



# GigaVUE V Series Quick Start Guide

**GigaVUE Cloud Suite**

Product Version: 6.7

Document Version: 1.1

Last Updated: Friday, October 11, 2024

(See Change Notes for document updates.)

**Copyright 2024 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](http://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
6.7.00	1.1	10/11/2024	This update includes bug fixes and minor cosmetic changes for improved usability and document consistency.
6.7.00	1.0	06/05/2024	The original release of this document with 6.7.00 GA.

# Contents

<b>GigaVUE V Series Quick Start Guide</b> .....	<b>1</b>
Change Notes .....	3
Contents .....	4
<b>GigaVUE V Series Quick Start Guide</b> .....	<b>6</b>
What is a GigaVUE V Series Node? .....	6
<b>Volume-Based Licensing</b> .....	<b>7</b>
Base Bundles .....	8
Bundle Replacement Policy .....	8
Add-on Packages .....	8
How GigaVUE-FM Tracks Volume-Based License Usage .....	9
<b>Manage Volume-based Licenses</b> .....	<b>10</b>
Activate Volume-based Licenses .....	11
Default Trial Licenses .....	12
Delete Default Trial Licenses .....	13
<b>GigaVUE Cloud Suite for AWS</b> .....	<b>13</b>
Recommended Instance Types for AWS .....	14
Network Firewall Requirements for AWS .....	14
<b>GigaVUE Cloud Suite for Azure</b> .....	<b>20</b>
Recommended Instance Type .....	20
Network Firewall Requirements for Azure .....	20
<b>GigaVUE Cloud Suite for OpenStack</b> .....	<b>26</b>
Minimum Compute Requirements for OpenStack .....	26
Recommended Instance Type for OpenStack .....	27
Network Firewall Requirements for OpenStack .....	28
Network Requirements .....	29
<b>GigaVUE Cloud Suite for Nutanix</b> .....	<b>30</b>
Minimum Compute Requirements for Nutanix .....	30
Network Firewall Requirements for Nutanix .....	31
<b>GigaVUE Cloud Suite for VMware</b> .....	<b>32</b>
<b>Prerequisites for Integrating GigaVUE V Series Nodes with vCenter</b> .....	<b>32</b>
Network Firewall Requirements for ESXi .....	33
Recommended Instance Types for ESXi .....	34

Required VMware Virtual Center Privileges .....	35
<b>Prerequisites for Integrating GigaVUE V Series Nodes with NSX-T .....</b>	<b>36</b>
Network Firewall Requirements for NSX-T .....	36
Recommended Instance Types for NSX-T .....	38
Required VMware Virtual Center Privileges .....	38
<b>GigaVUE-FM Version Compatibility Matrix .....</b>	<b>39</b>
Version Compatibility for GigaVUE V Series Node Configuration .....	39
<b>Supported GigaSMART Operations .....</b>	<b>44</b>
<b>Troubleshooting .....</b>	<b>47</b>
<b>GigaVUE V Series Logs and Commands .....</b>	<b>50</b>
CLI Commands .....	50
Logs .....	50
<b>Additional Sources of Information .....</b>	<b>51</b>
<b>Documentation .....</b>	<b>51</b>
How to Download Software and Release Notes from My Gigamon .....	54
<b>Documentation Feedback .....</b>	<b>54</b>
<b>Contact Technical Support .....</b>	<b>55</b>
<b>Contact Sales .....</b>	<b>56</b>
<b>Premium Support .....</b>	<b>56</b>
<b>The VÜE Community .....</b>	<b>56</b>
<b>Glossary .....</b>	<b>57</b>

# GigaVUE V Series Quick Start Guide

GigaVUE Cloud Suite are cloud-native solutions that acquire, optimize and distribute selected traffic to security and monitoring tools. The suites enable enterprises to extend their security posture to both public and private cloud and also accelerate the time to detect threats to applications while taking advantage of a reliable, scalable and available cloud environment.

This solution includes three main components:

**GigaVUE V Series Node:** Processes network traffic and allows administrators to provide additional functionality including forwarding, de-duplication, Application Intelligence, Application Metadata Intelligence, Application Filtering Intelligence, and NetFlow generation.

**UCT-Vs:** Acquires traffic from the host on which it is deployed and transfers it to the GigaVUE V Series Node.

**GigaVUE-FM:** A web-based fabric management interface that provides a single pane of glass visibility and management of both the physical and virtual traffic that forms the GigaVUE Cloud for Azure. GigaVUE-FM manages the configuration of the rest of the components in your cloud platform.

## What is a GigaVUE V Series Node?

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

### GigaVUE V Series Node:

- Platform support - AWS, Azure, VMware (ESXi and NSX-T), OpenStack, Nutanix
- GigaSMART support—De-duplication, NetFlow, AMI, AFI, Slicing, Masking, AMX, Header Stripping, SSL Decrypt, Load balancing, 5G-SBI, GENEVE Decapsulation, PCAPng. Refer to [Supported V Series Applications](#) for more detailed information on the applications supported in the respective platforms.

- Licensing—Licensed according to traffic volume. With Volume Based Licensing, the customer can choose any supported platform, or combination of platforms.

Cloud Platform	Guides
<b>Public Cloud</b>	
AWS	GigaVUE Cloud Suite for AWS Guide
Azure	GigaVUE Cloud Suite Deployment Guide - Azure
<b>Private Cloud</b>	
OpenStack	GigaVUE Cloud Suite for OpenStack Guide
VMware	GigaVUE Cloud Suite Deployment Guide - VMware
Nutanix	GigaVUE Cloud Suite Deployment Guide - Nutanix
<b>Other Platforms</b>	
Third Party Orchestration	GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration

Topics:

- [Volume-Based Licensing](#)
- [GigaVUE Cloud Suite for VMware](#)
- [GigaVUE Cloud Suite for OpenStack](#)
- [GigaVUE Cloud Suite for Azure](#)
- [GigaVUE Cloud Suite for AWS](#)
- [GigaVUE-FM Version Compatibility Matrix](#)
- [Supported GigaSMART Operations](#)
- [Troubleshooting](#)
- [GigaVUE V Series Logs and Commands](#)

## Volume-Based Licensing

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 provide information on the actual data volume that flows through the V Series Nodes. All licensed applications, when running on the node, generate usage statistics.

Licensing for GigaVUE Cloud Suite is volume-based. In the Volume-Based Licensing (VBL) scheme, a license entitles specific applications on your V Series Nodes to use a specified amount of total data volume over the term of the license. The distribution of the license to individual nodes becomes irrelevant for GigaVUE-FM accounting purpose. GigaVUE-FM tracks the total amount of data processed by the various licensed applications and provides visibility on the actual amount of data, each licensed application is using on each node, and tracks the overuse, if any.

Volume-based licenses are available as monthly subscription licenses with a service period of one month. Service period is the period of time for which the total usage or overage is tracked. There is a grace period for each license that is encoded in the license file. The license effectively provides data allowance for this additional time after the official end time of the license.

For purchasing licenses with the Volume-Based License (VBL) option, contact our Sales. Refer to [Contact Sales](#).

## Base Bundles

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

- CoreVUE
- NetVUE
- SecureVUEPlus

The bundles are available as SKUs<sup>1</sup>. The number in the SKU indicates the total volume allowance of the SKU for that base bundle. For example, VBL-250T-BN-CORE has a daily volume allowance of 250 terabytes for CoreVUE bundle.

## Bundle Replacement Policy

Refer to the following notes:

- You can always upgrade to a higher bundle but you cannot move to a lower version.
- You cannot have two different base bundles at the same time however, you can have multiple base bundles of the same type.
- Once upgraded to a higher bundle, the existing lower bundles will be automatically deactivated.

## Add-on Packages

GigaVUE-FM allows you to add additional packages called 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.

### Rules for add-on packages:

---

<sup>1</sup>Stock Keeping Unit. Refer to the [What is a License SKU?](#) section in the FAQs for Licenses chapter.



- Add-on packages can only be added when there is an active base bundle available in GigaVUE-FM.
- The base bundle limits the total volume usage of the add-on package.
- If your add-on package has volume allowance less than the base bundle, then your add-on package can only handle volume allocated for add-on package.
- When the life term of an add-on package extends beyond the base bundle, then when the base bundle expires, the volume allowance of the add-on package will be reduced to zero until a new base bundle is added.

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

GigaVUE Data Sheets
<a href="#">GigaVUE Cloud Suite for VMware Data Sheet</a>
<a href="#">GigaVUE Cloud Suite for AWS Data Sheet</a>
<a href="#">GigaVUE Cloud Suite for Azure Data Sheet</a>
<a href="#">GigaVUE Cloud Suite for OpenStack</a>
<a href="#">GigaVUE Cloud Suite for Nutanix</a>
<a href="#">GigaVUE Cloud Suite for Kubernetes</a>

## How GigaVUE-FM Tracks Volume-Based License Usage

GigaVUE-FM tracks the license usage for each V Series node as follows:

- When you create and deploy a monitoring session, GigaVUE-FM allows you to use only those applications that are licensed at that point (applicable only for ACTIVE licenses, licenses in grace period are not included).
- When a license goes into grace period, you will be notified with an audit log.
- When a license expires (and has not been renewed yet), the monitoring sessions using the corresponding license will not be undeployed.


For releases prior to 6.4:

- The monitoring sessions using the corresponding license will be undeployed (but not deleted from the database).
- When a license is later renewed or newly imported, any undeployed monitoring sessions are redeployed.

**NOTE:** When the license expires, GigaVUE-FM displays a notification on the screen.

# Manage Volume-based Licenses

To manage active Volume-based License:

1. On the left navigation pane, click .
2. Go to **System > Licenses**. From the top navigation bar, select the **VBL Active** from the **FM/Cloud** drop-down.

This page lists the following information about the active Volume-based Licenses:

Field	Description
SKUs	Unique identifier associated with the license
Bundles	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

**NOTE:** The License Type and Activation ID are displayed by default in the VBL Active page. To display the Entitlement ID field, click on the column setting configuration option to enable the Entitlement ID field.

The expired licenses are displayed in the **VBL Inactive** page, which can be found under the **FM/Cloud** drop-down in the top navigation bar. This page lists the following information about the inactive Volume-based Licenses:

Field	Description
SKUs	Unique identifier associated with the license.
Bundles	Bundle to which the license belongs to.
Ends	License end date
Grace Period	Number of days the license is in grace period
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 VBL Inactive page. To display these fields, click on the column setting configuration option and enable these fields.

Use the following buttons to manage your VBL.


Button	Description
<b>Activate Licenses</b>	Use this button to activate a Volume-based License. For more information, refer to the topic <a href="#">Activate Volume-based Licenses</a> of the GigaVUE Licensing Guide.
<b>Email Volume Usage</b>	Use this button to send the volume usage details to the email recipients.
<b>Filter</b>	Use this button to narrow down the list of active Volume-based Licenses that are displayed on the VBL active page.
<b>Export</b>	Use this button to export the details in the VBL active page to a CSV or XLSX file.
<b>Deactivate</b>	Use this button to deactivate the licenses. You can only deactivate licenses that are in grace period or that have expired.

For more detailed information on dashboards and reports 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 Licensed 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

## Activate Volume-based Licenses

To activate Volume-based licenses:

1. On the left navigation pane, click .
2. Go to **System > Licenses**. From the top navigation bar, select the **VBL Active** from the **FM/Cloud** drop-down.

3. Click **Activate Licenses**. The **Activate License** page appears. Perform the following steps:
  - a. Download the fabric inventory file that contains information about GigaVUE-FM. Click **Next**. Refer to the [What is a Fabric Inventory File?](#) section for more details.
  - b. Navigate to the Licensing Portal. Upload the Fabric Inventory file in the portal. Once the fabric inventory file is uploaded, select the required license and click **Activate**. A license key is provided. Record the license key or keys.
  - c. Return to GigaVUE-FM and add the additional licenses.

## Default Trial Licenses

After you install GigaVUE-FM, a default free 1TB of CoreVUE trial volume-based license (VBL) is provided one-time for 30 days (from the date of installation).

SKU	Feature	Type	Description	Start Date	End Date	Activation ID	Seats / Volume	Status
VBL-1T-BN-CORE-TRIAL	erspan	Trial	1T-AdvancedTu...	May 13, 2021	Jun 12, 2021	4e8cb5a4-7eb4...	1024 GB daily	Expired
VBL-1T-BN-CORE-TRIAL	geneve.slicing.m...	Trial	1T-BaseApps	May 13, 2021	Jun 12, 2021	4e8cb5a4-7eb4...	1024 GB daily	Expired
VBL-1T-BN-CORE-TRIAL	header-stripping...	Trial	1T-HeaderStripp...	May 13, 2021	Jun 12, 2021	4e8cb5a4-7eb4...	1024 GB daily	Expired
SMT-HC0-GEN1-DD1-SW-TM	dedup	Internal	HC2-GEN1-Ded...	May 14, 2021	May 14, 2022	a5d70642-95eb...	5 of 8 available	Grace Period
SMT-HC0-GEN1-APF-SW-TM	apf	Internal	HC2-GEN1-APF...	May 21, 2021	Never	ce782018-1b0f...	6 of 8 available	Active
SMT-HC0-GEN1-ASF-SW-TM	asf	Internal	HC2-GEN1-ASF...	May 21, 2021	Never	24618ae4-ddb6...	1 of 2 available	Active
SMT-HC0-GEN1-HS1-SW-TM	header-stripping...	Internal	HC2-GEN1-HS1...	May 21, 2021	Never	8d035388-013...	7 of 8 available	Active
SMT-HC0-GEN1-NF1-SW-TM	netflow	Internal	HC2-GEN1-Net...	May 21, 2021	Never	11d3f4dd-90c6...	7 of 8 available	Active
SMT-HC0-GEN1-SSL-SW-TM	ssl-decrypt	Internal	HC2-GEN1-SSL...	May 21, 2021	Never	30f7e2c0-aea5...	0 of 3 available	Active
SMT-HC3-GEN2-5GC-SW-TM	5G-Correlation n...	Commercial	HC3-GEN2-5GC...	Apr 22, 2021	Apr 22, 2022	760ceb6a-c919...	1 of 4 available	Expired
SMT-HC3-GEN2-GTPMAX-SW-TM	apfflowrule-gtp ...	Internal	HC3-GEN2-GTP...	Apr 22, 2021	Apr 22, 2022	7228d9a9-30ac...	4 of 4 available	Expired

This license includes the following applications:


- ERSPAN
- Geneve
- Slicing
- Masking
- Trailer
- Tunneling
- Load Balancing
- Enhanced Load Balancing
- Flowmap
- Header-stripping
- Add header

**NOTE:** There is no grace period for the trial license. If you do not have any other Volume-based licenses installed, then after 30 days, on expiry of the trial license, any deployed monitoring sessions will be undeployed from the existing GigaVUE V Series Nodes.

To deactivate the trial VBL refer to [Delete Default Trial Licenses](#) section for details.

## Delete Default Trial Licenses

GigaVUE-FM allows you to deactivate the default trial licenses from this page. To deactivate the license:

1. On the left navigation pane, click .
2. Go to **System > Licenses > Floating**. Click **Activated**.
3. Click **Deactivate > Default Trial VBL**.

The VBL trial licenses is deactivated and is no longer listed in the Activated page. However, you can view these deactivated licenses from the Deactivated page.

## GigaVUE Cloud Suite for AWS

GigaVUE Cloud Suite for AWS delivers a cloud-based visibility and analytics solution that eliminates network blind spots as you move workloads to the cloud, significantly reducing security and non-compliance risks and helps remediate performance issues.

GigaVUE Cloud Suite for AWS helps you obtain a unified view of all data in motion anywhere on your hybrid, single or multi-cloud network. Easily acquire data from any source, automatically optimize it and send to any destination. It closes the cloud visibility gap, giving your security and monitoring tools visibility across cloud environments, from raw packets up to the application layer and with the added context of network data.

You can deploy the GigaVUE Cloud Suite for AWS by subscribing in the marketplace or by installing the individual fabric components using the Amazon Machine Images (AMI).

This section describes the requirements and prerequisites for configuring the GigaVUE Cloud Suite for AWS. Refer to the following section for details.

- [Recommended Instance Types for AWS](#)
- [Network Firewall Requirements for AWS](#)

## Recommended Instance Types for AWS

Product	Instance Type	vCPU	RAM
GigaVUE-FM	m4.xlarge	4 vCPU	16 GB
GigaVUE V Series Node	c5n.xlarge	4 vCPU	10.5 GB
GigaVUE V Series Proxy	t2.medium	2 vCPU	4 GB
UCT-V	t2.micro	1 vCPU	1 GB
UCT-V Controller	t2.medium	2 vCPU	4 GB

**NOTE:** Additional instance types are also supported. Refer to Support, Sales, or Professional Services for deployment optimization.

GigaVUE V Series Node deployments in AWS can also be deployed in conjunction with a Network and Gateway Load Balancer.

## Network Firewall Requirements for AWS

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

**NOTE:** When using dual stack network, the below mentioned ports must be opened for both IPv4 and IPv6.

GigaVUE-FM				
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 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-C 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	5671	UCT-C 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	GigaVUE-FM 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 (default)	UCT-C Controller IP	Allows GigaVUE-FM to communicate control and management plane traffic to UCT-C Controller.
Outbound	TCP	443	Any IP Address	Allows GigaVUE-FM to reach the Public Cloud Platform APIs.
<b>UCT-V Controller</b>				

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 (This port is used for Third Party Orchestration)	TCP	8891	UCT-V or Subnet IP	Allows UCT-V Controller to receive the registration requests from UCT-V.
Inbound	TCP	22	Administrator Subnet	Allows CLI access for user-initiated management and diagnostics, specifically when using third party orchestration.
Direction	Protocol	Port	Destination CIDR	Purpose
Outbound (This port is 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	9901	UCT-V Controller IP	Allows UCT-V Controller to communicate control and management plane traffic with UCT-Vs.
Outbound	TCP	5671	GigaVUE-FM IP	Allows UCT-V Controller to send traffic health updates to GigaVUE-FM.
<b>UCT-V</b>				
Direction	Protocol	Port	Source CIDR	Purpose
Inbound	TCP	9901	UCT-V Controller IP	Allows UCT-V to receive control and management plane traffic from UCT-V Controller
Direction	Protocol	Port	Destination CIDR	Purpose
Outbound (This port is used for Third Party Orchestration)	TCP	8891	UCT-V Controller IP	Allows UCT-V to communicate with UCT-V Controller for registration and Heartbeat
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.
<b>GigaVUE V Series Node</b>				
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 (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 traffic to an external tool.
Outbound	UDP	514	Tool IP	Allows GigaVUE V Series Node to send Application Metadata Intelligence log messages to external tools.
Bidirectional (optional)	ICMP	<ul style="list-style-type: none"> <li>echo request</li> <li>echo reply</li> </ul>	Tool IP	Allows GigaVUE V Series Node to send health check tunnel destination traffic.
Outbound (This port is 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.
Outbound (This port is 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.
<b>GigaVUE V Series Proxy (optional)</b>				
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 (This port is used for	TCP	8891	GigaVUE V Series Node IP	Allows GigaVUE V Series Proxy to receive registration requests

Third Party Orchestration)				and heartbeat messages from GigaVUE V Series Node.
Inbound	TCP	22	Administrator Subnet	Allows CLI access for user-initiated management and diagnostics, specifically when using third party orchestration.
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
<b>Universal Cloud Tap - Container</b> deployed inside Kubernetes worker node				
Direction	Protocol	Port	Destination CIDR	Purpose
Outbound	TCP	42042	Any IP address	Allows UCT-C to send statistical information to UCT-C Controller.
Outbound	UDP	VXLAN (default 4789)	Any IP address	Allows UCT-C to tunnel traffic to the GigaVUE V Series Node or other destination.
<b>UCT-C Controller</b> 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.

# GigaVUE Cloud Suite for Azure

This section describes the requirements and prerequisites for configuring the . Refer to the following section for details.

- [Recommended Instance Type](#)
- [Network Firewall Requirements for Azure](#)

## Recommended Instance Type

**NOTE:** Additional instance types are also supported. Refer to Support, Sales, or Professional Services for deployment optimization.

Product	Instance Type	vCPU	RAM
GigaVUE V Series Node	Standard_D4s_v4	4 vCPU	16 GB
	Standard_D8S_V4	8 vCPU	32 GB
GigaVUE V Series Proxy	Standard_B1s	1 vCPU	1 GB
UCT-V Controller	Standard_B1s	1 vCPU	1 GB

## Network Firewall Requirements for Azure

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

**NOTE:** When using dual stack network, the below mentioned ports must be opened for both IPv4 and IPv6.

GigaVUE-FM				
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 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-C 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	5671	UCT-C 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	GigaVUE-FM 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 (default)	UCT-C Controller IP	Allows GigaVUE-FM to communicate control and management plane traffic to

				UCT-C Controller.
Outbound	TCP	443	Any IP Address	Allows GigaVUE-FM to reach the Public Cloud Platform APIs.
<b>UCT-V Controller</b>				
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 (This port is used for Third Party Orchestration)	TCP	8891	UCT-V or Subnet IP	Allows UCT-V Controller to receive the registration requests from UCT-V.
Inbound	TCP	22	Administrator Subnet	Allows CLI access for user-initiated management and diagnostics, specifically when using third party orchestration.
Direction	Protocol	Port	Destination CIDR	Purpose
Outbound (This port is 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	9901	UCT-V Controller IP	Allows UCT-V Controller to communicate control and management plane traffic with UCT-Vs.
Outbound	TCP	5671	GigaVUE-FM IP	Allows UCT-V Controller to send traffic health updates to GigaVUE-FM.
<b>UCT-V</b>				
Direction	Protocol	Port	Source CIDR	Purpose
Inbound	TCP	9901	UCT-V Controller IP	Allows UCT-V to receive control and management plane traffic from UCT-V Controller
Direction	Protocol	Port	Destination CIDR	Purpose
Outbound (This port is used for Third Party)	TCP	8891	UCT-V Controller IP	Allows UCT-V to communicate with UCT-V Controller for registration and Heartbeat

Orchestration)				
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.
<b>GigaVUE V Series Node</b>				
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 (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)	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 traffic to an external tool.
Outbound	UDP	514	Tool IP	Allows GigaVUE V Series Node to send Application Metadata Intelligence log messages to external tools.
Bidirectional (optional)	ICMP	<ul style="list-style-type: none"> <li>echo request</li> <li>echo reply</li> </ul>	Tool IP	Allows GigaVUE V Series Node to send health check tunnel destination traffic.
Outbound (This port is 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.
Outbound (This port is 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.
<b>GigaVUE V Series Proxy (optional)</b>				
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 (This port is used for Third Party Orchestration)	TCP	8891	GigaVUE V Series Node IP	Allows GigaVUE V Series Proxy to receive registration requests and heartbeat messages from GigaVUE V Series Node.
Inbound	TCP	22	Administrator Subnet	Allows CLI access for user-initiated management and diagnostics, specifically when using third party orchestration.
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
<b>Universal Cloud Tap - Container</b> deployed inside Kubernetes worker node				
Direction	Protocol	Port	Destination CIDR	Purpose
Outbound	TCP	42042	Any IP address	Allows UCT-C to send statistical information to UCT-C Controller.
Outbound	UDP	VXLAN (default 4789)	Any IP address	Allows UCT-C to tunnel traffic to the GigaVUE V Series Node or other destination.
<b>UCT-C Controller</b> 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.

# GigaVUE Cloud Suite for OpenStack

The OpenStack software is designed for multi-tenancy (multiple projects), where a common set of physical compute and network resources are used to create project domains that provide isolation and security. Characteristics of a typical OpenStack deployment include the following:

- Projects are unaware of the physical hosts on which their instances are running.
- A project can have several virtual networks and may span across multiple hosts.

In a multi-project OpenStack cloud, where project isolation is critical, the Gigamon solution extends visibility for the project's workloads without impacting others by doing the following:

- Support project-wide monitoring domains—a project may monitor any of its instances.
- Honor project isolation boundaries—no traffic leakage from one project to any other project during monitoring.
- Monitor traffic without needing cloud administration privileges. There is no requirement to create port mirror sessions and so on.
- Monitor traffic activity of one project without adversely affecting other projects.

This section describes the requirements and prerequisites for configuring the GigaVUE Cloud Suite for OpenStack. Refer to the following section for details.

- [Minimum Compute Requirements for OpenStack](#)
- [Recommended Instance Type for OpenStack](#)
- [Security Group](#)
- [Network Requirements](#)

## Minimum Compute Requirements for OpenStack

In OpenStack, flavors set the vCPU, memory, and storage requirements for an image. Gigamon recommends that you create a flavor that matches or exceeds the minimum recommended requirements listed in the following table.

Compute Instances	vCPU	Memory	Disk Space	Description
UCT-V	2 vCPU	4GB	N/A	Available as rpm or Debian package. Instances can have a single vNIC or dual vNICs configured for monitoring the traffic.
UCT-V Controller	1 vCPU	4GB	8GB	Based on the number of agents being monitored, multiple controllers will be required to scale out horizontally.
GigaVUE V Series Node	2 vCPU	3.75GB	20GB	NIC 1: Monitored Network IP; Can be used as Tunnel IP NIC 2: Tunnel IP (optional) NIC 3: Management IP
GigaVUE V Series Proxy	1 vCPU	4GB	8GB	Based on the number of GigaVUE V Series nodes being monitored, multiple controllers will be required to scale out horizontally.
GigaVUE-FM	4 vCPU	8GB	40GB	GigaVUE-FM must be able to access the controller instance for relaying the commands. Use a flavor with a root disk of minimum 40GB and an ephemeral disk of minimum 41GB.

## Recommended Instance Type for OpenStack

The instance size of the GigaVUE V Series Node is configured and packaged as part of the qcow2 image file. The following table lists the available instance types and sizes based on memory and the number of vCPUs for a single GigaVUE V Series Node. Instance sizes can be different for GigaVUE V Series Nodes in different OpenStack VMs and the default size is Small.

Type	Memory	vCPU	Disk space	vNIC
Small	4GB	2 vCPU	8GB	1 Management interface, 1 to 8 Tunnel interfaces
Medium	8GB	4 vCPU		
Large	16GB	8 vCPU		

## Network Firewall Requirements for OpenStack

Direction	Ether Type	Protocol	Port	CIDR	Purpose
<b>GigaVUE-FM</b>					
Inbound	HTTPS	TCP	443	Any IP address	Allows users to connect to the GigaVUE-FM GUI.
Inbound	IPv4	UDP	53	Any IP address	Allows GigaVUE-FM to communicate with standard DNS server
Inbound	Custom TCP Rule	TCP	5671	GigaVUE V Series Node IP	Allows GigaVUE V Series Nodes to send traffic health updates to GigaVUE-FM Allows Next Generation UCT-V to send statistics to GigaVUE-FM.
Outbound (optional)	Custom TCP Rule	TCP	8890	V Series Proxy IP	Allows GigaVUE-FM to communicate with V Series Proxy
Outbound	Custom TCP Rule	TCP	8889	GigaVUE V Series Node IP	Allows GigaVUE-FM to communicate with V Series node
<b>UCT-V Controller</b>					
Inbound	Custom TCP Rule	TCP	9900	Custom GigaVUE-FM IP	Allows GigaVUE-FM to communicate with UCT-V Controllers
Outbound	Custom TCP Rule	TCP	5671	GigaVUE-FM IP	Allows UCT-V Controller to send traffic health updates to GigaVUE-FM.
<b>UCT-V</b>					
Inbound	Custom TCP Rule	TCP	9901	Custom UCT-V Controller IP	Allows UCT-V Controllers to communicate with UCT-Vs
Outbound	Custom TCP Rule	TCP	11443	UCT-V subnet	Allows UCT-V to securely transfer the traffic to GigaVUE V Series Node
<b>UCT-V OVS Controller</b>					
Inbound	Custom TCP Rule	TCP	9900	Custom GigaVUE-FM IP	Allows GigaVUE-FM to communicate with UCT-V OVS Controllers

Direction	Ether Type	Protocol	Port	CIDR	Purpose
<b>UCT-V OVS Agent</b>					
Inbound	Custom TCP Rule	TCP	9901	Custom UCT-V OVS Controller IP	Allows UCT-V OVS Controllers to communicate with UCT-V OVS Agents
<b>GigaVUE V Series Proxy</b>					
Inbound	IPv4	TCP	8890	GigaVUE-FM IP address	Allows GigaVUE-FM to communicate with GigaVUE Cloud Suite V Series Proxys.
Outbound	Custom TCP Rule	TCP	8889	GigaVUE V Series Node IP	Allows V Series Proxy to communicate with GigaVUE V Series Nodes
<b>GigaVUE V Series Node</b>					
Inbound	Custom TCP Rule	TCP(6)	8889	GigaVUE V Series Proxy IP address	Allows GigaVUE V Series Proxys to communicate with GigaVUE V Series nodes
Outbound	IPv4	TCP	8890	GigaVUE-FM IP address	Allows GigaVUE V Series Node to communicate with GigaVUE V Series Proxy
Outbound	Custom UDP Rule	UDP	<ul style="list-style-type: none"> <li>VXLAN (default 4789)</li> <li>L2GRE (IP 47)</li> </ul>	Tool IP	Allows V Series node to communicate and tunnel traffic to the Tool
Outbound	Custom TCP Rule	TCP	5671	GigaVUE-FM IP	Allows GigaVUE V Series Node to send traffic health updates to GigaVUE-FM
Bi-directional	Custom TCP Rule	TCP	11443	GigaVUE V Series Node subnet	Allows to securely transfer the traffic in between GigaVUE V Series Nodes.

**NOTE:** The Security Group Rules table lists only the ingress rules. Make sure the egress ports are open for communication. Along with the ports listed in the Security Group Rules table, make sure the suitable ports required to communicate with Service Endpoints such as Identity, Compute, and Cloud Metadata are also open.

## Network Requirements

The following table lists the recommended requirements to setup the network topology.

Network	Purpose
<b>Management</b>	Identify the subnets that GigaVUE-FM uses to communicate with the GigaVUE V Series Nodes and Proxy
<b>Data</b>	Identify the subnets that receives the mirrored tunnel traffic from the monitored instances.  In data network, if a tool subnet is selected then the GigaVUE V Series Node egress traffic on to the destinations or tools.

## GigaVUE Cloud Suite for Nutanix

GigaVUE-FM integrates with the Nutanix Platform and deploys the components of the GigaVUE Cloud Suite for Nutanix in the underlay environment.

Once the GigaVUE Cloud Suite for Nutanix instance is launched in the Nutanix Prism central, the rest of the VM instances are automatically launched from GigaVUE-FM.

This section describes the requirements and prerequisites for configuring the GigaVUE Cloud Suite for Nutanix. Refer to the following section for details.

- [Minimum Compute Requirements for Nutanix](#)
- [Network Firewall Requirements for Nutanix](#)

### Minimum Compute Requirements for Nutanix

Compute Instances	vCPU	Memory	Disk Space	Description
GigaVUE-FM	2 vCPU	16GB	2 x 40GB	GigaVUE-FM must be able to access the GigaVUE V Series Nodes directly or a GigaVUE V Series Proxy that will relay the commands to the GigaVUE V Series Nodes.
GigaVUE V Series Node	4 vCPU	8GB	10GB	NIC 1: Monitored Network IP; Can be used as Tunnel IP NIC 2: Tunnel IP (optional) NIC 3: Management IP
GigaVUE V Series Proxy	1 vCPU	4GB	8GB	Based on the number GigaVUE V Series Nodes being monitored, multiple proxies will be required to scale out horizontally.

## Network Firewall Requirements for Nutanix

Direction	Type	Protocol	Port	CIDR	Purpose
<b>GigaVUE-FM</b>					
Inbound	HTTPS	TCP	443	Anywhere Any IP	Allows GigaVUE® V Series Nodes, GigaVUE V Series Proxy, and GigaVUE-FM administrators to communicate with GigaVUE-FM
Inbound	SSH	TCP	22	Anywhere Any IP	Allows GigaVUE® V Series Nodes, GigaVUE V Series Proxy, and GigaVUE-FM administrators to communicate with GigaVUE-FM
Outbound (optional)	Custom TCP Rule	TCP	8890	GigaVUE V Series Proxy IP	Allows GigaVUE-FM to communicate with GigaVUE V Series Proxy
Outbound	Custom TCP Rule	TCP	8889	GigaVUE V Series Node IP	Allows GigaVUE-FM to communicate with GigaVUE V Series Node
Outbound	Custom TCP Rule	TCP	9440	Prism Central IP, Prism Element IP	Allows GigaVUE-FM to communicate with Prism Central and Prism Element.
<b>GigaVUE V Series Node</b>					
Inbound	Custom TCP Rule	TCP	9903	GigaVUE V Series Proxy IP	Allows GigaVUE V Series Proxy to communicate with GigaVUE® V Series Nodes
Inbound	UDP	UDPGRE	4754	Ingress Tunnel	Allows to UDPGRE tunnel to communicate and tunnel traffic to GigaVUE V Series Nodes
Outbound	Custom TCP Rule	TCP	5671	GigaVUE-FM IP	Allows GigaVUE® V Series Node to communicate and tunnel traffic to the Tool
Outbound	Custom UDP Rule	<ul style="list-style-type: none"> <li>• UDP (VXLAN)</li> <li>• IP Protocol (L2GRE)</li> </ul>	<ul style="list-style-type: none"> <li>• VXLAN (default 4789)</li> <li>• L2GRE (IP 47)</li> </ul>	Tool IP	Allows GigaVUE® V Series Node to communicate and tunnel traffic to the Tool
Outbound (optional)	Custom ICMP Rule	ICMP	<ul style="list-style-type: none"> <li>• echo request</li> <li>• echo reply</li> </ul>	Tool IP	Allows GigaVUE® V Series Node to health check the tunnel destination traffic.

Direction	Type	Protocol	Port	CIDR	Purpose
<b>GigaVUE V Series Proxy (optional)</b>					
Inbound	Custom TCP Rule	TCP	8890	GigaVUE-FM IP	Allows GigaVUE-FM to communicate with GigaVUE V Series Proxy
Outbound	Custom TCP Rule	TCP	8889	GigaVUE V Series Node IP	Allows GigaVUE-FM to communicate with GigaVUE V Series Node

## GigaVUE Cloud Suite for VMware

GigaVUE Cloud Suite for VMware acquires, optimizes, and distributes selected traffic to your monitoring and security tools. GigaVUE Cloud Suite for VMware provides tight integration with orchestration tools to deliver intelligent network traffic visibility for workloads running in Virtual machine in VMware. GigaVUE-FM, part of the Cloud Suite, works with VMware vCenter and NSX-T to automatically deploy GigaVUE V Series Node to support a growing private cloud infrastructure. GigaVUE-FM leverages dynamic service chaining and workload relocation monitoring to ensure visibility and policy integrity.

Refer to the following topics for the requirements and prerequisites for configuring the GigaVUE Cloud Suite for VMware on the vCenter and NSX-T

- [Prerequisites for Integrating GigaVUE V Series Nodes with vCenter](#)
- [Prerequisites for Integrating GigaVUE V Series Nodes with NSX-T](#)

## Prerequisites for Integrating GigaVUE V Series Nodes with vCenter

This section describes the requirements and prerequisites for configuring the vCenter. Refer to the following section for details.

- [Network Firewall Requirements for ESXi](#)
- [Recommended Instance Types for ESXi](#)
- [Required VMware Virtual Center Privileges](#)



**NOTE:** To support internationalized characters in the VMware vCenter environment ensure that the vCenter character encoding is set to UTF-8.

## Network Firewall Requirements for ESXi

Following are the Network Firewall Requirements for GigaVUE V Series Node deployment.

Source	Destination	Source Port	Destination Port	Protocol	Service	Purpose
GigaVUE-FM	ESXi hosts	Any (1024-65535)	443	TCP	https	Allows GigaVUE-FM to communicate with vCenter and all ESXi hosts to import the V Series OVA files. OVA files require access to the host IP/URL for bulk deployment
	vCenter					
GigaVUE-FM	GigaVUE V Series Nodes	Any (1024-65535)	8889	TCP	Custom API	Allows GigaVUE-FM to communicate with GigaVUE V Series Node
GigaVUE-FM	GigaVUE V Series Nodes	Any (1024-65535)	5671	TCP	Custom TCP	Allows GigaVUE-FM to receive the traffic health updates with GigaVUE V Series Node
Administrator	GigaVUE-FM	Any (1024-65535)	443	TCP	https	Management connection to GigaVUE-FM
			22		ssh	
Administrator	GigaVUE V Series Nodes	Not Applicable	22		ssh	Troubleshooting GigaVUE V Series Nodes.

Remote Source	GigaVUE V Series Nodes	Custom Port (VXLAN and UDPGRE),N/A for GRE	4789	UDP	VXLAN	Allows to UDPGRE Tunnel to communicate and tunnel traffic to GigaVUE V Series Nodes (Applicable for Tunnel Ingress option only)
			N/A	IP 47	GRE	
			4754	UDP	UDPGRE	
GigaVUE V Series Nodes	Tool/ GiagVUE HC Series instance	Custom Port (VXLAN),N/A for GRE	4789	UDP	VXLAN	Allows GigaVUE V Series Node to communicate and tunnel traffic to the Tool
			Not Applicable	IP 47	GRE	
GigaVUE V Series Nodes	Tool/ GigaVUE HC Series instance	Not Applicable	Not Applicable	ICMP	Echo Request	Allows GigaVUE V Series Node to health check tunnel destination traffic (Optional)
					Echo Response	
GigaVUE V Series Nodes	GigaVUE-FM	Any (1024-65535)	Any (1024-65535)	TCP	Custom TCP	Allows GigaVUE V Series Nodes to communicate the traffic health updates with GigaVUE-FM

## Recommended Instance Types for ESXi

The instance size of the V Series is configured on the OVF file and packaged as part of the OVA image file. The following table lists the available instance types and sizes based on memory and the number of vCPUs for a single V Series node. Instances sizes can be different for V Series nodes in different ESXi hosts and the default size is Small.

Type	Memory	vCPU	Disk space	vNIC
Small	4GB	2 vCPU	8GB	1 Management interface, 1 Tunnel interface, and 8 vTAP interfaces
Medium	8GB	4 vCPU		
Large	16GB	8 vCPU		

**Note:** Refer to Support, Sales, or Professional Services for deployment optimization.

## Required VMware Virtual Center Privileges

This section lists the minimum privileges required for the GigaVUE-FM user in Virtual Center. You assign privileges to Virtual Center users by selecting **Administration** from the left navigation pane. Then select **Roles** under the **Access Control**. Roles should be applied at the vSphere Virtual Center level and not the Data Center or Host levels.

The following table lists the minimum required permissions for GigaVUE-FM to manage the virtual center user with roles specified above.

Category	Required Privilege	Purpose
<b>Datastore</b>	Allocate space	V Series Node Deployment
<b>Distributed Switch</b>	VSPAN Operation	VDS Tapping
<b>Folder</b>	Create Folder	V Series Node Deployment
<b>Host</b>	<b>Configuration</b> <ul style="list-style-type: none"> <li>Network Configuration</li> </ul>	VSS Tapping
	<b>Inventory</b> <ul style="list-style-type: none"> <li>Modify Cluster</li> </ul>	Pin V Series Node to the host in cluster configurations. This prevents automatic migration.
<b>Network</b>	<ul style="list-style-type: none"> <li>Assign network</li> <li>Configure</li> </ul>	<ul style="list-style-type: none"> <li>V Series Node Deployment/VSS Tapping</li> <li>V Series Node Deployment</li> </ul>
<b>Resource</b>	Assign virtual machine to resource pool	V Series Node Deployment
<b>vApp</b>	<ul style="list-style-type: none"> <li>Import</li> <li>vApp instance configuration</li> <li>vApp application configuration</li> </ul>	V Series Node Deployment
<b>Virtual machine</b>	<b>Configuration</b> <ul style="list-style-type: none"> <li>Add new disk</li> <li>Add or remove device</li> <li>Modify device settings</li> <li>Rename</li> </ul>	V Series Node Deployment V Series Node Deployment/VSS Tapping
	<b>Interaction</b> <ul style="list-style-type: none"> <li>Connect devices</li> <li>Power on</li> </ul>	V Series Node Deployment

Category	Required Privilege	Purpose
	<ul style="list-style-type: none"> <li>Power Off</li> <li>Reset</li> </ul>	
	<b>Inventory</b> <ul style="list-style-type: none"> <li>Create from existing</li> <li>Remove</li> </ul>	V Series Node Deployment
	<b>Provisioning</b> <ul style="list-style-type: none"> <li>Clone virtual machine</li> </ul>	V Series Node Deployment

## Prerequisites for Integrating GigaVUE V Series Nodes with NSX-T

This section describes the requirements and prerequisites for configuring the NSX-T. Refer to the following section for details.

- [Network Firewall Requirements for NSX-T](#)
- [Recommended Instance Types for NSX-T](#)
- [Required VMware Virtual Center Privileges](#)

**NOTE:** NSX-T is different than the ESXi implementation for hosting the V Series OVA file on an image server. In that you need to have an image server to host the V Series image file. The default http port supported is 80. However, if the image server listens on any port other than the default http port then, the port number should be provided in the image URL. For example: If the image server listens on port 8080, then the image URL should be `http://IP_Address:8080/path_to_ova` .

## Network Firewall Requirements for NSX-T

Following are the Network Firewall Requirements for GigaVUE V Series Node deployment.

Source	Destination	Source Port	Destination Port	Protocol	Service	Purpose
GigaVUE-FM	ESXi hosts	Any (1024-65535)	443	TCP	https	Allows GigaVUE-FM to communicate with vCenter, NSX-T and all ESXi hosts.
	NSX-T Manager					
	vCenter					
GigaVUE-FM	GigaVUE V Series Node	Any (1024-65535)	8889	TCP	Custom API	Allows GigaVUE-FM to communicate with GigaVUE V Series Node
Administrator	GigaVUE-FM	Any (1024-65535)	443	TCP	https	Management connection to GigaVUE-FM
			22		ssh	
GigaVUE-FM	GigaVUE V Series Node	Any (1024-65535)	5671	TCP	Custom TCP	Allows GigaVUE-FM to receive the traffic health updates with GigaVUE V Series Node
Remote Source	GigaVUE V Series Node	Custom Port (VXLAN and UDPGRE),N/A for GRE	4789	UDP	VXLAN	Allows to UDPGRE Tunnel to communicate and tunnel traffic to GigaVUE V Series Nodes (Applicable for Tunnel Ingress option only)
			N/A	IP 47	GRE	
			4754	UDP	UDPGRE	
GigaVUE V Series Node	Tool/ GigaVUE HC Series instance	Custom Port (VXLAN),N/A for GRE	4789	UDP	VXLAN	Allows GigaVUE V Series Node to communicate and tunnel traffic to the Tool
			N/A	IP 47	GRE	
GigaVUE V Series Node	Tool/ GigaVUE HC Series instance	N/A	N/A	ICMP	echo Request	Allows V Series node to health check tunnel destination traffic (Optional)
					echo Response	

GigaVUE V Series Node	GigaVUE-FM	Any (1024-65535)	5671	TCP	Custom TCP	Allows GigaVUE V Series Nodes to communicate the traffic health updates with GigaVUE-FM
GigaVUE-FM	External Image Server URL	Any (1024-65535)	Custom port on web Server	TCP	http	Access to image server to image lookup and checks, and downloading the image
NSX-T Manager						
vCenter						
ESXi host						
NSX-T Manager	GigaVUE-FM	Any (1024-65535)	443	TCP	http	When using GigaVUE-FM as the image server for uploading the GigaVUE V Series Image.
vCenter						
ESXi host						

## Recommended Instance Types for NSX-T

The instance size of the V Series is configured on the OVF file and packaged as part of the OVA image file. The following table lists the available instance types and sizes based on memory and the number of vCPUs for a single V Series node. Instances sizes can be different for V Series nodes in different NSX-T hosts and the default size is Small.

Type	Memory	vCPU	Disk space	Recommended Traffic Volume
Small	4GB	2 vCPU	8GB	upto 2G
Medium	8GB	4 vCPU	8GB	upto 4G
Large	16GB	8 vCPU	8GB	More than 4G

For more specific throughput information on specific applications, please contact Gigamon Support.

## Required VMware Virtual Center Privileges

This section lists the minimum privileges required for the GigaVUE-FM user in Virtual Center.

The following table lists the minimum required permissions for GigaVUE-FM to manage the virtual center user with roles specified above.

Category	Required Privilege	Purpose
vApp	<ul style="list-style-type: none"> <li>vApp application configuration</li> </ul>	V Series Node Deployment
Virtual machine	<b>Interaction</b> <ul style="list-style-type: none"> <li>Power on</li> <li>Power Off</li> </ul>	<ul style="list-style-type: none"> <li>V Series Node Deployment</li> <li>Used to power on and power off GigaVUE V Series Node.</li> </ul>

## GigaVUE-FM Version Compatibility Matrix

The following tables list the different versions of GigaVUE Fabric components with different versions of GigaVUE-FM.

**NOTE:** GigaVUE-FM version 6.7 supports the latest fabric components version as well as (n-2) versions. It is always recommended to use the latest version of fabric components with GigaVUE-FM, for better compatibility.

### Version Compatibility for GigaVUE V Series Node Configuration

 The following fabric components are renamed as follows:

- G-vTAP Agents - UCT-V
- Next Generation G-vTAP Agents - Next Generation UCT-V
- G-vTAP Controller - UCT-V Controller

GigaVUE-FM	GigaVUE Cloud Suite	UCT-V	UCT-V Controller	GigaVUE V Series Node	GigaVUE V Series Proxy
6.7.00	AWS	v6.7.00	v6.7.00	v6.7.00	v6.7.00
	Azure	v6.7.00	v6.7.00	v6.7.00	v6.7.00
	OpenStack	v6.7.00	v6.7.00	v6.7.00	v6.7.00
	VMware	N/A	N/A	v6.7.00	N/A
	VMware ESXi (using Third Party Orchestration)	v6.7.00	v6.7.00	v6.7.00	v6.7.00
	VMware NSX-T Federated Environment (using Third party Orchestration)	v6.7.00	v6.7.00	v6.7.00	v6.7.00
	Nutanix	N/A	N/A	v6.7.00	v6.7.00
	Third Party Orchestration	v6.7.00	v6.7.00	v6.7.00	v6.7.00
	6.6.00	AWS	v6.6.00	v6.6.00	v6.6.00
Azure		v6.6.00	v6.6.00	v6.6.00	v6.6.00
OpenStack		v6.6.00	v6.6.00	v6.6.00	v6.6.00
VMware		N/A	N/A	v6.6.00	N/A
VMware ESXi (using Third Party Orchestration)		v6.6.00	v6.6.00	v6.6.00	v6.6.00
VMware NSX-T Federated Environment (using Third party Orchestration)		v6.6.00	v6.6.00	v6.6.00	v6.6.00
Nutanix		N/A	N/A	v6.6.00	v6..00
Third Party Orchestration		v6.6.00	v6.6.00	v6.6.00	v6.6.00



GigaVUE-FM	GigaVUE Cloud Suite	UCT-V	UCT-V Controller	GigaVUE V Series Node	GigaVUE V Series Proxy
6.5.00	AWS	v6.5.00	v6.5.00	v6.5.00	v6.5.00
	Azure	v6.5.00	v6.5.00	v6.5.00	v6.5.00
	OpenStack	v6.5.00	v6.5.00	v6.5.00	v6.5.00
	VMware	N/A	N/A	v6.5.00	N/A
	VMware ESXi (using Third Party Orchestration)	v6.5.00	v6.5.00	v6.5.00	v6.5.00
	VMware NSX-T Federated Environment (using Third party Orchestration)	v6.5.00	v6.5.00	v6.5.00	v6.5.00
	Nutanix	N/A	N/A	v6.5.00	v6.5.00
	Third Party Orchestration	v6.5.00	v6.5.00	v6.5.00	v6.5.00
	6.4.00	AWS	v6.4.00	v6.4.00	v6.4.00
Azure		v6.4.00	v6.4.00	v6.4.00	v6.4.00
OpenStack		v6.4.00	v6.4.00	v6.4.00	v6.4.00
VMware		N/A	N/A	v6.4.00	N/A
VMware ESXi (using Third Party Orchestration)		v6.4.00	v6.4.00	v6.4.00	v6.4.00
VMware NSX-T Federated Environment (using Third party Orchestration)		v6.4.00	v6.4.00	v6.4.00	v6.4.00
Nutanix		N/A	N/A	v6.4.00	v6.4.00
Third Party Orchestration		v6.4.00	v6.4.00	v6.4.00	v6.4.00

GigaVUE-FM	GigaVUE Cloud Suite	G-vTAP Agent	G-vTAP Controller	GigaVUE V Series Node	GigaVUE V Series Proxy
6.3.00	AWS	v6.3.00	v6.3.00	v6.3.00	v6.3.00
	Azure	v6.3.00	v6.3.00	v6.3.00	v6.3.00
	OpenStack	v6.3.00	v6.3.00	v6.3.00	v6.3.00
	VMware	N/A	N/A	v6.3.00	N/A
	Nutanix	N/A	N/A	v6.3.00	v6.3.00
	Third Party Orchestration	v6.3.00	v6.3.00	v6.3.00	v6.3.00
6.2.00	AWS	v6.2.00	v6.2.00	v6.2.00	v6.2.00
	Azure	v6.2.00	v6.2.00	v6.2.00	v6.2.00
	OpenStack	v6.2.00	v6.2.00	v6.2.00	v6.2.00
	VMware	N/A	N/A	v6.2.00	N/A
	Nutanix	N/A	N/A	v6.2.00	v6.2.00
	Third Party Orchestration	v6.2.00	v6.2.00	v6.2.00	v6.2.00
6.1.00	AWS	v6.1.00	v6.1.00	v6.1.00	v6.1.00
	Azure	v6.1.00	v6.1.00	v6.1.00	v6.1.00
	OpenStack	v6.1.00	v6.1.00	v6.1.00	v6.1.00
	VMware	N/A	N/A	v6.1.00	N/A
	Nutanix	N/A	N/A	v6.1.00	v6.1.00
	Third Party Orchestration	v6.1.00	v6.1.00	v6.1.00	v6.1.00

GigaVUE-FM	GigaVUE Cloud Suite	G-vTAP Agent	G-vTAP Controller	GigaVUE V Series Node	GigaVUE V Series Proxy
6.0.00	AWS	v1.8-7	v1.8-7	v2.7.0	v2.7.0
	Azure	v1.8-7	v1.8-7	v2.7.0	v2.7.0
	OpenStack	v1.8-7	v1.8-7	v2.7.0	v2.7.0
	VMware	N/A	N/A	v2.7.0	N/A
	AnyCloud	v1.8-7	v1.8-7	v2.7.0	v2.7.0
5.16.00	AWS	v1.8-5	v1.8-5	v2.6.0	v2.6.0
	Azure	v1.8-5	v1.8-5	v2.6.0	v2.6.0
	OpenStack	v1.8-5	v1.8-5	v2.6.0	v2.6.0
	VMware	N/A	N/A	v2.6.0	N/A
	AnyCloud	v1.8-5	v1.8-5	v2.6.0	v2.6.0
5.15.00	AWS	v1.8-5	v1.8-5	v2.5.0	v2.5.0
	Azure	v1.8-5	v1.8-5	v2.5.0	v2.5.0
	OpenStack	v1.8-5	v1.8-5	v2.5.0	v2.5.0
	VMware	N/A	N/A	v2.5.0	N/A
	AnyCloud	v1.8-5	v1.8-5	v2.5.0	v2.5.0
5.14.00	AWS	v1.8-4	v1.8-4	v2.4.0	v2.4.0
	Azure	v1.8-4	v1.8-4	v2.4.0	v2.4.0
	OpenStack	v1.8-4	v1.8-4	v2.4.0	v2.4.0
	VMware	N/A	N/A	v2.4.0	N/A
	AnyCloud	v1.8-4	v1.8-4	v2.4.0	v2.4.0

GigaVUE-FM	GigaVUE Cloud Suite	G-vTAP Agent	G-vTAP Controller	GigaVUE V Series Node	GigaVUE V Series Proxy
5.13.01	AWS	v1.8-3	v1.8-3	v2.3.3	v2.3.3
	Azure	v1.8-3	v1.8-3	v2.3.3	v2.3.3
	OpenStack	v1.8-3	v1.8-3	v2.3.3	v2.3.3
	VMware	N/A	N/A	v2.3.3	N/A
	AnyCloud	v1.8-3	v1.8-3	v2.3.3	v2.3.3
5.13.00	AWS	v1.8-2	v1.8-2	v2.3.0	v2.3.0
	Azure	v1.8-2	v1.8-2	v2.3.0	v2.3.0
	OpenStack	v1.8-2	v1.8-2	v2.3.0	v2.3.0
	VMware	N/A	N/A	v2.3.1	N/A
5.12.01	AWS	v1.8-1	v1.8-1	v2.2.0	v2.2.0
	OpenStack	v1.8-1	v1.8-1	v2.2.0	v2.2.0
	VMware	N/A	N/A	v2.2.1	N/A
5.12.00	AWS	v1.7-1	v1.7-1	v2.1.0	v2.1.0
	OpenStack	v1.7-1	v1.7-1	v2.1.0	v2.1.0
	VMware	N/A	N/A	v2.2.0	N/A

## Supported GigaSMART Operations

The following table lists the supported GigaSMART operations by GigaVUE V Series Nodes.

GigaSMART Operation	GigaVUE Cloud Suite for AWS	GigaVUE Cloud Suite for Azure	GigaVUE Cloud Suite for OpenStack	GigaVUE Cloud Suite for VMware (ESXi)	GigaVUE Cloud Suite for VMware (NSX-T)	GigaVUE Cloud Suite for Third Party Orchestration	GigaVUE Cloud Suite for Nutanix
Masking	✓	✓	✓	✓	✓	✓	✓
Packet Slicing	✓	✓	✓	✓	✓	✓	✓
De-Duplication	✓	✓	✓	✓	✓	✓	✓
Application Metadata Exporter	✓	✓	x	✓	✓ (Only when deploying GigaVUE V Series Node using Third party Orchestration)	✓	x
L2GRE Tunnel Encapsulation	✓	x	✓	✓	✓	✓	✓
VXLAN Tunnel Encapsulation	✓	✓	✓	✓	✓	✓	✓
L2GRE Tunnel Decapsulation	✓	x	✓	✓	✓	✓	✓
VXLAN Tunnel Decapsulation	✓	✓	✓	✓	✓	✓	✓
ERSPAN Tunnel Decapsulation	✓	x	✓	✓	✓	✓	✓
UDPGRE Tunnel Decapsulation	✓	x	✓	✓	✓	✓	x
GENEVE Decapsulation	✓	x	x	x	✓	x	x

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

### Supported GigaSMART Operations

Version Compatibility for GigaVUE V Series Node Configuration

GigaSMART Operation	GigaVUE Cloud Suite for AWS	GigaVUE Cloud Suite for Azure	GigaVUE Cloud Suite for OpenStack	GigaVUE Cloud Suite for VMware (ESXi)	GigaVUE Cloud Suite for VMware (NSX-T)	GigaVUE Cloud Suite for Third Party Orchestration	GigaVUE Cloud Suite for Nutanix
SSL Decryption for Inline Tools	x	x	x	x	x	x	x
5G-Service Based Interface Application (5G-SBI)	x	x	✓	✓	✓	✓	x
5G Cloud CASA VTAP Support	x	x	✓	✓	x	✓	x

## Troubleshooting

The following commands can be used for debugging and troubleshooting.

Command	Location	Use
apiv node		This command can be used to the Software Version and the build information.
<pre> 1   apiv -x post system/sysdumpGenerate &lt;&lt;      EOF 2   EOF </pre>	<ul style="list-style-type: none"> <li>/var/crash</li> <li>/var/opt/vseries/sysdumps</li> </ul>	This command is used to generate the system dump and to collect statistics and logs.

		Sysdumps are also generated automatically by the process manager when there is a crash. These sysdump files can be used to troubleshoot the system
apiv stats	/var/opt/vseries/sysdumps/sysdump-vseries-date-time/	This command can be used in system console to troubleshoot networking issues.
ip rule > /tmp/networks.txt	/tmp/networks.txt	This command can be used in system console to troubleshoot networking issues.
ip -6 rule >> /tmp/networks.txt	/tmp/networks.txt	This command can be used in system console to troubleshoot networking issues.
cat /etc/iproute2/rt_tables >> /tmp/networks.txt	/tmp/networks.txt	This



		command can be used in system console to troubleshoot networking issues.
<code>ip route list table all &gt;&gt; /tmp/networks.txt</code>	<code>/tmp/networks.txt</code>	This command can be used in system console to troubleshoot networking issues.
<code>ip -6 route list table all &gt;&gt; /tmp/networks.txt</code>	<code>/tmp/networks.txt</code>	This command can be used in system console to troubleshoot networking issues.
<code>find /etc/netplan/* -print -exec cat {} &gt;&gt; /tmp/networks.txt \;</code>	<code>/tmp/networks.txt</code>	This command can be used in system console to troubleshoot networking issues.

# GigaVUE V Series Logs and Commands

## CLI Commands

Device/Component	Platform	Commands
UCT-V Controller	AWS/OpenStack/Azure/Anycloud	uctvr
UCT-V OVS Controller	OpenStack	uctvr
UCT-V	AWS/OpenStack/Azure/Anycloud	uctvl
UCT-V OVS Agent	OpenStack	uctvl

## Logs

Device/Component	Platform	Logs
GigaVUE-FM fabric manager	NA	<b><i>https://&lt;FM IP&gt;/api/0.9/sys/log/file/vmm.log</i></b>
UCT-V Controller	AWS/OpenStack/Azure/Anycloud	<b><i>/var/log</i></b>
UCT-V OVS Controller	OpenStack	<b><i>/var/log/syslog</i></b>
UCT-V	AWS/OpenStack/Azure/Anycloud	<b><i>/var/log</i></b>
UCT-V OVS Agent	OpenStack	<b><i>/var/log/uctv.log</i></b>
GigaVUE V Series Proxy	AWS/OpenStack/Azure/Anycloud	<b><i>/var/log</i></b>

# Additional Sources of Information

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

- [Documentation](#)
- [Documentation Feedback](#)
- [Contact Technical Support](#)
- [Contact Sales](#)
- [The VÜE Community](#)

## Documentation

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

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

Table 1: Documentation Set for Gigamon Products

GigaVUE Cloud Suite 6.7 Hardware and Software Guides
<p><b>DID YOU KNOW?</b> If you keep all PDFs for a release in common folder, you can easily search across the doc set by opening one of the files in Acrobat and choosing <b>Edit &gt; Advanced Search</b> from the menu. This opens an interface that allows you to select a directory and search across all PDFs in a folder.</p>
<p><b>Hardware</b></p> <p>how to unpack, assemble, rackmount, connect, and initially configure ports the respective GigaVUE Cloud Suite devices; reference information and specifications for the respective GigaVUE Cloud Suite devices</p>
<b>GigaVUE-HC1 Hardware Installation Guide</b>
<b>GigaVUE-HC3 Hardware Installation Guide</b>
<b>GigaVUE-HC1-Plus Hardware Installation Guide</b>
<b>GigaVUE-HCT Hardware Installation Guide</b>
<b>GigaVUE-TA25 Hardware Installation Guide</b>
<b>GigaVUE-TA25E Hardware Installation Guide</b>
<b>GigaVUE-TA100 Hardware Installation Guide</b>

## GigaVUE Cloud Suite 6.7 Hardware and Software Guides

**GigaVUE-TA200 Hardware Installation Guide**

**GigaVUE-TA200E Hardware Installation Guide**

**GigaVUE-TA400 Hardware Installation Guide**

**GigaVUE-OS Installation Guide for DELL S4112F-ON**

**G-TAP A Series 2 Installation Guide**

**GigaVUE M Series Hardware Installation Guide**

**GigaVUE-FM Hardware Appliances Guide**

### Software Installation and Upgrade Guides

**GigaVUE-FM Installation, Migration, and Upgrade Guide**

**GigaVUE-OS Upgrade Guide**

**GigaVUE V Series Migration Guide**

### Fabric Management and Administration Guides

**GigaVUE Administration Guide**

covers both GigaVUE-OS and GigaVUE-FM

**GigaVUE Fabric Management Guide**

how to install, deploy, and operate GigaVUE-FM; how to configure GigaSMART operations; covers both GigaVUE-FM and GigaVUE-OS features

### Cloud Guides

how to configure the GigaVUE Cloud Suite components and set up traffic monitoring sessions for the cloud platforms

**GigaVUE V Series Applications Guide**

**GigaVUE V Series Quick Start Guide**

**GigaVUE Cloud Suite Deployment Guide - AWS**

**GigaVUE Cloud Suite Deployment Guide - Azure**

**GigaVUE Cloud Suite Deployment Guide - OpenStack**

**GigaVUE Cloud Suite Deployment Guide - Nutanix**

**GigaVUE Cloud Suite Deployment Guide - VMware (ESXi)**

**GigaVUE Cloud Suite Deployment Guide - VMware (NSX-T)**

**GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration**

**Universal Cloud TAP - Container Deployment Guide**

## GigaVUE Cloud Suite 6.7 Hardware and Software Guides

### Gigamon Containerized Broker Deployment Guide

### GigaVUE Cloud Suite Deployment Guide - AWS Secret Regions

### GigaVUE Cloud Suite Deployment Guide - Azure Secret Regions

## Reference Guides

### GigaVUE-OS CLI Reference Guide

library of GigaVUE-OS CLI (Command Line Interface) commands used to configure and operate GigaVUE HC Series and GigaVUE TA Series devices

### GigaVUE-OS Security Hardening Guide

### GigaVUE Firewall and Security Guide

### GigaVUE Licensing Guide

### GigaVUE-OS Cabling Quick Reference Guide

guidelines for the different types of cables used to connect Gigamon devices

### GigaVUE-OS Compatibility and Interoperability Matrix

compatibility information and interoperability requirements for Gigamon devices

### GigaVUE-FM REST API Reference in GigaVUE-FM User's Guide

samples uses of the GigaVUE-FM Application Program Interfaces (APIs)

## Release Notes

### GigaVUE-OS, GigaVUE-FM, GigaVUE-VM, G-TAP A Series, and GigaVUE Cloud Suite Release Notes

new features, resolved issues, and known issues in this release ;  
important notes regarding installing and upgrading to this release

**NOTE:** Release Notes are not included in the online documentation.

**NOTE:** Registered Customers can log in to [My Gigamon](#) to download the Software and Release Notes from the Software and Docs page on to [My Gigamon](#). Refer to [How to Download Software and Release Notes from My Gigamon](#).

## In-Product Help

### GigaVUE-FM Online Help

how to install, deploy, and operate GigaVUE-FM.

## How to Download Software and Release Notes from My Gigamon

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

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

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

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

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

## Documentation Feedback

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

[documentationfeedback@gigamon.com](mailto:documentationfeedback@gigamon.com)

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

Documentation Feedback Form		
About You	Your Name	
	Your Role	
	Your Company	

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

## Contact Technical Support

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

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

Email Technical Support at [support@gigamon.com](mailto:support@gigamon.com).

# Contact Sales

Use the following information to Gigamon channel partner or Gigamon sales representatives.

**Telephone:** +1.408.831.4025

**Sales:** [inside.sales@gigamon.com](mailto:inside.sales@gigamon.com)

**Partners:** [www.gigamon.com/partners.html](http://www.gigamon.com/partners.html)

# Premium Support

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

# The VÜE Community

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

Visit the VÜE Community site to:

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

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

**Register today at** [community.gigamon.com](http://community.gigamon.com)

**Questions?** Contact our Community team at [community@gigamon.com](mailto:community@gigamon.com).



# Glossary

## D

---

### decrypt list

need to decrypt (formerly blacklist)

### decryptlist

need to decrypt - CLI Command (formerly blacklist)

### drop list

selective forwarding - drop (formerly blacklist)

## F

---

### forward list

selective forwarding - forward (formerly whitelist)

## L

---

### leader

leader in clustering node relationship (formerly master)

## M

---

### member node

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

## N

---

### no-decrypt list

no need to decrypt (formerly whitelist)

**nodecryptlist**

no need to decrypt- CLI Command (formerly whitelist)

**P**

---

**primary source**

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

**R**

---

**receiver**

follower in a bidirectional clock relationship (formerly slave)

**S**

---

**source**

leader in a bidirectional clock relationship (formerly master)