer to Install GigaVUE-FM on AWS for steps to install GigaVUE-FM on AWS and the steps to start GigaVUE-FM instance and configure it.

Configure the permissions required in AWS

If you are using inline policy or basic authentication, then you must update the policy with the relevant IAM service. For more information, see Minimum Permissions Required for Inline Policies and Basic Authentication.

This policy allows you to acquire traffic using Traffic Mirroring with Gateway Load Balancer and authenticate using an IAM instance role.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "autoscaling:DescribeAutoScalingGroups",
                "elasticloadbalancing:DescribeLoadBalancers",
                "elasticloadbalancing:DescribeTargetGroups",
                "elasticloadbalancing:RegisterTargets",
                "elasticloadbalancing:DeregisterTargets",
                "elasticloadbalancing:DescribeTargetHealth",
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeAddresses",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeSecurityGroups",
                "ec2:CreateTags",
                "ec2:DeleteTags",
                "ec2:DescribeImages",
                "ec2:DescribeVolumes",
                "ec2:CreateTrafficMirrorFilterRule",
                "ec2:CreateTrafficMirrorTarget",
                "ec2:CreateTrafficMirrorSession",
                "ec2:CreateTrafficMirrorFilter",
                "ec2:DeleteTrafficMirrorTarget",
                "ec2:DeleteTrafficMirrorSession",
                "ec2:DeleteTrafficMirrorFilter",
                "ec2:DescribeTrafficMirrorSessions",
                "ec2:DescribeTrafficMirrorTargets",
                "ec2:DescribeTrafficMirrorFilters",
                "ec2:DescribeVpcEndpointServiceConfigurations",
                "ec2:DescribeVpcEndpoints",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedRolePolicies",
                "iam:ListRolePolicies",
                "iam:ListAccountAliases",
                "kms:ListAliases",
                "kms:GenerateDataKeyWithoutPlaintext"
            ],
            "Resource": "*"
        }
    ]
}
```

For more information regarding policies and permissions, refer to AWS Documentation.

If you are using inline policy or basic authentication, then you must update the policy with the relevant IAM service. For more information, see Prerequisites.

Create the AWS Credentials

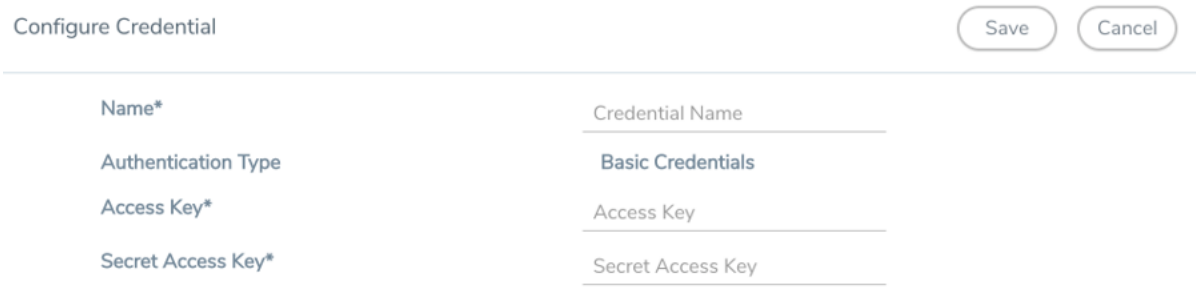
You can monitor workloads across multiple AWS accounts within one Monitoring Domain.

- After launching GigaVUE-FM in AWS, if the IAM is attached to the running instance of FM, then the **EC2 Instance Role** authentication credential is automatically added to the **Credential** page as the default credential. You must attach the IAM prior to creating a Monitoring Domain.
- If you use the **Basic Credentials** authentication credentials, you must add these to the GigaVUE-FM on the **AWS Settings** page, or on the Monitoring Domain creation page.

For details, refer to Create a Monitoring Domain.

To create AWS credentials:

1. Go to **Inventory > VIRTUAL > AWS**, and select **Settings > Credentials**
2. On the **Credential** page, select **Add**. The **Credential Configure** page appears.



3. Enter a name to identify the AWS Credential in the **Name** Field.
4. Basic Credentials is selected as the default **Authentication Type**. For more information, refer to AWS Security Credentials
5. Enter the credential of an IAM user or the AWS account root user in the **Access Key** field.
6. Enter the security password or key in the **Secret Access Key** field.
7. Select **Save**. You can view the list of available credentials on the AWS Credential page.

Configure Gateway Load Balancer and deploy GigaVUE V Series Nodes

Prerequisites

- Create or update Security Group policies of GigaVUE Cloud Suite components. For details, refer to Security Group topic for detailed information.

- Create or update route tables in the VPCs across all mirrored AWS accounts. Ensure each mirrored account VPC can connect to the target account VPC where you deploy the Gateway Load Balancer. For details, refer to Subnet and Security Group for Amazon VPC.
- Create or update an IAM role for GigaVUE-FM in the centralized VPC. Establish a trust relationship between the mirrored and the target account for GigaVUE-FM to execute the above permissions at the IAM role level. For details, refer to Permissions and Privileges (AWS).
  For more information on AWS recommended design for Gateway Load Balancer implementation with inline services, such as firewall. see Getting started with Gateway Load Balancers - Elastic Load Balancing (amazon.com)
- Create a VPC endpoint and endpoint service. For more information, see Create endpoint service
- Create a routing table. For more information, see Amazon documentation.
- Configure a token in the **User Management** page. For details, refer to Configure Tokens.

Points to Note:

When configuring Gateway Load Balancer, you need to deploy the GigaVUE V Series Nodes using Third Party Orchestration.

Perform the following steps to configure an external load balancer in AWS:

1. Create a Target Group
2. Create a Load Balancer
3. Create a Launch Template for Auto Scaling group
4. Create an Auto Scaling group using a Launch Template

Create a Target Group

Enter or select the following details as mentioned in the table to configure target groups in AWS.

Parameters	Description	Reference	Mandatory field
Basic Configuration			
Choose a target type	Select IP address as the target type	Create a target group for your Gateway Load Balancer	Yes
Protocol	Verify that Protocol is GENEVE		Yes
Port	Verify that the port value is 6081		Yes
Health Checks			

Parameters	Description	Reference	Mandatory field
HealthCheckProtocol	Select TCP as the protocol.	Health checks for Gateway Load Balancer target groups	Yes
HealthCheckPort	Enter 8888 as the port.		Yes
HealthCheckIntervalSeconds	Enter 10 seconds as the approximate amount of time, in seconds.		Yes

Create a Load Balancer

Enter or select the following details as mentioned in the table to configure a load balancer in AWS.

Parameters	Description	Reference	Mandatory field
Network Mapping			
VPC	Select the VPC for your targets (GigaVUE V Series Node)	Create a Gateway Load Balancer	Yes
IP Listener routing			
Default action	Select the target group to receive traffic. If you don't have a target group, choose Create target group.	Create a target group	Yes

Create a Launch Template for Auto Scaling group

Enter or select the following details to create a launch template for auto scaling groups in AWS.

Parameters	Description	Reference	Mandatory field
Launch Template contents			
Application and OS Images (Amazon Machine Image)	Select the AMI of the GigaVUE V Series Node.	Create a launch template for an Auto Scaling group	Yes
Instance type	Select **c5n.xlarge** as the instance type.		Yes

Parameters	Description	Reference	Mandatory field
Key pair name	Select a Key pair for the instance.		Yes
Network Settings			
Device Index	Add 2 Network Interfaces for the GigaVUE V Series Node with device index as **0** and **1** (mgmt and data interface respectively) and for the interfaces,	Create a launch template for an Auto Scaling group	Yes
Firewall (security groups)	Keep this blank and configure one or more security groups as part of the network interface.		Yes
Advanced Settings			

Advanced details	Enter the User data as text in the following format and deploy the instance. The GigaVUE V Series Nodes uses this user data to generate config file (**/etc/gigamon-cloud.conf**) used to register with GigaVUE-FM using Third Party Orchestration.
	`#cloud-config`
	`write_files:`
	`- path: /etc/gigamon-cloud.conf`
	`owner: root:root`
	`permissions: '0644'`
	`content: |`
	`Registration:`
	`groupName: <Monitoring Domain Name>`
	`subGroupName: <VPC Name>`
	`token: <Token>`
	`remoteIP: <IP address of the GigaVUE-FM>`
	`remotePort: 443`
		Create a launch template using advanced settings	Yes

Create an Auto Scaling group using a Launch Template

Enter or select the following details to create an auto scaling group and launch the fabric components using the launch template in AWS.

Parameters	Description	Reference	Mandatory field
Configure group size and scaling policies			
Group Size	Enter the Desired capacity as 0. The Desired capacity value must be less than the Maximum Capacity value. **Note**: Once the monitoring Domain and connection is configured, edit this value to the number of GigaVUE V Series Node.	Creating an Auto Scaling group using a launch template	Yes

Parameters	Description	Reference	Mandatory field
Automatic Scaling	Select **Target tracking scaling policy** and enter the following details to define a policy: Metric Type: 1000000000 (bytes) Instance warmup: **300** seconds	Create a target tracking scaling policy	Yes
Add tag	Provide a tag key and value for each tag.	Tag Auto Scaling groups and instances	No

In the Instances page, you can view the GigaVUE V Series Node instance that the load balancer deploys.

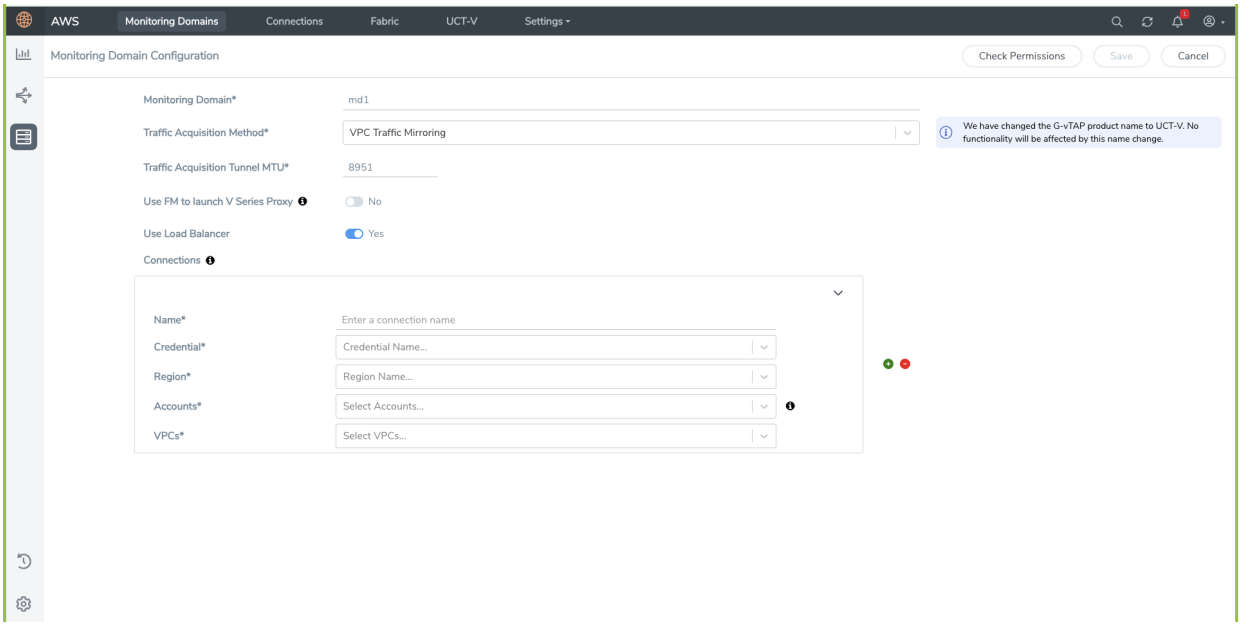
Deploy Visibility Fabric with Gateway Load Balancer

You can deploy GigaVUE V Series Node across the AWS accounts with Gateway Load Balancing in GigaVUE-FM.

To deploy,

1. In the **Monitoring Domain Configuration** page, select **VPC Traffic Mirroring** or **Customer Orchestrated Source** or **Inline** as the Traffic Acquisition method. For details, refer to Create a Monitoring Domain.
2. Enter the **Monitoring Domain** Name and the **Connection** Name as mentioned in the user data provided during the template launch in AWS. For details, refer to Configure a Gateway Load Balancer in AWS.
3. For the **Use Load Balancer** field, select **Yes**.

4. Select **No** for the **Use FM to Launch Fabric** option. This allows you to deploy the fabric components using Third Party Orchestration.



5. Select **Save**. The Monitoring Domain is created successfully and you are navigated to the **AWS Fabric Launch Configuration** page.
6. In the **AWS Fabric Launch Configuration** page, perform the following for the load balancer.
    a. Select the **VPC** from the drop down list.
    b. Select the **Load Balancer** configured in AWS.
    c. Select the **Auto Scaling Group** configured in AWS.
7. Select **Save** to save the configuration.

Once the Monitoring Domain is successfully configured, edit the **Desire capacity** value for the Auto Scaling Group in AWS. For details, refer to Configure a Gateway Load Balancer in AWS.

Configure and Deploy Monitoring Session

In GigaVUE-FM, you must do the following to configure and deploy the Monitoring Session. Refer to Configure Monitoring Session section for more details.

1. **Access the Monitoring Session Page**:
    a. In GigaVUE-FM, go to **Traffic** > **Virtual** > **Orchestrated Flows > AWS**.
    b. 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.
2. **Add components to the canvas**:
    a. Drag and drop the required components to the canvas.

b. From the **Applications** expand menu, drag and drop the required applications to the graphical workspace.

3. **Deploy the Monitoring Session**:

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

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

What to do Next

You can view the detailed statistics of an individual traffic processing element in the **TRAFFIC PROCESSING** tab. For more details, refer to View Monitoring Session Statistics (AWS).

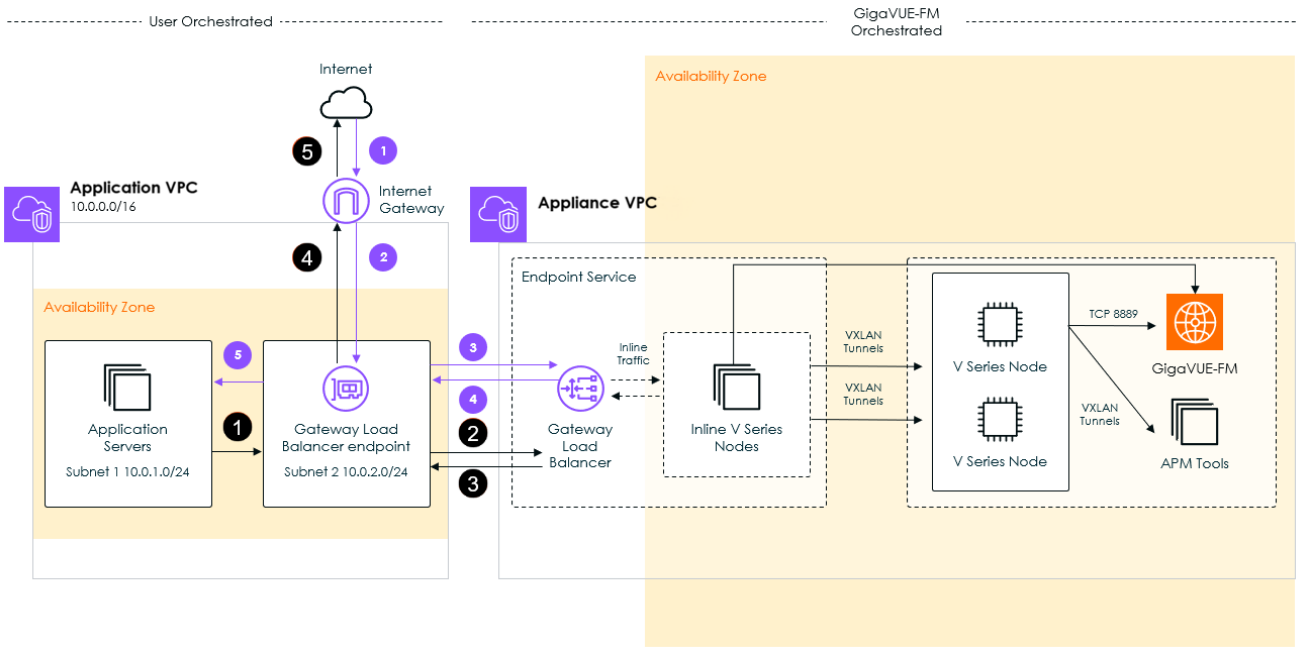
Acquire Traffic using Inline V Series Solution

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 WS topic

This section outlines the workflow 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.

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.



Create a Virtual Private Cloud

A Virtual Private Cloud (VPC) creates a secure, logically isolated network within AWS, allowing you to deploy and manage resources with full control over IP ranges, subnets, routing, and connectivity. To create a VPC in AWS, refer to Create a VPC topic in AWS documentation.

NOTE: We recommend to create a VPC with no additional VPC resources (VPC only).

Create Subnets

Next, you must create subnets within the VPC you previously created. Subnets in a VPC divide the VPC's IP address range into smaller, manageable networks within specific availability zones. To create subnets in the VPC using AWS, refer to Create a subnet - Amazon Virtual Private Cloud topic in AWS documentation.

NOTE: You must create a minimum of three subnets: one for the management subnet, one for the traffic path, and one for the tools.

Create Internet Gateway

To enable communication between your subnets and the internet, you must create and configure an Internet Gateway. Since virtual machines (VMs) are connected to subnets, and these subnets need to communicate with each other and with external networks, an Internet Gateway is essential.

The Internet Gateway serves as a bridge between your VPC and the internet. When attached to a VPC and configured through route tables, it allows resources within the subnets to send and receive traffic from the internet.

To establish internet connectivity:

- Create an Internet Gateway
- Attach it to your VPC

For Navigation steps and detailed instructions, refer to Add internet access to a subnet topic in AWS documentation.

Create Route Tables

A route table acts as the traffic controller for your VPC. It contains a set of rules, called routes, that determine how network traffic is directed from subnets or gateways to their destinations.

Route table plays a critical role in:

- Enabling communication between the subnets
- Establishing connectivity between the subnets and the internet through the Internet Gateway.

For Navigation steps and detailed instructions, refer to Create a route table for your VPC topic in AWS documentation.

When you create a route table, it is initially empty. To enable proper routing:

- Add routes that define how traffic should flow (Example: A route that directs all outbound traffic (0.0.0.0/0 for IPv4 and ::/0 for IPv6) to the Internet Gateway).

  NOTE: During VPC creation, if you specify IPv4 and IPv6 CIDR blocks, AWS automatically associates these with the route table. However, you must manually add the Internet Gateway as the target for internet-bound traffic.

- Associate the route table with the required subnets.

By configuring the route table, you ensure that:

- Subnets can communicate with each other
- VMs deployed within the subnets can access the internet.

Create Security Group

When you launch GigaVUE-FM or GigaVUE V Series Nodes, a security group defines virtual firewall rules for the instance. These rules regulate both inbound and outbound traffic.

You can configure:

- **Inbound rules** to manage traffic coming into the instance.
- **Outbound rules** to control traffic leaving the instance.

To create a security group, refer to the Create a security group for your Amazon EC2 instance topic in the AWS Documentation.

We recommend to create a separate security group for each component using the rules and port numbers listed Network Firewall Requirement for GigaVUE Cloud Suite topic.

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

Launch Instance

You can launch an EC2 instance in a subnet associated with the VPC you created. EC2 allows you to deploy VMs using the configurations defined in your VPC setup.

For navigation steps and detailed instructiuons, refer to Launch an EC2 instance using the launch instance wizard in the console topic in AWS 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.

Create a Target Group

Enter or select the following details as mentioned in the table to create a target groups in AWS.

The following table lists the specific options you must select when creating a Target Groups for an inline V Series deployment. For navigation steps and detailed instructions, refer to Create a target group for your Gateway Load Balancer topic in AWS documentation.

Parameters	Instructions	Mandatory field
Basic Configuration		
Choose a target type	Select **Instance** as the target type.	Yes
Protocol	Verify that Protocol is **GENEVE**.	Yes
Port	Verify that the port value is **6081**.	Yes
VPC	Select the VPC for your targets (GigaVUE V Series Node).	Yes
Health Checks		
Health check protocol	Select **HTTP** as the protocol.	Yes
Health Check path	Enter **/health** as path	Yes
Health check port	Select the option to override the port and enter **8888** as the port value.	Yes
Healthy threshold	Enter 2 as the threshold count value.	Yes
Unhealthy threshold	Enter 2 as the threshold value.	Yes
Timeout	Enter 2 seconds as the timeout.	Yes
Interval	Enter 5 seconds as the approximate amount of time.	Yes

Once the target group details are configured and saved, you are prompted to select targets. Skip this step and select **Create target group** to finalize the configuration.

Create a Gateway Load Balancer

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, prerequisites, and detailed instructions, refer to Getting started with Gateway Load Balancers topic in AWS documentation.

Parameters	Instructions	Mandatory field
Network Mapping		
VPC	Select the VPC for your targets (GigaVUE V Series Node)	Yes
Availability Zone and subnets	Select the zones and the corresponding subnets where you want to launch the GigaVUE V Series Node.	Yes
IP Address Type	Select the **Dual Stack** option as the IP address type if you have configured both **IPv4 and IPv6**.	Yes
IP Listener routing		
Default action	Select the target group to receive traffic. If you don't have a target group, choose Create target group.	Yes

NOTE: After creating and associating the Gateway Load Balancer with subnets and Availability Zones, you cannot modify these settings. If you need to make changes later, delete and recreate the load balancer.

After creating the Gateway Load balancer, configure Cross-zone load balancing to balance traffic flows between the GigaVUE V Series Nodes deployed across multiple availability zones. For details, refer to the Cross-zone load balancing section in AWS Documentation.

Create a Launch Template for Inline GigaVUE V Series Node

The following table lists the specific options you must select when creating a Launch Template for Inline GigaVUE V Series Node. For navigation steps and detailed instructions, refer to Create a launch template for an Auto Scaling group topic in AWS documentation.

Parameters	Instructions	Mandatory field
Launch Template contents		
Application and OS Images (Amazon Machine Image)	Select the AMI of the GigaVUE V Series Node. From the **AWS Marketplace AMIs**. Search Gigamon and choose the **GigaVUE Cloud Suite V Series** Image. Subscribe to it.	Yes
Instance type	Select **c5n.xlarge** as the instance type.	Yes
Key pair name	Select a Key pair for the instance.	Yes
Network Settings		
Subnet	Select **Don't include in launch template** option.	Yes
Firewall (security groups)	Choose **Select existing security group** option. Keep the security group field blank and configure one or more security groups as part of the network interface as mentioned in the following	Yes

Parameters	Instructions	Mandatory field
	steps.	
Advanced Network configurations GigaVUE V Series Node requires a minimum of 2 Network Interfaces one for data and other one for mgmt. Add 2 Network Interfaces.		
Network interface 1 - Data Interface		
Device Index	Enter the device index as **0** for the data interface	Yes
Subnet	The subnet is automatically assigned by AWS.	
Security Group	Choose the security group.	
Network interface 2 - Management Interface		
Device Index	Enter the device index as **1** for the mgmt interface	Yes
Subnet	Select the subnet.	

Parameters	Instructions	Mandatory field
Security Group	Select the same security group.	
Advanced Settings		

Advanced details	Enter the User 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 **/etc/vseries-inline.conf**) and register with GigaVUE-FM using Third Party Orchestration.
	Enter the token you configured in step Create a GigaVUE-FM Token.
	`#cloud-config`
	`write_files:`
	`- path: /etc/gigamon-cloud.conf`
	`owner: root:root`
	`permissions: '0644'`
	`content: |`
	`Registration:`
	`groupName: <Enter a name for the Monitoring Domain>`
	`subGroupName: <Enter the VPC Name>`
	`remoteIP: <IP address of GigaVUE-FM reachable from V Series>`
	`remotePort: 443`
	`token: <token created in GigaVUE-FM>`
	`- path: /etc/vseries-inline.conf`
	`owner: root:root`
	`permissions: '0644'`
	`content: ""`
	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.
		Yes

Create an Auto Scaling group using a Launch Template for Inline GigaVUE V Series Node

The following table lists the specific options you must select when creating a auto scaling group and launch the fabric components using the launch template in AWS. For navigation steps and detailed instructions, refer to Creating an Auto Scaling group using a launch template topic in AWS documentation.

Parameters	Instructions	Mandatory field
Choose launch template or configuration		
Launch template	Choose the Launch Template you created for Inline GigaVUE V Series Node	Yes
Choose launch template or configuration		
VPC	Select the VPC for your targets (GigaVUE V Series Node)	
Availability Zone and subnets	Select the zones and the corresponding subnets where you want to launch the GigaVUE V Series Node.	
Integrate with other services		
Load balancing	Choose **Attach to an existing load balancer** option.	
Existing load balancer target groups	Select the Target Group created above.	
Attach to an existing load balancer	Choose the **Choose from your load balancer target groups** option.	Yes
Configure group size and scaling		
Group Size	Enter the Min desired capacity as 0. The Desired capacity value must be less that the Maximum Capacity value. **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
Automatic Scaling	Select **Target tracking scaling policy** and enter the following details to define a policy: Metric to use: Network In Value: 1000000000 bytes Instance warmup: **300** seconds	Yes
Add tags		
Tags	Provide **Key** as GigamonNode and **Value** as VSeriesNode for each tag.	No

Create a Launch Template for Out of Band GigaVUE V Series Node

NOTE: This step is optional. You can create a launch template for Out of Band GigaVUE V Series Node if you wish to send to process the acquired traffic.

The following table lists the specific options you must select when creating a Launch Template for Out of Band GigaVUE V Series Node. For navigation steps and detailed instructions, refer to Create a launch template for an Auto Scaling group topic in AWS documentation.

Parameters	Instructions	Mandatory field
Launch Template contents		
Application and OS Images (Amazon Machine Image)	Select the AMI of the GigaVUE V Series Node.	Yes
Instance type	Select **c5n.xlarge** as the instance type.	Yes
Key pair name	Select a Key pair for the instance.	Yes
Network Settings		
Device Index	Add 2 Network Interfaces for the GigaVUE V Series Node with device index as **0** and **1** (mgmt and data interface respectively) and for the interfaces.	Yes
Firewall (security groups)	Keep this blank and configure one or more security groups as part of the network interface.	Yes
Advanced Settings		

Advanced details	Enter the User data as text in the following format and deploy the instance. The GigaVUE V Series Nodes uses this user data to generate config file (**/etc/gigamon-cloud.conf**) used to register with GigaVUE-FM using Third Party Orchestration.
	Enter the token you configured in step Create a GigaVUE-FM Token.
	`#cloud-config`
	`write_files:`
	`  - path: /etc/gigamon-cloud.conf`
	`  owner: root:root`
	`  permissions: '0644'`
	`  content: |`
	`  Registration:`
	`  groupName: <Enter a name for the Monitoring Domain>`
	`  subGroupName: <Enter the VPC Name>`
	`  remoteIP: <IP address of GigaVUE-FM reachable from V Series>`
	`  remotePort: 443`
	`  token: <token created in GigaVUE-FM>`
	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.
		Yes

Create an Auto Scaling group using a Launch Template for Out of Band GigaVUE V Series Node

NOTE: This step is optional. You can create a auto scaling groups for Out of Band GigaVUE V Series Node if you wish to send to process the acquired traffic. You can configure multiple auto-scaling groups based on the number of node groups or tiers you need to set up.

The following table lists the specific options you must select when creating a Auto Scaling group using a Launch Template for Out of Band GigaVUE V Series Node. For navigation steps and detailed instructions, refer to Creating an Auto Scaling group using a launch template topic in AWS documentation.

Parameters	Instructions	Mandatory field
Choose launch template or configuration		
Launch template	Choose the Launch Template created for Out-of-Band GigaVUE V Series Node	Yes
Configure group size and scaling		
Group Size	Enter the Desired capacity as 0. The Desired capacity value must be less that the Maximum Capacity value. **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
Automatic Scaling	Select **Target tracking scaling policy** and enter the following details to define a policy: Metric to use: Network In Value: 1000000000 bytes Instance warmup: **300** seconds	Yes
Add tag	Provide **Key** as GigamonNode and **Value** as VSeriesNode for each tag.	No

In the Instances page, you can view the GigaVUE V Series Node instance that the load balancer deploys.

Create Endpoint Service

The following table lists the specific options you must select when creating an Endpoint Service. For navigation steps and detailed instructions, refer to Create an endpoint service topic in AWS documentation.

Parameters	Instructions	Mandatory field
Endpoint service settings		
Load Balancer Type	Choose **Gateway**.	Yes
Available load balancers	Select the gateway load balancer you created.	Yes
Additional Settings		
Supported IP address types	Select the **Dual Stack** option as the IP address type if you have configured both **IPv4 and IPv6**.	Yes
Tags	Provide **Key** and **Value** for each tag.	No

Once created, copy the end point service name.

By default, your endpoint service is not available to service consumers. You must add permissions that allow specific AWS principals to create an interface VPC endpoint to connect to your endpoint service.

To manage permissions that allow each service consumer to connect to your endpoint service:

1. Select the endpoint service and choose the Allow principals tab.
2. Add the required principals and choose Allow principals. Once allowed Endpoint service will be shown in available state.

Create VPC Endpoint

The following table lists the specific options you must select when creating a VPC Endpoint. For navigation steps and detailed instructions, refer to Create a VPC endpoint topic in AWS documentation.

Parameters	Instructions	Mandatory field
Endpoint settings		
Type	Choose **Endpoint services that use NLBs and GWLBs**.	Yes
Service Settings		
Service name	Paste the end point service name.	Yes
Network Settings		
VPC	Select the VPC	Yes
Availability Zone and subnets	Select the zones and the corresponding subnets to which the VPC end point should be associated. VPC Endpoint uses this subnet to create a private link with the gateway load balancer.	Yes
IP Address Type	Select the **Dual Stack** option as the IP address type if you have configured both **IPv4 and IPv6**.	Yes

After creating the endpoint, go to the service. Select the endpoint and select **Actions > Accept endpoint connection request**. A private link gets created between the Gateway LoadBalancer endpoint and the Gateway LoadBalancer Endpoint service.

Modify the Routing table configurations

In your EC2 Instances page, you can modify the routing tables to ensure all inbound and outbound traffic flows through the configured VPC Endpoint and Gateway Load Balancer.

Within the customer VPC, multiple routing tables exist. For example:

- A default routing table associated with the VPC.
- A routing table associated with the monitored subnets (typically five).
- A dedicated routing table for the subnet containing the VPC endpoint.

Each routing table must be updated to properly route egress (outbound) and ingress (inbound) traffic through the solution.

For navigation steps and detailed instructions, refer to Configure routing topic in AWS documentation.

Egress Traffic (Outbound to Internet)

1. In the routing table of the monitored subnets, update the route for Internet-bound traffic (0.0.0.0/0 and ::/0) to point to the VPC Endpoint instead of the Internet Gateway.
2. The VPC Endpoint forwards traffic to the GWLB, which processes and returns it.
3. The endpoint routing table then forwards the processed traffic to the Internet Gateway.

Flow: VM → Subnet Route → VPC Endpoint → GWLB → VPC Endpoint → IGW → Internet

Ingress Traffic (Inbound from Internet)

1. In the default routing table, add routes for monitored subnet CIDRs pointing to the VPC Endpoint.
2. Incoming Internet traffic is routed through the endpoint to the GWLB for inspection, then back to the endpoint and finally to the destination VM.

Flow: Internet → IGW → Default Route → VPC Endpoint → GWLB → VPC Endpoint → VM

Notes:

- The Internet Gateway must remain associated with the default route table.
- The VPC Endpoint requires its own subnet and routing table.

- Routing configurations are applied in the customer's VPC.

Install GigaVUE-FM on AWS

You can subscribe to GigaVUE-FM in the marketplace and launch in AWS.

Refer to the following topics for instruction on installing GigaVUE-FM in AWS:

- Subscribe to GigaVUE-FM
- Initial Configuration

Subscribe to GigaVUE-FM

You can deploy the GigaVUE Cloud Suite for AWS from the AWS Marketplace.

NOTE: Only users with **aws-marketplace:ViewSubscriptions** permission in their IAM policy can subscribe to GigaVUE products.

To subscribe to the GigaVUE-FM, perform the following steps:

1. Log in to your AWS account.
2. Go to AWS Marketplace: https://aws.amazon.com/marketplace/.
3. In the **Search** field, type Gigamon and select **Search**.
4. Select the latest version GigaVUE Cloud Suite BYOL version. For details, refer to Licensing for GigaVUE Cloud Suite for AWS
5. Select **View Purchase Options**. The terms and condition page is displayed.
6. Review the Terms and Conditions and select **"Accept Terms**".
7. Review the summary and then select **Continue to Configuration**.
8. In the **Configure this software** page, enter the following details for your deployment:
   a. Set **Fulfillment Option** to the default value.
   b. Select the latest version in the **Software Version** field.
   c. Choose your deployment **Region**.
   d. Select **Continue to Launch.**

9. In the **Configure this software** page, perform the following:
    a. In the **Choose Action** field, select the **Launch from Website** option.
    b. From the **EC2 Instance Type** drop-down list, select the instance type. Refer to Recommended and Supported Instance Types for AWS.
    c. From the **VPC Settings** drop-down list, select the VPC for deploying GigaVUE-FM.
    d. In the **Subnet Settings**, select your desired Subnet.
    e. In the **Security Group Settings**, configure the security group to match your access and permissions needs. For details, refer to Security Group
    f. Select your preferred **Key Pair** for secure access to the instance.
    g. In the **Advanced details** section, select **V2 only (token required)** from the Metadata version drop-down list.
    h. Select **Launch**.

For details, refer to Launch an instance using defined parameters in AWS documentation.

GigaVUE-FM is launched in AWS. You must perform the initial configuration to view the GigaVUE-FM UI.

Initial Configuration

It may take several minutes for the GigaVUE-FM instance to start up. Once it is up and running, perform the following steps to verify:

1. In your EC2 Instances page, select the **Instance ID** of the launched GigaVUE-FM to view the instance information.
2. Copy and paste the **Public IP address** into a new browser window or tab. The GigaVUE-FM GUI appears.

Notes:

- If GigaVUE-FM is deployed inside AWS, use **admin** as the username and the **Instance ID** as the default password for the admin user to login to GigaVUE-FM, for example i-079173111e2d73753 **(Instance ID)**. You can get the **Instance ID** of GigaVUE-FM in the EC2 Instances page.
- If GigaVUE-FM is deployed outside the AWS, use admin123A!! as the default admin password.

When you first log in to GigaVUE-FM, you will be asked to change your default password.

Create Gigamon Custom Role

This policy allows you to acquire traffic using Inline V Series and authenticate using an IAM instance role. For more information regarding policies and permissions, refer to Policies and permissions in AWS Identity and Access Management topic in AWS documentation.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:GetGroupPolicy",
                "iam:ListAttachedRolePolicies",
                "iam:ListRolePolicies",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAccountAliases",
                "iam:ListGroupsForUser"
                "iam:ListAttachedUserPolicies"
                "iam:ListAttachedGroupPolicies"
                "iam:ListUserPolicies"
                "iam:ListGroupPolicies"
                "autoscaling:DescribeAutoScalingGroups",
                "elasticloadbalancing:DescribeLoadBalancers",
                "elasticloadbalancing:DescribeTargetGroups",
                "elasticloadbalancing:DescribeTargetHealth",
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:CreateTags"
            ],
            "Resource": "*"
        }
    ]
}
```

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.

Create AWS Credentials

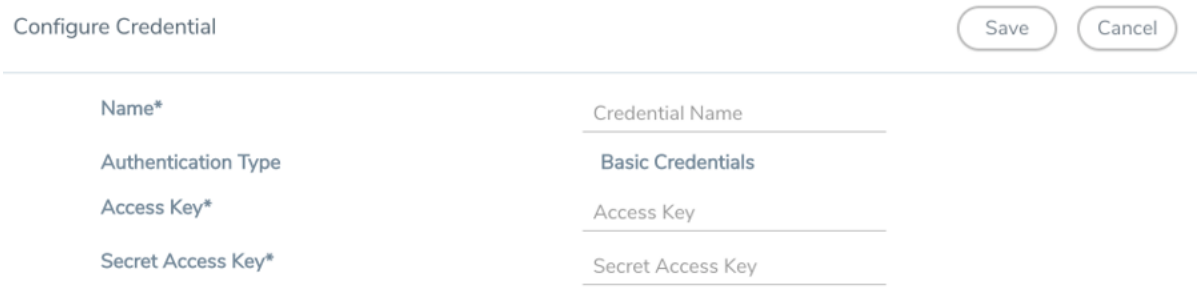
You can monitor workloads across multiple AWS accounts within one Monitoring Domain.

- After launching GigaVUE-FM in AWS, if the IAM is attached to the running instance of FM, then the **EC2 Instance Role** authentication credential is automatically added to the **Credential** page as the default credential. You must attach the IAM prior to creating a Monitoring Domain.
- If you use the **Basic Credentials** authentication credentials, you must add these to the GigaVUE-FM on the **AWS Settings** page, or on the Monitoring Domain creation page.

For details, refer to Create Monitoring Domain.

To create AWS credentials:

1. Go to **Inventory > VIRTUAL > AWS**, and select **Settings > Credentials**
2. On the **Credential** page, select **Add**. The **Credential Configure** page appears.



3. Enter a name to identify the AWS Credential in the **Name** Field.
4. Basic Credentials is selected as the default **Authentication Type**.
5. Enter the credential of an IAM user or the AWS account root user in the **Access Key** field.
6. Enter the security password or key in the **Secret Access Key** field.
7. Select **Save**. You can view the list of available credentials on the AWS Credential page.

Create Monitoring Domain

AWS 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 > AWS** .
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 AWS. Refer to Advanced section in Acquire Traffic using Inline V Series Solution.
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 a 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**:
      - Select the **IP Address Type** as Private or Public.
      - From the **Subnet** drop-down list, select the management subnet.
      - Select **Add Subnet** under **Additional Subnets** to add additional subnets.
   e. Select **Add** under **Tags** to assign tags for resource identification.
7. Select **Save**.

Note:

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

- Create an Auto Scaling group using a Launch Template for Inline GigaVUE V Series Node
- Create an Auto Scaling group using a Launch Template for Out of Band GigaVUE V Series Node

Adjust the desired capacity value in the scaling group to match the required number of nodes for your deployment.

Deploy GigaVUE V Series Nodes for Inline V Series Solution

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

1. From the **Centralized VPC** drop-down list, select VPC.
2. From the **Gateway Load Balancer** drop-down list, select the Load Balancer configured in AWS
3. Under **Node Groups**, you can configure multiple node groups based on the deployment use case. For details, refer to Inline V Series.

a. **Inline Node Group:** This node group is used for the Inline V Series Node required for traffic acquisition.
   - In the **Inline Node Group Name** field, enter a name for the node group.
   - From the **Inline Auto Scaling Group** drop-down list, select the auto scaling group in which the Inline V Series Node is deployed.

b. (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.
   - In the **Node Group Name** field, enter a name for the node group.
   - From the **Auto Scaling Group** drop-down list, select the auto scaling group configured in AWS.

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

4. Select **Save**.

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 (AWS) for details.
   - On an existing Monitoring Session, navigate to the **TRAFFIC PROCESSING** tab.

   The GigaVUE-FM Monitoring Session canvas page appears.

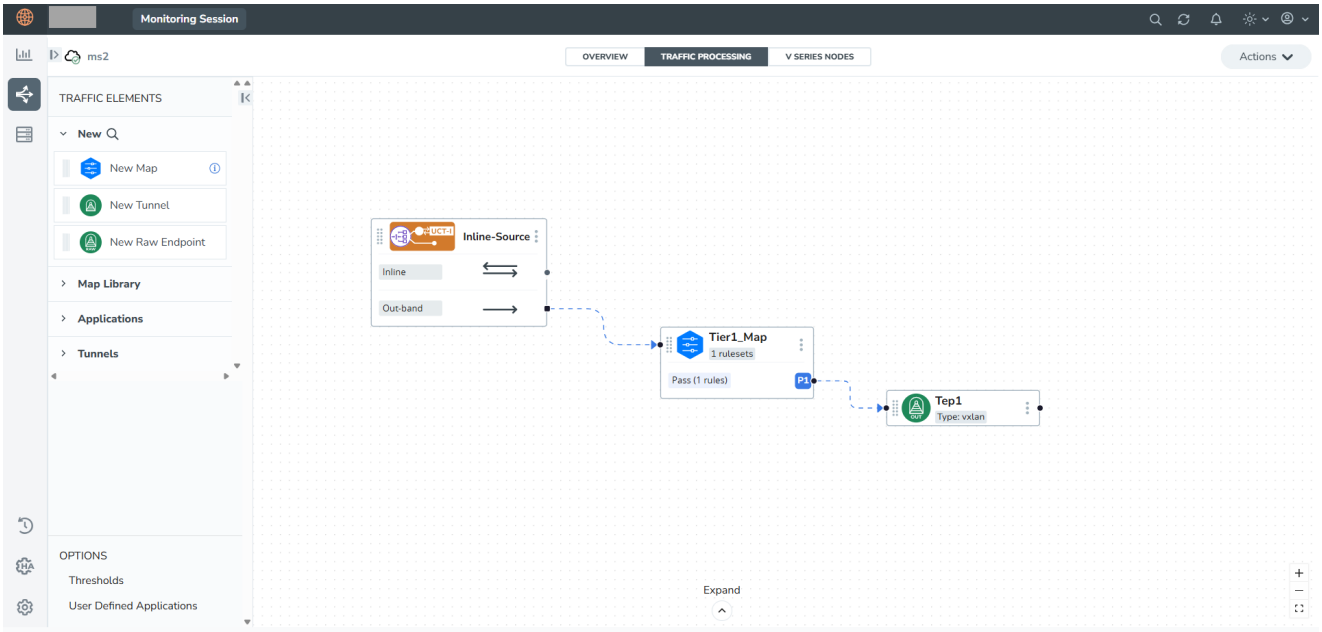
   When the **Traffic Acquisition Method** is **Inline**, the **UCT-I** application is available on the canvas by default.

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 (AWS) 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 (AWS) 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)

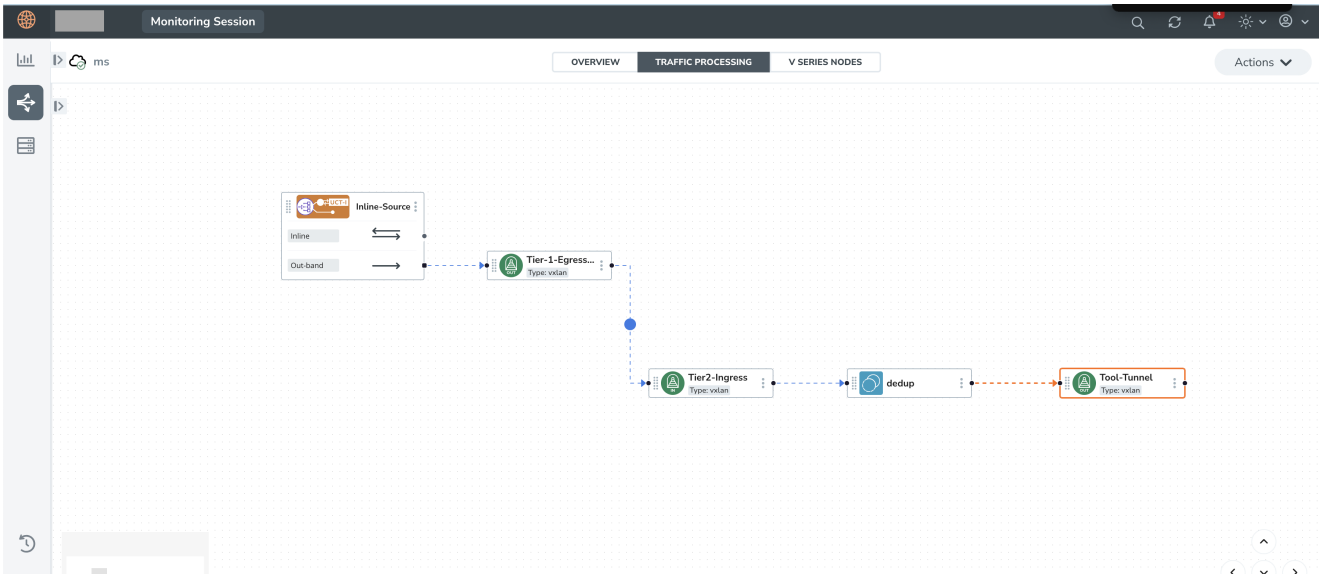
1. From the Actions drop-down list, select **Deploy**. The Deploy Monitoring Session pop-up appears.
2. Enter the following details:
   - In the **Policy Name** field, verify the auto-generated policy name or enter a custom name.
   - From the **Node Group** drop-down list, select the appropriate node 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 (AWS) for details.
   - Maps from the **New Map** section. Refer to Create a New Map (AWS) for details.
   - GigaSMART apps from the Applications section. Refer to Add Applications to Monitoring Session (AWS).
   - 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 (AWS)
- Analytics for Inline V Series Solution (AWS)

Deploy GigaVUE Cloud Suite for AWS using Third Party Orchestration

The GigaVUE Cloud Suite fabric components can be deployed in generic and integrated modes.

Generic Mode

In Generic Mode, you can deploy GigaVUE V Series Nodes using your own orchestration system. Provide the monitoring domain name and connection name in the user data during deployment.

GigaVUE-FM automatically creates the Monitoring Domain under the **Third Party Orchestration** monitoring domain page. It assigns the deployed fabric components to that domain after the deployment completes.

Integrated Mode

In integrated mode, using GigaVUE-FM, you create a monitoring domain in your respective GigaVUE Cloud Suite. Then, use your own orchestration system just deploy GigaVUE V Series nodes.

GigaVUE-FM displays the deployed Nodes under the monitoring domain you created in your respective GigaVUE Cloud Suite. In this case, ensure that the monitoring domain and the connection name given in GigaVUE-FM matches the groupName and subGroupName in the user data provided in your orchestration system.

You can also create a monitoring domain and connection under Third party Orchestration in GigaVUE-FM. Then, use the monitoring domain name and connection name as the groupName and sunGroupName in the registration data used in your respective cloud platform.

Refer to the following topics on more detailed information on how to deploy your fabric components in the AWS using Third Party Orchestration:

- Deployment Options for GigaVUE Cloud Suite for AWS - Generic Mode
- Deployment Options for GigaVUE Cloud Suite for AWS - Integrated Mode

Deployment Options for GigaVUE Cloud Suite for AWS - Generic Mode

This topic provides details on how you can configure GigaVUE Cloud Suite for Third Party Orchestration in multiple ways to gain visibility into both physical and virtual traffic. The configuration options depend on two factors:

- The traffic acquisition method
- The deployment method for fabric components

GigaVUE-FM supports four deployment options based on these variables.

- Create a Custom User
- Create a Custom User
- Create a Custom User
- Create a Custom User
  - Deployment Options for GigaVUE Cloud Suite for AWS - Generic Mode
  - Deployment Options for GigaVUE Cloud Suite for AWS - Generic Mode

Acquire Traffic using UCT-V - Without creating Monitoring Domain

This section outlines the workflow to acquire traffic directly from virtual machines and send it to GigaVUE V Series Nodes using UCT-V. Refer to the following topics for instruction on configuring traffic acquisition, processing, and forwarding to your desired destination.

- Install GigaVUE-FM on AWS
- Configure Role-Based Access for Third Party Orchestration
- Install UCT-Vs
- Create a Custom User
- Configure and Deploy Monitoring Session

Install GigaVUE-FM on AWS

This step is optional and applies only when an existing GigaVUE-FM instance is not available.
Refer to Install GigaVUE-FM on AWS for steps to ìnstall GigaVUE-FM on AWS and the steps to start GigaVUE-FM instance and configure it.

Configure Role-Based Access for Third Party Orchestration

If you do not want to use an **Admin Profile** to deploy GigaVUE V Series through a Third Party orchestrator, you can create the required users, roles, and user groups in GigaVUE-FM.

Create a Custom User

You can add users only if you are a user with **fm_super_admin role** or a user with either read or write access to the GigaVUE-FM security Management category.

To add users:

1. Go to **Settings** and select **Authentication** > **GigaVUE-FM User Management > Users**.
2. On the User page, select **New User**.
3. In the Add User page, enter the following details:
   - **Name:** Actual name of the user
   - **Username**: User name configured in GigaVUE-FM
   - **Email**: Email ID of the user
   - **Password/Confirm Password**: Password for the user. For more details, refer to Change Your Password.
   - **User Group:** Select the desired User Group to associate the user.

   GigaVUE-FM prompts for your password.
4. Click **Ok**. The new user is added.

Create a Custom Role and Assign the User

A user role defines permission for users to perform any task or operation in GigaVUE-FM or on the managed device. You can associate a role with user.

NOTE: A user with read-only access cannot perform configurations on the screen. The menus and action buttons in the UI pages are disabled appropriately.

To create a role:

1. Go to **Settings** and select **Authentication> GigaVUE-FM User Management >Roles**.
2. Select **New Role**.
3. In the New Role page, select or enter the following details:
   - **Role Name**: Name of the role.
   - **Description**: Description of the role.
   - **Select Permission**: From the **Select Permissions** tab, select **Third Party Orchestration**, and provide write permissions.
4. Select **Apply** to save the configuration.

Create a Custom User Group and Assign the Custom Role and the User

A user group consists of a set of roles and set of tags associated with users in that group. You can associate the user to one or more groups.

To create a new user group:

1. Go to **Settings**, and then select **Authentication> GigaVUE-FMUser Management >User Groups**.
2. Select **New Group.**
3. In the New User Group page, select **Next** to progress forward and **Back** to navigate backward.
4. In the **Group Info** tab, enter the Group Name and Description details:
5. In the **Assign Roles** tab, select the role that you want to assign to the user group.
6. In the **Assign Tags** tab, select the required tag key and tag value.
7. In the **Assign Users** tab, select the required users.
8. Select **Apply** to save the configuration. The new user group is added.

Install UCT-Vs

You can install UCT-V on both Linux and Windows environments. For details, refer to the following topics:

- Linux UCT-V Installation
- Windows UCT-V Installation

NOTE: If you want to avoid downloading and installing the UCT-Vs every time there is a new instance to be monitored, you can save the UCT-V running on an instance as a private AMI.
To save the UCT-V as an AMI from your EC2 console, right click on the instance and navigate to **Image and Templates** > **Create Image**.

Linux UCT-V Installation

You can install UCT-V on various Linux distributions using Debian or RPM packages.

You must have sudo/root access to edit the UCT-V configuration file. Establish an SSH connection to the virtual machine and ensure you have permission to execute the sudo command.

You may need to modify the network configuration files for dual or multiple network interface configurations to ensure that the extra NIC/Network interface initializes at boot time.

Refer to the following sections:

- Linux Network Firewall Requirements
- Install Linux UCT-Vs
- Register Linux UCT-V

Prerequisites

- UCT-V is a standalone service. By default, most modern Linux operating systems come pre-installed with all the necessary packages for the UCT-V to function without additional configuration.
- Before registering Linux UCT-V, you should generate a token and place it in the **/etc/gigamon-cloud.conf** configuration file. Refer to Configure Tokens.

Linux Network Firewall Requirements

If Network Firewall requirements or security groups are configured in your environment, you must open the following ports for the virtual machine.

Direction	Port	Protocol	CIDR	Purpose
Inbound	9902	TCP	UCT-V Controller IP	Allows UCT-V to receive control and management plane traffic from UCT-V Controller

You can use the following commands to add the Network Firewall rule.

```
sudo firewall-cmd --add-port=9902/tcp
sudo firewall-cmd --runtime-to-permanent
```

Install Linux UCT-Vs

You can install the UCT-Vs either from Debian or RPM packages using one of the following options:.

- Install Linux UCT-Vs using Installation Script
- Install Linux UCT-Vs using Manual Configuration

Refer to the following sections for more detailed information and step-by-step instructions.

Install Linux UCT-Vs using Installation Script

Using installation script, you can complete installation.

Perform the following steps:

1. **To install UCT-V from Ubuntu/Debian:**
    a. Download the UCT-V**6.14.00** Debian (.deb) package from the Gigamon Customer Portal. For assistance, contact Gigamon Technical Support.
    b. Copy this package to your instance and Install the package with root privileges. For example,

    ```
    $ ls gigamon-gigavue-uctv-6.14.00-amd64.deb
    $ sudo dpkg -i gigamon-gigavue-uctv-6.14.00-amd64.deb
    ```

2. **To install UCT-V from RPM, Red Hat Enterprise Linux, and CentOS:**
    a. Download the UCT-V**6.14.00** RPM (.rpm) package from the Gigamon Customer Portal. For assistance, contact Gigamon Technical Support.
    b. Copy this package to your instance and install the package with root privileges. For example,

    ```
    $ ls gigamon-gigavue-uctv-6.14.00-x86_64.rpm
    $ sudo rpm -i gigamon-gigavue-uctv-6.14.00-x86_64.rpm
    ```

3. Use the command given below to perform pre-check, installation, and configuration functionalities.

```
sudo uctv-wizard
```

> **NOTE:** The installation script is not provided with the Debian or RPM packages. You can use the script (installation_wizard.sh/uctv-wizard) only after the UCT-V is installed.

Refer to the table below to know more about **uctv-wizard** command usage options and functionalities:

Options	Use Command	Description
pre-check	sudo uctv-wizard pre-check	Checks the status of the required packages and firewall requirements. • If any package is missing, it displays an appropriate message with the missing package details. • If installation includes all the packages, it displays a success message indicating that UCT-V is ready for configuration.
pkg-install	sudo uctv-wizard pkg-install **NOTE:** The uctv-wizard install command requires access to a repository, either public (internet-based) or local, that hosts prerequisite packages for installation. If no repository is accessible, you must manually install the required packages.	Displays the missing package and version details. To proceed with the installation, you can choose between the following: If you wish to skip the prompts and proceed with the system update, enter your option as **y**. The console interface installs the missing packages and restarts the UCT-V service. Enter **N** if you wish to install it manually. For details, refer to Install Linux UCT-Vs using Manual Configuration.
configure	sudo uctv-wizard configure	First, it checks for any existing configured file in the tmp directory (file named gigamon-cloud.conf in the **C:\Users\<username>\AppData\Local** (Windows) or **/etc/uctv/uctv.conf** (Linux) location). If available, UCT-V uses that configuration. If unavailable, UCT-V automatically adds the interface configuration in uctv.conf file, excluding the loopback (lo) interface, with all permissions enabled (source ingress, source egress, and destination). You can add the required policy for the available port if a firewall is installed. If you wish to skip the prompts to add the

Options	Use Command	Description
		required firewall policy, enter your option as **y**. The console interface adds the firewall rules automatically. Enter **N** if you wish to configure manually. For details, refer to Install Linux UCT-Vs using Manual Configuration section.
uninstall	sudo uctv-wizard uninstall	Automatically stops the UCT-V service, removes the firewall rules, and uninstalls the UCT-V.

Notes:

- Use the command below to view all the log messages generated from uctv-wizard. These log messages are stored at **/var/log/uctv-installation.log**

  ```
  sudo vi /var/log/uctv-installation.log
  ```

- Use the command below to know the usage descriptions for the individual operations.

  ```
  sudo uctv-wizard help
  ```

Linux UCT-V Installation Scenarios

1. **Zero Touch Installation** - When using a cloud-integrated script to deploy UCT-V in a virtual machine, no interference is required as the script installs and configures everything automatically.
2. **One Touch Installation** - When using .deb or .rpm packages with all prerequisite packages in place, UCT-V determines that all dependencies are met. It performs auto-configuration and restarts the service.
3. **Two Touch Installation** - When using .deb or .rpm packages with missing prerequisite packages, the platform displays a warning message about the missing packages. You need to install the missing packages using the **sudo uctv-wizard pkg-install** command.

Install Linux UCT-Vs using Manual Configuration

- Install UCT-V from Ubuntu/Debian Package
- Install UCT-V from RPM, Red Hat Enterprise Linux, and CentOS

Install UCT-V from Ubuntu/Debian Package

To install from a Debian package:

1. Download the UCT-V**6.14.00** Debian (.deb) package from the Gigamon Customer Portal. For assistance contact Gigamon Technical Support.
2. Copy this package to your instance.

3. Install the package with root privileges. For example,

```
$ ls gigamon-gigavue-uctv-6.14.00-amd64.deb
$ sudo dpkg -i gigamon-gigavue-uctv-6.14.00-amd64.deb
```

4. Modify the file **/etc/uctv/uctv.conf** to configure and register the source and destination interfaces.
   The following examples registers eth0 as the mirror source for both ingress and egress traffic and eth1 as the destination for this traffic:

   NOTE: When you have an active, successful monitoring session deployed, any modification to the UCT-V config file made after the initial setup requires a UCT-V restart and an inventory refresh or sync from GigaVUE-FM to pick up the new changes and re-initiate the traffic mirroring. GigaVUE-FM does a periodic sync on its own every 15 minutes.

   Example 1—Configuration example to monitor ingress and egress traffic at interface eth0 and use the same interface to send out the mirrored packets

```
# eth0   mirror-src-ingress mirror-src-egress mirror-dst
```

   Example 2—Configuration example to monitor ingress and egress traffic at interface eth0 and use the interface eth1 to send out the mirrored packets

```
# eth0   mirror-src-ingress mirror-src-egress
# eth1   mirror-dst
```

   Example 3—Configuration example to monitor ingress and egress traffic at interface eth0 and eth 1; use the interface eth1 to send out the mirrored packets

```
# eth0   mirror-src-ingress mirror-src-egress
# eth1   mirror-src-ingress mirror-src-egress mirror-dst
```

   Example 4—Configuration example to monitor ingress traffic at iface 'eth0' and egress traffic at iface 'eth1' and use iface 'eth2' to transmit the mirrored packets.

```
# eth0   mirror-src-ingress
# eth1   mirror-src-egress
# eth2 mirror-dst
```

   Example 5—Configuration example to monitor traffic at iface 'lo' that is always registered as bidirectional traffic regardless of the config and use iface 'eth0' to transmit the mirrored packets.

```
# lo mirror-src-ingress mirror-src-egress
# eth0 mirror-dst
```

   NOTE: Ensure that the configuration for a single interface is provided on a single line.

5. Save the file.

6. Restart the UCT-V service.

   ```
   $ systemctl restart uctv.service
   ```

The UCT-V status is displayed as running. Verify the status using the following command:

```
$ systemctl status uctv.service
```

Install UCT-V from RPM, Red Hat Enterprise Linux, and CentOS

To install from an RPM (.rpm) package on a RedHat, CentOS, or other RPM-based system:

1. Download the UCT-V**6.14.00** RPM (.rpm) package from the Gigamon Customer Portal.
   For assistance contact Gigamon Technical Support.
2. Copy this package to your instance.
3. Install the package with root privileges. For example,

   ```
   $ ls gigamon-gigavue-uctv-6.14.00-x86_64.rpm
   $ sudo rpm -i gigamon-gigavue-uctv-6.14.00-x86_64.rpm
   ```

4. Modify the **/etc/uctv/uctv.conf** file to configure and register the source and destination interfaces.
   The following example registers the eth0 as the mirror source for both ingress and egress traffic and registers eth1 as the destination for this traffic as follows:

   NOTE: When you have an active, successful monitoring session deployed, any changes to the UCT-V config file made after the initial setup require an UCT-V restart and an inventory refresh or sync from GigaVUE-FM to pick up the new changes and re-initiate the traffic mirroring. GigaVUE-FM does a periodic sync on its own every 15 minutes.

   Example 1—Configuration example to monitor ingress and egress traffic at interface eth0 and use the same interface to send out the mirrored packets

   ```
   # eth0   mirror-src-ingress mirror-src-egress mirror-dst
   ```

   Example 2—Configuration example to monitor ingress and egress traffic at interface eth0 and use the interface eth1 to send out the mirrored packets

   ```
   # eth0   mirror-src-ingress mirror-src-egress
   # eth1   mirror-dst
   ```

   Example 3—Configuration example to monitor ingress and egress traffic at interface eth0 and eth 1; use the interface eth1 to send out the mirrored packets

   ```
   # eth0   mirror-src-ingress mirror-src-egress
   # eth1   mirror-src-ingress mirror-src-egress mirror-dst
   ```

   Example 4—Configuration example to monitor ingress traffic at iface 'eth0' and egress traffic at iface 'eth1' and use iface 'eth2' to transmit the mirrored packets.

   ```
   # eth0   mirror-src-ingress
   # eth1   mirror-src-egress
   # eth2 mirror-dst
   ```

   Example 5—Configuration example to monitor traffic at iface 'lo' that is always registered as bidirectional traffic regardless of the config and use iface 'eth0' to transmit the mirrored packets.

   ```
   # lo mirror-src-ingress mirror-src-egress
   # eth0 mirror-dst
   ```

   NOTE: Ensure that the configuration for a single interface is provided on a single line.

5. Save the file.
6. Restart the UCT-V service.
   ```
   $ sudo service uctv restart
   ```

The UCT-V status is displayed as running. Verify the status with the following command:

```
$ sudo service uctv status
```

Notes:

- When UCT-V fails to start due to a "**start-limit-hit**" (caused by repeated restarts within 10 minutes), you should correct the underlying issue first. To clear the failure and allow UCT-V to restart, run the following command:

  ```
  sudo systemctl reset-failed uctv.service
  ```

Post Deployment Check:

After installing UCT-V, you can perform the following to verify the version of UCT-V:

1. Enter the command:

   ```
   sudo uctvl uctv-show
   ```

2. Manually execute the following command:

   ```
   export LD_LIBRARY_PATH=/usr/lib/uctv/ssl-lib64/
   ```

Register Linux UCT-V

It is mandatory to create a cloud configuration file and add the token to authenticate the UCT-V package with GigaVUE-FM. The token is required only for initial registration before generating the certificate. You can use the token only once and do not need to maintain.

You can register UCT-V in your virtual machine using:

- **Third Party Orchestration**: The third-party orchestration feature allows you to deploy UCT-V using your own orchestration system. UCT-V uses the information of the user to register with GigaVUE-FM. You can register UCT-V toGigaVUE-FM using Third Party Orchestration with the following two modes:
  a. Generic Mode - Deploy GigaVUE Fabric Components using Generic Mode section in GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration
  b. Integrated Mode - Deploy GigaVUE Fabric Components using Integrated Mode section in GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration

NOTE: If you have already configured gigamon-cloud.conf file in the /tmp directory, you can directly use the **uctv-wizard configure** command (sudo uctv-wizard configure). This action automatically fetches the configuration file and completes the registration process.

Windows UCT-V Installation

Windows UCT-V allows you to select the network interfaces by subnet/CIDR and modify the corresponding monitoring permissions in the configuration file. This options helps you get granular control over the monitored and mirrored traffic.

Refer to the following sections for the Windows UCT-V installation:

- Windows Network Firewall Requirements
- Install Linux UCT-Vs
- Register Linux UCT-V

Windows Network Firewall Requirements

If your environment uses network firewall rules or security groups, you must open specific ports for the virtual machine.

Ensure to use UCT-V Wizard with the configure option to configure Windows local firewall rules. Refer to Install Linux UCT-Vs using Installation Script for more details.

Install Windows UCT-Vs

Rules and Notes:

- VXLAN is the only tunnel type supported for Windows UCT-V.
- Loopback Interface is not supported for Windows UCT-V.
- Before registering Windows UCT-V, generate a token and place it in the **C:\ProgramData\uctv\gigamon-cloud.conf** configuration file. Refer to Configure Tokens.
- Do not manually edit the UCT-V Windows service registry settings. Use the supported installation and upgrade workflows instead.

You can install the UCT-Vs with MSI package using one of the following options:

- Install Linux UCT-Vs using Installation Script
- Install Linux UCT-Vs using Manual Configuration

The Windows UCT-V MSI is a self-contained package that includes all necessary dependencies. However, during set up, it automatically installs the following components:

- **Visual C++ Redistributable 2019 (x86)**
- **Npcap (v1.81 OEM)**

> Before installing the Windows Agent, ensure that Npcap is not already present on the system. If an existing version of Npcap is present, uninstall it manually to avoid conflicts and ensure compatibility with the version bundled in the UCT-V.

Refer to the following sections for more detailed information and instructions.

Install Windows UCT-Vs using Installation Script

1. Download the Windows UCT-V **`6.14.00`** MSI package from the Gigamon Customer Portal. For assistance, contact Gigamon Technical Support.
2. Install the downloaded MSI package as **Administrator**.
   The UCT-V service starts automatically.

3. Use the command below to perform pre-check, adapter setup, adapter restore, and configuration functionalities.

   ```
   uctv-wizard
   ```

   Refer to the table below to know more about **uctv-wizard** command usage options and functionalities:

Options	Use Command	Description
pre-check	uctv-wizard pre-check	Checks the network adapter properties and firewall requirements. It notifies the user if the network adapter's send buffer size is smaller than the required size for the Windows UCT-V and if any firewall rules need to be added. **NOTE:** We recommend to Increase the send buffer size of network adapters to 128 MB during the UCT-V installation to optimize performance and minimize traffic disruption.
adapter-setup	uctv-wizard adapter-setup	Checks the compatible network adapters, increases the send buffer size and restarts the service. Before changing the buffer size, the existing configuration is saved as a backup. You can choose between the following: • If you wish to skip the prompts for changing the buffer size of compatible network adapters, enter the option as **y**. • Enter **N** if you wish to set it up manually. For details, refer to Install Linux UCT-Vs using Manual Configuration.
adapter-restore	uctv-wizard adapter-restore	Using this command, you can restore the backup copy of the network adapter buffer size configuration saved in the in the **uctv-wizard adapter-setup** step. **NOTE:** You need to manually restart the network adapters for changes to take effect immediately. You can choose between the following: • If you wish to skip the prompts for restoring the buffer size of the compatible network adapters, enter the option as **y**.

Options	Use Command	Description
		• Enter **N** if you wish to restore it manually. For details, refer to
configure	uctv-wizard configure	First, it checks for any existing configured file in the tmp directory (file named gigamon-cloud.conf in the **C:\Users\<username>\AppData\Local** location). If available, UCT-V will use that configuration. If unavailable, UCT-V automatically adds the interface configuration in uctv.conf file, excluding the loopback (lo) interface, with all permissions enabled (source ingress, source egress, and destination). You can add the required policy for the available port if a firewall is installed. • If you wish to skip the prompts to add the required firewall policy, enter your option as **y**. The console interface adds the firewall rules automatically. • Enter **N** if you wish to configure manually.
uninstall	uctv-wizard uninstall	Automatically stops the UCT-V service, removes the firewall rules, and uninstalls the UCT-V.

Notes:

- The log messages generated from uctv-wizard are stored at **/C:\ProgramData\uctv\uctv-installation.txt**
- Use the command below to know the usage descriptions for the individual operations.

```
uctv-wizard help
```

Windows UCT-V Installation Scenarios

1. **Zero Touch Installation**: When using a cloud integrated script to deploy UCT-V in a virtual machine, zero interference is required as the script installs and configures everything automatically.
2. **One Touch Installation**: When using a .msi package with all prerequisite packages in place, UCT-V determines that all dependencies are met. It performs auto-configuration and restarts the service.

Install Windows UCT-Vs using Manual Configuration

1. Download the Windows UCT-V**6.14.00** MSI package from the Gigamon Customer Portal. For assistance, contact Gigamon Technical Support.
2. Install the downloaded MSI package as **Administrator**. The UCT-V service starts automatically.

3. Modify the file **C:\ProgramData\Uct-v\uctv.conf** to configure and register the source and destination interfaces.

   NOTE: When you have an active, successful monitoring session deployed, any changes to the UCT-V config file made after the initial setup require a UCT-V restart and an inventory refresh or sync from GigaVUE-FM to pick up the new changes and re-initiate the traffic mirroring. GigaVUE-FM does a periodic sync on its own every 15 minutes.

   Following are the rules to modify the UCT-V configuration file:
   - Interface is selected by matching its CIDR address with config entries.
   - For the VMs with single interface *(.conf file modification is optional)*:
     - if neither mirror-src permissions is granted to the interface, both mirror-src-ingress and mirror-src-egress are granted to it.
     - mirror-dst is always granted implicitly to the interface.
   - For the VMs with multiple interfaces:
     - mirror-dst is granted explicitly in the config file. Only the first matched interface is selected for mirror-dst, all other matched interfaces are ignored.
     - if none interfaces is granted any mirror-src permission, all interfaces are granted mirror-src-ingress and mirror-src-egress.

   Example 1—Configuration example to monitor ingress and egress traffic at interface 192.168.1.0/24 and use the same interface to send out the mirrored packets.

   For IPv4:

   ```
   192.168.1.0/24  mirror-src-ingress mirror-src-egress mirror-dst
   ```

   For IPv6:

   ```
   2001:db8:abcd:ef01::/64 mirror-src-ingress mirror-src-egress mirror-dst
   ```

   Example 2—Configuration example to monitor ingress and egress traffic at interface 192.168.1.0/24 and use the interface 192.168.2.0/24 to send out the mirrored packets.

   For IPv4:

   ```
   192.168.1.0/24   mirror-src-ingress mirror-src-egress
   192.168.2.0/24   mirror-dst
   ```

   For IPv6:

   ```
   2001:db8:abcd:ef01::/64 mirror-src-ingress mirror-src-egress
    2001:db8:abcd:ef01::2/64 mirror-dst
   ```

4. Save the file.

5. Restart the Windows UCT-V using one of the following actions:
   - From the command prompt, run **sc stop uctv** and **sc start uctv**.
   - From the Windows Task Manager, restart the UCT-V.

You can verify the status of the UCT-V in the Service tab of the Windows Task Manager.

Register Windows UCT-V

It is mandatory to create a cloud configuration file and add the token to authenticate the UCT-V package with GigaVUE-FM. The token is required only for initial registration before generating the certificate. You can use the token only once and do not need to maintain.

You can register UCT-V in your virtual machine using:

- **Third Party Orchestration**: The third-party orchestration feature allows you to deploy UCT-V using your own orchestration system. UCT-V uses the information of user to register with GigaVUE-FM.
  UCT-V can register with GigaVUE-FM using Third Party Orchestration in one of the following two modes:
  a. Generic Mode - Deploy GigaVUE Fabric Components using Generic Mode section in GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration
  b. Integrated Mode - Deploy GigaVUE Fabric Components using Integrated Mode section in GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration

NOTE: If you have already configured gigamon-cloud.conf file in the directory (C:\Users\<username>\AppData\Local), you can directly use the **uctv-wizard configure** command (sudo uctv-wizard configure). This action automatically fetches the configuration file and complete the registration process.

Configure and Deploy GigaVUE Fabric Components using AWS - Generic Mode

This section provides instructions on how to register GigaVUE fabric components using AWS EC2 or a configuration file.

Recommended Instance Type

The following table lists the recommended instance type for deploying the fabric components:

Fabric Component	Machine type
GigaVUE V Series Node	c5n.xlarge
UCT-V Controller	t2.medium

Deployment Guidelines

Points to remember before deploying the fabric components using generic mode:

- Set the correct MTU for tunnels: Use 8950 for IPv4 tunnels and 8930 for IPv6. To update the Traffic Acquisition Tunnel MTU:

  1. Select the monitoring domain.
  2. Select the **Edit Monitoring Domain** option.
  3. Enter the **Traffic Acquisition Tunnel MTU** value and select **Save**.

  > **NOTE:** Set the correct MTU before deploying the Monitoring Session. If not, you must undeploy and redeploy the session after updating the MTU.

- When deploying the fabric components using generic mode, you must use subGroupName in the registration data as the connection name.
- You can also create a Monitoring Domain under Third Party Orchestration and provide the monitoring domain name and the connection name as groupName and subGroupName in the registration data. For details, refer to Create Monitoring Domain.
- You can use only **UCT-V** or **Customer Orchestrated Source** as the traffic acquisition method when using generic mode.
- When you deploy the fabric components using Third Party Orchestration, you cannot delete the Monitoring Domain without unregistering the registered fabric components.
- GigaVUE V Series Node must have a minimum of two Networks Interfaces (NIC) attached to it, a management NIC and a data NIC. You can add both these interfaces when deploying the GigaVUE V Series Node in AWS. For details, refer to the Launch an instance using the Launch Instance Wizard topic in Amazon EC2 Documentation.
- Create tokens in the **User Management** page in GigaVUE-FM. For details, refer to Configure Tokens for Third Party Orchestration .
- When GigaVUE-FM is 6.10.00 or above and the Fabric Components are on (n-1) or (n-2) versions, you must create a **Username** and **Password** instead of using tokens in the registration data. For details, refer to the Configure Role-Based Access for Third-Party Orchestration section in the v6.9 Documentation.

In your AWS EC2, you can configure the following GigaVUE fabric components:

Configure UCT-V Controller in AWS

IMPORTANT: You must enable the basic authentication to launch the GigaVUE fabric components for version 6.9 and lower. For more instructions on the steps to enable the basic authentication, refer to Authentication Type.

You can configure more than one UCT-V Controller in a monitoring domain.

To register UCT-V Controller in AWS EC2, use any one of the following methods:

Register UCT-V Controller during Instance Launch

In your AWS EC2 portal, you can launch the UCT-V Controller AMI instance and register UCT-V Controller using user data.

Perform the following steps:

1. On the Instances page of AWS EC2, select **Launch instances**. The Launch Instance wizard appears. For details, refer to the Launch an instance using the Launch Instance Wizard topic in Amazon EC2 Documentation.
2. On the **Step 3: Configure Instance Details** tab:
   a. In the **Advanced details** section, select **V2 only** from the Metadata version drop-down list.
   b. Enter the User data as text in the following format and deploy the instance. The UCT-V Controller uses this user data to generate config file (**/etc/gigamon-cloud.conf**) used to register with GigaVUE-FM.

```
#cloud-config
 write_files:
 - path: /etc/gigamon-cloud.conf
   owner: root:root
   permissions: '0644'
   content: |
     Registration:
        groupName: <Monitoring Domain Name>
        subGroupName: <Connection Name>
        token: <Token>
        remoteAddress: <IP address of the GigaVUE-FM>
        sourceIP: <IP address of UCT-V> (Optional. Required only in multi-NIC deployments
to specify which UCT-V interface to use for communicating with the UCT-V Controller.)
        remotePort: 443
```

3. Go to **Instances > Actions > Instance Settings > Edit user data** and edit the user data.

The UCT-V Controller deployed in AWS EC2 appears on the Monitoring Domain page of GigaVUE-FM.

Register UCT-V Controller after Instance Launch

To register UCT-V Controller after launching a Virtual Machine using a configuration file, perform the following steps:

1. Log in to the UCT-V Controller.
2. Create a local configuration file (**/etc/gigamon-cloud.conf**) and enter the following user data.

```
Registration:
    groupName: <Monitoring Domain Name>
    subGroupName: <Connection Name>
    token: <Token>
    remoteAddress: <IP address of the GigaVUE-FM>
    sourceIP: <IP address of UCT-V Controller> (Optional. Required only in multi-NIC
deployments to specify which UCT-V Controller interface to use for communicating with GigaVUE-
FM.)
    remotePort: 443
```

3. Restart theUCT-V Controller service.

```
$ sudo service uctv-cntlr restart
```

Assign Static IP address for UCT-V Controller

By default, the UCT-V Controller gets assigned an IP address using DHCP.

To assign a static IP address, perform the following steps:

1. Navigate to **/etc/netplan/** directory.
2. Create a new **.yaml** file.

   NOTE: Do not use the default 50-cloud-init.yaml file.

3. Update the file as shown in the following sample:

```
network:
  version: 2
  renderer: NetworkManager
  ethernets:
    <interface>:                # Replace with your actual interface name (e.g., eth0)
      dhcp4: no
      dhcp6: no
      addresses:
        - <IPV4/24>             # e.g., 192.168.1.10/24
        - <IPV6/64>             # e.g., 2001:db8:abcd:0012::1/64
      nameservers:
        addresses:
          - <DNS_IPV4>          # e.g., 8.8.8.8
          - <DNS_IPV6>          # e.g., 2001:4860:4860::8888
      routes:
        - to: 0.0.0.0/0
          via: <IPV4_GW>        # e.g., 192.168.1.1
        - to: ::/0
          via: <IPV6_GW>        # e.g., 2001:db8:abcd:0012::fffe

Example netplan config:

network:
  version: 2
  renderer: NetworkManager
  ethernets:
```

```
ens3:
  addresses:
    - 10.114.53.24/21
  dhcp4: no
  dhcp6: no
  accept-ra: false
  routes:
    - to: 10.114.48.1/32
      scope: link
    - to: default
      via: 10.114.48.1
```

4. Save the file.
5. Apply the configuration.

   $ sudo netplan apply

6. Restart the UCT-V Controller service.

   $ sudo service uctv-cntlr restart

The deployed UCT-V Controller registers with the GigaVUE-FM. After successful registration the UCT-V Controller sends heartbeat messages to GigaVUE-FM every 30 seconds. If one heartbeat is missing, the fabric component status appears as **Unhealthy**. If more than five heartbeats fail to reach GigaVUE-FM, GigaVUE-FM tries to reach the UCT-V Controller. If that fails as well then GigaVUE-FM unregisters the UCT-V Controller and removes from GigaVUE-FM.

Configure UCT-V in AWS

NOTE: Deployment of GigaVUE fabric components through a third-party orchestrator is supported on Linux and Windows platforms. Refer toLinux UCT-V Installation andWindows UCT-V Installation for detailed information on Linux and Windows UCT-V.

You need to register UCT-V through the registered UCT-V Controller. It communicates through PORT 8891.

NOTE: You can configure more than one UCT-V Controller for a UCT-V, so that if one UCT-V Controller goes down, the UCT-V registration will happen through another Controller that is active.

To register UCT-V using a configuration file, follow the steps:

1. Install the UCT-V in the Linux or Windows platform. For details, refer to Linux UCT-V Installation and Windows UCT-V Installation.
2. Log in to the UCT-V.

3. Create a local configuration file and enter the following user data.

   - **/etc/gigamon-cloud.conf** is the local configuration file in Linux platform.
   - **C:\ProgramData\uctv\gigamon-cloud.conf** is the local configuration file in Windows platform.
   - When creating **C:\ProgramData\uctv\gigamon-cloud.conf** file, ensure that the file name extension is **.conf**. To view the file name extension in Windows, follow the steps given below:
     a. Go to File Explorer and open the File Location.
     b. On the top navigation bar, click **View**.
     c. In the **View** tab, enable the **File name extensions** check box.

```
Registration:
    groupName: <Monitoring Domain Name>
    subGroupName: <Connection Name>
    token: <Token>
    remoteAddress: <IP address of the UCT-V Controller 1>,<IP address of the UCT-V
Controller 2>
    sourceIP: <IP address of UCT-V> (Optional. Required only in multi-NIC deployments to
specify which UCT-V interface to use for communicating with the UCT-V Controller.)
```

   NOTE: If you are using multiple interface in UCT-V and UCT-V Controller is not connected to the primary interface, then add the following to the above registration data:

   localInterface:<Interface to which UCT-V Controller is connected>

4. Restart the UCT-V service.
   - Linux platform:
     $ sudo service uctv restart
   - Windows platform: Restart from the Task Manager.

The deployed UCT-V registers with the GigaVUE-FM through the UCT-V Controller. After successful registration the UCT-V sends heartbeat messages to GigaVUE-FM every 30 seconds. If one heartbeat is missing, UCT-V status appears as 'Unhealthy'. If more than five heartbeats fail to reach GigaVUE-FM, then GigaVUE-FM tries to reach the UCT-V. If the effort fails, then GigaVUE-FM unregisters the UCT-V to remove it from GigaVUE-FM.

Configure GigaVUE V Series Nodes and V Series Proxy in AWS

NOTE: It is not mandatory to register GigaVUE V Series Nodes via V Series proxy however, if there is a large number of nodes connected to GigaVUE-FM or if you do not wish to reveal the IP addresses of the GigaVUE V Series 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 Node and GigaVUE V Series Proxy in AWS EC2, use any one of the following methods.

IMPORTANT: You must enable the basic authentication to launch the GigaVUE fabric components for version 6.9 and lower. For more instructions on the steps to enable the basic authentication, refer to Authentication Type.

Register GigaVUE V Series Node and GigaVUE V Series Proxy during Instance Launch

1. On the Instances page of AWS EC2, select **Launch instances**. The Launch Instance wizard appears. For details, refer to Launch an instance using the Launch Instance Wizard topic in Amazon EC2 Documentation.
2. On the **Step 3: Configure Instance Details** tab:
   a. In the **Advanced details** section, select **V2 only** from the Metadata version drop-down list.
   b. Enter the User data as text in the following format and deploy the instance. The GigaVUE V Series Nodes or V Series proxy uses this user data to generate config file (**/etc/gigamon-cloud.conf**) used to register with GigaVUE-FM.

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

NOTE: You can register your GigaVUE V Series Nodes directly with GigaVUE-FM or you can use V Series Proxy to register your GigaVUE V Series Nodes with GigaVUE-FM. If you wish to register GigaVUE V Series Nodes 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 Nodes using V Series proxy then, enter the `remotePort` value as 8891 and `remoteIP` as <IP address of the Proxy>.

3. You can navigate to **Instances > Actions > Instance Settings > Edit user data** and edit the user data.

Register GigaVUE V Series Node and GigaVUE V Series Proxy after Instance Launch

To register GigaVUE V Series Node and GigaVUE V Series Proxy after launching the virtual machine using a configuration file, follow the steps given below:

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

```
Registration:
    groupName: <Monitoring Domain Name>
    subGroupName: <Connection Name>
    token: <Token>
    remoteAddress: <IP address of the GigaVUE-FM> or <IP address of the proxy>
    remotePort: 443
```

> **NOTE:** You can register your GigaVUE V Series Nodes directly with GigaVUE-FM or you can use GigaVUE V Series proxy to register your GigaVUE V Series Nodes with GigaVUE-FM. If you wish to register GigaVUE V Series Nodes 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 Nodes using V Series proxy then, enter the `remotePort` value as 8891 and `remoteIP` as <IP address of the Proxy>.

3. Restart the GigaVUE V Series Node or Proxy service.
   - V Series node:
     ```
     $ sudo service vseries-node restart
     ```
   - V Series proxy:
     ```
     $ sudo service vps restart
     ```

The deployed GigaVUE V Series Proxy registers with the GigaVUE-FM. After successful registration the GigaVUE V Series Proxy sends heartbeat messages to GigaVUE-FM every 30 seconds. If one heartbeat is missing, the fabric component status appears as 'Unhealthy'. If more than five heartbeats fail to reach GigaVUE-FM, GigaVUE-FM tries to reach the GigaVUE V Series proxy and if that fails as well then GigaVUE-FM unregisters the GigaVUE V Series proxy and it will be removed from GigaVUE-FM.

> **NOTE:** When the GigaVUE V Series Node is stopped or terminated from the AWS, it does not send any unregistration request and GigaVUE-FM unregisters the GigaVUE V Series Node soon after.

Assign Static IP address for GigaVUE V Series

By default, the GigaVUE V Series gets assigned an IP address using DHCP.

To assign a static IP address, perform the following steps:

1. Navigate to **/etc/netplan/** directory.
2. Create a new **.yaml** file.

   > **NOTE:** Do not use the default 50-cloud-init.yaml file.

3. Update the file as shown in the following sample:

```
network:
  version: 2
  renderer: NetworkManager
  ethernets:
    <interface>:                # Replace with your actual interface name (e.g., eth0)
      dhcp4: no
      dhcp6: no
      addresses:
        - <IPV4/24>             # e.g., 192.168.1.10/24
        - <IPV6/64>             # e.g., 2001:db8:abcd:0012::1/64
      nameservers:
        addresses:
          - <DNS_IPV4>          # e.g., 8.8.8.8
          - <DNS_IPV6>          # e.g., 2001:4860:4860::8888
      routes:
        - to: 0.0.0.0/0
          via: <IPV4_GW>        # e.g., 192.168.1.1
        - to: ::/0
          via: <IPV6_GW>        # e.g., 2001:db8:abcd:0012::fffe

Example netplan config:

network:
  version: 2
  renderer: NetworkManager
  ethernets:
    ens3:
      addresses:
        - 10.114.53.24/21
      dhcp4: no
      dhcp6: no
      accept-ra: false
      routes:
        - to: 10.114.48.1/32
          scope: link
        - to: default
          via: 10.114.48.1
```

4. Save the file.
5. Apply the configuration.

   $ sudo netplan apply

6. Restart the GigaVUE V Series service.

   $ sudo service vseries-node restart

The deployed GigaVUE V Series registers with the GigaVUE-FM. After successful registration the GigaVUE V Series sends heartbeat messages to GigaVUE-FM every 30 seconds. If one heartbeat is missing, the fabric component status appears as **Unhealthy**. If more than five heartbeats fail to reach GigaVUE-FM, GigaVUE-FM tries to reach the GigaVUE V Series. If that fails as well then GigaVUE-FM unregisters the GigaVUE V Series and removes from GigaVUE-FM.

Configure and Deploy Monitoring Session

In GigaVUE-FM, you must do the following to configure and deploy the Monitoring Session. Refer to Configure Monitoring Session section for more details.

1. **Access the Monitoring Session Page**:
   a. In GigaVUE-FM, go to **Traffic** > **Virtual** > **Orchestrated Flows > AWS**.
   b. 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.
2. **Add components to the canvas**:
   a. Drag and drop the required components to the canvas.
   b. From the **Applications** expand menu, drag and drop the required applications to the graphical workspace.
3. **Deploy the Monitoring Session**:
   a. From the **Actions** menu, select **Deploy**.
   b. After successful deployment on all the V Series Nodes, the status appears as **Success** on the Monitoring Sessions **Sources** tab.

What to do Next

You can view the detailed statistics of an individual traffic processing element in the **TRAFFIC PROCESSING** tab. For more details, refer to View Monitoring Session Statistics (AWS).

Acquire Traffic using Customer Orchestrated Source - Without creating Monitoring Domain

This section outlines the workflow to tunnel traffic directly to GigaVUE V Series Nodes without deploying UCT-V or its controllers. using Customer Orchestrated Source. Refer to the following topics for instruction on configuring traffic acquisition, processing, and forwarding to your desired destination.

- Install GigaVUE-FM on AWS
- Configure Role-Based Access for Third Party Orchestration
- Create a Custom User
- Configure and Deploy Monitoring Session

Install GigaVUE-FM on AWS

This step is optional and applies only when an existing GigaVUE-FM instance is not available.
Refer to Install GigaVUE-FM on AWS for steps to ìnstall GigaVUE-FM on AWS and the steps to start GigaVUE-FM instance and configure it.

Configure Role-Based Access for Third Party Orchestration

If you do not want to use an **Admin Profile** to deploy GigaVUE V Series through a Third Party orchestrator, you can create the required users, roles, and user groups in GigaVUE-FM.

Create a Custom User

You can add users only if you are a user with **fm_super_admin role** or a user with either read or write access to the GigaVUE-FM security Management category.

To add users:

1. Go to **Settings** and select **Authentication** > **GigaVUE-FM User Management > Users**.
2. On the User page, select **New User**.
3. In the Add User page, enter the following details:
   - **Name:** Actual name of the user
   - **Username**: User name configured in GigaVUE-FM
   - **Email**: Email ID of the user
   - **Password/Confirm Password**: Password for the user. For more details, refer to Change Your Password.
   - **User Group:** Select the desired User Group to associate the user.

   GigaVUE-FM prompts for your password.
4. Click **Ok**. The new user is added.

Create a Custom Role and Assign the User

A user role defines permission for users to perform any task or operation in GigaVUE-FM or on the managed device. You can associate a role with user.

> **NOTE:** A user with read-only access cannot perform configurations on the screen. The menus and action buttons in the UI pages are disabled appropriately.

To create a role:

1. Go to **Settings** and select **Authentication> GigaVUE-FM User Management >Roles**.

2. Select **New Role**.
3. In the New Role page, select or enter the following details:
   - **Role Name**: Name of the role.
   - **Description**: Description of the role.
   - **Select Permission**: From the **Select Permissions** tab, select **Third Party Orchestration**, and provide write permissions.
4. Select **Apply** to save the configuration.

Create a Custom User Group and Assign the Custom Role and the User

A user group consists of a set of roles and set of tags associated with users in that group. You can associate the user to one or more groups.

To create a new user group:

1. Go to **Settings**, and then select **Authentication> GigaVUE-FMUser Management >User Groups**.
2. Select **New Group.**
3. In the New User Group page, select **Next** to progress forward and **Back** to navigate backward.
4. In the **Group Info** tab, enter the Group Name and Description details:
5. In the **Assign Roles** tab, select the role that you want to assign to the user group.
6. In the **Assign Tags** tab, select the required tag key and tag value.
7. In the **Assign Users** tab, select the required users.
8. Select **Apply** to save the configuration. The new user group is added.

Configure and Deploy GigaVUE Fabric Components using AWS - Generic Mode

This section provides instructions on how to register GigaVUE fabric components using AWS EC2 or a configuration file.

Recommended Instance Type

The following table lists the recommended instance type for deploying the fabric components:

Fabric Component	Machine type
GigaVUE V Series Node	c5n.xlarge
UCT-V Controller	t2.medium

Deployment Guidelines

Points to remember before deploying the fabric components using generic mode:

- Set the correct MTU for tunnels: Use 8950 for IPv4 tunnels and 8930 for IPv6. To update the Traffic Acquisition Tunnel MTU:

  1. Select the monitoring domain.
  2. Select the **Edit Monitoring Domain** option.
  3. Enter the **Traffic Acquisition Tunnel MTU** value and select **Save**.

  > **NOTE:** Set the correct MTU before deploying the Monitoring Session. If not, you must undeploy and redeploy the session after updating the MTU.

- When deploying the fabric components using generic mode, you must use subGroupName in the registration data as the connection name.
- You can also create a Monitoring Domain under Third Party Orchestration and provide the monitoring domain name and the connection name as groupName and subGroupName in the registration data. For details, refer to Create Monitoring Domain.
- You can use only **UCT-V** or **Customer Orchestrated Source** as the traffic acquisition method when using generic mode.
- When you deploy the fabric components using Third Party Orchestration, you cannot delete the Monitoring Domain without unregistering the registered fabric components.
- GigaVUE V Series Node must have a minimum of two Networks Interfaces (NIC) attached to it, a management NIC and a data NIC. You can add both these interfaces when deploying the GigaVUE V Series Node in AWS. For details, refer to the Launch an instance using the Launch Instance Wizard topic in Amazon EC2 Documentation.
- Create tokens in the **User Management** page in GigaVUE-FM. For details, refer to Configure Tokens for Third Party Orchestration .
- When GigaVUE-FM is 6.10.00 or above and the Fabric Components are on (n-1) or (n-2) versions, you must create a **Username** and **Password** instead of using tokens in the registration data. For details, refer to the Configure Role-Based Access for Third-Party Orchestration section in the v6.9 Documentation.

In your AWS EC2, you can configure the following GigaVUE fabric components:

Configure UCT-V Controller in AWS

IMPORTANT: You must enable the basic authentication to launch the GigaVUE fabric components for version 6.9 and lower. For more instructions on the steps to enable the basic authentication, refer to Authentication Type.

You can configure more than one UCT-V Controller in a monitoring domain.

To register UCT-V Controller in AWS EC2, use any one of the following methods:

Register UCT-V Controller during Instance Launch

In your AWS EC2 portal, you can launch the UCT-V Controller AMI instance and register UCT-V Controller using user data.

Perform the following steps:

1. On the Instances page of AWS EC2, select **Launch instances**. The Launch Instance wizard appears. For details, refer to the Launch an instance using the Launch Instance Wizard topic in Amazon EC2 Documentation.
2. On the **Step 3: Configure Instance Details** tab:
   a. In the **Advanced details** section, select **V2 only** from the Metadata version drop-down list.
   b. Enter the User data as text in the following format and deploy the instance. The UCT-V Controller uses this user data to generate config file (**/etc/gigamon-cloud.conf**) used to register with GigaVUE-FM.

```
#cloud-config
 write_files:
 - path: /etc/gigamon-cloud.conf
   owner: root:root
   permissions: '0644'
   content: |
     Registration:
        groupName: <Monitoring Domain Name>
        subGroupName: <Connection Name>
        token: <Token>
        remoteAddress: <IP address of the GigaVUE-FM>
        sourceIP: <IP address of UCT-V> (Optional. Required only in multi-NIC deployments
to specify which UCT-V interface to use for communicating with the UCT-V Controller.)
        remotePort: 443
```

3. Go to **Instances > Actions > Instance Settings > Edit user data** and edit the user data.

The UCT-V Controller deployed in AWS EC2 appears on the Monitoring Domain page of GigaVUE-FM.

Register UCT-V Controller after Instance Launch

To register UCT-V Controller after launching a Virtual Machine using a configuration file, perform the following steps:

1. Log in to the UCT-V Controller.
2. Create a local configuration file (**/etc/gigamon-cloud.conf**) and enter the following user data.

```
Registration:
    groupName: <Monitoring Domain Name>
    subGroupName: <Connection Name>
    token: <Token>
    remoteAddress: <IP address of the GigaVUE-FM>
    sourceIP: <IP address of UCT-V Controller> (Optional. Required only in multi-NIC
deployments to specify which UCT-V Controller interface to use for communicating with GigaVUE-
FM.)
    remotePort: 443
```

3. Restart theUCT-V Controller service.

```
$ sudo service uctv-cntlr restart
```

Assign Static IP address for UCT-V Controller

By default, the UCT-V Controller gets assigned an IP address using DHCP.

To assign a static IP address, perform the following steps:

1. Navigate to **/etc/netplan/** directory.
2. Create a new **.yaml** file.

   NOTE: Do not use the default 50-cloud-init.yaml file.

3. Update the file as shown in the following sample:

```
network:
  version: 2
  renderer: NetworkManager
  ethernets:
    <interface>:                # Replace with your actual interface name (e.g., eth0)
      dhcp4: no
      dhcp6: no
      addresses:
        - <IPV4/24>             # e.g., 192.168.1.10/24
        - <IPV6/64>             # e.g., 2001:db8:abcd:0012::1/64
      nameservers:
        addresses:
          - <DNS_IPV4>          # e.g., 8.8.8.8
          - <DNS_IPV6>          # e.g., 2001:4860:4860::8888
      routes:
```

```
        - to: 0.0.0.0/0
          via: <IPV4_GW>        # e.g., 192.168.1.1
        - to: ::/0
          via: <IPV6_GW>        # e.g., 2001:db8:abcd:0012::fffe

Example netplan config:

network:
  version: 2
  renderer: NetworkManager
  ethernets:
    ens3:
      addresses:
        - 10.114.53.24/21
      dhcp4: no
      dhcp6: no
      accept-ra: false
      routes:
        - to: 10.114.48.1/32
          scope: link
        - to: default
          via: 10.114.48.1
```

4. Save the file.
5. Apply the configuration.

   $ sudo netplan apply

6. Restart the UCT-V Controller service.

   $ sudo service uctv-cntlr restart

The deployed UCT-V Controller registers with the GigaVUE-FM. After successful registration the UCT-V Controller sends heartbeat messages to GigaVUE-FM every 30 seconds. If one heartbeat is missing, the fabric component status appears as **Unhealthy**. If more than five heartbeats fail to reach GigaVUE-FM, GigaVUE-FM tries to reach the UCT-V Controller. If that fails as well then GigaVUE-FM unregisters the UCT-V Controller and removes from GigaVUE-FM.

Configure UCT-V in AWS

NOTE: Deployment of GigaVUE fabric components through a third-party orchestrator is supported on Linux and Windows platforms. Refer toLinux UCT-V Installation andWindows UCT-V Installation for detailed information on Linux and Windows UCT-V.

You need to register UCT-V through the registered UCT-V Controller. It communicates through PORT 8891.

NOTE: You can configure more than one UCT-V Controller for a UCT-V, so that if one UCT-V Controller goes down, the UCT-V registration will happen through another Controller that is active.

To register UCT-V using a configuration file, follow the steps:

1. Install the UCT-V in the Linux or Windows platform. For details, refer to Linux UCT-V Installation and Windows UCT-V Installation.
2. Log in to the UCT-V.
3. Create a local configuration file and enter the following user data.

   - **/etc/gigamon-cloud.conf** is the local configuration file in Linux platform.
   - **C:\ProgramData\uctv\gigamon-cloud.conf** is the local configuration file in Windows platform.
   - When creating **C:\ProgramData\uctv\gigamon-cloud.conf** file, ensure that the file name extension is **.conf**. To view the file name extension in Windows, follow the steps given below:
     a. Go to File Explorer and open the File Location.
     b. On the top navigation bar, click **View**.
     c. In the **View** tab, enable the **File name extensions** check box.

   ```
   Registration:
       groupName: <Monitoring Domain Name>
       subGroupName: <Connection Name>
       token: <Token>
       remoteAddress: <IP address of the UCT-V Controller 1>,<IP address of the UCT-V
   Controller 2>
       sourceIP: <IP address of UCT-V> (Optional. Required only in multi-NIC deployments to
   specify which UCT-V interface to use for communicating with the UCT-V Controller.)
   ```

   NOTE: If you are using multiple interface in UCT-V and UCT-V Controller is not connected to the primary interface, then add the following to the above registration data:

   ```
   localInterface:<Interface to which UCT-V Controller is connected>
   ```

4. Restart the UCT-V service.
   - Linux platform:
     ```
     $ sudo service uctv restart
     ```
   - Windows platform: Restart from the Task Manager.

The deployed UCT-V registers with the GigaVUE-FM through the UCT-V Controller. After successful registration the UCT-V sends heartbeat messages to GigaVUE-FM every 30

seconds. If one heartbeat is missing, UCT-V status appears as 'Unhealthy'. If more than five heartbeats fail to reach GigaVUE-FM, then GigaVUE-FM tries to reach the UCT-V. If the effort fails, then GigaVUE-FM unregisters the UCT-V to remove it from GigaVUE-FM.

Configure GigaVUE V Series Nodes and V Series Proxy in AWS

NOTE: It is not mandatory to register GigaVUE V Series Nodes via V Series proxy however, if there is a large number of nodes connected to GigaVUE-FM or if you do not wish to reveal the IP addresses of the GigaVUE V Series 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 Node and GigaVUE V Series Proxy in AWS EC2, use any one of the following methods.

IMPORTANT: You must enable the basic authentication to launch the GigaVUE fabric components for version 6.9 and lower. For more instructions on the steps to enable the basic authentication, refer to Authentication Type.

Register GigaVUE V Series Node and GigaVUE V Series Proxy during Instance Launch

1. On the Instances page of AWS EC2, select **Launch instances**. The Launch Instance wizard appears. For details, refer to Launch an instance using the Launch Instance Wizard topic in Amazon EC2 Documentation.
2. On the **Step 3: Configure Instance Details** tab:
   a. In the **Advanced details** section, select **V2 only** from the Metadata version drop-down list.
   b. Enter the User data as text in the following format and deploy the instance. The GigaVUE V Series Nodes or V Series proxy uses this user data to generate config file (**/etc/gigamon-cloud.conf**) used to register with GigaVUE-FM.

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

> **NOTE:** You can register your GigaVUE V Series Nodes directly with GigaVUE-FM or you can use V Series Proxy to register your GigaVUE V Series Nodes with GigaVUE-FM. If you wish to register GigaVUE V Series Nodes 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 Nodes using V Series proxy then, enter the **`remotePort`** value as 8891 and **`remoteIP`** as <IP address of the Proxy>.

3. You can navigate to **Instances > Actions > Instance Settings > Edit user data** and edit the user data.

Register GigaVUE V Series Node and GigaVUE V Series Proxy after Instance Launch

To register GigaVUE V Series Node and GigaVUE V Series Proxy after launching the virtual machine using a configuration file, follow the steps given below:

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

```
Registration:
    groupName: <Monitoring Domain Name>
    subGroupName: <Connection Name>
    token: <Token>
    remoteAddress: <IP address of the GigaVUE-FM> or <IP address of the proxy>
    remotePort: 443
```

> **NOTE:** You can register your GigaVUE V Series Nodes directly with GigaVUE-FM or you can use GigaVUE V Series proxy to register your GigaVUE V Series Nodes with GigaVUE-FM. If you wish to register GigaVUE V Series Nodes 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 Nodes using V Series proxy then, enter the **`remotePort`** value as 8891 and **`remoteIP`** as <IP address of the Proxy>.

3. Restart the GigaVUE V Series Node or Proxy service.
   - V Series node:
     ```
     $ sudo service vseries-node restart
     ```
   - V Series proxy:
     ```
     $ sudo service vps restart
     ```

The deployed GigaVUE V Series Proxy registers with the GigaVUE-FM. After successful registration the GigaVUE V Series Proxy sends heartbeat messages to GigaVUE-FM every 30 seconds. If one heartbeat is missing, the fabric component status appears as 'Unhealthy'. If more than five heartbeats fail to reach GigaVUE-FM, GigaVUE-FM tries to reach the GigaVUE V Series proxy and if that fails as well then GigaVUE-FM unregisters the GigaVUE V Series proxy and it will be removed from GigaVUE-FM.

NOTE: When the GigaVUE V Series Node is stopped or terminated from the AWS, it does not send any unregistration request and GigaVUE-FM unregisters the GigaVUE V Series Node soon after.

Assign Static IP address for GigaVUE V Series

By default, the GigaVUE V Series gets assigned an IP address using DHCP.

To assign a static IP address, perform the following steps:

1. Navigate to **/etc/netplan/** directory.
2. Create a new **.yaml** file.

   NOTE: Do not use the default 50-cloud-init.yaml file.

3. Update the file as shown in the following sample:

```
network:
  version: 2
  renderer: NetworkManager
  ethernets:
    <interface>:                # Replace with your actual interface name (e.g., eth0)
      dhcp4: no
      dhcp6: no
      addresses:
        - <IPV4/24>             # e.g., 192.168.1.10/24
        - <IPV6/64>             # e.g., 2001:db8:abcd:0012::1/64
      nameservers:
        addresses:
          - <DNS_IPV4>          # e.g., 8.8.8.8
          - <DNS_IPV6>          # e.g., 2001:4860:4860::8888
      routes:
        - to: 0.0.0.0/0
          via: <IPV4_GW>        # e.g., 192.168.1.1
        - to: ::/0
          via: <IPV6_GW>        # e.g., 2001:db8:abcd:0012::fffe

Example netplan config:

network:
  version: 2
  renderer: NetworkManager
  ethernets:
    ens3:
      addresses:
        - 10.114.53.24/21
      dhcp4: no
      dhcp6: no
      accept-ra: false
      routes:
        - to: 10.114.48.1/32
          scope: link
        - to: default
          via: 10.114.48.1
```

4. Save the file.
5. Apply the configuration.

```
$ sudo netplan apply
```

6. Restart the GigaVUE V Series service.

```
$ sudo service vseries-node restart
```

The deployed GigaVUE V Series registers with the GigaVUE-FM. After successful registration the GigaVUE V Series sends heartbeat messages to GigaVUE-FM every 30 seconds. If one heartbeat is missing, the fabric component status appears as **Unhealthy**. If more than five heartbeats fail to reach GigaVUE-FM, GigaVUE-FM tries to reach the GigaVUE V Series. If that fails as well then GigaVUE-FM unregisters the GigaVUE V Series and removes from GigaVUE-FM.

Configure and Deploy Monitoring Session

In GigaVUE-FM, you must do the following to configure and deploy the Monitoring Session. Refer to Configure Monitoring Session section for more details.

1. **Access the Monitoring Session Page**:
   a. In GigaVUE-FM, go to **Traffic** > **Virtual** > **Orchestrated Flows > AWS**.
   b. 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.
2. **Create an ingress REP**:
   a. In the canvas, from the **New** expand menu, drag and drop New Tunnel to the graphical workspace.
   b. On the new tunnel icon, select the ⋮ menu button and select **Details**. The **Add Tunnel Spec** quick view page appears.
   c. Enter the **Alias**, **Description**, and the **Type** details and click **Save**.
3. **Add components to the canvas**:
   a. Drag and drop the required components to the canvas.
   b. From the **Applications** expand menu, drag and drop the required applications to the graphical workspace.
4. **Deploy the Monitoring Session**:
   a. From the **Actions** menu, select **Deploy**.
   b. After successful deployment on all the V Series Nodes, the status appears as **Success** on the Monitoring Sessions **Sources** tab.

What to do Next

You can view the detailed statistics of an individual traffic processing element in the **TRAFFIC PROCESSING** tab. For more details, refer to View Monitoring Session Statistics (AWS).

Acquire Traffic using UCT-V - By Creating Monitoring Domain

In generic mode, you can also create a Monitoring Domain under Third Party Orchestration and provide the Monitoring Domain name and the connection name in the user data that used by your orchestrator.

This section outlines the workflow to acquire traffic directly from virtual machines and send it to GigaVUE V Series Nodes using UCT-V. Refer to the following topics for instruction on configuring traffic acquisition, processing, and forwarding to your desired destination.

- Install GigaVUE-FM on AWS
- Configure Role-Based Access for Third Party Orchestration
- Install UCT-Vs
- Create a Monitoring Domain
- Configure and Deploy GigaVUE Fabric Components using AWS - Generic Mode
- Configure and Deploy Monitoring Session

Install GigaVUE-FM on AWS

This step is optional and applies only when an existing GigaVUE-FM instance is not available.
Refer to Install GigaVUE-FM on AWS for steps to ìnstall GigaVUE-FM on AWS and the steps to start GigaVUE-FM instance and configure it.

Configure Role-Based Access for Third Party Orchestration

If you do not want to use an **Admin Profile** to deploy GigaVUE V Series through a Third Party orchestrator, you can create the required users, roles, and user groups in GigaVUE-FM.

Create a Custom User

You can add users only if you are a user with **fm_super_admin role** or a user with either read or write access to the GigaVUE-FM security Management category.

To add users:

1. Go to **Settings** and select **Authentication** > **GigaVUE-FM User Management > Users**.

2. On the User page, select **New User**.
3. In the Add User page, enter the following details:
   - **Name:** Actual name of the user
   - **Username**: User name configured in GigaVUE-FM
   - **Email**: Email ID of the user
   - **Password/Confirm Password**: Password for the user. For more details, refer to Change Your Password.
   - **User Group:** Select the desired User Group to associate the user.

   GigaVUE-FM prompts for your password.
4. Click **Ok**. The new user is added.

Create a Custom Role and Assign the User

A user role defines permission for users to perform any task or operation in GigaVUE-FM or on the managed device. You can associate a role with user.

NOTE: A user with read-only access cannot perform configurations on the screen. The menus and action buttons in the UI pages are disabled appropriately.

To create a role:

1. Go to **Settings** and select **Authentication> GigaVUE-FM User Management >Roles**.
2. Select **New Role**.
3. In the New Role page, select or enter the following details:
   - **Role Name**: Name of the role.
   - **Description**: Description of the role.
   - **Select Permission**: From the **Select Permissions** tab, select **Third Party Orchestration**, and provide write permissions.
4. Select **Apply** to save the configuration.

Create a Custom User Group and Assign the Custom Role and the User

A user group consists of a set of roles and set of tags associated with users in that group. You can associate the user to one or more groups.

To create a new user group:

1. Go to **Settings**, and then select **Authentication> GigaVUE-FMUser Management >User Groups**.
2. Select **New Group.**

3. In the New User Group page, select **Next** to progress forward and **Back** to navigate backward.
4. In the **Group Info** tab, enter the Group Name and Description details:
5. In the **Assign Roles** tab, select the role that you want to assign to the user group.
6. In the **Assign Tags** tab, select the required tag key and tag value.
7. In the **Assign Users** tab, select the required users.
8. Select **Apply** to save the configuration. The new user group is added.

Install UCT-Vs

You can install UCT-V on both Linux and Windows environments. For details, refer to the following topics:

- Linux UCT-V Installation
- Windows UCT-V Installation

Linux UCT-V Installation

You can install UCT-V on various Linux distributions using Debian or RPM packages.

You must have sudo/root access to edit the UCT-V configuration file. Establish an SSH connection to the virtual machine and ensure you have permission to execute the sudo command.

You may need to modify the network configuration files for dual or multiple network interface configurations to ensure that the extra NIC/Network interface initializes at boot time.

Refer to the following sections:

- Linux Network Firewall Requirements
- Install Linux UCT-Vs
- Register Linux UCT-V

Prerequisites

- UCT-V is a standalone service. By default, most modern Linux operating systems come pre-installed with all the necessary packages for the UCT-V to function without additional configuration.
- Before registering Linux UCT-V, you should generate a token and place it in the **/etc/gigamon-cloud.conf** configuration file. Refer to Configure Tokens.

Linux Network Firewall Requirements

If Network Firewall requirements or security groups are configured in your environment, you must open the following ports for the virtual machine.

Direction	Port	Protocol	CIDR	Purpose
Inbound	9902	TCP	UCT-V Controller IP	Allows UCT-V to receive control and management plane traffic from UCT-V Controller

You can use the following commands to add the Network Firewall rule.

```
sudo firewall-cmd --add-port=9902/tcp
sudo firewall-cmd --runtime-to-permanent
```

Install Linux UCT-Vs

You can install the UCT-Vs either from Debian or RPM packages using one of the following options:.

- Install Linux UCT-Vs using Installation Script
- Install Linux UCT-Vs using Manual Configuration

Refer to the following sections for more detailed information and step-by-step instructions.

Install Linux UCT-Vs using Installation Script

Using installation script, you can complete installation.

Perform the following steps:

1. **To install UCT-V from Ubuntu/Debian:**
    a. Download the UCT-V**6.14.00** Debian (.deb) package from the Gigamon Customer Portal. For assistance, contact Gigamon Technical Support.
    b. Copy this package to your instance and Install the package with root privileges. For example,

```
$ ls gigamon-gigavue-uctv-6.14.00-amd64.deb
$ sudo dpkg -i gigamon-gigavue-uctv-6.14.00-amd64.deb
```

2. **To install UCT-V from RPM, Red Hat Enterprise Linux, and CentOS:**

    a. Download the UCT-V**6.14.00** RPM (.rpm) package from the Gigamon Customer Portal. For assistance, contact Gigamon Technical Support.

    b. Copy this package to your instance and install the package with root privileges. For example,

    ```
    $ ls gigamon-gigavue-uctv-6.14.00-x86_64.rpm
    $ sudo rpm -i gigamon-gigavue-uctv-6.14.00-x86_64.rpm
    ```

3. Use the command given below to perform pre-check, installation, and configuration functionalities.

```
sudo uctv-wizard
```

> **NOTE:** The installation script is not provided with the Debian or RPM packages. You can use the script (installation_wizard.sh/uctv-wizard) only after the UCT-V is installed.

Refer to the table below to know more about **uctv-wizard** command usage options and functionalities:

Options	Use Command	Description
pre-check	sudo uctv-wizard pre-check	Checks the status of the required packages and firewall requirements. • If any package is missing, it displays an appropriate message with the missing package details. • If installation includes all the packages, it displays a success message indicating that UCT-V is ready for configuration.
pkg-install	sudo uctv-wizard pkg-install **NOTE:** The uctv-wizard install command requires access to a repository, either public (internet-based) or local, that hosts prerequisite packages for installation. If no repository is accessible, you must manually install the required packages.	Displays the missing package and version details. To proceed with the installation, you can choose between the following: If you wish to skip the prompts and proceed with the system update, enter your option as **y**. The console interface installs the missing packages and restarts the UCT-V service. Enter **N** if you wish to install it manually. For details, refer to Install Linux UCT-Vs using Manual Configuration.
configure	sudo uctv-wizard configure	First, it checks for any existing configured file in the tmp directory (file named gigamon-cloud.conf in the **C:\Users\<username>\AppData\Local** (Windows) or **/etc/uctv/uctv.conf** (Linux) location). If available, UCT-V uses that configuration. If unavailable, UCT-V automatically adds the interface configuration in uctv.conf file, excluding the loopback (lo) interface, with all permissions enabled (source ingress, source egress, and destination). You can add the required policy for the available port if a firewall is installed. If you wish to skip the prompts to add the

Options	Use Command	Description
		required firewall policy, enter your option as **y**. The console interface adds the firewall rules automatically. Enter **N** if you wish to configure manually. For details, refer to Install Linux UCT-Vs using Manual Configuration section.
uninstall	sudo uctv-wizard uninstall	Automatically stops the UCT-V service, removes the firewall rules, and uninstalls the UCT-V.

Notes:

- Use the command below to view all the log messages generated from uctv-wizard. These log messages are stored at **/var/log/uctv-installation.log**

  ```
  sudo vi /var/log/uctv-installation.log
  ```

- Use the command below to know the usage descriptions for the individual operations.

  ```
  sudo uctv-wizard help
  ```

Linux UCT-V Installation Scenarios

1. **Zero Touch Installation** - When using a cloud-integrated script to deploy UCT-V in a virtual machine, no interference is required as the script installs and configures everything automatically.
2. **One Touch Installation** - When using .deb or .rpm packages with all prerequisite packages in place, UCT-V determines that all dependencies are met. It performs auto-configuration and restarts the service.
3. **Two Touch Installation** - When using .deb or .rpm packages with missing prerequisite packages, the platform displays a warning message about the missing packages. You need to install the missing packages using the **sudo uctv-wizard pkg-install** command.

Install Linux UCT-Vs using Manual Configuration

- Install UCT-V from Ubuntu/Debian Package
- Install UCT-V from RPM, Red Hat Enterprise Linux, and CentOS

Install UCT-V from Ubuntu/Debian Package

To install from a Debian package:

1. Download the UCT-V**6.14.00** Debian (.deb) package from the Gigamon Customer Portal. For assistance contact Gigamon Technical Support.
2. Copy this package to your instance.

3. Install the package with root privileges. For example,

```
$ ls gigamon-gigavue-uctv-6.14.00-amd64.deb
$ sudo dpkg -i gigamon-gigavue-uctv-6.14.00-amd64.deb
```

4. Modify the file **/etc/uctv/uctv.conf** to configure and register the source and destination interfaces.
   The following examples registers eth0 as the mirror source for both ingress and egress traffic and eth1 as the destination for this traffic:

   NOTE: When you have an active, successful monitoring session deployed, any modification to the UCT-V config file made after the initial setup requires a UCT-V restart and an inventory refresh or sync from GigaVUE-FM to pick up the new changes and re-initiate the traffic mirroring. GigaVUE-FM does a periodic sync on its own every 15 minutes.

   Example 1—Configuration example to monitor ingress and egress traffic at interface eth0 and use the same interface to send out the mirrored packets

```
# eth0   mirror-src-ingress mirror-src-egress mirror-dst
```

   Example 2—Configuration example to monitor ingress and egress traffic at interface eth0 and use the interface eth1 to send out the mirrored packets

```
# eth0   mirror-src-ingress mirror-src-egress
# eth1   mirror-dst
```

   Example 3—Configuration example to monitor ingress and egress traffic at interface eth0 and eth 1; use the interface eth1 to send out the mirrored packets

```
# eth0   mirror-src-ingress mirror-src-egress
# eth1   mirror-src-ingress mirror-src-egress mirror-dst
```

   Example 4—Configuration example to monitor ingress traffic at iface 'eth0' and egress traffic at iface 'eth1' and use iface 'eth2' to transmit the mirrored packets.

```
# eth0   mirror-src-ingress
# eth1   mirror-src-egress
# eth2 mirror-dst
```

   Example 5—Configuration example to monitor traffic at iface 'lo' that is always registered as bidirectional traffic regardless of the config and use iface 'eth0' to transmit the mirrored packets.

```
# lo mirror-src-ingress mirror-src-egress
# eth0 mirror-dst
```

   NOTE: Ensure that the configuration for a single interface is provided on a single line.

5. Save the file.

6. Restart the UCT-V service.

   ```
   $ systemctl restart uctv.service
   ```

The UCT-V status is displayed as running. Verify the status using the following command:

```
$ systemctl status uctv.service
```

Install UCT-V from RPM, Red Hat Enterprise Linux, and CentOS

To install from an RPM (.rpm) package on a RedHat, CentOS, or other RPM-based system:

1. Download the UCT-V**6.14.00** RPM (.rpm) package from the Gigamon Customer Portal.
   For assistance contact Gigamon Technical Support.
2. Copy this package to your instance.
3. Install the package with root privileges. For example,

   ```
   $ ls gigamon-gigavue-uctv-6.14.00-x86_64.rpm
   $ sudo rpm -i gigamon-gigavue-uctv-6.14.00-x86_64.rpm
   ```

4. Modify the **/etc/uctv/uctv.conf** file to configure and register the source and destination interfaces.
   The following example registers the eth0 as the mirror source for both ingress and egress traffic and registers eth1 as the destination for this traffic as follows:

   NOTE: When you have an active, successful monitoring session deployed, any changes to the UCT-V config file made after the initial setup require an UCT-V restart and an inventory refresh or sync from GigaVUE-FM to pick up the new changes and re-initiate the traffic mirroring. GigaVUE-FM does a periodic sync on its own every 15 minutes.

   Example 1—Configuration example to monitor ingress and egress traffic at interface eth0 and use the same interface to send out the mirrored packets

   ```
   # eth0   mirror-src-ingress mirror-src-egress mirror-dst
   ```

   Example 2—Configuration example to monitor ingress and egress traffic at interface eth0 and use the interface eth1 to send out the mirrored packets

   ```
   # eth0   mirror-src-ingress mirror-src-egress
   # eth1   mirror-dst
   ```

   Example 3—Configuration example to monitor ingress and egress traffic at interface eth0 and eth 1; use the interface eth1 to send out the mirrored packets

   ```
   # eth0   mirror-src-ingress mirror-src-egress
   # eth1   mirror-src-ingress mirror-src-egress mirror-dst
   ```

   Example 4—Configuration example to monitor ingress traffic at iface 'eth0' and egress traffic at iface 'eth1' and use iface 'eth2' to transmit the mirrored packets.

   ```
   # eth0   mirror-src-ingress
   # eth1   mirror-src-egress
   # eth2 mirror-dst
   ```

   Example 5—Configuration example to monitor traffic at iface 'lo' that is always registered as bidirectional traffic regardless of the config and use iface 'eth0' to transmit the mirrored packets.

   ```
   # lo mirror-src-ingress mirror-src-egress
   # eth0 mirror-dst
   ```

   NOTE: Ensure that the configuration for a single interface is provided on a single line.

5. Save the file.
6. Restart the UCT-V service.
   ```
   $ sudo service uctv restart
   ```

The UCT-V status is displayed as running. Verify the status with the following command:

```
$ sudo service uctv status
```

Notes:

- When UCT-V fails to start due to a "**start-limit-hit**" (caused by repeated restarts within 10 minutes), you should correct the underlying issue first. To clear the failure and allow UCT-V to restart, run the following command:

  ```
  sudo systemctl reset-failed uctv.service
  ```

Post Deployment Check:

After installing UCT-V, you can perform the following to verify the version of UCT-V:

1. Enter the command:

   ```
   sudo uctvl uctv-show
   ```

2. Manually execute the following command:

   ```
   export LD_LIBRARY_PATH=/usr/lib/uctv/ssl-lib64/
   ```

Register Linux UCT-V

It is mandatory to create a cloud configuration file and add the token to authenticate the UCT-V package with GigaVUE-FM. The token is required only for initial registration before generating the certificate. You can use the token only once and do not need to maintain.

You can register UCT-V in your virtual machine using:

- **Third Party Orchestration**: The third-party orchestration feature allows you to deploy UCT-V using your own orchestration system. UCT-V uses the information of the user to register with GigaVUE-FM. You can register UCT-V toGigaVUE-FM using Third Party Orchestration with the following two modes:
  a. Generic Mode - Deploy GigaVUE Fabric Components using Generic Mode section in GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration
  b. Integrated Mode - Deploy GigaVUE Fabric Components using Integrated Mode section in GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration

NOTE: If you have already configured gigamon-cloud.conf file in the /tmp directory, you can directly use the **uctv-wizard configure** command (sudo uctv-wizard configure). This action automatically fetches the configuration file and completes the registration process.

Windows UCT-V Installation

Windows UCT-V allows you to select the network interfaces by subnet/CIDR and modify the corresponding monitoring permissions in the configuration file. This options helps you get granular control over the monitored and mirrored traffic.

Refer to the following sections for the Windows UCT-V installation:

- Windows Network Firewall Requirements
- Install Linux UCT-Vs
- Register Linux UCT-V

Windows Network Firewall Requirements

If your environment uses network firewall rules or security groups, you must open specific ports for the virtual machine.

Ensure to use UCT-V Wizard with the configure option to configure Windows local firewall rules. Refer to Install Linux UCT-Vs using Installation Script for more details.

Install Windows UCT-Vs

Rules and Notes:

- VXLAN is the only tunnel type supported for Windows UCT-V.
- Loopback Interface is not supported for Windows UCT-V.
- Before registering Windows UCT-V, generate a token and place it in the **C:\ProgramData\uctv\gigamon-cloud.conf** configuration file. Refer to Configure Tokens.
- Do not manually edit the UCT-V Windows service registry settings. Use the supported installation and upgrade workflows instead.

You can install the UCT-Vs with MSI package using one of the following options:

- Install Linux UCT-Vs using Installation Script
- Install Linux UCT-Vs using Manual Configuration

The Windows UCT-V MSI is a self-contained package that includes all necessary dependencies. However, during set up, it automatically installs the following components:

- **Visual C++ Redistributable 2019 (x86)**
- **Npcap (v1.81 OEM)**

> Before installing the Windows Agent, ensure that Npcap is not already present on the system. If an existing version of Npcap is present, uninstall it manually to avoid conflicts and ensure compatibility with the version bundled in the UCT-V.

Refer to the following sections for more detailed information and instructions.

Install Windows UCT-Vs using Installation Script

1. Download the Windows UCT-V **`6.14.00`** MSI package from the Gigamon Customer Portal. For assistance, contact Gigamon Technical Support.
2. Install the downloaded MSI package as **Administrator**.
   The UCT-V service starts automatically.

3. Use the command below to perform pre-check, adapter setup, adapter restore, and configuration functionalities.

   ```
   uctv-wizard
   ```

   Refer to the table below to know more about **uctv-wizard** command usage options and functionalities:

Options	Use Command	Description
pre-check	uctv-wizard pre-check	Checks the network adapter properties and firewall requirements. It notifies the user if the network adapter's send buffer size is smaller than the required size for the Windows UCT-V and if any firewall rules need to be added. **NOTE:** We recommend to Increase the send buffer size of network adapters to 128 MB during the UCT-V installation to optimize performance and minimize traffic disruption.
adapter-setup	uctv-wizard adapter-setup	Checks the compatible network adapters, increases the send buffer size and restarts the service. Before changing the buffer size, the existing configuration is saved as a backup. You can choose between the following: • If you wish to skip the prompts for changing the buffer size of compatible network adapters, enter the option as **y**. • Enter **N** if you wish to set it up manually. For details, refer to Install Linux UCT-Vs using Manual Configuration.
adapter-restore	uctv-wizard adapter-restore	Using this command, you can restore the backup copy of the network adapter buffer size configuration saved in the in the **uctv-wizard adapter-setup** step. **NOTE:** You need to manually restart the network adapters for changes to take effect immediately. You can choose between the following: • If you wish to skip the prompts for restoring the buffer size of the compatible network adapters, enter the option as **y**.

Options	Use Command	Description
		• Enter **N** if you wish to restore it manually. For details, refer to
configure	uctv-wizard configure	First, it checks for any existing configured file in the tmp directory (file named gigamon-cloud.conf in the **C:\Users\<username>\AppData\Local** location). If available, UCT-V will use that configuration. If unavailable, UCT-V automatically adds the interface configuration in uctv.conf file, excluding the loopback (lo) interface, with all permissions enabled (source ingress, source egress, and destination). You can add the required policy for the available port if a firewall is installed. • If you wish to skip the prompts to add the required firewall policy, enter your option as **y**. The console interface adds the firewall rules automatically. • Enter **N** if you wish to configure manually.
uninstall	uctv-wizard uninstall	Automatically stops the UCT-V service, removes the firewall rules, and uninstalls the UCT-V.

Notes:

- The log messages generated from uctv-wizard are stored at **/C:\ProgramData\uctv\uctv-installation.txt**
- Use the command below to know the usage descriptions for the individual operations.

```
uctv-wizard help
```

Windows UCT-V Installation Scenarios

1. **Zero Touch Installation**: When using a cloud integrated script to deploy UCT-V in a virtual machine, zero interference is required as the script installs and configures everything automatically.
2. **One Touch Installation**: When using a .msi package with all prerequisite packages in place, UCT-V determines that all dependencies are met. It performs auto-configuration and restarts the service.

Install Windows UCT-Vs using Manual Configuration

1. Download the Windows UCT-V**6.14.00** MSI package from the Gigamon Customer Portal. For assistance, contact Gigamon Technical Support.
2. Install the downloaded MSI package as **Administrator**. The UCT-V service starts automatically.

3. Modify the file **C:\ProgramData\Uct-v\uctv.conf** to configure and register the source and destination interfaces.

   NOTE: When you have an active, successful monitoring session deployed, any changes to the UCT-V config file made after the initial setup require a UCT-V restart and an inventory refresh or sync from GigaVUE-FM to pick up the new changes and re-initiate the traffic mirroring. GigaVUE-FM does a periodic sync on its own every 15 minutes.

   Following are the rules to modify the UCT-V configuration file:
   - Interface is selected by matching its CIDR address with config entries.
   - For the VMs with single interface *(.conf file modification is optional)*:
     - if neither mirror-src permissions is granted to the interface, both mirror-src-ingress and mirror-src-egress are granted to it.
     - mirror-dst is always granted implicitly to the interface.
   - For the VMs with multiple interfaces:
     - mirror-dst is granted explicitly in the config file. Only the first matched interface is selected for mirror-dst, all other matched interfaces are ignored.
     - if none interfaces is granted any mirror-src permission, all interfaces are granted mirror-src-ingress and mirror-src-egress.

   Example 1—Configuration example to monitor ingress and egress traffic at interface 192.168.1.0/24 and use the same interface to send out the mirrored packets.

   For IPv4:

   ```
   192.168.1.0/24  mirror-src-ingress mirror-src-egress mirror-dst
   ```

   For IPv6:

   ```
   2001:db8:abcd:ef01::/64 mirror-src-ingress mirror-src-egress mirror-dst
   ```

   Example 2—Configuration example to monitor ingress and egress traffic at interface 192.168.1.0/24 and use the interface 192.168.2.0/24 to send out the mirrored packets.

   For IPv4:

   ```
   192.168.1.0/24   mirror-src-ingress mirror-src-egress
   192.168.2.0/24   mirror-dst
   ```

   For IPv6:

   ```
   2001:db8:abcd:ef01::/64 mirror-src-ingress mirror-src-egress
    2001:db8:abcd:ef01::2/64 mirror-dst
   ```

4. Save the file.

5. Restart the Windows UCT-V using one of the following actions:
   - From the command prompt, run **sc stop uctv** and **sc start uctv**.
   - From the Windows Task Manager, restart the UCT-V.

You can verify the status of the UCT-V in the Service tab of the Windows Task Manager.

Register Windows UCT-V

It is mandatory to create a cloud configuration file and add the token to authenticate the UCT-V package with GigaVUE-FM. The token is required only for initial registration before generating the certificate. You can use the token only once and do not need to maintain.

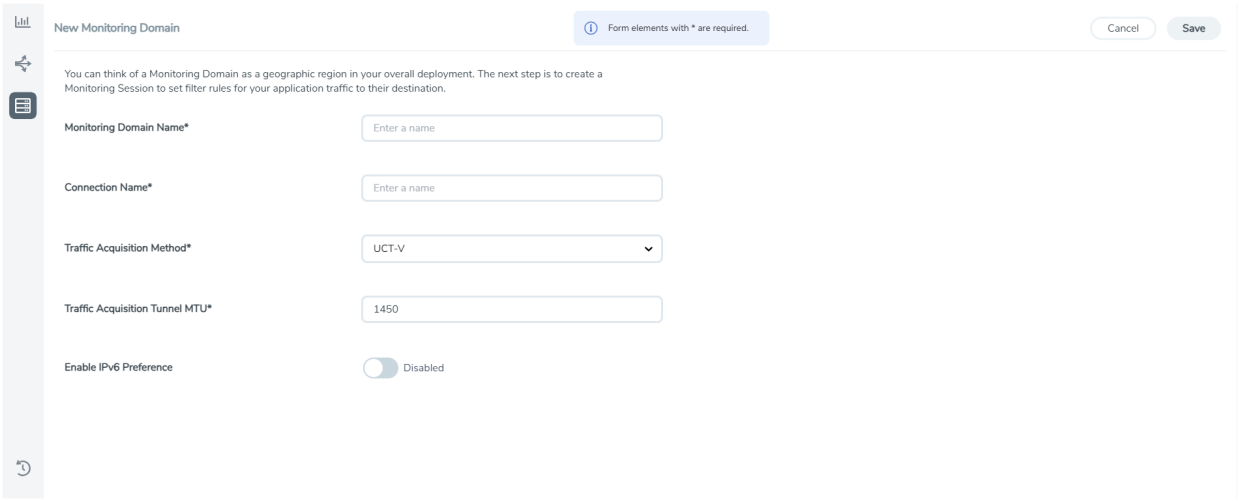
You can register UCT-V in your virtual machine using:

- **Third Party Orchestration**: The third-party orchestration feature allows you to deploy UCT-V using your own orchestration system. UCT-V uses the information of user to register with GigaVUE-FM.
  UCT-V can register with GigaVUE-FM using Third Party Orchestration in one of the following two modes:
  a. Generic Mode - Deploy GigaVUE Fabric Components using Generic Mode section in GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration
  b. Integrated Mode - Deploy GigaVUE Fabric Components using Integrated Mode section in GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration

NOTE: If you have already configured gigamon-cloud.conf file in the directory (C:\Users\<username>\AppData\Local), you can directly use the **uctv-wizard configure** command (sudo uctv-wizard configure). This action automatically fetches the configuration file and complete the registration process.

Create a Monitoring Domain

1. Go to **Inventory > VIRTUAL > Third Party Orchestration**, and then click **Monitoring Domain**. The **Monitoring Domain** page appears.
2. In the Monitoring Domain page, select **New**. The **Monitoring Domain Configuration** page appears.



3. Select or enter appropriate information as described in the following table:

Field	Description
Monitoring Domain	An alias used to identify the monitoring domain. A monitoring domain consists of set of connections.
Connection Alias	An alias used to identify the connection.
Traffic Acquisition Method	Select a tapping method. The available options are: • **UCT-V**: UCT-Vs are deployed on your VMs to acquire the traffic and forward the acquired traffic to the GigaVUE V Series nodes. If you select UCT-V as the tapping method, you must configure the UCT-V Controller to communicate to the UCT-Vs from GigaVUE-FM. The default MTU value is 1450.
Uniform Traffic Policy (When Traffic Acquisition Method is Customer Orchestrated Source)	Enable this option if you wish to use the same monitoring session configuration for the GigaVUE V Series Node deployed under this monitoring domain. Enable this check box when using packet mirroring configuration for GCP. **NOTE:** Once the monitoring session is deployed for the monitoring domain you cannot enable or disable this option.
Traffic Acquisition Tunnel MTU (When Traffic Acquisition Method is UCT-V)	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry from the UCT-V to the GigaVUE V Series Node. The MTU values for the respective platforms when using IPv4 tunnels: AWS - 8950 Azure - 1450 OpenStack - 1450 Nutanix - 1250 GCP - 1410 When using IPv4 tunnels, the MTU must be 50 bytes less than the native MTU of the respective platform. The MTU values for the respective platforms when using IPv6 tunnels: AWS - 8930 Azure - 1430 OpenStack - 1430 Nutanix - 1230 GCP - 1390 When using IPv6 tunnels, the MTU must be 70 bytes less than the native MTU of the respective platform.
Enable IPv6 Preference	Enable this option to create IPv6 tunnels between UCT-V and the GigaVUE V Series Nodes.

4. Click **Save**.

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 perform the following actions in the Monitoring domain page:

Actions	Description
Edit Monitoring Domain	Use to edit a monitoring domain.
Delete Monitoring Domain	Use to delete a Monitoring Domain.
Edit SSL Configuration	Use to add Certificate Authority and the SSL Keys when using the Secure Tunnels.
Generate Sysdump	You can select one or multiple GigaVUE V Series Nodes (Maximum 10) to generate the system files. The generation of sysdump takes a few minutes in a GigaVUE V Series Node. You can proceed with other tasks, and upon completion, the status appears in the GUI. These system files are helpful for troubleshooting. For more information, refer to Debuggability and Troubleshooting.
Manage Certificates	You can use this button to perform the following actions: • **Re-issue**- Certificates can be reissued to address security compromises, key changes, or configuration updates, like validity period adjustments. • **Renew**- Renewing a certificate just extends its expiration date and usually happens automatically unless you decide to do it during scheduled downtime. Auto-renewal is performed based on the duration specified in the **Certificate Settings** page. Refer to Configure Certificate Settings for more details.
Download Cloud Configuration File	Use this option to download the cloud configuration file (for example, md_gigamon-cloud.conf). The file contains monitoring domain connection details such as groupName, subGroupName, and token, and can be used to register fabric components in GigaVUE-FM using third party orchestration.

To view and manage the generated sysdump files, select the GigaVUE V SeriesNode and select the **Sysdump** tab in the lower pane.

To view the certificates associated with the fabric, select the fabric nodes and select the **Certificates** tab in the lower pane.

Configure and Deploy GigaVUE Fabric Components using AWS - Generic Mode

This section provides instructions on how to register GigaVUE fabric components using AWS EC2 or a configuration file.

Recommended Instance Type

The following table lists the recommended instance type for deploying the fabric components:

Fabric Component	Machine type
GigaVUE V Series Node	c5n.xlarge
UCT-V Controller	t2.medium

Deployment Guidelines

Points to remember before deploying the fabric components using generic mode:

- Set the correct MTU for tunnels: Use 8950 for IPv4 tunnels and 8930 for IPv6. To update the Traffic Acquisition Tunnel MTU:

  1. Select the monitoring domain.
  2. Select the **Edit Monitoring Domain** option.
  3. Enter the **Traffic Acquisition Tunnel MTU** value and select **Save**.

  > **NOTE:** Set the correct MTU before deploying the Monitoring Session. If not, you must undeploy and redeploy the session after updating the MTU.

- When deploying the fabric components using generic mode, you must use subGroupName in the registration data as the connection name.
- You can also create a Monitoring Domain under Third Party Orchestration and provide the monitoring domain name and the connection name as groupName and subGroupName in the registration data. For details, refer to Create Monitoring Domain.
- You can use only **UCT-V** or **Customer Orchestrated Source** as the traffic acquisition method when using generic mode.
- When you deploy the fabric components using Third Party Orchestration, you cannot delete the Monitoring Domain without unregistering the registered fabric components.
- GigaVUE V Series Node must have a minimum of two Networks Interfaces (NIC) attached to it, a management NIC and a data NIC. You can add both these interfaces when deploying the GigaVUE V Series Node in AWS. For details, refer to the Launch an instance using the Launch Instance Wizard topic in Amazon EC2 Documentation.
- Create tokens in the **User Management** page in GigaVUE-FM. For details, refer to Configure Tokens for Third Party Orchestration .

- When GigaVUE-FM is 6.10.00 or above and the Fabric Components are on (n-1) or (n-2) versions, you must create a **Username** and **Password** instead of using tokens in the registration data. For details, refer to the Configure Role-Based Access for Third-Party Orchestration section in the v6.9 Documentation.

In your AWS EC2, you can configure the following GigaVUE fabric components:

Configure UCT-V Controller in AWS

IMPORTANT: You must enable the basic authentication to launch the GigaVUE fabric components for version 6.9 and lower. For more instructions on the steps to enable the basic authentication, refer to Authentication Type.

You can configure more than one UCT-V Controller in a monitoring domain.

To register UCT-V Controller in AWS EC2, use any one of the following methods:

Register UCT-V Controller during Instance Launch

In your AWS EC2 portal, you can launch the UCT-V Controller AMI instance and register UCT-V Controller using user data.

Perform the following steps:

1. On the Instances page of AWS EC2, select **Launch instances**. The Launch Instance wizard appears. For details, refer to the Launch an instance using the Launch Instance Wizard topic in Amazon EC2 Documentation.

2. On the **Step 3: Configure Instance Details** tab:
   a. In the **Advanced details** section, select **V2 only** from the Metadata version drop-down list.
   b. Enter the User data as text in the following format and deploy the instance. The UCT-V Controller uses this user data to generate config file (**/etc/gigamon-cloud.conf**) used to register with GigaVUE-FM.

```
#cloud-config
 write_files:
 - path: /etc/gigamon-cloud.conf
   owner: root:root
   permissions: '0644'
   content: |
     Registration:
        groupName: <Monitoring Domain Name>
        subGroupName: <Connection Name>
        token: <Token>
        remoteAddress: <IP address of the GigaVUE-FM>
        sourceIP: <IP address of UCT-V> (Optional. Required only in multi-NIC deployments
to specify which UCT-V interface to use for communicating with the UCT-V Controller.)
        remotePort: 443
```

3. Go to **Instances > Actions > Instance Settings > Edit user data** and edit the user data.

The UCT-V Controller deployed in AWS EC2 appears on the Monitoring Domain page of GigaVUE-FM.

Register UCT-V Controller after Instance Launch

To register UCT-V Controller after launching a Virtual Machine using a configuration file, perform the following steps:

1. Log in to the UCT-V Controller.
2. Download the cloud configuration file (for example, md_gigamon-cloud.conf) using the Download Cloud Configuration File option in the Monitoring Domain Actions tab, and use the details for registering UCT-V Controller.

```
Registration:
    groupName: <Monitoring Domain Name>
    subGroupName: <Connection Name>
    token: <Token>
    remoteAddress: <IP address of the GigaVUE-FM>
    sourceIP: <IP address of UCT-V Controller> (Optional. Required only in multi-NIC
deployments to specify which UCT-V Controller interface to use for communicating with GigaVUE-
FM.)
    remotePort: 443
```

3. Restart theUCT-V Controller service.
   ```
   $ sudo service uctv-cntlr restart
   ```

Assign Static IP address for UCT-V Controller

By default, the UCT-V Controller gets assigned an IP address using DHCP.

To assign a static IP address, perform the following steps:

1. Navigate to **/etc/netplan/** directory.
2. Create a new **.yaml** file.

   NOTE: Do not use the default 50-cloud-init.yaml file.

3. Update the file as shown in the following sample:

```
network:
  version: 2
  renderer: NetworkManager
  ethernets:
    <interface>:                # Replace with your actual interface name (e.g., eth0)
      dhcp4: no
      dhcp6: no
      addresses:
        - <IPV4/24>             # e.g., 192.168.1.10/24
        - <IPV6/64>             # e.g., 2001:db8:abcd:0012::1/64
      nameservers:
        addresses:
          - <DNS_IPV4>          # e.g., 8.8.8.8
          - <DNS_IPV6>          # e.g., 2001:4860:4860::8888
      routes:
        - to: 0.0.0.0/0
          via: <IPV4_GW>        # e.g., 192.168.1.1
        - to: ::/0
          via: <IPV6_GW>        # e.g., 2001:db8:abcd:0012::fffe

Example netplan config:

network:
  version: 2
  renderer: NetworkManager
  ethernets:
    ens3:
      addresses:
        - 10.114.53.24/21
      dhcp4: no
      dhcp6: no
      accept-ra: false
      routes:
        - to: 10.114.48.1/32
          scope: link
        - to: default
          via: 10.114.48.1
```

4. Save the file.
5. Apply the configuration.

```
$ sudo netplan apply
```

6. Restart the UCT-V Controller service.

```
$ sudo service uctv-cntlr restart
```

The deployed UCT-V Controller registers with the GigaVUE-FM. After successful registration the UCT-V Controller sends heartbeat messages to GigaVUE-FM every 30 seconds. If one heartbeat is missing, the fabric component status appears as **Unhealthy**. If more than five heartbeats fail to reach GigaVUE-FM, GigaVUE-FM tries to reach the UCT-V Controller. If that fails as well then GigaVUE-FM unregisters the UCT-V Controller and removes from GigaVUE-FM.

Configure UCT-V in AWS

NOTE: Deployment of GigaVUE fabric components through a third-party orchestrator is supported on Linux and Windows platforms. Refer toLinux UCT-V Installation andWindows UCT-V Installation for detailed information on Linux and Windows UCT-V.

You need to register UCT-V through the registered UCT-V Controller. It communicates through PORT 8891.

NOTE: You can configure more than one UCT-V Controller for a UCT-V, so that if one UCT-V Controller goes down, the UCT-V registration will happen through another Controller that is active.

To register UCT-V using a configuration file, follow the steps:

1. Install the UCT-V in the Linux or Windows platform. For details, refer to Linux UCT-V Installation and Windows UCT-V Installation.
2. Log in to the UCT-V.

3. Create a local configuration file and enter the following user data.

   - **/etc/gigamon-cloud.conf** is the local configuration file in Linux platform.
   - **C:\ProgramData\uctv\gigamon-cloud.conf** is the local configuration file in Windows platform.
   - When creating **C:\ProgramData\uctv\gigamon-cloud.conf** file, ensure that the file name extension is **.conf**. To view the file name extension in Windows, follow the steps given below:
     a. Go to File Explorer and open the File Location.
     b. On the top navigation bar, click **View**.
     c. In the **View** tab, enable the **File name extensions** check box.

```
Registration:
    groupName: <Monitoring Domain Name>
    subGroupName: <Connection Name>
    token: <Token>
    remoteAddress: <IP address of the UCT-V Controller 1>,<IP address of the UCT-V
Controller 2>
    sourceIP: <IP address of UCT-V> (Optional. Required only in multi-NIC deployments to
specify which UCT-V interface to use for communicating with the UCT-V Controller.)
```

   NOTE: If you are using multiple interface in UCT-V and UCT-V Controller is not connected to the primary interface, then add the following to the above registration data:

   localInterface:<Interface to which UCT-V Controller is connected>

4. Restart the UCT-V service.
   - Linux platform:
     $ sudo service uctv restart
   - Windows platform: Restart from the Task Manager.

The deployed UCT-V registers with the GigaVUE-FM through the UCT-V Controller. After successful registration the UCT-V sends heartbeat messages to GigaVUE-FM every 30 seconds. If one heartbeat is missing, UCT-V status appears as 'Unhealthy'. If more than five heartbeats fail to reach GigaVUE-FM, then GigaVUE-FM tries to reach the UCT-V. If the effort fails, then GigaVUE-FM unregisters the UCT-V to remove it from GigaVUE-FM.

Configure GigaVUE V Series Nodes and V Series Proxy in AWS

NOTE: It is not mandatory to register GigaVUE V Series Nodes via V Series proxy however, if there is a large number of nodes connected to GigaVUE-FM or if you do not wish to reveal the IP addresses of the GigaVUE V Series 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 Node and GigaVUE V Series Proxy in AWS EC2, use any one of the following methods.

IMPORTANT: You must enable the basic authentication to launch the GigaVUE fabric components for version 6.9 and lower. For more instructions on the steps to enable the basic authentication, refer to Authentication Type.

Register GigaVUE V Series Node and GigaVUE V Series Proxy during Instance Launch

1. On the Instances page of AWS EC2, select **Launch instances**. The Launch Instance wizard appears. For details, refer to Launch an instance using the Launch Instance Wizard topic in Amazon EC2 Documentation.
2. On the **Step 3: Configure Instance Details** tab:
   a. In the **Advanced details** section, select **V2 only** from the Metadata version drop-down list.
   b. Enter the User data as text in the following format and deploy the instance. The GigaVUE V Series Nodes or V Series proxy uses this user data to generate config file (**/etc/gigamon-cloud.conf**) used to register with GigaVUE-FM.

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

NOTE: You can register your GigaVUE V Series Nodes directly with GigaVUE-FM or you can use V Series Proxy to register your GigaVUE V Series Nodes with GigaVUE-FM. If you wish to register GigaVUE V Series Nodes 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 Nodes using V Series proxy then, enter the `remotePort` value as 8891 and `remoteIP` as <IP address of the Proxy>.

3. You can navigate to **Instances > Actions > Instance Settings > Edit user data** and edit the user data.

Register GigaVUE V Series Node and GigaVUE V Series Proxy after Instance Launch

To register GigaVUE V Series Node and GigaVUE V Series Proxy after launching the virtual machine using a configuration file, follow the steps given below:

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

```
Registration:
    groupName: <Monitoring Domain Name>
    subGroupName: <Connection Name>
    token: <Token>
    remoteAddress: <IP address of the GigaVUE-FM> or <IP address of the proxy>
    remotePort: 443
```

> **NOTE:** You can register your GigaVUE V Series Nodes directly with GigaVUE-FM or you can use GigaVUE V Series proxy to register your GigaVUE V Series Nodes with GigaVUE-FM. If you wish to register GigaVUE V Series Nodes 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 Nodes using V Series proxy then, enter the `remotePort` value as 8891 and `remoteIP` as <IP address of the Proxy>.

3. Restart the GigaVUE V Series Node or Proxy service.
   - V Series node:
     ```
     $ sudo service vseries-node restart
     ```
   - V Series proxy:
     ```
     $ sudo service vps restart
     ```

The deployed GigaVUE V Series Proxy registers with the GigaVUE-FM. After successful registration the GigaVUE V Series Proxy sends heartbeat messages to GigaVUE-FM every 30 seconds. If one heartbeat is missing, the fabric component status appears as 'Unhealthy'. If more than five heartbeats fail to reach GigaVUE-FM, GigaVUE-FM tries to reach the GigaVUE V Series proxy and if that fails as well then GigaVUE-FM unregisters the GigaVUE V Series proxy and it will be removed from GigaVUE-FM.

> **NOTE:** When the GigaVUE V Series Node is stopped or terminated from the AWS, it does not send any unregistration request and GigaVUE-FM unregisters the GigaVUE V Series Node soon after.

Assign Static IP address for GigaVUE V Series

By default, the GigaVUE V Series gets assigned an IP address using DHCP.

To assign a static IP address, perform the following steps:

1. Navigate to **/etc/netplan/** directory.
2. Create a new **.yaml** file.

   > **NOTE:** Do not use the default 50-cloud-init.yaml file.

3. Update the file as shown in the following sample:

```
network:
  version: 2
  renderer: NetworkManager
  ethernets:
    <interface>:                # Replace with your actual interface name (e.g., eth0)
      dhcp4: no
      dhcp6: no
      addresses:
        - <IPV4/24>             # e.g., 192.168.1.10/24
        - <IPV6/64>             # e.g., 2001:db8:abcd:0012::1/64
      nameservers:
        addresses:
          - <DNS_IPV4>          # e.g., 8.8.8.8
          - <DNS_IPV6>          # e.g., 2001:4860:4860::8888
      routes:
        - to: 0.0.0.0/0
          via: <IPV4_GW>        # e.g., 192.168.1.1
        - to: ::/0
          via: <IPV6_GW>        # e.g., 2001:db8:abcd:0012::fffe

Example netplan config:

network:
  version: 2
  renderer: NetworkManager
  ethernets:
    ens3:
      addresses:
        - 10.114.53.24/21
      dhcp4: no
      dhcp6: no
      accept-ra: false
      routes:
        - to: 10.114.48.1/32
          scope: link
        - to: default
          via: 10.114.48.1
```

4. Save the file.
5. Apply the configuration.

   $ sudo netplan apply

6. Restart the GigaVUE V Series service.

   $ sudo service vseries-node restart

The deployed GigaVUE V Series registers with the GigaVUE-FM. After successful registration the GigaVUE V Series sends heartbeat messages to GigaVUE-FM every 30 seconds. If one heartbeat is missing, the fabric component status appears as **Unhealthy**. If more than five heartbeats fail to reach GigaVUE-FM, GigaVUE-FM tries to reach the GigaVUE V Series. If that fails as well then GigaVUE-FM unregisters the GigaVUE V Series and removes from GigaVUE-FM.

Configure and Deploy Monitoring Session

In GigaVUE-FM, you must do the following to configure and deploy the Monitoring Session. Refer to Configure Monitoring Session section for more details.

1. **Access the Monitoring Session Page**:
   a. In GigaVUE-FM, go to **Traffic** > **Virtual** > **Orchestrated Flows > AWS**.
   b. 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.
2. **Create an ingress REP**:
   a. In the canvas, from the **New** expand menu, drag and drop New Tunnel to the graphical workspace.
   b. On the new tunnel icon, select the ⋮ menu button and select **Details**. The **Add Tunnel Spec** quick view page appears.
   c. Enter the **Alias**, **Description**, and the **Type** details and click **Save**.
3. **Add components to the canvas**:
   a. Drag and drop the required components to the canvas.
   b. From the **Applications** expand menu, drag and drop the required applications to the graphical workspace.
4. **Deploy the Monitoring Session**:
   a. From the **Actions** menu, select **Deploy**.
   b. After successful deployment on all the V Series Nodes, the status appears as **Success** on the Monitoring Sessions **Sources** tab.

What to do Next

You can view the detailed statistics of an individual traffic processing element in the **TRAFFIC PROCESSING** tab. For more details, refer to View Monitoring Session Statistics (AWS).

Acquire Traffic using Customer Orchestrated Source - By Creating Monitoring Domain

In generic mode, you can also create a Monitoring Domain under Third Party Orchestration and provide the Monitoring Domain name and the connection name in the user data that used by your orchestrator.

This section outlines the workflow to tunnel traffic directly to GigaVUE V Series Nodes without deploying UCT-V or its controllers. using Customer Orchestrated Source. Refer to the following topics for instruction on configuring traffic acquisition, processing, and forwarding to your desired destination.

- Install GigaVUE-FM on AWS
- Configure Role-Based Access for Third Party Orchestration
- Create a Monitoring Domain
- Configure and Deploy GigaVUE Fabric Components using AWS - Generic Mode
- Configure and Deploy Monitoring Session

Install GigaVUE-FM on AWS

This step is optional and applies only when an existing GigaVUE-FM instance is not available.
Refer to Install GigaVUE-FM on AWS for steps to ìnstall GigaVUE-FM on AWS and the steps to start GigaVUE-FM instance and configure it.

Configure Role-Based Access for Third Party Orchestration

If you do not want to use an **Admin Profile** to deploy GigaVUE V Series through a Third Party orchestrator, you can create the required users, roles, and user groups in GigaVUE-FM.

Create a Custom User

You can add users only if you are a user with **fm_super_admin role** or a user with either read or write access to the GigaVUE-FM security Management category.

To add users:

1. Go to **Settings** and select **Authentication** > **GigaVUE-FM User Management > Users**.
2. On the User page, select **New User**.
3. In the Add User page, enter the following details:
   - **Name:** Actual name of the user
   - **Username**: User name configured in GigaVUE-FM
   - **Email**: Email ID of the user
   - **Password/Confirm Password**: Password for the user. For more details, refer to Change Your Password.
   - **User Group:** Select the desired User Group to associate the user.

     GigaVUE-FM prompts for your password.
4. Click **Ok**. The new user is added.

Create a Custom Role and Assign the User

A user role defines permission for users to perform any task or operation in GigaVUE-FM or on the managed device. You can associate a role with user.

NOTE: A user with read-only access cannot perform configurations on the screen. The menus and action buttons in the UI pages are disabled appropriately.

To create a role:

1. Go to **Settings** and select **Authentication> GigaVUE-FM User Management >Roles**.
2. Select **New Role**.
3. In the New Role page, select or enter the following details:
   - **Role Name**: Name of the role.
   - **Description**: Description of the role.
   - **Select Permission**: From the **Select Permissions** tab, select **Third Party Orchestration**, and provide write permissions.
4. Select **Apply** to save the configuration.

Create a Custom User Group and Assign the Custom Role and the User

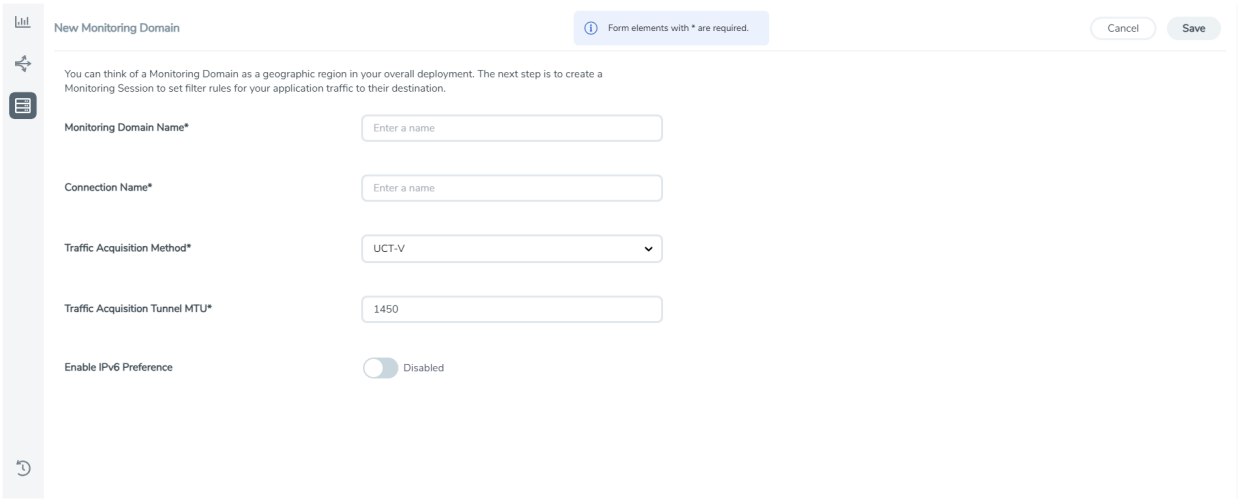
A user group consists of a set of roles and set of tags associated with users in that group. You can associate the user to one or more groups.

To create a new user group:

1. Go to **Settings**, and then select **Authentication> GigaVUE-FMUser Management >User Groups**.
2. Select **New Group.**
3. In the New User Group page, select **Next** to progress forward and **Back** to navigate backward.
4. In the **Group Info** tab, enter the Group Name and Description details:
5. In the **Assign Roles** tab, select the role that you want to assign to the user group.
6. In the **Assign Tags** tab, select the required tag key and tag value.
7. In the **Assign Users** tab, select the required users.
8. Select **Apply** to save the configuration. The new user group is added.

Create a Monitoring Domain

1. Go to **Inventory > VIRTUAL > Third Party Orchestration**, and then click **Monitoring Domain**. The **Monitoring Domain** page appears.
2. In the Monitoring Domain page, select **New**. The **Monitoring Domain Configuration** page appears.



3. Select or enter appropriate information as described in the following table:

Field	Description
Monitoring Domain	An alias used to identify the monitoring domain. A monitoring domain consists of set of connections.
Connection Alias	An alias used to identify the connection.
Traffic Acquisition Method	Select a tapping method. The available options are: • **Customer Orchestrated Source**: If you select the Customer Orchestrated Source option, the mirrored, tunneled or the raw traffic from your workloads is directed directly to the GigaVUE V Series Nodes, and you need not configure the UCT-Vs and UCT-V Controllers.
Uniform Traffic Policy (When Traffic Acquisition Method is Customer Orchestrated Source)	Enable this option if you wish to use the same monitoring session configuration for the GigaVUE V Series Node deployed under this monitoring domain. Enable this check box when using packet mirroring configuration for GCP. **NOTE:** Once the monitoring session is deployed for the monitoring domain you cannot enable or disable this option.
Traffic Acquisition Tunnel MTU (When Traffic Acquisition Method is UCT-V)	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry from the UCT-V to the GigaVUE V Series Node. The MTU values for the respective platforms when using IPv4 tunnels: AWS - 8950 Azure - 1450 OpenStack - 1450 Nutanix - 1250 GCP - 1410 When using IPv4 tunnels, the MTU must be 50 bytes less than the native MTU of the respective platform. The MTU values for the respective platforms when using IPv6 tunnels: AWS - 8930 Azure - 1430 OpenStack - 1430 Nutanix - 1230 GCP - 1390 When using IPv6 tunnels, the MTU must be 70 bytes less than the native MTU of the respective platform.
Enable IPv6 Preference	Enable this option to create IPv6 tunnels between UCT-V and the GigaVUE V Series Nodes.

4. Click **Save**.

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 perform the following actions in the Monitoring domain page:

Actions	Description
Edit Monitoring Domain	Use to edit a monitoring domain.
Delete Monitoring Domain	Use to delete a Monitoring Domain.
Edit SSL Configuration	Use to add Certificate Authority and the SSL Keys when using the Secure Tunnels.
Generate Sysdump	You can select one or multiple GigaVUE V Series Nodes (Maximum 10) to generate the system files. The generation of sysdump takes a few minutes in a GigaVUE V Series Node. You can proceed with other tasks, and upon completion, the status appears in the GUI. These system files are helpful for troubleshooting. For more information, refer to Debuggability and Troubleshooting.
Manage Certificates	You can use this button to perform the following actions: • **Re-issue**- Certificates can be reissued to address security compromises, key changes, or configuration updates, like validity period adjustments. • **Renew**- Renewing a certificate just extends its expiration date and usually happens automatically unless you decide to do it during scheduled downtime. Auto-renewal is performed based on the duration specified in the **Certificate Settings** page. Refer to Configure Certificate Settings for more details.
Download Cloud Configuration File	Use this option to download the cloud configuration file (for example, md_gigamon-cloud.conf). The file contains monitoring domain connection details such as groupName, subGroupName, and token, and can be used to register fabric components in GigaVUE-FM using third party orchestration.

To view and manage the generated sysdump files, select the GigaVUE V SeriesNode and select the **Sysdump** tab in the lower pane.

To view the certificates associated with the fabric, select the fabric nodes and select the **Certificates** tab in the lower pane.

Configure and Deploy GigaVUE Fabric Components using AWS - Generic Mode

This section provides instructions on how to register GigaVUE fabric components using AWS EC2 or a configuration file.

Recommended Instance Type

The following table lists the recommended instance type for deploying the fabric components:

Fabric Component	Machine type
GigaVUE V Series Node	c5n.xlarge
UCT-V Controller	t2.medium

Deployment Guidelines

Points to remember before deploying the fabric components using generic mode:

- Set the correct MTU for tunnels: Use 8950 for IPv4 tunnels and 8930 for IPv6. To update the Traffic Acquisition Tunnel MTU:

  1. Select the monitoring domain.
  2. Select the **Edit Monitoring Domain** option.
  3. Enter the **Traffic Acquisition Tunnel MTU** value and select **Save**.

  > **NOTE:** Set the correct MTU before deploying the Monitoring Session. If not, you must undeploy and redeploy the session after updating the MTU.

- When deploying the fabric components using generic mode, you must use subGroupName in the registration data as the connection name.
- You can also create a Monitoring Domain under Third Party Orchestration and provide the monitoring domain name and the connection name as groupName and subGroupName in the registration data. For details, refer to Create Monitoring Domain.
- You can use only **UCT-V** or **Customer Orchestrated Source** as the traffic acquisition method when using generic mode.
- When you deploy the fabric components using Third Party Orchestration, you cannot delete the Monitoring Domain without unregistering the registered fabric components.
- GigaVUE V Series Node must have a minimum of two Networks Interfaces (NIC) attached to it, a management NIC and a data NIC. You can add both these interfaces when deploying the GigaVUE V Series Node in AWS. For details, refer to the Launch an instance using the Launch Instance Wizard topic in Amazon EC2 Documentation.
- Create tokens in the **User Management** page in GigaVUE-FM. For details, refer to Configure Tokens for Third Party Orchestration .

- When GigaVUE-FM is 6.10.00 or above and the Fabric Components are on (n-1) or (n-2) versions, you must create a **Username** and **Password** instead of using tokens in the registration data. For details, refer to the Configure Role-Based Access for Third-Party Orchestration section in the v6.9 Documentation.

In your AWS EC2, you can configure the following GigaVUE fabric components:

Configure UCT-V Controller in AWS

IMPORTANT: You must enable the basic authentication to launch the GigaVUE fabric components for version 6.9 and lower. For more instructions on the steps to enable the basic authentication, refer to Authentication Type.

You can configure more than one UCT-V Controller in a monitoring domain.

To register UCT-V Controller in AWS EC2, use any one of the following methods:

Register UCT-V Controller during Instance Launch

In your AWS EC2 portal, you can launch the UCT-V Controller AMI instance and register UCT-V Controller using user data.

Perform the following steps:

1. On the Instances page of AWS EC2, select **Launch instances**. The Launch Instance wizard appears. For details, refer to the Launch an instance using the Launch Instance Wizard topic in Amazon EC2 Documentation.

2. On the **Step 3: Configure Instance Details** tab:
   a. In the **Advanced details** section, select **V2 only** from the Metadata version drop-down list.
   b. Enter the User data as text in the following format and deploy the instance. The UCT-V Controller uses this user data to generate config file (**/etc/gigamon-cloud.conf**) used to register with GigaVUE-FM.

```
#cloud-config
 write_files:
 - path: /etc/gigamon-cloud.conf
   owner: root:root
   permissions: '0644'
   content: |
     Registration:
        groupName: <Monitoring Domain Name>
        subGroupName: <Connection Name>
        token: <Token>
        remoteAddress: <IP address of the GigaVUE-FM>
        sourceIP: <IP address of UCT-V> (Optional. Required only in multi-NIC deployments
to specify which UCT-V interface to use for communicating with the UCT-V Controller.)
        remotePort: 443
```

3. Go to **Instances > Actions > Instance Settings > Edit user data** and edit the user data.

The UCT-V Controller deployed in AWS EC2 appears on the Monitoring Domain page of GigaVUE-FM.

Register UCT-V Controller after Instance Launch

To register UCT-V Controller after launching a Virtual Machine using a configuration file, perform the following steps:

1. Log in to the UCT-V Controller.
2. Create a local configuration file (**/etc/gigamon-cloud.conf**) and enter the following user data.

```
Registration:
    groupName: <Monitoring Domain Name>
    subGroupName: <Connection Name>
    token: <Token>
    remoteAddress: <IP address of the GigaVUE-FM>
    sourceIP: <IP address of UCT-V Controller> (Optional. Required only in multi-NIC
deployments to specify which UCT-V Controller interface to use for communicating with GigaVUE-
FM.)
    remotePort: 443
```

3. Restart theUCT-V Controller service.

```
$ sudo service uctv-cntlr restart
```

Assign Static IP address for UCT-V Controller

By default, the UCT-V Controller gets assigned an IP address using DHCP.

To assign a static IP address, perform the following steps:

1. Navigate to **/etc/netplan/** directory.
2. Create a new **.yaml** file.

   NOTE: Do not use the default 50-cloud-init.yaml file.

3. Update the file as shown in the following sample:

```
network:
  version: 2
  renderer: NetworkManager
  ethernets:
    <interface>:                # Replace with your actual interface name (e.g., eth0)
      dhcp4: no
      dhcp6: no
      addresses:
        - <IPV4/24>             # e.g., 192.168.1.10/24
        - <IPV6/64>             # e.g., 2001:db8:abcd:0012::1/64
      nameservers:
        addresses:
          - <DNS_IPV4>          # e.g., 8.8.8.8
          - <DNS_IPV6>          # e.g., 2001:4860:4860::8888
      routes:
        - to: 0.0.0.0/0
          via: <IPV4_GW>        # e.g., 192.168.1.1
        - to: ::/0
          via: <IPV6_GW>        # e.g., 2001:db8:abcd:0012::fffe

Example netplan config:

network:
  version: 2
  renderer: NetworkManager
  ethernets:
    ens3:
      addresses:
        - 10.114.53.24/21
      dhcp4: no
      dhcp6: no
      accept-ra: false
      routes:
        - to: 10.114.48.1/32
          scope: link
        - to: default
          via: 10.114.48.1
```

4. Save the file.
5. Apply the configuration.

   $ sudo netplan apply

6. Restart the UCT-V Controller service.

```
$ sudo service uctv-cntlr restart
```

The deployed UCT-V Controller registers with the GigaVUE-FM. After successful registration the UCT-V Controller sends heartbeat messages to GigaVUE-FM every 30 seconds. If one heartbeat is missing, the fabric component status appears as **Unhealthy**. If more than five heartbeats fail to reach GigaVUE-FM, GigaVUE-FM tries to reach the UCT-V Controller. If that fails as well then GigaVUE-FM unregisters the UCT-V Controller and removes from GigaVUE-FM.

Configure UCT-V in AWS

NOTE: Deployment of GigaVUE fabric components through a third-party orchestrator is supported on Linux and Windows platforms. Refer toLinux UCT-V Installation andWindows UCT-V Installation for detailed information on Linux and Windows UCT-V.

You need to register UCT-V through the registered UCT-V Controller. It communicates through PORT 8891.

NOTE: You can configure more than one UCT-V Controller for a UCT-V, so that if one UCT-V Controller goes down, the UCT-V registration will happen through another Controller that is active.

To register UCT-V using a configuration file, follow the steps:

1. Install the UCT-V in the Linux or Windows platform. For details, refer to Linux UCT-V Installation and Windows UCT-V Installation.
2. Log in to the UCT-V.

3. Create a local configuration file and enter the following user data.

   - **/etc/gigamon-cloud.conf** is the local configuration file in Linux platform.
   - **C:\ProgramData\uctv\gigamon-cloud.conf** is the local configuration file in Windows platform.
   - When creating **C:\ProgramData\uctv\gigamon-cloud.conf** file, ensure that the file name extension is **.conf**. To view the file name extension in Windows, follow the steps given below:
     a. Go to File Explorer and open the File Location.
     b. On the top navigation bar, click **View**.
     c. In the **View** tab, enable the **File name extensions** check box.

```
Registration:
    groupName: <Monitoring Domain Name>
    subGroupName: <Connection Name>
    token: <Token>
    remoteAddress: <IP address of the UCT-V Controller 1>,<IP address of the UCT-V
Controller 2>
    sourceIP: <IP address of UCT-V> (Optional. Required only in multi-NIC deployments to
specify which UCT-V interface to use for communicating with the UCT-V Controller.)
```

   NOTE: If you are using multiple interface in UCT-V and UCT-V Controller is not connected to the primary interface, then add the following to the above registration data:

   localInterface:<Interface to which UCT-V Controller is connected>

4. Restart the UCT-V service.
   - Linux platform:
     $ sudo service uctv restart
   - Windows platform: Restart from the Task Manager.

The deployed UCT-V registers with the GigaVUE-FM through the UCT-V Controller. After successful registration the UCT-V sends heartbeat messages to GigaVUE-FM every 30 seconds. If one heartbeat is missing, UCT-V status appears as 'Unhealthy'. If more than five heartbeats fail to reach GigaVUE-FM, then GigaVUE-FM tries to reach the UCT-V. If the effort fails, then GigaVUE-FM unregisters the UCT-V to remove it from GigaVUE-FM.

Configure GigaVUE V Series Nodes and V Series Proxy in AWS

NOTE: It is not mandatory to register GigaVUE V Series Nodes via V Series proxy however, if there is a large number of nodes connected to GigaVUE-FM or if you do not wish to reveal the IP addresses of the GigaVUE V Series 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 Node and GigaVUE V Series Proxy in AWS EC2, use any one of the following methods.

IMPORTANT: You must enable the basic authentication to launch the GigaVUE fabric components for version 6.9 and lower. For more instructions on the steps to enable the basic authentication, refer to Authentication Type.

Register GigaVUE V Series Node and GigaVUE V Series Proxy during Instance Launch

1. On the Instances page of AWS EC2, select **Launch instances**. The Launch Instance wizard appears. For details, refer to Launch an instance using the Launch Instance Wizard topic in Amazon EC2 Documentation.
2. On the **Step 3: Configure Instance Details** tab:
   a. In the **Advanced details** section, select **V2 only** from the Metadata version drop-down list.
   b. Enter the User data as text in the following format and deploy the instance. The GigaVUE V Series Nodes or V Series proxy uses this user data to generate config file (**/etc/gigamon-cloud.conf**) used to register with GigaVUE-FM.

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

NOTE: You can register your GigaVUE V Series Nodes directly with GigaVUE-FM or you can use V Series Proxy to register your GigaVUE V Series Nodes with GigaVUE-FM. If you wish to register GigaVUE V Series Nodes 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 Nodes using V Series proxy then, enter the `remotePort` value as 8891 and `remoteIP` as <IP address of the Proxy>.

3. You can navigate to **Instances > Actions > Instance Settings > Edit user data** and edit the user data.

Register GigaVUE V Series Node and GigaVUE V Series Proxy after Instance Launch

To register GigaVUE V Series Node and GigaVUE V Series Proxy after launching the virtual machine using a configuration file, follow the steps given below:

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

```
Registration:
    groupName: <Monitoring Domain Name>
    subGroupName: <Connection Name>
    token: <Token>
    remoteAddress: <IP address of the GigaVUE-FM> or <IP address of the proxy>
    remotePort: 443
```

> **NOTE:** You can register your GigaVUE V Series Nodes directly with GigaVUE-FM or you can use GigaVUE V Series proxy to register your GigaVUE V Series Nodes with GigaVUE-FM. If you wish to register GigaVUE V Series Nodes 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 Nodes using V Series proxy then, enter the `remotePort` value as 8891 and `remoteIP` as <IP address of the Proxy>.

3. Restart the GigaVUE V Series Node or Proxy service.
   - V Series node:
     ```
     $ sudo service vseries-node restart
     ```
   - V Series proxy:
     ```
     $ sudo service vps restart
     ```

The deployed GigaVUE V Series Proxy registers with the GigaVUE-FM. After successful registration the GigaVUE V Series Proxy sends heartbeat messages to GigaVUE-FM every 30 seconds. If one heartbeat is missing, the fabric component status appears as 'Unhealthy'. If more than five heartbeats fail to reach GigaVUE-FM, GigaVUE-FM tries to reach the GigaVUE V Series proxy and if that fails as well then GigaVUE-FM unregisters the GigaVUE V Series proxy and it will be removed from GigaVUE-FM.

> **NOTE:** When the GigaVUE V Series Node is stopped or terminated from the AWS, it does not send any unregistration request and GigaVUE-FM unregisters the GigaVUE V Series Node soon after.

Assign Static IP address for GigaVUE V Series

By default, the GigaVUE V Series gets assigned an IP address using DHCP.

To assign a static IP address, perform the following steps:

1. Navigate to **/etc/netplan/** directory.
2. Create a new **.yaml** file.

   > **NOTE:** Do not use the default 50-cloud-init.yaml file.

3. Update the file as shown in the following sample:

```
network:
  version: 2
  renderer: NetworkManager
  ethernets:
    <interface>:                # Replace with your actual interface name (e.g., eth0)
      dhcp4: no
      dhcp6: no
      addresses:
        - <IPV4/24>             # e.g., 192.168.1.10/24
        - <IPV6/64>             # e.g., 2001:db8:abcd:0012::1/64
      nameservers:
        addresses:
          - <DNS_IPV4>          # e.g., 8.8.8.8
          - <DNS_IPV6>          # e.g., 2001:4860:4860::8888
      routes:
        - to: 0.0.0.0/0
          via: <IPV4_GW>        # e.g., 192.168.1.1
        - to: ::/0
          via: <IPV6_GW>        # e.g., 2001:db8:abcd:0012::fffe

Example netplan config:

network:
  version: 2
  renderer: NetworkManager
  ethernets:
    ens3:
      addresses:
        - 10.114.53.24/21
      dhcp4: no
      dhcp6: no
      accept-ra: false
      routes:
        - to: 10.114.48.1/32
          scope: link
        - to: default
          via: 10.114.48.1
```

4. Save the file.
5. Apply the configuration.

   $ sudo netplan apply

6. Restart the GigaVUE V Series service.

   $ sudo service vseries-node restart

The deployed GigaVUE V Series registers with the GigaVUE-FM. After successful registration the GigaVUE V Series sends heartbeat messages to GigaVUE-FM every 30 seconds. If one heartbeat is missing, the fabric component status appears as **Unhealthy**. If more than five heartbeats fail to reach GigaVUE-FM, GigaVUE-FM tries to reach the GigaVUE V Series. If that fails as well then GigaVUE-FM unregisters the GigaVUE V Series and removes from GigaVUE-FM.

Configure and Deploy Monitoring Session

In GigaVUE-FM, you must do the following to configure and deploy the Monitoring Session. Refer to Configure Monitoring Session section for more details.

1. **Access the Monitoring Session Page**:
   a. In GigaVUE-FM, go to **Traffic** > **Virtual** > **Orchestrated Flows > AWS**.
   b. 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.
2. **Create an ingress REP**:
   a. In the canvas, from the **New** expand menu, drag and drop New Tunnel to the graphical workspace.
   b. On the new tunnel icon, select the ⋮ menu button and select **Details**. The **Add Tunnel Spec** quick view page appears.
   c. Enter the **Alias**, **Description**, and the **Type** details and click **Save**.
3. **Add components to the canvas**:
   a. Drag and drop the required components to the canvas.
   b. From the **Applications** expand menu, drag and drop the required applications to the graphical workspace.
4. **Deploy the Monitoring Session**:
   a. From the **Actions** menu, select **Deploy**.
   b. After successful deployment on all the V Series Nodes, the status appears as **Success** on the Monitoring Sessions **Sources** tab.

What to do Next

You can view the detailed statistics of an individual traffic processing element in the **TRAFFIC PROCESSING** tab. For more details, refer to View Monitoring Session Statistics (AWS).

Deployment Options for GigaVUE Cloud Suite for AWS - Integrated Mode

This section describes various options to configure GigaVUE Cloud Suite for AWS to provide visibility for both physical and virtual traffic. You can configure GigaVUE Cloud Suite for AWS in ten different ways, based on the traffic acquisition method and your approach to deploying fabric components.

Different deployment options for GigaVUE Cloud Suite for AWS based on the Traffic Acquisition Method

Refer to the following topics for detailed information:

- Acquire Traffic using UCT-V - GigaVUE-FM Orchestration
- Acquire Traffic using UCT-V - Third Party Orchestration
- Acquire Traffic using Traffic Mirroring – GigaVUE-FM Orchestration
- Acquire Traffic using Traffic Mirroring – Third Party Orchestration
- Acquire Traffic Using AWS Traffic Mirroring – Network Load Balancing
- Acquire Traffic using Traffic Mirroring with Gateway Load Balancing
- Acquire Traffic using Customer Orchestrated Source with Network Load Balancing
- Acquire Traffic using Customer Orchestrated Source with Gateway Load Balancing
- Acquire Traffic using Customer Orchestrated Source - GigaVUE-FM Orchestration
- Acquire Traffic using Customer Orchestrated Source - Third Party Orchestration
- Acquire Traffic using Inline V Series Solution

Prerequisite:

Before deploying GigaVUE Fabric Components in AWS, create a Monitoring Domain in GigaVUE-FM with the **Use FM to Launch Fabric** toggle button disabled.

Key Considerations:

- When you deploy the fabric components using third party orchestration, you cannot delete the Monitoring Domain without unregistering the registered fabric components.
- When using Traffic Mirroring as the traffic acquisition method, you must add a key and value when deploying the respective fabric components in the AWS orchestrator. Set the key to **GigamonNode** and any string to the value. The string cannot contain numbers and special characters.
- GigaVUE V Series Node must have a minimum of two Network Interfaces (NIC) attached to it, a management NIC, and a data NIC. You can add both interfaces when deploying the GigaVUE V Series Node in AWS. For details, refer to the Launch an instance using the Launch Instance Wizard topic in Amazon EC2 Documentation.
- When GigaVUE-FM is 6.10.00 or above and the Fabric Components are on (n-1) or (n-2) versions, you must create a **Username** and **Password** instead of using tokens in the registration data. For more details, refer to Configure Role-Based Access for Third Party Orchestration.
- You must configure a token in the **User Management** page. For details, refer to Configure Tokens.

Acquire Traffic using UCT-V - Third Party Orchestration

This section outlines the workflow for acquiring traffic with UCT-V and deploying GigaVUE Fabric Components using Third Party Orchestration. Refer to the following topics for instruction on configuring traffic acquisition, processing, and forwarding to your desired destination.

- Install GigaVUE-FM on AWS
- Configure the permissions required in AWS
- Create the AWS Credentials
- Configure Role-Based Access for Third Party Orchestration
- Configure Tokens
- Create a Monitoring Domain
- Configure GigaVUE Fabric Components using Integrated Mode
- Install UCT-Vs
- Configure and Deploy Monitoring Session

Install GigaVUE-FM on AWS

This step is optional and applies only when an existing GigaVUE-FM instance is not available.
Refer to Install GigaVUE-FM on AWS for steps to ìnstall GigaVUE-FM on AWS and the steps to start GigaVUE-FM instance and configure it.

Configure the permissions required in AWS

If you are using inline policy or basic authentication, then you must update the policy with the relevant IAM service. For details, see Minimum Permissions Required for Inline Policies and Basic Authentication.

These are the minimum permissions that are required to acquire traffic using the UCT-V and authenticate using an IAM instance role.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags",
                "ec2:DeleteTags",
                "ec2:RunInstances",
                "ec2:TerminateInstances",
                "ec2:AssociateAddress",
                "ec2:DisassociateAddress",
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
```

```
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeVolumes",
                "ec2:DescribeAddresses",
                "ec2:RebootInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedRolePolicies",
                "iam:ListAccountAliases",
                "iam:ListRolePolicies",
                "kms:ListAliases",
                "kms:GenerateDataKeyWithoutPlaintext"

            ],
            "Resource": "*"
        }
    ]
}
```

For more information regarding policies and permissions, refer to AWS Documentation.

Create the AWS Credentials

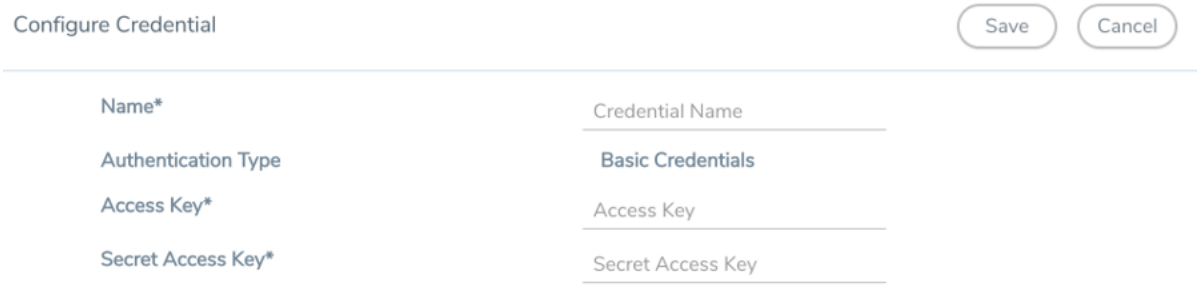
You can monitor workloads across multiple AWS accounts within one Monitoring Domain.

- After launching GigaVUE-FM in AWS, if the IAM is attached to the running instance of FM, then the **EC2 Instance Role** authentication credential is automatically added to the **Credential** page as the default credential. You must attach the IAM prior to creating a Monitoring Domain.
- If you use the **Basic Credentials** authentication credentials, you must add these to the GigaVUE-FM on the **AWS Settings** page, or on the Monitoring Domain creation page.

For details, refer to Create a Monitoring Domain.

To create AWS credentials:

1. Go to **Inventory > VIRTUAL > AWS**, and select **Settings > Credentials**
2. On the **Credential** page, select **Add**. The **Credential Configure** page appears.



3. Enter a name to identify the AWS Credential in the **Name** Field.
4. Basic Credentials is selected as the default **Authentication Type**. For more information, refer to AWS Security Credentials
5. Enter the credential of an IAM user or the AWS account root user in the **Access Key** field.
6. Enter the security password or key in the **Secret Access Key** field.
7. Select **Save**. You can view the list of available credentials on the AWS Credential page.

Configure Role-Based Access for Third Party Orchestration

If you do not want to use an **Admin Profile** to deploy GigaVUE V Series through a Third Party orchestrator, you can create the required users, roles, and user groups in GigaVUE-FM.

Create a Custom User

You can add users only if you are a user with **fm_super_admin role** or a user with either read or write access to the GigaVUE-FM security Management category.

To add users:

1. Go to **Settings** and select **Authentication** > **GigaVUE-FM User Management > Users**.
2. On the User page, select **New User**.
3. In the Add User page, enter the following details:
   - **Name:** Actual name of the user
   - **Username**: User name configured in GigaVUE-FM
   - **Email**: Email ID of the user
   - **Password/Confirm Password**: Password for the user. For more details, refer to Change Your Password.
   - **User Group:** Select the desired User Group to associate the user.

   GigaVUE-FM prompts for your password.

4. Click **Ok**. The new user is added.

Create a Custom Role and Assign the User

A user role defines permission for users to perform any task or operation in GigaVUE-FM or on the managed device. You can associate a role with user.

> **NOTE:** A user with read-only access cannot perform configurations on the screen. The menus and action buttons in the UI pages are disabled appropriately.

To create a role:

1. Go to **Settings** and select **Authentication> GigaVUE-FM User Management >Roles**.
2. Select **New Role**.
3. In the New Role page, select or enter the following details:
   - **Role Name**: Name of the role.
   - **Description**: Description of the role.
   - **Select Permission**: From the **Select Permissions** tab, select **Third Party Orchestration**, and provide write permissions.
4. Select **Apply** to save the configuration.

Create a Custom User Group and Assign the Custom Role and the User

A user group consists of a set of roles and set of tags associated with users in that group. You can associate the user to one or more groups.

To create a new user group:

1. Go to **Settings**, and then select **Authentication> GigaVUE-FMUser Management >User Groups**.
2. Select **New Group.**
3. In the New User Group page, select **Next** to progress forward and **Back** to navigate backward.
4. In the **Group Info** tab, enter the Group Name and Description details:
5. In the **Assign Roles** tab, select the role that you want to assign to the user group.
6. In the **Assign Tags** tab, select the required tag key and tag value.
7. In the **Assign Users** tab, select the required users.
8. Select **Apply** to save the configuration. The new user group is added.

Configure Tokens

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.

You can create tokens only if you are a user with fm_super_admin role or a user with write access to the GigaVUE-FM security Management category.

To create a token:

1. Go to **Settings > Authentication** > **GigaVUE-FM User Management**. The **User Management** page appears.
2. Select **Current User Tokens** from the **Tokens** drop-down list.
3. Click **New Token**. The **New Token** pop-up appears.
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 the GigaVUE-FM from the **User Group** drop-down list. The token inherits the read or write RBAC privileges of this group.
7. Select **OK** to generate a new token. You can copy and use the generated token to authenticate the GigaVUE-FM REST APIs.

Create a Monitoring Domain

GigaVUE-FM connects to the AWS Platform through the public API endpoint and uses HTTPS, the default protocol to communicate with API. For more information about the endpoint and the protocol used, refer to AWS service endpoints.

GigaVUE-FM provides you the flexibility to monitor multiple VPCs. You can choose the VPC ID and launch the GigaVUE fabric components in the desired VPCs.

NOTE: To configure the Monitoring Domain and launch the fabric components in AWS, you must have the **fm_super_admin** role or the write access to the **Infrastructure Management** category. For details, refer to Role Based Access Control.

To create a Monitoring Domain:

1. Go to **Inventory > VIRTUAL > AWS** , and select **Monitoring Domain**.
2. On the **Monitoring Domain** page, select **New**. The **Monitoring Domain Configuration** page appears.
3. Select **Check Permissions** and validate whether you have the required permissions.

4. In the **Monitoring Domain** field, enter an alias used to identify the Monitoring Domain.
5. From the **Traffic Acquisition Method** drop-down list, select one of the following tapping methods:
   - **UCT-V**: UCT-Vs are deployed on your VMs to acquire the traffic and forward the acquired traffic to the GigaVUE V Series Nodes. If you select UCT-V as the tapping method, you must configure the UCT-V Controller to communicate to the UCT-Vs from GigaVUE-FM.
     You can also configure the UCT-V Controller and UCT-Vs from your own orchestrator. For details, refer to Configure GigaVUE Fabric Components in AWS using Third Party Orchestration - Integrated Mode.
6. In the **Traffic Acquisition Tunnel MTU**, enter the MTU value. The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry from the UCT-V to the GigaVUE V Series Node. The default value is 8951.
   - When using IPv4 tunnels, the maximum MTU value is 8951. Ensure that the UCT-V tunnel MTU is 50 bytes less than the destination interface MTU size of the UCT-V.
   - When using IPv6 tunnels, the maximum MTU value is 8931. Ensure that UCT-V tunnel MTU is 70 bytes less than the destination interface MTU size of the UCT-V.
7. Disable the **Use FM to Launch Fabric** toggle, to deploy GigaVUE Fabric Components using Third Party Orchestration.
8. Turn on the **Enable IPv6 Preference** toggle to create IPv6 tunnels between UCT-V and the GigaVUE V Series Nodes.

   NOTE: This appears only when **Use FM to Launch Fabric** is disabled and **Traffic Acquisition Method** is **UCT-V**.
9. Under Connections, in the **Name** field, enter an alias used to identify the connection.
10. From the **Credential** drop-down list, select an AWS credential. For details, refer to Create AWS Credentials.
11. From the **Region** drop-down list, select AWS region for the Monitoring Domain. For example, US West.

    NOTE: China regions are not supported.
12. From the **Accounts** drop-down list, select the AWS accounts.
13. From the **VPCs** drop-down list, select the VPCs to monitor.
14. Click **Save**.

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 view the new Monitoring Domain in the **Monitoring Domain** page list view.

To edit a Monitoring Domain, select the deployed Monitoring Domain and select **Actions**. From the drop-down list, select **Edit** and the **Monitoring Domain Configuration** page appears.

For details regarding the Check permissions while creating a Monitoring Domain, refer to Manage a Monitoring Domain .

Configure GigaVUE Fabric Components using Integrated Mode

In your AWS EC2, you can configure the following GigaVUE fabric components:

- Register UCT-V Controller in AWS
- Register UCT-V Controller in AWS
- Register GigaVUE V Series Nodes and GigaVUE V Series Proxy in AWS

Register UCT-V Controller in AWS

You can deploy UCT-V Controller in AWS using any of the following methods:

- Register UCT-V Controller using User Data
- Register UCT-V Controller using a Configuration File

Register UCT-V Controller using User Data

To register UCT-V Controller using the user data in AWS GUI, enter or select the following details:

Parameters	Description	Reference	Mandatory field
Application and OS Images (Amazon Machine Image)	Select AMI of UCT-V Controller.	Launch an instance using defined parameters	Yes
Instance Type	Select an Instance Type from the drop-down list. The recommended instance type is t2.medium.		Yes

Parameters	Description	Reference	Mandatory field
Advanced Details			
Metadata Version	Select **V2 only (token required)** as the version.		Yes

User Data	The UCT-V Controller uses this user data to generate config file (**/etc/gigamon-cloud.conf**) used to register with GigaVUE-FM.
	`#cloud-config`
	`write_files:`
	`- path: /etc/gigamon-cloud.conf`
	`owner: root:root`
	`permissions: '0644'`
	`content: |`
	`Registration:`
	`groupName: <Monitoring Domain Name>`
	`subGroupName: <VPC Name>`
	`token: <Token>`
	`remoteIP: <IP address of the GigaVUE-FM>`
	`sourceIP: <IP address of UCT-V Controller>`
	`(Optional Field)`
	`remotePort: 443`		

The UCT-V Controller deployed in AWS EC2 appears on the Monitoring Domain page of GigaVUE-FM.

Register UCT-V Controller using a Configuration File

To register UCT-V Controller using a configuration file:

1. Log in to the UCT-V Controller.
2. Edit the local configuration file (**/etc/gigamon-cloud.conf**) and enter the following user data. You can also install custom certificates to UCT-V Controller, refer to the below table for details:

```
Registration:
   groupName: <Monitoring Domain Name>
   subGroupName: <VPC Name>
   token: <Token>
   remoteIP: <IP address of the GigaVUE-FM>
   sourceIP: <IP address of UCT-V Controller> (Optional Field)
   remotePort: 443
```

3. Restart the UCT-V Controller service.
   $ sudo service uctv-cntlr restart

To assign a static IP address, perform the following steps:

1. Navigate to **/etc/netplan/** directory.
2. Create a new **.yaml** file.

   NOTE: Do not use the default 50-cloud-init.yaml file.

3. Update the file as shown in the following sample:

```
network:
  version: 2
  renderer: NetworkManager
  ethernets:
    <interface>:                # Replace with your actual interface name (e.g., eth0)
      dhcp4: no
      dhcp6: no
      addresses:
        - <IPV4/24>             # e.g., 192.168.1.10/24
        - <IPV6/64>             # e.g., 2001:db8:abcd:0012::1/64
      nameservers:
        addresses:
          - <DNS_IPV4>          # e.g., 8.8.8.8
          - <DNS_IPV6>          # e.g., 2001:4860:4860::8888
      routes:
        - to: 0.0.0.0/0
          via: <IPV4_GW>        # e.g., 192.168.1.1
        - to: ::/0
          via: <IPV6_GW>        # e.g., 2001:db8:abcd:0012::fffe

Example netplan config:

network:
  version: 2
  renderer: NetworkManager
  ethernets:
    ens3:
      addresses:
        - 10.114.53.24/21
      dhcp4: no
      dhcp6: no
      accept-ra: false
      routes:
        - to: 10.114.48.1/32
          scope: link
        - to: default
          via: 10.114.48.1
```

4. Save the file.
5. Apply the configuration.

   $ sudo netplan apply

Register UCT-V in AWS

You must register UCT-V through the registered UCT-V Controller. You can configure more than one UCT-V Controller for a UCT-V, so that if one UCT-V Controller goes down, the UCT-V registration takes placethrough another active Controller.

NOTE: Deployment of UCT-Vs through a third-party orchestrator is supported for both Linux and Windows platforms. Refer to UCT-V Installation and Windows UCT-V Installation. for detailed information.

To register UCT-V using a configuration file:

1. Install the UCT-V in the Linux or Windows platform. For detailed instructions, refer to Linux UCT-V Installation and Windows UCT-V Installation.
2. Log in to the UCT-V.
3. Create a local configuration file and enter the following user data.

   - **/etc/gigamon-cloud.conf** is the local configuration file in Linux platform.
   - **C:\ProgramData\uctv\gigamon-cloud.conf** is the local configuration file in Windows platform.
   - If you are using multiple interface in UCT-V and UCT-V Controller is not connected to the primary interface, then add the following to the above registration data:
     localInterface:<Interface to which UCT-V Controller is connected>

   ```
   Registration:
       groupName: <Monitoring Domain Name>
       subGroupName: <VPC Name>
       token: <Token>
       remoteIP: <IP address of the UCT-V Controller 1>,
       <IP address of the UCT-V Controller 2>
       sourceIP: <IP address of UCT-V> (Optional Field)
   ```

4. Restart the UCT-V service.
   - Linux platform:
     $ sudo service uctv restart
   - Windows platform: Restart from the Task Manager.

The deployed UCT-V registers with the GigaVUE-FM through the UCT-V Controller. After successful registration, every 30 seconds the UCT-V sends heartbeat messages to GigaVUE-FM. If one heartbeat is missing, UCT-V status appears as **Unhealthy**. If more than five heartbeats fail to reach GigaVUE-FM, then GigaVUE-FM tries to reach the UCT-V. If that also fails, then GigaVUE-FM unregisters the UCT-V and removes from GigaVUE-FM.

Register GigaVUE V Series Nodes and GigaVUE V Series Proxy in AWS

You can deploy GigaVUE V Series Nodes and GigaVUE V Series Proxy in AWS using any of the following methods:

- Register GigaVUE V Series Nodes without GigaVUE V Series Proxy using User Data
- Create a Custom User

Register GigaVUE V Series Node and GigaVUE V Series Proxy using User Data

This section provides information on how to register GigaVUE V Series and GigaVUE V Series Proxy (if used) when launching the virtual machine in AWS using user data. For details, refer to the following sections:

- Register GigaVUE V Series Nodes without GigaVUE V Series Proxy using User Data
- Register UCT-V Controller using User Data

Register GigaVUE V Series Nodes without GigaVUE V Series Proxy using User Data

To register GigaVUE V Series Node using the user data in AWS GUI, enter or select the following details:

Parameters	Instructions	Reference	Mandatory field
Application and OS Images (Amazon Machine Image)	Select AMI of the GigaVUE V Series Node.	Launch an instance using defined parameters	Yes
Instance Type	Select an Instance Type from the drop-down list. The recommended instance type is c5n.xlarge.		Yes
Advanced Details			
Metadata Version	Select **V2 only (token required)** as the version.		Yes

User Data	The GigaVUE V Series Node uses this user data to generate config file (**/etc/gigamon-cloud.conf**) used to register with GigaVUE-FM.
	`#cloud-config`
	`write_files:`
	`- path: /etc/gigamon-cloud.conf`
	`owner: root:root`
	`permissions: '0644'`
	`content: |`
	`Registration:`
	`groupName: <Monitoring Domain Name>`
	`subGroupName: <Connection Name>`
	`token: <Token>`
	`remoteIP: <IP address of the GigaVUE-FM>`
	`remotePort: 443`		

Register GigaVUE V Series Nodes with GigaVUE V Series Proxy using User Data

When deploying GigaVUE V Series Node with GigaVUE V Series Proxy, deploy the GigaVUE V Series Proxy first and then deploy the GigaVUE V Series Node.

Register GigaVUE V Series Proxy using User Data

To register GigaVUE V Series Proxy using the user data in AWS GUI, enter or select the following details:

Parameters	Description	Reference	Mandatory field
Application and OS Images (Amazon Machine Image)	Select AMI of the GigaVUE V Series Proxy.	Launch an instance using defined parameters	Yes
Instance Type	Select an Instance Type from the drop-down list.		Yes
Advanced Details			
Metadata Version	Select **V2 only (token required)** as the version.		Yes

User Data	The GigaVUE V Series Proxy uses this user data to generate config file (**/etc/gigamon-cloud.conf**) used to register with GigaVUE-FM.
	`#cloud-config`
	`write_files:`
	`- path: /etc/gigamon-cloud.conf`
	`owner: root:root`
	`permissions: '0644'`
	`content: |`
	`Registration:`
	`groupName: <Monitoring Domain Name>`
	`subGroupName: <Connection Name>`
	`token: <Token>`
	`remoteIP: <IP address of the GigaVUE-FM>`
	`remotePort: 443`
			Yes

Register GigaVUE V Series Node when using GigaVUE V Series Proxy using User Data

To register GigaVUE V Series Node via GigaVUE V Series Proxy using the user data in AWS GUI, enter or select the following details:

Parameters	Instructions	Reference	Mandatory field
Application and OS Images (Amazon Machine Image)	Select AMI of the GigaVUE V Series Node.	Launch an instance using defined parameters	Yes
Instance Type	Select an Instance Type from the drop-down list. The recommended instance type is c5n.xlarge.		Yes
Advanced Details			
Metadata Version	Select **V2 only (token required)** as the version.		Yes

User Data	The GigaVUE V Series Node uses this user data to generate config file (**/etc/gigamon-cloud.conf**) used to register with GigaVUE-FM.
	`#cloud-config`
	`write_files:`
	`- path: /etc/gigamon-cloud.conf`
	`owner: root:root`
	`permissions: '0644'`
	`content: |`
	`Registration:`
	`groupName: <Monitoring Domain Name>`
	`subGroupName: <Connection Name>`
	`token: <Token>`
	`remoteIP: <IP address of the GigaVUE V Series Proxy>`
	`remotePort: 8891`
			Yes

Register GigaVUE V Series Node and Proxy using a Configuration File

This section provides information on how to register GigaVUE V Series Node and GigaVUE V Series Proxy (if used) using a configuration file after launching the virtual machine in AWS. For details, refer to the following sections:

- Register UCT-V Controller using a Configuration File
- Register GigaVUE V Series Nodes with GigaVUE V Series Proxy using a Configuration file

Register GigaVUE V Series Nodes without GigaVUE V Series Proxy using a Configuration file

To register GigaVUE V Series Node using a configuration file,

1. Log in to the GigaVUE V Series Node.
2. Edit the local configuration file (**/etc/gigamon-cloud.conf**) and enter the following user data. You can also install custom certificates to GigaVUE V Series Node, refer to the below table for details:

```
Registration:
   groupName: <Monitoring Domain Name>
   subGroupName: <Connection Name>
   token: <Token>
   remoteIP: <IP address of the GigaVUE-FM>
   remotePort: 443
```

3. Restart the GigaVUE V Series Node service.

```
$ sudo service vseries-node restart
```

Register GigaVUE V Series Nodes with GigaVUE V Series Proxy using a Configuration file

When deploying GigaVUE V Series Node with GigaVUE V Series Proxy, deploy the GigaVUE V Series Proxy first and then deploy the GigaVUE V Series Node.

Register GigaVUE V Series Proxy using Configuration file:

1. Log in to the GigaVUE V Series Node.
2. Edit the local configuration file (**/etc/gigamon-cloud.conf**) and enter the following user data. You can also install custom certificates to GigaVUE V Series Node. For details, refer to the below table.

```
Registration:
   groupName: <Monitoring Domain Name>
   subGroupName: <Connection Name>
   token: <Token>
   remoteIP: <IP address of the GigaVUE-FM>
   remotePort: 443
```

3. Restart the GigaVUE V Series Proxy service.

```
$ sudo service vps restart
```

Register GigaVUE V Series Node when using GigaVUE V Series Proxy using Configuration File

To register GigaVUE V Series Node using a configuration file,

1. Log in to the GigaVUE V Series Node.
2. Edit the local configuration file (**/etc/gigamon-cloud.conf**) and enter the following user data. You can also install custom certificates to GigaVUE V Series Node, refer to the below table for details:

```
Registration:
   groupName: <Monitoring Domain Name>
   subGroupName: <Connection Name>
   token: <Token>
   remoteIP: <IP address of the GigaVUE V Series Proxy>
   remotePort: 8891
```

3. Restart the GigaVUE V Series Node service.

```
$ sudo service vseries-node restart
```

The deployed GigaVUE V Series node or proxy registers with GigaVUE-FM. After successful registration, every 30 seconds the GigaVUE V Series node or proxy sends heartbeat messages to GigaVUE-FM. If one heartbeat is missing ,the fabric components status appears as **Unhealth**'. If more than five heartbeats fail to reach GigaVUE-FM, then GigaVUE-FM tries to reach the GigaVUE V Series node or proxy. If that fails, then GigaVUE-FM unregisters the GigaVUE V Series node or proxy and removes from GigaVUE-FM.

Install UCT-Vs

You can install UCT-V on both Linux and Windows environments. For details, refer to the following topics:

- Linux UCT-V Installation
- Windows UCT-V Installation

Linux UCT-V Installation

You can install UCT-V on various Linux distributions using Debian or RPM packages.

You must have sudo/root access to edit the UCT-V configuration file. Establish an SSH connection to the virtual machine and ensure you have permission to execute the sudo command.

You may need to modify the network configuration files for dual or multiple network interface configurations to ensure that the extra NIC/Network interface initializes at boot time.

Refer to the following sections:

- Linux Network Firewall Requirements
- Install Linux UCT-Vs
- Register GigaVUE V Series Nodes without GigaVUE V Series Proxy using User Data

Prerequisites

- UCT-V is a standalone service. By default, most modern Linux operating systems come pre-installed with all the necessary packages for the UCT-V to function without additional configuration.
- Before registering Linux UCT-V, you should generate a token and place it in the **/etc/gigamon-cloud.conf** configuration file. Refer to Configure Tokens.

Linux Network Firewall Requirements

If Network Firewall requirements or security groups are configured in your environment, you must open the following ports for the virtual machine.

Direction	Port	Protocol	CIDR	Purpose
Inbound	9902	TCP	UCT-V Controller IP	Allows UCT-V to receive control and management plane traffic from UCT-V Controller

You can use the following commands to add the Network Firewall rule.

```
sudo firewall-cmd --add-port=9902/tcp
sudo firewall-cmd --runtime-to-permanent
```

Install Linux UCT-Vs

You can install the UCT-Vs either from Debian or RPM packages using one of the following options:.

- Install Linux UCT-Vs using Installation Script
- Install Linux UCT-Vs using Manual Configuration

Refer to the following sections for more detailed information and step-by-step instructions.

Install Linux UCT-Vs using Installation Script

Using installation script, you can complete installation.

Perform the following steps:

1. **To install UCT-V from Ubuntu/Debian:**
    a. Download the UCT-V**6.14.00** Debian (.deb) package from the Gigamon Customer Portal. For assistance, contact Gigamon Technical Support.
    b. Copy this package to your instance and Install the package with root privileges. For example,

    ```
    $ ls gigamon-gigavue-uctv-6.14.00-amd64.deb
    $ sudo dpkg -i gigamon-gigavue-uctv-6.14.00-amd64.deb
    ```

2. **To install UCT-V from RPM, Red Hat Enterprise Linux, and CentOS:**
    a. Download the UCT-V**6.14.00** RPM (.rpm) package from the Gigamon Customer Portal. For assistance, contact Gigamon Technical Support.
    b. Copy this package to your instance and install the package with root privileges. For example,

    ```
    $ ls gigamon-gigavue-uctv-6.14.00-x86_64.rpm
    $ sudo rpm -i gigamon-gigavue-uctv-6.14.00-x86_64.rpm
    ```

3. Use the command given below to perform pre-check, installation, and configuration functionalities.

```
sudo uctv-wizard
```

> **NOTE:** The installation script is not provided with the Debian or RPM packages. You can use the script (installation_wizard.sh/uctv-wizard) only after the UCT-V is installed.

Refer to the table below to know more about **uctv-wizard** command usage options and functionalities:

Options	Use Command	Description
pre-check	sudo uctv-wizard pre-check	Checks the status of the required packages and firewall requirements. • If any package is missing, it displays an appropriate message with the missing package details. • If installation includes all the packages, it displays a success message indicating that UCT-V is ready for configuration.
pkg-install	sudo uctv-wizard pkg-install **NOTE:** The uctv-wizard install command requires access to a repository, either public (internet-based) or local, that hosts prerequisite packages for installation. If no repository is accessible, you must manually install the required packages.	Displays the missing package and version details. To proceed with the installation, you can choose between the following: If you wish to skip the prompts and proceed with the system update, enter your option as **y**. The console interface installs the missing packages and restarts the UCT-V service. Enter **N** if you wish to install it manually. For details, refer to Install Linux UCT-Vs using Manual Configuration.
configure	sudo uctv-wizard configure	First, it checks for any existing configured file in the tmp directory (file named gigamon-cloud.conf in the **C:\Users\<username>\AppData\Local** (Windows) or **/etc/uctv/uctv.conf** (Linux) location). If available, UCT-V uses that configuration. If unavailable, UCT-V automatically adds the interface configuration in uctv.conf file, excluding the loopback (lo) interface, with all permissions enabled (source ingress, source egress, and destination). You can add the required policy for the available port if a firewall is installed. If you wish to skip the prompts to add the

Options	Use Command	Description
		required firewall policy, enter your option as **y**. The console interface adds the firewall rules automatically. Enter **N** if you wish to configure manually. For details, refer to Install Linux UCT-Vs using Manual Configuration section.
uninstall	sudo uctv-wizard uninstall	Automatically stops the UCT-V service, removes the firewall rules, and uninstalls the UCT-V.

Notes:

- Use the command below to view all the log messages generated from uctv-wizard. These log messages are stored at **/var/log/uctv-installation.log**

  ```
  sudo vi /var/log/uctv-installation.log
  ```

- Use the command below to know the usage descriptions for the individual operations.

  ```
  sudo uctv-wizard help
  ```

Linux UCT-V Installation Scenarios

1. **Zero Touch Installation** - When using a cloud-integrated script to deploy UCT-V in a virtual machine, no interference is required as the script installs and configures everything automatically.
2. **One Touch Installation** - When using .deb or .rpm packages with all prerequisite packages in place, UCT-V determines that all dependencies are met. It performs auto-configuration and restarts the service.
3. **Two Touch Installation** - When using .deb or .rpm packages with missing prerequisite packages, the platform displays a warning message about the missing packages. You need to install the missing packages using the **sudo uctv-wizard pkg-install** command.

Install Linux UCT-Vs using Manual Configuration

- Install UCT-V from Ubuntu/Debian Package
- Install UCT-V from RPM, Red Hat Enterprise Linux, and CentOS

Install UCT-V from Ubuntu/Debian Package

To install from a Debian package:

1. Download the UCT-V**6.14.00** Debian (.deb) package from the Gigamon Customer Portal. For assistance contact Gigamon Technical Support.
2. Copy this package to your instance.

3. Install the package with root privileges. For example,

```
$ ls gigamon-gigavue-uctv-6.14.00-amd64.deb
$ sudo dpkg -i gigamon-gigavue-uctv-6.14.00-amd64.deb
```

4. Modify the file **/etc/uctv/uctv.conf** to configure and register the source and destination interfaces.
   The following examples registers eth0 as the mirror source for both ingress and egress traffic and eth1 as the destination for this traffic:

   NOTE: When you have an active, successful monitoring session deployed, any modification to the UCT-V config file made after the initial setup requires a UCT-V restart and an inventory refresh or sync from GigaVUE-FM to pick up the new changes and re-initiate the traffic mirroring. GigaVUE-FM does a periodic sync on its own every 15 minutes.

   Example 1—Configuration example to monitor ingress and egress traffic at interface eth0 and use the same interface to send out the mirrored packets

```
# eth0   mirror-src-ingress mirror-src-egress mirror-dst
```

   Example 2—Configuration example to monitor ingress and egress traffic at interface eth0 and use the interface eth1 to send out the mirrored packets

```
# eth0   mirror-src-ingress mirror-src-egress
# eth1   mirror-dst
```

   Example 3—Configuration example to monitor ingress and egress traffic at interface eth0 and eth 1; use the interface eth1 to send out the mirrored packets

```
# eth0   mirror-src-ingress mirror-src-egress
# eth1   mirror-src-ingress mirror-src-egress mirror-dst
```

   Example 4—Configuration example to monitor ingress traffic at iface 'eth0' and egress traffic at iface 'eth1' and use iface 'eth2' to transmit the mirrored packets.

```
# eth0   mirror-src-ingress
# eth1   mirror-src-egress
# eth2 mirror-dst
```

   Example 5—Configuration example to monitor traffic at iface 'lo' that is always registered as bidirectional traffic regardless of the config and use iface 'eth0' to transmit the mirrored packets.

```
# lo mirror-src-ingress mirror-src-egress
# eth0 mirror-dst
```

   NOTE: Ensure that the configuration for a single interface is provided on a single line.

5. Save the file.

6. Restart the UCT-V service.

   ```
   $ systemctl restart uctv.service
   ```

The UCT-V status is displayed as running. Verify the status using the following command:

```
$ systemctl status uctv.service
```

Install UCT-V from RPM, Red Hat Enterprise Linux, and CentOS

To install from an RPM (.rpm) package on a RedHat, CentOS, or other RPM-based system:

1. Download the UCT-V**6.14.00** RPM (.rpm) package from the Gigamon Customer Portal.
   For assistance contact Gigamon Technical Support.
2. Copy this package to your instance.
3. Install the package with root privileges. For example,

   ```
   $ ls gigamon-gigavue-uctv-6.14.00-x86_64.rpm
   $ sudo rpm -i gigamon-gigavue-uctv-6.14.00-x86_64.rpm
   ```

4. Modify the **/etc/uctv/uctv.conf** file to configure and register the source and destination interfaces.
   The following example registers the eth0 as the mirror source for both ingress and egress traffic and registers eth1 as the destination for this traffic as follows:

   NOTE: When you have an active, successful monitoring session deployed, any changes to the UCT-V config file made after the initial setup require an UCT-V restart and an inventory refresh or sync from GigaVUE-FM to pick up the new changes and re-initiate the traffic mirroring. GigaVUE-FM does a periodic sync on its own every 15 minutes.

   Example 1—Configuration example to monitor ingress and egress traffic at interface eth0 and use the same interface to send out the mirrored packets

   ```
   # eth0   mirror-src-ingress mirror-src-egress mirror-dst
   ```

   Example 2—Configuration example to monitor ingress and egress traffic at interface eth0 and use the interface eth1 to send out the mirrored packets

   ```
   # eth0   mirror-src-ingress mirror-src-egress
   # eth1   mirror-dst
   ```

   Example 3—Configuration example to monitor ingress and egress traffic at interface eth0 and eth 1; use the interface eth1 to send out the mirrored packets

   ```
   # eth0   mirror-src-ingress mirror-src-egress
   # eth1   mirror-src-ingress mirror-src-egress mirror-dst
   ```

   Example 4—Configuration example to monitor ingress traffic at iface 'eth0' and egress traffic at iface 'eth1' and use iface 'eth2' to transmit the mirrored packets.

   ```
   # eth0   mirror-src-ingress
   # eth1   mirror-src-egress
   # eth2 mirror-dst
   ```

   Example 5—Configuration example to monitor traffic at iface 'lo' that is always registered as bidirectional traffic regardless of the config and use iface 'eth0' to transmit the mirrored packets.

   ```
   # lo mirror-src-ingress mirror-src-egress
   # eth0 mirror-dst
   ```

   NOTE: Ensure that the configuration for a single interface is provided on a single line.

5. Save the file.
6. Restart the UCT-V service.
   ```
   $ sudo service uctv restart
   ```

The UCT-V status is displayed as running. Verify the status with the following command:

```
$ sudo service uctv status
```

Notes:

- When UCT-V fails to start due to a "**start-limit-hit**" (caused by repeated restarts within 10 minutes), you should correct the underlying issue first. To clear the failure and allow UCT-V to restart, run the following command:

  ```
  sudo systemctl reset-failed uctv.service
  ```

Post Deployment Check:

After installing UCT-V, you can perform the following to verify the version of UCT-V:

1. Enter the command:

   ```
   sudo uctvl uctv-show
   ```

2. Manually execute the following command:

   ```
   export LD_LIBRARY_PATH=/usr/lib/uctv/ssl-lib64/
   ```

Register Linux UCT-V

It is mandatory to create a cloud configuration file and add the token to authenticate the UCT-V package with GigaVUE-FM. The token is required only for initial registration before generating the certificate. You can use the token only once and do not need to maintain.

You can register UCT-V in your virtual machine using:

- **Third Party Orchestration**: The third-party orchestration feature allows you to deploy UCT-V using your own orchestration system. UCT-V uses the information of the user to register with GigaVUE-FM. You can register UCT-V toGigaVUE-FM using Third Party Orchestration with the following two modes:
  a. Generic Mode - Deploy GigaVUE Fabric Components using Generic Mode section in GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration
  b. Integrated Mode - Deploy GigaVUE Fabric Components using Integrated Mode section in GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration

NOTE: If you have already configured gigamon-cloud.conf file in the /tmp directory, you can directly use the **uctv-wizard configure** command (sudo uctv-wizard configure). This action automatically fetches the configuration file and completes the registration process.

Windows UCT-V Installation

Windows UCT-V allows you to select the network interfaces by subnet/CIDR and modify the corresponding monitoring permissions in the configuration file. This options helps you get granular control over the monitored and mirrored traffic.

Refer to the following sections for the Windows UCT-V installation:

- Windows Network Firewall Requirements
- Install Linux UCT-Vs
- Register GigaVUE V Series Nodes without GigaVUE V Series Proxy using User Data

Windows Network Firewall Requirements

If your environment uses network firewall rules or security groups, you must open specific ports for the virtual machine.

Ensure to use UCT-V Wizard with the configure option to configure Windows local firewall rules. Refer to Install Linux UCT-Vs using Installation Script for more details.

Install Windows UCT-Vs

Rules and Notes:

- VXLAN is the only tunnel type supported for Windows UCT-V.
- Loopback Interface is not supported for Windows UCT-V.
- Before registering Windows UCT-V, generate a token and place it in the **C:\ProgramData\uctv\gigamon-cloud.conf** configuration file. Refer to Configure Tokens.
- Do not manually edit the UCT-V Windows service registry settings. Use the supported installation and upgrade workflows instead.

You can install the UCT-Vs with MSI package using one of the following options:

- Install Linux UCT-Vs using Installation Script
- Install Linux UCT-Vs using Manual Configuration

The Windows UCT-V MSI is a self-contained package that includes all necessary dependencies. However, during set up, it automatically installs the following components:

- **Visual C++ Redistributable 2019 (x86)**
- **Npcap (v1.81 OEM)**

> Before installing the Windows Agent, ensure that Npcap is not already present on the system. If an existing version of Npcap is present, uninstall it manually to avoid conflicts and ensure compatibility with the version bundled in the UCT-V.

Refer to the following sections for more detailed information and instructions.

Install Windows UCT-Vs using Installation Script

1. Download the Windows UCT-V **`6.14.00`** MSI package from the Gigamon Customer Portal. For assistance, contact Gigamon Technical Support.
2. Install the downloaded MSI package as **Administrator**.
   The UCT-V service starts automatically.

3. Use the command below to perform pre-check, adapter setup, adapter restore, and configuration functionalities.

   ```
   uctv-wizard
   ```

   Refer to the table below to know more about **uctv-wizard** command usage options and functionalities:

Options	Use Command	Description
pre-check	uctv-wizard pre-check	Checks the network adapter properties and firewall requirements. It notifies the user if the network adapter's send buffer size is smaller than the required size for the Windows UCT-V and if any firewall rules need to be added. **NOTE:** We recommend to Increase the send buffer size of network adapters to 128 MB during the UCT-V installation to optimize performance and minimize traffic disruption.
adapter-setup	uctv-wizard adapter-setup	Checks the compatible network adapters, increases the send buffer size and restarts the service. Before changing the buffer size, the existing configuration is saved as a backup. You can choose between the following: • If you wish to skip the prompts for changing the buffer size of compatible network adapters, enter the option as **y**. • Enter **N** if you wish to set it up manually. For details, refer to Install Linux UCT-Vs using Manual Configuration.
adapter-restore	uctv-wizard adapter-restore	Using this command, you can restore the backup copy of the network adapter buffer size configuration saved in the in the **uctv-wizard adapter-setup** step. **NOTE:** You need to manually restart the network adapters for changes to take effect immediately. You can choose between the following: • If you wish to skip the prompts for restoring the buffer size of the compatible network adapters, enter the option as **y**.

Options	Use Command	Description
		• Enter **N** if you wish to restore it manually. For details, refer to
configure	uctv-wizard configure	First, it checks for any existing configured file in the tmp directory (file named gigamon-cloud.conf in the **C:\Users\<username>\AppData\Local** location). If available, UCT-V will use that configuration. If unavailable, UCT-V automatically adds the interface configuration in uctv.conf file, excluding the loopback (lo) interface, with all permissions enabled (source ingress, source egress, and destination). You can add the required policy for the available port if a firewall is installed. • If you wish to skip the prompts to add the required firewall policy, enter your option as **y**. The console interface adds the firewall rules automatically. • Enter **N** if you wish to configure manually.
uninstall	uctv-wizard uninstall	Automatically stops the UCT-V service, removes the firewall rules, and uninstalls the UCT-V.

Notes:

- The log messages generated from uctv-wizard are stored at **/C:\ProgramData\uctv\uctv-installation.txt**
- Use the command below to know the usage descriptions for the individual operations.

```
uctv-wizard help
```

Windows UCT-V Installation Scenarios

1. **Zero Touch Installation**: When using a cloud integrated script to deploy UCT-V in a virtual machine, zero interference is required as the script installs and configures everything automatically.
2. **One Touch Installation**: When using a .msi package with all prerequisite packages in place, UCT-V determines that all dependencies are met. It performs auto-configuration and restarts the service.

Install Windows UCT-Vs using Manual Configuration

1. Download the Windows UCT-V**6.14.00** MSI package from the Gigamon Customer Portal. For assistance, contact Gigamon Technical Support.
2. Install the downloaded MSI package as **Administrator**. The UCT-V service starts automatically.

3. Modify the file **C:\ProgramData\Uct-v\uctv.conf** to configure and register the source and destination interfaces.

   NOTE: When you have an active, successful monitoring session deployed, any changes to the UCT-V config file made after the initial setup require a UCT-V restart and an inventory refresh or sync from GigaVUE-FM to pick up the new changes and re-initiate the traffic mirroring. GigaVUE-FM does a periodic sync on its own every 15 minutes.

   Following are the rules to modify the UCT-V configuration file:
   - Interface is selected by matching its CIDR address with config entries.
   - For the VMs with single interface *(.conf file modification is optional)*:
     - if neither mirror-src permissions is granted to the interface, both mirror-src-ingress and mirror-src-egress are granted to it.
     - mirror-dst is always granted implicitly to the interface.
   - For the VMs with multiple interfaces:
     - mirror-dst is granted explicitly in the config file. Only the first matched interface is selected for mirror-dst, all other matched interfaces are ignored.
     - if none interfaces is granted any mirror-src permission, all interfaces are granted mirror-src-ingress and mirror-src-egress.

   Example 1—Configuration example to monitor ingress and egress traffic at interface 192.168.1.0/24 and use the same interface to send out the mirrored packets.

   For IPv4:

   ```
   192.168.1.0/24  mirror-src-ingress mirror-src-egress mirror-dst
   ```

   For IPv6:

   ```
   2001:db8:abcd:ef01::/64 mirror-src-ingress mirror-src-egress mirror-dst
   ```

   Example 2—Configuration example to monitor ingress and egress traffic at interface 192.168.1.0/24 and use the interface 192.168.2.0/24 to send out the mirrored packets.

   For IPv4:

   ```
   192.168.1.0/24   mirror-src-ingress mirror-src-egress
   192.168.2.0/24   mirror-dst
   ```

   For IPv6:

   ```
   2001:db8:abcd:ef01::/64 mirror-src-ingress mirror-src-egress
    2001:db8:abcd:ef01::2/64 mirror-dst
   ```

4. Save the file.

5. Restart the Windows UCT-V using one of the following actions:
   - From the command prompt, run **sc stop uctv** and **sc start uctv**.
   - From the Windows Task Manager, restart the UCT-V.

You can verify the status of the UCT-V in the Service tab of the Windows Task Manager.

Register Windows UCT-V

It is mandatory to create a cloud configuration file and add the token to authenticate the UCT-V package with GigaVUE-FM. The token is required only for initial registration before generating the certificate. You can use the token only once and do not need to maintain.

You can register UCT-V in your virtual machine using:

- **Third Party Orchestration**: The third-party orchestration feature allows you to deploy UCT-V using your own orchestration system. UCT-V uses the information of user to register with GigaVUE-FM.
  UCT-V can register with GigaVUE-FM using Third Party Orchestration in one of the following two modes:
  a. Generic Mode - Deploy GigaVUE Fabric Components using Generic Mode section in GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration
  b. Integrated Mode - Deploy GigaVUE Fabric Components using Integrated Mode section in GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration

NOTE: If you have already configured gigamon-cloud.conf file in the directory (C:\Users\<username>\AppData\Local), you can directly use the **uctv-wizard configure** command (sudo uctv-wizard configure). This action automatically fetches the configuration file and complete the registration process.

Configure and Deploy Monitoring Session

In GigaVUE-FM, you must do the following to configure and deploy the Monitoring Session. Refer to Configure Monitoring Session section for more details.

1. **Access the Monitoring Session Page**:
   a. In GigaVUE-FM, go to **Traffic** > **Virtual** > **Orchestrated Flows > AWS**.
   b. 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.
2. **Add components to the canvas**:
   a. Drag and drop the required components to the canvas.

b. From the **Applications** expand menu, drag and drop the required applications to the graphical workspace.

3. **Deploy the Monitoring Session**:

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

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

What to do Next

You can view the detailed statistics of an individual traffic processing element in the **TRAFFIC PROCESSING** tab. For more details, refer to View Monitoring Session Statistics (AWS).

Uninstall UCT-V

This section describes how to uninstall Linux UCT-V and Windows UCT-V.

Uninstallation Method

- Linux:
  - Uninstall the UCT-V in Ubuntu/Debian, RPM, Red Hat Enterprise Linux, and CentOS packages
  - Use the following command: **`sudo uctv-wizard uninstall`**
- Windows
  - Uninstall the UCT-V in the MSI package.
  - Use the following command: **`CMD uctv-wizard uninstall`**

NOTE: Uninstall command automatically stops the UCT-V service, removes the firewall rules, and uninstalls the UCT-V.

Upgrade or Reinstall UCT-V

You can upgrade UCT-V in your virtual machine using the following options:

- Upgrade UCT-V through GigaVUE-FM (Recommended Method)
- Upgrade UCT-V Manually

Refer to the below sections for detailed information and instructions.

Upgrade UCT-V through GigaVUE-FM (Recommended Method)

Upgrading UCT-V manually involves a series of steps to uninstall, install, and restart the service again. This upgrade method is applicable to both GigaVUE-FM Orchestration and Third Party orchestration. For a list of supported platforms, refer to Install UCT-V.

NOTE: This method is complicated if you need to upgrade UCT-Vs for a large number of VMs. However, you can upgrade UCT-V in the workload VM without any hands-on involvement through GigaVUE-FM.

Refer to the sections below for details and instructions:

1. Upload the UCT-V Images
2. Upgrade the UCT-V

Rules and Notes:

- Upgrade is allowed only to versions 6.9.00 or later. Ensure that the UCT-V Controller version is compatible with the version to which you are upgrading.
- Do not trigger system upgrades or other upgrades at the same time as the UCT-V upgrade.
- You should have Infrastructure Management permission to upgrade the UCT-Vs.
- Currently, you can upgrade the UCT-Vs to n+2 versions and any number of patch releases through GigaVUE-FM.
- Before you proceed with the upgrade, ensure that the UCT-Vs are in a healthy state.
- Make sure that a UCT-V is performing only one active job at a time. If the selected UCT-V is part of another job, you cannot trigger the immediate job using the same UCT-V.
- You must upload a compatible image type to upgrade the UCT-V; otherwise, the UCT-V is rejected for the upgrade job.
- Upgrade through GigaVUE-FM is not applicable to OVS Modules. For OVS tapping, you should upgrade the UCT-Vs manually.

Upload the UCT-V Images

Perform the following steps to upload UCT-V image files in GigaVUE-FM:

1. Go to **Inventory > Virtual** and select your cloud platform.
   The **Monitoring Domain** page appears.
2. Select the **UCT-V Upgrade** drop-down menu and select **Images**.
3. In the **Images** page, click **Upload**. The **Upload Internal Image Files** wizard appears.

4. Select **Choose File**, upload the UCT-V files from your local, and select **Ok**.

   Notes:
   - You can download the UCT-V image files from Gigamon software portal.
   - You can upload a maximum of 15 UCT-V files at a time.
   - The supported file formats are **.deb**, **.rpm**, and **.msi**.
   - Ensure that you do not change the file names. GigaVUE-FM does not accept the image files with modified names.
   - When the upload is in process, GigaVUE-FM does not allow uploading a file with similar type and version.

5. Verify if the uploaded UCT-V images is listed in the **Images** page.

Delete the file

You can delete one or multiple images.

1. In the **Images** page, select **Filter** to find the images based on Image Name, Version, and Image Type.
2. Select the required images.
3. From the Actions drop-down menu, select **Delete** or **Delete All**.

You can only delete those image files that are not associated with any tasks created for the upgrade process.

Upgrade the UCT-V

Follow the steps below to upgrade UCT-V in GigaVUE-FM:

1. In the **UCT-V Upgrade** drop-down menu, select **Dashboard** to view the UCT-V upgrade landing page.
   In the Dashboard page, you can view the upgrade status of individual UCT-Vs and the stages of the upgrade process (Fetch, Install, Verify). The page also displays the overall progress of the upgrade.
2. Select the required UCT-Vs, and from the **Actions** drop-down menu, select **Upgrade**.
   The **UCT-V Upgrade task** page appears.
3. Enter the task name.
4. In the **Image Version** drop-down menu, select the required version you want to upgrade to from the list of available image versions. You can choose to upgrade immediately or schedule a time for the upgrade to happen.
5. Select the required option in the **Time Selection** field. If you prefer to schedule the upgrade, enter the choice of your date and time in the respective fields.
   Do not schedule the upgrade for a time in the past.

6. Select **Create**.
   The image upgrade task is now created.

   Note:
   - You cannot edit the upgrade task once it is created.
   - You can only reschedule the scheduled task but cannot edit the UCT-V selected for the particular task.
   - In the event of the errors listed below, GigaVUE-FM displays a pop-up message with the list of UCT-Vs that are not compatible for upgrade. Select **Proceed** to ignore the unsupported UCT-Vs and upgrade the compatible ones, or sekect "**Edit**" to modify your changes. The errors include:
     - Controller version is not compatible with the upgrade version.
     - Inconsistency between the uploaded image file type and the selected UCT-V.

You can view the created task details (both immediate and scheduled) in the **UCT-V Upgrade > Jobs** section.

Notes:
- For better progress monitoring, it is recommended to split the upgrade task to a limited number, such as 50 or 100 UCT-Vs.
- When you create a new upgrade task for the same UCT-V, the status of any existing UCT-V changes to 'In Progress' until the latest task is completed. Once the upgrade for the existing tasks is successfully finished, you can create another task for that same UCT-V.

You can view the different stages of the upgrade process in UCT-V Upgrade Dashboard page. Each stage is marked with if it is successful and in case of failure. If the upgrade is successful, GigaVUE-FM updates the upgrade status as **Success** for the selected UCT-V.

Notes:
- The default wait time for the **Upgrade Status** to get updated is 15 minutes.
- The default wait time for the **Image Version** to get updated is 5 minutes.
- In case of failure, you can upgrade the failed instance manually.

Upgrade UCT-V Manually

To upgrade UCT-V manually on a virtual machine, delete the existing UCT-V and install the new version of UCT-V.

NOTE: Before deleting the UCT-V, take a backup copy of the **/etc/uctv/uctv.conf** configuration file. This step avoids reconfiguring the source and destination interfaces.

1. Uninstall the existing UCT-V. Refer to the *Uninstall UCT-V* section in the respective GigaVUE Cloud Suite Deployment Guide.
2. Install the latest version of the new UCT-V. Refer to the Linux UCT-V Installation and the Windows UCT-V Installation topics in the respective GigaVUE Cloud Suite Deployment Guides.
3. Restart the UCT-V service.
   - Linux platform:
     ```
     $ sudo service uctv restart
     ```
   - Windows platform: Restart from the Task Manager.

Acquire Traffic using Traffic Mirroring – Third Party Orchestration

This section outlines the workflow for acquiring traffic with Traffic Mirroring and deploying GigaVUE Fabric Components using Third Party Orchestration. Refer to the following topics for instruction on configuring traffic acquisition, processing, and forwarding to your desired destination.

NOTE: When GigaVUE-FM and the workload VMs requiring monitoring are in different AWS accounts, you must configure a load balancer. For steps to configure, refer to Acquire Traffic using Traffic Mirroring with Network Load Balancer or Acquire Traffic using Traffic Mirroring with Gateway Load Balancing.

- Install GigaVUE-FM on AWS
- Configure the permissions required in AWS
- Create the AWS Credentials
- Configure Role-Based Access for Third Party Orchestration
- Configure Tokens
- Create a Monitoring Domain
- Configure GigaVUE Fabric Components using Integrated Mode
- Configure and Deploy Monitoring Session

Install GigaVUE-FM on AWS

This step is optional and applies only when an existing GigaVUE-FM instance is not available.
Refer to Install GigaVUE-FM on AWS for steps to install GigaVUE-FM on AWS and the steps to start GigaVUE-FM instance and configure it.

Configure the permissions required in AWS

If you are using inline policy or basic authentication, then you must update the policy with the relevant IAM service. For more information, see Minimum Permissions Required for Inline Policies and Basic Authentication.

These are the minimum permissions that are required to acquire traffic using Traffic Mirroring and authenticate using an IAM instance role.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags",
                "ec2:DeleteTags",
                "ec2:AssociateAddress",
                "ec2:DisassociateAddress",
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeVolumes",
                "ec2:DescribeAddresses",
                "ec2:RunInstances",
                "ec2:TerminateInstances",
                "ec2:RebootInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:DescribeTrafficMirrorFilters",
                "ec2:DescribeTrafficMirrorSessions",
                "ec2:DescribeTrafficMirrorTargets",
                "ec2:CreateTrafficMirrorTarget",
                "ec2:CreateTrafficMirrorSession",
                "ec2:DeleteTrafficMirrorTarget",
                "ec2:DeleteTrafficMirrorSession",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedRolePolicies",
                "iam:ListRolePolicies",
                "iam:ListAccountAliases",
                "kms:ListAliases"
            ],
            "Resource": "*"
        }
    ]
}
```

For more information regarding policies and permissions, refer to AWS Documentation.

Create the AWS Credentials

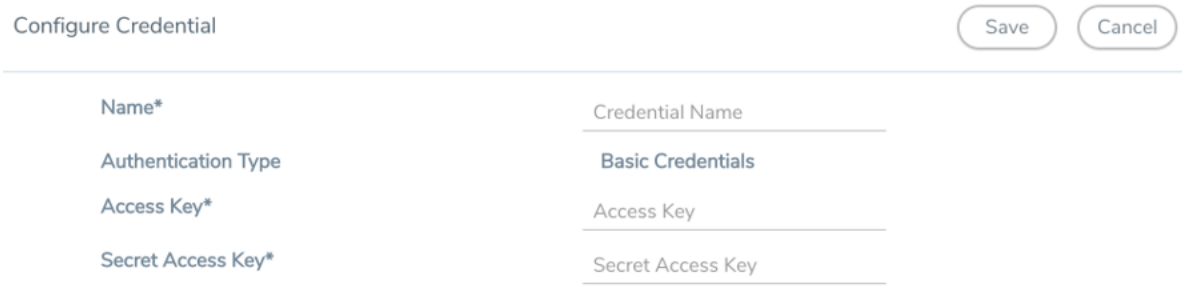
You can monitor workloads across multiple AWS accounts within one Monitoring Domain.

- After launching GigaVUE-FM in AWS, if the IAM is attached to the running instance of FM, then the **EC2 Instance Role** authentication credential is automatically added to the **Credential** page as the default credential. You must attach the IAM prior to creating a Monitoring Domain.
- If you use the **Basic Credentials** authentication credentials, you must add these to the GigaVUE-FM on the **AWS Settings** page, or on the Monitoring Domain creation page.

For details, refer to Create a Monitoring Domain.

To create AWS credentials:

1. Go to **Inventory > VIRTUAL > AWS**, and select **Settings > Credentials**
2. On the **Credential** page, select **Add**. The **Credential Configure** page appears.



3. Enter a name to identify the AWS Credential in the **Name** Field.
4. Basic Credentials is selected as the default **Authentication Type**. For more information, refer to AWS Security Credentials
5. Enter the credential of an IAM user or the AWS account root user in the **Access Key** field.
6. Enter the security password or key in the **Secret Access Key** field.
7. Select **Save**. You can view the list of available credentials on the AWS Credential page.

Configure Role-Based Access for Third Party Orchestration

If you do not want to use an **Admin Profile** to deploy GigaVUE V Series through a Third Party orchestrator, you can create the required users, roles, and user groups in GigaVUE-FM.

Create a Custom User

You can add users only if you are a user with **fm_super_admin role** or a user with either read or write access to the GigaVUE-FM security Management category.

To add users:

1. Go to **Settings** and select **Authentication** > **GigaVUE-FM User Management > Users**.
2. On the User page, select **New User**.
3. In the Add User page, enter the following details:
   - **Name:** Actual name of the user
   - **Username**: User name configured in GigaVUE-FM
   - **Email**: Email ID of the user
   - **Password/Confirm Password**: Password for the user. For more details, refer to Change Your Password.
   - **User Group:** Select the desired User Group to associate the user.

   GigaVUE-FM prompts for your password.
4. Click **Ok**. The new user is added.

Create a Custom Role and Assign the User

A user role defines permission for users to perform any task or operation in GigaVUE-FM or on the managed device. You can associate a role with user.

> **NOTE:** A user with read-only access cannot perform configurations on the screen. The menus and action buttons in the UI pages are disabled appropriately.

To create a role:

1. Go to **Settings** and select **Authentication> GigaVUE-FM User Management >Roles**.
2. Select **New Role**.
3. In the New Role page, select or enter the following details:
   - **Role Name**: Name of the role.
   - **Description**: Description of the role.
   - **Select Permission**: From the **Select Permissions** tab, select **Third Party Orchestration**, and provide write permissions.
4. Select **Apply** to save the configuration.

Create a Custom User Group and Assign the Custom Role and the User

A user group consists of a set of roles and set of tags associated with users in that group. You can associate the user to one or more groups.

To create a new user group:

1. Go to **Settings**, and then select **Authentication> GigaVUE-FMUser Management >User Groups**.
2. Select **New Group.**
3. In the New User Group page, select **Next** to progress forward and **Back** to navigate backward.
4. In the **Group Info** tab, enter the Group Name and Description details:
5. In the **Assign Roles** tab, select the role that you want to assign to the user group.
6. In the **Assign Tags** tab, select the required tag key and tag value.
7. In the **Assign Users** tab, select the required users.
8. Select **Apply** to save the configuration. The new user group is added.

Configure Tokens

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.

You can create tokens only if you are a user with fm_super_admin role or a user with write access to the GigaVUE-FM security Management category.

To create a token:

1. Go to **Settings > Authentication** > **GigaVUE-FM User Management**. The **User Management** page appears.
2. Select **Current User Tokens** from the **Tokens** drop-down list.
3. Click **New Token**. The **New Token** pop-up appears.
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 the GigaVUE-FM from the **User Group** drop-down list. The token inherits the read or write RBAC privileges of this group.
7. Select **OK** to generate a new token. You can copy and use the generated token to authenticate the GigaVUE-FM REST APIs.

Create a Monitoring Domain

GigaVUE-FM connects to the AWS Platform through the public API endpoint and uses HTTPS, the default protocol to communicate with API. For more information about the endpoint and the protocol used, refer to AWS service endpoints.

GigaVUE-FM provides you the flexibility to monitor multiple VPCs. You can choose the VPC ID and launch the GigaVUE fabric components in the desired VPCs.

NOTE: To configure the Monitoring Domain and launch the fabric components in AWS, you must have the **fm_super_admin** role or the write access to the **Infrastructure Management** category. For details, refer to Role Based Access Control.

To create a Monitoring Domain:

1. Go to **Inventory > VIRTUAL > AWS** , and select **Monitoring Domain**.
2. On the **Monitoring Domain** page, select **New**. The **Monitoring Domain Configuration** page appears.
3. Select **Check Permissions** and validate whether you have the required permissions.
4. In the **Monitoring Domain** field, enter an alias used to identify the Monitoring Domain.

5. From the **Traffic Acquisition Method** drop-down list, select one of the following tapping methods:
   - **VPC Traffic Mirroring**: If you select the Traffic Mirroring option, the mirrored traffic from your workloads is directed to the GigaVUE V Series nodes, and you need not configure the UCT-Vs and UCT-V Controllers.
     For more information on VPC Peering, refer to VPC peering connections in the AWS Documentation. Peering is required to send mirrored traffic from other VPCs into a centralized GigaVUE V Series deployment. You can choose to use an external load balancer for Traffic Mirroring. Select **Yes** to use load balancer. For details, refer to Configure AWS Elastic Load Balancing.

     NOTE:
     - UCT-V Controller configuration is not applicable for Traffic Mirroring.
     - Traffic Mirroring does not support cross-account solutions without a load balancer.
     - For VPC Traffic Mirroring option, additional permissions are required. For details, refer to the Permissions and Privileges (AWS).
     - After deploying the Monitoring Session, a traffic mirror session is created in your AWS VPC consisting of a session, a filter, sources, and targets. For more details, refer to Traffic Mirroring in AWS Documentation.
6. In the **Traffic Acquisition Tunnel MTU**, enter the MTU value. The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry from the UCT-V to the GigaVUE V Series Node. The default value is 8951.
   - When using IPv4 tunnels, the maximum MTU value is 8951. Ensure that the UCT-V tunnel MTU is 50 bytes less than the destination interface MTU size of the UCT-V.
   - When using IPv6 tunnels, the maximum MTU value is 8931. Ensure that UCT-V tunnel MTU is 70 bytes less than the destination interface MTU size of the UCT-V.
7. Disable the **Use FM to Launch Fabric** toggle, to deploy GigaVUE Fabric Components using Third Party Orchestration.
8. Turn on the **Enable IPv6 Preference** toggle to create IPv6 tunnels between UCT-V and the GigaVUE V Series Nodes.

   NOTE: This appears only when **Use FM to Launch Fabric** is disabled and **Traffic Acquisition Method** is **UCT-V**.
9. Under Connections, in the **Name** field, enter an alias used to identify the connection.
10. From the **Credential** drop-down list, select an AWS credential. For details, refer to Create AWS Credentials.

11. From the **Region** drop-down list, select AWS region for the Monitoring Domain. For example, US West.

    NOTE: China regions are not supported.

12. From the **Accounts** drop-down list, select the AWS accounts.
13. From the **VPCs** drop-down list, select the VPCs to monitor.
14. Click **Save**.

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 view the new Monitoring Domain in the **Monitoring Domain** page list view.

To edit a Monitoring Domain, select the deployed Monitoring Domain and select **Actions**. From the drop-down list, select **Edit** and the **Monitoring Domain Configuration** page appears.

For details regarding the Check permissions while creating a Monitoring Domain, refer to Manage a Monitoring Domain .

Configure GigaVUE Fabric Components using Integrated Mode

In your AWS EC2, you can configure the following GigaVUE fabric components:

- Register UCT-V Controller in AWS
- Register UCT-V Controller in AWS
- Register GigaVUE V Series Nodes and GigaVUE V Series Proxy in AWS

Register UCT-V Controller in AWS

You can deploy UCT-V Controller in AWS using any of the following methods:

- Register UCT-V Controller using User Data
- Register UCT-V Controller using a Configuration File

Register UCT-V Controller using User Data

To register UCT-V Controller using the user data in AWS GUI, enter or select the following details:

Parameters	Description	Reference	Mandatory field
Application and OS Images (Amazon Machine Image)	Select AMI of UCT-V Controller.	Launch an instance using defined parameters	Yes
Instance Type	Select an Instance Type from the drop-down list. The recommended instance type is t2.medium.		Yes
Advanced Details			
Metadata Version	Select **V2 only (token required)** as the version.		Yes

User Data	The UCT-V Controller uses this user data to generate config file (**/etc/gigamon-cloud.conf**) used to register with GigaVUE-FM.
	`#cloud-config`
	`write_files:`
	`- path: /etc/gigamon-cloud.conf`
	`owner: root:root`
	`permissions: '0644'`
	`content: |`
	`Registration:`
	`groupName: <Monitoring Domain Name>`
	`subGroupName: <VPC Name>`
	`token: <Token>`
	`remoteIP: <IP address of the GigaVUE-FM>`
	`sourceIP: <IP address of UCT-V Controller>`
	`(Optional Field)`
	`remotePort: 443`		

The UCT-V Controller deployed in AWS EC2 appears on the Monitoring Domain page of GigaVUE-FM.

Register UCT-V Controller using a Configuration File

To register UCT-V Controller using a configuration file:

1. Log in to the UCT-V Controller.
2. Edit the local configuration file (**/etc/gigamon-cloud.conf**) and enter the following user data. You can also install custom certificates to UCT-V Controller, refer to the below table for details:

```
Registration:
   groupName: <Monitoring Domain Name>
   subGroupName: <VPC Name>
   token: <Token>
   remoteIP: <IP address of the GigaVUE-FM>
   sourceIP: <IP address of UCT-V Controller> (Optional Field)
   remotePort: 443
```

3. Restart the UCT-V Controller service.
   $ sudo service uctv-cntlr restart

To assign a static IP address, perform the following steps:

1. Navigate to **/etc/netplan/** directory.
2. Create a new **.yaml** file.

   NOTE: Do not use the default 50-cloud-init.yaml file.

3. Update the file as shown in the following sample:

```
network:
  version: 2
  renderer: NetworkManager
  ethernets:
    <interface>:                # Replace with your actual interface name (e.g., eth0)
      dhcp4: no
      dhcp6: no
      addresses:
        - <IPV4/24>             # e.g., 192.168.1.10/24
        - <IPV6/64>             # e.g., 2001:db8:abcd:0012::1/64
      nameservers:
        addresses:
          - <DNS_IPV4>          # e.g., 8.8.8.8
          - <DNS_IPV6>          # e.g., 2001:4860:4860::8888
      routes:
        - to: 0.0.0.0/0
          via: <IPV4_GW>        # e.g., 192.168.1.1
        - to: ::/0
          via: <IPV6_GW>        # e.g., 2001:db8:abcd:0012::fffe

Example netplan config:

network:
  version: 2
  renderer: NetworkManager
  ethernets:
    ens3:
```

```
      addresses:
        - 10.114.53.24/21
      dhcp4: no
      dhcp6: no
      accept-ra: false
      routes:
        - to: 10.114.48.1/32
          scope: link
        - to: default
          via: 10.114.48.1
```

4. Save the file.
5. Apply the configuration.

   ```
   $ sudo netplan apply
   ```

Register UCT-V in AWS

You must register UCT-V through the registered UCT-V Controller. You can configure more than one UCT-V Controller for a UCT-V, so that if one UCT-V Controller goes down, the UCT-V registration takes placethrough another active Controller.

NOTE: Deployment of UCT-Vs through a third-party orchestrator is supported for both Linux and Windows platforms. Refer to UCT-V Installation and Windows UCT-V Installation. for detailed information.

To register UCT-V using a configuration file:

1. Install the UCT-V in the Linux or Windows platform. For detailed instructions, refer to Linux UCT-V Installation and Windows UCT-V Installation.
2. Log in to the UCT-V.

3. Create a local configuration file and enter the following user data.

   - **/etc/gigamon-cloud.conf** is the local configuration file in Linux platform.
   - **C:\ProgramData\uctv\gigamon-cloud.conf** is the local configuration file in Windows platform.
   - If you are using multiple interface in UCT-V and UCT-V Controller is not connected to the primary interface, then add the following to the above registration data:
     localInterface:<Interface to which UCT-V Controller is connected>

   ```
   Registration:
       groupName: <Monitoring Domain Name>
       subGroupName: <VPC Name>
       token: <Token>
       remoteIP: <IP address of the UCT-V Controller 1>,
       <IP address of the UCT-V Controller 2>
       sourceIP: <IP address of UCT-V> (Optional Field)
   ```

4. Restart the UCT-V service.
   - Linux platform:
     $ sudo service uctv restart
   - Windows platform: Restart from the Task Manager.

The deployed UCT-V registers with the GigaVUE-FM through the UCT-V Controller. After successful registration, every 30 seconds the UCT-V sends heartbeat messages to GigaVUE-FM. If one heartbeat is missing, UCT-V status appears as **Unhealthy**. If more than five heartbeats fail to reach GigaVUE-FM, then GigaVUE-FM tries to reach the UCT-V. If that also fails, then GigaVUE-FM unregisters the UCT-V and removes from GigaVUE-FM.

Register GigaVUE V Series Nodes and GigaVUE V Series Proxy in AWS

You can deploy GigaVUE V Series Nodes and GigaVUE V Series Proxy in AWS using any of the following methods:

- Register GigaVUE V Series Nodes without GigaVUE V Series Proxy using User Data
- Create a Custom User

Register GigaVUE V Series Node and GigaVUE V Series Proxy using User Data

This section provides information on how to register GigaVUE V Series and GigaVUE V Series Proxy (if used) when launching the virtual machine in AWS using user data. For details, refer to the following sections:

- Register GigaVUE V Series Nodes without GigaVUE V Series Proxy using User Data
- Register UCT-V Controller using User Data

Register GigaVUE V Series Nodes without GigaVUE V Series Proxy using User Data

To register GigaVUE V Series Node using the user data in AWS GUI, enter or select the following details:

Parameters	Instructions	Reference	Mandatory field
Application and OS Images (Amazon Machine Image)	Select AMI of the GigaVUE V Series Node.	Launch an instance using defined parameters	Yes
Instance Type	Select an Instance Type from the drop-down list. The recommended instance type is c5n.xlarge.		Yes
Advanced Details			
Metadata Version	Select **V2 only (token required)** as the version.		Yes

User Data	The GigaVUE V Series Node uses this user data to generate config file (**/etc/gigamon-cloud.conf**) used to register with GigaVUE-FM.
	`#cloud-config`
	`write_files:`
	`- path: /etc/gigamon-cloud.conf`
	`owner: root:root`
	`permissions: '0644'`
	`content: |`
	`Registration:`
	`groupName: <Monitoring Domain Name>`
	`subGroupName: <Connection Name>`
	`token: <Token>`
	`remoteIP: <IP address of the GigaVUE-FM>`
	`remotePort: 443`		

Register GigaVUE V Series Nodes with GigaVUE V Series Proxy using User Data

When deploying GigaVUE V Series Node with GigaVUE V Series Proxy, deploy the GigaVUE V Series Proxy first and then deploy the GigaVUE V Series Node.

Register GigaVUE V Series Proxy using User Data

To register GigaVUE V Series Proxy using the user data in AWS GUI, enter or select the following details:

Parameters	Description	Reference	Mandatory field
Application and OS Images (Amazon Machine Image)	Select AMI of the GigaVUE V Series Proxy.	Launch an instance using defined parameters	Yes
Instance Type	Select an Instance Type from the drop-down list.		Yes
Advanced Details			
Metadata Version	Select **V2 only (token required)** as the version.		Yes

User Data	The GigaVUE V Series Proxy uses this user data to generate config file (**/etc/gigamon-cloud.conf**) used to register with GigaVUE-FM.
	`#cloud-config`
	`write_files:`
	`- path: /etc/gigamon-cloud.conf`
	`owner: root:root`
	`permissions: '0644'`
	`content: |`
	`Registration:`
	`groupName: <Monitoring Domain Name>`
	`subGroupName: <Connection Name>`
	`token: <Token>`
	`remoteIP: <IP address of the GigaVUE-FM>`
	`remotePort: 443`
			Yes

Register GigaVUE V Series Node when using GigaVUE V Series Proxy using User Data

To register GigaVUE V Series Node via GigaVUE V Series Proxy using the user data in AWS GUI, enter or select the following details:

Parameters	Instructions	Reference	Mandatory field
Application and OS Images (Amazon Machine Image)	Select AMI of the GigaVUE V Series Node.	Launch an instance using defined parameters	Yes
Instance Type	Select an Instance Type from the drop-down list. The recommended instance type is c5n.xlarge.		Yes

Parameters	Instructions	Reference	Mandatory field
Advanced Details			
Metadata Version	Select **V2 only (token required)** as the version.		Yes

User Data	The GigaVUE V Series Node uses this user data to generate config file (**/etc/gigamon-cloud.conf**) used to register with GigaVUE-FM.
	`#cloud-config`
	`write_files:`
	`- path: /etc/gigamon-cloud.conf`
	`owner: root:root`
	`permissions: '0644'`
	`content: |`
	`Registration:`
	`groupName: <Monitoring Domain Name>`
	`subGroupName: <Connection Name>`
	`token: <Token>`
	`remoteIP: <IP address of the GigaVUE V Series Proxy>`
	`remotePort: 8891`
			Yes

Register GigaVUE V Series Node and Proxy using a Configuration File

This section provides information on how to register GigaVUE V Series Node and GigaVUE V Series Proxy (if used) using a configuration file after launching the virtual machine in AWS. For details, refer to the following sections:

- Register UCT-V Controller using a Configuration File
- Register GigaVUE V Series Nodes with GigaVUE V Series Proxy using a Configuration file

Register GigaVUE V Series Nodes without GigaVUE V Series Proxy using a Configuration file

To register GigaVUE V Series Node using a configuration file,

1. Log in to the GigaVUE V Series Node.
2. Edit the local configuration file (**/etc/gigamon-cloud.conf**) and enter the following user data. You can also install custom certificates to GigaVUE V Series Node, refer to the below table for details:

```
Registration:
   groupName: <Monitoring Domain Name>
   subGroupName: <Connection Name>
   token: <Token>
   remoteIP: <IP address of the GigaVUE-FM>
   remotePort: 443
```

3. Restart the GigaVUE V Series Node service.

```
$ sudo service vseries-node restart
```

Register GigaVUE V Series Nodes with GigaVUE V Series Proxy using a Configuration file

When deploying GigaVUE V Series Node with GigaVUE V Series Proxy, deploy the GigaVUE V Series Proxy first and then deploy the GigaVUE V Series Node.

Register GigaVUE V Series Proxy using Configuration file:

1. Log in to the GigaVUE V Series Node.
2. Edit the local configuration file (**/etc/gigamon-cloud.conf**) and enter the following user data. You can also install custom certificates to GigaVUE V Series Node. For details, refer to the below table.

```
Registration:
   groupName: <Monitoring Domain Name>
   subGroupName: <Connection Name>
   token: <Token>
   remoteIP: <IP address of the GigaVUE-FM>
   remotePort: 443
```

3. Restart the GigaVUE V Series Proxy service.

```
$ sudo service vps restart
```

Register GigaVUE V Series Node when using GigaVUE V Series Proxy using Configuration File

To register GigaVUE V Series Node using a configuration file,

1. Log in to the GigaVUE V Series Node.
2. Edit the local configuration file (**/etc/gigamon-cloud.conf**) and enter the following user data. You can also install custom certificates to GigaVUE V Series Node, refer to the below table for details:

```
Registration:
   groupName: <Monitoring Domain Name>
   subGroupName: <Connection Name>
   token: <Token>
   remoteIP: <IP address of the GigaVUE V Series Proxy>
   remotePort: 8891
```

3. Restart the GigaVUE V Series Node service.

```
$ sudo service vseries-node restart
```

The deployed GigaVUE V Series node or proxy registers with GigaVUE-FM. After successful registration, every 30 seconds the GigaVUE V Series node or proxy sends heartbeat messages to GigaVUE-FM. If one heartbeat is missing ,the fabric components status appears as **Unhealth**'. If more than five heartbeats fail to reach GigaVUE-FM, then GigaVUE-FM tries to reach the GigaVUE V Series node or proxy. If that fails, then GigaVUE-FM unregisters the GigaVUE V Series node or proxy and removes from GigaVUE-FM.

Configure and Deploy Monitoring Session

In GigaVUE-FM, you must do the following to configure and deploy the Monitoring Session. Refer to Configure Monitoring Session section for more details.

1. **Access the Monitoring Session Page**:
   a. In GigaVUE-FM, go to **Traffic** > **Virtual** > **Orchestrated Flows > AWS**.
   b. 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.
2. **Add components to the canvas**:
   a. Drag and drop the required components to the canvas.
   b. From the **Applications** expand menu, drag and drop the required applications to the graphical workspace.
3. **Deploy the Monitoring Session**:
   a. From the **Actions** menu, select **Deploy**.
   b. After successful deployment on all the V Series Nodes, the status appears as **Success** on the Monitoring Sessions **Sources** tab.

What to do Next

You can view the detailed statistics of an individual traffic processing element in the **TRAFFIC PROCESSING** tab. For more details, refer to View Monitoring Session Statistics (AWS).

Acquire Traffic using Customer Orchestrated Source - Third Party Orchestration

This section outlines the workflow for acquiring traffic with Customer Orchestrated Source and deploying GigaVUE Fabric Components using Third Party Orchestration. Refer to the following topics for instructions on configuring traffic acquisition, processing, and forwarding to your desired destination.

- Install GigaVUE-FM on AWS
- Configure the permissions required in AWS
- Create the AWS Credentials
- Configure Role-Based Access for Third Party Orchestration
- Configure Tokens
- Create a Monitoring Domain
- Configure GigaVUE Fabric Components using Integrated Mode
- Configure and Deploy Monitoring Session

Install GigaVUE-FM on AWS

This step is optional and applies only when an existing GigaVUE-FM instance is not available.
Refer to Install GigaVUE-FM on AWS for steps to install GigaVUE-FM on AWS and the steps to start GigaVUE-FM instance and configure it.

Configure the permissions required in AWS

If you are using inline policy or basic authentication, then you must update the policy with the relevant IAM service. For details, see Minimum Permissions Required for Inline Policies and Basic Authentication.

These are the minimum permissions that are required to acquire traffic using the UCT-V and authenticate using an IAM instance role.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
```

```
                "ec2:CreateTags",
                "ec2:DeleteTags",
                "ec2:RunInstances",
                "ec2:TerminateInstances",
                "ec2:AssociateAddress",
                "ec2:DisassociateAddress",
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeVolumes",
                "ec2:DescribeAddresses",
                "ec2:RebootInstances",
                "ec2:StartInstances",
                "ec2:StopInstances",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedRolePolicies",
                "iam:ListAccountAliases",
                "iam:ListRolePolicies",
                "kms:ListAliases",
                "kms:GenerateDataKeyWithoutPlaintext"

            ],
            "Resource": "*"
        }
    ]
}
```

For more information regarding policies and permissions, refer to AWS Documentation.

Create the AWS Credentials

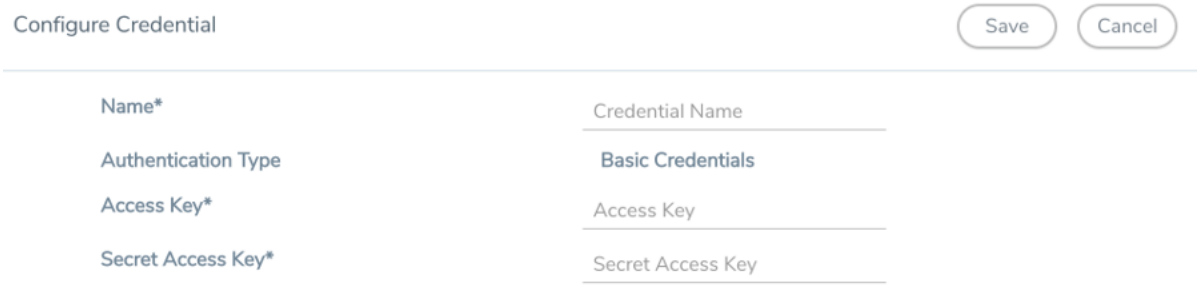
You can monitor workloads across multiple AWS accounts within one Monitoring Domain.

- After launching GigaVUE-FM in AWS, if the IAM is attached to the running instance of FM, then the **EC2 Instance Role** authentication credential is automatically added to the **Credential** page as the default credential. You must attach the IAM prior to creating a Monitoring Domain.
- If you use the **Basic Credentials** authentication credentials, you must add these to the GigaVUE-FM on the **AWS Settings** page, or on the Monitoring Domain creation page.

For details, refer to Create a Monitoring Domain.

To create AWS credentials:

1. Go to **Inventory > VIRTUAL > AWS**, and select **Settings > Credentials**
2. On the **Credential** page, select **Add**. The **Credential Configure** page appears.



3. Enter a name to identify the AWS Credential in the **Name** Field.
4. Basic Credentials is selected as the default **Authentication Type**. For more information, refer to AWS Security Credentials
5. Enter the credential of an IAM user or the AWS account root user in the **Access Key** field.
6. Enter the security password or key in the **Secret Access Key** field.
7. Select **Save**. You can view the list of available credentials on the AWS Credential page.

Configure Role-Based Access for Third Party Orchestration

If you do not want to use an **Admin Profile** to deploy GigaVUE V Series through a Third Party orchestrator, you can create the required users, roles, and user groups in GigaVUE-FM.

Create a Custom User

You can add users only if you are a user with **fm_super_admin role** or a user with either read or write access to the GigaVUE-FM security Management category.

To add users:

1. Go to **Settings** and select **Authentication** > **GigaVUE-FM User Management > Users**.
2. On the User page, select **New User**.
3. In the Add User page, enter the following details:
   - **Name:** Actual name of the user
   - **Username**: User name configured in GigaVUE-FM
   - **Email**: Email ID of the user
   - **Password/Confirm Password**: Password for the user. For more details, refer to Change Your Password.
   - **User Group:** Select the desired User Group to associate the user.

   GigaVUE-FM prompts for your password.

4. Click **Ok**. The new user is added.

Create a Custom Role and Assign the User

A user role defines permission for users to perform any task or operation in GigaVUE-FM or on the managed device. You can associate a role with user.

> **NOTE:** A user with read-only access cannot perform configurations on the screen. The menus and action buttons in the UI pages are disabled appropriately.

To create a role:

1. Go to **Settings** and select **Authentication> GigaVUE-FM User Management >Roles**.
2. Select **New Role**.
3. In the New Role page, select or enter the following details:
   - **Role Name**: Name of the role.
   - **Description**: Description of the role.
   - **Select Permission**: From the **Select Permissions** tab, select **Third Party Orchestration**, and provide write permissions.
4. Select **Apply** to save the configuration.

Create a Custom User Group and Assign the Custom Role and the User

A user group consists of a set of roles and set of tags associated with users in that group. You can associate the user to one or more groups.

To create a new user group:

1. Go to **Settings**, and then select **Authentication> GigaVUE-FMUser Management >User Groups**.
2. Select **New Group.**
3. In the New User Group page, select **Next** to progress forward and **Back** to navigate backward.
4. In the **Group Info** tab, enter the Group Name and Description details:
5. In the **Assign Roles** tab, select the role that you want to assign to the user group.
6. In the **Assign Tags** tab, select the required tag key and tag value.
7. In the **Assign Users** tab, select the required users.
8. Select **Apply** to save the configuration. The new user group is added.

Configure Tokens

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.

You can create tokens only if you are a user with fm_super_admin role or a user with write access to the GigaVUE-FM security Management category.

To create a token:

1. Go to **Settings > Authentication** > **GigaVUE-FM User Management**. The **User Management** page appears.
2. Select **Current User Tokens** from the **Tokens** drop-down list.
3. Click **New Token**. The **New Token** pop-up appears.
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 the GigaVUE-FM from the **User Group** drop-down list. The token inherits the read or write RBAC privileges of this group.
7. Select **OK** to generate a new token. You can copy and use the generated token to authenticate the GigaVUE-FM REST APIs.

Create a Monitoring Domain

GigaVUE-FM connects to the AWS Platform through the public API endpoint and uses HTTPS, the default protocol to communicate with API. For more information about the endpoint and the protocol used, refer to AWS service endpoints.

GigaVUE-FM provides you the flexibility to monitor multiple VPCs. You can choose the VPC ID and launch the GigaVUE fabric components in the desired VPCs.

NOTE: To configure the Monitoring Domain and launch the fabric components in AWS, you must have the **fm_super_admin** role or the write access to the **Infrastructure Management** category. For details, refer to Role Based Access Control.

To create a Monitoring Domain:

1. Go to **Inventory > VIRTUAL > AWS** , and select **Monitoring Domain**.
2. On the **Monitoring Domain** page, select **New**. The **Monitoring Domain Configuration** page appears.
3. Select **Check Permissions** and validate whether you have the required permissions.

4. In the **Monitoring Domain** field, enter an alias used to identify the Monitoring Domain.
5. From the **Traffic Acquisition Method** drop-down list, select one of the following tapping methods:
   - **Customer Orchestrated Source**: If you select **Customer Orchestrated Source** as the tapping method, you can use the Customer Orchestrated Source as a source option in the Monitoring Session, where the traffic is directly tunneled to the GigaVUE V Series nodes without deploying UCT-Vs and UCT-V Controllers. The user is responsible for creating this tunnel feed and pointing it to the GigaVUE V Series Node(s).

     NOTE: When using Application Metadata Exporter (AMX) application, select the **Traffic Acquisition Method** as **Customer Orchestrated Source**.
6. In the **Traffic Acquisition Tunnel MTU**, enter the MTU value. The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry from the UCT-V to the GigaVUE V Series Node. The default value is 8951.
   - When using IPv4 tunnels, the maximum MTU value is 8951. Ensure that the UCT-V tunnel MTU is 50 bytes less than the destination interface MTU size of the UCT-V.
   - When using IPv6 tunnels, the maximum MTU value is 8931. Ensure that UCT-V tunnel MTU is 70 bytes less than the destination interface MTU size of the UCT-V.
7. Disable the **Use FM to Launch Fabric** toggle, to deploy GigaVUE Fabric Components using Third Party Orchestration.
8. Turn on the **Enable IPv6 Preference** toggle to create IPv6 tunnels between UCT-V and the GigaVUE V Series Nodes.

   NOTE: This appears only when **Use FM to Launch Fabric** is disabled and **Traffic Acquisition Method** is **UCT-V**.
9. Under Connections, in the **Name** field, enter an alias used to identify the connection.
10. From the **Credential** drop-down list, select an AWS credential. For details, refer to Create AWS Credentials.
11. From the **Region** drop-down list, select AWS region for the Monitoring Domain. For example, US West.

    NOTE: China regions are not supported.
12. From the **Accounts** drop-down list, select the AWS accounts.
13. From the **VPCs** drop-down list, select the VPCs to monitor.
14. Click **Save**.

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 view the new Monitoring Domain in the **Monitoring Domain** page list view.

To edit a Monitoring Domain, select the deployed Monitoring Domain and select **Actions**. From the drop-down list, select **Edit** and the **Monitoring Domain Configuration** page appears.

For details regarding the Check permissions while creating a Monitoring Domain, refer to Manage a Monitoring Domain .

Configure GigaVUE Fabric Components using Integrated Mode

In your AWS EC2, you can configure the following GigaVUE fabric components:

- Register UCT-V Controller in AWS
- Register UCT-V Controller in AWS
- Register GigaVUE V Series Nodes and GigaVUE V Series Proxy in AWS

Register UCT-V Controller in AWS

You can deploy UCT-V Controller in AWS using any of the following methods:

- Register UCT-V Controller using User Data
- Register UCT-V Controller using a Configuration File

Register UCT-V Controller using User Data

To register UCT-V Controller using the user data in AWS GUI, enter or select the following details:

Parameters	Description	Reference	Mandatory field
Application and OS Images (Amazon Machine Image)	Select AMI of UCT-V Controller.	Launch an instance using defined parameters	Yes
Instance Type	Select an Instance Type from the drop-down list. The recommended instance type is t2.medium.		Yes

Parameters	Description	Reference	Mandatory field
Advanced Details			
Metadata Version	Select **V2 only (token required)** as the version.		Yes

User Data	The UCT-V Controller uses this user data to generate config file (**/etc/gigamon-cloud.conf**) used to register with GigaVUE-FM.
	`#cloud-config`
	`write_files:`
	`- path: /etc/gigamon-cloud.conf`
	`owner: root:root`
	`permissions: '0644'`
	`content: |`
	`Registration:`
	`groupName: <Monitoring Domain Name>`
	`subGroupName: <VPC Name>`
	`token: <Token>`
	`remoteIP: <IP address of the GigaVUE-FM>`
	`sourceIP: <IP address of UCT-V Controller>`
	`(Optional Field)`
	`remotePort: 443`		

The UCT-V Controller deployed in AWS EC2 appears on the Monitoring Domain page of GigaVUE-FM.

Register UCT-V Controller using a Configuration File

To register UCT-V Controller using a configuration file:

1. Log in to the UCT-V Controller.
2. Edit the local configuration file (**/etc/gigamon-cloud.conf**) and enter the following user data. You can also install custom certificates to UCT-V Controller, refer to the below table for details:

```
Registration:
   groupName: <Monitoring Domain Name>
   subGroupName: <VPC Name>
   token: <Token>
   remoteIP: <IP address of the GigaVUE-FM>
   sourceIP: <IP address of UCT-V Controller> (Optional Field)
   remotePort: 443
```

3. Restart the UCT-V Controller service.
   $ sudo service uctv-cntlr restart

To assign a static IP address, perform the following steps:

1. Navigate to **/etc/netplan/** directory.
2. Create a new **.yaml** file.

   NOTE: Do not use the default 50-cloud-init.yaml file.

3. Update the file as shown in the following sample:

```
network:
  version: 2
  renderer: NetworkManager
  ethernets:
    <interface>:                # Replace with your actual interface name (e.g., eth0)
      dhcp4: no
      dhcp6: no
      addresses:
        - <IPV4/24>             # e.g., 192.168.1.10/24
        - <IPV6/64>             # e.g., 2001:db8:abcd:0012::1/64
      nameservers:
        addresses:
          - <DNS_IPV4>          # e.g., 8.8.8.8
          - <DNS_IPV6>          # e.g., 2001:4860:4860::8888
      routes:
        - to: 0.0.0.0/0
          via: <IPV4_GW>        # e.g., 192.168.1.1
        - to: ::/0
          via: <IPV6_GW>        # e.g., 2001:db8:abcd:0012::fffe

Example netplan config:

network:
  version: 2
  renderer: NetworkManager
  ethernets:
    ens3:
      addresses:
        - 10.114.53.24/21
      dhcp4: no
      dhcp6: no
      accept-ra: false
      routes:
        - to: 10.114.48.1/32
          scope: link
        - to: default
          via: 10.114.48.1
```

4. Save the file.
5. Apply the configuration.

   $ sudo netplan apply

Register UCT-V in AWS

You must register UCT-V through the registered UCT-V Controller. You can configure more than one UCT-V Controller for a UCT-V, so that if one UCT-V Controller goes down, the UCT-V registration takes placethrough another active Controller.

NOTE: Deployment of UCT-Vs through a third-party orchestrator is supported for both Linux and Windows platforms. Refer to UCT-V Installation and Windows UCT-V Installation. for detailed information.

To register UCT-V using a configuration file:

1. Install the UCT-V in the Linux or Windows platform. For detailed instructions, refer to Linux UCT-V Installation and Windows UCT-V Installation.
2. Log in to the UCT-V.
3. Create a local configuration file and enter the following user data.

   - **/etc/gigamon-cloud.conf** is the local configuration file in Linux platform.
   - **C:\ProgramData\uctv\gigamon-cloud.conf** is the local configuration file in Windows platform.
   - If you are using multiple interface in UCT-V and UCT-V Controller is not connected to the primary interface, then add the following to the above registration data:
     localInterface:<Interface to which UCT-V Controller is connected>

   ```
   Registration:
       groupName: <Monitoring Domain Name>
       subGroupName: <VPC Name>
       token: <Token>
       remoteIP: <IP address of the UCT-V Controller 1>,
       <IP address of the UCT-V Controller 2>
       sourceIP: <IP address of UCT-V> (Optional Field)
   ```

4. Restart the UCT-V service.
   - Linux platform:
     $ sudo service uctv restart
   - Windows platform: Restart from the Task Manager.

The deployed UCT-V registers with the GigaVUE-FM through the UCT-V Controller. After successful registration, every 30 seconds the UCT-V sends heartbeat messages to GigaVUE-FM. If one heartbeat is missing, UCT-V status appears as **Unhealthy**. If more than five heartbeats fail to reach GigaVUE-FM, then GigaVUE-FM tries to reach the UCT-V. If that also fails, then GigaVUE-FM unregisters the UCT-V and removes from GigaVUE-FM.

Register GigaVUE V Series Nodes and GigaVUE V Series Proxy in AWS

You can deploy GigaVUE V Series Nodes and GigaVUE V Series Proxy in AWS using any of the following methods:

- Register GigaVUE V Series Nodes without GigaVUE V Series Proxy using User Data
- Create a Custom User

Register GigaVUE V Series Node and GigaVUE V Series Proxy using User Data

This section provides information on how to register GigaVUE V Series and GigaVUE V Series Proxy (if used) when launching the virtual machine in AWS using user data. For details, refer to the following sections:

- Register GigaVUE V Series Nodes without GigaVUE V Series Proxy using User Data
- Register UCT-V Controller using User Data

Register GigaVUE V Series Nodes without GigaVUE V Series Proxy using User Data

To register GigaVUE V Series Node using the user data in AWS GUI, enter or select the following details:

Parameters	Instructions	Reference	Mandatory field
Application and OS Images (Amazon Machine Image)	Select AMI of the GigaVUE V Series Node.	Launch an instance using defined parameters	Yes
Instance Type	Select an Instance Type from the drop-down list. The recommended instance type is c5n.xlarge.		Yes
Advanced Details			
Metadata Version	Select **V2 only (token required)** as the version.		Yes

User Data	The GigaVUE V Series Node uses this user data to generate config file (**/etc/gigamon-cloud.conf**) used to register with GigaVUE-FM.
	`#cloud-config`
	`write_files:`
	`- path: /etc/gigamon-cloud.conf`
	`owner: root:root`
	`permissions: '0644'`
	`content: |`
	`Registration:`
	`groupName: <Monitoring Domain Name>`
	`subGroupName: <Connection Name>`
	`token: <Token>`
	`remoteIP: <IP address of the GigaVUE-FM>`
	`remotePort: 443`		

Register GigaVUE V Series Nodes with GigaVUE V Series Proxy using User Data

When deploying GigaVUE V Series Node with GigaVUE V Series Proxy, deploy the GigaVUE V Series Proxy first and then deploy the GigaVUE V Series Node.

Register GigaVUE V Series Proxy using User Data

To register GigaVUE V Series Proxy using the user data in AWS GUI, enter or select the following details:

Parameters	Description	Reference	Mandatory field
Application and OS Images (Amazon Machine Image)	Select AMI of the GigaVUE V Series Proxy.	Launch an instance using defined parameters	Yes
Instance Type	Select an Instance Type from the drop-down list.		Yes
Advanced Details			
Metadata Version	Select **V2 only (token required)** as the version.		Yes

User Data	The GigaVUE V Series Proxy uses this user data to generate config file (**/etc/gigamon-cloud.conf**) used to register with GigaVUE-FM.
	`#cloud-config`
	`write_files:`
	`- path: /etc/gigamon-cloud.conf`
	`owner: root:root`
	`permissions: '0644'`
	`content: |`
	`Registration:`
	`groupName: <Monitoring Domain Name>`
	`subGroupName: <Connection Name>`
	`token: <Token>`
	`remoteIP: <IP address of the GigaVUE-FM>`
	`remotePort: 443`
			Yes

Register GigaVUE V Series Node when using GigaVUE V Series Proxy using User Data

To register GigaVUE V Series Node via GigaVUE V Series Proxy using the user data in AWS GUI, enter or select the following details:

Parameters	Instructions	Reference	Mandatory field
Application and OS Images (Amazon Machine Image)	Select AMI of the GigaVUE V Series Node.	Launch an instance using defined parameters	Yes
Instance Type	Select an Instance Type from the drop-down list. The recommended instance type is c5n.xlarge.		Yes
Advanced Details			
Metadata Version	Select **V2 only (token required)** as the version.		Yes

User Data	The GigaVUE V Series Node uses this user data to generate config file (**/etc/gigamon-cloud.conf**) used to register with GigaVUE-FM.
	`#cloud-config`
	`write_files:`
	`- path: /etc/gigamon-cloud.conf`
	`owner: root:root`
	`permissions: '0644'`
	`content: |`
	`Registration:`
	`groupName: <Monitoring Domain Name>`
	`subGroupName: <Connection Name>`
	`token: <Token>`
	`remoteIP: <IP address of the GigaVUE V Series Proxy>`
	`remotePort: 8891`
			Yes

Register GigaVUE V Series Node and Proxy using a Configuration File

This section provides information on how to register GigaVUE V Series Node and GigaVUE V Series Proxy (if used) using a configuration file after launching the virtual machine in AWS. For details, refer to the following sections:

- Register UCT-V Controller using a Configuration File
- Register GigaVUE V Series Nodes with GigaVUE V Series Proxy using a Configuration file

Register GigaVUE V Series Nodes without GigaVUE V Series Proxy using a Configuration file

To register GigaVUE V Series Node using a configuration file,

1. Log in to the GigaVUE V Series Node.
2. Edit the local configuration file (**/etc/gigamon-cloud.conf**) and enter the following user data. You can also install custom certificates to GigaVUE V Series Node, refer to the below table for details:

```
Registration:
   groupName: <Monitoring Domain Name>
   subGroupName: <Connection Name>
   token: <Token>
   remoteIP: <IP address of the GigaVUE-FM>
   remotePort: 443
```

3. Restart the GigaVUE V Series Node service.

```
$ sudo service vseries-node restart
```

Register GigaVUE V Series Nodes with GigaVUE V Series Proxy using a Configuration file

When deploying GigaVUE V Series Node with GigaVUE V Series Proxy, deploy the GigaVUE V Series Proxy first and then deploy the GigaVUE V Series Node.

Register GigaVUE V Series Proxy using Configuration file:

1. Log in to the GigaVUE V Series Node.
2. Edit the local configuration file (**/etc/gigamon-cloud.conf**) and enter the following user data. You can also install custom certificates to GigaVUE V Series Node. For details, refer to the below table.

```
Registration:
   groupName: <Monitoring Domain Name>
   subGroupName: <Connection Name>
   token: <Token>
   remoteIP: <IP address of the GigaVUE-FM>
   remotePort: 443
```

3. Restart the GigaVUE V Series Proxy service.

```
$ sudo service vps restart
```

Register GigaVUE V Series Node when using GigaVUE V Series Proxy using Configuration File

To register GigaVUE V Series Node using a configuration file,

1. Log in to the GigaVUE V Series Node.
2. Edit the local configuration file (**/etc/gigamon-cloud.conf**) and enter the following user data. You can also install custom certificates to GigaVUE V Series Node, refer to the below table for details:

```
Registration:
   groupName: <Monitoring Domain Name>
   subGroupName: <Connection Name>
   token: <Token>
   remoteIP: <IP address of the GigaVUE V Series Proxy>
   remotePort: 8891
```

3. Restart the GigaVUE V Series Node service.

```
$ sudo service vseries-node restart
```

The deployed GigaVUE V Series node or proxy registers with GigaVUE-FM. After successful registration, every 30 seconds the GigaVUE V Series node or proxy sends heartbeat messages to GigaVUE-FM. If one heartbeat is missing ,the fabric components status appears as **Unhealth**'. If more than five heartbeats fail to reach GigaVUE-FM, then GigaVUE-FM tries to reach the GigaVUE V Series node or proxy. If that fails, then GigaVUE-FM unregisters the GigaVUE V Series node or proxy and removes from GigaVUE-FM.

Configure and Deploy Monitoring Session

In GigaVUE-FM, you must do the following to configure and deploy the Monitoring Session. Refer to Configure Monitoring Session section for more details.

1. **Access the Monitoring Session Page**:
   a. In GigaVUE-FM, go to **Traffic** > **Virtual** > **Orchestrated Flows > AWS**.
   b. 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.
2. **Create an ingress REP**:
   a. In the canvas, from the **New** expand menu, drag and drop New Tunnel to the graphical workspace.
   b. On the new tunnel icon, select the ⋮ menu button and select **Details**. The **Add Tunnel Spec** quick view page appears.
   c. Enter the **Alias**, **Description**, and the **Type** details and click **Save**.
3. **Add components to the canvas**:
   a. Drag and drop the required components to the canvas.
   b. From the **Applications** expand menu, drag and drop the required applications to the graphical workspace.

4. **Deploy the Monitoring Session**:
    a. From the **Actions** menu, select **Deploy**.
    b. After successful deployment on all the V Series Nodes, the status appears as **Success** on the Monitoring Sessions **Sources** tab.

What to do Next

You can view the detailed statistics of an individual traffic processing element in the **TRAFFIC PROCESSING** tab. For more details, refer to View Monitoring Session Statistics (AWS).

Deploy GigaVUE Cloud Suite for VMware ESXi using Terraform

Terraform automates the deployment and management of supported GigaVUE Cloud Suite configurations. It uses reusable configuration files to define the required infrastructure. This approach enables consistent deployment, updates, and maintenance without manual work in the GigaVUE-FM UI.

Terraform applies these configurations to keep the system in the desired state. It updates only the parts that change, which helps reduce errors and maintain consistency across environments. Version-controlled files make it easier to track and manage configuration changes.

Terraform supports repeatable deployments and helps integrate GigaVUE Cloud Suite into automated workflows.

License

The GigaVUE-FM Terraform Collection does not require any additional licensing. However, you must procure a valid GigaVUE-FM license and the corresponding feature licenses to enable the GigaVUE-FM features required for your deployment.

For detailed information on license types, acquisition, and usage, refer to the Gigamon Licensing Guide.

Supportability

Use the Terraform version 1.14 or later for the GigaVUE-FM deployment. If multiple provider builds are available, select the build validated for the target deployment.

Platform support depends on the deployment model and traffic acquisition method.

Supported Deployment Models

GigaVUE-FM Orchestration

- VMware ESXi-Traffic acquisition using Platform Mirroring.

Third-Party Orchestration (Generic Mode)

Supported platforms

- AWS
- Azure
- Google Cloud Platform (GCP)
- Nutanix
- OpenStack
- VMware ESXi
- NSX-T Federation
- Oracle Cloud Infrastructure (OCI)

Supported traffic acquisition methods

- UCT-V
- Customer-Orchestrated Source

Supported GigaSMART Applications

The Gigamon Terraform provider supports the following GigaSMART applications:

- AMX
- Dedup
- Header Stripping
- Load Balancing
- Masking
- Slicing

Rules and notes

- Install a supported version of Terraform.
- Ensure GigaVUE-FM is installed and reachable from the system running Terraform.

- Always review `terraform plan` output before running `terraform apply` or `terraform destroy`.

Prerequisites

Before starting a Terraform deployment, ensure the following:

- Install a supported version of Terraform (1.14 or later).
- Ensure GigaVUE-FM is installed and reachable from the system running Terraform. GigaVUE-FM token authentication is required for the Terraform provider to connect to GigaVUE-FM. For details on generating a token, refer to Configure Tokens.
- Refer the sample configurations from the Terraform Registry.
- Prepare the required deployment values, including connection details, authentication credentials, and environment-specific inputs.

Get Started

Install Terraform

Install Terraform 1.14 or later on the system from which you will run the deployment.

Terraform runs the provider and the deployment profile that you create for GigaVUE Cloud Suite. If Terraform is not installed, or if the installed version is not supported, the deployment can fail during initialization or when Terraform reads the deployment files.

- Download and install Terraform version 1.14 or later on the deployment system:
  - Install Terraform on Windows
  - Install Terraform on Linux
- Open a terminal or command prompt on the deployment system.
- To verify the installation, run the following command:

```
terraform version
```

Confirm that the command runs successfully and that the displayed version is 1.14 or later.

If the command returns an error such as **command not found,** verify that Terraform is installed correctly

The deployment system is ready to initialize the provider and run the Terraform workflow.

Create a working directory

1. Create a folder on the deployment system where you will store the Terraform files and run the Terraform commands.
2. This folder is the working directory. Terraform reads all .tf files in the working directory together as one configuration.
3. Use one working directory for each deployment profile so that the provider settings, resource definitions, variables, values, and outputs for that deployment stay together.
4. Use the published Gigamon Terraform documentation as the primary reference when you create the deployment profile.
5. The provider documentation tells you:

- which resources are available
- which arguments each resource requires
- which values each argument accepts
- how each resource is used in Terraform

Refer to: Gigamon Terraform provider documentation

Deployment Using Terraform

This section describes the supported Terraform-based deployment paths for GigaVUE Cloud Suite.

Third-Party Orchestration

- Acquire traffic using UCT-V
- Acquire traffic using Customer-Orchestrated Source

Deploy Third Party Orchestration by using Terraform

Third Party Orchestration (3PO) deployments (Terraform-based) use Generic Mode. In this mode of deployment, the third-party orchestrator is responsible for deploying and managing the GigaVUE V Series nodes and the underlying infrastructure. Terraform communicates with GigaVUE-FM only to create and manage the monitoring configuration. i.e the monitoring domain, the connection, and the monitoring session objects.

Supported platforms (Generic Mode):

- AWS

- Azure
- Google Cloud Platform (GCP)
- Nutanix
- OpenStack
- VMware ESXi
- NSX-T Federation
- Oracle Cloud Infrastructure (OCI)

This deployment supports the following traffic acquisition methods:

- UCT-V
- Customer-Orchestrated Source

Before you begin

Complete the following setup before starting the Terraform deployment.

1. **Install GigaVUE-FM.**

- Terraform uses GigaVUE-FM as the management system for this deployment. For installation instructions, see the GigaVUE-FM installation topic
- GigaVUE-FM token authentication is required for the Terraform provider to connect to GigaVUE-FM. For details on generating a token, refer to Configure Tokens.
- If GigaVUE-FM is not installed or is not reachable from the deployment system, Terraform cannot create or update the 3PO deployment objects.

2. **Ensure that the third-party orchestration environment is available.**

- Confirm that the third-party orchestrator is running and that the target platform environment is reachable. The third-party orchestrator is responsible for deploying and managing the GigaVUE V Series nodes.
- Terraform does not deploy V Series nodes in a 3PO deployment.

3. **Verify third-party networking configuration**

   Ensure that the required management, data, and tool-side networks are available and correctly configured in the target environment. The third-party orchestrator uses these values when deploying the GigaVUE V Series nodes. For more details, refer to Prerequisites .

4. **Install and verify Terraform 1.14 or later**

   Run the `terraform version` command and confirm that respective version 1.14 or later is displayed.

5. **Run the `terraform init` command**

   Terraform downloads the Gigamon provider automatically from the Terraform Registry and prepares the working directory for deployment. You do not need to download or extract the provider package manually.

The Gigamon provider is available at the Terraform Registry.

Install the Gigamon Terraform Provider Without Internet Access

If the deployment system does not have internet access or cannot reach the Terraform Registry, you can download the Gigamon Terraform provider binary directly from the Terraform provider GitHub Releases page and install it locally

Step 1: Download and install the provider binary

1. **Download the provider zip file for your platform from the GitHub releases page.**

   The following example uses the Linux AMD64 platform. Replace linux_amd64 with the directory name that matches your operating system and architecture.

2. **Create the local plugin directory:**

   ```
   mkdir -p ~/.terraform.d/plugins/local/gigamon/gigamon/6.14.0/linux_amd64
   ```

3. **Extract the zip file:**

   ```
   unzip terraform-provider-gigamon_6.14.0_linux_amd64.zip
   ```

4. **Move the binary to the local plugin directory:**

   ```
   mv terraform-provider-gigamon ~/.terraform.d/plugins/local/gigamon/gigamon/6.14.0/linux_amd64/
   ```

5. **Make the binary executable:**

   ```
   chmod +x ~/.terraform.d/plugins/local/gigamon/gigamon/6.14.0/linux_amd64/terraform-provider-gigamon
   ```

Step 2: Update the provider block

In your .tf file, update the provider source to point to the local plugin directory instead of the Terraform Registry:

```
terraform {
  required_providers {
    gigamon = {
      source  = "local/gigamon/gigamon"
      version = ">= 6.14"
    }
  }
}
```

NOTE: The source value `local/gigamon/gigamon` tells Terraform to look for the provider in the local plugin directory. Do not use the registry source address when using the local installation method.

Step 3: Continue with the standard deployment flow

After the binary is in place and the provider block is updated, the remaining deployment steps are the same as the registry-based installation. Run **`terraform init`**, **`terraform plan`**, and **`terraform apply`** from the working directory as described in Run the Terraform Deployment File.

Prepare the Third Party Orchestration Deployment Files

Sample configuration files for the UCT-V and Customer-Orchestrated Source deployment paths are available in the Terraform Registry.

These sample files provide working examples that demonstrate the resource structure and required configuration arguments for supported traffic acquisition methods. Use them as a reference when creating deployment files, or building custom deployment files based on requirements. Review and update all placeholder values before using the configuration in an environment.

> **NOTE:** Terraform reads all .tf files in the working directory as a single configuration and processes them together during plan and apply operations.

Before you create the deployment files, decide how to handle the monitoring domain:

- If the monitoring domain does not exist in GigaVUE-FM, include a resource block to create it as part of the deployment.
- If the monitoring domain already exists in GigaVUE-FM, supply the monitoring domain name and connection name in the values file. Do not include a resource block to create it.

You can use either of the following approaches depending on the complexity of your deployment.

1. Single-file configurationModule-based configuration

Single-file configuration

Write all provider settings and resource definitions in a single main.tf file. Use this approach for straightforward deployments where you want to keep all configuration in one place.

Your **main.tf** (Main deployment configuration file)must include the following blocks:

1. Provider block

   Declare the Gigamon provider and specify the GigaVUE-FM connection details.

   Example:

```
terraform {
  required_providers {
    gigamon = {
      source  = "gigamon-engg/gigamon"
      version = ">= 6.14"
    }
  }
}

provider "gigamon" {
  fm_ip = "<GigaVUE-FM IP address or hostname>"
  token = "<Token>"
}
```

2. Resource blocks

   Add a resource block for each third-party orchestration object that Terraform must create or manage. The resources you include depend on your traffic acquisition method.

   For UCT-V deployments, define the resources in the following sample order:

   - Monitoring domain (if not pre-existing in GigaVUE-FM)
   - Connection
   - Monitoring session
   - Applications
   - Maps
   - Links
   - Tunnels

   For Customer-Orchestrated Source deployments, define the resources in the following sample order:

   - Monitoring domain (if not pre-existing in GigaVUE-FM)
   - Connection
   - Monitoring session
   - Applications, maps, links, and tunnels

   Refer to the Terraform Registry documentation for the resource type names, required arguments, and argument descriptions for each resource.

Module-based configuration

Organize the configuration across multiple files or modules. Use this approach when you want to reuse configuration across environments, manage a large deployment, or separate concerns across teams.

In a module-based setup, you create a root configuration that calls one or more child modules. Each module groups related resources and accepts input variables. The module structure varies depending on the traffic acquisition method you use.

Example main.tf - calling modules

```
module "monitoring_domain" {
  source       = "./modules/monitoring-domain"
  fm_ip        = var.fm_ip
  domain_alias = var.domain_alias
  # Omit this module block if using an existing monitoring domain.
}

module "connection" {
  source               = "./modules/connection"
  monitoring_domain_id = module.monitoring_domain.id
  connection_alias     = var.connection_alias
  # Add required variables for your environment.
}

module "monitoring_session" {
  source               = "./modules/monitoring-session"
  monitoring_domain_id = module.monitoring_domain.id
  connection_id        = module.connection.id
  # Add required variables for your environment.
}
```

Each module's **main.tf** contains the resource blocks for that group. Pass values between modules using module outputs.

Refer to the Terraform provider documentation for the full list of resources and arguments for each module.

Run the Terraform Deployment File

After you finish the sample-file updates, run the deployment from the working directory.

1. Initialize the working directory. Run the following command:

   ```
   terraform init
   ```

   Terraform initializes the working directory, downloads Gigamon provider automatically from the Terraform Registry and prepares the working directory for deployment.

2. Optional: Validate the configuration.

   - Run:

     ```
     terraform validate
     ```

   - Run this command when you want Terraform to check the configuration for syntax and structural issues before it generates the deployment plan.

3. Review the deployment plan.
    - Run:
      ```
      terraform plan
      ```
    - Review the output carefully. Confirm that Terraform will create or update the expected third-party objects.
    - Do not continue until the plan matches the deployment that you expect.
4. Apply the configuration.
    - Run:
      ```
      terraform apply
      ```
    - When prompted, confirm the deployment.
    - Terraform connects to GigaVUE-FM, creates or updates the third-party monitoring domain and connection, and applies the monitoring session configuration defined in the deployment files.

      NOTE: Manage monitoring domain, connection, CA, and SSL key/certificate resources separately from the monitoring session configuration. Create them in GigaVUE-FM and reference them as data sources, or manage them through a separate Terraform configuration. This approach ensures the resources exist before deployment and reduces the risk of unintended modifications during update or destroy operations.

Update an existing Third Party Orchestration deployment

To update an existing deployment, change only the required values in the deployment files and rerun:

```
terraform plan
terraform apply
```

Make small, controlled changes and verify the deployment after each update. This approach simplifies review and troubleshooting.

Destroy a Third-Party Orchestration Deployment

Use terraform destroy to remove the Third-Party Orchestration objects that Terraform manages in GigaVUE-FM.

NOTE: In a Third-Party Orchestration deployment, terraform destroy cannot complete in a single run if the configuration includes a monitoring domain and connection. GigaVUE-FM does not allow deletion of a monitoring domain or connection while UCT-V agents or V Series nodes remain registered. Terraform

will destroy the monitoring session, certificate application, CA, and SSL key or certificate in the first run, but will fail when it attempts to delete the connection and monitoring domain.

To destroy the deployment completely, follow the two-step process below.

1. **Run the first destroy**
   - Run the following command from the working directory:

     ```
     terraform destroy
     ```

   - Terraform removes the monitoring session in this run:

   Terraform cannot delete the connection and monitoring domain during this run. This occurs because GigaVUE-FM does not allow deletion of a monitoring domain or connection while UCT-V agents or V Series nodes remain registered.

2. **Unregister agents and nodes, then re-run destroy**
   - In GigaVUE-FM, manually unregister the following from the monitoring domain and connection before the CA and SSL keys and certificates are deleted:
     - **UCT-V deployment** - Unregister all UCT-V agents, the UCT-V controller, and V Series nodes.
     - **Customer-Orchestrated Source deployment** - Unregister all V Series nodes.
   - Confirm that no agents or nodes remain registered under the monitoring domain or connection.
   - Re-run the destroy command:

     ```
     terraform destroy
     ```

   Terraform deletes the CA and SSL key or certificate, connection and monitoring domain.

NOTE: If you configure the monitoring domain and connection as data sources instead of managed resources in your Terraform configuration, terraform destroy completes in a single run. In this case, Terraform does not attempt to delete the monitoring domain or connection, and manual unregistration is not required.

Verify the deployment

After the deployment completes, verify the deployment in GigaVUE-FM.

1. **Verify the monitoring domain and connection**

- Go to the monitoring domain page.
- Confirm that:
  - monitoring domain is present
  - connection is present
  - connection is associated with the expected monitoring domain

If the monitoring domain or connection does not appear in the expected location, review the monitoring domain name and connection name in the values file and rerun the deployment.

2. **Verify node and tunnel health**

- Confirm that the deployed components appear under the correct monitoring domain and connection.
- Confirm that node health is normal. GigaVUE-FM places components in the correct monitoring domain and connection by using the supplied registration data and tracks health through heartbeat messages.

3. **Verify the monitoring session configuration**

- Go to the monitoring session view for the deployment.
- Confirm that:
  - monitoring session is present
  - expected applications are attached
  - expected maps are attached
  - expected links are attached
  - expected tunnels are attached
- If the deployment uses secure tunnel settings, confirm that the secure tunnel configuration is present and healthy.

If any required object is missing, review **main.tf** and the monitoring session values in the values file, then rerun terraform plan and terraform apply.

4. **Verify traffic flow**

- Confirm that traffic reaches the configured tool destination.
- If traffic does not reach the tool destination, review the traffic acquisition method, monitoring session values, application values, and tunnel or link configuration in the sample files.

After you complete this verification, GigaVUE-FM contains the third-party orchestration monitoring domain, the connection, and the monitoring session configuration defined in the Terraform deployment files

OpenTofu Support

OpenTofu is an open-source alternative to Terraform that is compatible with the Gigamon Terraform provider. All configuration files, scripts, and deployment steps described in this guide work with OpenTofu without modification.

OpenTofu Registry

To use OpenTofu instead of Terraform:

- Install OpenTofu v1.12.3 or later on the deployment system:
  - Install OpenTofu on Windows
  - Install OpenTofu on Linux
- Replace all terraform CLI commands with the equivalent tofu commands.
- Follow the same deployment steps described in this guide.

For the Gigamon provider, refer to the OpenTofu Registry to download the provider package compatible with OpenTofu.

Best Practices

Use the following best practices when you deploy by using Terraform:

1. Store Terraform configuration files in version control.
2. Run `terraform validate` before `terraform plan` to catch syntax and configuration errors early.
3. Review `terraform plan` before you run `terraform apply`.
4. Pin the provider version in **provider.tf** to avoid unexpected behavior from automatic provider upgrades.
5. Keep sensitive values out of configuration files and protect access to the state file.
6. Make small, controlled changes and verify the deployment after each update.

7. Use a shared remote backend for production deployments.

   - A shared backend ensures that all users working on the same deployment share the same Terraform state file. Without a remote backend, concurrent changes from multiple users can corrupt the state, and accidental deletion of a local state file results in loss of all tracked resources.

   - Configure the remote backend in the .tf file using the http backend block. Store the backend connection values separately in a .hcl file and pass it at initialization, do not store credentials directly in the .tf file.

     Example: main.tf - backend and provider configuration

     ```
     terraform {
       required_providers {
         gigamon = {
           source  = "gigamon-engg/gigamon"
           version = ">= 6.14"
         }
       }
     }
     ```

     Example: backend.hcl - backend connection values

     ```
     address                = "https://{fm_address}/terraform-state/{project_name}"
     lock_address           = "https://{fm_address}/terraform-state/{project_name}/lock"
     unlock_address         = "https://{fm_address}/terraform-state/{project_name}/lock"
     skip_cert_verification = true
     username               = "{project_name}"
     password               = "{fm_token}"
     ```

   - Pass the .hcl file when you initialize the working directory:

     ```
     terraform init -backend-config=<hcl file location>
     ```

     NOTE:
     - Save the **.hcl** file locally and do not commit it to version control. The file contains credentials and backend connection details that must remain secure.
     - Keep credentials and sensitive values out of configuration files and protect access to the state file.

Verification and Troubleshooting

Verify the deployment

After you run Terraform, verify the deployment in GigaVUE-FM.

- Log in to GigaVUE-FM.
- Verify that the monitoring domain and connection are present.
- Verify that the monitoring session is present.
- Verify that the required applications, maps, links, and tunnels are attached to the monitoring session.
- Verify that the deployed nodes are healthy.
- Verify that traffic is flowing as expected.

If any required object is missing or unhealthy, review the Terraform output, correct the configuration, and rerun the deployment.

Troubleshoot the deployment

If the deployment does not complete successfully, use the following checks.

Provider issues

- Verify that the provider source is correct.
- Verify that the provider version is supported for your release.
- Rerun `terraform init`.

Authentication or connectivity issues

- Verify the GigaVUE-FM IP address or hostname.
- Verify the authentication values.
- Verify network connectivity between the system running Terraform and GigaVUE-FM.

Configuration issues

- Run `terraform validate`.
- Run `terraform plan`.
- Correct any configuration errors before you rerun terraform apply.

Deployment timeout issues

- Verify whether the deployment includes operations that require additional time to complete.
- Increase the timeout value only if your deployment requires it.

State file issues

- Verify that all users managing the same production deployment use the same shared backend.
- Do not use separate local state files for the same production deployment.

Recover after a failed deployment

- Identify and correct the root cause.
- Rerun the Terraform workflow.
- Verify that the deployment reaches the intended state.

Configure

Configure UCT-V Features

Refer to the following sections for more detailed information:

- Configure Prefiltering
- Create Precryption Template for UCT-V
- Configure Secure Tunnel (AWS)

Configure Prefiltering

For prefiltering the traffic, GigaVUE-FM enables you to create a prefiltering policy template and apply it to a Monitoring Session,

Considerations

- You can create and reuse a policy template across multiple monitoring sessions.
- Each monitoring session supports up to 16 prefiltering rules.
- You can edit the policy template during monitoring session configuration to customize rules and filter values.
- GigaVUE-FM does not save changes made to the template during monitoring session edits. These changes apply only to that specific session.

Rules and Notes

- Prefiltering is supported on UCT-V for Windows systems and Linux systems running Kernel version 4.18 or later.
- Prefiltering is supported for both Linux and Windows UCT-Vs .

- For single monitoring session only one prefiltering policy is applicable. All UCT-Vs in that monitoring sessions are configured with respective prefiltering policy .
- For multiple monitoring session using the same agent to acquire the traffic, if a monitoring session uses a prefilter and the other monitoring session does not use a prefilter, then you cannot apply the prefiltering policy. The policy is set to PassAll and prefiltering is not performed.

Create Prefiltering Policy Template

GigaVUE-FM allows you to create a prefiltering policy template with one or more rules. You can configure a rule with one or more filters. A single monitoring session supports a maximum of 16 rules.

To create a prefiltering policy template,

1. Go to **Traffic > Resources > Prefiltering** and select **UCT-V**.

2. Select **New**.

3. In the **Template Name** field, enter the name of the template,

4. In the **Rule Name** field, enter the name of a rule.

5. Select one of the following options:

- Pass: Allows the traffic.
- Drop: Blocks the traffic..

> **NOTE:** If no prefilter rules are defined, traffic is implicitly allowed. When rules are defined, an implicit drop rule applies. Traffic that does not match any specified rule is dropped.

6. Select one of the following options:

- **Bi-Directional:** Allows the traffic in both directions of the flow. A single Bi-direction rule requires 1 Ingress and 1 Egress rule.
- **Ingress:** Filters incoming traffic.
- **Egress:** Filters outgoing traffic.

> **NOTE:** When using loopback interface in Linux UCT-V, you can use only Bi-directional.

7. Select a priority value from 1-8.

- 1: Select the value as 1 to pass or drop a rule in top priority.
- 2-8 Select the value as 2, 3, 4 to 8, where 8 indicates a rule with the least priority.

  Drop rules are added first based on the priority and then pass rules are added.

8. Select one of the following options as **Filter Type**:
   - L3
   - L4
9. Select one of the following options **Filter Name**:
   - ip4Src
   - ip4Dst
   - ip6Src
   - ip6Dst
   - Proto: Applies toboth ipv4 and ipv6.
10. Select one of the following options for **Filter Relation**:
    - Not Equal to
    - Equal to
11. In the **Value** field, enter the source or destination port.
12. Select **Save**.

> **NOTE:** Select **+** to add more rules or filters or select **-** to remove a rule or a filter.

To enable prefiltering for a Monitoring Session, refer to Enable Prefiltering.

Create Precryption Template for UCT-V

GigaVUE-FM allows you to filter packets during Precryption in the Data Acquisition at the UCT-V level. This filtering is based on L3/L4 5 tuple information (5-tuple filtering) and the applications running on the workload virtual machines.

Rules and Notes:

- Selective Precryption works with GigaVUE-FM and the fabric components version 6.8.00 or above.
- When a single UCT-V is associated with two different Monitoring Sessions with contrasting pass and drop rules, then instead of prioritizing a single rule, GigaVUE-FM passes all the traffic.
- Once the templates are associated with a Monitoring Session, the changes made in the template are not reflected in the Monitoring Session.

Refer to the section the following sections for more detailed information:

- Create Precryption Template for Filtering based on Applications
- Create Precryption Template for Filtering based on L3-L4 details

Create Precryption Template for Filtering based on Applications

The application filter allows you to select the applications for which you apply Precryption in the Monitoring Session Options page.

To create,

1. Step Go to **Traffic > Resources > Precryption**.

   The **Precryption Policies** page appear
2. Step Select the **APPLICATION** tab.
3. Select **Add**.

   The New Precryption Template page appears.
4. Select **csv** as the **Type**, if you wish to add applications using a .csv file.
   a. Download the sample .csv file and edit it.
   b. Save your .csv file.
   c. Select **Choose File** and upload the file.
5. Select **Manual** as the **Type** if you wish to add the applications manually.
6. Enter the **Application Name** select + icon to add more applications.
7. Select **Save**.

You can view the added applications in the **APPLICATION** tab.

You can delete a selected application or you can delete all the application using the **Actions** button.

Create Precryption Template for Filtering based on L3-L4 details

To create,

1. Go to **Traffic > Resources > Precryption**. The **Precryption Policies** page appears.
2. Select the **L3-L4** tab.

3. Perform the following steps:

    a. In the **Template** field, enter a name for the template.

    b. In the **Rule Name** field, enter a name for the rule.

    c. For **Action**, select one of the following options:

    - **Pass:** Passes the traffic.
    - **Drop:** Drops the traffic.

    > **NOTE:** In the absence of a Precryption rule, traffic is implicitly allowed. However, the defined rules include an implicit pass all rule. Should the traffic not conform to any of the specified rules, it is passed.

    d. For **Direction**, select one of the following options:

    - **Bi-Directional:** Allows the traffic in both directions of the flow. A single Bi-direction rule should consist of 1 Ingress and 1 Egress rule.
    - **Ingress:** Filters the traffic that flows in.
    - **Egress:** Filters the traffic that flows out.

    e. In the **Priority** field, select one of the following values:

    - 1: Select to pass or drop a rule in top priority.
    - 2 to 8: Select to decide priority where 8 is used for setting a rule with the least priority.

    > **NOTE:** Drop rules are added based on the priority, and then pass rules are added.

f. Select **Filter Type** from the following options:

- L3
- L4

> **NOTE:** You can use L4 Filter Type only with L3.

For L3, perform the following:

i. Select **Filter Name** from the following options:

- IPv4 Source
- IPv4 Destination
- IPv6 Source
- IPv6 Destination
- Protocol: It is common for both IPv4 and IPv6.

ii. Select **Filter Relation** from any one of the following options:

- Not Equal to
- Equal to

iii. Enter or Select the Value based on the selected **Filter Name**.

> **NOTE:** When using **Protocol** as **Filter Name**, select **TCP** from the drop-down menu.

For L4, perform the following:

i. Select the **Filter Name** from the following options:

- Source Port
- Destination Port

ii. Select the **Filter Relation** from any one of the following options:

- Not Equal to
- Equal to

iii. Enter the source or destination port value.

4. Select **Save**.

> **NOTE:** Select **+** to add more rules or filters. Select **-** to remove a rule or a filter.

The template is successfully created. To enable Precryption, refer to Enable Prefiltering section.

You can delete a selected template or you can delete all the templates using the **Actions** button.

You can also edit a selected template using **Actions > Edit**.

Configure Secure Tunnel (AWS)

You can configure the Secure tunnel:

- Precryption Traffic
- Mirrored Traffic

Precryption Traffic

You can send the Precryption traffic through a secure tunnel. When secure tunnels for Precryption is enabled, packets are framed and sent in PCAPng format.

When you enable the secure tunnel option for mirrored traffic and Precryption traffic, two TLS secure tunnel sessions are created.

We recommend always to enable secure tunnels for Precryption traffic to securely transfer sensitive information.

For more information about PCAPng, refer to PCAPng Application.

Mirrored Traffic

You can enable the Secure Tunnel for mirrored traffic. By default, Secure Tunnel is disabled.

Refer to the following sections for Secure Tunnel Configuration:

- Configure Secure Tunnel from UCT-V to GigaVUE V Series Node
- Configure Secure Tunnel between GigaVUE V Series Nodes
- Configure Secure Tunnel between GigaVUE V Series Nodes and GigaVUE HC Series

Prerequisites

- Enable TCP Port 11443 in security group settings. For details on Network Firewall / Security Group, refer to .
- While creating Secure Tunnel, you must provide the following details:
  - SSH key pair
  - CA Certificate chain

Notes

- Protocol versions IPv4 and IPv6 are supported.

- For IPv6 tunnels, GigaVUE-FM and the fabric components versions are 6.6.00 or above.
- For UCT-V with a version lower than 6.6.00, if the secure tunnel is enabled in the monitoring session, secure mirror traffic will be transmitted over IPv4, regardless of IPv6 preference.

Configure Secure Tunnel from UCT-V to GigaVUE V Series Node

To configure a secure tunnel in UCT-V, you must configure one end of the tunnel to the UCT-V and the other end to GigaVUE V Series node. You must configure the CA Certificate chain in UCT-V and the private keys and SSL certificates in GigaVUE V Series node. Refer to the following steps for configuration:

<table>
<tr><th>S. No</th><th>Task</th><th>Refer to</th></tr>
<tr><td>1</td><td>Upload a CA Certificate chain in a single file</td><td>You must upload a CA Certificate chain for establishing a connection with the GigaVUE V Series node.
To upload the CA using GigaVUE-FM follow the steps given below:
1. Go to Inventory > Resources > Security > CA List.
2. Click New, to add a new CA Certificate chain Authority. The Add Custom Authority page appears.
3. In the Alias field, enter the CA name.
<table>
<tr><th>Field</th><th>Action</th></tr>
<tr><td>Alias</td><td>Alias name of the CA.</td></tr>
<tr><td>File Upload</td><td>Choose the certificate from the desired location.</td></tr>
</table>
4. Select Save.
NOTE: Ensure that the Intermediate CA Certificate(s) are included in the CA certificate chain file in the correct signing order, followed by the Root CA Certificate at the end.
For more information, refer to the section Adding Certificate Authority.</td></tr>
<tr><td>2</td><td>Upload an SSL Key Pair</td><td>You must add an SSL key pair to GigaVUE V Series node. Follow the steps in the Upload SSL Keys section for detailsUpload SSL Key Pairs</td></tr>
<tr><td>3</td><td>Select the SSL Key Pair while creating a monitoring domain and configuring the fabric components in GigaVUE-FM.</td><td>You must select the added SSL Key Pair in GigaVUE V Series Node Key while creating a monitoring domain configuring the fabric components in GigaVUE-FM. To select the SSL key pair, follow the steps in the Configure GigaVUE Fabric Components in GigaVUE-FM section
If the existing Monitoring Domain does not have an SSL key pair, you can add it by following the given steps:
1. Select the Monitoring Domain for which you want to</td></tr>
</table>

S. No	Task	Refer to
		add the SSL key pair. 2. Select the **Actions** drop down list and select **Edit SSL Configuration**. An **Edit SSL Configuration** window appears. 3. Select the CA in the **UCT-V Agent Tunnel CA** drop down list. 4. Select the SSL key pair in the **V Series Node SSL key** drop down list. 5. Select **Save**.
4	Select the CA Certificate chain while creating the monitoring domain configuring the fabric components in GigaVUE-FM.	You should select the added CA Certificate chain in UCT-V Controller. To select the CA Certificate chain, follow the steps in the section Configure GigaVUE Fabric Components in GigaVUE-FM.
5	Enable the secure tunnel	You should enable the secure tunnel feature to establish a connection between the UCT-V and GigaVUE V Series Node. To enable the secure tunnel feature follow these steps: 1. Go to **Traffic > Virtual > Orchestrated Flows > Select your cloud platform**. 2. Select a Monitoring Session from the Monitoring Sessions list view on the left side of the screen and click the **TRAFFIC ACQUISITION** tab. 3. Enable the **Secure Tunnel** button. You can enable secure tunnel for both mirrored and Precryption traffic. **NOTE:** When GigaVUE V Series Node is upgraded or deployed to 6.5, all the existing monitoring sessions will be redeployed, and individual TLS Tunnel End Points are created for each UCT-V.

Configure Secure Tunnel between GigaVUE V Series Nodes

You can create secure tunnel:

- Between two GigaVUE V Series Nodes.
- From one GigaVUE V Series Node to multiple GigaVUE V Series Nodes.

You must have the following details before you start configuring secure tunnels between two GigaVUE V Series Nodes:

- IP address of the tunnel destination endpoint (Second GigaVUE V Series Node).
- SSH key pair (pem file).

To configure secure tunnel between two GigaVUE V Series Nodes, refer to the following steps:

<table>
<tr><th>S. No</th><th>Task</th><th>Refer to</th></tr>
<tr><td>1</td><td>Upload a CA Certificate chain in a single file</td><td>You must upload a CA Certificate chain to UCT-V Controller to establish a connection between the GigaVUE V Series node.
To upload the CA using GigaVUE-FM follow these steps:
1. Go to Inventory > Resources > Security > CA List.
2. Click Add, to add a new Certificate Authority. The Add Certificate Authority page appears.
3. Enter or select the following information.<table><tr><th>Field</th><th>Action</th></tr><tr><td>Alias</td><td>Alias name of the CA.</td></tr><tr><td>File Upload</td><td>Choose the certificate from the desired location.</td></tr></table>4. Select Save.
5. Select Deploy All.
NOTE: Ensure that the Intermediate CA Certificate(s) are included in the CA certificate chain file in the correct signing order, followed by the Root CA Certificate at the end.
For more information, refer to the section Adding Certificate Authority.</td></tr>
<tr><td>2</td><td>Upload an SSL Key Pair</td><td>You must add an SSL key pair to GigaVUE V Series Node. Follow the steps in the section Upload SSL Key PairsUpload SSL Key Pairs</td></tr>
<tr><td>3</td><td>Select the added SSL Key Pair while creating a Monitoring Domain</td><td>Select the SSL Key Pair added in the Step 2 while creating a Monitoring Domain and configuring the fabric components in GigaVUE-FM for the first GigaVUE V Series Node.
You must select the SSL Key Pair added in the first GigaVUE V Series Node.
To select the SSL key pair, follow the steps in the section Configure GigaVUE Fabric Components in GigaVUE-FM</td></tr>
<tr><td>4</td><td>Select the added CA Certificate chain while creating the monitoring domain</td><td>You should select the added CA Certificate chain in UCT-V Controller. To select the CA Certificate chain, follow the steps in the section Configure GigaVUE Fabric Components in GigaVUE-FM.</td></tr>
<tr><td>5</td><td>Creating a secure tunnel between UCT-V and the first GigaVUE V Series Node.</td><td>You should enable the secure tunnel feature to establish a connection between the UCT-V and the first GigaVUE V Series Node. To enable the secure tunnel feature follow these steps:
1. Go to Traffic > Virtual > Orchestrated Flows ></td></tr>
</table>

<table>
<tr><th>S. No</th><th>Task</th><th>Refer to</th></tr>
<tr><td></td><td></td><td>Select your cloud platform.
2. Select a Monitoring Session from the Monitoring Sessions list view on the left side of the screen and click the TRAFFIC ACQUISITION tab.
3. Enable the Secure Tunnel button. You can enable secure tunnel for both mirrored and Precryption traffic.</td></tr>
<tr><td>6</td><td>Create an Egress tunnel from the first GigaVUE V Series Node with tunnel type as TLS-PCAPNG while creating the Monitoring Session.</td><td>You must create a tunnel for traffic to flow out from the first GigaVUE V Series Node with tunnel type as TLS-PCAPNG while creating the monitoring session. Refer to Configure Monitoring Session to know about monitoring session.
To create the egress tunnel, follow these steps:
1. 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.
2. In the canvas, click the icon on the left side of the page to view the traffic processing elements. Select New > New Tunnel, drag and drop a new tunnel template to the workspace. The Add Tunnel Spec quick view appears.
3. On the New Tunnel quick view, enter or select the required information as described in the following table:
<table>
<tr><th>Field</th><th>Action</th></tr>
<tr><td>Alias</td><td>The name of the tunnel endpoint.</td></tr>
<tr><td>Description</td><td>The description of the tunnel endpoint.</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>S. No</th><th>Task</th><th>Refer to</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><th>Field</th><th>Action</th></tr>
<tr><td>Type</td><td>Select TLS-PCAPNG for creating egress secure tunnel</td></tr>
<tr><td>Traffic Direction</td><td>Choose Out (Encapsulation) for creating an egress tunnel from the GigaVUE V Series Node to the destination. Select or enter the following values:
MTU- The default value is 1500.
Time to Live - Enter the value of the time interval till which the session needs to be available. The value ranges from 1 to 255. The default value is 64.
DSCP - Enter the Differentiated Services Code Point (DSCP) value.
Flow Label - Enter the Flow Label value.
Source L4 Port- Enter the Souce L4 Port value
Destination L4 Port - Enter the Destination L4 Port value.
Flow Label
Cipher- Only SHA 256 is supported.
TLS Version - Select TLS Version1.3.
Selective Acknowledgments - Choose Enable to turn on the TCP selective acknowledgments.
SYN Retries - Enter the value for number of times the SYN has to be tried. The value ranges from 1 to 6.
Delay Acknowledgments - Choose Enable to turn on delayed acknowledgments.</td></tr>
<tr><td>Remote Tunnel IP</td><td>Enter the interface IP address of the second GigaVUE V Series Node (Destination IP).</td></tr>
</table>
4. Click Save.
</td></tr>
</table>

<table>
<tr><th>S. No</th><th>Task</th><th>Refer to</th></tr>
<tr><td>7</td><td>Select the added SSL Key Pair while creating a monitoring domain and configuring the fabric components in GigaVUE-FM in the second GigaVUE V Series Node.</td><td>You must select the added SSL Key pair in GigaVUE V Series Node. To select the SSL key pair, refer to Configure GigaVUE Fabric Components in GigaVUE-FM section.</td></tr>
<tr><td>8</td><td>Create an ingress tunnel in the second GigaVUE V Series Node with tunnel type as TLS-PCAPNG while creating the Monitoring Session for the second GigaVUE V Series Node.</td><td>You must create a ingress tunnel for traffic to flow in from GigaVUE V Series Node with tunnel type as TLS-PCAPNG while creating the monitoring session. Refer to Configure Monitoring Session to know about monitoring session.

To create the ingress tunnel, follow these steps:
1. 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.
2. In the canvas, click the icon on the left side of the page to view the traffic processing elements. Select New > New Tunnel, drag and drop a new tunnel template to the workspace. The Add Tunnel Spec quick view appears.
3. On the New Tunnel quick view, enter or select the required information as described in the following table:
<table><tr><th>Field</th><th>Action</th></tr><tr><td>Alias</td><td>The name of the tunnel endpoint.</td></tr><tr><td>Description</td><td>The description of the tunnel endpoint.</td></tr><tr><td>Type</td><td>Select TLS-PCAPNG for creating egress secure tunnel.
NOTE: If you are enabling Secure tunnel in Monitoring Session with traffic acquisition method as UCT-V, you must not create TLS-PCAPNG Tunnel with direction IN, Destination L4 port 11443, and GigaVUE V Series Node version 6.5 and above.</td></tr><tr><td>Traffic Direction</td><td>Choose in (Decapsulation) for creating an ingress tunnel that receives traffic from the first GigaVUE V Series Node. Select or enter the</td></tr></table></td></tr>
</table>

<table>
<tr><th>S. No</th><th>Task</th><th>Refer to</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><th>Field</th><th>Action</th></tr>
<tr><td></td><td>values as described in Step 6.</td></tr>
<tr><td>IP Version</td><td>The version of the Internet Protocol. IPv4 and IPv6 are supported.</td></tr>
<tr><td>Remote Tunnel IP</td><td>Enter the interface IP address of the first GigaVUE V Series Node (Destination IP).</td></tr>
</table>
4. Select Save.
</td></tr>
</table>

Adding Certificate Authority

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**.

Edit SSL Configuration

You can add certificate authority and SSL keys to your fabric components after deploying it.

To add certificate authority and SSL keys when using secure tunnels,

1. Go to **Inventory > VIRTUAL > Third Party Orchestration**.
2. Select **Monitoring Domain**.

   The **Monitoring Domain** page appears.
3. From the page, select the desired monitoring domain to add the SSL key.

4. From the **Actions** drop down list, select **Edit SSL Configuration**.

   An **Edit SSL Configuration** window appears.

5. From the **UCT-V Agent Tunnel CA** drop down list, select **CA**.
6. From the **V Series Node SSL key** drop down list, select the SSL key.
7. Select **Save**.

Viewing Status of Secure Tunnel for UCT-V

GigaVUE-FM allows you to view the status of secure tunnel connection in UCT-V. You can verify whether the tunnel is connected to the tool or GigaVUE V Series Node through the status.

To verify the status of secure tunnel,

1. Go to **Inventory > VIRTUAL > AWS**, and then select **Monitoring Domain**.
2. In the **Monitoring Domain** page, view the status.

   Tunnel status displays the status of the tunnel. The green color represents that the tunnel is connected and the red represents that the tunnel is not connected.

For configuring secure tunnel, refer to the **Configure Secure Tunnel** section.

Configure Monitoring Session

This chapter describes how to set up ingress and egress tunnel, maps, applications in a monitoring session to receive and send traffic to the GigaVUE Cloud Suite V Series node. The chapter 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 (AWS)
- Configure Monitoring Session for Inline V Series
- Create Ingress and Egress Tunnels (AWS)
- Create Raw Endpoint (AWS)
- Create a New Map (AWS)
- Add Applications to Monitoring Session (AWS)
- Interface Mapping (AWS)
- Deploy Monitoring Session (AWS)

Create a Monitoring Session (AWS)

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

You can view the following tabs on the Monitoring Session page:

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 (AWS)
Sources	Displays the sources and target details monitored by the Monitoring Session. You can view and edit 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 template and apply it to the Monitoring Session. Refer to Enable Prefiltering for more detailed information. **NOTE:** Traffic Acquisition is only applicable for Monitoring Domain created with UCT-V as 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 template, enable user defined applications, and enable or disable distributed De-duplication. Refer to Enable Prefiltering for more detailed information.
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 name of the V Series Node, health status (Configuration Health, Traffic Health, Operational Health) , deployment status, Host VPC, version, and Management IP. You can also change the interfaces mapped to an individual GigaVUE V Series Node. Refer to Interface Mapping (AWS) section for details.
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 (AWS).

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

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

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 pane of the Monitoring Session page to view the Monitoring Sessions list. Select to filter the Monitoring Sessions list. In the left pane, you can:

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

Configure Monitoring Session Options (AWS)

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-d efined 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.

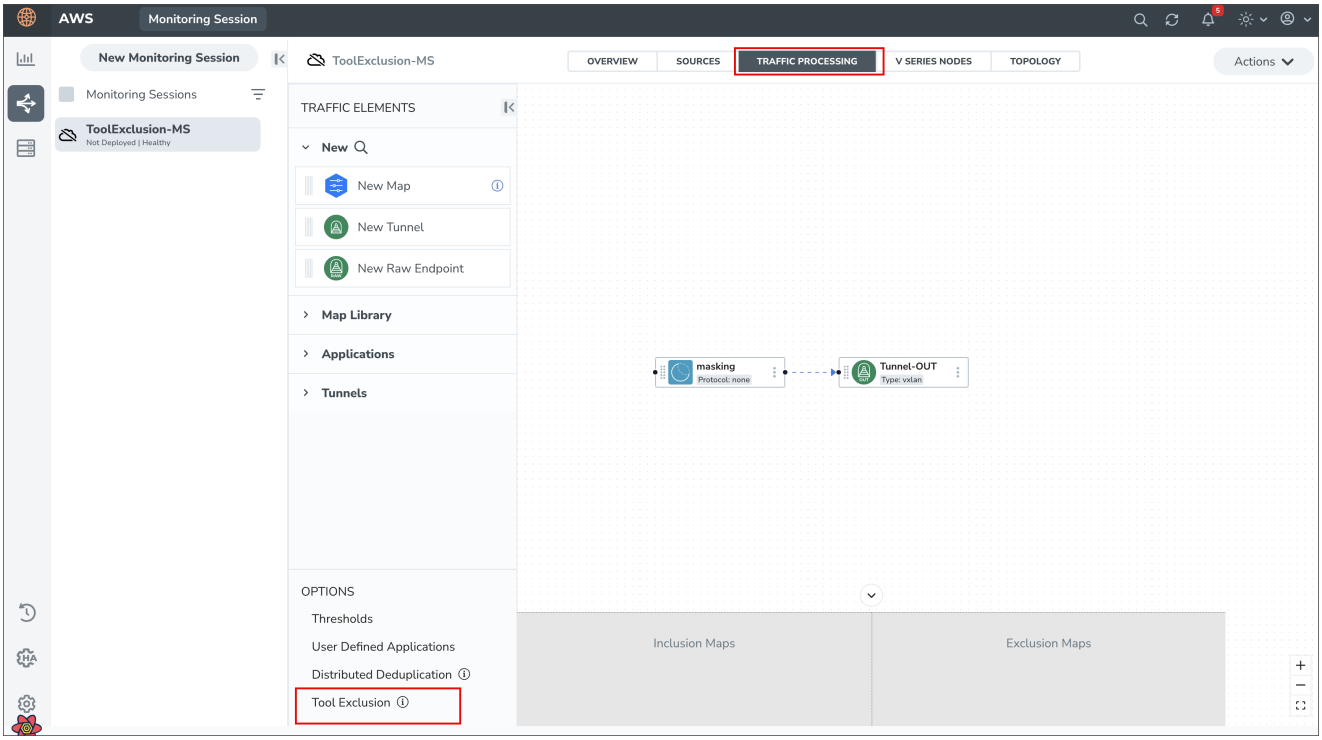
You can exclude tool instances using either of the following methods:

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.



Configure a Traffic Pre-filter

When you create a Monitoring Session, GigaVUE-FM creates a traffic mirror filter with a **Pass All** rule and associates it with the traffic mirroring session. The Pass All filter forwards all the traffic without filtering.

If you want to filter the traffic, then you can create a traffic mirror filter on AWS and add rules to determine the traffic that is mirrored. This traffic mirror filter acts as a pre-filter and pass only the filtered traffic to the GigaVUE V Series Nodes.

To apply the filter to the traffic mirror session that GigaVUE-FM creates, add the tag **in_use_by_gigamon** to the traffic mirror filter.0

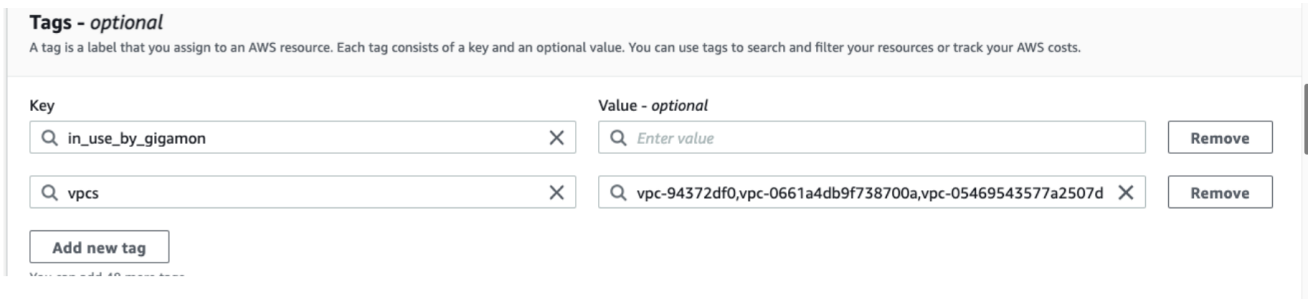
GigaVUE-FM collects all the traffic mirror filters having the tag **in_use_by_gigamon**. It then applies these filters on the traffic mirror sessions to replace the default Pass All filter.

In addition to the **in_use_by_gigamon** tag, you can add the tag **vpc**" to apply specific VPCs. The tag value is a list of vpc separated by comma ",".

You can apply filters at two levels. The two level filters can work together. The VPC level filter overrides the Account level filter for the VPC defined in VPC level filter.

1. **Account level:** You can define a filter (only one filter) which applies on every VPC in an account. You need to tag this filter only with **in_use_by_gigamon**. Do not use the **vpcs** tag.

2. **VPC level:** To filter the traffic at VPC level, in addition to the tag **in_use_by_gigamon**, add the tag **vpcs**.



NOTE: You can define a filter for multiple VPCs. Two filters should not have intersection on VPC. In case of an intersection on VPC, the GigaVUE-FM picks a random filter and no error is displayed.

For more information on creating a traffic mirror, refer to the AWS documentation.

Configure Monitoring Session for Inline V Series

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
   - On an existing Monitoring Session, navigate to the **TRAFFIC PROCESSING** tab.

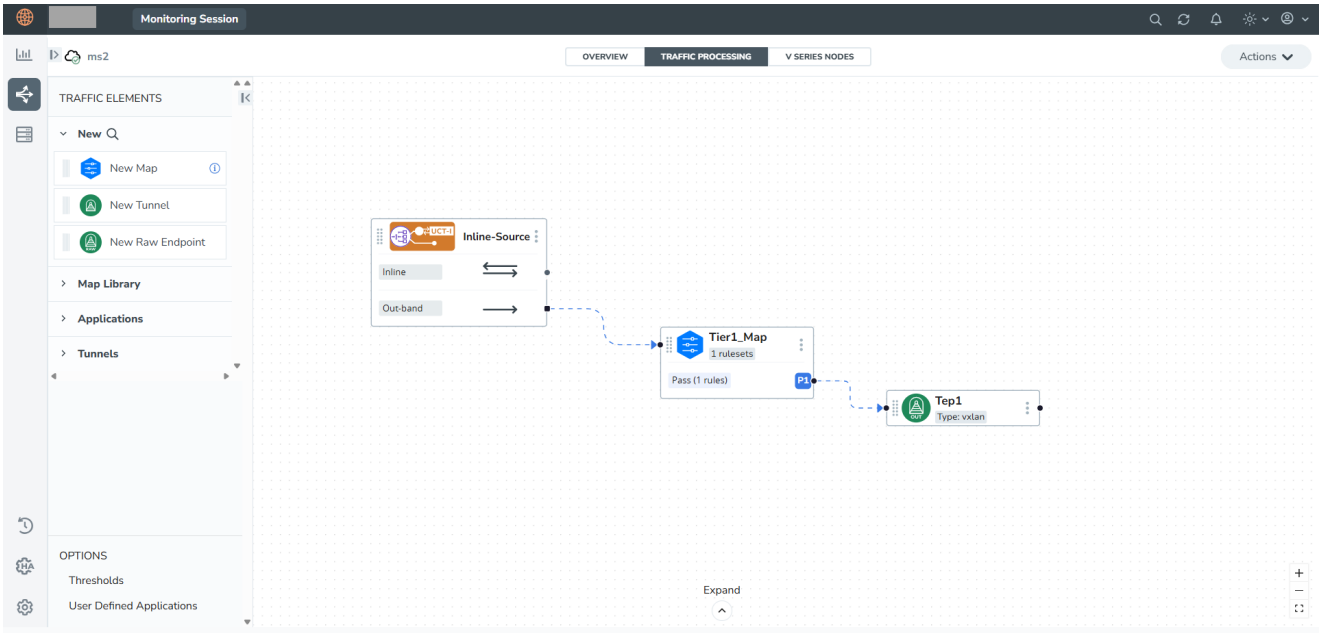
   The GigaVUE-FM Monitoring Session canvas page appears.

   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:

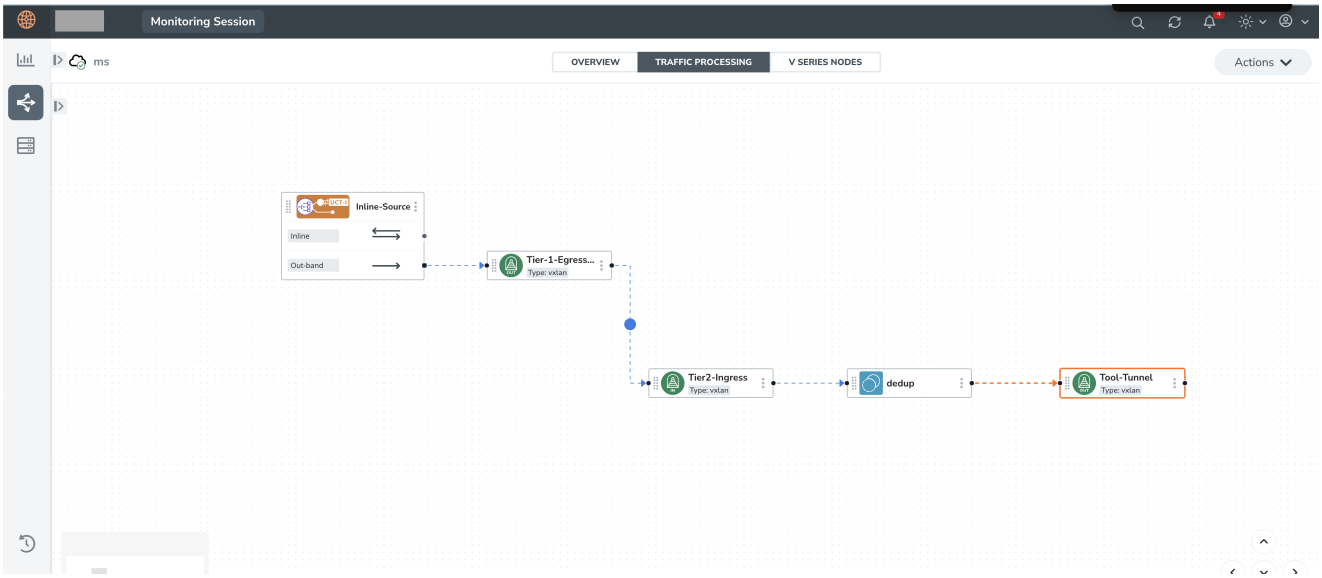
   - (Optional) Maps from the **new map** section.
   - Egress tunnels from the **new tunnel** section. When configuring Egress Tunnel, configure the **Remote Tunnel IP** if you intend to send the traffic directly from Tier 1 to the tool.

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



Tier 2 Monitoring Session (Optional):

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.
   - Maps from the **New Map** section.
   - GigaSMART apps from the Applications section.
   - 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 Step 1 to configure a third tier, if required.



Deploy Monitoring Session

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:

> **NOTE:** To ensure traffic is routed to the GigaVUE V Series Node, you must create routing tables in AWS.

After deploying the Monitoring Session in GigaVUE-FM, you must create routing tables in AWS with the configurations specified in the Architecture patterns for inline inspection section in AWS Documentation. For more details on how to configure routing table refer to Configure routing.

Create Ingress and Egress Tunnels (AWS)

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,

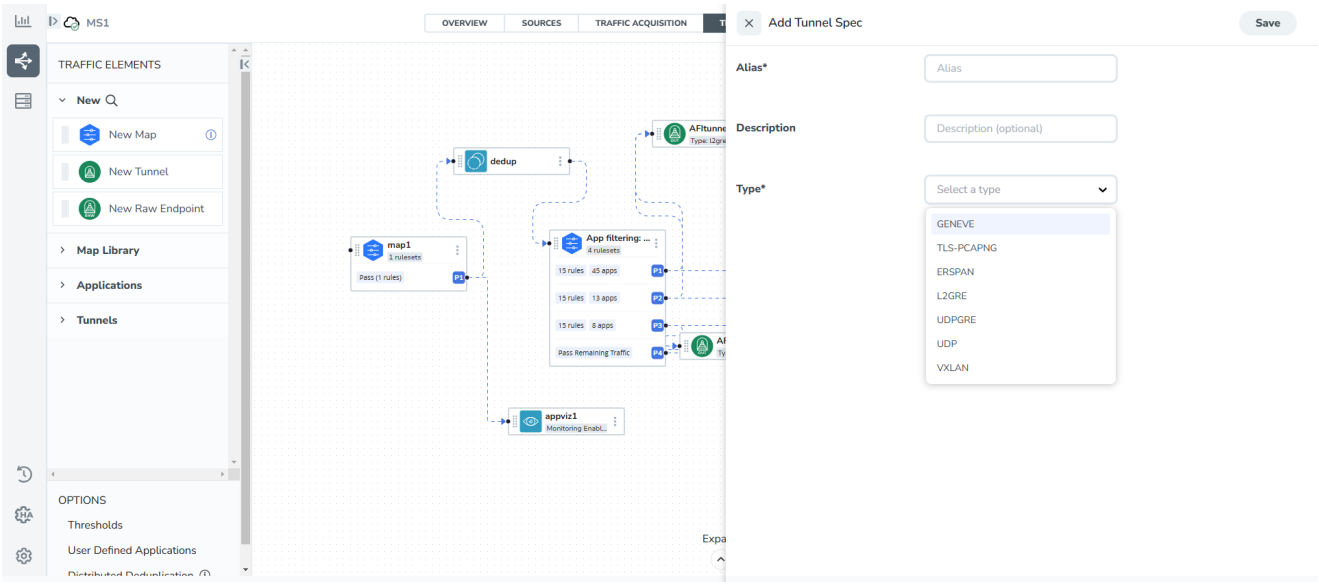
1. Perform one of the following and navigate to the **TRAFFIC PROCESSING** tab:
   - Create a new monitoring session
   - Select **Actions > Edit** on an existing monitoring session.

   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 2: 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.

Field	Description	
	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 to the destination endpoint.	
	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,

Field	Description	
		VMware ESXi **Notes:** • You can configure either a single-tep or multi-tep 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. 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

Field	Description	
		the tunnel source.
	Key	Identifier used to differentiate different UPDGRE/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.	
	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.

Field	Description	
	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.
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.

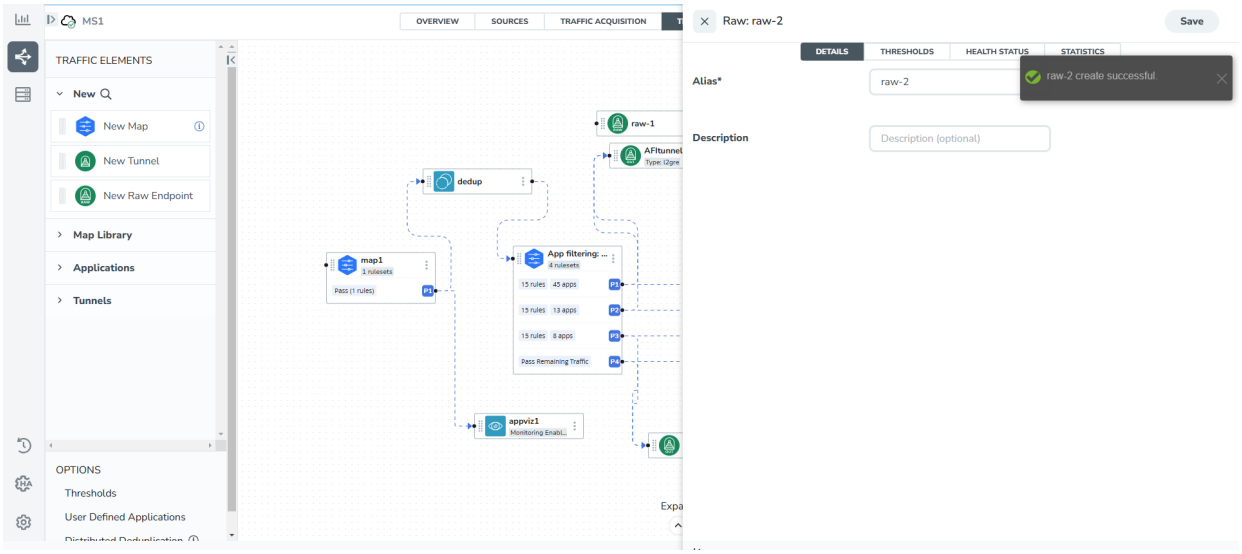
Create Raw Endpoint (AWS)

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 (AWS)

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.

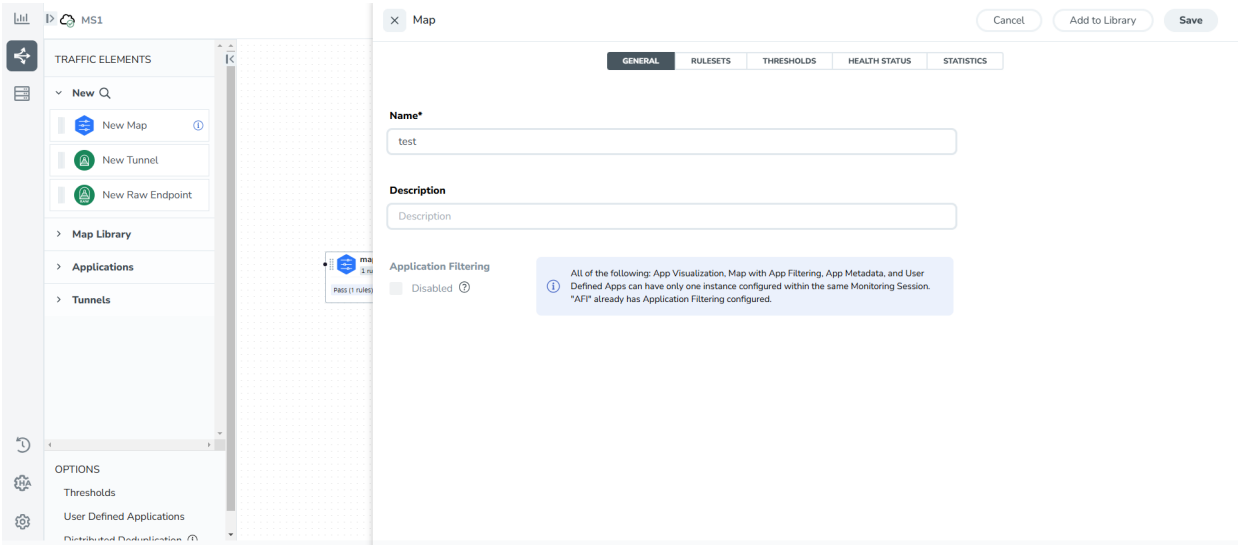
Exclusion Map	An exclusion map determines the instances to be excluded from monitoring. This map is used only for target selection.
Automatic Target Selection (ATS)	A built-in feature that automatically selects the cloud instances based on the rules defined in the traffic filter maps, inclusion maps, and exclusion maps in the Monitoring Session. The below formula describes how ATS works: **Selected Targets = Traffic Filter Maps ∩ 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 (AWS)

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	✓	✓	✓	✓	✓	✓	✓
De-	✓	✓	✓	✓	✓	✓	✓

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
duplication							
L2GRE Tunnel Encapsulation Refer to *Create Ingress and Egress Tunnels* section on the retrospective GigaVUE Cloud Suite Deployment Guide.	✓	✗	✓	✓	✓	✓	✓
VXLAN Tunnel Encapsulation Refer to *Create Ingress and Egress Tunnels* section on the retrospective GigaVUE Cloud Suite Deployment Guide.	✓	✓	✓	✓	✓	✓	✓
L2GRE Tunnel Decapsulation	✓	✗	✓	✓	✓	✓	✓

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
Refer to *Create Ingress and Egress Tunnels* section on the retrospective GigaVUE Cloud Suite Deployment Guide.							
VXLAN Tunnel Decapsulation Refer to *Create Ingress and Egress Tunnels* section on the retrospective GigaVUE Cloud Suite Deployment Guide.	✓	✓	✓	✓	✓	✓	✓
ERSPAN Tunnel Decapsulation Refer to *Create Ingress and Egress Tunnels* section on	✓	✗	✓	✓	✓	✓	✓

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
the retrospective GigaVUE Cloud Suite Deployment Guide.							
UDPGRE Tunnel Decapsulation Refer to *Create Ingress and Egress Tunnels* section on the retrospective GigaVUE Cloud Suite Deployment Guide.	✓	✗	✓	✓	✓	✓	✗
GigaSMART NetFlow Generation	✓	✓	✓	✓	✓	✓	✓
GRE-In-UDP Tunnel Decapsulation	✗	✗	✓	✓	✗	✓	✗
GENEVE Decapsulation	✓	✗	✗	✗	✓	✗	✗
Header Stripping	✓	✓	✓	✓	✓	✓	✓
Load Balancing	✓	✓	✓	✓	✓	✓	✓

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
Masking	✓	✓	✓	✓	✓	✓	✓
SSL Decrypt	✓	✓	✓	✓	×	✓	✓
Secure Tunnels Encapsulation	×	✓	×	✓	✓	✓	✓
Secure Tunnels Decapsulation	×	✓	×	✓	✓	✓	✓
Slicing	✓	✓	✓	✓	✓	✓	✓
5G-Cloud Application	×	×	✓	✓	×	✓	×
5G-Service Based Interface Application	×	×	✓	✓	✓	✓	×

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
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)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:

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Name</td><td>Enter a name for the application.</td></tr>
<tr><td>Description</td><td>Enter the description.</td></tr>
<tr><td>Export Interval</td><td>The time interval in seconds at which the export must be done. The export interval is set to 300 seconds. It cannot be modified.</td></tr>
<tr><td colspan="2">Advanced Settings</td></tr>
<tr><td>Number of Flows</td><td>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>
<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>AWS</td><td>AMD - Large (c5n.2xlarge)</td><td>300k</td></tr>
<tr><td></td><td>AMD - Medium (t3a.xlarge)</td><td>100k</td></tr>
<tr><td></td><td>ARM - Large (c7gn.2xlarge)</td><td>100k</td></tr>
<tr><td></td><td>ARM - Medium (m7g.xlarge)</td><td>200k</td></tr>
<tr><td>Nutanix</td><td>Large (8 vCPU and 16GB RAM)</td><td>200k</td></tr>
</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.
</td></tr>
<tr><td>Monitoring</td><td>You can use this option, enable or disable the Application Visualization application functionality.</td></tr>
<tr><td>Fast Mode</td><td>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.</td></tr>
</table>

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 sectionfor 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 with in the past 7 days.

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

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 redirected to			
	cts-cookie	Cookie (Raw)	Raw value of the HTTP Cookie header line	Client to Server Only	REGEXP	.*tEstCoOkie.*
	content	Content	Message body content	Both, Client to Server or Server to Client	REGEXP	.*GIGAMON.* mindata = 206 Refer Mindata
http2	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
	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	common_name	Domain 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 Address	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 > Resouces > 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.

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td colspan="2">Advanced Settings</td></tr>
<tr><td>Number of Flows</td><td>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>Nutanix</td><td>Large (8 vCPU and 16GB RAM)</td><td>200k</td></tr>
</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.
</td></tr>
<tr><td>Fast Mode</td><td>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.</td></tr>
</table>

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

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

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

Parameter	Description
Condition	Select any one of the conditions from the drop-down menu and search or select the attributes. Use the + and - buttons to add or remove a condition with a Rule. Click and select **Add Condition** to add more conditions. **Note**: A maximum of 4 conditions can be created per Rule.
APPLICATION FILTERING Select the applications and their attributes for traffic filtering by layer seven applications. You can select a maximum of 64 attributes for each application.	
Add Application	Click on the **Add Application** button. The **Add Application** dialog box opens. Select 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. **a.** 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. **b.** In this **Add Application** dialog box, select **User Defined Applications** from the **Application Family** list.

6. To pass or drop any remaining traffic in the network, enter the priority and AE ID in the default rule set available. Select **Pass** or **Drop** option for **Any Remaining Traffic** field.
7. Click the **THRESHOLDS** tab. For more details on how to create and apply threshold template, refer to Traffic Health Monitoring section in the respective cloud deployment guides.

8. To reuse the configuration, click **Add to Library**. Save the application filtering configurations using one of the following ways:
    a. Select an existing group from the **Select Group** list or create a **New Group** with a name.
    b. Enter a description in the **Description** field, and click **Save**.
    c. The saved map can be found in the **Map Library** in the **Edit Monitoring Session** Canvas Page.
9. Click **Save**.

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

When using 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.

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td></td><td>
<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>Nutanix</td><td>Large (8 vCPU and 16GB RAM)</td><td>200k</td></tr>
</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.

</td></tr>
<tr><td>Fast Mode</td><td>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.</td></tr>
<tr><td>Aggregate Round-trip Time</td><td>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.
<table>
<tr><th>Protocol</th><th>Arrtibute</th></tr>
<tr><td>http</td><td>rtt</td></tr>
<tr><td>icmp</td><td>rtt</td></tr>
<tr><td>icmp6</td><td>rtt</td></tr>
<tr><td>ssh</td><td>rtt</td></tr>
<tr><td>tcp</td><td>rtt</td></tr>
<tr><td>tcp</td><td>rtt_app</td></tr>
<tr><td>telnet</td><td>rtt</td></tr>
<tr><td>wsp</td><td>connect_rtt</td></tr>
<tr><td>wsp</td><td>query_rtt</td></tr>
</table>
</td></tr>
</table>

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 *Tool Templates*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.

Application Metadata Exporter

Application Metadata Exporter (AMX) is an Application Intelligence component that runs on GigaVUE V Series Nodes and works with Application Metadata Intelligence (AMI) and other telemetry sources to deliver standardized metadata to your monitoring and analytics tools.

GigaVUE-FM manages both AMX and AMI and provides a central point to deploy, configure, and monitor AMX across on-premises and cloud environments.

You can use AMX to:

- Transform and export application metadata in JSON and Parquet formats to cloud-native tools/data lakes.
- Transform and export NetFlow/IPFIX, and mobility metadata in JSON format to cloud-native tools and Kafka-based data pipeline.
- Enrich mobile-network metadata for 3G/4G/5G visibility and analytics.
- Enrich AMI records with cloud and Kubernetes workload metadata with host, environment, and container context to reduce Mean Time To Identification (MTTI) and Mean Time To Resolution (MTTR).
- Enrich AMI records with user identity information using Zscaler Private Access (ZPA), adding customer, user, and service details to help pinpoint performance issues and monitor the effectiveness and compliance of network access policies.

Refer to the following topics for more detailed information on the various deployment options and scenarios:

- Application Metadata Exporter Deployment Options
- Application Metadata Exporter - Export Scenarios

Application Metadata Exporter Deployment Options

The output from the Application Metadata Intelligence or GTP Correlation Engine is sent to the AMX application, which exports it to the tools in JSON format over HTTPS/Kafka. AMX application is always deployed in GigaVUE V Series Node. The GigaSMART application sending data to the AMX application can be on GigaVUE HC Series or the GigaVUE V Series Node. Based on where the GigaSMART applications reside, there can be four deployment methods:

NOTE: For exporting GigaVUE Enriched Metadata for Cloud Workloads, AMI should be deployed in GigaVUE V Series Nodes.

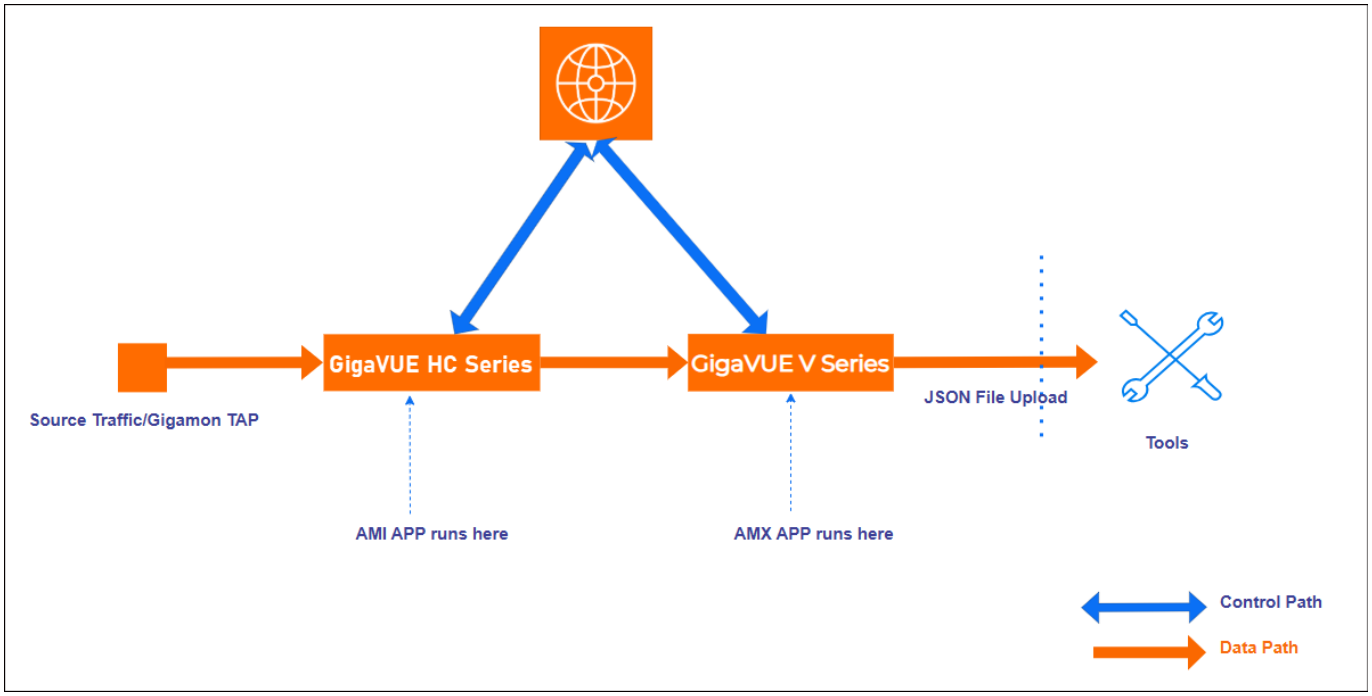
- On-Premises
    - Hardware (AMI)
    - Hardware (Control Plane Metadata)
    - Virtual (VMware, Nutanix, KVM)
- Public Cloud

On-Premises

Hardware (AMI)

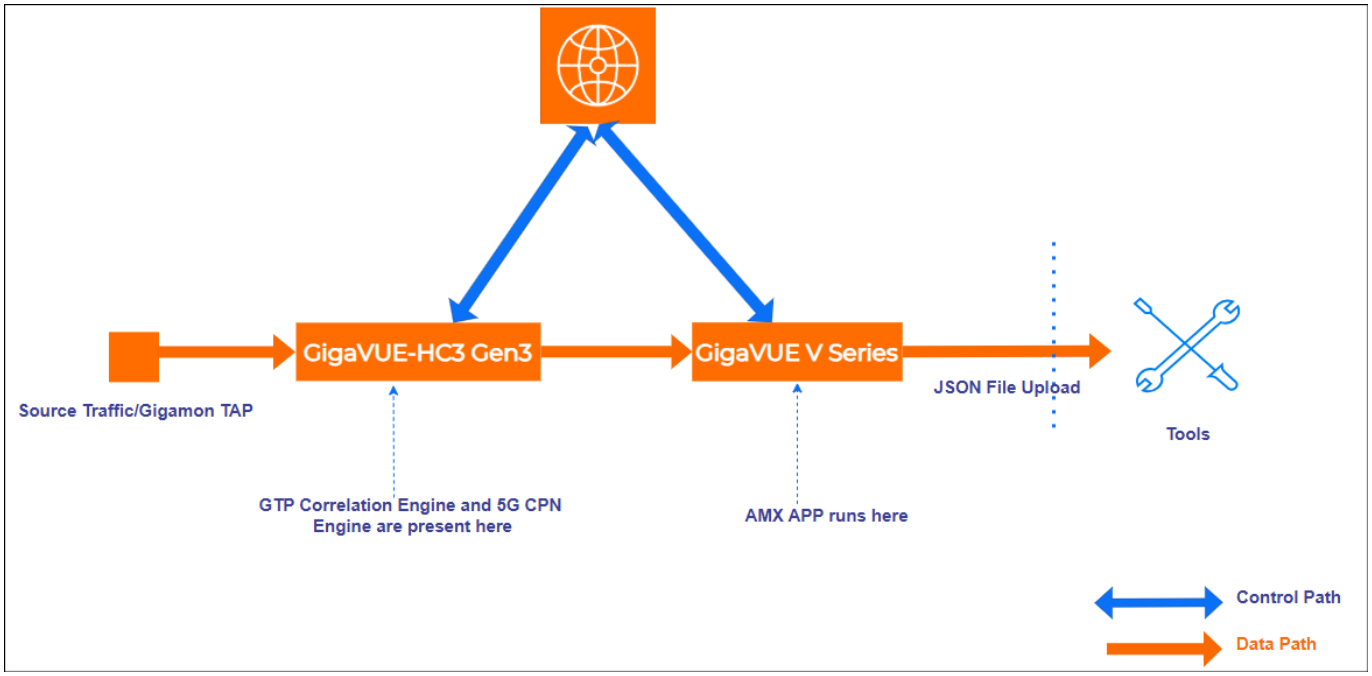
In hardware deployments, the Application Metadata Intelligence (AMI) runs on a physical node/cluster, and the AMX application is deployed on a GigaVUE V Series Node running on VMware ESXi, OpenStack, or Nutanix. The output from the AMI in CEF format is sent to the AMX application in GigaVUE V Series Node. GigaVUE-FM handles the orchestration of the configuration between the Gigamon devices. The following devices support the integration of AMX application:

- GigaVUE-HC1
- GigaVUE-HC3
- GigaVUE-HC1-Plus
- GigaVUE-HCT



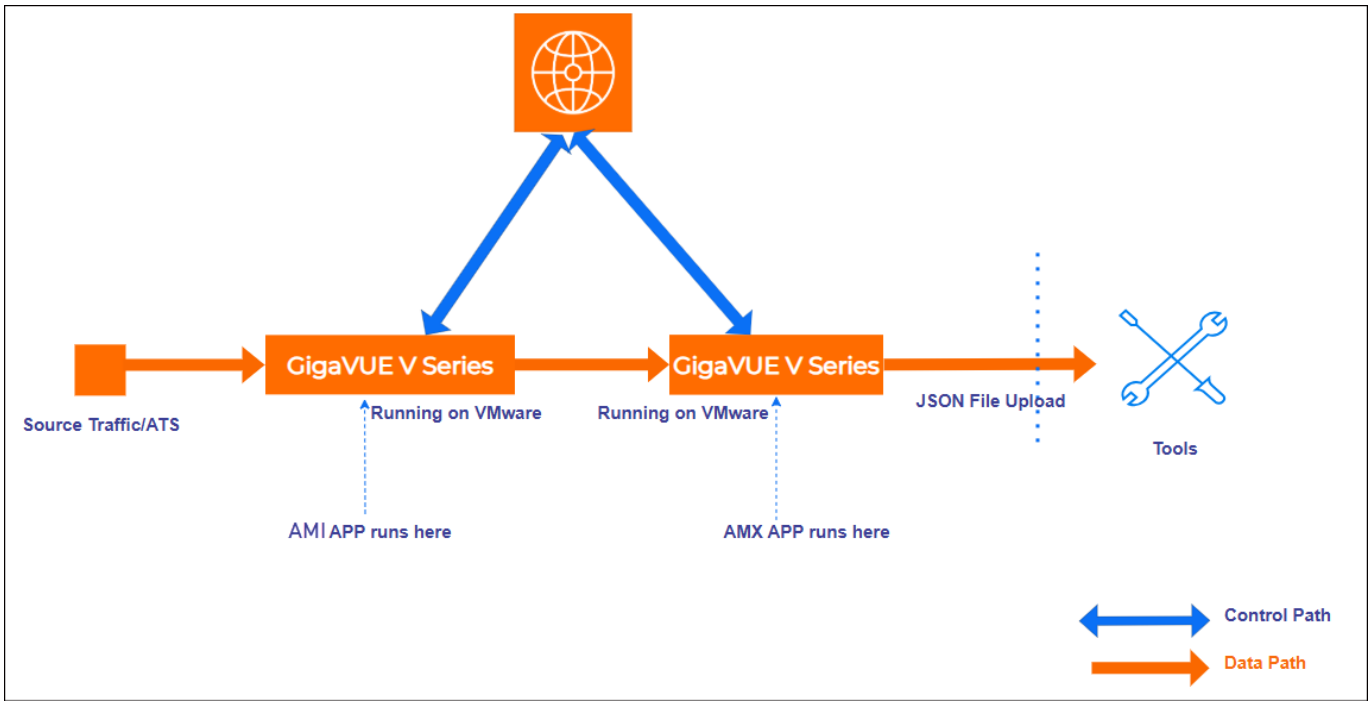
Hardware (Control Plane Metadata)

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



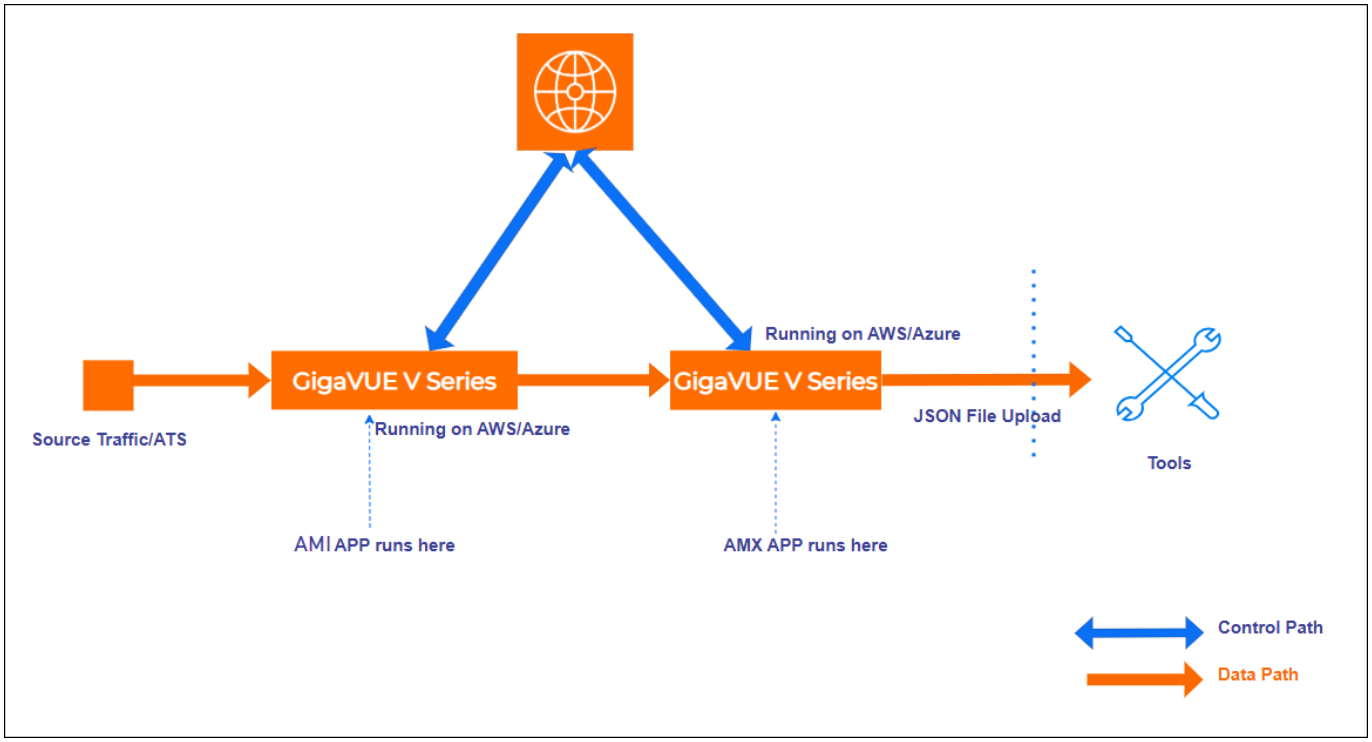
Private Cloud (VMware)

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



Public Cloud

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



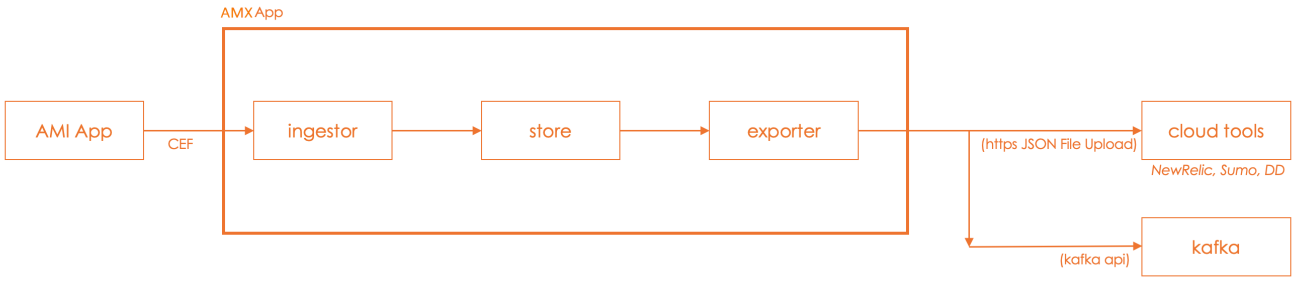
Application Metadata Exporter - Export Scenarios

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

- Export Application Metadata in JSON format over HTTPS/Kafka
- Transform NetFlow/IPFIX records to JSON format and export over HTTPS/Kafka
- Export of 3G/4G/5G Control Plane Metadata by AMX
- Export GigaVUE Enriched Metadata for Mobile Networks and Export over HTTPS/Kafka
- Export GigaVUE Enriched Metadata for Cloud Workloads and Export over HTTPS/Kafka
- On-Premises

Export Application Metadata in JSON format over HTTPS/Kafka

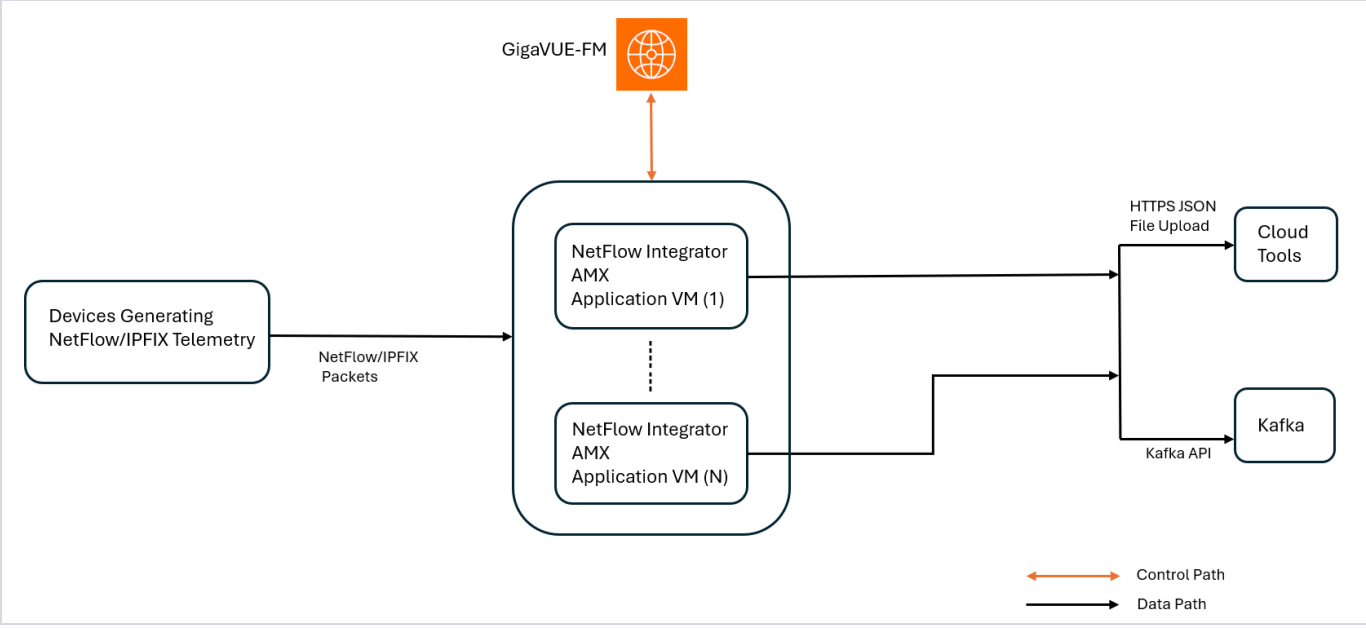
Application Metadata Exporter (AMX) application converts the output from the Application Metadata Intelligence (AMI) in CEF format into JSON format and sends it to the cloud tools and Kafka Consumers. The following image illustrates this end-to-end flow.



Transform NetFlow/IPFIX records to JSON format and export over HTTPS/Kafka

The AMX application with NetFlow Integrator functionality supports ingesting NetFlow/IPFIX flow records from various sources and devices, such as firewalls, routers, and switches, including AMI. It normalizes these records into JSON and exports them to external tools, providing a consolidated view of network traffic and NetFlow/IPFIX insights in a standard format compatible with most Network Performance Monitoring (NPM) tools.

The following image illustrates how the NetFlow Integrator collects NetFlow/IPFIX telemetry from network devices, converts it into JSON, and exports it over HTTPS or Kafka to external cloud tools. GigaVUE-FM acts as the central control system for AMX.



Supported Platforms

- VMware ESXi
- VMware NSX-T

Important Notes

- **NetFlow v9 and v5 Timestamps**:
  - The NetFlow header contains system uptime (in seconds) and an export timestamp.
  - Flow start time is derived using the following formula:
    - Flow_Start = Export Timestamp - System Uptime + First_Switched
  - Flow end time is derived using the following formula:
    - Flow_End = Export Timestamp - System Uptime + Last_Switched
  - The calculated start and end time are converted into nanoseconds.
  - Unsupported attributes such as flow start/end in milliseconds, microseconds, or nanoseconds will be ignored. Instead, the export timestamp is used as both the flow start and end times, which are then converted to nanoseconds.
- **NetFlow v10/IPFIX Timestamps**:
  - NetFlow v10/IPFIX directly incorporates timestamps without the need for system uptime.
  - Even if Flow start and end timestamps are available in seconds, milliseconds, microseconds, or nanoseconds, they are always converted to nanoseconds for output.
- **Missing Flow Start/End Attributes** - For records that do not include flow start or end attributes, AMX automatically assigns both values to the export timestamp.

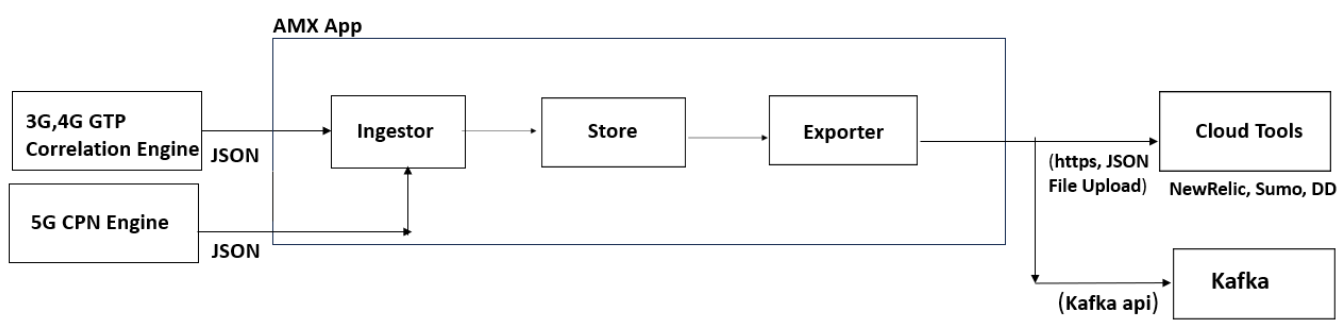
The image below explains how flow start and end times are calculated using system uptime, export timestamp and flow switch times.

```
        Boot - Device boot , uptime init
        FS - First Packet for the flow switched
        LS -  Last Packet for the flow switched
        Export - When the flow is exported
        EXP_TS  -  abs ts at export [present in netflow v9 header]
        UPTIME  - Time since this device is booted [present in netflow v9 header]
        FIRST_SWITCHED - System uptime at which the first packet of this flow was switched
        LAST_SWITCHED - System uptime at which the last packet of this flow was switched



       epoc                          EXP_TS
        |<------------------------------------------------------------------------->
TIMELINE|_________________|[Boot]_______________|[FS]_______________|[LS]___________|[Export]_________________
        |                 <------------------------------------------------------------>
        |                                          UPTIME
        |                 <-------------------->
                           FIRST_SWITCHED
                          <----------------------------------------->
                                       LAST_SWITCHED


        Flow_Start = EXP_TS - UPTIME + FIRST_SWITCHED
        Flow_End   = EXP_TS - UPTIME + LAST_SWITCHED
```

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

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

The AMX application can be deployed only on a GigaVUE V Series Node and can be connected to a GTP Correlation / 5G CPN engine running on a physical node.



Export GigaVUE Enriched Metadata for Mobile Networks and Export over HTTPS/Kafka

The metadata enrichment enhances service provider analytics, by generating metadata on 5G/4G/3G network traffic. The AMX correlates the user plane metadata produced by AMI with the control plane metadata produced by the GTP/5G correlation mobility application to produce an enriched metadata feed for the mobile networks. This data feed helps with use cases like service personalization, planning, and many others by containing information about the:

- Subscriber Session
- Over the Top Application
- Handset Type
- Location
- Flow throughput calculation attributes - DL, UL bytes, and time stamps.
- Application Protocol
- Core Network Information
- User Tunnel Information

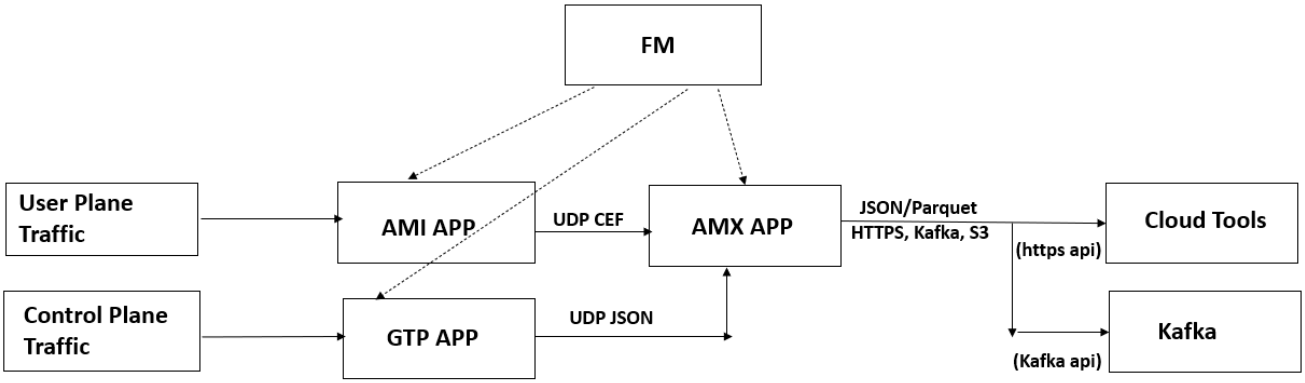
Export of GigaVUE Enriched Metadata for Mobile Networks is supported only for GigaVUE V Series Node deployed using Third Party Orchestration on VMware ESXi.

User Plane and Control Plane traffic from the following devices are supported for exporting GigaVUE Enriched Metadata for Mobile Networks:

- GigaVUE-HC3
- GigaVUE-HC1-Plus

> **NOTE:** For GigaVUE-HC1-Plus, the AMI application must be configured on the built-in engine to efficiently handle higher traffic loads. The plug-in engine can be used for the Control Plane traffic.

For information on Control Plane Metadata, refer to Control Plane Metadata.



Export GigaVUE Enriched Metadata for Cloud Workloads and Export over HTTPS/Kafka

GigaVUE Enriched Metadata for Cloud Workloads provides comprehensive situational awareness to address security and performance pain points in a timely manner. It enriches application metadata from N/S and lateral traffic with key host environment details that allow you to find critical information as follows:

- The location of the workloads hosted and their virtual network.
- The operational environment to which the workloads belong.
- The instance types used, images, and tags that the workload contains.
- The host name, the security associations like security group name, IAM instance profile name.

Export of GigaVUE Enriched Metadata for Cloud Workloads (Virtual Machines)

Export of GigaVUE® Enriched Metadata (GEM) for Cloud Workloads is supported on the following cloud platforms:

- AWS
- Azure
- VMware (ESXi and NSX-T)

This functionality works by using the inventory API which is queried in the following intervals.

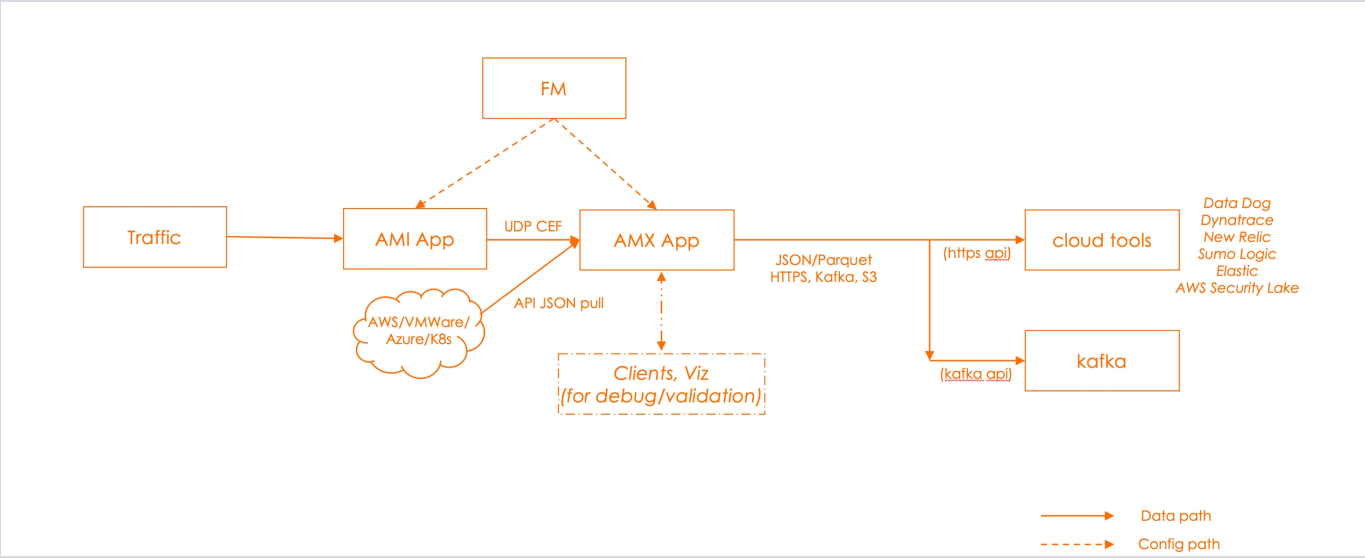
- VMware: 300 sec
- AWS: 30 sec
- Azure: 60 sec

The default inventory query interval should suffice in most cases, however the interval can be customized in extreme situations. Contact Gigamon Support for assistance.

In addition to these fixed inventory polling intervals, you can subscribe to optional services to receive automatic workload updatesin AWS (Event Bridge)/Azure (Event Grid). For VMware, no additional configuration is required because dynamic updates are enabled by default.

AMX application performs the enrichment every 10 seconds. It picks the flow records, which are 15 seconds or older, to allow any delays in fetching the inventory details, and uses the IP address of the endpoints to enrich the records based on the selected attributes. Refer to the following figure for a high-level illustration of the solution. The solution can be deployed using GigaVUE-FM or Third Party Orchestration.

The following image illustrates how AMX exports GigaVUE Enriched Metadata for cloud workloads by converting flow records into JSON/Parquet format and streaming them over HTTPS or Kafka to cloud tools.

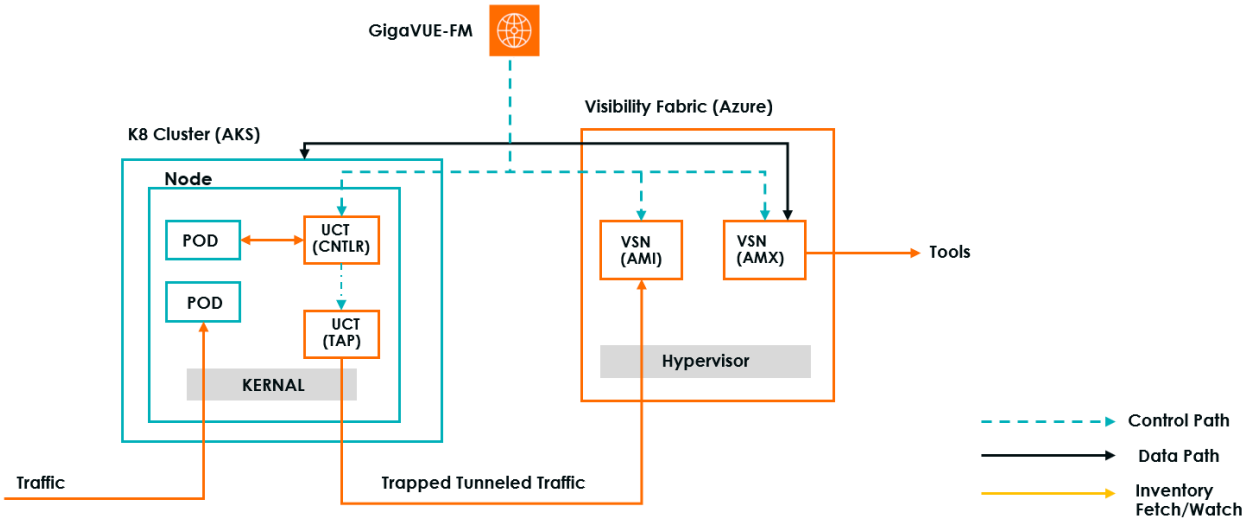


The enrichment supported depends on the type of platform. Refer to AWS for more details.

Export of GigaVUE Enriched Metadata for Cloud Workloads Kubernetes containers - Azure Kubernetes Service (AKS)

This feature enables the enrichment of flow records with Kubernetes inventory data, unlocking deeper visibility and advanced use cases for containerized environments. In the current Kubernetes visibility solution for AKS, UCT-TAP ships tapped traffic (both east-west and north-south) to the AMI node deployed in Azure. The AMI node then forwards metadata

to the AMX node, also deployed in Azure. With the new enhancement, the AMX node enriches the AMI metadata using Kubernetes inventory details fetched directly from the AKS cluster.



GigaVUE-FM queries the Kubernetes inventory every 300 seconds, which is the default interval for monitoring events between inventory fetches. The default inventory query interval should suffice in most cases; however the interval can be customized in extreme situations. Please contact Gigamon Support for assistance.

NOTE: In addition to sending regular queries every 300 seconds, GigaVUE-FM enables a watch mechanism that updates AMX with every event—create, delete, and modify.

For Kubernetes environments, GigaVUE-FM uses a controller with access to the Kubernetes API. The controller subscribes to cluster events and pushes updates in near real-time. No built-in optional services are required.

Refer to Prerequisites for Export of GigaVUE Enriched Metadata for Cloud Workloads for more detailed information.

Rules and Notes

- With any AMI entitlement (AMI SKU, ZTA bundle, or SecureVUE PLUS bundle), you are also entitled to deploy AMX.
- The GigaVUE V Series Node deployed must be entirely dedicated to the AMX application, it cannot have other applications in it.

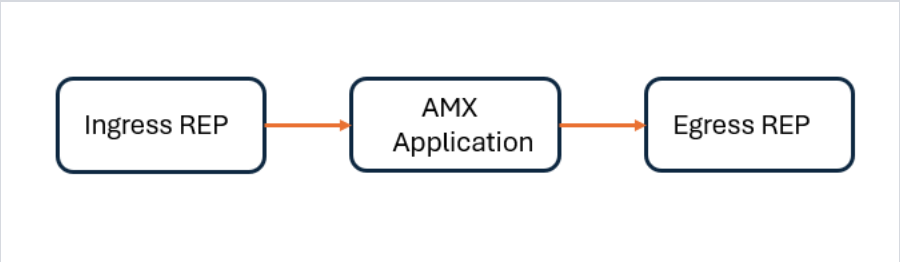
- The monitoring session can only have Raw End Point (REP), it cannot have other applications, maps, or tunnels when using the AMX application. Refer to *Create Raw Endpoint*section in GigaVUE Cloud Suite Deployment Guide - VMware (ESXi) for more detailed information on how to add a REP to the monitoring session and how to configure it.
- When using this application for production usage, it is recommended to use large size Virtual Machines.
- If you reload the GigaVUE V Series Node after configuring the AMX application, then the Ingestor in the AMX application fails.
- When using GigaVUE Enriched Metadata for Cloud Workloads, if duplicate IP address is assigned to workloads, the metadata received from the most recently queried workload will be enriched. Hence, it is not recommended to use the feature in environments that are prone to have duplicate IP addresses.
- When using GigaVUE Enriched Metadata for Cloud Workloads, endpoints and the GigaVUE V Series Node running AMI and AMX should be co-located in the same cloud platform.

Configure Application Metadata Exporter

NOTE: Refer to Prerequisites for Application Metadata Exporter topic for all information related to the prerequisites.

In GigaVUE-FM, you must do the following to configure the Application Metadata Exporter application in the Monitoring Session.

S.No	Steps	Refer to
1	Create an ingress REP	Create Raw Endpoint (VMware vCenter) Create Raw Endpoint (VMware NSX-T) Create Raw Endpoint (AWS) Create Raw Endpoint (Azure) Create Raw Endpoint (Third Party Orchestration)
2	Create a link between the ingress REP and Application Metadata Exporter application	N/A
3	Create an egress REP	Create Raw Endpoint (VMware vCenter) Create Raw Endpoint (VMware NSX-T) Create Raw Endpoint (AWS) Create Raw Endpoint (Azure) Create Raw Endpoint (Third Party Orchestration)
4	Create a link between the Application Metadata Exporter application and egress REP	N/A



To add AMX application:

1. Go to **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. The **Monitoring Session** page appears.

   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.
   - You can use the Third-Party Orchestration method when deploying fabric components—such as the AMX V Series Node—on your own.
   - When deploying AMX using the Third-Party Orchestration method, Monitoring Session must also be configured in the same work flow. To deploy through Third Party Orchestration, go to **Traffic > Virtual > Orchestrated Flows > Third Party Orchestration**.
   - Before deploying AMX, ensure to change the **Traffic Acquisition Method** to **Customer Orchestrated Source** in the Monitoring Domain. Refer to Create Monitoring Domain.

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. In the canvas, click the icon on the left side of the page to view the traffic processing elements. Drag and drop **AMX** from **APPLICATIONS** to the graphical workspace. The application quick view appears.
4. Enter the **Alias** for the application.

5. In the **Ingestor** section, enter or select the following details. Click to add another ingestor to add multiple inputs to the AMX application and click to remove an existing ingestor.

Fields	Description
Name	Enter name for the Ingestor.
Port	Enter the port number to which the Application Metadata or the NetFlow/IPFIX or the Control Plane metadata must be ingested.
Type	Select any one of the following: AMI - Select this option if the input is AMI. Mobility Control Plane - Select this option if the input is Control Plane Metadata. NetFlow/IPFIX - Select this option if the input type is NetFlow/IPFIX. **Note**: If your selected ingestor type is NetFlow/IPFIX, Metadata Enrichment will be disabled by default. NetFlow/IPFIX input type is not supported for Metadata Enrichment.

6. Enter or select the following details in the **Metadata Enrichment** section:

> You can use the **Actions** button to add multiple Metadata Enrichment. Keep in mind the following when configuring multiple Metadata Enrichment:
>
> - You can only configure either Mobility or Workload enrichment
> - You can only configure one Metadata enrichment with either **Mobility** or **Workload** as the **Type**
> - You can only configure a maximum of 5 Metadata enrichment with **Others** as the **Type**.

Fields	Description
Enrichment Name	Enter a unique name for each enrichment.
Enable	Use this option to enable the enrichment.
Type	Select the type from the drop-down menu. o Mobility o Workload o Others
Mobility	
Attribute Fields	Select the attributes from the list. You can use the **Select All** option to select all the available attributes. Refer to Control Plane Attributes for more detailed information on the list of available attributes and their description.
Workload	
Platforms	Select the platform in which your Workload Virtual Machines are present. • VMware vCenter • AWS • Azure • Kubernetes
Attribute Fields	Select the attributes from the list. You can use the **Select All** option to select all the available attributes. Refer to AWSfor more detailed information on the list of available attributes and their description. **Advanced Options** The advanced options allow you to configure additional details like interval and delay. Click **Add**. Enter the following details: o Enter the **Key**. o Enter the **Value**.
Source Information	Enter the details of the source. **Name**: Enter a unique name for each Source Information. The name should be unique across the ingestor and the source information. **Key**: The default keys for each platform are listed as follows. Click **+** to add more keys.

Fields	Description
	AWS: Refer to Manage access keys for IAM users section in AWS documentation for more detailed information on how to create an access key ID and a secret access key. ▪ aws_access_key_id ▪ aws_secret_access_key ▪ aws_region **Azure**: Refer to Register a Microsoft Entra app and create a service principal section in Azure documentation for more detailed information on how to configure client ID, client secret, tenant ID, and subscription ID in Azure. ▪ azure_client_id ▪ azure_client_secret ▪ azure_tenant_id ▪ azure_subscription_id **VMware**: ▪ url - The URL of VMware vCenter. ▪ username - Username of the VMware vCenter ▪ password - vCenter password used to connect to the vCenter ▪ self_signed_certificate **Kubernetes**: ▪ Upload **kubeconfig** YAML file from your local. Refer to Kubernetes for Prerequisites details. **Value**: Enter the value for the keys. This field is editable after saving the changes. **Secure Keys**: Use this option to mask the value. After saving the changes, **Secure Keys** and **Key** fields are disabled and the value is masked. Click ⊕ to add another Source Information and click ⊖ to remove a Source Information. You can add multiple Source Information if your workloads are across different vCenters, AWS Accounts, or Azure Subscriptions. You can create an individual Source Information for each of the vCenters, AWS Accounts, or Azure Subscriptions.
Others: Use this setting to perform custom mapping for advanced use cases. For details contact Gigamon Support.	
Attribute Fields	Click **Add** and enter the attribute.
Settings	Click **Add** and enter the details.

7. Enter or select the following details in **Cloud Tools Export** section:

Fields	Description
Alias	Enter the alias name for the cloud tool export.
Endpoint	Enter the endpoint URL where the cloud tool instance is installed and the ports are configured. Enable **Secure Endpoint** option to hide the API keys from the URL. Example: • Normal Endpoint: http://examples.com/mykey/key123 • Masked Endpoint: http://examples.com/mykey/****
Headers	Enter the custom header value of the cloud tool instance. Example: Add Content-Type: application/json in a separate header field. Ensure that the **Secure Keys** option is enabled.
Type	Select any one of the following: **AMI** - Select this option to export AMI. **Mobility Control**- Select this option to export control plane metadata. **AMI Enriched** - Select this option to export enriched metadata for cloud workloads. **NetFlow/IPFIX** - Select this option to export NetFlow/IPFIX packets to tools such as HTTPS or Kafka.
Account ID	Enter the account ID number of the selected Cloud Tool.
API Key	Enter the API key of the Cloud Tool.
Source IP Address	Source IP Address is needed when the egress interface is configured with multiple IP addresses. Configure the source IP address which is connected to the Cloud Tool. Both IPv4 and IPv6 are supported. This field is optional.
Enable Export	Enable the box to export the Application Metadata Intelligence output in JSON format.
Format	The default output format is JSON.
Zip	Enable the box to compress the output file. **Note**: Enable this field when using New Relic as the cloud tool.
Interval	The time interval (in seconds) in which the data should be uploaded periodically. The recommended minimum time interval is 10 seconds and the maximum time interval is 90 seconds.
Parallel Writer	Specifies the number of simultaneous JSON exports done.
Export Retries	The number of times the application tries to export the entries to Cloud Tool. The recommended minimum value is 4 and the maximum is 10.
Maximum Entries	The number of JSON entries in a file. The maximum number of allowed entries is 20000 and the minimum is 10, however 1000 is the default value.

Fields	Description
Backoff Reset Window	With a non-zero value, the exporter keeps trying to reach the tool as many times as the retry. The default setting is 0, and the Backoff Reset Window is disabled at this value.
Request Timeout	This is the time exporter waits for a response back from the tool. The default value is 10 seconds.
Labels	Click **Add**. Enter the following details: o Enter the **Key**. o Enter the **Value**. **Note**: Refer to the deployment guides of the respective cloud tools for configuring the Key and Value.

8. Enter or select the following details in the **Kafka Exports** section:

Fields	Description
Alias	Enter the alias name for the Kafka Export.
Topic	The topic name to push JSON streams to, which is generally given to users part of the Kafka administration.
Type	Select any one of the following: AMI - Select this option to export AMI. Mobility Control - Select this option to export control plane metadata. AMI Enriched - Select this option to export enriched metadata. NetFlow/IPFIX - Select this option to export NetFlow/IPFIX ingestor types.
Brokers	The URL that contains the Kafka cluster endpoints. Click ⊕ to add another broker and click ⊖ to remove an existing broker.
Source IP Address	Source IP Address is needed when the egress interface is configured with multiple IP addresses. Configure the source IP address which is connected to the Kafka Broker. Both IPv4 and IPv6 are supported. This field is optional.
Enable Export	Enable the box to export the Application Metadata Intelligence output in JSON format.
Format	The default output format is JSON.
Zip	Enable the box to compress the output file.
Interval	The time interval (in seconds) in which the data should be uploaded periodically. The recommended minimum time interval is 10 seconds and the maximum time interval is 90 seconds. The default time interval is 30 seconds.
Parallel Writer	Specifies the number of simultaneous JSON exports done.
Export Retries	The number of times the application tries to export the entries to Kafka. The recommended minimum value is 4 and the maximum is 10.
Maximum Entries	The number of JSON entries in a file. The maximum number of allowed entries is 20000 and the minimum is 10, however 1000 is the default value.

Fields	Description
Backoff Reset Window	With a non-zero value, the exporter keeps trying to reach the tool as many times as the retry. The default setting is 0, and the Backoff Reset Window is disabled at this value.
Labels	Click **Add**. Enter the following details: o Enter the **Key**. o Enter the **Value**.
Producer Configurations	Click **Add** to enter the authentication details if a Kafka broker needs authentication. For Example: • security.protocol=SASL_SSL • sasl.mechanism=PLAIN or sasl.mechanisms=PLAIN • sasl.username=username • sasl.password=password

9. Click **Save** to deploy the Monitoring Session. The **Select nodes to deploy the Monitoring Session** dialog box appears. Select the GigaVUE V Series Node for which you wish to deploy the Monitoring Session.
10. 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 all the V Series Nodes.

Switching to outer_ip for Mobility Enrichment

In 5G Control Plane (CP) records, only the lower 64 bits of the inner IP address are captured. To overcome this limitation, you can switch to outer_ip. Follow the steps below based on your configuration:

If AMX is already configured and the Monitoring Session is deployed:

1. Undeploy the Monitoring Session in GigaVUE-FM.
2. Create a new .yaml file in the GigaVUE V Series Node: vi /etc/amx_settings.yaml
3. Modify the enrichment mode:

```
# Default mobility enrichment mode: inner_ip (default) or outer_ip
mobility_outer_ip_version: <Enter version as v6 or v4>
mobility_enrichment_mode: outer_ip
```

4. Deploy the Monitoring Session.

During Initial AMX Configuration:

1. Create a new .yaml file in the GigaVUE V Series Node: vi /etc/amx_settings.yaml
2. Modify the enrichment mode:

```
# Default mobility enrichment mode: inner_ip (default) or outer_ip
mobility_outer_ip_version: <Enter version as v6 or v4>
mobility_enrichment_mode: outer_ip
```

3. Save the file and proceed with the deployment.

Application Monitoring Options

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. Refer to View Application Metadata Exporter Statistics for more detailed information.

Deploy Application Metadata Exporter in AWS using Third Party Orchestration

This section outlines the workflow for deploying Application Metadata Exporter (AMX) application using Third Party Orchestration on AWS.

Predeployment Checklist:

1. The minimum resource requirements for deploying V Series to configure AMX are as follows. You can deploy one or more V Series for deploying AMX subject to your traffic volume (flows per second). Contact Gigamon Support for sizing guidance, if needed.
   - **8 vCPUs, 16 GB memory, and 80 GB disk space** for exporting Application Metadata in JSON format.
   - **40 vCPUs, 64 GB RAM, 128 GB disk space** for exporting NetFlow/IPFIX records in JSON format.

   Exporting JSON records involves file read/write operations; using SSD storage is recommended.
2. Ensure you have a valid SecureVUE Plus VBL license to deploy AMX and to export NetFlow/IPFIX records in JSON format. With any AMI entitlement (AMI SKU, ZTA bundle, or SecureVUE PLUS bundle), you are also entitled to deploy AMX.

3. Ensure you have access to the VUE Gigamon Community portal for downloading V Series OVA image.
4. V Series requires three interfaces for deploying AMX—management, data, and tool. It is recommended to allocate dedicated interface for each. Create three separate subnets:
   a. A Management Port Group for connectivity to GigaVUE-FM
   b. A Data Port Group for receiving traffic such as application metadata in CEF or NetFlow/IPFIX formats, and
   c. A Tool Port Group for exporting JSON records.

   Note: Preparing a network topology with the IP layout helps in configuration, monitoring, and troubleshooting.
5. Select the appropriate deployment mode for the GigaVUE V Series node based on your requirements:
   - Single physical uplink for Management, Data and Tool connectivity.
   - Single physical uplink for Management and Tool connectivity, and another uplink for Data connectivity.
   - (Recommended) Separate uplinks (three) for Management, Data, and Tool connectivity.
6. If static IP addressing is used, obtain the following details from your server team:
   - IP addresses for the management, data, and tool interfaces.
   - IP address of the DNS server and the gateway connected to the tool interface.
   - Subnet Mask and MTU.
7. Verify whether remote web console access to the V Series is available. Console access is required for troubleshooting. If remote access is not available, request the server team to enable SSH access.
8. Review the deployment guide for the tool specific configuration needed to export records from AMX. Refer to AMX Tool Integration.
9. Review the connectivity requirements for GigaVUE-FM, AMI, AMX, and the associated tools in your environment. Ensure that the required ports are open and any external connectivity dependencies are addressed.
10. Ensure that the standalone GigaVUE-FM deployment meets the recommended requirements shown in the following table. For medium and large scale deployments, refer to Recommended Requirements for GigaVUE-FM Deployments. This step is optional. A standalone GigaVUE-FM instance is required only when an existing GigaVUE-FM is not available for managing AMX.

Requirements	Small Scale Deployment
CPU	
CPU count(minimum)	2
CPU Min speed (per CPU)	2.30GHz
Memory	
Memory Size	16GB
Disk Space	
OS Disk Size (min)	40GB
Config Disk Size - 15 Days Data	80GB
Config Disk Size - 35 Days Data	160GB
Config Disk Size - Rollup 35 Days + 120 Days Rollup	200GB
NIC	1
Number of NICs	1GB
Management/Data	
Appliance Scalability	Up to 50
Number of GigaVUE HC Series/GigaVUE TA Series Devices	Up to 50
Number of GigaVUE V Series Nodes	1 Cluster with 100 Nodes and 10000 pods with 2 rules
Number of Worker Pods monitored	

Refer to the following topics to deploy AMX using Third Party Orchestration:

- (Optional) Install GigaVUE-FM on AWS
- (Optional) Configure Metadata Export Filter for AMX
- (Optional) Configure Role-Based Access for Third Party Orchestration
- Create Monitoring Domain to Acquire Traffic from Customer Orchestrated Source
- Create Tokens to Secure REST API and Third Party Orchestration Access to GigaVUE-FM
- Deploy V Series Node and Register with GigaVUE-FM
- Create a Monitoring Session to Configure Application Metadata Exporter
- Configure Ingestor in AMX to Process Traffic
- Integrate AMX with Third Party Tool
- Configure Exporter to Export Attributes to Third Party tools
- Verify Your Deployment

(Optional) Install GigaVUE-FM on AWS

You can subscribe to GigaVUE-FM in the marketplace and launch in AWS.

Refer to the following topics for instruction on installing GigaVUE-FM in AWS:

- Subscribe to GigaVUE-FM
- Initial Configuration

Subscribe to GigaVUE-FM

You can deploy the GigaVUE Cloud Suite for AWS from the AWS Marketplace.

NOTE: Only users with **aws-marketplace:ViewSubscriptions** permission in their IAM policy can subscribe to GigaVUE products.

To subscribe to the GigaVUE-FM, perform the following steps:

1. Log in to your AWS account.
2. Go to AWS Marketplace: https://aws.amazon.com/marketplace/.
3. In the **Search** field, type Gigamon and select **Search**.
4. Select the latest version GigaVUE Cloud Suite BYOL version. For details, refer to Licensing.
5. Select **View Purchase Options**. The terms and condition page is displayed.
6. Review the Terms and Conditions and select **"Accept Terms**".
7. Review the summary and then select **Continue to Configuration**.
8. In the **Configure this software** page, enter the following details for your deployment:
   a. Set **Fulfillment Option** to the default value.
   b. Select the latest version in the **Software Version** field.
   c. Choose your deployment **Region**.
   d. Select **Continue to Launch.**

9. In the **Configure this software** page, perform the following:
    a. In the **Choose Action** field, select the **Launch from Website** option.
    b. From the **EC2 Instance Type** drop-down list, select the instance type. Refer to Recommended and Supported Instance Types for AWS.
    c. From the **VPC Settings** drop-down list, select the VPC for deploying GigaVUE-FM.
    d. In the **Subnet Settings**, select your desired Subnet.
    e. In the **Security Group Settings**, configure the security group to match your access and permissions needs. For details, refer to Security Group.
    f. Select your preferred **Key Pair** for secure access to the instance.
    g. In the **Advanced details** section, select **V2 only (token required)** from the Metadata version drop-down list.
    h. Select **Launch**.

For details, refer to Launch an instance using defined parameters in AWS documentation.

GigaVUE-FM is launched in AWS. You must perform the initial configuration to view the GigaVUE-FM UI.

Initial Configuration

It may take several minutes for the GigaVUE-FM instance to start up. Once it is up and running, perform the following steps to verify:

1. In your EC2 Instances page, select the **Instance ID** of the launched GigaVUE-FM to view the instance information.
2. Copy and paste the **Public IP address** into a new browser window or tab.
   The GigaVUE-FM GUI appears.

NOTE:

- If GigaVUE-FM is deployed inside AWS, use **admin** as the username and the **Instance ID** as the default password for the admin user to login to GigaVUE-FM, (Ex: i-079173111e2d73753). You can get the **Instance ID** of GigaVUE-FM in the EC2 Instances page.
- If GigaVUE-FM is deployed outside the AWS, use admin123A!! as the default admin password.

When you first log in to GigaVUE-FM, you are asked to change your default password.

What to do Next:

Configure the required permission and privileges in AWS. For detailed instructions on configuring required AWS permissions and privileges for your chosen deployment option, refer to the following topics:

Deployment Options	Reference Topics
Acquire Traffic using UCT-V	Acquire Traffic using UCT-V - GigaVUE-FM Orchestration
Acquire Traffic using Customer Orchestrated Source	Acquire Traffic using Customer Orchestrated Source - GigaVUE-FM Orchestration
Acquire Traffic using Customer Orchestrated Source when configuring Gateway Load Balancer in AWS	Acquire Traffic using Customer Orchestrated Source with Gateway Load Balancing
Acquire Traffic using Customer Orchestrated Source when configuring Network Load Balancer in AWS	Acquire Traffic using Customer Orchestrated Source with Network Load Balancer
Acquire Traffic using Traffic Mirroring	Acquire Traffic using Traffic Mirroring – GigaVUE-FM Orchestration
Acquire Traffic using Traffic Mirroring when configuring Gateway Load Balancer in AWS	Acquire Traffic using Traffic Mirroring with Gateway Load Balancing
Acquire Traffic using Traffic Mirroring when configuring Network Load Balancer in AWS	Acquire Traffic using Traffic Mirroring with Network Load Balancer

(Optional) Configure Metadata Export Filter for AMX

Optionally, you can configure an export filter to control which metadata records are exported from AMX. For more information, see Configure Metadata Export Filter.

(Optional) Configure Role-Based Access for Third Party Orchestration

If you do not want to use an **Admin Profile** to deploy GigaVUE V Series through a Third Party orchestrator, you can create the required users, roles, and user groups in GigaVUE-FM.

Create a Custom User

You can add users only if you are a user with **fm_super_admin role** or a user with either read or write access to the GigaVUE-FM security Management category.

To add users:

1. Go to **Settings** and select **Authentication** > **GigaVUE-FM User Management > Users**.
2. On the User page, select **New User**.
3. In the Add User page, enter the following details:
   - **Name:** Actual name of the user
   - **Username**: User name configured in GigaVUE-FM
   - **Email**: Email ID of the user
   - **Password/Confirm Password**: Password for the user. For more details, refer to Change Your Password.
   - **User Group:** Select the desired User Group to associate the user.

   GigaVUE-FM prompts for your password.
4. Click **Ok**. The new user is added.

Create a Custom Role and Assign the User

A user role defines permission for users to perform any task or operation in GigaVUE-FM or on the managed device. You can associate a role with user.

NOTE: A user with read-only access cannot perform configurations on the screen. The menus and action buttons in the UI pages are disabled appropriately.

To create a role:

1. Go to **Settings** and select **Authentication> GigaVUE-FM User Management >Roles**.
2. Select **New Role**.
3. In the New Role page, select or enter the following details:
   - **Role Name**: Name of the role.
   - **Description**: Description of the role.
   - **Select Permission**: From the **Select Permissions** tab, select **Third Party Orchestration**, and provide write permissions.
4. Select **Apply** to save the configuration.

Create a Custom User Group and Assign the Custom Role and the User

A user group consists of a set of roles and set of tags associated with users in that group. You can associate the user to one or more groups.

To create a new user group:

1. Go to **Settings**, and then select **Authentication> GigaVUE-FMUser Management >User Groups**.

2. Select **New Group.**
3. In the New User Group page, select **Next** to progress forward and **Back** to navigate backward.
4. In the **Group Info** tab, enter the Group Name and Description details:
5. In the **Assign Roles** tab, select the role that you want to assign to the user group.
6. In the **Assign Tags** tab, select the required tag key and tag value.
7. In the **Assign Users** tab, select the required users.
8. Select **Apply** to save the configuration. The new user group is added.

Create Monitoring Domain to Acquire Traffic from Customer Orchestrated Source

To create a Monitoring Domain in GigaVUE-FM:

1. Go to **Inventory > VIRTUAL > Third Party Orchestration**, and select **Monitoring Domain**. The **Monitoring Domain** page appears.
2. On the **Monitoring Domain** page, select **New**. The **Monitoring Domain Configuration page** appears.
3. Enter a name for the **Monitoring Domain**.
4. Enter a name for the **Connection**.
5. Select **Customer Orchestrated Source** as the **Traffic Acquisition Method**.
6. Click **Save**.

Create Tokens to Secure REST API and Third Party Orchestration Access to GigaVUE-FM

Use tokens when applications or users access GigaVUE-FM through REST APIs or when registering GigaVUE V Series using Third Party Orchestration. Tokens let GigaVUE-FM verify who is making the API calls and what they are allowed to do, without exposing passwords.

You can create tokens only if you are a user with **fm_super_admin role** or a user with write access to the GigaVUE-FM security Management category.

To create a token:

1. Go to **Settings > Authentication** > **GigaVUE-FM User Management**. The **User Management** page appears.
2. Select **Current User Tokens** from the **Tokens** drop-down list.

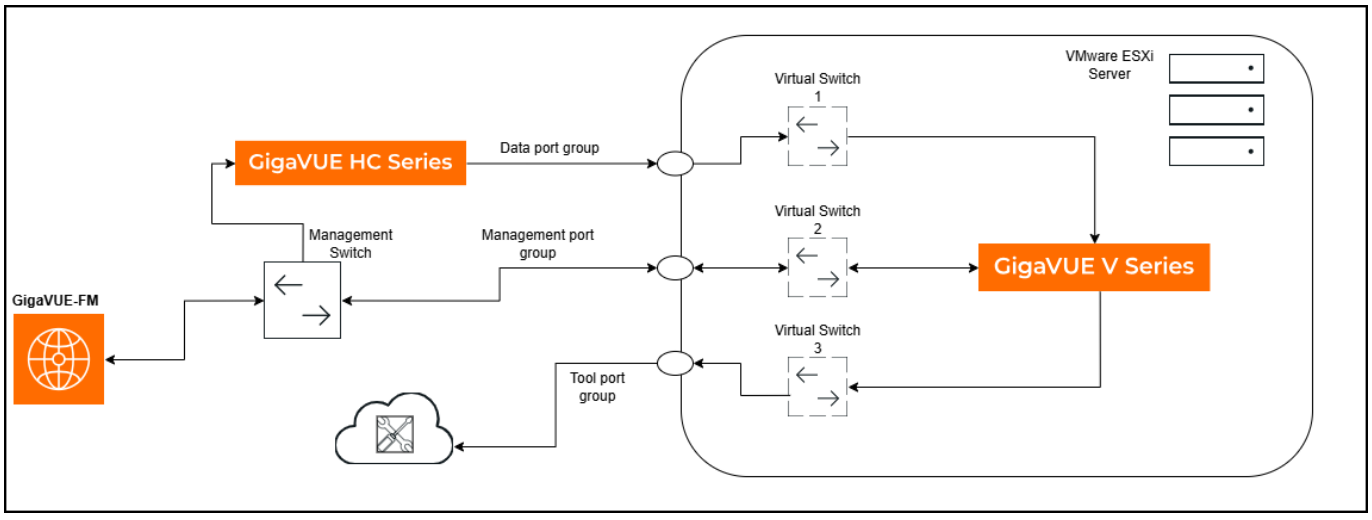
3. Click **New Token**. The **New Token** pop-up appears.
4. Enter a name for the new token in the **Name** field.
5. Enter the days until the token is valid in the **Expiry** field.
6. Select the user group for which you are privileged to access the GigaVUE-FM from the **User Group** drop-down list. The token inherits the read or write RBAC privileges of this group.
7. Select **OK** to generate a new token. You can copy and use the generated token to authenticate the GigaVUE-FM REST APIs.

Deploy V Series Node and Register with GigaVUE-FM

The following image illustrates a scenario for deploying and registering a GigaVUE V Series node. In this example, a GigaVUE HC Series device monitors north-south traffic and forwards Application Metadata to a SIEM/observability tool that accepts only JSON records. The entire solution is managed through GigaVUE-FM.

The GigaVUE HC Series uses Application Metadata Intelligence to generate application metadata in CEF format. Application Metadata Exporter, running on the GigaVUE V Series node, converts these CEF records to JSON before exporting them to the tool over HTTPS or Kafka.

NOTE: AMI is supported on both GigaVUE HC Series and GigaVUE V Series platforms. You can also deploy a separate GigaVUE V Series node to generate application metadata for monitoring east-west traffic.



To deploy and register:

1. Log into the vSphere or VMware ESXi web interface.
2. Right-click the ESXi Host, Cluster or data center (if using vSphere) on which you want to deploy the GigaVUE V Series Node and then select **Create/Register VM**. The **New Virtual Machine** wizard appears.
3. In the **Select Creation Type** page, select Deploy a virtual machine from an OVF and OVA file option. Downloaded the AMX supported OVA from the VUE Gigamon Community portal. Extract the OVA to obtain the OVF and VMDK files, then select **vseries-node-file-ovf15.ovf** (AMX-supported OVF that brings up three interfaces) for the AMX deployment.
4. Click **Next**. The **Select OVF and VMDK files** page appears.
5. In the **Select and VMDK files** page, enter a unique name for the virtual machine and upload the .ovf and .vmdk files from your local machine.
6. Click **Next** and the **Select storage** page appears.
7. Select a datastore where the virtual machine's files will be stored.
8. Click **Next**. The **Deployment Options** page appears.
9. In the **Deployment Options** page, select the management port, data port, and tool port as referenced in the prerequisites.
   a. Select the **Deployment Type** from the list:
      - Do Not Use DHCP – Select this option if you want to use static IP addresses for the management, data, and tool ports.
      - Management, Data and Tool Port DHCP – Select this option if you want to use dynamic IP addresses for the management, data, and tool ports.
      - Management Port DHCP – Select this option if you want to use dynamic IP address only for the management port.
      - Tool Port DHCP - Select this option if you want to use dynamic IP address only for the tool port.
      - Data Port DHCP – Select this option if you want to use dynamic IP address only for the data port.

   b. Select Thin/Thick in the **Disk Provisioning** field.

   c. Unselect the **Power on automatically** check box. This is selected by default. It is recommended to disable the Power on automatically option and review all configuration before switching on the virtual machine.
10. Click **Next**. The **Additional Settings** page appears.
11. Do the following configuration in the **Additional Settings** page.
    a. In the **System** section, enter the hostname of the V Series node instance in the **Hostname** field and create a new admin password for the V Series node instance in the **Administrative Login Password** field.

This credential will be used for V series SSH access. The default username is gigamon. If the deployment fails, you can login to V Series SSH/Console and check the logs for troubleshooting.

b. In the **Network Connectivity** section, enter the required fields based on the selected network configuration.

> **NOTE:** Ensure to unselect the **Management Port DHCP** checkbox if you want to use static IP address for the management port. If you select the Management Port DHCP checkbox, dynamic IP address will be configured for the management port even if you have selected Do Not Use DHCP option in the Configuration page.

c. Enter the required value in the **Management Port MTU size in bytes** field. The default value is 1500B.

d. Enter the DNS server address in the **Nameserver** field to resolve the domain name of the tool destination URL.

e. In the **Optional Parameters** section, enter the Monitoring Domain name in the **GroupName** field and connection name in the **SubGroupName** field. The Monitoring Domain and connection name corresponds to the domain name and connection that you created during the Create Monitoring Domain to Acquire Traffic from Customer Orchestrated Source configuration.

f. Enter the token created in GigaVUE-FM in the **JWT Token used for registration** field. Refer to Create Tokens to Secure REST API and Third Party Orchestration Access to GigaVUE-FM.

g. Enter the GigaVUE-FM IP address and remote port in the **RemoteIP** and **RemotePort** fields respectively. In case of any error, you should re-deploy the V Series.

h. In the **Custom node properties** field enter app_mode=linux_apps (mandatory).

12. Click **Next** and the **Ready to complete** page appears.
13. Review all the entered information and modify the configuration if required.
14. Click **Finish**. When the operation completes, you have successfully deployed a GigaVUE V Series Node.

Verify GigaVUE V Series Node Registration

During the initial bring up, the V Series reboots multiple times for initialization. After few minutes, you can check the status of the deployment in GigaVUE-FM. If the status is failed, you can check the logs to perform troubleshooting.

To check the logs:

1. Log in to V Series Node via console or SSH to management IP address.
2. Enter the below path in the terminal to check the registration details.

   ```
   tail -f /var/log/vseries-node-reg.log
   ```

A single AMX instance processes traffic within the published performance KPIs. Deploy additional instances when traffic volume exceeds these thresholds or when packet drops occur, or CPU or memory utilization remains consistently high, to maintain stable and efficient performance. For details regarding performance KPIs, Contact Technical Support.

Create a Monitoring Session to Configure Application Metadata Exporter

In GigaVUE-FM, you must do the following to configure the Application Metadata Exporter application in the Monitoring Session.

1. **Access the Monitoring Session Page**:
   a. In GigaVUE-FM, go to **Traffic** > **Virtual** > **Orchestrated Flows > Third Party Orchestration**.
   b. 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.
2. **Create an ingress REP**:
   a. In the canvas, from the New expand menu, drag and drop New Raw Endpoint to the graphical workspace.
   b. On the new raw endpoint icon, select the ⋮ menu button and select **Details**. The **Raw** quick view page appears.
   c. Enter the Alias and Description details for the Ingress Raw End Point and click **Save**.
3. **Add AMX Application**:
   a. In the canvas, from the **Applications** expand menu, drag and drop AMX to the graphical workspace.
   b. Configure the ingestor settings to process traffic. Refer to Configure Ingestor in AMX to Process Traffic for details.
   c. Configure the required exporter settings to export attributes to Third Party tools. Refer to Configure Exporter to Export Attributes to Third Party tools for details.
   d. Create a link between the ingress REP and Application Metadata Exporter application.

4. **Create an egress REP**:
   a. From the **New** expand menu, drag and drop New Raw Endpoint to the graphical workspace.
   b. On the new raw endpoint icon, select the ⋮ menu button and select **Details**. The **Raw** quick view page appears.
   c. Enter the Alias and Description details for the Egress Raw End Point and click **Save**.
   d. Create a link between the Application Metadata Exporter application and egress REP

> **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.
> - When deploying AMX using the Third-Party Orchestration method, Monitoring Session must also be configured in the same work flow.

Configure Ingestor in AMX to Process Traffic

The following scenarios provide more information about the different ways to configure Ingestor AMX:

- Scenario 1 - Export Application Metadata in JSON format over HTTPS/Kafka
- Scenario 2 - Export GigaVUE Enriched Metadata for Mobile Networks and Export over HTTPS/Kafka
- Scenario 3 - Export GigaVUE Enriched Metadata for Cloud Workloads and Export over HTTPS/Kafka
- Scenario 4 - Transform NetFlow/IPFIX records to JSON format and export over HTTPS/Kafka
- Scenario 5 - Configure Identity Enrichment Metadata using Zscaler Private Access (ZPA)

Scenario 1 - Export Application Metadata in JSON format over HTTPS/Kafka

Refer to Application Metadata Exporter - Export Scenarios topic for more details and conceptual information.

To configure ingestor for AMI:

1. On the AMX quick view in the **Ingestor** section, enter an alias name for the ingestor.

2. In the **Type** field, select **AMI** as the input type.
3. Enter the port number on which Application Metadata must be ingested. The default port value is 514.
4. Click ⊕ to add another ingestor to add multiple inputs to the AMX application and click ⊖ to remove an existing ingestor.

Scenario 2 - Export GigaVUE Enriched Metadata for Mobile Networks and Export over HTTPS/Kafka

Refer to Application Metadata Exporter - Export Scenarios topic for more details and conceptual information.

To export GigaVUE Enriched Metadata for Mobile Workloads:

1. On the AMX quick view in the **Ingestor** section, enter an alias name for the ingestor.
2. In the **Type** field, select **AMI** as the input type.
3. Enter the port number on which Application Metadata must be ingested. The default port value is 514.
4. Click ⊕ to add another ingestor.
5. In the Type field, select **Mobility Control Plane** as the input type.
6. Enter the port number on which application metadata must be ingested.
7. Click ⊕ again to add another ingestor to add multiple inputs to the AMX application and click ⊖ to remove an existing ingestor.
8. In the **Metadata Enrichment** section, enter a unique name for the enrichment.
9. Select the Enable option to enable the enrichment.
10. Select **Mobility** from the **Type** drop-down menu.
11. Select the required attributes from the list. You can use **Select All** to choose all available attributes. Refer to the Control Plane Attributes for more details.

Scenario 3 - Export GigaVUE Enriched Metadata for Cloud Workloads and Export over HTTPS/Kafka

Refer to Application Metadata Exporter - Export Scenarios topic for more details and conceptual information.

To export GigaVUE Enriched Metadata for Cloud Workloads:

1. On the AMX quick view in the **Ingestor** section, enter an alias name for the ingestor.
2. In the Type field, select **AMI** as the input type.
3. Enter the port number on which Application Metadata must be ingested. The default port value is 514.
4. Click ⊕ to add another ingestor.
5. In the Type field, select **Mobility Control Plane** as the input type.
6. Enter the port number on which Application Metadata must be ingested.
7. Click ⊕ again to add another ingestor to add multiple inputs to the AMX application and click ⊖ to remove an existing ingestor.
8. In the **Metadata Enrichment** section, enter a unique name for the enrichment.
9. Select the Enable option to enable the enrichment.
10. Select **Workload** from the **Type** drop down menu.
11. Select the platform as **VMware VCenter** from the drop down list.
12. Select the required attributes from the list. You can use **Select All** to choose all available attributes. Refer to the AWS for more details.

Scenario 4 - Transform NetFlow/IPFIX records to JSON format and export over HTTPS/Kafka

Refer to Application Metadata Exporter - Export Scenarios topic for more details and conceptual information.

To configure ingestor for NetFlow/IPFIX:

1. On the AMX quick view in the **Ingestor** section, enter an alias name for the ingestor.
2. In the Type field, select the input type as **NetFlow/IPFIX**. Only the elements specified in the mapping file will be included in the JSON output. Editing or customizing the mapping file is not supported. Refer to Supported Element Types for NetFlow Integrator Element Mapping.
3. Enter the port number on which NetFlow/IPFIX must be ingested. The default port value is 2055.

4. Click to add another ingestor to add multiple inputs to the AMX application and click to remove an existing ingestor. A maximum of 12 NetFlow/IPFIX type ingestors can be configured per deployment.

   NOTE: If you select NetFlow/IPFIX as the ingestor type, Metadata Enrichment is disabled by default. Metadata Enrichment is not supported for NetFlow/IPFIX inputs.

Scenario 5 - Configure Identity Enrichment Metadata using Zscaler Private Access (ZPA)

Refer to Application Metadata Exporter - Export Scenarios topic for more details and conceptual information.

Prerequisites

Before configuring identity enrichment using Zscaler Private Access (ZPA), ensure that the following prerequisites are met.

Zscaler Infrastructure

The following Zscaler components must already be set up in your environment. These are standard ZPA deployment requirements. For detailed instructions, refer to the Zscaler documentation.

- **Acquire Zscaler Tenant Access**: Ensure that you have admin access to the Zscaler Private Access admin portal (ZPA tenant). Refer to Zscaler Tenant Access for more information.
- **Integrate Identity Provider (IdP)**: An IdP (such as Okta, Microsoft Azure AD, or any supported IdP) must be configured and integrated with ZPA. ZPA uses the IdP to authenticate users before granting access to private applications. Refer to About External Identity Providers for more information.
- **Configure App Connector Group** : At least one App Connector group must be created and have active App Connectors registered to it. You can use an existing App Connector group or create a new one before proceeding. For instructions, refer to the Zscaler documentation. Refer to Configuring App Connector Groups for more information.
- **Install App Connector**: The Zscaler App Connector package must be downloaded and installed on a Linux-based VM (Ubuntu, plain Linux, or similar) in the domain where your private applications reside. Refer to the scaler App Connector deployment guide for platform-specific instructions (Linux, Docker, GCP, Kubernetes, and so on). Refer to App Connectors for more information.

- **Define Private Applications**: Application segments must be created for all private applications you want to monitor (for example, internal web apps, Jira, databases). Each application segment must include the application IP address and port range, and must be linked to a server group and an App Connector group. Refer to Configuring Defined Application Segments for more information.

Gigamon Infrastructure

- **Deploy VSN Node with AMX on ESXi**: The Application Metadata Exporter (AMX) must be deployed on a V Series Node (VSN). In this release, only the ESXi platform is supported. The IP address of the VSN node on which AMX is running, as it is required when configuring the ZPA Log Receiver. Refer to Deploy V Series Node and Register with GigaVUE-FM for more information.
- **Configure AMI**: Application Metadata Intelligence (AMI) must be active and generating flow records. The AMI metadata (source IP, destination IP, source port, destination port) is used to match and enrich flows with ZPA log data. For more information on configuring AMI, refer to Configure Application Metadata Intelligence for Virtual Environment.

Integrate ZPA with Gigamon AMX

After the Zscaler infrastructure and Gigamon infrastructure are set up, configure a Log Receiver in the ZPA admin portal to stream ZPA logs to AMX. This is the key step that establishes the integration between ZPA and Gigamon.

The following table lists the specific options you must select when configuring a log receiver to integrate with AMX. For navigation steps and detailed instructions, refer to Configuring Log Receiver topic in Zscaler documentation.

Parameters	Description
Log Receiver	
Name	Enter a name for the log receiver.
Domain or IP Address	Enter the domain or IP address to the IP address of the VSN node on which AMX is deployed (not the ESXi host IP address).
TCP Port	Enter the same port that is configured as the ZPA LSS ingestor port on AMX.
App Connector Groups	Select an app connector group that was created.
Log Stream	
Log Type	Select User Activity as the log type.
Log Template	Select the Custom template.
Log Stream Content	Add the new user activity log ("ConnectionSetupTime": %j {ConnectionSetupTime} }\n) in the content.

Configure Ingestor for AMX

You can configure metadata enrichment for ZPA only. Optionally, you can combine it with GEM for Cloud Workloads for VMware vCenter.

To export identity enrichment metadata using ZPA :

1. Configure an ingestor for AMX
   a. On the AMX quick view in the **Ingestor** section, enter an alias name for the ingestor.
   b. In the **Type** field, select **AMI** as the input type.
   c. Enter the port number on which application metadata must be ingested. The default port value is 514.
   d. Click ⊕ to add another ingestor to add multiple inputs to the AMX application and click ⊖ to remove an existing ingestor.
2. Configure identity metadata enrichment using ZPA
   a. On the AMX quick view in the **Metadata Enrichment** section, enter an alias for the enrichment.
   b. Select the **Enable** option to enable the enrichment.
   c. In the **Type** field, select **Identity** as the input type.
   d. Select **Zscaler Private Access** from the **Platform** dropdown list.
   e. Select the attributes for identity enrichment from the **Attributes** tab.
   f. In the **Source Information** tab, enter the port number on which AMX receives the ZPA LSS logs.
   g. Click ⊕ to add another ZPA source information to add multiple inputs to the AMX application and click ⊖ to remove an existing source information.
3. (Optional) Configure GigaVUE Enriched Metadata workload for ESXi
   a. On the AMX quick view in the **Metadata Enrichment** section, enter an alias for the enrichment.
   b. Select the Enable option to enable the enrichment.
   c. In the **Type** field, select **Workload** as the input type.
   d. Select **VMware vCenter** from the **Platform** dropdown list.

> **NOTE:** Only VMware vcenter platform is applicable as additional workload along with ZPA.

e. Select the required workload attributes for ESXi.

f. In the Source Information tab, enter the Key-Value pair details as given:

- Key - url and Value - Primary URL for the vCenter Server SDK. For example, https://<vCenter-IP-or-FQDN>/sdk.
- Key - username and Value - VMware vCenter username.
- Key - password and Value - vCenter password.

g. Click ⊕ to add another ESXi source information to add multiple inputs to the AMX application and click ⊖ to remove an existing source information.

Integrate AMX with Third Party Tool

This section explains how to set up the third-party tool and configure the exporter settings required to route application metadata attributes for analysis and visualization.

Set up the Third Party Tool for AMX Integration

You must set up the third party tools to ingest and visualize application metadata.

Refer to AMX Tool Integration for configuration guidance and the verification steps required to confirm that data export and visualization are functioning correctly.

Configure Exporter to Export Attributes to Third Party tools

AMX supports the following types of exporters:

- Configure Cloud Tool Exporter
- Configure Kafka Exporter

Configure Cloud Tool Exporter

To configure Cloud Tool Export settings in AMX:

1. On the AMX quick view in the **Cloud Tool Exports** section, enter or select the required details as described in Cloud Tool Exporter - Field References.
2. Click **Save**.

Deploy the Monitoring Session

1. Click **Deploy** from the **Actions** menu.
2. The **Select nodes to deploy the Monitoring Session** dialog box appears. Select the GigaVUE V Series Node for which you wish to map the interfaces and deploy the Monitoring Session.
3. Select the interfaces for the ingress and egress REPs configured in the Monitoring Session. The interface naming includes the type and IP address of the interface, for example, DATA (ens192) IPv4: 10.114.42.135 IPv6: fcab:0:1:2040:a0a1:874e:7a66:40a2.
4. Select **Deploy**. Once deployed, the status is displayed as **Success** in the Monitoring Sessions **Sources** tab. The session is successfully deployed on the selected V Series Node.

Cloud Tool Exporter - Field References

Fields	Description
Alias	Enter the alias name for the cloud tool export.
Endpoint	Enter the endpoint URL where the cloud tool instance is installed and the ports are configured. Enable **Secure Endpoint** option to hide the API keys from the URL. Example: • Normal Endpoint: http://examples.com/mykey/key123 • Masked Endpoint: http://examples.com/mykey/****
Headers	Enter the custom header value of the cloud tool instance. Example: Add Content-Type: application/json in a separate header field. Ensure that the **Secure Keys** option is enabled.
Type	Select any one of the following: **AMI** - Select this option to export AMI or identity enrichment metadata **Mobility Control**- Select this option to export control plane metadata. **AMI Enriched** - Select this option to export enriched metadata for cloud workloads and identity enrichment using ZPA. **NetFlow/IPFIX** - Select this option to transform NetFlow/IPFIX records to JSON format.
Labels	Click **Add**. Enter the following details: o Enter the **Key**. o Enter the **Value**. **Note**: Refer to the deployment guides of the respective cloud tools for configuring the Key and Value.
Advanced Settings	
Enable Export	Enable the box to export the Application Metadata Intelligence output in JSON format.
Zip	Enable the box to compress the output file. **Note**: Enable this field when using New Relic as the cloud tool.
Interval (sec)	The time interval (in seconds) in which the data should be uploaded periodically. The

Fields	Description
	recommended minimum time interval is 10 seconds and the maximum time interval is 90 seconds.
Parallel Writer	Specifies the number of simultaneous JSON exports done.
Max Entries	The number of JSON entries in a file. The valid range is 5000–20000 and the default value is 5000.
Request Timeout	This is the time exporter waits for a response back from the tool. The default value is 10 seconds.
Source IP Address	Source IP Address is needed when the egress interface is configured with multiple IP addresses. Configure the source IP address which is connected to the Cloud Tool. Both IPv4 and IPv6 are supported. This field is optional.

Configure Kafka Exporter

To configure Kafka Export settings in AMX:

1. On the AMX quick view in the **Kafka Exports** section, enter or select the required details as described in Kafka Exporter - Field References.
2. Click **Save**.

Deploy the Monitoring Session

1. Click **Deploy** from the **Actions** menu.
2. The **Select nodes to deploy the Monitoring Session** dialog box appears. Select the GigaVUE V Series Node for which you wish to map the interfaces and deploy the Monitoring Session.
3. Select the interfaces for the ingress and egress REPs configured in the Monitoring Session. The interface naming includes the type and IP address of the interface for example, DATA (ens192) IPv4: 10.114.42.135 IPv6: fcab:0:1:2040:a0a1:874e:7a66:40a2.
4. Select **Deploy**. Once deployed, the status is displayed as **Success** in the Monitoring Sessions **Sources** tab. The session is successfully deployed on the selected V Series Node.

Kafka Exporter - Field References

Fields	Description
Alias	Enter the alias name for the Kafka Export.
Topic	The topic name to push JSON streams to, which is generally given to users part of the Kafka administration.
Type	Select any one of the following: **AMI** - Select this option to export AMI or identity enrichment metadata **Mobility Control** - Select this option to export control plane metadata.

Fields	Description
	AMI Enriched - Select this option to export enriched metadata for cloud workloads and identity enrichment using ZPA. **NetFlow/IPFIX** - Select this option to export NetFlow/IPFIX ingestor types.
Brokers	The URL that contains the Kafka cluster endpoints. Click ⊕ to add another broker and click ⊖ to remove an existing broker.
Labels	Click **Add**. Enter the following details: o Enter the **Key**. o Enter the **Value**.
Advanced Settings	
Enable Export	Enable the box to export the Application Metadata Intelligence output in JSON format.
Interval	The time interval (in seconds) in which the data should be uploaded periodically. The recommended minimum time interval is 10 seconds and the maximum time interval is 90 seconds. The default time interval is 30 seconds.
Parallel Writer	Specifies the number of simultaneous JSON exports done.
Max Entries	The number of JSON entries in a file. The valid range is 5000–20000 and the default value is 5000.
Source IP Address	Source IP Address is needed when the egress interface is configured with multiple IP addresses. Configure the source IP address which is connected to the Kafka Broker. Both IPv4 and IPv6 are supported. This field is optional.
Producer Configurations	Click **Add** to enter the authentication details if a Kafka broker needs authentication. For Example: • security.protocol=SASL_SSL • sasl.mechanism=PLAIN or sasl.mechanisms=PLAIN • sasl.username=username • sasl.password=password
Message Configurations	Use this field to specify custom Kafka message settings, such as partition key selection, that GigaVUE-FM passes to the Kafka exporter within the Application Metadata Exporter application. Valid values are: • **Key** - partition.key and **Value** - flow_id, five_tuple, three_tuple, round_robin (default) • **Key** - partition.keyRotateInterval and **Value** - <seconds> (default: 3600; range: 60–86400). This key is rotated every <value> seconds, and this rotated key is used as a fallback when the selected key option (flow_id, three_tuple, or five_tuple) cannot be determined for a record. **NOTE:** If the five_tuple option is selected, but port attributes are not found in the record, the partition selection will be determined using the three_tuple.

Verify Your Deployment

You can view the Ingestor, Exporter and Enrichment statistics for the deployed Monitoring Session in the **TRAFFIC PROCESSING** tab. For more details, refer to View Application Metadata Exporter Statistics.

To troubleshoot any issues in Application Metadata Exporter deployment, refer to Troubleshoot Application Metadata Exporter Deployment.

View Application Metadata Exporter Statistics

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

1. Go to **Traffic > Virtual > Orchestrated Flows > Third Party Orchestration**. The **Monitoring Sessions** Overview page appears.
2. Select the monitoring session you want to view the statistics.
3. Go to the **TRAFFIC PROCESSING** tab. In the canvas page, click the ⋮ menu button on the **AMX** application and select **Details**. The Application quick view appears.
4. Click on **STATISTICS** tab.
5. To view the statistics of a particular GigaVUE V Series Nodes, select the required GigaVUE V Series Node from the **V Series Node IP** dropdown menu to view the **Ingestor**, **Exporter**, and **Attributes Enrichment** statistics.

You can download the Ingestor and Exporter statistics using the following options:

- **Download TCP Dump** (Ingestor)- Select this option to download the PCAP file (for example, cap_ens192_20260407_073719655-run-001.pcap.gz). The TCP dump capture is limited to 100 packets and runs for up to 30 seconds, or until 100 packets are captured (whichever occurs first). You can capture a TCP dump for only one AMX ingestor at a time. The TCP dump download option is available only for the following ingestor types: AMI, NetFlow/IPFIX, Mobility, and Zscaler LSS.
- **Download Records** (Exporter) - Select this option to download the JSON file (for example, Elastic-exporter-records.json.gz) of the exporter records. You can download records for a single AMX exporter or for multiple exporters. The exporter record download waits up to 30 seconds for records to be exported. If no records are produced, the operation times out.

For instructions on how to download the ingestor and exporter records, and troubleshoot AMI/AMX issues, refer to Troubleshoot AMI/AMX Deployment.

For more information on health status of exporters, refer to View Health Status.

You can view the following parameters in the Application Metadata Exporter application statistics page.

Exporter - Statistics to monitor exports from AMX

Parameters	Description
Name	Displays the name of exporters created for this application.
Exported Entries	Displays the number of entries available in the files that will be uploaded from AMX to the cloud tool or the Kafka consumers.
Average File Size	Displays the average size of the file.
File Upload Errors	Displays the number of file uploaded from the AMX to the cloud tool or the Kafka consumers.
File Upload Errors	Displays the number of times the file was not uploaded to the cloud tools or Kafka consumers due to errors.
Re Exported Entries (Only for Kafka Tool Exporter)	Displays the number of records re-exported from the errors directory after the Kafka tool is restored. Errored files are re-exported automatically at a rate of 10 files per 5 seconds.
Exported Entries Rolling 15 Sec	Displays the rolling average of entries exported per second over the past 15 seconds.
Exported Entries Rolling 30 Sec	Displays the rolling average of entries exported per second over the past 30 seconds.
Exported Entries Rolling 60 Sec	Displays the rolling average of entries exported per second over the past 60 seconds.
Exported MBytes	Total number of megabytes exported.
Exported MBytes Rolling 15 Sec	Rolling average of megabytes exported over the past 15 seconds.
Exported MBytes Rolling 30 Sec	Rolling average of megabytes exported over the past 30 seconds.
Exported MBytes Rolling 60 Sec	Rolling average of megabytes exported over the past 60 seconds.

Ingestor - Statistics to monitor ingestion

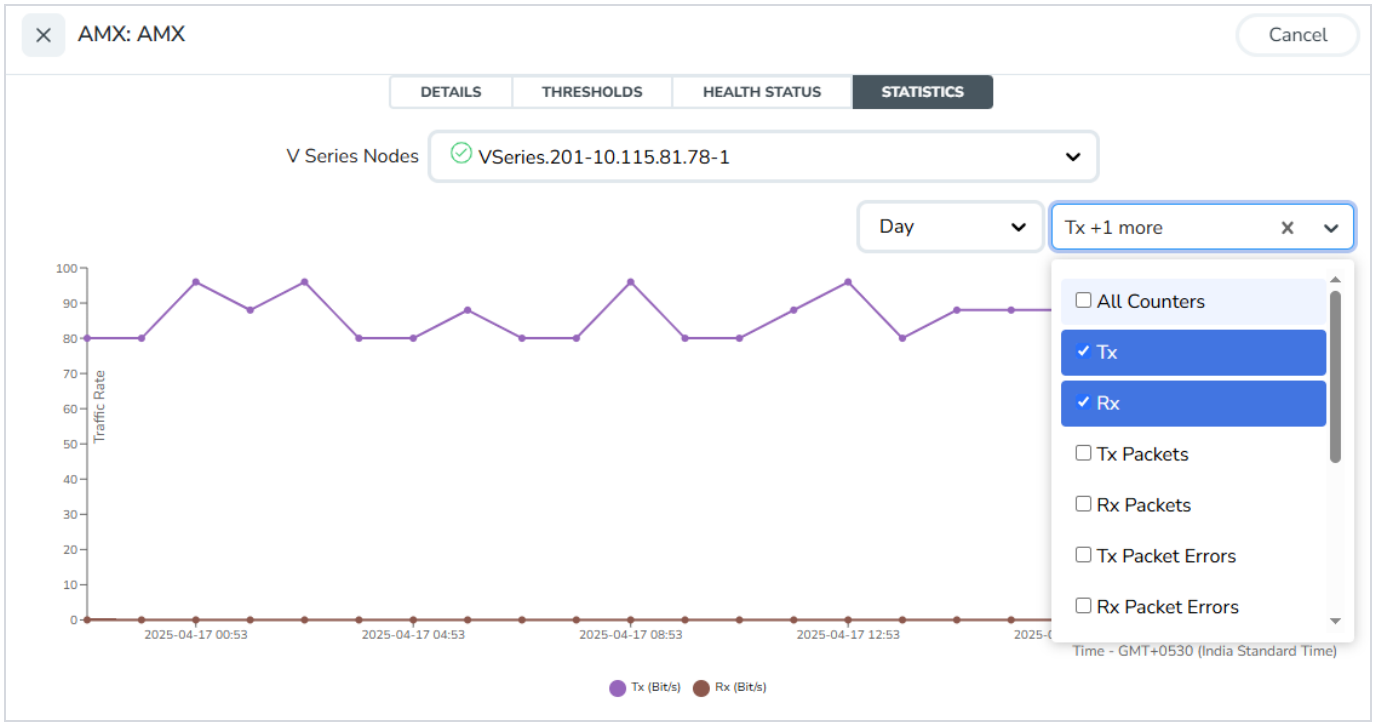
Parameters	Description
Name	Displays the name of the ingestor created for this application.
Packets Received	Displays the packets received from the AMI to AMX ingestor.
Packets Dropped	Displays the packets dropped when the traffic passes from AMI to AMX ingestor.

Parameters	Description
Octets Received	Displays the octets received from the AMI to AMX ingestor.
Octets Dropped	Displays the octets dropped when the traffic passes from AMI to AMX ingestor.
Records Added	Displays the number of workload information pulled from the workload environment.
Records Dropped	Displays the number of the workload details that were dropped from the workload environment.
Request Success	Displays if the workload information was fetched from the cloud environment. The default interval at which the AMX fetches the workload information is 60 seconds.
Request Authentication Errors	Displays if the workload information was not fetched from the cloud environment due to any authentication errors like wrong password.
Request Timedout Errors	Displays if the workload information was not fetched from the cloud environment even after the default interval of 60 seconds.
Request Errors	Displays when the workload information could not be fetched from the cloud environment due to issues other than authentication failures or timeout conditions.
Decode Success	Displays number of successful decoding operations performed by a system when processing NETFLOW/IPFIX packets.
Decode Fail	Displays the number of failed attempts to decode NETFLOW/IPFIX packets.
Elements Skipped	Displays number of data elements that were not processed or were omitted during the NETFLOW/IPFIX ingestion process.
Pkts Rx Rolling 15 Sec	Rolling average of packets received per second over the past 15 seconds.
Pkts Rx Rolling 30 Sec	Rolling average of packets received per second over the past 30 seconds.
Pkts Rx Rolling 60 Sec	Rolling average of packets received per second over the past 60 seconds.
Mbytes Rx	Total number of megabytes ingested.
Mbytes Rx Rolling 15 Sec	Rolling average of total megabytes received over the past 15 seconds.
Mbytes Rx Rolling 30 Sec	Rolling average of total megabytes received over the past 30 seconds.
Mbytes Rx Rolling 60 Sec	Rolling average of total megabytes received over the past 60 seconds.

Attributes Enrichment - Statistics to monitor enrichment

Parameters	Description
Name	Displays the name of the Metadata enrichment.
One Min Percent	Displays the percentage of the traffic that is enriched from the last 1 minute.
Five Min Percent	Displays the percentage of the traffic that is being enriched from the last 5 minutes.
Ten Min Percent	Displays the percentage of the traffic that is being enriched from the last 10 minutes.

The following image shows the statistical details for general AMX application.

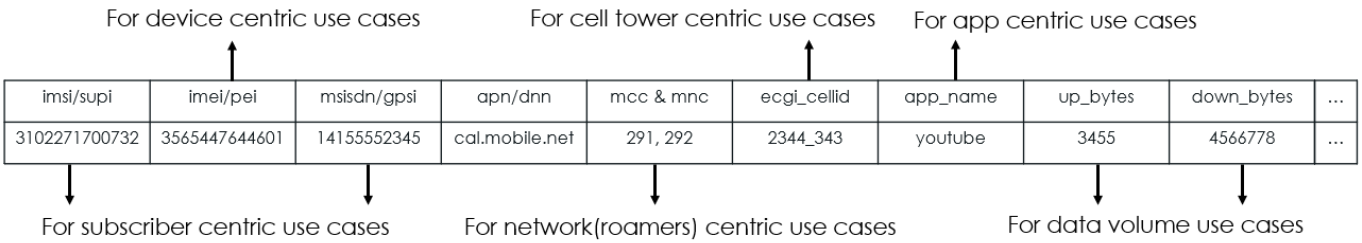


Attributes for GigaVUE Enriched Metadata for Mobile Networks

This section describes the various attributes available within GigaVUE Enriched Metadata for Mobile Networks.

Each flow will generate only one record per export interval; however, in this section, the attributes are separated into the following categories:

- Control Plane Attributes
- User Plane Attributes



Control Plane Attributes

The control plane attributes are generated based on network signaling message transactions with successful responses. These include signaling transactions for session establishment, modification, deletion, and others. These attributes are used for enriching the user plane metadata with the corresponding control plane subscriber, device, and location information.

Attribute	Description
imsi	International Mobile Subscriber Identity. A 3GPP-defined unique private identifier for a mobile user on a 4G network.
imei	International Mobile Equipment Identity. A 3GPP-defined unique identifier for a mobile device on a 4G network.
msisdn	Mobile Station Integrated Services Digital Network. A 3GPP-defined identifier for a mobile device on a 4G network.
supi	Subscription Permanent Identifier. A 3GPP-defined unique identifier for a mobile user on a 5G network.
gpsi	Generic Public Subscription Identifier. A 3GPP-defined public identifier for a mobile user on a 5G network.
pei	Permanent Equipment identifier. A 3GPP-defined unique identifier for a mobile device on a 5G network.
ctrl_tun_ access_ ipv4_addr	Control Plane Access Tunnel IPv4 Address. MME identifier for S11, SGW identifier for S5/S8-C, AMF identifier for N11 and SGSN for Gn, GP
ctrl_tun_ access_ ipv6_addr	Control Plane Access Tunnel IPv6 Address. MME identifier for S11, SGW identifier for S5/S8-C, AMF identifier for N11 and SGSN for Gn, GP
ctrl_tun_ access_teid	Control Plane Access Tunnel Endpoint Identifier
ctrl_tun_ core_ipv4_ addr	Control Plane Core Tunnel IPv4 Address. SGW identifier for S11, PGW identifier for S5/S8-C, SMF identifier for N11 and GGSN for Gn,Gp
ctrl_tun_ core_ipv6_ addr	Control Plane Core Tunnel IPv6 Address. SGW identifier for S11, PGW identifier for S5/S8-C, SMF identifier for N11 and GGSN for Gn,Gp
ctrl_tun_	Control Plane Core Tunnel Endpoint Identifier

core_teid	
user_tun_up_link_ipv4_addr	User Plane Uplink Tunnel IPv4 Address. Identifier of the SGW/UPF that receives the uplink user plane data from the eNodeB/gNodeB
user_tun_up_link_ipv6_addr	User Plane Uplink Tunnel IPv6 Address. Identifier of the SGW/UPF that receives the uplink user plane data from the eNodeB/gNodeB
user_tun_up_link_teid	User Plane Uplink Tunnel Endpoint Identifier
user_tun_down_link_ipv4_addr	User Plane Downlink Tunnel IPv4 Address. Identifier of the eNodeB/gNodeB that receives the uplink user plane data from the SGW/UPF
user_tun_down_link_ipv6_addr	User Plane Downlink Tunnel IPv6 Address. Identifier of the eNodeB/gNodeB that receives the uplink user plane data from the SGW/UPF
user_tun_down_link_teid	User Plane Downlink Tunnel Endpoint Identifier
if_name	3GPP Control Plane Interface Name
name	Name of the event on the 3GPP control plane interface
cause_code	Outcome of the event on the 3GPP control plane interface. Mostly set to 16 to indicate a successful event
sm_context_ref	Session Management Context
ebi	EPS(Evolved Packet System) Bearer ID
lbi	Linked Bearer Identity
pdu_session_id	PDU(Packet Data Unit) Session ID
apn	Access Point Name
dnn	Data Network Name
ue_ipv4_addr	User Equipment IPv4 Address
ue_ipv6_addr	User Equipment IPv6 Address
ue_ipv4v6_addr	User Equipment IPv4v6 Address
ue_non_ip_addr	User Equipment non-IP Address
ue_addr_type	User Equipment IP address type (IPv4 or IPv6)
qci	QoS Class Identifier
qfi	QoS Flow Identifier

five_qi	5G QoS Identifier
cgi_mcc	Mobile Country Code from Cell Global Identity
cgi_mnc	Mobile Network Code from Cell Global Identity
cgi_lac	Local Area Code from Cell Global Identity
cgi_cell_id	Cell Identification from Cell Global Identity
sai_mcc	Mobile Country Code from Service Area Identifier
sai_mnc	Mobile Network Code from Service Area Identifier
sai_lac	Local Area Code from Service Area Identifier
sai_sac	Service Area Code from Service Area Identifier
tai_mcc	Mobile Country Code from Tracking Area Identity
tai_mnc	Mobile Network Code from Tracking Area Identity
tai_tac	Tracking Area Code from Tracking Area Identity
ecgi_mcc	Mobile Country Code from E-UTRAN Cell Global Identifier
ecgi_mnc	Mobile Network Code from E-UTRAN Cell Global Identifier
ecgi_cell_id	Cell Identification from E-UTRAN Cell Global Identifier
lai_mcc	Mobile Country Code from Location Area Identity
lai_mnc	Mobile Network Code from Location Area Identity
lai_lac	Local Area Code from Location Area Identity
enode_id_mcc	Mobile Country Code from Evolved Node
enode_id_mnc	Mobile Network Code from Evolved Node
macro_enode_id	Evolved Node ID
ncgi_mcc	Mobile Country Code from NR Cell Global Identity
ncgi_mnc	Mobile Network Code from NR Cell Global Identity
ncgi_nr_cell_id	Cell Identification from NR Cell Global Identity
rat_type	Type of Radio Access Technology
snssai_sst	Slice/Service Type from Single Network Slice Selection Assistance Information
snssai_sd	Slice Differentiator id from Single Network Slice Selection Assistance Information

User Plane Attributes

The user plane attributes are generated by Application Metadata Intelligence (AMI), and include information such as IP addresses, protocols, timestamps, and byte/packet counters. These attributes are generated from the network flows and do not require DPI capabilities. The attributes for the mobile network traffic are generated for the inner IP flow by bypassing the outer headers

Attribute	Description
ts	Timestamp of the metadata generated in UTC
vendor	Identifying Gigamon as the vendor providing the metadata
version	Version number of the GigaSMART software release from the AMI application
generator	Identifies the Gigamon device that generates the user plane metadata. For example - HC3
src_ip	Source IPv4 address of the inner flow
dst_ip	Destination IPv4 address of the inner flow
src_mac	Source MAC address of the inner flow
dst_mac	Destination MAC address of the inner flow
mpls	MPLS Label if the flow has the MPLS header
protocol	Layer 4 protocol of the inner flow
src_port	Layer 4 protocol source port of the inner flow
dst_port	Layer 4 protocol destination port of the inner flow
device_inbound_ interface	Traffic receiving port on the Gigamon device example HC3
tcp-sport	Source TCP port
tcp_dport	Destination TCP port
udp_sport	Source UDP port
udp_dport	Destination UDP port
src_bytes	Source bytes from client to server in the flow including the outer and the inner IP header
dst_bytes	Destination bytes from client to server in the flow including the outer and the inner IP header
src_inner_bytes	Source bytes from the client to the server in the flow with the inner IP header (without the outer header)
dst_inner_bytes	Destination bytes from the server to the client in the flow with the inner IP header (without the outer header)
src_packets	Source packets from client to server in the flow including the header
dst_packets	Destination packets from client to server in the flow including header
total_bytes	Total bytes is sum of source and destination bytes
total_packets	Total packets is sum of source and destination packets
id	Unique flow id assigned to a flow
ingress_vlan_id	Vlan id in the packet received for the flow
src_ipv6	Source IPv6 address of the inner flow
dst_ipv6	Destination IPv6 address of the inner flow
ip_version	IP version v4, v6
ip_cos_id	QOS value in the IPv4 header
ip_dscp	DSCP value in the IPv4 header

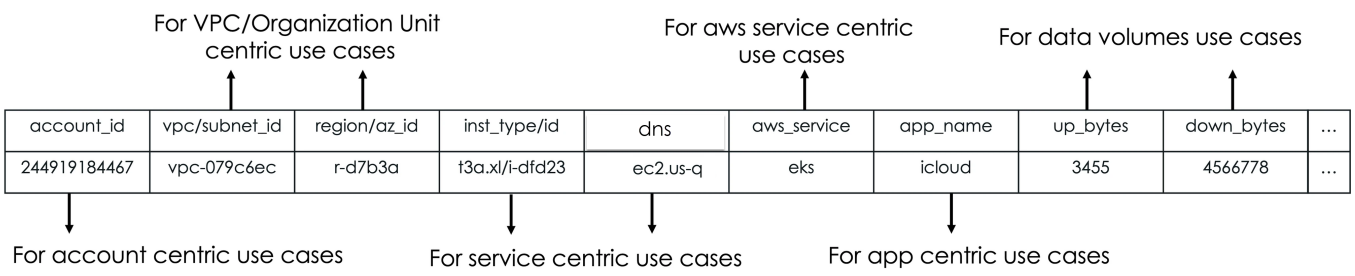
ip_ttl	Time to live in the IPv4 header
ip6hop_limit	Hop limit in the IPv6 header
flow_labelv6	flow label in the IPv6 header
ip6_ds	DSCP value in the IPv6 header
tcp_flags	TCP flag in the TCP header
gre_key	Generic routing encapsulation header key in the GRE header
ip_hdr_len	IPv4 header length
ip_frag_flags	IPv4 fragmentation flags
ipv6frag_flags	IPv6 fragmentation flags
ip_frag_id	IPv4 fragment id
ipv6frag_id	IPv6 fragment id
ip_frag_offset	IPv4 fragment offset
ipv6frag_offset	IPv6 fragment offset
ipv4opt	IPv4 options
ip_precendence_id	IPv4 precedence id
ip6precendence_id	IPv6 precedence id
ip_tot_len	IPv4 total length
ip6tot_len	IPv6 total length
ipv6hdr_len	IPv6 header length
payload_len_id	Payload length for the flow excluding the L3 IPv4 header
next_hdr_v6	Layer 4 protocol
icmp_type_v4	ICMP message type IPv4
icmp_code_v4	ICMP response code IPv4
icmp_code_v6	ICMP response code IPv6
icmp_type_v6	ICMP message type IPv6
tcp_ack_id	TCP ack id
tcp_hdr_len	TCP header length
tcp_seq_no	TCP sequence number
tcp_urgent_ptr	TCP urgent pointer
tcp_win_size	TCP window size
udp_msg_len	UDP message length
ip6traffic_class	IPv6 traffic class same as QoS in IPv4
flow_start_usec	Inner flow start time in microseconds in UTC
flow_end_usec	Inner flow end time in microseconds in UTC
flow_start_sec	Inner flow start time in seconds in UTC
flow_end_sec	Inner flow end time in seconds in UTC
start_time	Inner flow start time in milliseconds in UTC
end_time	Inner flow end time in milliseconds in UTC

egress_intf_id	egress IP interface-id for the Gigamon device sending the metadata
sys_up_time_first	Difference between the flow start time and the gigaSMART uptime in milliseconds
sys_up_time_last	Difference between the flow end time and the gigaSMART uptime in milliseconds
end_reason	Inner flow end reason – TCP ack, reset, inactive, etc
tcpflagsyn	TCP flag SYN from TCP header
tcpflagsynack	TCP flag SYNACK from TCP header
tcpflagfin	TCP flag FIN (finish)from TCP header
tcpflagrst	TCP flag RST (reset) from TCP header
Labels	Labels are added to the metadata by configuration in AMX. There can be multiple labels configured and added. Each label is configured as a key and a string value.
Labels configured in the JSON example in the section below	
label_event_type	Label identifying the vendor generating the event in the AMX exporter
label_deployment	Label identifying the deployment address of the AMX exporter
label_traffic	Label identifying the traffic region where the AMX is deployed
MSS	Maximum payload size a TCP segment can carry without the headers. The MSS value is exported at the beginning of a flow. Its exported only when bidirectional flows are configured.
aggr-window-size	The actual TCP window size minimum, mean, and maximum values, calculated separately for both sender and receiver packets.
zero-window	This captures TCP zero window event statistics for both sender and receiver, indicating when the TCP receive buffer is full and data transmission is temporarily paused due to flow control.

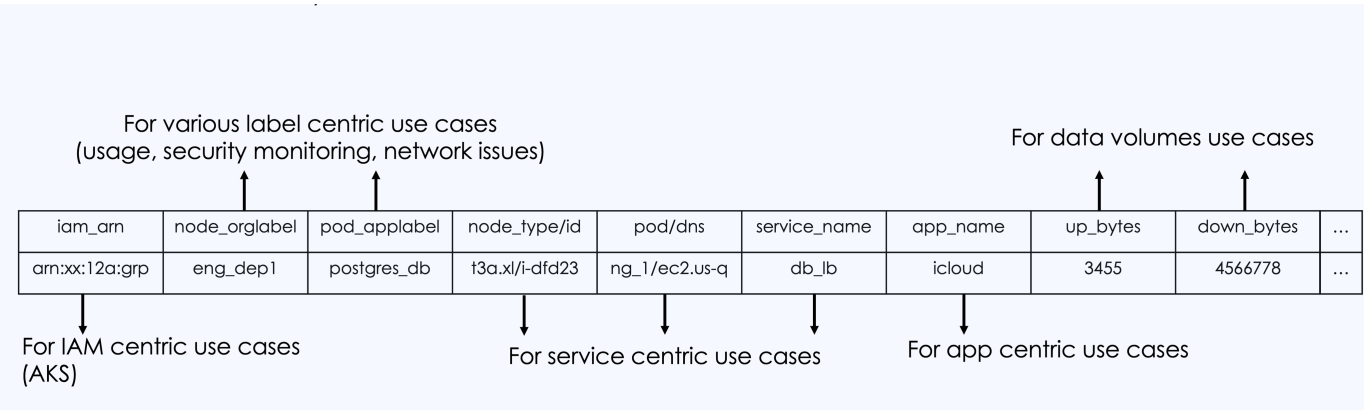
Attributes for GigaVUE Enriched Metadata for Cloud Workloads

This section describes the various attributes available within GigaVUE Enriched Metadata for Cloud Workloads for the following platforms:

- AWS
- Azure
- VMware vCenter
- Azure Kubernetes Service (AKS)
- Zscaler Private Access (ZPA) Attributes



- Azure Kubernetes Service (AKS)



The following table defines the purpose and scope of each referenced dataset, detailing configuration, resource, and operational parameters across AWS, Azure, and Kubernetes environments to support multi-cloud infrastructure documentation.

AWS

Attribute	Description	Source	Destination
aws_instance_id	ID of the EC2 instance	✓	✓
aws_instance_type	Type of EC2 instance	✓	✓
aws_availability_zone	Availability Zone of the EC2 instance	✓	✓
aws_image_id	ID of the base image use for EC2 instance	✓	✓
aws_private_dns_name	Private DNS hostname name assigned to the EC2 instance	✓	✓
aws_private_ip	Private IPv4 address assigned to the EC2 instance	✓	✓
aws_public_dns_name	Public DNS name assigned to the EC2 instance	✓	✓
aws_public_ip	Public IPv4 address assigned to the EC2 instance	✓	✓
aws_instance_state	Current state of the EC2 instance	✓	✓
aws_subnet_id	ID of the subnet in which the EC2 instance is running	✓	✓

aws_vpc_id	ID of the VPC in which the EC2 instance is running	✓	✓
aws_iam_instance_profile_arn	Amazon Resource Name (ARN) of the IAM instance profile	✓	✓
aws_iam_instance_profile_id	ID of the IAM instance profile	✓	✓
aws_security_group_name	Security group name assigned for the EC2 instance	✓	✓
aws_security_group_id	Security group ID assigned for the EC2 instance	✓	✓
aws_network_if_id	ID of the network interface	✓	✓
aws_network_if_attach_id	ID of the network interface attachment	✓	✓
aws_tags	Tags assigned to the EC2 instance in kv format with kv delimiter ':' and pair delimiter ','	✓	✓
aws_flat_tags	Tags assigned to the EC2 instance extracted to top level keys and values	✓	✓
aws_owner_id	ID of the AWS account that created the network interface	✓	✓
workload_platform	Platform Name - AWS	✓	✓

Azure

Attribute	Description	Source	Destination
azure_subscription_id	Subscription ID of the Azure account that created the VM	✓	✓
azure_resource_group	Resource Group of the VM	✓	✓
azure_vm_id	Complete path of the Azure VM. This includes subscription	✓	✓
azure_instance_id	Instance ID of the Azure VM	✓	✓
azure_instance_type	Instance type of the Azure VM	✓	✓
azure_availability_zone	Availability zone of the Azure VM	✓	✓

azure_image_id	Image ID of the Azure VM	✓	✓
azure_private_dns_name	Private DNS name assigned to the VM instance	✓	✓
azure_private_ip	Private IP address assigned to the VM instance	✓	✓
azure_public_dns_name	Public DNS name assigned to the VM instance	✓	✓
azure_public_ip	Public IP address assigned to the VM instance	✓	✓
azure_instance_state	Current state of the VM instance	✓	✓
azure_subnet_id	Subnet ID of the VM instance	✓	✓
azure_vnet_id	ID of the VNET in which the VM instance is running	✓	✓
azure_network_if_id	ID of the network interface	✓	✓
azure_network_if_attach_id	ID of the network interface attachment	✓	✓
azure_tags	Tags assigned to the VM instance in kv format with kv delimiter ':' and pair delimiter ','	✓	✓
azure_flat_tags	Tags assigned to the VM instance extracted to top level keys and values	✓	✓
azure_owner_id	Owner of the VM instance	✓	✓
azure_location	Resource Location	✓	✓
azure_scaleset_name	Scale set name	✓	✓
azure_scaleset_mode	Scale set orchestration mode	✓	✓
workload_platform	Platform Name - Azure	✓	✓

VMware vCenter

Attribute	Description	Source	Destination
vmware_vm_name	Name of the guest VM	✓	✓
vmware_vm_network	Network name of the guest VM	✓	✓
vmware_vm_status	Current status of the guest VM	✓	✓
vmware_vm_tags	Tags assigned to the guest VM in kv format with kv delimiter ':' and pair delimiter ','	✓	✓

vmware_vm_flat_tags	Tags assigned to the guest VM extracted to top level keys and values	✓	✓
vmware_vm_os_family_name	OS type of the guest VM (eg: Linux)	✓	✓
vmware_vm_os_distro_name	OS distribution name of the guest VM	✓	✓
vmware_vm_os_distro_version	OS distribution version of the guest VM	✓	✓
vmware_vm_os_distro_pretty_name	OS distribution pretty name of the guest VM	✓	✓
vmware_vm_dns_host_name	Host DNS name of the guest VM	✓	✓
vmware_vm_dns_host_domain_name	Host DNS domain name of the guest VM	✓	✓
vmware_host_name	Host name of the guest VM	✓	✓
vmware_host_ip	Host IP address of the guest VM	✓	✓
vmware_datacenter_name	Datacenter name of the guest VM	✓	✓
vmware_cluster_name	Cluster name of the guest VM	✓	✓
vmware_vcenter_name	vCenter name of the guest VM	✓	✓
workload_platform	Platform Name - VMware	✓	✓

Azure Kubernetes Service (AKS)

Attribute	Description	Source	Destination
k8s_cluster_name	Name identifying the Kubernetes cluster	✓	✗
k8s_cluster_version	Version of Kubernetes running on the cluster	✓	✗
k8s_cluster_status	Operational state of the Kubernetes cluster	✓	✗
k8s_node_name	Identifier for the node within the cluster	✓	✗
k8s_node_internal_ip	Internal IP address assigned to the node	✓	✗
k8s_node_external_ip	External IP address of the node	✓	✗
k8s_node_os_version	Operating system version installed on the node	✓	✗
k8s_node_os_image	Name of the OS image used by the node	✓	✗
k8s_node_kernel_version	Kernel version of the node	✓	✗
k8s_node_cri_version	Version of the container runtime	✓	✗

	interface used on the node		
k8s_node_status	Health and availability status of the node	✓	✗
k8s_node_labels	Node labels parsed into key-value pairs for metadata enrichment	✓	✗
k8s_pod_name	Name assigned to the Kubernetes pod	✓	✗
k8s_pod_labels	Pod labels parsed into key-value pairs for metadata enrichment	✓	✗
k8s_pod_namespace	Namespace in which the pod is deployed	✓	✗
k8s_pod_status	Operational state of the pod	✓	✗
k8s_pod_ip	IP address assigned to the pod	✓	✗
k8s_service_name	Name of the Kubernetes service	✓	✗
k8s_service_type	Type of service	✓	✗
k8s_container_name	Name of the container running inside the pod	✓	✗
k8s_container_image	Image used to create the container	✓	✗
k8s_container_port	Container port details	✓	✗
k8s_cluster_name	Name identifying the Kubernetes cluster	✗	✓
k8s_cluster_version	Version of Kubernetes running on the cluster	✗	✓
k8s_cluster_status	Operational state of the Kubernetes cluster	✗	✓
k8s_node_name	Identifier for the node within the cluster	✗	✓
k8s_node_internal_ip	Internal IP address assigned to the node	✗	✓
k8s_node_external_ip	External IP address of the node	✗	✓
k8s_node_os_version	Operating system version installed on the node	✗	✓
k8s_node_os_image	Name of the OS image used by the node	✗	✓
k8s_node_kernel_version	Kernel version of the node's operating system	✗	✓
k8s_node_cri_version	Version of the container runtime interface used on the node	✗	✓
k8s_node_status	Health and availability status of the node	✗	✓
k8s_node_labels	Node labels parsed into key-value pairs for metadata enrichment	✗	✓
k8s_pod_name	Name assigned to the Kubernetes	✗	✓

	pod		
k8s_pod_labels	Pod labels parsed into key-value pairs for metadata enrichment	✖	✓
k8s_pod_namespace	Namespace in which the pod is deployed	✖	✓
k8s_pod_status	Operational state of the pod	✖	✓
k8s_pod_ip	IP address assigned to the pod	✖	✓
k8s_service_name	Name of the Kubernetes service	✖	✓
k8s_service_type	Type of service	✖	✓
k8s_container_name	Name of the container running inside the pod	✖	✓
k8s_container_image	Docker image used to create the container	✖	✓
k8s_container_port	Container port details	✖	✓

Zscaler Private Access (ZPA) Attributes

Attribute	Description
z_lss_username	Username of Zscaler Private Access user.
z_lss_client_private_ip	Private IP address of the Zscaler Private Access client
z_lss_client_public_ip	Public IP address of the Zscaler Private Access. client.
z_lss_customer	Name of Zscaler Private Access customer.
z_lss_connection_id	ID of the Zscaler Private Access connection.
z_lss_connection_status	Status of the Zscaler Private Access connection.
z_lss_connection_status_code	Status code of the Zscaler Private Access connection.
z_lss_connector	Name of the Zscaler Private Access application connector.
z_lss_hostname	Name of the host device as given by the Zscaler client connector.
z_lss_client_country_code	Country code of the Zscaler Private Access client location.
z_lss_policy	Name of the Zscaler Private Access policy.
z_lss_app_group	Group name of the Zscaler Private Access application.
z_lss_policy_processing_time	Processing time of the Zscaler Private Access policy.
z_lss_idp	Identity provider used by Zscaler Private Access.
z_lss_client_city	City of the Zscaler Private Access client location.
z_lss_platform	Client platform of Zscaler Private Access.
z_lss_connection_setup_time	Connection setup time for Zscaler Private Access.

Supported Element Types for NetFlow Integrator Element Mapping

This section outlines the element types (v5, v9, and v10) supported by the AMX application for element mapping from the ingest NetFlow/IPFIX flow records to JSON on the following platforms. These elements are predefined and cannot be configured:

- VMware ESXi
- VMware NSX-T

Elements	Description[1]	Supported for NetFlow v5	Supported for NetFlow v9	Supported for NetFlow v10/IPFIX
type	Type of flow message	✓	✓	✓
sampler_ address	Address of the device that generated the packet	✓	✓	✓
sampling_ rate	Sampling rate of the flow	✓	✓	✓
export_time_ ns	Export time in Nano seconds	✓	✓	✓
time_ received_ns	Timestamp in nanoseconds of when the message was received	✓	✓	✓
sequence_ num	Sequence number of the flow packet	✓	✓	✓
source_id	An identifier that uniquely identifies the flow source. For IPFIX it refers to the observation domain ID.	✗	✓	✓
etype	Ethernet type (0x86dd for IPv6...)	✓	✓	✓
src_addr	Source address (IP) • NetFlow v5 - IPv4 only • NetFlow v9 - IPV4_SRC_ADDR(8), IPV6_ SRC_ADDR(27) • NetFlow v10/IPFIX - sourceIPv4Address(8), sourceIPv6Address(27)	✓	✓	✓
dst_addr	Destination address (IP) • NetFlow v5 - IPv4 only • NetFlow v9 - IPV4_DST_ADDR (12), IPV6_ DST_ADDR (28) • NetFlow v10/IPFIX - destinationIPv4Address(12), destinationIPv6Address(28)	✓	✓	✓
ip_tos	IP Type of Service • NetFlow v5 – tos • NetFlow v9 - SRC_TOS (5) • NetFlow v10/IPFIX - ipClassOfService (5)	✓	✓	✓

[1]The numbers within the enclosed brackets represent the element ID in IPFIX/NetFlow v10 and the field type ID in NetFlow v9.

ip_dscp	Differentiated Services Code Point • ipDiffServCodePoint (195)	✖	✓	✓
ip_ precedence	The value of the IP Precedence • ipPrecedence (196)	✖	✓	✓
proto	Protocol (UDP, TCP, ICMP...) • NetFlow v5 – proto • NetFlow v9 - PROTOCOL (4) • NetFlow v10/IPFIX - protocolIdentifier (4)	✓	✓	✓
ip_ttl_max	Maximum TTL value observed for packets of the flow • NetFlow v9 - MAX_TTL (53) • NetFlow v10/IPFIX - maximumTTL (53)	✖	✓	✓
src_port	Source port (when UDP/TCP/SCTP) • NetFlow v5 – srcport • NetFlow v9 - L4_SRC_PORT (7) • NetFlow v10/IPFIX - sourceTransportPort (7)	✓	✓	✓
dst_port	Destination port (when UDP/TCP/SCTP) • NetFlow v5 – dstport • NetFlow v9 - L4_DST_PORT (11) • NetFlow v10/IPFIX - destinationTransportPort (11)	✓	✓	✓
bytes	Number of bytes in a flow • NetFlow v5 – dOctets • NetFlow v9 - IN_BYTES (1), OUT_BYTES (23) • NetFlow v10/IPFIX - octetDeltaCount (1), postOctetDeltaCount (23)	✓	✓	✓
packets	Number of packets in a flow • NetFlow v5 – dPkts • NetFlow v9 - IN_PKTS (2), OUT_PKTS (24) • NetFlow v10/IPFIX - packetDeltaCount (2), postPacketDeltaCount (24)	✓	✓	✓
bytes_total	Running byte counter for a permanent flow • NetFlow v9 - IN_PERMANENT_BYTES (85) • NetFlow v10/IPFIX - octetTotalCount(85)	✖	✓	✓
packets_total	Running packet counter for a permanent flow • NetFlow v9 - IN_PERMANENT_PKTS (86) • NetFlow v10/IPFIX - packetTotalCount(86)	✖	✓	✓
flow_ direction	Flow direction • NetFlow v9 - DIRECTION (61) • NetFlow v10/IPFIX - flowDirection(61)	✖	✓	✓
in_if	Input interface	✓	✓	✓

	• NetFlow v5 – input • NetFlow v9 - INPUT_SNMP (10) • NetFlow v10/IPFIX - ingressInterface (10)			
out_if	Output interface • NetFlow v5 – output • NetFlow v9 - OUTPUT_SNMP (14) • NetFlow v10/IPFIX - egressInterface (14)	✓	✓	✓
time_flow_start_ns	Time the flow started in nanoseconds. Refer to Important Notes. • NetFlow v5 – System uptime and first • NetFlow v9 - System uptime and FIRST_SWITCHED (22) • NetFlow v10 - flowStartXXX (150, 152, 154, 156)	✓	✓	✓
time_flow_end_ns	Time the flow ended in nanoseconds. Refer to Important Notes. • NetFlow v5 – System uptime and last • NetFlow v9 - System uptime and LAST_SWITCHED (21) • NetFlow v10/IPFIX - flowEndXXX (151, 153, 155, 157)	✓	✓	✓
tcp_flags	TCP flags • NetFlow v5 – tcp_flags • NetFlow v9 - TCP_FLAGS (6) • NetFlow v10/IPFIX - tcpControlBits (6)	✓	✓	✓
ip_length_min	Minimum IP packet length • NetFlow v9 - MIN_PKT_LNGTH (25) • NetFlow v10/IPFIX - minimumIpTotalLength (25)	✗	✓	✓
ip_length_max	Maximum IP packet length • NetFlow v9 - MAX_PKT_LNGTH (26) • NetFlow v10/IPFIX - maximumIpTotalLength (26)	✗	✓	✓
next_hop	Nexthop IP address • NetFlow v5 – nexthop • NetFlow v9 - IPV4_NEXT_HOP (15), IPV6_NEXT_HOP (62) • NetFlow v10/IPFIX - ipNextHopIPv4Address (15), ipNextHopIPv6Address (62)	✓	✓	✓
ipv4_next_hop	Nexthop IPv4 address • NetFlow v9 - IPV4_NEXT_HOP (15) • NetFlow v10/IPFIX - ipNextHopIPv4Address (15)	✗	✓	✓
ipv6_next_	Nexthop IPv6 address	✗	✓	✓

hop	• NetFlow v9 - IPV6_NEXT_HOP (62) • NetFlow v10/IPFIX - ipNextHopIPv6Address (62)			
flow_id	An identifier of a flow that is unique within an Observation Domain • NetFlow v9 - flowId (148) • NetFlow v10/IPFIX - flowId (148)	✖	✓	✓
firewall_event	Indicates a firewall event. Allowed values are listed in the firewall Event registry. • firewallEvent(233)	✖	✓	✓
icmp_type	Type of the ICMP message • NetFlow v9 - ICMP_TYPE (32) • NetFlow v10/IPFIX - icmpTypeXXX (176, 178), icmpTypeCodeXXX (32, 139)	✖	✓	✓
icmp_code	Code of the ICMP message • NetFlow v9 - ICMP_TYPE (32) • NetFlow v10/IPFIX - icmpCodeXXX (177, 179) icmpTypeCodeXXX (32, 139)	✖	✓	✓
flow_end_reason	The reason for flow termination. Values are listed in the flowEndReason registry.	✖	✓	✓
application_id	Specifies an Application ID • NetFlow v9 - APPLICATION TAG (95) • NetFlow v10/IPFIX - applicationId (95)	✖	✓	✓
application_description	Specifies the description of an application • NetFlow v9 - APPLICATION DESCRIPTION (94) • NetFlow v10/IPFIX - applicationDescription (94)	✖	✓	✓
application_name	Specifies the name of an application • NetFlow v9 - APPLICATION NAME (96) • NetFlow v10/IPFIX - applicationName (96)	✖	✓	✓
tcp_window_size	The window field in the TCP header • tcpWindowsSize (186)	✖	✓	✓
viptela_vpn_id	Private enterprise number for vIPtela Inc. (41916)	✖	✖	✓

Migrate Application Intelligence Session to Monitoring Session

Starting from Software version 6.5.00, you must configure the Application Intelligence solution from Monitoring Session Page. After upgrading to 6.5.00, you cannot create a new Application Intelligence Session or edit an existing Application Intelligence Session for a virtual environment from the **Application Intelligence** page.

The following actions are available only when using the existing Application Intelligence Session:

- View Details
- Delete
- Forced Delete

We recommend to migrate the existing sessions to Monitoring Session for full functionality. GigaVUE-FM seamlessly migrates all your virtual Application Intelligence sessions and their connections. If migration fails, all sessions return to their original states.

Points to Note:

- You must have write access for the **Traffic Control Management** Resource in GigaVUE-FM to perform this migration. For details, refer to Create Roles section In GigaVUE Administration Guide
- The migration does not proceed:
  - If any of the existing Application Intelligence Session is in PENDING or SUSPENDED. Resolve the issue and start the migration process.
  - If any of the existing Application Intelligence Session is in FAILED state due to incorrect configuration. Resolve the issue and start the migration process.
  - If an existing Monitoring Session has the same name as the Application Intelligence Session. Change the existing Monitoring Session name to continue with the migration process.
- You cannot continue the session if any of the existing Application Intelligence Session has Application Filtering configured with Advanced Rules as Drop Rule and No Rule Match Pass All in the 5th rule set. In the Monitoring Session, the fifth Rule Set supports either Pass All or Advanced Rules as Drop. Delete this session and start the migration.
- When migrating the Application Intelligence Session, in rare scenarios, the migration process might fail after the pre-validation. In such cases, all the Application Intelligence Session roll back to the Application Intelligence page. Contact Technical Support for assistance.

Migrate your existing Application Intelligence **Session to Monitoring Session Page**

Follow these steps:

1. In the left navigation pane, select **Traffic > Solutions >Application Intelligence**. You cannot create a new Application Intelligence Session from this page.When you have an existing virtual Application Intelligence Session in the above page, the **Migrate Virtual Application Intelligence** dialog box appears.
2. Review the message and select **Migrate.**The **Confirm Migration** dialog box appears with the list of Application Intelligence Session that you need to migrate.
3. Review the list and select **Migrate**. GigaVUE-FM verifies the requirements and then migrates the Application Intelligence Sessions to the Monitoring Session Page.
4. Select **Go to Monitoring Session Page.**

You can view that all the virtual Application Intelligence Sessions in the Application Intelligence page are migrated to the Monitoring Session Page.

Post Migration Notes for Application Intelligence

After migrating Application Intelligence session to Monitoring Session page, consider the following:

1. **Secure Tunnels in the Options page** If you wish to enable Secure tunnels after migrating the Session, follow these steps:
   a. Go to **Traffic > Virtual > Orchestrated Flows > Select your cloud platform**.
   b. Select a Monitoring Session from the Monitoring Sessions list view on the left pane and select the **TRAFFIC ACQUISITION** tab.
   c. Enable **Secure tunnels**. For information about how to enable secure tunnel for a Monitoring Session, refer to the *Configure Monitoring Session Options* topic in the respective GigaVUE Cloud Suite Deployment Guide.
   d. Go to **Traffic > Virtual > Orchestrated Flows** and select your cloud platform.
   e. From the **Monitoring Sessions** page, select the Monitoring Session for which you enabled Secure Tunnels.
   f. Select **Actions > Undeploy**. The Monitoring Session is undeployed.
   g. Select the Monitoring Session for which you enabled Secure Tunnels and edit the Monitoring Session.
   h. Add the Application Intelligence applications.
   i. Modify the Number of Flows as per the below table.

Cloud Platform	Instance Size	Maximum Number of Flows
AWS	AMD - Large (c5n.2xlarge)	300k
	AMD - Medium (t3a.xlarge)	100k
	ARM - Large (c7gn.2xlarge)	100k
	ARM - Medium (m7g.xlarge)	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.

   j. Select **Deploy**. For details on how to deploy, refer to Application IntelligenceApplication Intelligence section in the GigaVUE V Series Applications Guide.

2. **Temporary Loss of Statistics with Version Mismatch**

   When GigaVUE-FM version is 6.5.00, and the GigaVUE V Series Node version is below 6.5.00, after migrating the Application Intelligence Session to the Monitoring Session and redeploying the monitoring session, a momentary loss in the statistical data of the Application Visualization application appears while redeploying the monitoring session.

3. **Configuration Changes Post-Migration**

   After migrating the Application Intelligence Session to monitoring session, if you wish to make any configuration changes, then make sure that the GigaVUE V Series Node version is greater than or equal to 6.3.00.

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.

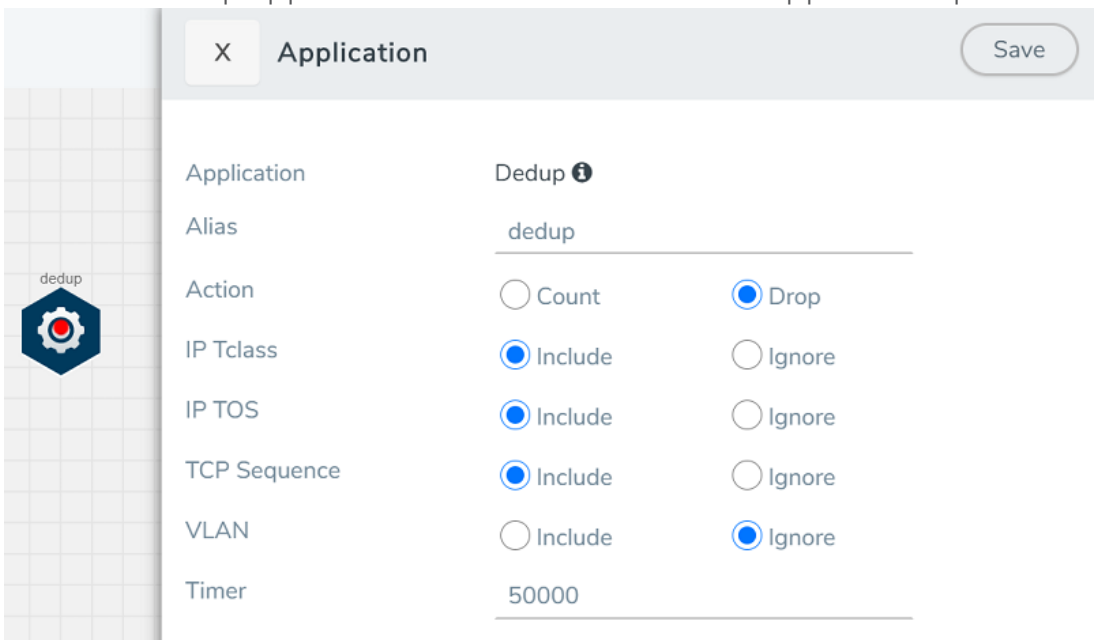
For IPv4 and IPv6 packets, to determine if a packet is considered to be a duplicate, parts of the IP headers (Layer 3 and Layer 4), as well as part of the payload are compared.

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.



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.

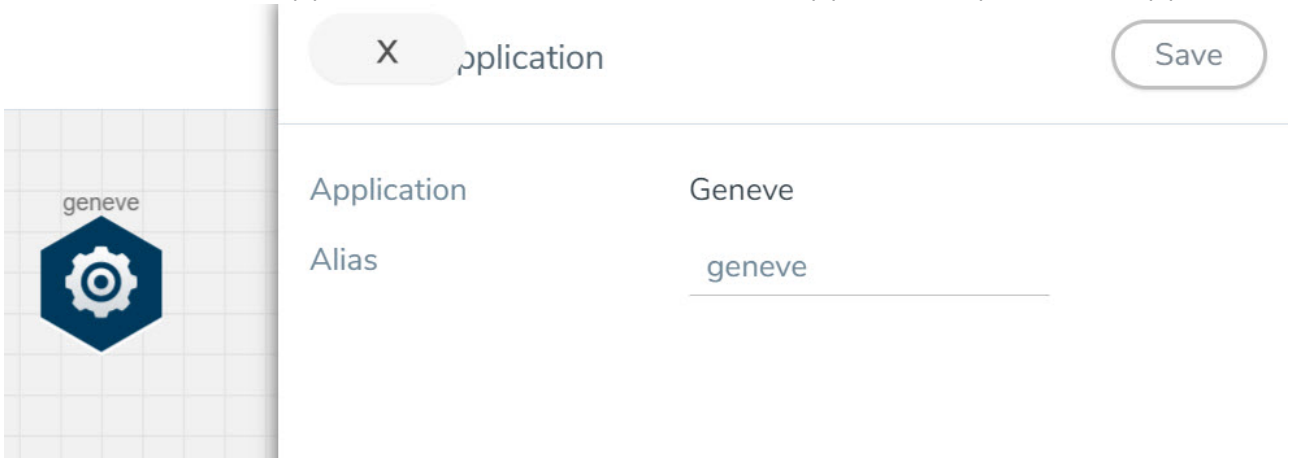
You can view the statistics of the application in the **STATISTICS** tab.

GENEVE Decapsulation

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

To add a GENEVE application:

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



3. Enter an alias for the GENEVE application.
4. Click **Save**.

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.

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:

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Name</td><td>Enter a name for the application.</td></tr>
<tr><td>Description</td><td>Enter the description.</td></tr>
<tr><td colspan="2">Application Metadata Settings</td></tr>
<tr><td>Flow Direction</td><td>Enable or Disable Bi-Directional Flow behavior. Bi-Directional is enabled by default. Disable this option for Uni-Directional Flow behavior.</td></tr>
<tr><td>Timeout</td><td>Specify the traffic flow inactivity timeout, in seconds. The session will be removed due to inactivity when no packets match.</td></tr>
<tr><td>Data Link</td><td>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.</td></tr>
<tr><td>Observation ID</td><td>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.</td></tr>
<tr><td colspan="2">Advanced Settings</td></tr>
<tr><td>Number of Flows</td><td>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>AWS</td><td>AMD - Large (c5n.2xlarge)</td><td>300k</td></tr>
<tr><td></td><td>AMD - Medium (t3a.xlarge)</td><td>100k</td></tr>
<tr><td></td><td>ARM - Large (c7gn.2xlarge)</td><td>100k</td></tr>
<tr><td></td><td>ARM - Medium (m7g.xlarge)</td><td>200k</td></tr>
<tr><td>Nutanix</td><td>Large (8 vCPU and 16GB RAM)</td><td>200k</td></tr>
</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.
</td></tr>
</table>

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**.

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 striping:

- 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 ERSPAN Type II and Type III headers. When choosing ESPRAN as your protocol for stripping, enter the following details:	
ESPRAN FlowID	Specify an ERSPAN flow ID 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.

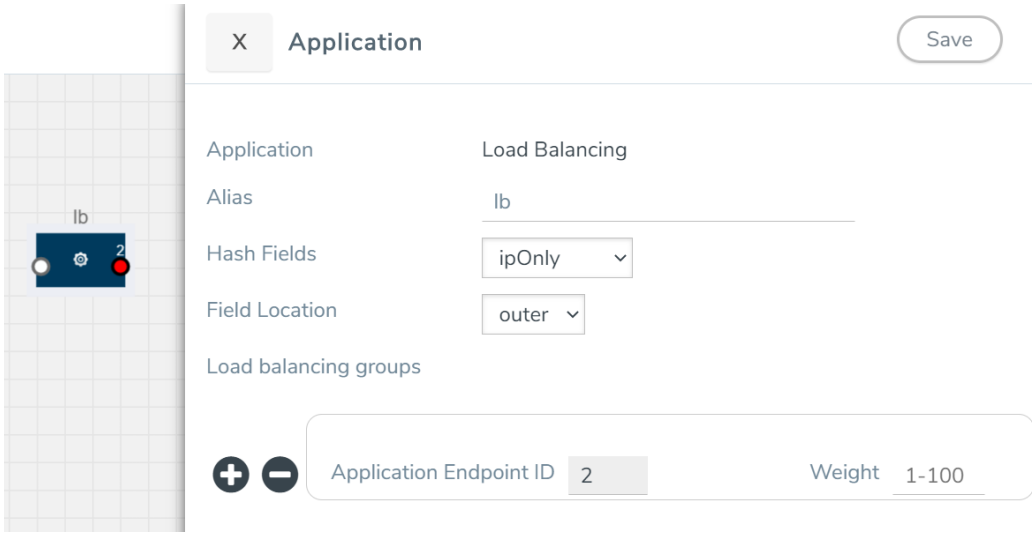
Load Balancing

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

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

To add a load balancing application:

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



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

Metric	Description
Alias	Enter a name for the load balancing application
Stateless	Select this option to enable Stateless Load Balancing
Enhanced Load Balancing	Select this option to enable Enhanced Load Balancing and select the ELB profile.
Hash Field	• **ipOnly** : The source IP and destination IP addresses. • **ipAndPort**: The source IP and destination IP addresses, and Layer 4 source port and destination port numbers. • **fiveTupl**e: The source IP and destination IP addresses, source port and destination port numbers, and protocol field in the IP header. • **gtpuTeid** The GTP-u tunnel identifier (ID). **NOTE:** There is no inner or outer field location for **GTPU-TEID**. • **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

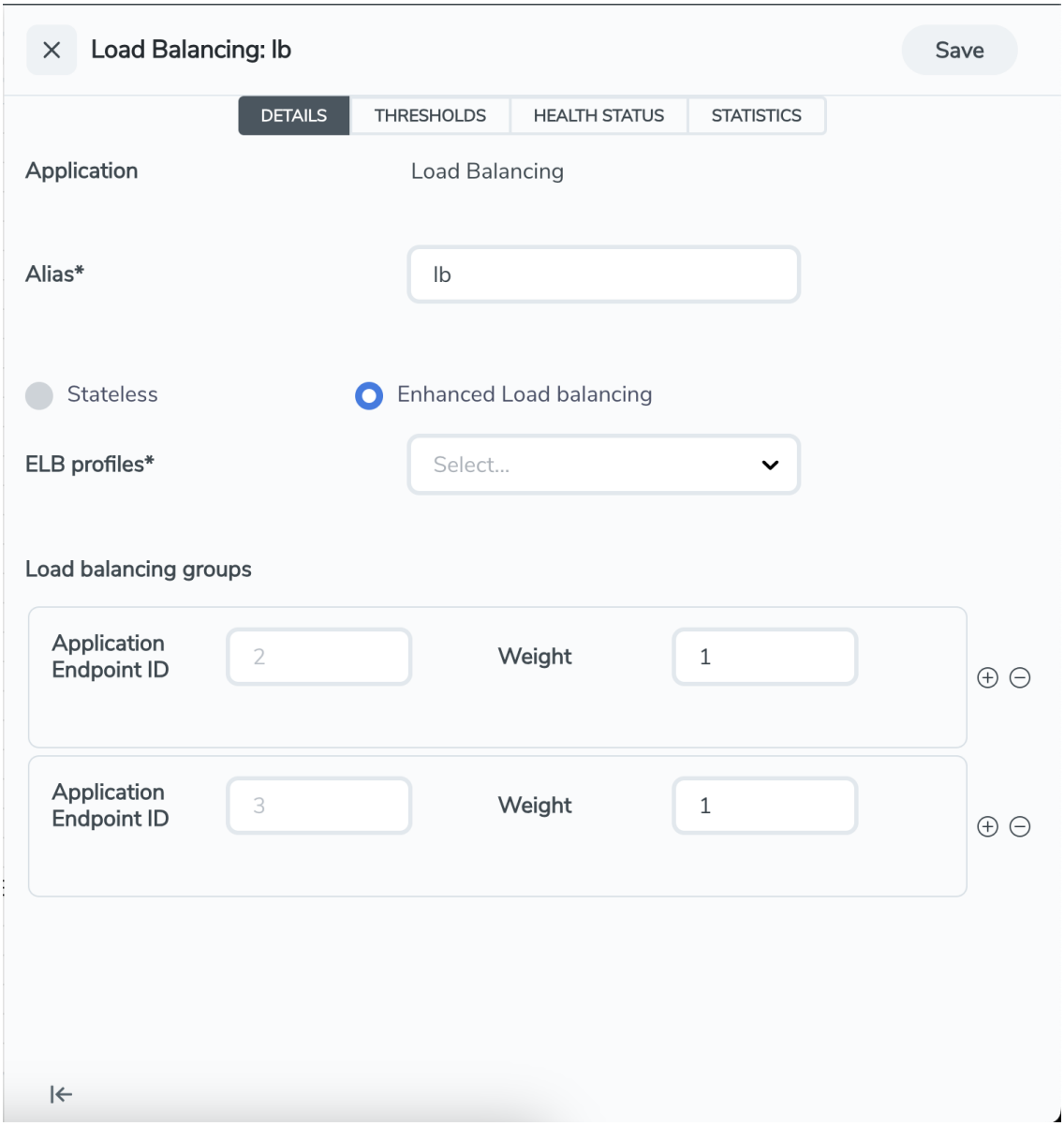
Enhanced Load Balancing redistributes the traffic from a failed endpoint to another endpoint which is a part of the ELB group. When the failed endpoint recovers, the redistributed traffic is restored to the recovered endpoint. The traffic across other endpoints remain undisturbed during this process. 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 gtputeid
Position	Select either inner/outer location of the hash field to be matched with the incoming packet..
Hash-mask	When the hash-fields ip-src/ip-dst are defined along with the IP, then ip-src/ip-dst hash-mask will overwrite the IP hash mask. For load balancing, you must apply this mask before hashing the IP. The default options and their default values are: IPv4 : 255.255.255.255 IPv6 :FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF

2. Go to monitoring session page and
    a. Drag and drop **Load Balancing** from **APPLICATIONS** to the graphical workspace.
    b. Click the load balancing application and select **Details**. The Application quick view appears.



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

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

3. Click **Save**.

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

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.

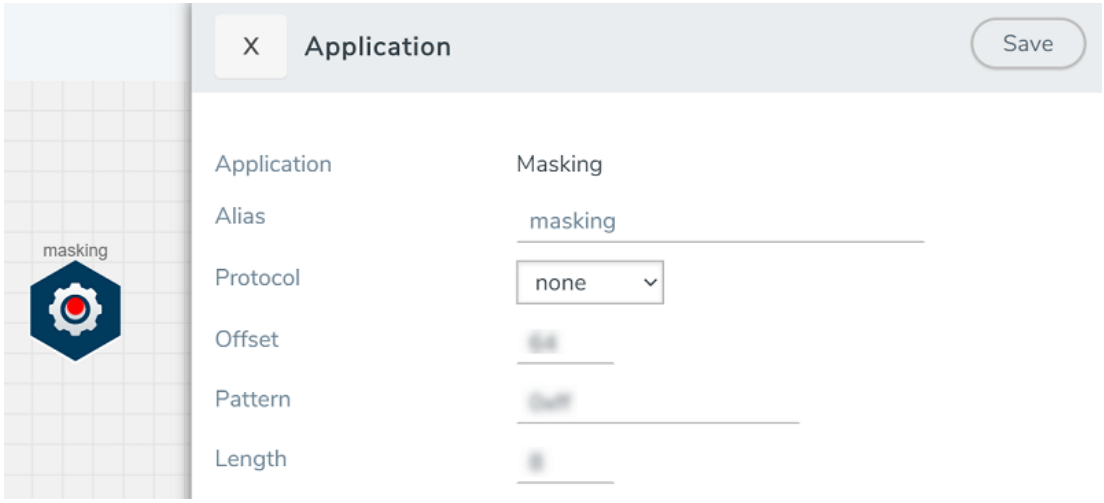
You can view the statistics of the application in the **STATISTICS** tab.

Masking

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

To add a Masking application:

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



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

Component	Description
Alias	Enter a name for the 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

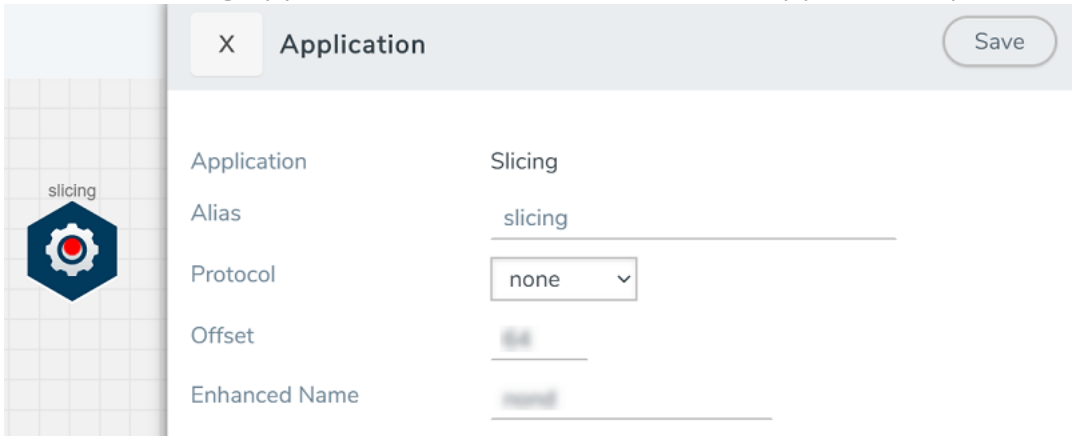
Packet Slicing allows you to truncate packets after a specified header and slice length, preserving the portion of the packet required for monitoring purposes. Slicing operations are typically configured to preserve specific packet header information, allowing effective network analysis without the overhead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



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.

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 forSSL Decrypt

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

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**.

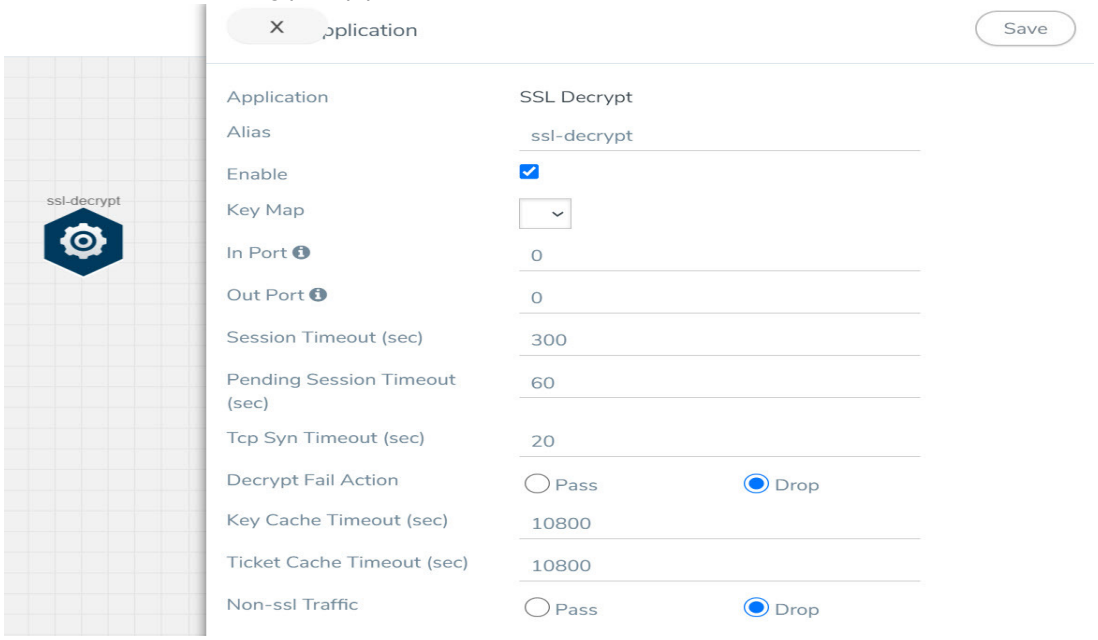
The following actions can also be performed from the SSL Key Pair Store Page:

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**.



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**.

Deploy Monitoring Session (AWS)

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

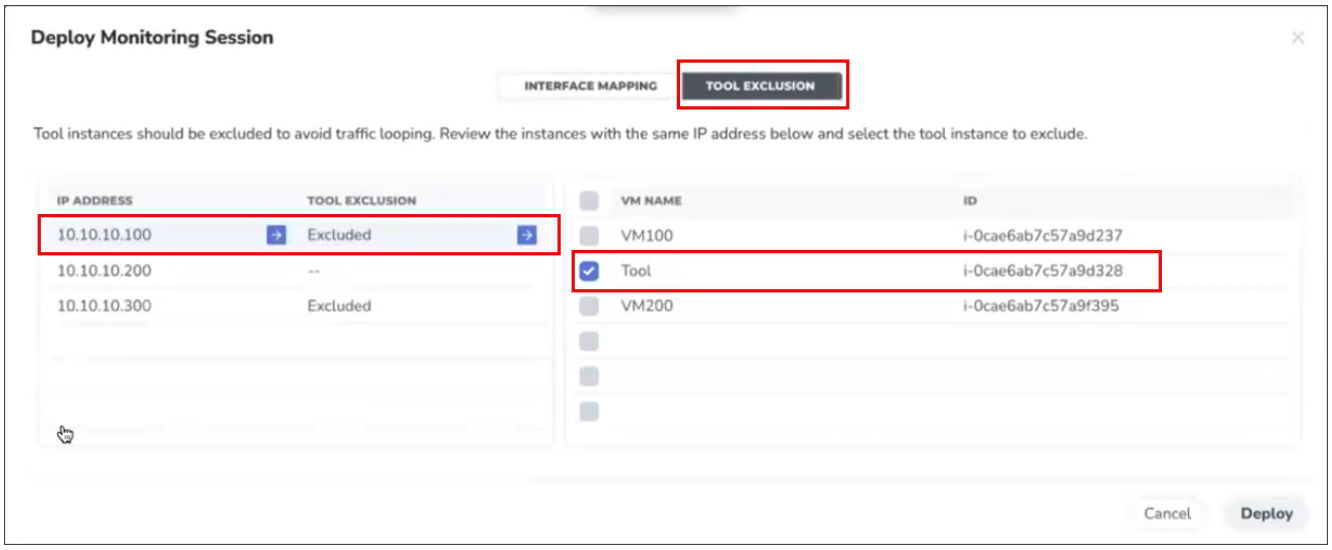
Interface Mapping

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

Monitor Cloud Health

GigaVUE-FM allows you to monitor the traffic and configuration health status of the monitoring session and its individual components. This section provides detailed information on how to view the traffic and configuration health status of the monitoring session and its individual components.

For details, refer to the following topics:

- Configuration Health Monitoring
- Traffic Health Monitoring
- View Health Status
- View Monitoring Session Statistics (AWS)
- Visualize the Network Topology (AWS)

Configuration Health Monitoring

The configuration health status provides detailed information about the configuration and deployment status of the deployed monitoring session.

It supports specific fabric components and features on the respective cloud platforms.

Configuration Health Monitoring	GigaVUE Cloud Suite for AWS	GigaVUE Cloud Suite for Azure	GigaVUE Cloud Suite for OpenStack	GigaVUE Cloud Suite for VMware	GigaVUE Cloud Suite for Nutanix
GigaVUE V Series Nodes	✓	✓	✓	✓	✓
UCT-V	✓	✓	✓	×	×
VPC Mirroring	✓	×	×	×	×
OVS Mirroring and VLAN Trunk Port	×	×	✓	×	×

Refer to the View Health Status section to view the configuration health status.

Traffic Health Monitoring

GigaVUE-FM monitors the traffic health of the entire Monitoring Session and each individual GigaVUE V Series Node in that session. It checks for issues like packet drops or traffic overflows.

When it detects a problem, GigaVUE-FM updates the health status of the related Monitoring Session. It monitors traffic health in near real-time.

The GigaVUE V Series Node tracks traffic levels. If traffic goes above or below the configured threshold, it alerts GigaVUE-FM. Then, GigaVUE-FM then uses this data to calculate traffic health.

If you deploy GigaVUE-FM and GigaVUE V Series Nodes in different cloud platforms, you must add the GigaVUE-FM public IP address as the Target Address in the Data Notification Interface on the Event Notifications page.

For details, refer to the Configuration Settings section in the *GigaVUE Administration Guide* .

This feature supports GigaVUE V Series Nodes on the respective cloud platforms:

For V Series Nodes:

- AWS
- Azure
- OpenStack
- VMware
- Third Party Orchestration

For instructions on creating and applying threshold templates across a Monitoring Session or an application, and viewing the traffic health status, refer to the following topics:

- Supported Resources and Metrics
- Create Threshold Templates
- Apply Threshold Template
- Clear Thresholds

Consideration to configure a threshold template

- By default, Threshold Template is not configured to any Monitoring Session. If you wish to monitor the traffic health status, then create and apply threshold template to the Monitoring Session.
- Editing or redeploying the Monitoring Session reapplies all the threshold policies associated with that Monitoring Session.

- Deleting the Monitoring Session clears all the threshold policies associated with that Monitoring Session.
- Threshold configuration is applied before deploying a Monitoring Session and remains even if the session is undeployed.
- After applying threshold template to a particular application, you need not deploy the Monitoring Session again.

Supported Resources and Metrics

The following table lists the resources and the respective metrics supported for traffic health monitoring. Refer to Create Threshold Templates and Apply Threshold Template sections for details on Threshold types and Threshold events.

Resource	Metrics	Threshold types	Trigger Condition
Tunnel End Point	1. Tx Packets 2. Rx Packets 3. Tx Bytes 4. Rx Bytes 5. Tx Dropped 6. Rx Dropped 7. Tx Errors 8. Rx Errors	1. Difference 2. Derivative	1. Over 2. Under
RawEnd Point	1. Tx Packets 2. Rx Packets 3. Tx Bytes 4. Rx Bytes 5. Tx Dropped 6. Rx Dropped 7. Tx Errors 8. Rx Errors	1. Difference 2. Derivative	1. Over 2. Under
Map	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
Slicing	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
Masking	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
Dedup	1. Tx Packets	1. Difference	1. Over

	2. Rx Packets 3. Packets Dropped	2. Derivative	2. Under
HeaderStripping	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
TunnelEncapsulation	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
LoadBalancing	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
SSLDecryption	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
Application Metadata	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
AMX	1. Tx Packets 2. Rx Packets 3. Packets Dropped 4. Ingestor - Rx packets 5. Ingestor - Packets Dropped 6. Ingestor - Rx Octets 7. Ingestor - Octets Dropped 8. Ingestor - Records Dropped 9. Workload - Records Dropped 10. Workload - Req Auth Errors 11. Workload - Req Timedout Errors 12. Workload - Req Errors 13. Exporter - Avg File Size	1. Difference 2. Derivative	1. Over 2. Under

	14. Exporter - File Uploads 15. Exporter - File Uploads Errors 16. Enrichment - One Minute Percent		
Geneve	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
5G-SBI	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
SBIPOE	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under
PCAPNG	1. Tx Packets 2. Rx Packets 3. Packets Dropped	1. Difference 2. Derivative	1. Over 2. Under

Create Threshold Templates

To create threshold templates:

1. Go to **Inventory > Resouces > Threshold Templates**.

   The **Threshold Templates** page appears.

2. Select **Create** to open the New Threshold Template page.

3. Enter the appropriate information for the threshold template as described in the following table:

Field	Description
Threshold Template Name	The name of the threshold template.
Thresholds	
Traffic Element	Select the resource for which you wish to apply the threshold template. Ex: TEP, REP, Maps, Applications like Slicing, De-dup etc
Time Interval	Frequency at which the traffic flow needs to be monitored.
Metric	Metrics that need to be monitored. For example: Tx Packets, Rx Packets.
Type	**Difference**: The difference between the stats counter at the start and end time of an interval, for a given metric. **Derivative**: Average value of the statistics counter in a time interval, for a given metric.
Condition	**Over**: Checks if the statistics counter value is greater than the 'Set Trigger Value'. **Under**: Checks if the statistics counter value is lower than the 'Set Trigger Value'.
Set Trigger Value	Value at which a traffic health event is raised, if statistics counter goes below or above this value, based on the condition configured.
Clear Trigger Value	Value at which a traffic health event is cleared, if statistics counter goes below or above this value, based on the condition configured.

4. Select **Save**.
   The newly created threshold template is saved, and it appears on the **Threshold** templates page.

Apply Threshold Template

You can apply your threshold template across the entire Monitoring Session and also to a particular application.

Apply Threshold Template to Monitoring Session

To apply the threshold template across a Monitoring Session, follow these steps:

1. On the left pane in GigaVUE-FM, select **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. The **Monitoring Session** page appears.
2. In the **TRAFFIC PROCESSING** tab, select **Options>Thresholds** menu.
3. From the **Select Template** drop-down list, select the template you wish to apply across the Monitoring Session.
4. Select **Apply**.

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.

Apply Threshold Template to Applications

Applying threshold template across Monitoring Session does not overwrite the threshold value applied specifically for an application. When a threshold value is applied to a particular application, it overwrites the existing threshold value for that particular application.

To apply the threshold template to a particular application in the Monitoring Session, follow these steps:

1. On the **Monitoring Session** page, select **TRAFFIC PROCESSING** tab. The Monitoring Session canvas page appears.
2. Select on the application for which you wish to apply or change a threshold template and select **Details**. The **Application** quick view opens.
3. Select the **Thresholds** tab.
4. Select the template you wish to apply from the Threshold Template drop-down menu or enter the threshold values manually.
5. Select **Save**.

Clear Thresholds

You can clear the thresholds across the entire Monitoring Session and also to a particular application.

Clear Thresholds for Applications

To clear the thresholds of a particular application in the Monitoring Session, follow these steps:

1. On the **Monitoring Session** page, select the **TRAFFIC PROCESSING** tab. The Monitoring Session canvas page appears.
2. Select the application for which you wish to clear the thresholds and click **Details**. The **Application** quick view opens.
3. Select the **Thresholds** tab.
4. Select **Clear All** and then select **Save**.

Clear Thresholds across the Monitoring Session

To clear the applied thresholds across a Monitoring Session, follow these steps:

1. On the left navigation pane in GigaVUE-FM, go to **Traffic > Virtual > Orchestrated Flows** and select your cloud platform. The **Monitoring Sessions** landing page appears.
2. Select the Monitoring Session and navigate to **TRAFFIC PROCESSING > Options > Thresholds**,
3. Select **Clear Thresholds**.
4. On the **Clear Threshold** pop-up appears, select **Ok**.

NOTE: Clearing thresholds at Monitoring Session level does not clear the thresholds that were applied specifically at the application level. To clear thresholds for a particular application, refer to Clear Thresholds for Applications

View Health Status

You can view the health status of the Monitoring Session on the Monitoring Session details page. The health status of the Monitoring Session is healthy only if both the configuration health and traffic health are healthy.

View Health Status of an Application

To view the health status of an application across an entire Monitoring Session,

1. Go to **Traffic > Virtual > Orchestrated Flows** and select your cloud platform.
2. Select a Monitoring Session and navigate to the **TRAFFIC PROCESSING** tab.
3. Select the application for which you wish to see the health status and select **Details**. The quick view page appears.
4. Select the **HEALTH STATUS** tab.

This displays the application's **Configuration Health**, **Traffic Health**, and the **Operational Health**, along with the thresholds applied to each.

NOTE: The secure tunnel status is refreshed every 5 minutes, and the GigaVUE-FM does not display UCT-V secure tunnel status that is older than 7 minutes. If the secure tunnel in the UCT-V is removed, it takes up to 7 minutes to reset the status on the GigaVUE-FM.

View Operational Health Status of an Application

When you configure the Application Metadata Exporter to use **Kubernetes** as the workload platform, the V Series Node transmits failure and error events to GigaVUE-FM, which processes them and updates the node's health status on the Monitoring Session page. When interacting with Kubernetes workloads, the system may encounter errors while retrieving resources such as pods, services, nodes, or endpoints. Refer to Errors for additional error details.

Operational events for Exporter:

Refer below for message format and messages that indicate common issues that can occur during the operations:

Format: <Server Type>_<Message>

Server Types: CLOUD EXPORT, KAFKA

Message	Description
UPLOAD_MAX_TRIES_EXCEED	Upload retries exceeded the maximum limit **Example**: CLOUDEXPORTER_UPLOAD_MAX_TRIES_EXCEED
REACHABILITY_FROM_AMX_TO_TOOLS	AMX failed to reach the tool (Cloud Exporter server or Kafka server) **Example**: CLOUDEXPORTER_REACHABILITY_FROM_AMX_TO_TOOLS
NO_IP_ADDRESS	No IP address was configured on the interface **Example**: CLOUDEXPORTER_NO_IP_ADDRESS
EXPORTER_UPLOAD_ERROR	Upload to the exporter failed **Example**: CLOUDEXPORTER_EXPORTER_UPLOAD_ERROR
EXPORTER_ERR_EVENT_CONTEXT_DEADLINE_EXCEEDED	The exporter health-monitor probe or upload to the tool timed out. **Example:** CLOUDEXPORTER_EXPORTER_ERR_EVENT_CONTEXT_DEADLINE_EXCEEDED KAFKA_EXPORTER_ERR_EVENT_CONTEXT_DEADLINE_EXCEEDED
EXPORTER_ERR_EVENT_CONTEXT_CANCELED	The exporter health-monitor probe or upload was canceled before completion, typically due to shutdown or reconfiguration. **Example:** CLOUDEXPORTER_EXPORTER_ERR_EVENT_CONTEXT_CANCELED KAFKA_EXPORTER_ERR_EVENT_CONTEXT_CANCELED

Message	Description
EXPORTER_ERR_EVENT_DNS_LOOKUP_FAIL	The hostname of the configured Kafka broker or Cloud Exporter endpoint could not be resolved due to a DNS failure. **Example:** CLOUDEXPORTER_EXPORTER_ERR_EVENT_DNS_LOOKUP_FAIL KAFKA_EXPORTER_ERR_EVENT_DNS_LOOKUP_FAIL
EXPORTER_ERR_EVENT_NETWORK_UNREACHABLE	The exporter probe failed at the network layer, for example, due to no route to the host or an unreachable network. **Example:** CLOUDEXPORTER_EXPORTER_ERR_EVENT_NETWORK_UNREACHABLE KAFKA_EXPORTER_ERR_EVENT_NETWORK_UNREACHABLE
EXPORTER_ERR_EVENT_TRASPORT_LAYER_ERR	The exporter probe failed at the transport layer, such as connection refusal, TCP reset, or TLS handshake failure. **Example:** CLOUDEXPORTER_EXPORTER_ERR_EVENT_TRASPORT_LAYER_ERR KAFKA_EXPORTER_ERR_EVENT_TRASPORT_LAYER_ERR

Operational events for Enrichment:

Refer below for message format and messages that indicate common issues that can occur during the operations:

Format: <Operation Type>_<Message>

Operation Types: GETSERVICES, GETPODS, GETNODES, GETENDPOINTSLICES, WATCHALL

Message	Description
K8S_AUTHORIZATION_FAILURE	The request was denied due to insufficient permissions **Example**: GETPODS_K8S_AUTHORIZATION_FAILURE
K8S_AUTHENTICATION_FAILURE	Authentication failed. Verify your credentials **Example**: GETPODS_K8S_AUTHENTICAION_FAILURE
K8S_UNHANDLED_ERROR	An unspecified error occurred. Check the error description **Example**: GETPODS_K8S_UNHANDLED_ERROR

View Health Status for Individual GigaVUE V Series Nodes

You can also view the health status of an individual GigaVUE V Series Node. To view the configuration health status and traffic health status of the V Series Nodes:

1. On the Monitoring Session page, select the required Monitoring Session from the list view.
2. In the **Overview** tab, view the health status of the required GigaVUE V Series Node from the chart options.

View Application Health Status for Individual V Series Nodes

To view the application configuration and traffic health status of the GigaVUE V Series Nodes:

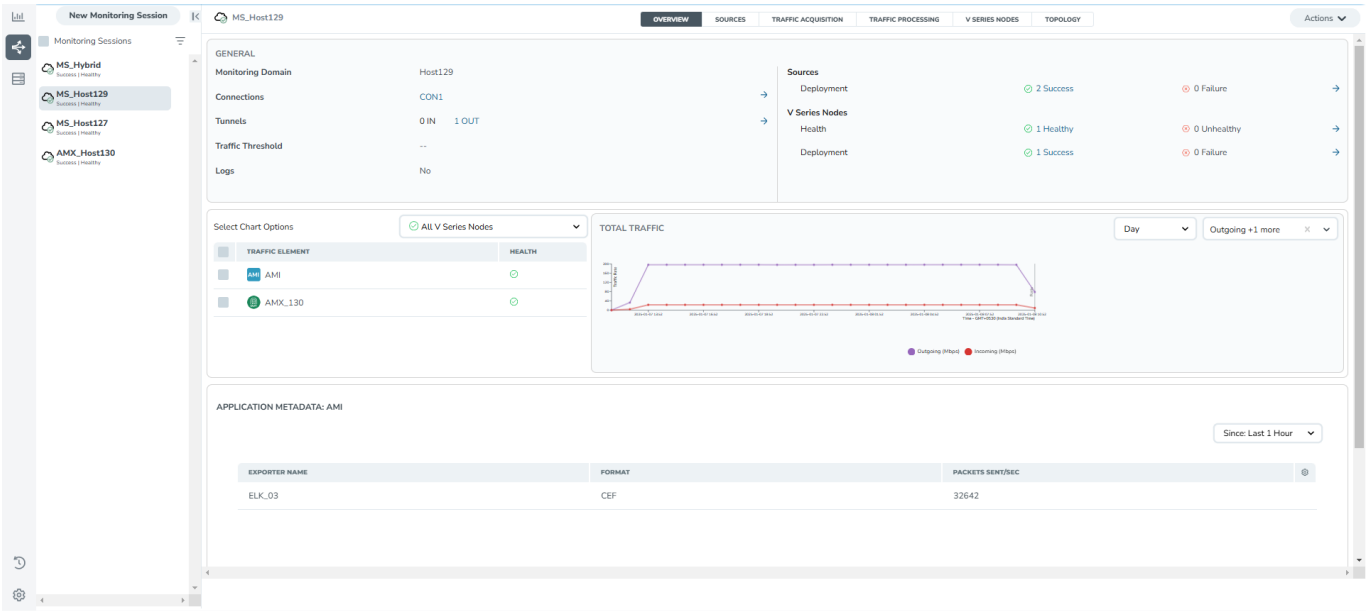
1. On the Monitoring Session page, select the required Monitoring Session from the list view.
2. On the Overview tab, select the GigaVUE V Series Node from the All V Series Nodes drop-down menu.

   The list view displays the list of applications for the selected GigaVUE V Series Node and the health status of each application.

View Monitoring Session Statistics (AWS)

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:

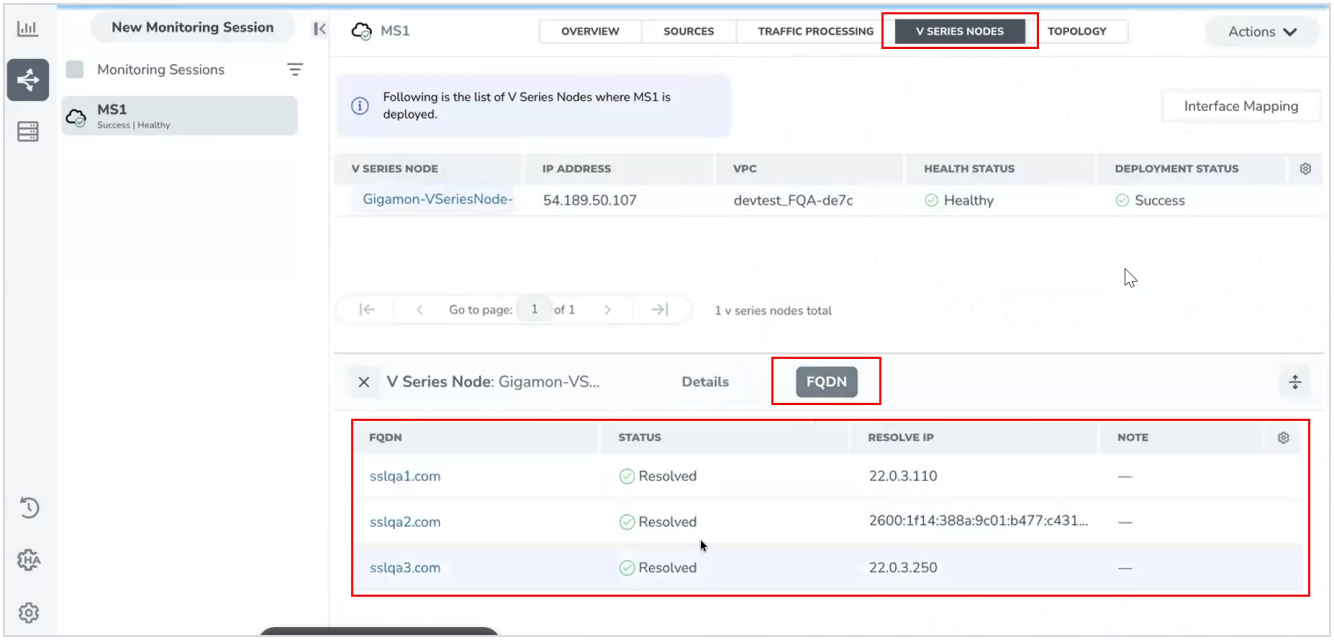
- You can view the incoming and outgoing traffic on an hourly, daily, weekly, and monthly basis.
- You can filter the traffic and view the statistics based on factors such as **Incoming**, **Outgoing**, **Ratio (Out/In), Incoming Packets**, **Outgoing Packets**, **Ratio (Out/In) Packets**. You can select 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.



Visualize the Network Topology (AWS)

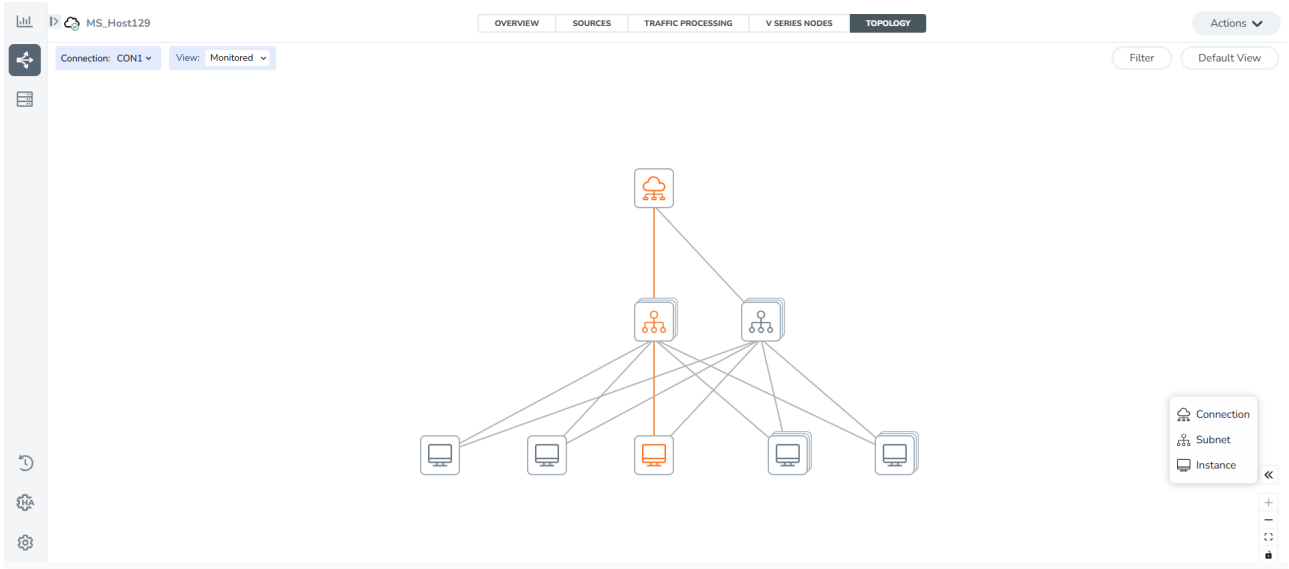
You can have multiple connections in GigaVUE-FM. Each connection can have multiple Monitoring Sessions configured within it. The Topology tab provides a visual representation of the monitored elements within a selected connection and Monitoring Session.

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.
4. 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.

5. From **View,** select one of the following instance types:
   - Fabric
   - Monitored



6. (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.
7. 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.

Administer GigaVUE Cloud Suite for AWS

You can perform the following administrative tasks in GigaVUE-FM for GigaVUE Cloud Suite for AWS:

- Manage a Monitoring Domain
- Check Permissions while Configuring GigaVUE Fabric Components using GigaVUE-FM
- Configure AWS Settings
- Interface Mapping (AWS)
- Configure Proxy Server
- Configure Certificate Settings
- About Events
- About Audit Logs
- High Availability for Cloud Infrastructure

Manage a Monitoring Domain

You can view the details of the Monitoring Domain that are created in the list view. The list view details can be viewed based on:

- Monitoring Domain
- VPC
- Fabric
- UCT-V
- UCT-V Upgrade

You can also filter the Monitoring Domain based on a specified criterion. The following filter options are available in the Monitoring Domain page:

- **Right filter:** Select the **Filter** button on the right to filter the Monitoring Domain based on a specific criterion.
- **Left filter:** Select the to filter the based on the Monitoring Domain and VPCs. You can select **+** to create a new monitoring domain. This filter, once applied, also works even when the tabs are swapped.

To edit or delete a specific Monitoring Domain,

1. Select the Monitoring Domain.
2. Select the ellipses.

When you select a Monitoring Domain, you can view details of it in a split view of the window. In the split view window, you can view the details such as **Configuration**, **Launch Configuration** and **V Series configuration**.

Monitoring Domain

The list view shows the following information in the monitoring domain page:

- Monitoring Domain

- VPC
- Tunnel MTU
- Acquisition Method
- Load Balancer
- Centralized VPC
- Management Subnet

NOTE: Select to select the columns that appears in the list view.

Use the following buttons to manage your Monitoring Domain:

Button	Description
New	Use to create new monitoring domain.
Manage Certificates	You can use this button to perform the following actions: • **Re-issue**- Certificates can be reissued to address security compromises, key changes, or configuration updates, like validity period adjustments. • **Renew**- Renewing a certificate just extends its expiration date and usually happens automatically unless you decide to do it during scheduled downtime. Auto-renewal is performed based on the duration specified in the **Certificate Settings** page. For details, refer to Configure Certificate Settings.

Button	Description
Actions	You can select a Monitoring Domain and then perform the following options: • **Edit Monitoring Domain**: Select a Monitoring Domain and then select **Edit Monitoring Domain** to update the configuration. • **Delete Fabric**: You can delete all the fabrics associated with the Monitoring Domain of the selected Fabric. • **Delete Monitoring Domain**: You can select a Monitoring Domain or multiple Monitoring Domains to delete them. • **Deploy Fabric**: You can select a Monitoring Domain to deploy a fabric, you cannot choose multiple Monitoring Domains at the same time to deploy fabrics. This option is only enabled when there is No FABRIC (launch configuration) for that specific Monitoring Domain and GigaVUE-FM orchestration is enabled. You must create a fabric in the monitoring domain, if the option is disabled • **Upgrade Fabric**: You can select a Monitoring Domain or multiple Monitoring Domains to upgrade the fabric. You can upgrade the V Series nodes using this option. • **Edit SSL Configuration**: You can use this option to add Certificate Authority and the SSL Keys when using the Secure Tunnels. • **Check Permissions**: You can use this option to validate whether policy attached to the GigaVUE-FM using "EC2 Instance Role" or "Access Credential" has the required IAM permissions and notifies the users about the missing permissions. • **View Permission Status Report**: You can use this option to get the reports of previously run **Check permissions**.
Filter	Filters the Monitoring Domain based on the list view options that are configured: • **Tunnel MTU** • **Acquisition Method** • **Load Balancer** • **Centralised Connection** • **Management Subnet** You can view the filters applied on the top of the Monitoring Domain page as a button. You can remove the filters by closing the button.

VPC

To view the VPC related details for a monitoring domain, select the **VPC** tab.

The list view shows the following details:

- VPC
- Monitoring Domain
- Status
- Fabric Nodes
- Credential
- Region

Fabric

To view the fabric related details for a monitoring domain, select the **Fabric** tab.

The list view shows the following details:

- VPC
- Monitoring Domain
- Fabric Nodes
- Type
- Management IP
- Version
- Status - Click to view the upgrade status for a Monitoring Domain.
- Security groups

You can use the Actions button to perform the following actions:

- **Edit Fabric**: You can select one fabric or multiple fabrics of the same Monitoring Domain to edit a fabric. You cannot choose different fabrics of multiple Monitoring Domains at the same time and edit their fabric components.
- **Delete Fabric**: You can delete all the fabrics associated with the Monitoring Domain of the selected fabric.
- **Upgrade Fabric**: You can select a Monitoring Domain or multiple Monitoring Domains to upgrade the fabric. You can upgrade the GigaVUE V Series Nodes using this option.
- **Generate Sysdump:** You can select one or multiple GigaVUE V Series Nodes (Maximum 10) to generate the system files. The generation of sysdump takes a few minutes in a GigaVUE V Series Node. You can proceed with other tasks, and upon completion, the status appears in the GUI. These system files are helpful for troubleshooting.For more information, refer to Debuggability and Troubleshooting

To view and manage the generated sysdump files, select the GigaVUE V Series Node and click the **Sysdump** tab in the lower pane.

To view the certificates associated with the fabric, select the fabric nodes and click the **Certificates** tab in the lower pane.

UCT-V

To view all the UCT-Vs associated with the available Monitoring Domains click the **UCT-V** tab.

The list view shows the following details:

- Monitoring Domain
- IP address
- Registration time

- Last heart beat time
- Mode
- Secure Tunnel Status
- Status
- Version

When an UCT-V is uninstalled, it moves to the **Unknown** status. If it remains in this state for more than 24 hours, GigaVUE-FM automatically removes it at 12:30 AM (system time), unless it is part of an active or scheduled upgrade.

UCT-V Upgrade

To upload and upgrade the UCT-V packages, select the **UCT-V** Upgrade tab . UCT-V Upgrade drop-down includes Dashboard, Jobs, and Images options.

Dashboard

The Dashboard list view shows the following details:

- Overview Stages
- UCT-V Upgrade Stages
- Name
- IP address
- Mode
- Type
- Monitoring Domain
- Fetch
- Install
- Verify
- Upgrade Status
- Image Version
- Image Type
- Health
- Registration Mode

Jobs

You can view Immediate and scheduled tasks in the Jobs tab. The list view shows the following details:

Immediate tab	Scheduled tab
Shows the following details: ▪ Task Name ▪ Task Status ▪ Created Time ▪ Created By ▪ Start Time ▪ End Time	Shows the following details: ▪ Task Name ▪ Task Status ▪ Created By ▪ Created Time ▪ Start Time ▪ End Time ▪ Scheduled Time ▪ Time Left

Images

The Images list view shows the following details:

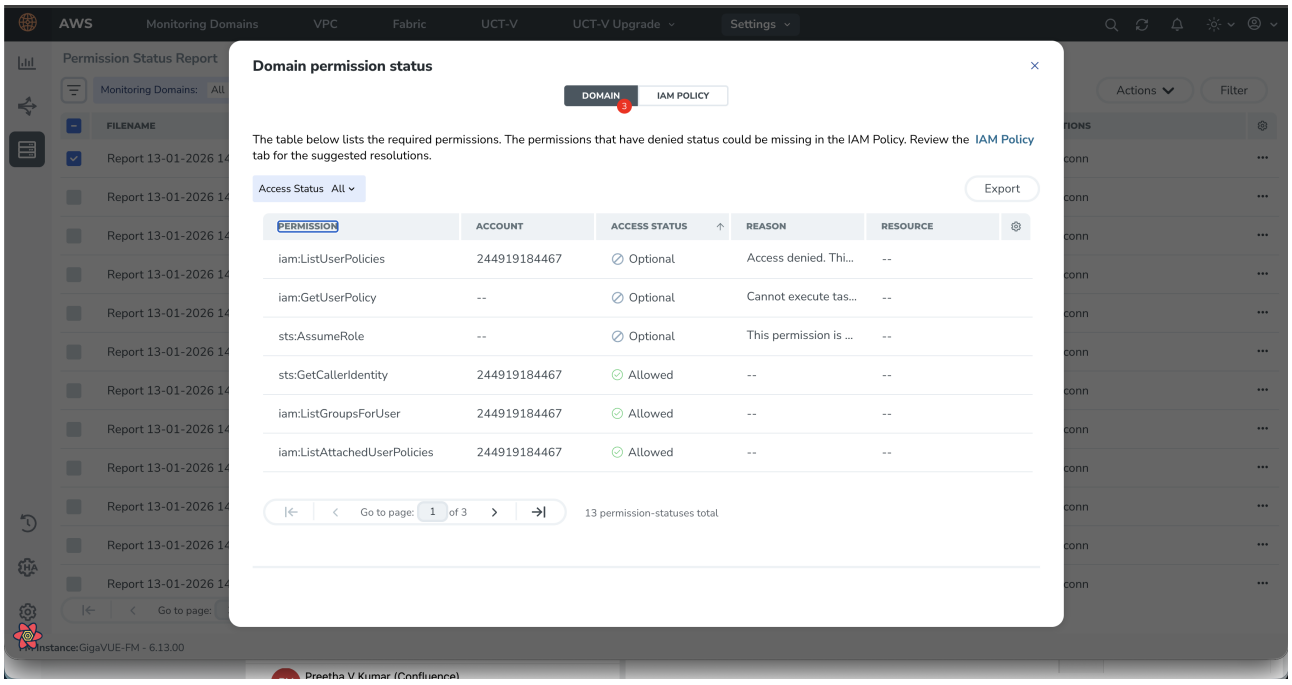
- Image Name
- Version
- Image Type
- Build Number
- Size

Check Permissions while Creating a Monitoring Domain

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

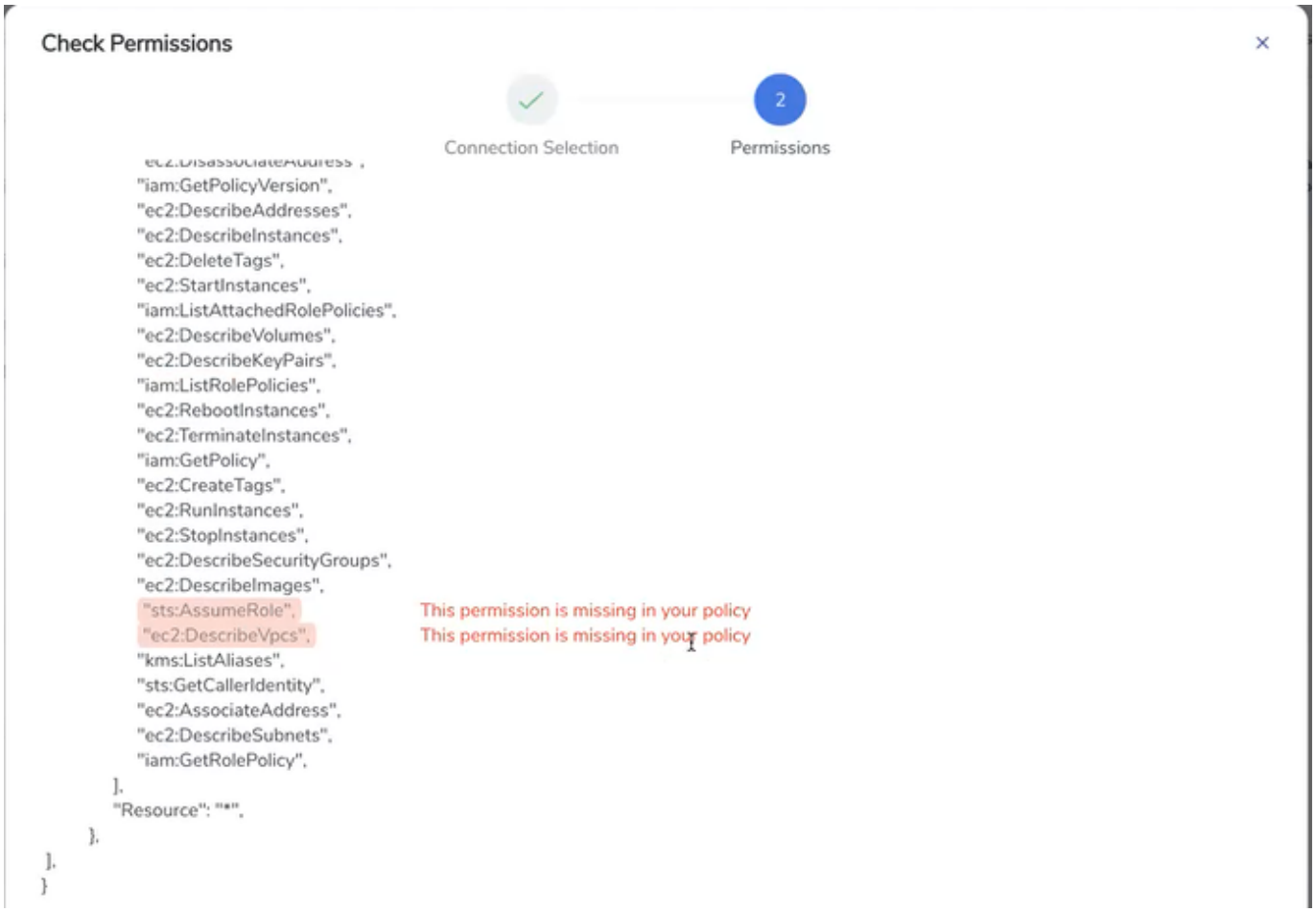
1. Go to **Inventory > VIRTUAL > AWS**, and then click **Monitoring Domain**. The **Monitoring Domain** page appears.
2. Select **New**. The **Monitoring Domain Configuration** page appears.
3. Enter the details as mentioned in the Create a Monitoring Domain section.
4. Select the **Check Permission** button. The **Check Permissions** widget opens.
5. Select the connection for which you wish to check the required permissions and then select **Next.**

6. Select the **Permission Status** to view the missing permissions. The **ACCOUNTS** tab lists the accounts and the following permissions status:
   - **Allowed** - The permission is granted and available for the Monitoring Domain.
   - **Optional** - The permission is not required for basic operation. It is recommended for specific advanced use cases, such as when inline policies or additional AWS features are configured.
   - **Denied** - This status is displayed if permission is missing.For Example: If a permission is not configured in the IAM policy or if the permission access is explicitly denied in Aws, then the status is displayed as Denied.
   - **Failed** - The permission check did not complete successfully due to an error such as a transient AWS issue, invalid configuration, or network problem. The permission state cannot be determined.
   - **notExecuted** - This status is displayed if a higher level of permission is denied or not configured, then GigaVUE-FM cannot validate a permission.For Example: If an IAM role policy permission(Iam:ListUserPolicy) is in denied or failed state, then the next-level permission (like IAM:getUserPolicy) cannot be validated.
7. Review the accounts that has an error in the permission status. The **PERMISSIONS** tab lists the permissions required to run GigaVUE Cloud Suite for AWS.
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 AWS. You must update the AWS IAM policy with the missing permissions that are highlighted in the JSON.

9. Go to the **PERMISSIONS** tab and select **Recheck** to recheck the IAM policy.



When you click Copy or Download, the entire JSON will be copied or downloaded.

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

You can view the permission status reports in the **Monitoring Domain** page. Permission status reports consist of previously run **Check permissions** reports. They are auto purged once every 30 days. You can change the purge interval from the **Advanced Settings** page. Refer to Configure AWS Settings for more detailed information.

To view permission status report, in the **Monitoring Domain** page, click **Actions > View Permission Status Report**. To view or delete individual reports, select the report and click **Actions** button.

Check Permissions while Configuring GigaVUE Fabric Components using GigaVUE-FM

To check for permissions from the AWS Fabric Launch page, follow these steps:

1. In the AWS Fabric Launch page, enter the details as mentioned in Check Permissions while Configuring GigaVUE Fabric Components using GigaVUE-FM.
2. Select the **Check Permissions** button.

   The **Check Permissions** widget opens. The widget displays the permission status for Inventory, Security Group, and Fabric Launch.
3. Select the **INVENTORY** tab and select **Check Inventory Permissions** to view the required inventory permissions.

   Inventory permissions with the access status **Denied** are missing in the IAM Policy or have a restricted boundary.
4. Select the **SECURITY GROUPS** tab and select **Check Security Group Permissions** to view the required ports.

   The ports need to open for the security groups. The ports in the **Denied** State are not open in the security group. The ports with the status **Explicit denied** are blocked or restricted by the user. The ports with status **Partially configured** have incorrect IP address.
5. Select the **FABRIC LAUNCH** tab and select **Check Fabric Launch Permissions** to view the permissions required for deploying the GigaVUE fabric components.

   The IAM Policy might be missing Virtual Machine permissions with the access status **Denied**.

   NOTE: The permissions **Microsoft.Compute/virtualMachines/write** and **Microsoft.Network/networkInterfaces/join/action** are dependent. You cannot validate them separately. So, if either of the permissions is denied or not configured, then both permissions are displayed as **Denied**.

The **IAM POLICY** tab lists the sample policy containing the required permissions for deploying the GigaVUE Cloud Suite for AWS. You must update the AWS IAM policy with the missing permissions that the JSON highlights.

Configure AWS Settings

This topic describes how to configure:

- Refresh intervals for instance and non-instance inventory.
- Maximum batch size for monitoring session updates.

To configure,

1. Go to **Inventory > VIRTUAL > AWS**.
2. Select **Settings > Advanced Setting**.

3. In the **Advanced Setting** page, you can edit the following details:

Settings	Description
Refresh interval for instance target selection inventory (secs)	Specifies the frequency for updating the state of EC2 instances in AWS.
Refresh interval for fabric deployment inventory (secs)	Specifies the frequency for deploying the fabric nodes
Number of UCT-Vs per V Series Node	Specifies the maximum number of instances you can assign to the GigaVUE V Series node. You can modify the number of instances for the nitro-based instance types
Refresh interval for UCT-V inventory (secs)	Specifies the frequency for discovering the UCT-Vs available in the VPC. **NOTE:** When you upgrade to version 6.5 or above, GigaVUE-FM resets the UCT-V Refresh Interval field to its default. To retain your custom value, you must manually reconfigure it.
Traffic distribution tunnel range start	Specifies the start range value of the tunnel ID.
Traffic distribution tunnel range end	Specifies the closing range value of the tunnel ID.
Traffic distribution tunnel MTU	Specifies the MTU value for the traffic distribution tunnel.
Permissions status purge interval in days	Specifies the number of days in which the permissions report must auto purge,
Use UCT-V conf file	Enable this option to allow interface mirroring to follow the configuration defined in the file. Disable it to mirror traffic from all physical interfaces. **Notes:** • When changing the UCT-V conf file option from **enabled to disabled**, ensure to undeploy the Monitoring Session and delete the Monitoring Domain. Once changed, create a new Monitoring Domain and configure the Monitoring Session.

Settings	Description
	• When changing the UCT-V conf file option from **disabled to enabled**, perform the following: a. Edit the uctv.conf file i. **Windows**: C:\ProgramData\Uctv\uctv.conf ii. **Linux**: /etc/uctv/uctv.conf b. Delete the skipConf file from the backup folder i. **Windows**: C:\ProgramData\Uctv\bak\skipConf ii. **Linux**: /var/lib/uctv/bak/skipConf c. Restart the UCT-V i. **Windows**: Restart from the Task Manager ii. **Linux**: sudo service uctv restart
Un-Registration Timeout For FabricNode (secs)	Specify the unregistration wait time between 150 to 900 seconds to control how long GigaVUE-FM waits before removing an unhealthy node; the default is 150 seconds.
Reboot threshold limit for UCT-V Controller down	Specifies the number of times GigaVUE-FM tries to reach UCT-V Controller, when the UCT-V Controller moves to down state. GigaVUE-FM retries every 60 seconds.

4. Select **Save**.

Interface Mapping (AWS)

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.

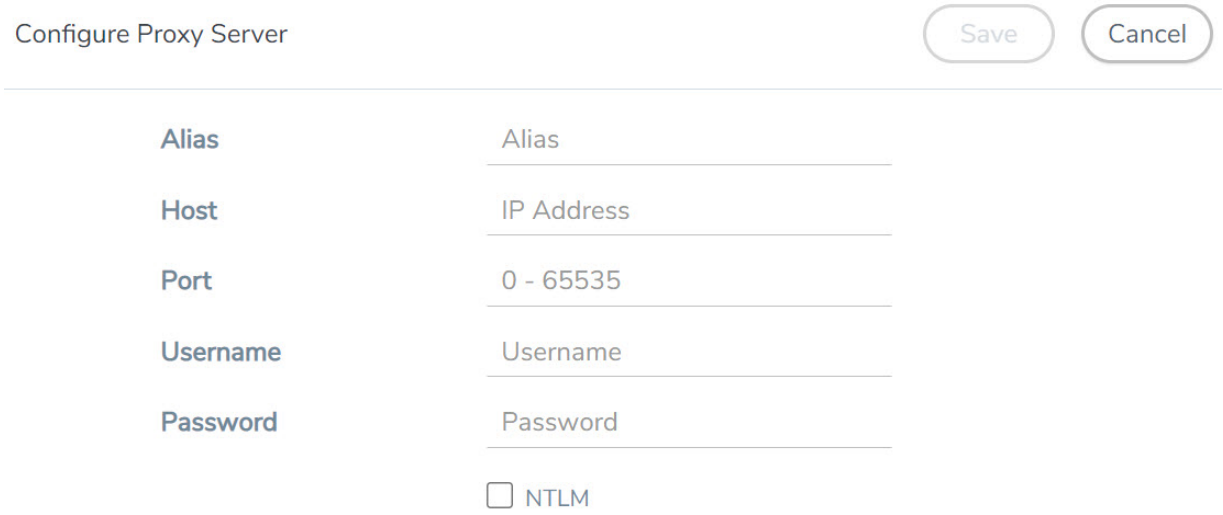
Configure Proxy Server

If the VPC hosting GigaVUE-FM does not have Internet access, GigaVUE-FM cannot reach AWS public API endpoints. You need to configure a proxy server to enable access.

Prerequisite: The fm_super_admin role or write access to the Infrastructure Management category.

To configure a proxy server,

1. Go to **Inventory > VIRTUAL > AWS**, and then select **Settings**.
2. From the Settings drop-down list, select **Proxy Server Configuration**.
3. Select **Add**. The **Configure Proxy Server** page is displayed.



4. On the page, enter the following details:
    a. In the **Alias** field, enter the name for the proxy server.
    b. In the **Host** field, enter the hostname or IP address of the proxy server.
    c. In the **Port** field, enter the port number the proxy server uses for connecting to the Internet(0–65535).
    d. (Optional) In the **Username** field, enter the proxy server username.
    e. In the **Password** field, enter the password for the proxy server.
5. (Optional) To use NTLM authentication, perform the following:
    - Select the **NTLM** checkbox.
    - Enter the **Domain** name of the client accessing the proxy server.
    - Enter the **Workstation** name or the computer accessing the proxy server.
6. Select **Save**.

The new proxy server configuration appears on the **Proxy Server Configuration** and AWS Connection pages.

Configure Certificate Settings

To configure certificate settings:

1. Go to **Inventory > VIRTUAL**.
2. Select your cloud platform.
3. Select **Settings > Certificate Settings**.
   The **Certificate Settings** page appears.
4. From the **Algorithm** drop-down list, select the algorithm that determines the cryptographic security of the certificate.

   NOTE: If selecting RSA 8192, the certificate generation may take longer due to the increased key size.
5. In the **Validity** field, enter the total validity period of the certificate.
6. In the **Auto Renewal** field, enter the number of days before expiration of the auto-renewal process should begin.
7. Select **Save**.

About Events

The Events page displays all the events occurring in the virtual fabric component, VM Domain, and VM manager. An event is an incident that occurs at a specific point in time. Examples of events include:

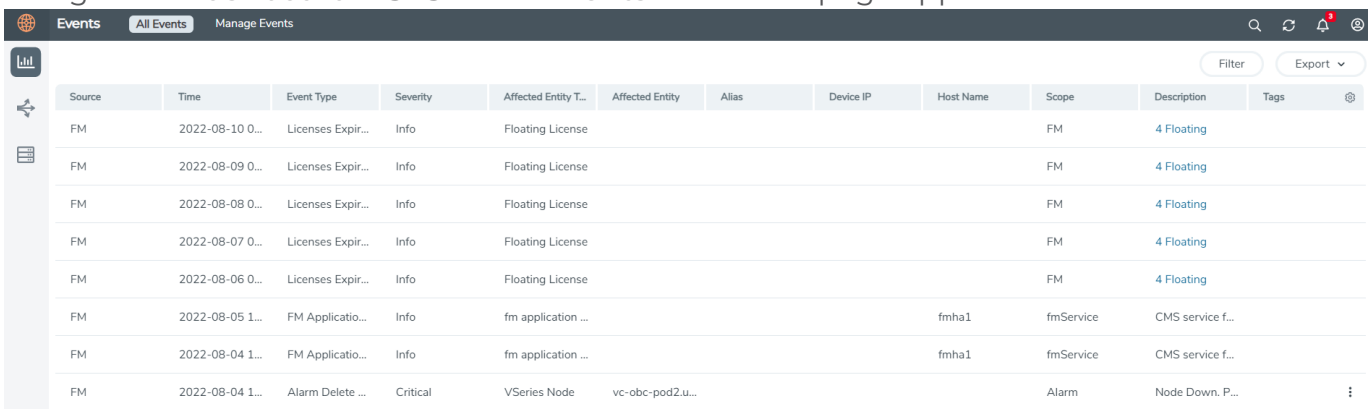
- Cloud provider License Expiry
- UCT-V Inventory Update Completed
- Cloud provider Connection Status Changed

An Alarm is a response to one or more related events. If an event is considered of high severity, then GigaVUE-FM raises an alarm. An example of alarm is your cloud provider license expiry.

The alarms and events broadly fall into the following categories: Critical, Major, Minor, or info.

Access Event

Navigate to **Dashboard > SYSTEM > Events**. The Event page appears.



The following table describes the parameters recording for each alarm or event. You can also use filters to narrow down the results.

Controls/ Parameters	Description
Source	The source from where the events are generated. The criteria are: • FM - indicates the event that the GigaVUE-FM fabric manager flagged. • VMM - indicates the event that the Virtual Machine Manager flagged. • FM Health - indicates the event that the health status change of GigaVUE-FM flagged.
Duration	The timestamp when the event occurred or the duration of the event. **IMPORTANT:** Timestamps or the duration appear in the time zone of the client browser's computer and not the time zone of the node reporting the event. The timestamp is based on the correctly configured clock on the GigaVUE-FM server and converted from UTC to the client computer's configured time zone.
Scope	The category to which the events belong. Events can belong to the following categories: Domain, Node, Card, Port, Stack, Cluster, Chassis, GigaVUE-FM, GigaVUE-VM, and so on. For example, if an event generates a notification for port utilization low threshold, the scope is displayed as Physical Node.
Alarm Type	The type of events that generates the alarms. The types of alarms are Abnormal Fan Operation, Card Unhealthy, Circuit Tunnel Unhealthy, CPU Over Loaded, Device Upgrade Failed.
Event Severity	The severity is one of Critical, Major, Minor, Warning, or Info. Info is informational messages. For example, when a power status change notification is displayed, the message is Info.

Controls/ Parameters	Description
Event Status	The status of the event. The status is either Acknowledged or Unacknowledged.
Event Type	The type of event that generated the events. The types of events are CPU utilization high, cluster updated, device discovery failed, fan tray changed, netflow generation statistics, and so on.
Affected Entity Type	The resource type associated with the event. For example, when a low disk space notification is generated, 'Chassis' is displayed as the affected entity type.
Cluster ID	Enter the Cluster ID.
Affected Entity	The resource ID of the affected entity type. For example, when low disk space notification is generated, the IP address of the node with the low disk space is displayed as the affected entity.
Device IP	The IP address of the device.
Host Name	The host name of the device.
Alias	Event Alias
Monitoring Domain	The name of the Monitoring Domain.
Connection	The name of the Connection.
Show Non-taggable Entities	Enable to display the events for entities that you cannot tag. For example, Policies, GigaVUE-FM instance, and other such entities.
Tags	Select the Key and the Value from the drop-down list.

To filter the alarms and events,

1. Select **Filter**.

   The Filter quick view is displayed.

2. Select the filtering criteria, and then select **Apply Filter**.

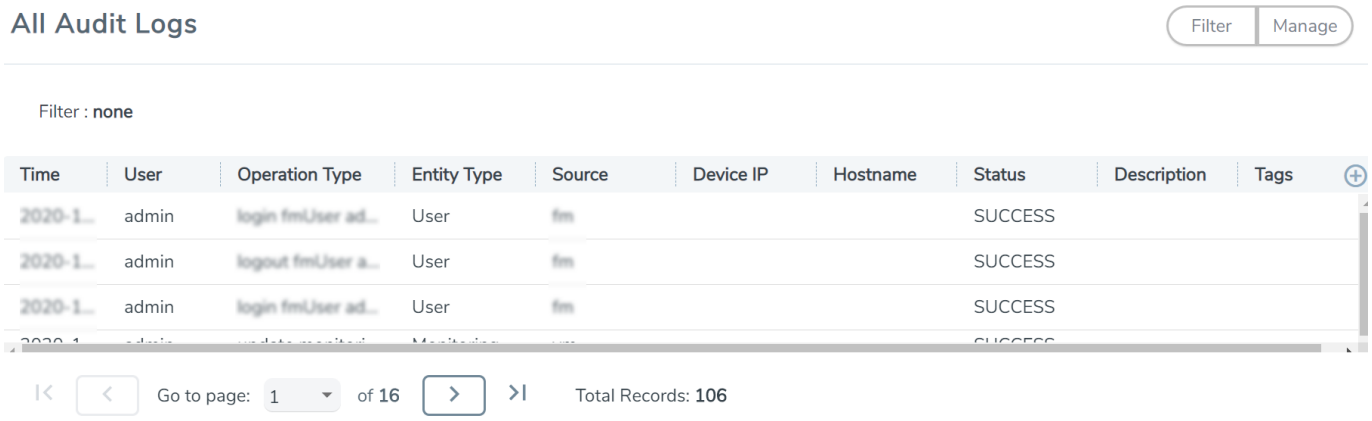
   The result appears on the Events page.

About Audit Logs

Audit logs track the changes and activities that occur in the virtual nodes due to user actions. You can filter the logs to view specific information.

Access Audit Logs

Navigate to **Dashboard > SYSTEM > Audit Logs**. The **All Audit Logs** page appears.



Parameters

The Audit Logs have the following parameters:

Parameters	Description
Time	Provides the timestamp on the log entries.
User	Provides the logged user information.
Operation Type	Provides specific entries that the system logs. For example, ▪ Log in and Log out based on users. ▪ Create/Delete/Edit tasks, GS operations, maps, virtual ports, and so on.
Source	Provides details about the usage either in GigaVUE-FM or on the node when the event occurred.
Status	Success or Failure of the event.
Description	For failed status provides a brief update on the reason..

NOTE: Verify if the GigaVUE-FM time is set correctly to ensure accuracy of the captured trending data.

Filtering the audit logs

You can filter to view specific type of logs based on the following criteria:

- **When**: Displays logs that occurred within a specified time range.
- **Who**: Displays logs related to a particular user or users.
- **What**: Displays logs for one or more operations, such as Create, Read, and Update.

- **Where**: Displays logs for GigaVUE-FM or devices.
- **Result**: Displays logs for success or failure.

To filter the audit logs,

1. Select **Filter**.

   A quick view for Audit Log Filters displays.

2. Specify one or all of the following:

   - **Start Date** and **End Date** to display logs within a specific time range.
   - **Who** limits the scope of what displays on the Audit Logs page to a specific user or users.
   - **What** narrows the logs to the types of operation that the log is related to. You can select multiple operations. Select **All Operations** to apply all operation types as part of the filter criteria.
   - **Where** narrows the logs to particular of system that the log is related to. Select **All Systems** apply both GigaVUE-FM and device to the filter criteria. **Result** narrows the logs related to failures or successes. Select **All Results** to apply both success and failure to the filter criteria.

3. Select **OK** to apply the selected filters to the **Audit Logs** page.

High Availability for Cloud Infrastructure

This section provides details about the GigaVUE-FM High Availability (HA) feature in Cloud environment and describes how to configure, upgrade, and troubleshoot the feature.

Refer to the following topics for details:

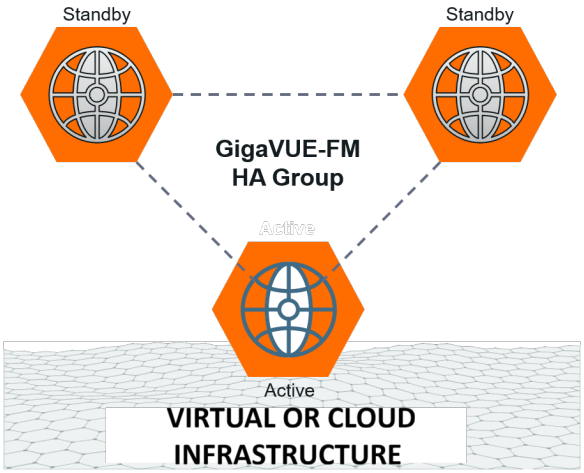
- About GigaVUE-FM High Availability
- Supportability Information
- Recommendations, Rules, Notes, and Limitations
- Licensing Information
- Hostname Setups
- Configure GigaVUE-FM HA
- Configure Secure Communication between Fabric Components in FMHA
- GigaVUE-FM HA Landing Page
- Remove Standby GigaVUE-FM Instance
- Disassemble GigaVUE-FM High Availability Group
- GigaVUE-FM High Availability States
- Fail over Mechanism

- GigaVUE-FM High Availability Scenarios
- Troubleshoot GigaVUE-FM High Availability Issues

About GigaVUE-FM High Availability

The GigaVUE-FM High Availability (HA) feature supports a highly available fabric management environment with minimal interruption. The GigaVUE-FM HA architecture consists of a minimum of three GigaVUE-FM instances that run together as a highly available group. The highly available group provides protection from failure of any one of the members in the group. The communication between the GigaVUE-FM instances in the highly available group can be encrypted using Pre-shared Secret Key or Certificate based Authentication.

The following image shows the high-level architecture of the GigaVUE-FM HA feature.



GigaVUE-FM allows you to add more than three GigaVUE-FM instances to the HA group (up to 7). The hardware requirements and resource allocation process for the additional instances are the same as that of the active and standby instances. The additional instances can be configured either as supporting instances or as active-eligible instances:

Supporting instances

Supporting instances are GigaVUE-FMs that run minimal services, thereby providing more resources to OpenSearch services. These instances:

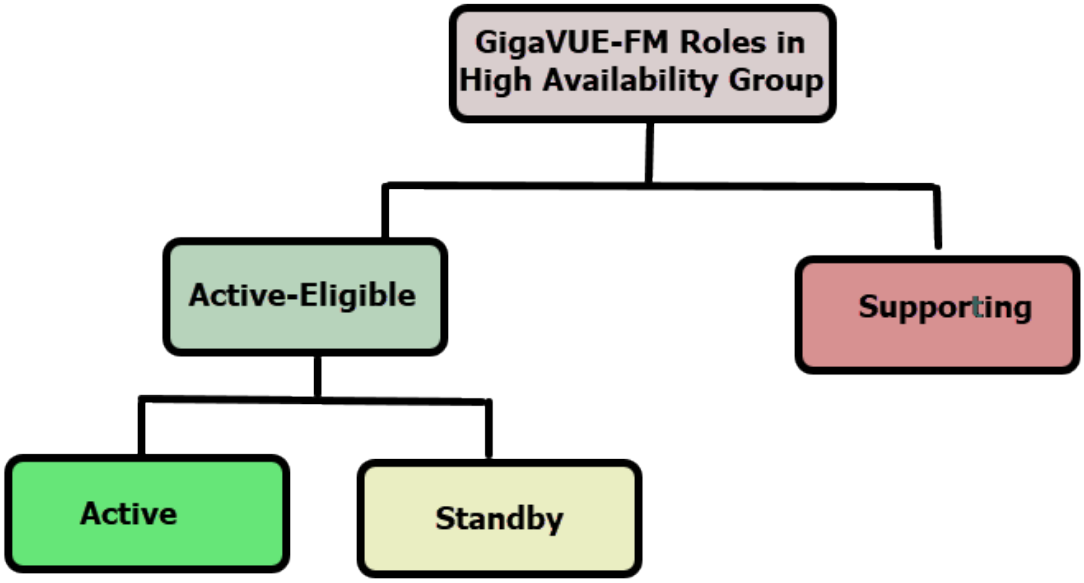
- Do not distribute application requests, as all application services are disabled by default.
- Do not participate in distributed services
- Provide enhanced scalability.
- Are excluded from active instance election

Active-Eligible instances

Active-Eligible instances are GigaVUE-FMs that distribute application requests and run distributed services. These instances:

- Enhance fault-tolerant and high available system.
- Are eligible for active instance election.

Refer to the following diagram for the roles in the HA group.



NOTE: When you add a GigaVUE-FM instance as either a supporting instance or a standby instance, the current configuration of that GigaVUE-FM instance will be removed once it is added to the existing GigaVUE-FM HA cluster.

Gigamon cloud solution deployments in GigaVUE-FM HA are supported on both public and private platforms. These deployments can operate in one of the following modes:

- GigaVUE-FM Orchestrated
- Third-party Orchestrated (Generic / Integrated)

In either scenario, you need to first launch GigaVUE-FM and run.

GigaVUE-FM Orchestration

Using GigaVUE-FM orchestration, you can deploy GigaVUE Fabric Components through the GigaVUE-FM user interface. After launching GigaVUE-FM and applying the required license, you can deploy components such as the GigaVUE V Series Node, GigaVUE V Series Proxy, and UCT-V Controller.

Once the deployment is complete, GigaVUE-FM continuously monitors the health and status of the deployed components. If any error condition occurs, GigaVUE-FM automatically relaunches or replaces the affected component to ensure system reliability.

Third-party Orchestration

With this method, you deploy GigaVUE Fabric Components using external orchestration solutions. GigaVUE-FM does not manage the deployment process directly, but you can still use it to monitor the health of the deployed components.

To enable monitoring, you need to provide an additional configuration file during deployment. This file allows components like the GigaVUE V Series Node, GigaVUE V Series Proxy, UCT-V Controller, UCT-V, UCT-C, and GCB to register with the Monitoring Domain in GigaVUE-FM . Refer to the following sections for more details:

- Deploy UCT-C Solution in Kubernetes
- Deploy GCB Controller Service and Pods

Supportability Information

The GigaVUE-FM HA feature is supported on the following platforms:

Orchestration Method	Platforms/components Supported
GigaVUE-FM Orchestration	• AWS • Azure • OpenStack • VMware ESXi • VMware NSX-T • Nutanix
Third-party Orchestration	**Generic Mode** • AWS • Azure • OpenStack • VMware ESXi • VMware NSX-T • Nutanix • GCP • UCT-C • GCB **Integrated Mode** • AWS • Azure • OpenStack

Recommendations, Rules, Notes, and Limitations

Keep in mind the following recommendations, rules and notes when you configure the GigaVUE-FM HA feature:

Recommendations

- Do not configure GigaVUE-FM High Availability (HA) across multiple regions or multi-cloud environments. This setup is not recommended and may lead to instability.
- You can deploy HA across multiple availability zones within the same cloud region. Ensure that you deploy a GigaVUE-FM instance in each availability zone.
- Use the orchestrated upgrade procedure to upgrade the GigaVUE-FM instances.
- It is recommended to configure reverse DNS configuration while configuring FMHA with FQDN.
- When creating a GigaVUE-FM HA group, it is highly recommended to create the High Availability group using DNS name. GigaVUE-FM HA cannot manage the individual GigaVUE-FM instances if the IP address changes (if GigaVUE-FM IP(s) are dynamic).

Rules and Notes

- GigaVUE-FM cannot support more than 7 active-eligible nodes (this is due to the underlying constraint in MongoDB).
- The GigaVUE-FM instances in the HA group must be identical in terms of system configuration such as hard disk, memory, and network interfaces, which include domain server, NTP server, and name server. Domain server, NTP server, and name server should be configured in all GigaVUE-FM instances.
- The GigaVUE-FMs in the high availability group can be accessed using the IPv4/IPv6 address (DNS name) that is used to form the High Availability group.

  > **NOTE:** Do not access all the GigaVUE-FM instances at the same time, as this will impact the performance of the HA group.

- You can deploy the GigaVUE-FM HA virtual machines on a WAN link with a maximum latency of 200 ms.
- You cannot add a GigaVUE-FM Hardware Appliance and a GigaVUE-FM virtual machine in the same HA group.
- The **`Reload All`** or **`Reload any FM`** commands will work only if there is an active GigaVUE-FM instance in the HA group.
- You must ensure that NTP is configured across all FM HA nodes.
- The GigaVUE-FM HA Cluster functions like standalone GigaVUE-FM's when a fail-over occurs during long-running operations, such as Fabric Launch, Monitoring Session Deployment, or Fabric Upgrade.
- When FMHA is configured with a reverse proxy, access to GigaVUE-FM requires non-SAML authentication, such as local authentication. Use the following sample URL to access GigaVUE-FM:

  ```
  https://<proxy_ip>/admin
  ```

- If GigaVUE-FM has multiple IPv6 addresses, ensure FMHA uses the permanent IPv6 as the source IP. GigaVUE-FM excludes temporary IPv6 addresses from the IP set, which causes connection failures and FMHA formation issues.

Shrinking the size of the HA group:

- When reducing the size of a HA group that has both active-eligible and supporting instances, it is always recommended to remove the supporting instances first so that the active-eligible instances remain intact in the HA group. If active-eligible instances are removed first from the HA group, then the HA group will become unstable. This, however, depends on the number of active-eligible and supporting instances in the HA group. Consider a GigaVUE-FM HA group with 7 instances. The number of active and supporting instances in a HA group may be as follows:

HA group 1	With 3 active instances and 4 supporting instances	The recommendation is specifically applicable for HA group 1 in which there are only 3 active eligible instances in the group. Removing the active-eligible instances may cause the HA group to become unstable.
HA group 2	With 5 active instances and 2 supporting instances.	The recommendation is not applicable for HA group 2 as removing the active-eligible instances will not impact the stability of the HA group.

  For a HA group to be stable, it must have a minimum of two active-eligible instances in the group.
- When reducing the size of HA group from 7 instance to 5 instance or 3 instance, the quorum is re-computed and adjusted accordingly. This is to ensure that the HA group remains intact with the available set of instances.

- When reducing the size of the HA cluster, during removal of an instance make sure to give time for the OpenSearch to rebalance and return to a complete (100%) healthy state before removing the next instance. If you remove the instances subsequently one after the other, the health state of the HA group will turn red as there will be no time for shard rebalancing amongst the available instances.
  Login to GigaVUE-FM CLI as a root user and execute the following command to check the ES cluster health:

  ```
  curl -XGET "http://localhost:9200/_cluster/health?pretty"
  ```

Supporting GigaVUE-FM Instances:

- When a supporting instance is added to the HA group, its system information will not be available immediately and will be available only after a minute.
- When the HA group is upgraded, application services of the supporting instances will be turned on automatically for the upgrade and once GigaVUE-FM HA upgrade is completed it will be turned off automatically. Application services will be turned off automatically irrespective of the upgrade completion status, that is, either success or failure.

Notes:

- For supporting instances, system information will be populated into MongoDB as the Application Service is down by default (scheduler populates the system information every minute into MongoDB). Hence any changes in the system hostname or GigaVUE-FM version will be reflected in the GUI only after a minute.
- In case of suspended mode, MongoDB will go into write protected mode. Therefore, any system related updates performed in the supporting nodes will not be reflected in the GUI.
- If the supporting instance is not reachable, all system related information that is populated in the GUI reflects the previous known values and not the latest values for Application Status, Up Time, and other system related information.
- Whenever the application services are up and running, events will be logged in the Events page (with the severity level - Info)

Licensing Information

You must install a Prime license on the active GigaVUE-FM instance to configure a High Availability group.

If the Prime license expires or if you accidentally delete the license, the existing configurations will still be present in the GigaVUE-FMs that are part of the HA group, but you will not be able to perform any new configurations. Moreover, if you disassemble the HA group, you cannot reconfigure the HA group without installing a valid Prime license. You can re-use the same Prime license to form the HA group again.

Hostname Setups

The GigaVUE-FM instances are not required to be in the same subnet, but still must be able to communicate with each other.

In addition, ensure that the instances have unique host names. You must be able to ping a GigaVUE-FM instance from the other instances using the hostname or the IP address.

To add a GigaVUE-FM instance to a GigaVUE-FM HA group:

- The GigaVUE-FM instances in the HA group must be reachable to each other.
- If host names are used to configure the HA group, the host names of the GigaVUE-FM instances must be resolvable through a DNS server.

Configure GigaVUE-FM HA

To configure the GigaVUE-FM HA feature, you must have access to at least three authenticated GigaVUE-FM instances that reside on a trusted network. All GigaVUE-FM instances must run the same software version. The interfaces in the GigaVUE-FM instances must be up and must be assigned IPv4/IPv6 addresses. You can also choose to use DNS host names.

NOTE: You can configure the GigaVUE-FM HA feature only if you have administrative privileges. You must have Prime license installed for forming the GigaVUE-FM HA group.

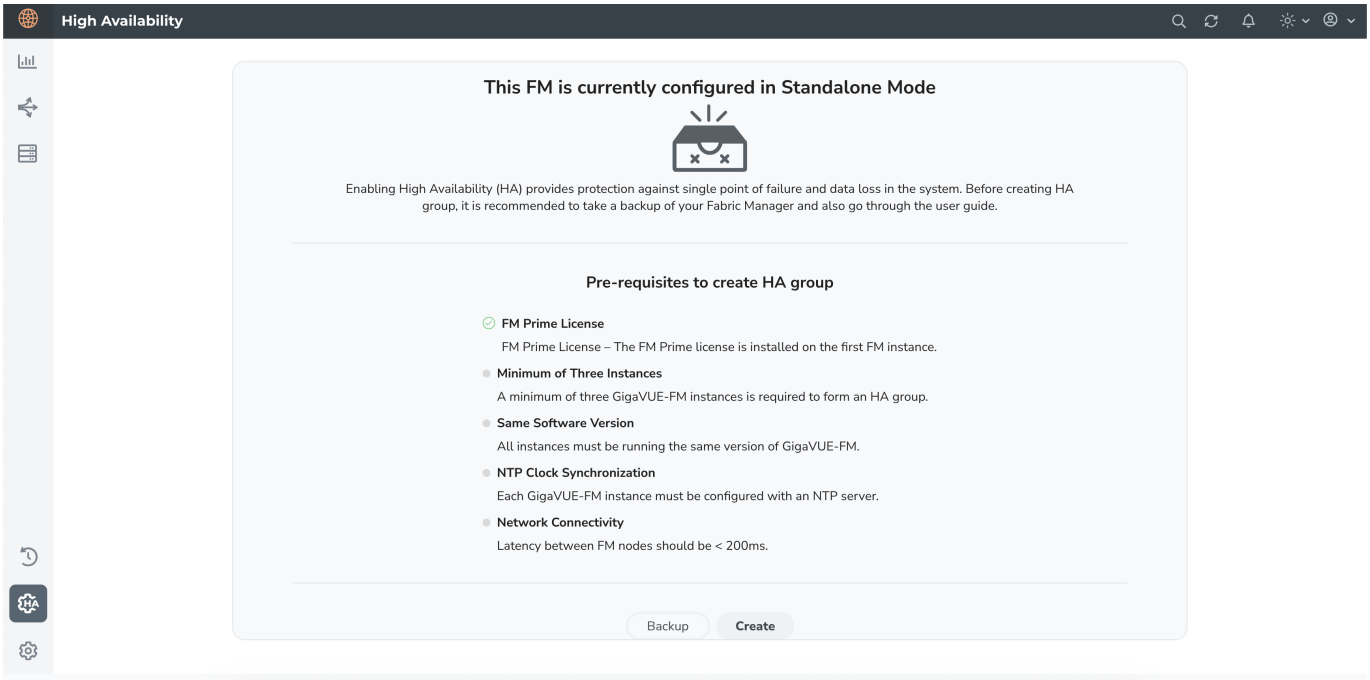
Refer to the following sections:

- Create and Add GigaVUE-FM Instances to HA Group
- Connect GigaVUE-FM High Availability to a Monitoring Domain using GigaVUE-FM Orchestration
- Connect GigaVUE-FM High Availability to a Monitoring Domain using Third Party Orchestration
- Integrate GigaVUE-FM High Availability with UCT-C
- Integrate GigaVUE-FM High Availability with Gigamon Containerized Broker

Create and Add GigaVUE-FM Instances to HA Group

To add instances and to configure the HA group:

1. Go to High Availability. The launch page displays the required prerequisites to create a HA group.



2. Click **Create**. In the **Group Name** field, enter a unique name for the HA group.

   NOTE: Avoid using functionality names as the group alias when creating an FMHA group. Functionality names typically refer to actions or operations within the system and can cause confusion and conflicts. Choose a unique and descriptive name instead.

3. Choose any one of the following options to encrypt the communication between nodes:
   - **Pre-shared Secret Key** – Encrypts communication between GigaVUE-FM nodes using an application-managed shared secret key. Refer to Encryption of Communication between FMHA Nodes.
   - **Certificate Based** – Encrypts communication between GigaVUE-FM nodes using manually uploaded certificates. Refer to Encryption of Communication between FMHA Nodes.
4. In the **Add GigaVUE-FM Instance** section, the details of the GigaVUE-FM instance from which the HA group is created will be fetched automatically.

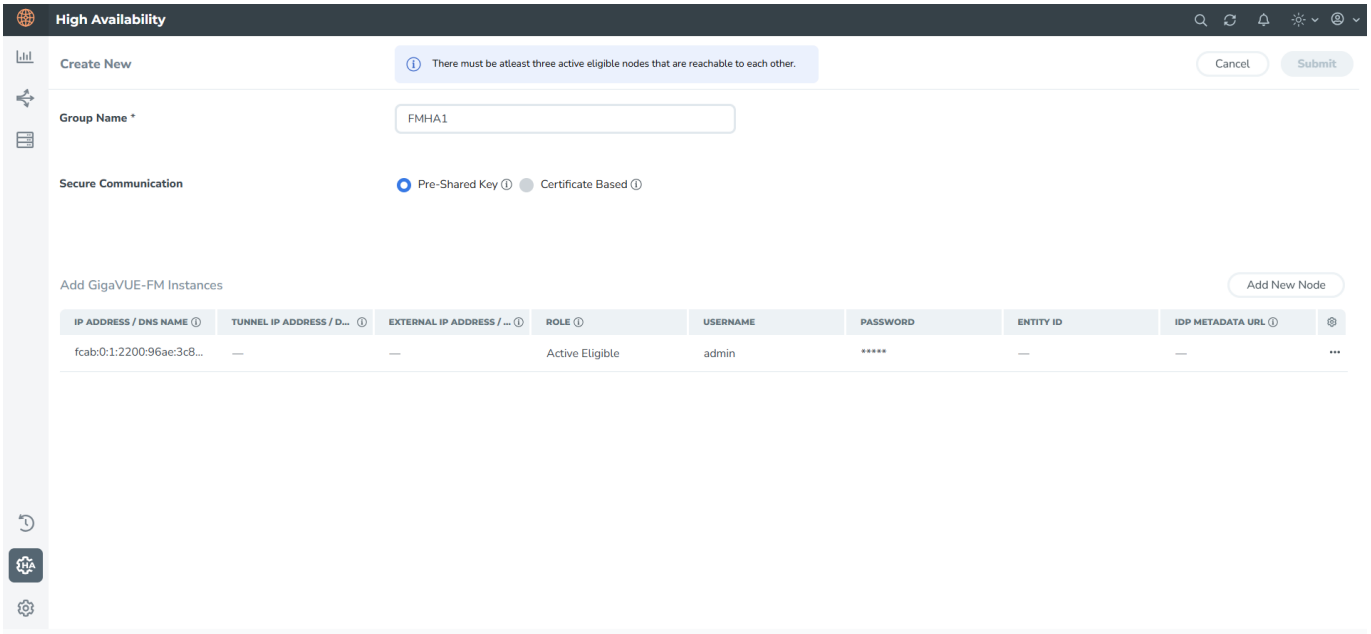
Edit the Primary Node

1. On the first instance, click the ellipses icon and select **Edit Node**.
2. Enter the following details: (These fields are optional)
   - Select the **Use Tunnel IP** check box to enable tunnel configuration. Selecting this check box reveals two additional fields:

- **Tunnel IP Address/DNS Name**: IP address used for establishing the secure communication tunnel between HA instances. This is required when the instances are reachable only through public or external IP addresses.
- **External IP Address / DNS Name is same as Tunnel IP Address / DNS Name**: If you check this box, GigaVUE-FM automatically copies the value from the Tunnel IP field to the External IP field and disables manual editing. If you uncheck it, the External IP field becomes editable again, retaining the previously entered value.

o Enter the Entity ID and the IdP Metadata URL.

3. Click the **save** icon to save the configuration. Refer to Additional Fields for details about other fields displayed on the HA page.



Add New Node

1. Click **Add New Node** to add the GigaVUE-FM instances. Enter the following details.:
   - **IP Address/DNS Name** - IP address/DNS name of the GigaVUE-FM instances (for communication between the GigaVUE-FMs and to configure the HA group). It is always recommended to use the DNS name while creating the GigaVUE-FM High Availability group.
   - (Optional) Select the **Use Tunnel IP** check box to enable tunnel configuration. Selecting this check box reveals two additional fields:
     - **Tunnel IP Address/DNS Name**: IP address used for establishing the secure communication tunnel between HA instances. This is required when the instances are reachable only through public or external IP addresses.
     - **External IP Address / DNS Name is same as Tunnel IP Address / DNS Name**: If you check this box, GigaVUE-FM automatically copies the value from the Tunnel IP field to the External IP field and disables manual editing. If you uncheck it, the External IP field becomes editable again, retaining the previously entered value.

- When you add a new node with a Tunnel IP address to an existing HA group, the FMHA table updates to reflect the information in the newly added column.

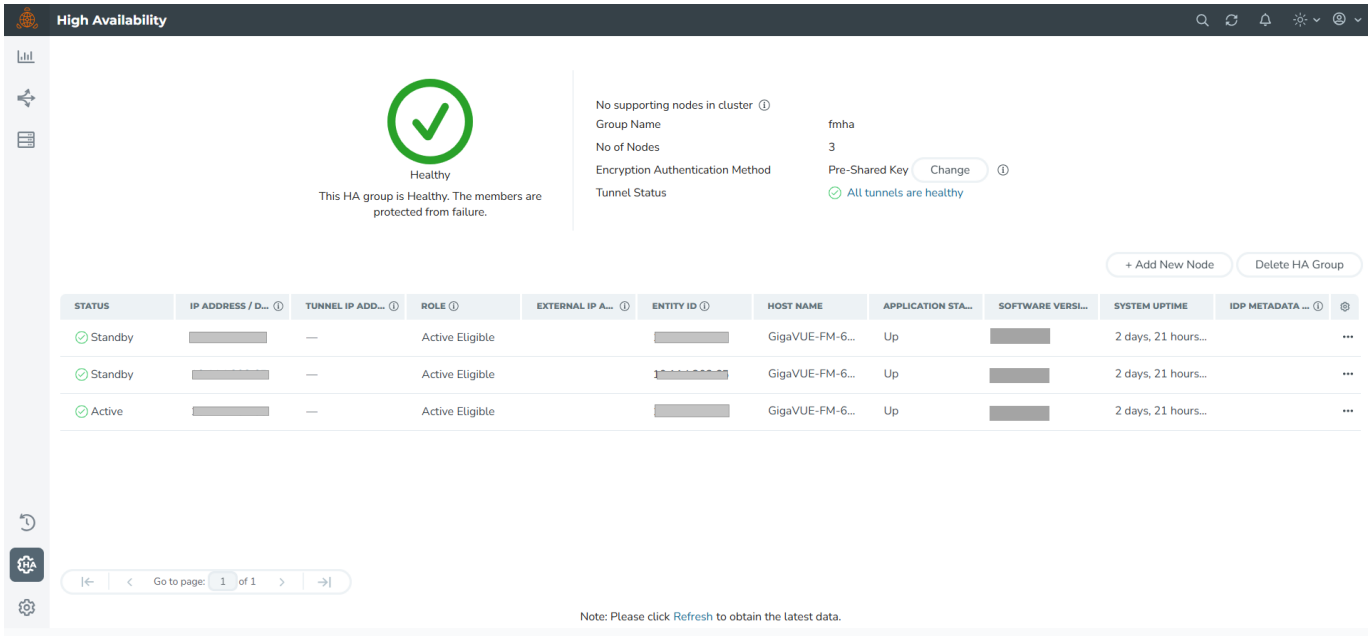
Notes:

- When you add a new node with a Tunnel IP address to an existing HA group, the FMHA table updates to reflect the information in the newly added column.
- When using unique DNS for HA cluster configuration, ensure it always resolves to only one IP address—not multiple IPs.

- **Role** - Role of the GigaVUE-FM instance. Can be configured as below. Refer to Active-Eligible instances for details.
  - **Active Eligible**- provides resiliency and load distribution.
  - **Supporting Node**- provides scalability and performance.
- **Username** - GigaVUE-FM GUI Username.
- **Password** - GigaVUE-FM GUI password.
- (Optional) **Entity ID** - Unique alphanumeric ID assigned to the GigaVUE-FM instance
- (Optional) **IdP Metadata URL** - URL pointing to the IdP's XML configuration

2. Click **Save** to validate the details entered for the instances.

Use the **Add New Node** button to continue to add the GigaVUE-FM HA instances. You can click the **Edit Node** icon to change the external IP address. After adding the instances to the HA group, click **Submit**. The HA group is configured and will be displayed as follows. Refer to Additional Fields for details about other fields displayed on the HA page.



Notes:

- When switching between the Pre-shared Secret Key and Certificate-Based options for encrypting communication between nodes, it's important to refresh the GigaVUE-FM to see the updated tunnel status. By clicking the link in the **Tunnel Status**, GigaVUE-FM displays the health status of the FMHA nodes.
- When creating a HA group, all the existing data on the first configured GigaVUE-FM instance will be preserved, allowing the system to continue using the data after it is fully set up. However, the data on the subsequent nodes will be lost during the setup.

The HA page also displays the following details:

Table 2: Additional Fields

Field	Description
Status and Reachability	Status of the GigaVUE-FM instances. Can be: • Active • Standby • Supporting Refer to Active-Eligible instances for details. Reachability: • - indicates that the instances are reachable. • - indicates that the instances are unreachable.
Host Name	Host name of the GigaVUE-FM instance.
Application Status	Status of application services that are responsible for handling the user requests: • **Up**: Indicates service is ready to handle the user requests • **Down**: Indicates service is not ready to handle the user requests with one or more underlying services being down. • **In Progress**: A state that appears between up and down indicating that the services are initializing.
Software Version	Software version of the GigaVUE-FM instance.
System Uptime	Time since the instance is up and active.
Third Party Authentication URL	Third party authentication URL required for SSO configuration.
Upgrade Status	Upgrade status of GigaVUE-FM. This is displayed only when the upgrade is triggered. Otherwise, this field is empty.

You can also remove the instances from the HA group and reduce the size of the HA group as required. However, while removing the instances ensure to retain the quorum[1] number of instances.

[1]Quorum number of instances is the minimum number of instances that must be active-eligible in a HA group. In a HA group with five instances, the quorum number is 3 (based on the formula n/2+1)).

NOTE: To scale components such as Fabric Health Analytics, topology visualization and to improve the performance of GigaVUE-FM by fully utilizing the resource available, it is recommended to configure three active eligible instances and additional supporting instances.

The following are the behavioral changes observed in the HA group with active, standby and supporting instances:

Task	Scenario	Behavior
Upgrade Operation	Few instances not being up (either active-eligible or supporting instances not up)	Upgrade will not be initiated.
	Few supporting instances are removed from the HA group after formation of the group	Upgrade will be initiated, and the supporting instances present in HA group will be upgraded first followed by the active-eligible instances.
	All instances are up and running	Upgrade will be initiated in an active instance. Upgrade will be done in a rolling fashion starting with supporting instances and ending with the active-eligible instances.
System Configurations	All instances are active-eligible	All GigaVUE-FM's GUI will be accessible, and user can configure the system through the same
	HA with active-eligible and few Supporting instances	For supporting instances, GUI will not be available (as application service is shut down). An option is provided in the GUI to turn on the application service and its dependent service(s) and the status can be seen in HA page. You can then configure the system related configuration from the logged in GigaVUE-FM instance once the application status of the supporting instance is up.
Background processes		

-FM Service Distribution	All GigaVUE-FMs are active-eligible instances.	Services will be equally distributed/redistributed among the instances based on the availability of the instances.
	HA group with active-eligible instances and supporting instances.	Services will be distributed/re-distributed only to active eligible instances
-Load Balancer	All GigaVUE-FMs are active-eligible instances.	All GigaVUE-FM API requests will be distributed to all instances in the HA group.
	With supporting instances.	All GigaVUE-FM API requests will be distributed only to active-eligible instances.

Connect GigaVUE-FM High Availability to a Monitoring Domain using GigaVUE-FM Orchestration

When fabric nodes need to communicate with GigaVUE-FM using public IP addresses, you should enable the **Use Public IP** option during Monitoring Domain creation. When **Use Public IP** option is enabled, GigaVUE-FM pushes its public IP address to Fabric Nodes. Fabric Nodes use this IP to communicate back to FM. FM does not initiate communication using its private IP. This setting is essential in cloud or hybrid environments where private IPs are not reachable, such as across cloud platforms. It ensures that GigaVUE-FM can send notifications and accept registrations using an externally accessible IP. Refer to Supportability Information for the list supported platforms.

Connect GigaVUE-FM High Availability to a Monitoring Domain using Third Party Orchestration

Fabric Nodes can be configured with either the IP address (remoteIP) or the Fully Qualified Domain Name (FQDN) (remoteAddress) of GigaVUE-FM to establish communication. The node sends registration requests to GigaVUE-FM until it successfully registers. In High Availability mode, if a node fails to register with one GigaVUE-FM instance, it automatically attempts registration with the next available GigaVUE-FM in its list until successful. Refer to Supportability Information for the list supported platforms.

Use the following data to manually configure **/etc/gigamon-cloud.conf** with registration configurations to register the fabric components with GigaVUE-FM.

```
Registration:
    groupName: <Monitoring Domain Name>
    subGroupName: <Connection Name/Alias>
    token: <Token>
    remoteAddress: <remoteIPs/FQDN of the GigaVUE-FM>
```

```
    remotePort: 443
    sourceIP: <IP address of the fabric node>
    nameServer: <DNS server's IP address>
    usePublicIP: <true/false>
    preferV6: <true/false><If set to true IPv6 will be preferred over IPv4, used only for DNS
resolution>
```

Notes:

- Configure either remoteIP or remoteAddress—not both. Using both prevents the node from registering with GigaVUE-FM.
- Remote IP will continue to work as expected. However, if you plan to use FQDN, update the configuration to use the Remote Address field instead.
- When configuring a remote address, you can specify multiple IP addresses. However, if you use a FQDN, ensure that you configure only one address
- FQDN configuration requires a valid nameserver.
- Ensure that the FQDN configured for Third Party Orchestration resolves to all IP addresses in the High Availability cluster.

Integrate GigaVUE-FM High Availability with UCT-C

UCT-C supports integration with GigaVUE-FM in high availability mode. You can configure the controller with either a Fully Qualified Domain Name (FQDN) or a comma-separated list of GigaVUE-FM IP addresses in the Helm configuration. The controller iterates through the provided FQDN or IP list and attempts to register with the master GigaVUE-FM node. If the GigaVUE-FM IP changes, you must update the configuration again. This enhancement enables UCT-C to maintain connectivity and recover from GigaVUE-FM failover events in HA deployments.

Below are the communication parameters:

- **fm_fqdn** – Specifies the GigaVUE-FM HA FQDN value used by the UCT-C Controller for communication with the GigaVUE-FM HA group. When this parameter is set, the controller uses the IP addresses resolved from the FQDN.
- **fmha_ip_list** – Specifies a comma-separated list of GigaVUE-FM HA IP addresses used by the UCT-C Controller for communication with the GigaVUE-FM HA group. If fm_fqdn is not set, the controller uses the IP addresses provided in fmha_ip_list by default.

Integrate GigaVUE-FM High Availability with Gigamon Containerized Broker

GigaVUE-FM High Availability group can be configured in an Gigamon Containerized Broker through a DNS Server in which the GigaVUE-FM instances are launched and deployed in the Gigamon Containerized Broker environment.

For GCB to make use of high availability feature of GigaVUE-FM, you must configure the FQDN (Fully Qualified Domain Name) of the GigaVUE-FM.

In a standalone GigaVUE-FM, the GCB uses the FQDN name of the GigaVUE-FM (if configured). It uses the legacy method of using the configured IP address when:

- The FQDN is not configured or
- The GCB fails to resolve to an IP address.

For example:

GCB Controller YAML file:

```
env:
- name: GCB_CNTLR_EXT_IP_DNS
value: "10.xxx.xx.xx" (IP address of the DNS server – external to the Kubernetes cluster)
- name: FM_FQDN
value: "fm.myorg.com" (FMs FQDN that is used for DNS lookups)
```

NOTE: The FQDN identifies either a standalone GigaVUE-FM or an FMHA cluster that includes multiple GigaVUE-FM instances. It returns the IP addresses (IPv4, IPv6, or both) for all GigaVUE-FMs associated with that FQDN.

For more details on the GigaVUE-FM High Availability configuration, refer to the *GigaVUE Administration Guide guide*.

Configure Secure Communication between Fabric Components in FMHA

IMPORTANT: Before upgrading the Fabric Components to version 6.10 or later, complete the following steps after upgrading GigaVUE-FM to version 6.10 or later.

Follow these steps:

1. Access the active GigaVUE-FM via CLI.
2. Archive the stepCA directory using the following commands:
   ```
   sudo su
   cd /var/lib
   tar -cvf /home/admin/stepca.tar stepca
   ```
3. Set the permissions of the tar file using the following commands:
   ```
   chmod 666 /home/admin/stepca.tar
   ```
4. Copy the tar file to all standby instances in the **/home/admin/ directory** using scp:
   ```
   scp /home/admin/stepca.tar <standby-node>:/home/admin/
   ```
5. Download the **runstepca_fmha** script from the Community Portal.
6. Log in to the standby instance using CLI.
7. Copy the script in the standby instance in the **/home/admin directory** and execute it using the following command:
   ```
   sh /home/admin/runstepca_fmha
   ```

GigaVUE-FM HA Landing Page

When you log in to any instance in the HA group, the Dashboard page appears. On specific pages, you can use the instance dropdown list in the page header to view information for a particular instance.

Remove Standby GigaVUE-FM Instance

To remove or replace a standby GigaVUE-FM instance from the GigaVUE-FM HA group follow the below listed steps:

1. Go to High Availability.
2. Click the ellipsis on the standby GigaVUE-FM instance widget in the High Availability page as shown in Figure 1Remove Standby GigaVUE-FM Instance.

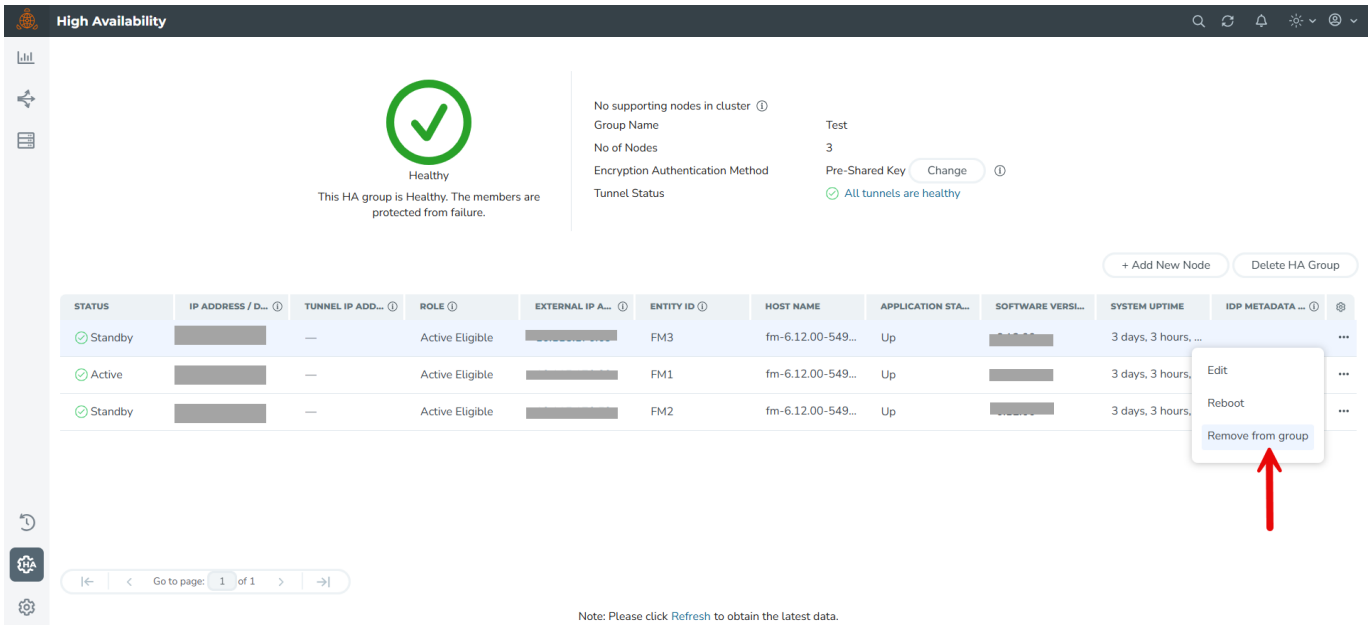


Figure 1 *Remove Standby GigaVUE-FM Instance*

3. Select the **Remove from group** option and confirm your chnages. The selected standby GigaVUE-FM instance is removed from the GigaVUE-FM HA group.

> **NOTE:** The status of the GigaVUE-FM HA group changes from **Healthy** to **At Risk**. You will not be allowed to remove the other standby GigaVUE-FM instance after the HA status changes to **At Risk**. To remove the standby node, if there is any network latency in GigaVUE-FM and the node is not removed correctly, use the command ***fmcs remove force*** in the GigaVUE-FM CLI of the standby node.

Disassemble GigaVUE-FM High Availability Group

To completely disassemble the GigaVUE-FM HA group:

1. Go to High Availability.

   NOTE: You cannot remove an active GigaVUE-FM instance or disassemble the GigaVUE-FM HA group by logging in from a standby GigaVUE-FM instance.

2. Click the **Delete HA group** option on the High Availability page and confirm your changes. The GigaVUE-FM HA group will be disassembled and each of the GigaVUE-FM instances become standalone GigaVUE-FM instances.

NOTE: Executing the above steps disassembles the GigaVUE-FM HA group completely. The database of the individual GigaVUE-FM HA group members (active, standby, and supporting instances) will be erased and reinitiated with the default database. If you had performed orchestrated configuration flows (such as the Flexible Inline Arrangement or Intent Based Orchestration) you must manually remove and recreate these if they do not backup the GigaVUE-FM database before choosing Delete HA Group.

If you cannot access the active GigaVUE-FM instance's GUI, use the following CLI command in all the GigaVUE-FM instances to disassemble the HA group:
/opt/fmcs/bin/fmcs leave force
Before disassembling the instances, take a backup of the configuration. After the GigaVUE-FM instances are disassembled from the HA group, the configurations present in the instances will be completely removed.

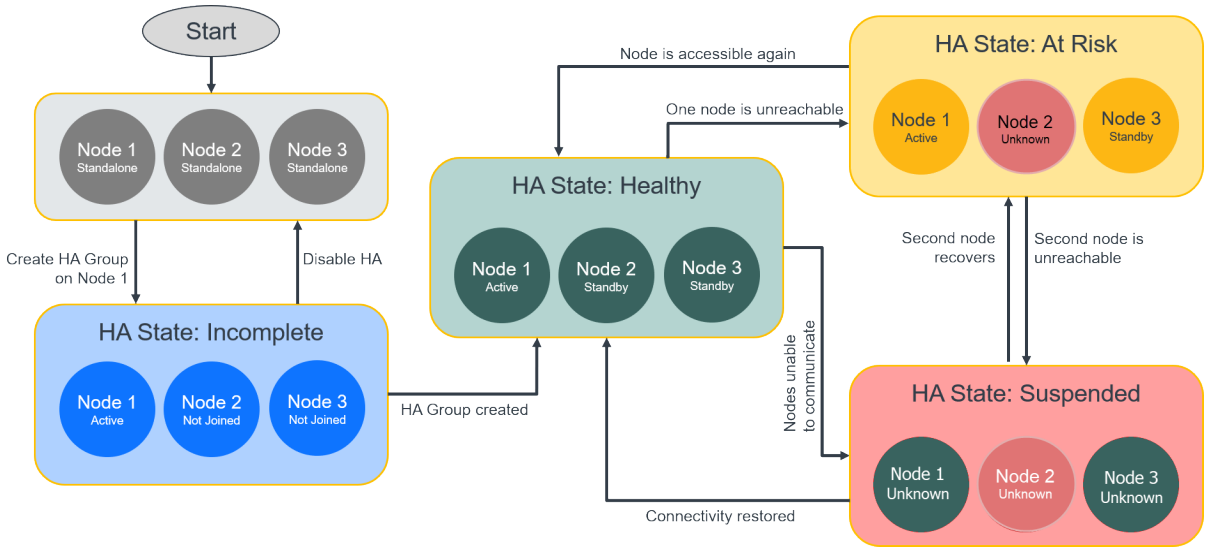
GigaVUE-FM High Availability States

The GigaVUE-FM HA state depends on the status of the three GigaVUE-FM instances. The following table lists the various states of the GigaVUE-FM HA group. You can view the HA group state from **Administration** > **High Availability** in the GigaVUE-FM GUI.

Table 3: High Availability States

State	Number of GigaVUE-FM Instances	Description
Healthy	Three GigaVUE-FM instances are up and running	One GigaVUE-FM instance is in active state. Other two instances are in standby state.
At Risk	Two GigaVUE-FM instances are up and running	One GigaVUE-FM instance is in active state. Another GigaVUE-FM instance is in standby state. The third GigaVUE-FM instance has either not joined the HA group or has left the HA group.

State	Number of GigaVUE-FM Instances	Description
		NOTE: You must recover the standby GigaVUE-FM instance with in 3 days (72 hours). Failure to do so will cause the instance to move out of the High Availability group.
Incomplete	One GigaVUE-FM instance is up and running	Only one GigaVUE-FM instance is in active state. The other two GigaVUE-FM instances have either not joined the HA group or have left the HA group.
Standalone	One GigaVUE-FM instance is up and running	HA is not configured on the GigaVUE-FM instance.
Suspended	Two or more GigaVUE-FM instances are up and running	HA is configured, but an active GigaVUE-FM instance is yet to be elected. **NOTE:** The GigaVUE-FM high availability group can move to a **Suspended** state from the **At Risk** state when the HA group has only one active-eligible and reachable GigaVUE-FM instance. Events will not be captured for the status of the GigaVUE-FM instance that went down (which causes the HA group to move into a suspended state) as there is no active/leader instance in the High Availability group.



In case of FMHA going to suspended mode from At-Risk mode, the reachability status of node which went down (due to which HA went into suspended mode) won't be audited as writes are not accepted if there is no active/leader instance in the DB cluster

Figure 2 *High Availability States*

Fail over Mechanism

The active GigaVUE-FM instance in the high availability group may fail at times resulting in one of the standby instances to take over and become the active instance. This process is called failover.

The following table provides the reasons for failover:

Reason for Failover	Description
Reloading the active GigaVUE-FM instance	An active GigaVUE-FM instance is reloaded (using the Reboot option) to bring back the HA group to healthy state again.
Planned downtime of the active GigaVUE-FM instance	An active GigaVUE-FM instance is brought down due to various reasons, for example to upgrade to a newer software version.
Monitoring session deployment during HA leader switchover	The new leader automatically redeploys Monitoring Sessions that failed during the switchover.
Node registration during HA leader switchover	Registration requests may temporarily fail or be delayed. Fabric nodes automatically retry registration. The new leader's IP address is configured as the RMQ notification target on all fabric nodes.
Certificate handling or fabric deployment/upgrade during HA leader switchover	The newly elected leader resumes certificate handling and continues any in-progress fabric deployment or upgrade from the last known state. No manual intervention is required.

GigaVUE-FM High Availability Scenarios

The High Availability page displays the current state of the GigaVUE-FM HA group. When a failover occurs, the HA group state changes in the GUI.

The following table lists the GUI changes for the various scenarios:

Scenario	Changes in GUI
What happens to the High Availability page immediately after a failover?	The High Availability page may not update immediately or may not show all the GigaVUE-FM instances.

Scenario	Changes in GUI
	NOTE: Refresh the page after a minute to view the new active GigaVUE-FM instance. However, the page will get updated automatically after 5 minutes.
What happens to an active GigaVUE-FM instance when it fails (either by itself or if failover is triggered manually)?	• One of the standby GigaVUE-FM instances changes to the active state. The GigaVUE-FM instance that was initially in the active state changes to the standby state. It takes a few seconds for this transition. • The GigaVUE-FM GUI of the new active instance will have all the menus and dashboards.
What happens to the GigaVUE-FM instances that were previously in standby state?	• One of the standby GigaVUE-FM instances changes to the active state • The other standby GigaVUE-FM instance remains in the standby state.
What happens to the embedded devices when a new Active instance takes over?	There are no changes to the devices except that they are being managed by the new active GigaVUE-FM instance.
How do you trigger a failover?	Click on the 'Reboot' option on the current active GigaVUE-FM instance to trigger a failover.

Troubleshoot GigaVUE-FM High Availability Issues

Use the following table to troubleshoot issues that you might encounter while working with the HA feature.

Problem	Solution
Unable to add a license to GigaVUE-FM HA group after a failover **Reason:** Using the MAC Address in the **About** page to generate the license	Always use the **Challenge MAC Address** in the **Licenses** page of the active GigaVUE-FM instance to generate licenses. Add the licenses to the HA group.
Unable to join the GigaVUE-FM HA group after changing the password	Always logout of GigaVUE-FM after changing the password and login again with the new password before joining the HA group.

Problem	Solution
Reason: Not logging out of GigaVUE-FM after changing the password and before joining the HA group	

(missing or bad snippet)(missing or bad snippet)

Analytics for Virtual Resources

Analytics in GigaVUE-FM is a standalone service that provides data visualization capabilities. Using Analytics[1] , you can create visual elements such as charts that are embedded as visualizations. The visualizations are grouped together in dashboards. You can also create search objects using Analytics. Dashboards, Visualizations and Search Objects are called Analytics objects. For details, refer to the Analytics section in *GigaVUE Fabric Management Guide*.

Rules and Notes:

- You cannot edit or delete these default dashboards. However, you can clone the dashboards and visualizations.

  For details, refer to the Clone Dashboard section in GigaVUE-FM Installation and Upgrade Guide

- Use the Time Filter option to select the required time interval for which you need to view the visualization.

Virtual Inventory Statistics and Cloud Applications Dashboard

Analytics dashboards allow users to monitor the physical and virtual environment and detect anomalous behavior and plan accordingly. For details on dashboard and visualization about the Discover page and Reports page. refer to the Analytics section.

To access the dashboards,

1. Go to -> **Analytics -> Dashboards.**
2. Select the required dashboard to view the visualizations.

The following table lists the various virtual dashboards:

[1]Analytics uses the OpenSearch front-end application to visualize and analyze the data in the OpenSearch database of GigaVUE-FM.

Dashboard	Displays	*Visualizations*	Displays
Inventory Status (Virtual)	Statistical details of the virtual inventory based on the platform and the health status. You can view the following metric details at the top of the dashboard: • Number of Monitoring Sessions • Number of V Series Nodes • Number of Connections • Number of GCB Nodes You can filter the visualizations based on the following control filters: • Platform • Health Status	*V Series Node Status by Platform*	Number of healthy and unhealthy GigaVUE V Series Nodes for each of the supported cloud platforms.
		Monitoring Session Status by Platform	Number of healthy and unhealthy monitoring sessions for each of the supported cloud platforms
		Connection Status by Platform	Number of healthy and unhealthy connections for each of the supported cloud platforms
		GCB Node Status by Platform	Number of healthy and unhealthy GCB nodes for each of the supported cloud platforms
V Series Node Statistics	Displays the Statistics of the V Series node such as the CPU usage, trend of the receiving and transmitting packets of the V Series node. You can filter the visualizations based on the following control filters: • Platform • Connection • V Series Node	*V Series Node Maximum CPU Usage Trend*	Line chart that displays maximum CPU usage trend of the GigaVUE V Series Node in 5 minutes interval, for the past one hour. **NOTE:** The maximum CPU Usage trend refers to the CPU usage for service cores only. Small form factor V Series nodes do not have service cores, therefore the CPU usage is reported as 0.
		V Series Node with Most CPU Usage For Past 5 minutes	Line chart that displays Maximum CPU usage of the GigaVUE V Series Node for the past 5 minutes. **NOTE:** You cannot use the time based filter options to filter and visualize the data.
		V Series Node Rx	Receiving trend of the

Dashboard	Displays	*Visualizations*	Displays
		Trend	GigaVUE V Series Node in 5 minutes interval, for the past one hour.
		V Series Network Interfaces with Most Rx for Past 5 mins	Total packets received by each of the GigaVUE V Series Node network interface for the past 5 minutes. **NOTE:** You cannot use the time based filter options to filter and visualize the data.
		V Series Node Tunnel Rx Packets/Errors	Displays the reception of packet at the Tunnel RX. This is the input to GigaVUE V Series Node, Grouping by tunnel identifier comprising {monDomain, conn, GigaVUE V Series Node, tunnelName}, before aggregation.
		V Series Node Tunnel Tx Packets/Errors	TX is for output tunnels from GigaVUE V Series Node. GigaVUE V Series Node Tunnel Tx Packets/Errors
Dedup	Displays visualizations related to Dedup application. You can filter the visualizations based on the following control filters: • Platform • Connection • V Series Node	*Dedup Packets Detected/Dedup Packets Overload*	Statistics of the total de-duplicated packets received (ipV4Dup, ipV6Dup and nonIPDup) against the de-duplication application overload.
		Dedup Packets Detected/Dedup Packets Overload Percentage	Percentage of the de-duplicated packets received against the de-duplication application overload.
		Total Traffic In/Out Dedup	Total incoming traffic against total outgoing traffic
Tunnel (Virtual)	Displays visualizations related to the tunneled traffic in both bytes as well as	*Tunnel Bytes*	Displays received tunnel traffic vs transmitted

Dashboard	Displays	*Visualizations*	Displays
	the number of packets. You can select the following control filters, based on which the visualizations will get updated: • **Monitoring session**: Select the required monitoring session. The cloud platform, monitoring domain and connection within the monitoring domain that the V Series node uses are shown in square brackets, comma-separated, after the name, to distinguish the whole path to it. • **V Series node**: Management IP of the V Series node. Choose the required V Series node from the drop-down. • **Tunnel:** Select any of the tunnels shown in the Tunnel drop-down. The direction for each tunnel is shown with the prefix in or out. The following statistics are displayed for the tunnel: • Received Bytes • Transmitted Bytes • Received Packets • Transmitted Packets • Received Errored Packets • Received Dropped Packets • Transmitted Errored Packets • Transmitted Dropped Packets		tunnel traffic, in bytes. • For input tunnel, transmitted traffic is displayed as zero. • For output tunnel, received traffic is displayed as zero.
		Tunnel Packets	Displays packet-level statistics for input and output tunnels that are part of a monitoring session.
App (Virtual)	Displays Byte and packet level statistics for the applications for the chosen monitoring session on the selected V Series node. You can select the following control filters, based on which the visualizations will get updated: • **Monitoring session** • **V Series node** • **Application**: Select the required application. By default, the visualizations displayed includes all the applications. By default, the following statistics are displayed:	*App Bytes*	Displays received traffic vs transmitted traffic, in Bytes.

Dashboard	Displays	*Visualizations*	Displays
	• Received Bytes • Transmitted Bytes • Received Packets • Transmitted Packets • Errored Packets • Dropped Packets		
		App Packets	Displays received traffic vs transmitted traffic, as the number of packets.
End Point (Virtual)	Displays Byte and packet level statistics for the un-tunneled traffic deployed on the V Series nodes. The following statistics that are shown for Endpoint (Virtual): • Received Bytes • Transmitted Bytes • Received Packets • Transmitted Packets • Received Errored Packets • Received Dropped Packets • Transmitted Errored Packets • Transmitted Dropped Packets The endpoint drop-down shows *<V Series Node Management IP address : Network Interface>* for each endpoint. You can select the following control filters that help to update the visualizations: • **Monitoring session** • **V Series node** • **Endpoint:** Management IP of the V Series node followed by the Network Interface (NIC)	*Endpoint Bytes*	Displays received traffic vs transmitted traffic, in Bytes.
		Endpoint Packets	Displays received traffic vs transmitted traffic, as the number of packets.

NOTE: The Tunnel (Virtual), App (Virtual) and Endpoint (Virtual) dashboards do not show data from the previous releases if the *Monitoring Session [Platform : Domain : Connection]* dashboard filter is applied. This filter relies on the new attributes in the OpenSearch database available only from software version 5.14.00 and beyond.

Analytics for Inline V Series Solution (AWS)

Analytics dashboards allow users to monitor the physical and virtual environment and detect anomalous behavior and plan accordingly.

Analytics support is available for the following cloud platforms:

- AWS
- Azure

To access the dashboards:

1. From the left navigation pane, go to -> **Analytics -> Dashboards.**
2. Navigate to **System Dashboards ->Inline**.
3. From the **Load Balancer** drop-down list, select the Gateway load Balancer configured in AWS.
4. From the **Monitoring Session** drop-down list, select the Monitoring Session in which Inline V Series solution is configured.
5. From the **Node Name** drop-down list, select the GigaVUE V Series Node.

The following tables lists the various visualizations for Inline V Series solution:

Table 4: Overall 5G Apps Dashboard

Dashboard	Description	Visualizations	Details
Inline Source (Packets)	Displays the overall visualization details of Inline V Series Solution	**LoadBalancer to Inline Source Average Packets**	Displays the Inline traffic received from the Load balancer to the Inline V Series Node interface in packets.
		Inline Source to Load Balancer Average Packets	Displays the Inline traffic sent back from the Inline V Series Node interface to the Load balancer in packets.
		LoadBalancer to Inline Source App Average Packets	Displays the Inline traffic received from the Inline V Series Node interface to the IVTAP application in packets.
		Inline Source to LoadBalancer App Average Packets	Displays the Inline traffic sent back from the IVTAP application to the Inline V Series Node interface in packets.
		Average IVTAP App Total Packets Drop	Displays the IVTAP application total packet drops while processing the Inline traffic received from Inline V Series Node interface.
		Average Inline Source IVTAP Errors	Displays the IVTAP application errors while processing the Inline traffic received from Inline V Series Node interface
		Average Out-of-band Ingress Tunnel rx	Displays the Out-of-Band traffic (Mirrored traffic) received from

Dashboard	Description	Visualizations	Details
		Packets	Inline V Series Node interface.
		Average Tool Tunnel tx Packets	Displays the bytes transmitted to the tool from GigaVUE V Series Node of the last tier.
		Average Out-of-band Ingress Tunnel Packets Drop	Displays the Out-of-Band traffic packet drops while receiving traffic (Mirrored traffic) from Inline V Series Node interface.
		Average Out-of-band Ingress Tunnel Errors	Displays the Out-of-Band errors while receiving traffic (Mirrored traffic) from Inline V Series Node interface.
Inline Source (Bytes)	Displays the overall visualization details of Inline V Series Solution	**Load Balancer to Inline Source Average Bytes**	Displays the Inline traffic received from the Load balancer to the Inline V Series Node interface in bytes.
		Inline Source to Load Balancer Average Bytes	Displays the Inline traffic sent back from the Inline V Series Node interface to the Load balancer in bytes.
		LoadBalancer to Inline Source App Average Bytes	Displays the Inline traffic received from the Inline V Series Node interface to the IVTAP application in bytes.
		Inline Source to LoadBalancer App Average Bytes	Displays the Inline traffic sent back from the IVTAP application to the Inline V Series Node interface in bytes.
		Average Out-of-band Ingress Tunnel rx Bytes	Displays the Out-of-Band traffic (Mirrored traffic) received from Inline V Series Node interface in bytes.
		Average Tool Tunnel tx Bytes	Displays the bytes transmitted to the tool from GigaVUE V Series Node of the last tier in bytes.
Heart Beat Analytics		**Average LoadBalancer To Inline Source Heart Beat Packets**	Displays the Health Check request packets (Heart beat packets) received by Inline V Series Node from Load balancer
		Average Inline Source To LoadBalancer Heart Beat Packets	Displays the Health Check response packets (Heart beat packets) sent by Inline V Series Node to Load balancer.

Debuggability and Troubleshooting

Use the following information to help diagnose and resolve GigaVUE V Series Nodes issues.

Sysdumps

A sysdump is a log and system data package generated when a GigaVUE V Series Node experiences a crash (such as kernel, application, or hardware failure). These files are essential for debugging.

You cannot download sysdump files if the associated fabric component is deleted or unreachable.

Sysdumps—Rules and Notes

Consider the following points before you generate sysdumps:

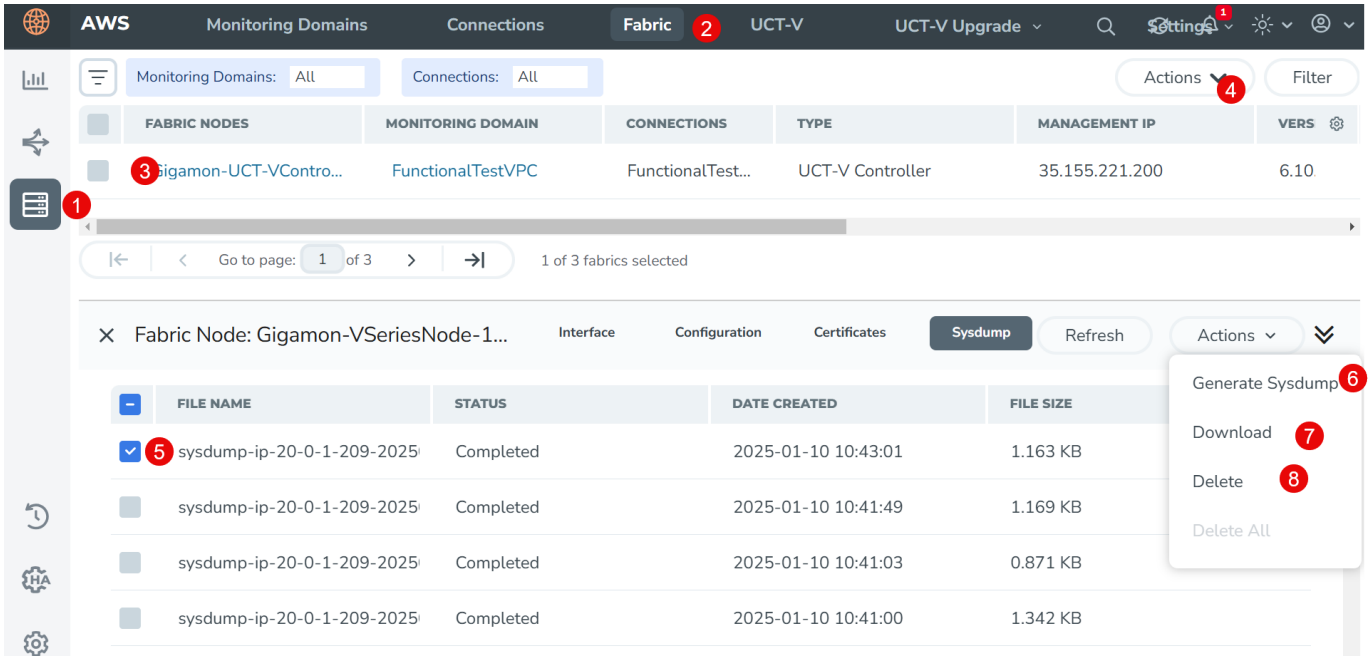
- You can generate only one sysdump file at a time for a GigaVUE V Series Node.
- You cannot generate a sysdump file when generation of another sysdump file is in progress.
- The limit of sysdump files available per GigaVUE V Series Node is six. When you generate a seventh sysdump file, the file overwrites the first sysdump file.
- You can download only one sysdump file per GigaVUE V Series Node at a time.
- You can delete sysdump files in bulk for a GigaVUE V Series Node.
- To ensure efficient usage, the system limits the number of simultaneous sysdump generation requests to 10 GigaVUE V Series Nodes.
- GigaVUE V Series Node sysdumps are not stored in Fabric Manager but generated and stored on the GigaVUE V Series Node itself.

Generate a Sysdump File

To generate a sysdumps file:

1. Perform one of the following:
   - Go to **Inventory > VIRTUAL > AWS > Fabric.**
   - Go to **Inventory > VIRTUAL > Azure > Fabric.**
   - Go to **Inventory > VIRTUAL > OpenStack > Fabric.**

   The **Fabric** page appears.
2. Select the required node, and use one of the following options to generate a sysdump file:
   - Select **Actions > Generate Sysdump**.
   - In the lower pane, go to **Sysdump**, and select **Actions > Generate Sysdump**.
3. View the latest status, click **Refresh**.



Other Actions

- To download a sysdump file, select the file in the lower pane, and then click **Actions > Download**.
- To delete a sysdump file,
    1. Select the file in the lower pane.
    2. Select the desired sysdump file.
    3. Select **Actions > Delete**.
- To bulk delete, select all the sysdump files, and then select **Actions > Delete All.**

FAQs - Secure Communication between GigaVUE Fabric Components (AWS)

This section addresses frequently asked questions about Secure Communication between GigaVUE Fabric Components and GigaVUE-FM. Refer to Secure Communication between GigaVUE Fabric Components section for more details.

1. **Is there a change in the upgrade process for GigaVUE-FM and GigaVUE V Series Node?**

   No. The upgrade process remains unchanged across all supported upgrade paths. You can upgrade your nodes without any additional steps. The upgrade results in the automatic deployment of the appropriate certificates based on the node versions

GigaVUE-FM	GigaVUE V Series Nodes	Custom Certificates Selected (Y/N)	Actual Node Certificate
6.10	6.10	Y	GigaVUE-FM PKI Signed Certificate
6.10	6.9 or earlier	Y	Custom Certificate
6.10	6.9 or earlier	N	Self-Signed Certificate

2. **What is the new authentication type used between GigaVUE-FM and the GigaVUE Fabric Components? Is backward compatibility supported?**

   Backward compatibility is supported, ensuring that fabric components running on version 6.9 or earlier remain compatible with GigaVUE-FM 6.10. The following authentication types are supported across different versions:

GigaVUE-FM	GigaVUE Fabric Components	Authentication
6.10	6.10	Tokens + mTLS Authentication (Secure Communication)
6.10	6.9 or earlier	User Name and Password

3. **What are the new ports that must be added to the security groups?**

   The following table lists the port numbers that must be opened for the respective fabric components:

Component	Port
GigaVUE-FM	9600
GigaVUE V Series Node	80, 8892
GigaVUE V Series Proxy	8300, 80, 8892
UCT-V Controller	8300, 80
UCT-V	8301, 8892, 9902 For more details, refer to Prerequisites for AWS.

4. **Is the registration process different for deploying the fabric components using Third-Party Orchestration?**

   Yes. Beginning with version 6.10, you must use tokens in the gigamon-cloud.conf file instead of the username and password. To generate the token in GigaVUE-FM, go to **Settings > Authentication > User Management > Token**. For more details, refer to Configure Tokens.

   Example Registration Data for UCT-V:

   ```
   #cloud-config
    write_files:
    - path: /etc/gigamon-cloud.conf
      owner: root:root
      permissions: '0644'
      content: |
        Registration:
           groupName: <Monitoring Domain Name>
           subGroupName: <Connection Name>
           token: <Token>
           remoteIP: <IP address of the UCT-V Controller 1, <IP address of the UCT-V Controller
   2>
           sourceIP: <IP address of UCT-V> (Optional Field)
   ```

5. **Are there any changes to the UCT-V manual installation and upgrade process?**

   Starting from version 6.10, you must add tokens during manual installation and upgrades.

   - Create a configuration file named gigamon-cloud.conf with the token and place it in the /tmp directory during UCT-V installation
   - After installing UCT-V, you can add the configuration file in the /etc directory.

   Important! Without this token, UCT-V cannot register with GigaVUE-FM.

6. **Can I use my PKI infrastructure to issue certificates for the Fabric Components?**

   Direct integration of your PKI with GigaVUE-FM is not supported. However, you can provide your Intermediate Certificate Authority (CA) to sign the node certificate.

7. **What happens to the existing custom certificates introduced in the 6.3 release?**

   The custom certificate feature is not supported for the fabric components with version 6.10 or higher, even if a custom certificate is selected in the Monitoring Domain. However, this feature remains available for older versions.

   - When upgrading from version 6.9 or earlier with custom certificates upgrades to version 6.10, the system automatically generates and deploys certificates signed by GigaVUE-FM.
   - If deploying version 6.9 or earlier components from a 6.10 GigaVUE-FM, custom certificates are still applied.

8. **How to issue certificates after upgrading the fabric components to 6.10?**

   When the upgrade process begins, GigaVUE-FM transmits the certificate specifications to the new fabric components using the launch script. The fabric components utilize these specifications to generate their own certificates.

9. **Is secure communication supported in FMHA deployment?**

   Yes, it is supported. However, you must follow a few manual steps before upgrading the fabric components to 6.10. For details, refer to Configure Secure Communication between Fabric Components in FMHA.

   NOTE: This step is essential if you are using cloud deployments in FMHA mode and would like to deploy or upgrade the fabric components to version 6.10 or later.