



# Universal Cloud Tap- Container Deployment Guide

**GigaVUE Cloud Suite**

Product Version: 6.4

Document Version: 1.0

Last Updated: Tuesday, February 27, 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
6.4.00	1.0	09/08/2023	The original release of this document with 6.4.00 GA.

# Contents

<b>Universal Cloud Tap-Container Deployment Guide</b> .....	<b>1</b>
Change Notes .....	3
Contents .....	4
<b>Universal Cloud Tap - Container</b> .....	<b>6</b>
<b>Components of Universal Cloud Tap - Container</b> .....	<b>6</b>
<b>Architecture of Universal Cloud Tap - Container</b> .....	<b>7</b>
<b>UCT-C and GigaVUE-FM Interaction</b> .....	<b>8</b>
UCT-C Registration .....	8
UCT-C Deregistration .....	8
UCT-C Heartbeats .....	9
Monitoring Domain and Traffic Policy .....	9
<b>Get Started with Universal Cloud Tap - Container</b> .....	<b>9</b>
Pre-requisites of UCT-C .....	10
License Information .....	10
Network Requirements .....	10
Compute Requirements .....	11
Supported Platforms for UCT-C .....	11
<b>Configure Universal Cloud Tap - Container</b> .....	<b>12</b>
Kernel and CPU Requirements: .....	12
Deploy UCT-C in Kubernetes .....	12
Deploy UCT-C Controller Service and Taps .....	13
Deploy UCT-C Taps .....	17
Configure UCT-C through GigaVUE-FM .....	20
Launch GigaVUE-FM .....	20
Create Monitoring Domain .....	20
Create Source Selectors .....	25
Create Tunnel Specifications .....	27
Configure Traffic Policy .....	27
Create Service Token .....	36
<b>Configure UCT-C Settings</b> .....	<b>37</b>
UCT-C General Settings .....	37
UCT-C Log Level Settings .....	38

	<b>39</b>
	<b>39</b>
<b>Precryption™</b> .....	<b>39</b>
How Gigamon Precryption Technology Works .....	40
Why Gigamon Precryption .....	41
Key Features .....	41
Key Benefits .....	41
How Gigamon Precryption Technology Works .....	42
Precryption Technology on Single Node .....	42
Precryption Technology on Multi-Node .....	43
Supported Platforms .....	44
Prerequisites .....	45
Note .....	45
Configure in UCT-C .....	45
<b>Secure Tunnels</b> .....	<b>46</b>
Supported Platforms .....	47
Configure Secure Tunnel .....	47
<b>Upgrade UCT-C</b> .....	<b>54</b>
Steps to Delete and Redeploy UCT-C .....	54
<b>Additional Sources of Information</b> .....	<b>57</b>
Documentation .....	57
How to Download Software and Release Notes from My Gigamon .....	59
Documentation Feedback .....	60
Contact Technical Support .....	61
Contact Sales .....	61
Premium Support .....	62
The VÜE Community .....	62
<b>Glossary</b> .....	<b>63</b>

# Universal Cloud Tap - Container

Universal Cloud Tap - Container (UCT-C) earlier known as Universal Container Tap (UCT) is a containerized component that provides the network broker features in a containerized form. UCT-C can perform traffic acquisition, basic filtering, and tunneling support. UCT-C is deployed as a Pod in the given worker node where the workloads are running.

The UCT-C is deployed by Kubernetes orchestrator and not by GigaVUE-FM. UCT-C initiates the traffic acquisition process with UCT-C Taps.

Following are the modules implemented in UCT-C:

- **Traffic Acquisition:** UCT-C supports traffic acquisition by replicating the traffic from the worker pods..
- **Filtering Module** - UCT-C provides basic filtering based on 5-Tuple. The filtering configuration is pushed by the GigaVUE-FM.
- **Tunneling Modules** - UCT-C supports L2GRE, VXLAN, and TLS-PCAPng tunneling to send the tapped traffic to the GigaVUE V Series or tools.

This guide provides an overview of Universal Cloud Tap - Container and describes how to install and deploy UCT-C components in your Pods.

Topics:

- [Architecture of Universal Cloud Tap - Container](#)
- [UCT-C and GigaVUE-FM Interaction](#)
- [Get Started with Universal Cloud Tap - Container](#)
- [Configure Universal Cloud Tap - Container](#)
- [Configure UCT-C Settings](#)

## Components of Universal Cloud Tap - Container

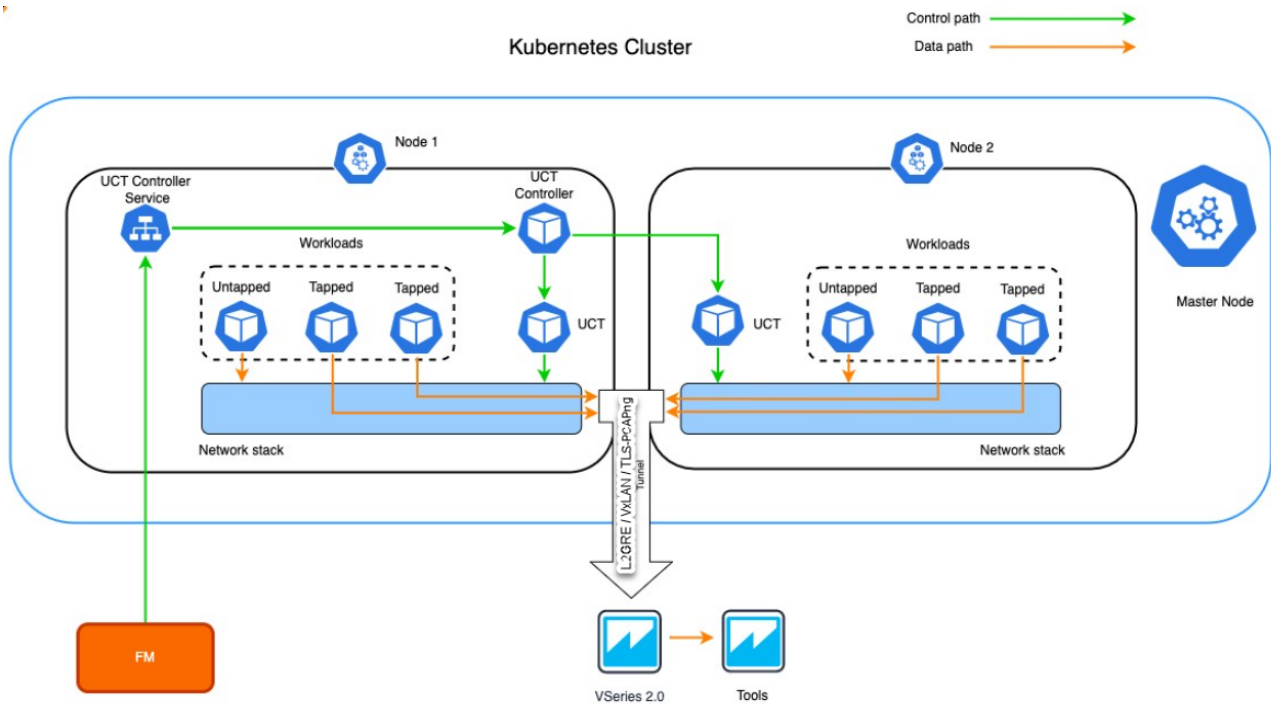
The Universal Container Tap works with the following components:

- **GigaVUE® Fabric Manager (GigaVUE-FM)** is a web-based fabric management and orchestration interface that provides a single pane of glass visibility, management, and orchestration of both the physical and virtual traffic that form the UCT-C.

- **UCT-C Tap** is the primary UCT-C module that collects the workload traffic, filters the traffic and tunnels the filtered traffic directly to the tools or through the GigaVUE V Series Nodes. UCT-C Tap also sends the statistics and heartbeats to UCT-C Controller. For tapping, don't select the taps which have **true** for the option **HostName**. UCT-C Tap should run as a **privileged pod**.
- **UCT-C Controller** is the management component of UCT-C to control and communicate with UCT-C Tap. UCT-C Controller collects the data from UCT-C Taps and sends the collected statistics and heartbeats to GigaVUE-FM.

# Architecture of Universal Cloud Tap - Container

The following diagram illustrates the architecture of Universal Container Tap environment.



1. The UCT-C Tap is registered with GigaVUE-FM through the UCT-C Controller
2. GigaVUE-FM deploys the traffic policy on the UCT-Cs.  
Communication of configuration, data, and statistics to and from UCT-C is performed through the UCT-C Controller Service. GigaVUE-FM communicates with the UCT-C Taps through the UCT-C Controller. GigaVUE-FM deploys the traffic policy on UCT-C and receives the statistics from UCT-C tap through UCT-C controller.
3. The customer workload collects the network traffic and sends the network packets to the Kernel space.
4. The Kernel space filters the packets based on the rules and filters.
5. The filtered network packets are tunneled directly to the Tools or through the GigaVUE V Series nodes running on any supported GigaVUE Cloud Suite on cloud environment.
6. The UCT-C Controller collects the data from UCT-C Taps and sends the collected statistics and heartbeats to GigaVUE-FM.

## UCT-C and GigaVUE-FM Interaction

Following are the interactions between UCT-C and GigaVUE-FM:

- [UCT-C Registration](#)
- [UCT-C Deregistration](#)
- [UCT-C Heartbeats](#)
- [Monitoring Domain and Traffic Policy](#)

### UCT-C Registration

When UCT-C comes up in the Kubernetes environment, UCT-C registers itself with GigaVUE-FM. When GigaVUE-FM is unreachable, UCT-C tries to reconnect infinite times. If the GigaVUE-FM is unreachable even after the retries, Kubernetes deployment of UCT-C fails. UCT-C only supports IPv4 protocol. For more information, refer to [Deploy UCT-C in Kubernetes](#)

### UCT-C Deregistration

When UCT-C is terminated normally, UCT-C sends the deregistration message to GigaVUE-FM. If UCT-C goes down abnormally, it will get deregistered when the GigaVUE-FM misses to receive couple of heartbeats.



## UCT-C Heartbeats

Periodically, UCT-C sends heartbeats to GigaVUE-FM. By default, the status of UCT-C is marked as **Connected**. The following are the various scenarios where the UCT-C status changes:

- If 3 consecutive heartbeats are missed, GigaVUE-FM marks the status as **Disconnected**.
- If 2 consecutive heartbeats are missed, GigaVUE-FM marks the status as **Pending**.
- GigaVUE-FM purges disconnected or terminated UCT-C taps after 30 days.

## Monitoring Domain and Traffic Policy

You can configure and manage the Monitoring Domains, Connections, Source Inventories, and Traffic Policies of UCT-C in GigaVUE-FM. For more information, refer to [Configure UCT-C through GigaVUE-FM](#)

Refer to the [GigaVUE API Reference](#) for detailed information on the REST APIs of UCT-C.



- A Traffic Policy is a combination of Rules and Tunnels.
- A rule contains specific filtering criteria that the packets must match. The filtering criteria lets you determine the target instances and the (egress or ingress) direction of tapping the network traffic.
- A tunnel is a communication path in which the traffic matching the filtered criteria is routed to the destination.

# Get Started with Universal Cloud Tap - Container

This section describes how to initiate UCT-C and GigaVUE-FM deployment with the required licenses and network requisites.

Refer to the following sections for details:

- [Pre-requisites of UCT-C](#)
- [Components of Universal Cloud Tap - Container](#)
- [License Information](#)
- [Network Requirements](#)
- [Compute Requirements](#)

## Pre-requisites of UCT-C

To work with UCT-C, you must have knowledge in the following platforms:

- Kubernetes
- GigaVUE-FM
- Knowledge to work in any platform such as AWS EKS, Azure AKS, and RedHat OpenShift where the Kubernetes clusters are deployed.

## License Information

All the UCT-C Taps deployed in your environment periodically report the statistics to UCT-C Controller. Then the UCT-C Controller periodically reports the collective statistics of UCT-C Taps to GigaVUE-FM for Volume-Based Licensing.

In the Volume-Based Licensing scheme, a license entitles specific applications on your devices to use a specified amount of total data volume over the term of the license. The distribution of the license to individual nodes or devices becomes irrelevant for Gigamon’s accounting purpose. GigaVUE-FM tracks the total amount of data processed by the UCT-C, and tracks the overuse if any.

Volume-based licensing has a service period of 1 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](#).

## Network Requirements

The following table describes the Kubernetes network requirements for UCT-C to work efficiently.

Direction	Type	Protocol	Port	CIDR	Purpose
<b>Universal Cloud Tap - Container</b> deployed inside Kubernetes worker node					
Outbound	HTTPS	TCP	443	Any IP address	Allows UCT-C Controller to communicate with GigaVUE-FM
Inbound	HTTPS	TCP	8443 (configurable)	Any IP address	Allows GigaVUE-FM to communicate with UCT-

Direction	Type	Protocol	Port	CIDR	Purpose
					C Controller.
Outbound	HTTPS	TCP	5671	Any IP address	Allows UCT-C to send statistics to GigaVUE-FM through Rabbit-MQ port.
Outbound	HTTPS	TCP	42042	Any IP address	Allows UCT-C to to send statistics information to UCT-Ccontroller.

## Compute Requirements

The following table describes the minimum compute network requirements for UCT-C.

Compute Instances	vCPU	Memory	Disk Space
Universal Container Tap (UCT)	1 vCPU	64MB	—
UCT-C Controller	1 vCPU	64MB	—
GigaVUE V Series Node	4 vCPUs	8GB	20GB
GigaVUE V Series Proxy	1 vCPU	1GB	2GB
GigaVUE-FM	4 vCPUs	16GB	41GB

## Supported Platforms for UCT-C

The following tables list the different platforms and their Kubernetes version, Container Run-time Interface (CRI), and Container Network Interface (CNI) that are qualified and supported for UCT-C.

**NOTE:** As an end user, you must have an understanding and knowledge of your container services.

Platform	Kubernetes Version	CRI	CNI
Amazon Elastic Kubernetes Service (EKS)	1.26	Containerd	VPC
Azure Kubernetes Service (AKS)	1.24	Containerd	Azure CNI
VMware Tanzu	1.20	Containerd	Antrea and Calico

Platform	Kubernetes Version	CRI	CNI
Red Hat OpenShift	1.22	CRI-O	OVN
Native Kubernetes	1.24	Docker	Flannel and Calico

# Configure Universal Cloud Tap - Container

Setting up UCT-C involves the following two steps:

- [Deploy UCT-C in Kubernetes](#)
- [Configure UCT-C through GigaVUE-FM](#)



The Red Hat supported base images of the UCT-C applications are built on the top of Red Hat Universal Base Image or Red Hat Enterprise Linux Image. The UCT-C images are **Red Hat Certified** for Red Hat OpenShift platform.

## Kernel and CPU Requirements:

The kernel requirements for different platforms are as follows:

- EKS – 5.4
- Native Kubernetes– 5.4, 4.19 (Photon+ OS)

The minimum CPU and RAM requirements for TAP and Controller are as follows:

- UCT-C — 1vcpu and 64Mi
- UCT-C-Controller— 1vcpu and 64Mi

## Deploy UCT-C in Kubernetes

To fully deploy UCT-C, the following steps are required to be completed:

1. Implement external access to the Kubernetes environment (e.g., ingress, external public IPs, load balancers) to allow communication between UCT-C and GigaVUE-FM.
2. Ensure that the firewall rules on Kubernetes nodes are met according to the [Network Requirements](#).

3. YAML files or HELM charts are available as part of the UCT images. You should untar the UCT image to get the readme files.
4. Add the UCT-C images to a private Docker registry or ensure that the files can be pulled from the Docker Hub registry. You can spin up or spin down the UCT-C instances based on your traffic load.
5. Deploy UCT-C Controller Service and Taps using [YAML files](#) or [Helm Charts](#).
6. Deploy UCT-C Taps using [YAML files](#) or [Helm Chart](#).

Refer to the following topics for UCT-C Controller and Taps:

- [Deploy UCT-C Controller Service and Taps](#)
- [Deploy UCT-C Taps](#)

## Deploy UCT-C Controller Service and Taps

You can deploy the UCT-C Controller Service and Taps using the YAML files or the Helm Charts. Refer to the following sections for detailed information.

- [Deploy UCT-C Controller Service and Taps using YAML files](#)
- [Deploy UCT-C Controller Service and Taps using Helm Chart](#)

Deploy UCT-C Controller Service and Taps using YAML files

### Deploy UCT-C Controller Service

Follow the instructions below to deploy UCT-C Controller Service in your Kubernetes environment using YAML file:

**NOTE:** [Contact Technical Support](#) or [Contact Sales](#) for the UCT-C images and YAML files.

1. In your Kubernetes orchestrator, edit the UCT-C Controller image name, commands, and other required information into your YAML file. The following is sample data from the YAML file. Edit your YAML file based on the sample given below. Do not copy and paste this content into your YAML file:

```

apiVersion: v1
kind: Service
metadata:
  labels:
    app: gigamon-uct
    pod: uct-cntlr
    service: uct-cntlr-service
    # change the namespace to match your namespace
  name: uct-cntlr-service
spec:
  ports:
    - name: uct-rest
      port: 8443
      protocol: TCP
      targetPort: 8443
    - name: uct-stats
      port: 42042
      protocol: TCP
      targetPort: 42042
  selector:
    app: uct-cntlr
    type: ClusterIP

```

The following table gives a description of all the field values in the YAML file that are updated:

Field Values	Description
Port: 443	The UCT-C Controller REST service port number.
Port: 42042	This port must be port 42042. This allows GigaVUE-FM to communicate with UCT-C to send statistical data.

2. Using the YAML file, Kubernetes creates the UCT-C Controller Service.

## Deploy UCT-C Controller

Follow the instructions below to deploy UCT-C Controller Service in your Kubernetes environment using YAML file:

**NOTE:** [Contact Technical Support](#) or [Contact Sales](#) for the UCT-C images and YAML files.

1. In your Kubernetes orchestrator, edit the UCT-C Controller image name, commands, and other required information into your YAML file. The following is sample data from the YAML file. Edit your YAML file based on the sample given below. Do not copy and paste this content into your YAML file:

```

name: uct-cntlr
image: gigamon/uct-cntlr:cntlr-<version>
command:
- # /uct-controller
- # <GigaVUE-FM IP>
- # <GigaVUE-FM REST Svc Port>
- # <UCT-C-Cntlr REST SVC Port>
env:
# Service name. Should match name specified in metadata section.
- name: UCT-C_CNTLR_SERVICE_NAME
  value: "GIGAMON_UCT-C_CNTLR_SERVICE"
# External LB balancer IP, for controller (FM) to connect to UCT-C-
cntlr
- name: UCT-C_CNTLR_EXT_IP_DNS
  value: "<external IP for GigaVUE-FM to reach UCT-C CNTLR>"
# K8S cluster end-point (typically, master nodes with default port of
6443)
- name: K8S_CLUSTER_ENDPOINT
  value: <K8s Cluster API URL>
- name: UCTC_DEBUG_MODE
  value: "0x0A000003"
# Namespace of Pod
- name: UCT-C_CNTLR_Tap_NAMESPACE
  valueFrom:
    fieldRef:
      fieldPath: metadata.namespace
ports:
- containerPort: 8443
  protocol: TCP
- containerPort: 42042
  protocol: TCP
imagePullPolicy: Always

```

The following table gives a description of all the field values in the YAML file that are changed or updated:

Field Values	Description
/uct-cntlr (image name)	UCT-C Controller image name and version. Make sure to use the latest image version.
GigaVUE-FM IP	The IP address of the GigaVUE-FM with which your UCT-C is connected.
FM REST Svc Port	The FM REST service port number. This must be opened on your Kubernetes to allow outbound traffic. This allows UCT-C Controller to communicate with GigaVUE-FM. Example: 443
UCT-C-Cntlr REST SVC Port	The UCT-C Controller REST service port number. This must be

Field Values	Description
	opened on your GigaVUE-FM to allow inbound traffic to Kubernetes. This allows GigaVUE-FM to communicate with UCT-C Controller. Example: 8443 (configurable)
Ports: <ul style="list-style-type: none"> <li>o containerPort: 443</li> <li>o containerPort: 42042</li> </ul>	Two ports must be opened. The first container port must be the same as UCT-C-Cntlr REST SVC Port. The second container port must be port 42042. This allows UCT-C to send statistical data to UCT-C controller.
External LB balancer IP	The external load balancer IP/DNS value to allow GigaVUE-FM to communication with UCT-C Controller within Kubernetes. The GigaVUE-FM IP entry may change when you upgrade or redeploy.
K8S cluster end-point	Kubernetes cluster end point for GigaVUE-FM to access the control plane. UCT supports eight policies per cluster. Example: https://<kubernetesapiserverurl>:6443

- Using the YAML file, Kubernetes automatically downloads the defined UCT-C Controller Taps and deploys it to the Kubernetes worker node.

#### Deploy UCT-C Controller Service and Taps using Helm Chart

Follow the instructions below to deploy UCT-C Controller Service and Taps in your Kubernetes environment using Helm Chart:

**NOTE:** [Contact Technical Support](#) or [Contact Sales](#) for the UCT-C images and Helm Charts (**uct-cntlr-<version>.tgz** and **uct-tap-<version>.tgz**).

- On your Kubernetes orchestrator, extract the received UCT-C Controller (service and Tap) **.tgz** package.

```
$ tar -xvf uct-cntlr-<version>.tgz
```
- After extraction, navigate to the uct-cntlr folder and edit the **values.yaml** file as per your environment. Refer to [Deploy UCT-C Controller Service](#) and [Deploy UCT-C Controller](#) for detailed information.
- From the extracted uct-cntlr folder, install the UCT-C Controller Helm using the following command:

```
$ helm install <Name for the UCT-C Controller> uct-cntlr <Extracted folder path> uct-cntlr/
```
- Using the Helm file, Kubernetes creates the UCT-C Controller Service, automatically downloads the defined UCT-C Controller Taps and deploys it to the your worker node.



## Deploy UCT-C Taps

You can deploy the UCT-C Taps using the YAML files or the Helm Charts. Refer to the following sections for detailed information.

- [Deploy UCT-C Taps using YAML files](#)
- [Deploy UCT-C Taps using Helm Chart](#)

### Deploy UCT-C Taps using YAML files

Follow the instructions below to deploy UCT-C Taps in your Kubernetes environment using YAML file:

**NOTE:** [Contact Technical Support](#) or [Contact Sales](#) for the UCT-C images and YAML files.

1. In your Kubernetes orchestrator, edit the UCT-C Tap image name, commands, and other required information in a YAML file. The following is sample data from the YAML file. Edit your YAML file based on the sample given below. Do not copy and paste this content into your YAML file:

```

name: gigamon-uct-c
command:
- # /uctcapp/uctc
- # (1=> default, 0=> rule)
- # (1=> L2GRE, 3=> VXLAN)
env:
  name: SECURE_TUNNEL_RING_BUFFER_MEMORY_MB
  value: '128'
  - name: PRECRYPTION_RING_BUFFER_MEMORY_MB
  value: '128'
- name: PRECRYPTION_PATH_MTU
  value: '1500'
etc
- name: LD_LIBRARY_PATH
  value: /usr/lib64
- name: UCTC_DEBUG_MODE
  value: "0x0A000003"
- name: UCTC_SERVICE_NAME
  value: "UCTC_SERVICE"
- name: UCTC_CNTLRL_SVC_DNS
  #value: "<UCTC-CNTLR-SVC-NAME.UCTC-CNTLR-
  NAMESPACE>.svc.cluster.local" - name: UCTC_CNTLRL_REST_SVC_PORT
  # port used to receive configuration from FM
  value: '8443'
- name: UCTC_WORKERNODE_NAME
valueFrom:
fieldRef:
fieldPath: metadata.namespace
image: gigamon/uct:<version>

```

The following table gives a description of all the field values in the YAML file that are changed or updated:

Field Value	Description
(1=> default, 0=> rule)	(0/1) Enter 1 to use the default destination IP, or enter 0 to use the rules configured by GigaVUE-FM
(1=> L2GRE, 3=> VXLAN)	(1/3) Enter 1 to use the L2GRE tunnel type or enter 3 to use the VXLAN tunnel type.
gigamon/uct-tap:<version>	UCT-C Controller image name and version. Make sure to use the latest image version.
UCT-C_DEBUG_MODE	The hex value for UCT-C debugging. This value must be in the <b>0xdd [aaaa][b][c]</b> format, where: <ul style="list-style-type: none"> <li>• aaaa is a hex value for the number of pcap messages to maintain before rollover</li> </ul>

Field Value	Description
	<ul style="list-style-type: none"> <li>• b is 0 = do not create pcap or 1 = create pcap</li> <li>• c is level. Level with 1 =fatal, 2 =error, 3 =info, 4 =debug</li> <li>• dd is the log file size multiplier                             <ul style="list-style-type: none"> <li>• dd = 0 1 - means default log file size (default 100,000 lines)</li> <li>• dd = 08 - means 8 * default log file size (default 8*100,000 lines)</li> <li>• dd = FF = 255 - means (255*100,000 lines)</li> </ul> </li> </ul>
UCT-C_CNTLR_SVC_DNS	UCT-C Controller Service Number. This value must match the metadata used for UCT-C Controller. Example: gigamon-uct-cntrlr-service.default.svc.cluster.local
UCT-C_CNTLR_REST_SVC_PORT	The UCT-C Controller REST service port number. This must be opened on your GigaVUE-FM to allow inbound traffic to Kubernetes.
Preryption Path MTU	This is an optional configuration. By default, preryption VxLAN encapsulated packets will be 4200 bytes. (4096 + 104 overhead) You can configure the path MTU and preryption module does the fragmentation at the source. The default value is 9000. The value ranges from 1400-9000.

2. Using the YAML file, Kubernetes automatically downloads and deploys the defined UCT-C Taps.

## Deploy UCT-C Taps using Helm Chart

Follow the instructions below to deploy UCT-C Taps in your Kubernetes environment using Helm Chart:

**NOTE:** [Contact Technical Support](#) or [Contact Sales](#) for the UCT-C images and Helm Charts (**uct-cntrlr-<version>.tgz** and **uct-tap-<version>.tgz**).

1. On your Kubernetes orchestrator, extract the received UCT-C Tap.tgz package.
 

```
$ tar -xvf uct-tap-<version>.tgz
```

 After extraction, navigate to the uct-tap folder and edit the **values.yaml** file as per your environment. Refer to [Deploy UCT-C Taps using YAML files](#) for detailed information.
2. From the extracted uct-tapfolder, install the UCT-C Helm using the following command:
 

```
$ helm install <Name for the UCT-C Tap> uct-tap<Extracted folder path> uct-tap/
```

3. Using the Helm file, Kubernetes creates the UCT-C Tap, automatically downloads the defined UCT-C Taps and deploys it to the Kubernetes worker node.

## Configure UCT-C through GigaVUE-FM

This section describes how to configure UCT-C through GigaVUE-FM GUI. Refer to the following section for details.

- [Launch GigaVUE-FM](#)
- [Create Monitoring Domain](#)
- [Create Source Selectors](#)
- [Create Tunnel Specifications](#)
- [Configure Traffic Policy](#)
- [Traffic Policy Statistics](#)

### Launch GigaVUE-FM

The recent GigaVUE-FM image files can be downloaded from [Gigamon Customer Portal](#). After fetching the image, upload and launch GigaVUE-FM on your GigaVUE V Series Node supported cloud environment. For assistance, [Contact Technical Support](#) of Gigamon or refer to GigaVUE Cloud Suites for more information on GigaVUE V Series configuration on the supported cloud environments.

### Create Monitoring Domain

To create a monitoring domain in GigaVUE-FM:



1. In GigaVUE-FM, on the left navigation pane, select **Inventory > CONTAINER > Universal Cloud Tap - Container > Monitoring Domains**. The **Monitoring Domain** page appears.
2. In the **Monitoring Domain** page, click **New**. The **New Monitoring Domain** wizard

appears.

3. Enter or select the required information as described in the following table,

Fields	Description
Monitoring Domain Name	Enter a name for the monitoring domain
Connections	
Connection Name	Enter a name for the UCT-C connection
Cluster Name	Enter a name for the cluster
URL	Enter the URL of the API server


Fields	Description
Inventory Discovery	<p>Select any one of the following options:</p> <ul style="list-style-type: none"> <li>● FM - When you select FM, you need to enter the authentication token.</li> </ul> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p><b>NOTE:</b> If you don't have an authentication token, the GigaVUE-FM can't pull the inventory. You can use the other options mentioned below to include the inventory.</p> </div> <p>References for POST and DELETE APIs:</p> <ul style="list-style-type: none"> <li>○ <b>POST</b>/cloud/kubernetes/inventory/pods/{connectionId} Add/Create UCT-C Kubernetes pods inventory.</li> <li>○ <b>DELETE</b>/cloud/kubernetes/inventory/pods/{connectionId} Delete UCT-C Kubernetes pods inventory.</li> <li>○ <b>POST</b>/cloud/kubernetes/inventory/services/{connectionId} Add/Create UCT-C Kubernetes services inventory in FM.</li> <li>○ <b>DELETE</b>/cloud/kubernetes/inventory/services/{connectionId} Delete UCT-C Kubernetes services inventory.</li> <li>○ <b>POST</b>/cloud/kubernetes/inventory/nodes/{connectionId} Add/Create UCT-C Kubernetes nodes inventory in FM.</li> <li>○ <b>DELETE</b>/cloud/kubernetes/inventory/nodes/{connectionId} Delete UCT-C Kubernetes nodes inventory.</li> </ul> <p>Refer to the <a href="#">GigaVUE API Reference</a> for detailed information.</p> <ul style="list-style-type: none"> <li>● Upload - You need to upload the inventory information into GigaVUE-FM. You must feed the inventory details through the REST APIs. Refer to the <a href="#">GigaVUE API Reference</a> for detailed information.</li> <li>● UCT-C controller-&lt;MadCap:variable name="featVar.feat-UCT-short" /&gt; controller running as a POD in each Kubernetes cluster collects the inventory information and sends it to GigaVUE-FM.</li> </ul>
Authentication Type	<p>Select token as the authentication type. By default, the authentication type is token. The option is applicable only if the Inventory Discovery is GigaVUE-FM.</p>
Token	<p>Enter the authentication token. The option is applicable only if the Inventory Discovery is GigaVUE-FM.</p>

- Click  to add another connection and click  to remove an existing connection.
4. Click **Save** to create a monitoring domain.

**NOTE:** If the connecting UCT-C Tap does not send 3 continuous heart beats, it is marked as disconnected and it is shown on the monitoring domain page as per the interval configured in the UCT-C Purge (the default purge interval is 30 days) before the GigaVUE-FM cleans them up.

You can view the monitoring domain created in the list view. The list view shows the following information for UCT-C and controllers:

- Monitoring Domain
- URL
- Connection
- Cluster Name
- Cluster Version
- Controller / TAP
- UCT-C UUID
- Management IP
- Version
- Node Name
- Node Kernel Version
- Status
- Discovered Sources

**NOTE:** Click the  to select the columns that should appear in the list view.

Use the following buttons to manage your Monitoring Domain:

Button	Description
New	Use to create new connection
Actions	Provides the following options: <ul style="list-style-type: none"> <li>▪ <b>Edit</b>- Edit the monitoring domain</li> <li>▪ <b>Delete Domain</b> - Delete the monitoring domain</li> </ul>
Filter	Filters the monitoring domain based on the following options: <ul style="list-style-type: none"> <li>▪ <b>Connected</b></li> <li>▪ <b>Pending</b></li> <li>▪ <b>Disconnected</b></li> <li>▪ <b>Terminated</b></li> </ul>



**NOTE:** You can click on the **Discovered Sources** link to view the source details. In the Discovered Sources window, you can enable the **Show System Pods** button to view the information related to the system pods that are not monitored.





## Create Source Selectors

When setting up a traffic flow, it is important to define the selection criteria for the sources of traffic. Use the Source Selectors page for configuring the sources of the traffic to be monitored.

To configure the Source Selectors:

1. Select **Inventory > Resources > Source Selectors**.
2. On the **Source Selectors** page, navigate to the **Container** tab and click **Create**. The **New Source Selector** wizard appears.

3. Enter or select the required information:

Field	Action
Name	Enter a name for the source
<b>Include Filters (Criteria 1)</b>	
You can select any one of the following options	
<ul style="list-style-type: none"> <li>● <b>All Sources</b> - Select this option to acquire traffic from all names, all pods and containers within the selected cluster(s). Depending on the size of the cluster(s), volume of traffic may be larger.</li> <li>● <b>Criteria1</b>- You must enter the following options:</li> </ul>	
Object Property	Select an object property to filter the traffic source.
Operator	Select the operator.
Values	Enter the values for the filter.
<p><b>On the Criteria, click  to add another Object and click  to remove an existing Object.</b></p>	
<b>Exclude Filters (Criteria 1)</b>	
On the Criteria, click  to add another Object and click  to remove an existing Object.	
Object Property	Select an object property to filter the traffic source.
Operator	Select any one of the operators: <ul style="list-style-type: none"> <li>● equals</li> <li>● contains</li> <li>● startswith</li> <li>● endwith</li> </ul>
Values	Enter the values for the filter.

On the Include or Exclude filters, click  to add another Criteria and click  to remove an existing Criteria.

4. Click **Save** to save the filter.



**Note:** You can create multiple filter criteria. Within each criterion, you can configure multiple filters.

- If you have configured multiple filters in a criterion, then the traffic will be filtered only if all the filter rules are true.
- If you have configured multiple criteria, then the traffic will be filtered even if one of the criteria is true.

## Create Tunnel Specifications

A tunnel of type L2GRE, VXLAN, or TLS-PCAPNG, can be created. The tunnel is an egress tunnel.

To configure the tunnels:

1. Select **Inventory > Resources > Tunnel Specifications**.
2. On the **Tunnel Specifications** page, navigate to **Container** tab and click **Create**. The **Create Tunnel Specification** wizard appears.

**Create Tunnel Specifications** Save Cancel

**Name**

**Tunnel Type**

**Destination IP Address**

**Key**

3. Enter or select the following information:

Field	Description
Name	The name of the tunnel endpoint.
Tunnel Type	Select L2GRE, VXLAN, or TLS-PCAPNG tunnel type to create a tunnel.
Destination IP Address	Enter the IP address of the destination endpoint
Key	Enter a value for the tunnel key

4. Click **Save** to save the configuration.

## Configure Traffic Policy





To create a UCT-C Traffic Policy in GigaVUE-FM:

1. From the GigaVUE-FM left navigation pane, select **Traffic > CONTAINER > Universal Cloud Tap - Container**. The **Policies** page appears.
2. In the **Policies** page, click **Create**. You can create a maximum of eight policies per monitoring domain. The Create Policy wizard appears.
3. In the **General** tab, enter or select the required information as described in the following table:

Fields	Description
Policy Name	Enter a name for the Traffic Policy. The name must be unique.
Monitoring Domain	Select an existing monitoring domain. To create a new monitoring domain, refer to <a href="#">Create Monitoring Domain</a> section.
Connections	Select one or more connections for the policy. Once traffic policy is created for monitoring domain, you cannot add or delete connections in a monitoring domain.

4. Switch to the **Source Selectors** tab, select an existing source selector or select **Create New** to create a new source selector, refer to [Create Source Selectors](#) section for detailed information.
5. Switch to the **Rules** tab, enter or select the required information for the **Ingress Rules** and the **Egress Rules** as described in the following table. You must select CA in the Monitoring Domain page to use secure tunnel in rules.

6.

Fields	Description
<b>Rules</b>	
On the Ingress or Egress rules, click  to add another rule and click  to remove an existing rule. You must select CA in the Monitoring Domain page to use secure tunnel in rules.	
Rule Name	Enter a name for the rule.  <b>NOTE:</b> Rule names ending with __I, __E, __RI, __RE are not recommended as the names are invalid in policy rules.
Enable	Select <b>On</b> to enable the filter or select <b>Off</b> to disable the filter
Action	Select Pass to allow the packets or select Drop to block the packets based on the filters.
Direction	Select any one of the following directions: <ul style="list-style-type: none"> <li>● Bi-directional - Taps the traffic in both directions. The maximum number of rules supported per direction is 32. Also, each directional rule will add 2 ingress rules and 2 egress rules.</li> <li>● Ingress- Taps the ingress traffic.</li> <li>● Egress - Taps the egress traffic.</li> </ul>
Priority	Enter a priority value to specify the precedence.
Tunnel Specifications	Select an existing tunnel or select <b>Create New</b> to create a new tunnel, refer to <a href="#">Create Tunnel Specifications</a> section for detailed information.
<b>Filters</b>	
On the rule section, click  to add another filter and click  to remove an existing filter.	
Filter Type	Select a filter type
Filter Name	Enter a name for the filter
Value	Enter a value for the filter

7. Switch to the **Deploy** tab, click **Deploy** and the selected traffic policy rules get deployed to the required UCT-C taps present on the nodes corresponding to the source pods selected for monitoring.

The Traffic Policy processes the customer workload traffic and UCT-C forwards the traffic to the tunnel destination IP address.

### Traffic Policy Statistics

Traffic Policy Statistics in the GigaVUE-FM provides the visibility of the policies within a Monitoring Domain and displays the information of the policies and its rules statistics in the dashboard. It also allows visualization and performance at every container level of the Policy Deployment.

Rules are configured in the UCT-C to either forward the traffic to a Tunnel or drop the flow of the traffic. In the Policies page, along with the UCT-C policy and its rules, you can also view the aggregated statistics of all the source selectors which are part of the policy.

The activities of the rules are reflected by the statistics counters. The statistics counters show how the policy statistics are directly co-related to the policy and its rules being configured through the GigaVUE-FM.


### Viewing Policy Statistics

To view the statistics of the traffic policy configured in the GigaVUE-FM, do the following steps:

1. Go to **Traffic > Container > UCT-C**. The **Policies** page appears. In the policy page, you can view various details related to a policy such as **Name, Monitoring Domain, Connection, Status**, etc., For each policy, the value correspond to the aggregate value of UCT-C taps associated with that policy. The fields and the description of the field names are given in the following table:

Table 1:

Field	Description
Name	Name of the Policy
Monitoring Domain	Monitoring Domain associated with the Policy.
Connection	The connection associated with the policy.
Status	Specifies whether the policy deployment is : <ul style="list-style-type: none"> <li>• Success</li> <li>• Failure</li> <li>• No Target Selected</li> </ul>
UCT-C Deployment Details	Specifies the count of successful deployment along with the total number of deployment for a policy.
Ingress packets	Total aggregate value of the ingress packets associated with the policy.
Egress packets	Total aggregate value of the egress packets associated with the policy.
Rx Dropped	Total aggregate value of the ingress packets dropped associated with the policy
Ingress Dropped	Total aggregate value of the ingress packets dropped associated with the policy
Tx Dropped	Total aggregate value of the egress packets dropped associated with the policy.
Egress Dropped	Total aggregate value of the egress packets dropped associated with the policy.
Ingress Bytes	Total aggregate value of the ingress bytes associated with the policy.
Egress Bytes	Total aggregate value of the egress bytes associated with the policy.
Ingress Errors	Total aggregate value of the ingress errors associated with the policy.
Egress Errors	Total aggregate value of the egress errors associated with the policy.

**NOTE:** Click the Gear icon  to add or remove column or columns as per your requirement.

2. Click the **name** of a policy to view the statistics of the policy. The statistics appears on the bottom of the **Policies** page.

You can view the following three tabs along with the policy name:

- [Source Specifications](#)
- [Rules](#)
- [Container](#)

You can scroll each of the tables to view more columns. The fields and description for the tab that appears when you click the tabs are described in the topics respectively.

### Source Specifications

You can view the criteria based on which a pod is selected for tapping.

The fields and descriptions of the source specifications tab are described in the following table:

Table 2:

Tab-	Field	Description
<b>Source Specifications</b>		
<b>Source Selector</b>		
	Name	Specifies the name of the Source selector.
<b>Include Criteria</b>		
	Criteria Name	Specifies the include criteria for the source selector. Pod that matches the include criteria is part of the source for the given traffic policy.
	Property	Specifies the attributes of the pod. The available attributes are: service
	Operator	Specifies the operator used in the criteria.
	Value	Specifies the value for the attributes in the criteria.
<b>Exclude Criteria</b>		
	Criteria Name	Specifies the exclude criteria for the source selector. Pod that matches the exclude criteria will be part of the source for the given traffic policy.

Tab-Source Specifications	Field	Description
	Property	Specifies the property in the exclude criteria based on which the pod associated with the source is tapped.
	Operator	Specifies the operator involved in the exclude criteria in tapping the traffic in the pod.
	Value	Specifies the value in the criteria based on which traffic in the pod is tapped.

**Rules**

You can view the aggregate value of all the rules the policy has been configured for the node in the UCT-C tap present in a cluster. The fields and descriptions of the source specifications tab are described in the following table:

Table 3:

Tab-Rules	Field	Description
<i>Rules</i>		
<b>Rules</b>		
	Name	Specifies the name of the rules in which the traffic is filtered in the pod
	Tunnel Specifications	Specifies the tunnel details which is associated with the rules to send the traffic out. When you hover over the tunnel specification value, you can view the details of the tunnel in a message box
	Priority	Specifies the priority assigned for the rule.
	Pass/Drop	Specifies whether to pass or drop the rule.
	Filters	Specifies the parameters used in the rule. When you hover over the filter value, you can view the details of the filters in a message box.
	Direction	Specifies the direction of the flow of traffic is ingress, egress, or in both direction.
	Ingress Packets	Specifies the aggregate value of the ingress packets associated with the rules.
	Egress Packets	Specifies the aggregate value of the egress packets associated with the rules.
	Ingress Dropped	Specifies the aggregate value of the ingress packets dropped associated with the rules.
	Egress Dropped	Specifies the aggregate value of the egress packets dropped associated with the rules.
	Ingress Errors	Specifies the aggregate value of the ingress errors associated with the rules.



<b>Tab-Rules</b>	<b>Field</b>	<b>Description</b>
<b>Rules</b>		
	Egress Errors	Specifies the aggregate value of the egress errors associated with the rules.
<b>UCT-C</b>		
	Name	Name of the UCT-C associated with the rule.
	Ingress Packets	Specifies the aggregate value of the ingress packets associated with the rules for an UCT-C.
	Egress Packets	Specifies the aggregate value of the egress packets associated with the rules for an UCT-C.
	Ingress Bytes	Specifies the total aggregate value of the ingress bytes associated with the rules for an UCT-C.
	Egress Bytes	Specifies the total aggregate value of the egress bytes associated with the rules for an UCT-C.
	Ingress Dropped	Specifies the aggregate value of the ingress packets dropped associated with the rules for an UCT-C.
	Egress Dropped	Specifies the aggregate value of the egress packets dropped associated with the rules for an UCT-C.
	Ingress Errors	Specifies the aggregate value of the ingress errors associated with the rules for an UCT-C.
	Egress Errors	Specifies the aggregate value of the egress errors associated with the rules for an UCT-C.
<b>Container</b>		
	Pod ID	Specifies the Pod ID associated with the rules .
	Ingress Packets	Specifies the aggregate value of the ingress packets associated with the ruled for a pod in the UCT-C.
	Egress Packets	Specifies the aggregate value of the egress packets associated with the ruled for a pod in the UCT-C.
	Ingress Bytes	Specifies the total aggregate value of the ingress bytes associated with the rules for an UCT-C.
	Egress Bytes	Specifies the total aggregate value of the egress bytes associated with the rules for an UCT-C.
	Ingress Dropped	Specifies the total aggregate value of the ingress bytes dropped associated with the rules for an UCT-C.
	Egress Dropped	Specifies the total aggregate value of the egress bytes dropped associated with the rules for an UCT-C.
	Ingress Errors	Specifies the total aggregate value of the ingress errors associated with the rules for an UCT-C.
	Egress Errors	Specifies the total aggregate value of the egress errors associated with the rules for an UCT-C.

## Container

You can view the aggregate value of the packets for a container, and also the rules associated with a container.

The fields and descriptions of the source specifications tab are described in the following table:

Table 4:

Tab-	Field	Description
<b>Container Box</b>		
<b>UCT-C</b>		
	Name	Specifies the name of the UCT-C associated with the rule.
	Ingress packets	Specifies the aggregate value of the ingress packets associated with the pod in a UCT-C
	Egress packets	Specifies the aggregate value of the egress packets associated with the pod in a UCT-C
	Ingress Bytes	Specifies the aggregate value of the ingress packets associated with the rules for a pod in the UCT-C.
	Egress Bytes	Specifies the aggregate value of the egress packets associated with the rules for a pod in the UCT-C.
	Ingress Dropped	Specifies the aggregate value of the ingress packets dropped associated with the rules for an UCT-C.
	Egress Dropped	Specifies the aggregate value of the egress packets dropped associated with the rules for an UCT-C.
	Ingress Errors	Specifies the aggregate value of the ingress errors associated with the rules for an UCT-C.
	Egress Errors	Specifies the aggregate value of the egress errors associated with the rules for an UCT-C.
<b>Container</b>		
	Pod ID	Specifies the Pod ID associated with the policy. To support pod name, following section should be added under deployment: name: UCT-C_POD_NAME valueFrom: field Ref: field Path: metadata.name
	Ingress packets	Specifies the aggregate value of the ingress packets associated with the rule for a pod in the

Tab-	Field	Description
<b>Container Box</b>		UCT-C.
	Egress packets	Specifies the aggregate value of the egress packets associated with the rule for a pod in the UCT-C.
	Ingress Bytes	Specifies the aggregate value of the ingress bytes associated with the rule for a pod in the UCT-C.
	Egress Bytes	Specifies the aggregate value of the egress bytes associated with the rule for a pod in the UCT-C.
	Ingress Dropped	Specifies the aggregate value of the ingress packets dropped associated with the rules for an UCT-C.
	Egress Dropped	Specifies the aggregate value of the egress packets dropped associated with the rules for an UCT-C.
	Ingress Errors	Specifies the aggregate value of the ingress errors associated with the rules for an UCT-C.
	Egress Errors	Specifies the aggregate value of the egress errors associated with the rules for an UCT-C.
<b>Rules</b>	Name	Specifies the rules associated with the container
	Tunnel Specifications	Specifies the tunnel associated with the rules
	Priority	Specifies the priority assigned for the rule.
	Pass/Drop	Specifies whether to pass or drop the rule.
	Filters	
	Direction	Specifies whether the direction of the flow of traffic is ingress or egress.
	Ingress packets	Specifies the aggregate value of the ingress packets associated with the rules.
	Egress packets	Specifies the aggregate value of the egress packets associated with the rules
	Ingress Bytes	Specifies the aggregate value of the ingress bytes associated with the rules.
	Egress Bytes	Specifies the aggregate value of the egress bytes associated with the rule.
	Ingress Errors	Specifies the aggregate value of the ingress errors associated with the rule.
	Egress Errors	Specifies the aggregate value of the egress errors associated with the rule.
	Ingress dropped	Specifies the aggregate value of the ingress packets dropped associated with the rule.

Tab-	Field	Description
<b>Container Box</b>		
	Egress dropped	Specifies the aggregate value of the egress packets dropped associated with the rules.
	Tunnel Specifications	Specifies the tunnel associated with the rules
	Priority	Specifies the priority assigned for the rule.

## Create Service Token

To create a service token that needs to be entered in the connection creation when GigaVUE-FM is selected as the inventory collector, follow these steps:

1. Create service account for GigaVUE-FM using the following command:
2. Create cluster role with permissions for reading the inventory using the command:

```
kubectl create serviceaccount <fm-serviceaccountname> -n <gigamonnamespace>
```

```
kubectl apply -f <clusterrolefilename>
```

the contents of clusterrolefilename file are as below:

```
kind: ClusterRole
apiVersion: rbac.authorization.k8s.io/v1
metadata: name: resource-list
rules: - apiGroups: [""]
resources: ["pods","services", "nodes"]
verbs: ["get","watch","list"]
- apiGroups: ["apps"]
resources: ["deployments"]
verbs: ["list"]
```

3. Create cluster role binding with the above cluster role and the previously created service account using the following command:

```
kubectl create clusterrolebinding <clusterrolebindingname> --
clusterrole=cluster-admin --
serviceaccount=<gigamonnamespace>:<fm-serviceaccountname>
```

4. Get the token value to use by following the command:

```
kubectl describe serviceaccount <fm-serviceaccountname>
kubectl describe secret <secretname from the above output>
```

# Configure UCT-C Settings

You can configure the following UCT-C settings in GigaVUE-FM:

- [UCT-C General Settings](#)
- [Configure UCT-C Settings](#)

## UCT-C General Settings

In GigaVUE-FM, you can control the number of permitted connections, refresh intervals and purge time intervals of the UCT-C solution. You can specify the purge interval to automatically remove the UCT-Cs that are disconnected for a long duration.

**NOTE:** GigaVUE-FM generates an alarm for the disconnected UCT-C when the UCT-C heartbeats are not received for more than 15 minutes. Refer to "Alarms" topic in the *GigaVUE Administration Guide* for detailed information on Alarms.

To edit the UCT-C general settings:

1. In GigaVUE-FM, navigate to **Inventory > CONTAINER > Universal Cloud Tap - Container > Settings**, the **Settings** page appears with the existing General settings and UCT-C information.
2. On the **Settings** page, on the **General** section, click **Edit**. The Edit General Setting's quick view appears.
3. To exclude the pods from monitoring, provide the source criteria. In **Criteria 1**, from the drop-down list box, select any of the following **Object Property** to exclude them from the monitoring domain, and provide the value for the property selected in the **Value** field:
  - o pod name
  - o pod ip
  - o pod labels

- o node name
4. Edit the required values in the **General Settings** section.

Field	Description
<b>Maximum number of connections allowed</b>	Enter the maximum number of connections allowed in the UCT-C solution
<b>Refresh interval for Container target selection inventory (secs)</b>	Enter a value for the refresh interval for container target selection inventory in seconds
<b>Purge time interval for disconnected UCT-Cs (days)</b>	Enter a value for the purge time interval for the disconnected UCT-Cs in days

5. Click **Save** to save the updates made on the General Settings.

### UCT-C Log Level Settings

In GigaVUE-FM, you can control the level of logs created at each individual UCT-C for troubleshooting. The regular UCT-C log file name format is **uct\_tap.log**.

To view or edit the UCT-C log level settings:

1. In GigaVUE-FM, navigate to **Inventory > CONTAINER > Universal Cloud Tap - Container > Settings**, the **Settings** page appears with the existing General settings and UCT-C information.
2. On the **Settings** page, on the **UCT-C** section, on any monitoring domain, click on the UCT-C fabric. The UCT-C setting's quick view appears.

The screenshot shows a configuration window titled "UCT: [redacted]". At the top right are "Cancel" and "Save" buttons. Below the title bar is a section for "Individual Settings". A blue information box states: "Individual setting will apply to this UCT only. When applying settings to a group try to consider the performance impact." Under the "LOGGING" section, there are two settings: "Log Level" is set to "DEBUG" with a dropdown arrow and a "Reset" button; "Log File Size" is set to "1000000" with a "Reset" button.

3. Edit the required UCT-C log values in the **LOGGING** section.

Field	Description
<b>Log Level</b>	<p>Select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>DEBUG</b>—fine-grained log information for application debugging</li> <li>• <b>INFO</b>—coarse-grained log information for highlighting application progress</li> <li>• <b>WARN</b>—log information of potentially harmful situations</li> <li>• <b>ERROR</b>—log information of the error events that allows the application to run continuously</li> <li>• <b>FATAL</b>—log information of very severe error events that presumably lead the application to abort.</li> </ul>
<b>Log File Size</b>	Enter a value for the number of lines in the UCT-C log file.

On any of the above fields, click **Reset** to reset the value to default.

# Preryption™

**License:** Requires **SecureVUE Plus** license.

Gigamon Precryption™ technology<sup>1</sup> redefines security for virtual, cloud, and containerized applications, delivering plaintext visibility of encrypted communications to the full security stack, without the traditional cost and complexity of decryption.

This section explains about:

- [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 native Linux functionality to tap, or copy, communications between the application and the encryption library, such as OpenSSL.



In this way, Precryption captures network traffic in plaintext, either before it has been encrypted, or after it has been decrypted. Precryption functionality doesn't interfere with the actual encryption of the message nor its transmission across the network. There's no proxy, no retransmissions, no break-and-inspect. Instead, this plaintext copy is forwarded to the Gigamon Deep Observability Pipeline for further optimization, transformation, replication, and delivery to tools.

---

<sup>1</sup>**Disclaimer:** The Precryption feature allows users to acquire traffic after it has been decrypted. This traffic can be acquired from both virtual machine (VM) and container-based solutions, and is then sent to the V Series product for further processing. The Precryption feature provides an option to use encrypted tunnels for communication between the acquisition (via UCT or G-vTAP) of unencrypted traffic and the traffic processing (at the V Series) which will better safeguard the traffic while in transit. However, if a user does not use the option for encrypted tunnels for communication, decrypted traffic will remain unencrypted while in transit between the point of acquisition and processing.

Please note that this information is subject to change, and we encourage you to stay updated on any modifications or improvements made to this feature.

By using this feature, you acknowledge and accept the current limitations and potential risks associated with the transmission of decrypted traffic.



Precryption technology is built on GigaVUE® Universal Cloud Tap (UCT) and works across hybrid and multi-cloud environments, including on-prem and virtual platforms. As a bonus, UCT with Precryption technology runs independent of the application, and doesn't have to be baked into the application 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, providing East-West visibility into virtual, cloud, and container platforms. It delivers unobscured visibility into all encryption types including TLS 1.3, without managing and maintaining decryption keys. IT organizations can now manage compliance, keep private communications private, architect the necessary foundation for Zero Trust, and boost security tool effectiveness by a factor of 5x or more.

## Key Features

The following are the key features of this technology:

- Plaintext visibility into communications with modern encryption (TLS 1.3, mTLS, and TLS 1.2 with Perfect Forward Secrecy).
- Plaintext visibility into communications with legacy encryption (TLS 1.2 and earlier).
- Nonintrusive 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:

- Eliminate blind spots for encrypted East-West (lateral) and North-South communications, including traffic that may not cross firewalls.
- Monitor application communications with an independent approach that enhances development team velocity.
- Extend security tools' visibility to all communications, regardless of encryption type.

- Achieve maximum traffic tapping efficiency across virtual environments.
- Leverage a 5–7x performance boost for security tools by consuming unencrypted data.
- Support a Zero Trust architecture founded on deep observability.
- Maintain privacy and compliance adherence associated with decrypted traffic management.

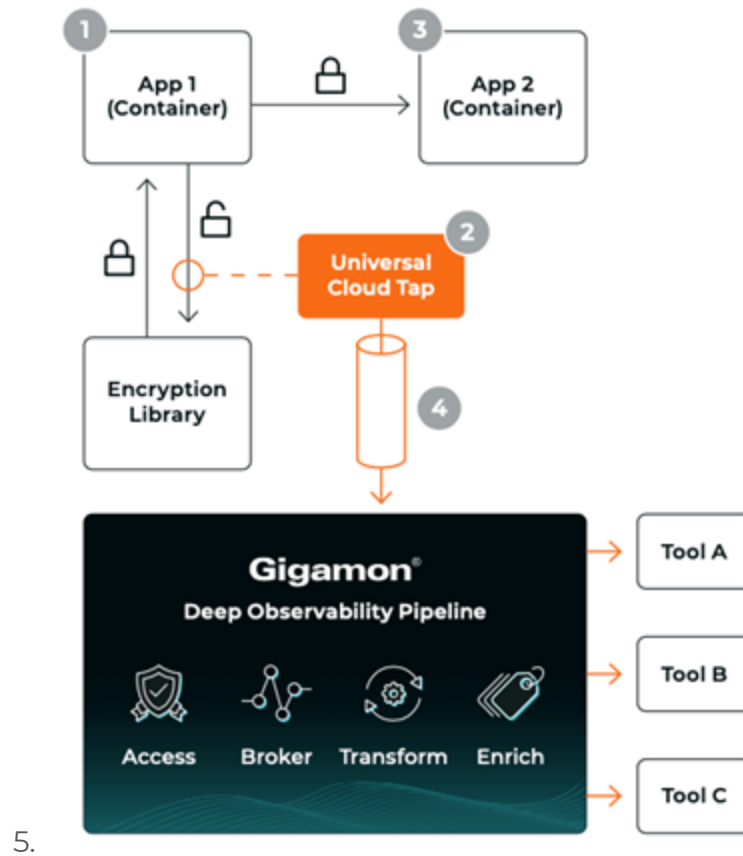
## How Gigamon Precryption Technology Works

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

- [Precryption Technology on Single Node](#)
- [Precryption Technology on Multi-Node](#)

### Precryption Technology on Single Node

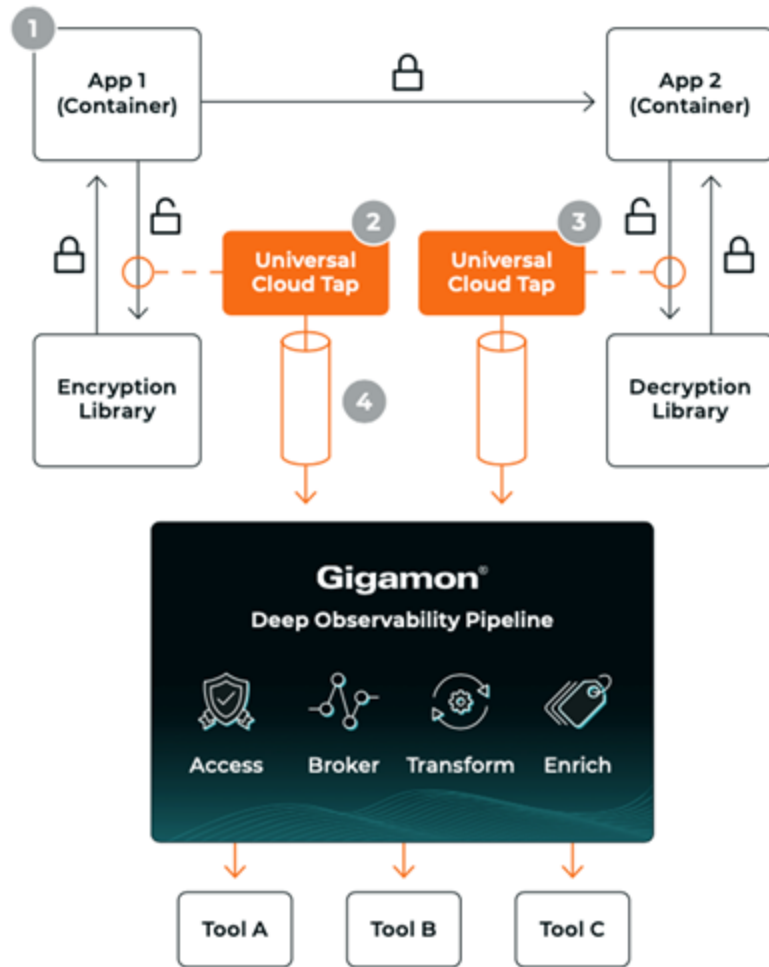
1. When any application needs to encrypt a message, it uses an encryption library, such as OpenSSL, to perform the actual encryption.
2. GigaVUE Universal Cloud Tap (UCT), enabled with Precryption technology, gets a copy of this message before it's encrypted on the network.
3. The encrypted message is sent to the receiving application, with unmodified encryption. No proxy, no re- encryption, no retransmissions.
4. GigaVUE UCT creates packet headers as needed, encapsulates in a tunnel, and forwards to GigaVUE V Series in the deep observability pipeline. Gigamon further optimizes, transforms, and delivers data to tools, without need for further decryption



5.

## Pre-encryption Technology on Multi-Node

1. When any application needs to encrypt a message, it uses an encryption library, such as OpenSSL, to perform the actual encryption.
2. GigaVUE Universal Cloud Tap (UCT), enabled with Pre-encryption, gets a copy of this message before it's encrypted on the network.
3. Optionally, GigaVUE UCT enabled with Pre-encryption can also acquire a copy of the message from the server end, after the decryption.
4. GigaVUE UCT creates packet headers as needed, encapsulates in a tunnel, and forwards to V Series in the deep observability pipeline where it is further enriched, transformed, and delivered to tools, without further decryption.



5.

## Supported Platforms

**VM environments:** Precryption™ is supported on the following VM platforms where UCT-V is supported:

Platform Type	Platform
<b>Public Cloud</b>	<ul style="list-style-type: none"> <li>● AWS</li> <li>● Azure</li> <li>● GCP (via Third Party Orchestration)</li> </ul>
<b>Private Cloud</b>	<ul style="list-style-type: none"> <li>● OpenStack</li> <li>● VMware ESXi (via Third Party Orchestration only)</li> <li>● VMware NSX-T (via Third Party Orchestration only)</li> </ul>

**Container environments:** Precryption™ is supported on the following container platforms where UCT-C is supported:

Platform Type	Platform
Public Cloud	<ul style="list-style-type: none"> <li>● EKS</li> <li>● AKS</li> </ul>
Private Cloud	<ul style="list-style-type: none"> <li>● OpenShift</li> <li>● Native Kubernetes (VMware)</li> </ul>

## Prerequisites

### Deployment Prerequisites

- Linux Kernel version 5.4 and above
- OpenSSL version 1.0.2, version 1.1.0, version 1.1.1, and version 3.x
- Protocol version IPv4
- For GigaVUE-FM, to capture the statistics, you must add the port 5671 in the security group
- Port 9900 should be enabled in security group settings on the UCT-V controller to receive the statistics information from UCT-V agent
- For UCT-C, you must add the port 42042 and port 5671 in the security group

### License Prerequisite

- Precryption™ requires SecureVUE Plus license.

### Note

- See the [Configure Precryption in UCT-V](#) section for details on how to enable Precryption™ in VM environments.
- See the [Configure in UCT-C](#) section for details on how to enable Precryption™ in container environments.
- See how [Secure Tunnels](#) feature can enable secure delivery of precrypted data.

## Configure in UCT-C

GigaVUE-FM allows you to enable or disable the precryption feature.

To configure the precryption feature in UCT-C, follow these steps:

1. Go to **Traffic > CONTAINER > Universal Cloud Tap - Container**. The Policies page appears.
2. In the Policies page, click **Create**.
3. In the **General** tab, enter or select the required information as described in the following table:

Fields	Description
Policy Name	Enter a name for the Traffic Policy. The name must be unique.
Monitoring Domain	Select an existing monitoring domain.  To create a new monitoring domain, refer to Create Monitoring Domain section in the UCT configuration guide.  Only one Precryption Policy is allowed per Monitoring Domain
Connections	Select one or more connections for the policy. Once traffic policy is created for monitoring domain, you cannot add or delete connections in a monitoring domain.
Precryption Policy	Click the radio button <b>Yes</b> , to enable the <b>Precryption Policy</b> ,

After enabling the Precryption, configure the **Source Selectors**, and the **Rules**. In this release, for Rules, Pass All option is supported.

### Rules and Notes

The following are the memory limits to be applied to the UCT-TAP in case of UCT-C.:

- The memory limit changes depending on the numbers of VCPUs in the worker node. For example, if the worker node has 16 VCPUs, then the precryption feature consumes around 1GB of memory ((16 \* 64 MB).
- When you deploy secure tunnels, it requires additional (16 \*64 MB) memory. Hence, a total memory that you must allocate for the TAP is 1 GB.

The YAML configuration option allows you to choose the amount of buffer size.

## Secure Tunnels

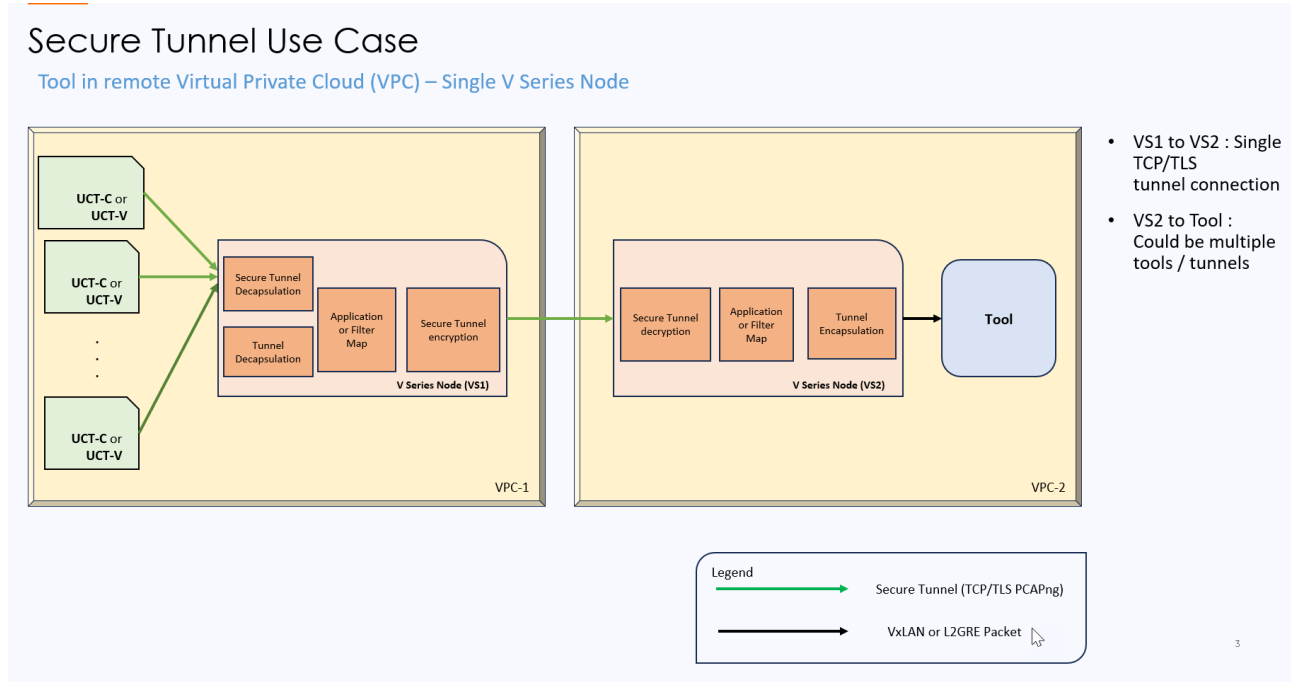
Secure Tunnel securely transfers the cloud captured packets on UCT-V and UCT-C to a GigaVUE V Series Node or Tool (only in case of UCT-C). The data from UCT-V and UCT-C are encapsulated in PCAPng format, and the encrypted data is sent over a TLS connection to a GigaVUE V Series Node.

Secure Tunnel can also transfer the cloud captured packets from a GigaVUE V Series Node to another GigaVUE V Series Node.

In case of GigaVUE V Series Node to GigaVUE V Series node, the traffic from the GigaVUE V Series Node 1 is encapped using PCAPNG format and transported to GigaVUE V Series Node 2 where the traffic is decapped. The secure tunnels between V Series Node to V Series Node have multiple uses cases.

The GigaVUE V Series Node decapsulates and processes the packet per the configuration. The decapsulated packet can be sent to the application such as De-duplication, Application Intelligence, Load balancer and to the tool. The Load Balancer on this node can send the packets to multiple V series Nodes, in this case the packets can be encapsulated again and sent over a secure tunnel.

For more information about PCAPng, refer to [PCAPng Application](#).



## Supported Platforms

Secure tunnel is 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)

For information about how to configure secure tunnels, refer to the section [Configure Secure Tunnel](#).

## Configure Secure Tunnel

Secure tunnel can be configured on:

- [Precrypted Traffic](#)
- [Mirrored Traffic](#)

## Precrypted Traffic

You can send the precrypted traffic through secure tunnel. When secure tunnel for precryption is enabled, packets are framed and sent to the TLS socket. PCAPng format is used to send the packet.

When you enable the secure tunnel option for both regular and precryption packets, then two TLS secure tunnel sessions are created.

It is recommended to always enable secure tunnels for precrypted traffic to securely transfer the 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 Container to GigaVUE V Series Node](#)
- [Configure Secure Tunnel from GigaVUE Cloud Suite V Series Node 1 to GigaVUE Cloud Suite V Series Node 2](#)

## Prerequisites

While creating Secure Tunnel, you must provide the following details:

- SSH key pair
- CA certificate

## Configure Secure Tunnel from UCT Container to GigaVUE V Series Node

To configure a secure tunnel in a UCT Container, you must configure one end of the tunnel to the UCT and the other end to a GigaVUE Cloud Suite V Series node. You must configure CA certificates in UCT Container, and the private keys and SSL certificates in the GigaVUE Cloud Suite V Series node. Refer to the following steps for configuration:



S. No	Task	Refer to						
1	Upload a Custom Certificate	<p>You must upload a CA to UCT Container for establishing a connection with the GigaVUE Cloud Suite V Series node.</p> <p>To upload the CA using GigaVUE-FM follow the steps given below:</p> <ol style="list-style-type: none"> <li>Go to <b>Inventory &gt; Resources &gt; Security &gt; CA List</b>.</li> <li>Click <b>New</b>, to add a new Certificate Authority. The <b>Add Certificate Authority</b> page appears.</li> <li>Enter or select the following information. <table border="1" data-bbox="737 554 1446 749"> <thead> <tr> <th>Field</th> <th>Action</th> </tr> </thead> <tbody> <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> </tbody> </table> </li> <li>Click <b>Save</b>.</li> </ol> <p>For more information, refer to the section <a href="#">Adding Certificate Authority</a>.</p>	Field	Action	Alias	Alias name of the CA.	File Upload	Choose the certificate from the desired location.
Field	Action							
Alias	Alias name of the CA.							
File Upload	Choose the certificate from the desired location.							
2.	Upload a SSL Key	You must add a SSL key to GigaVUE Cloud Suite V Series node. To add SSL Key, follow the steps in the section <a href="#">SSL Decrypt..</a>						
3	Selecting the SSL Key when you create a monitoring domain and configure the fabric components in GigaVUE-FM.	To select the SSL Key follow the steps in the section						
4	Selecting the CA certificate when you create a monitoring domain and configuring the fabric components in GigaVUE-FM.	You should select the added Certificate Authority (CA) in UCT-V Controller. To select the CA certificate, follow the steps in the section <a href="#">UCT-C and GigaVUE-FM Interaction</a>						
5.	Creating and adding the secure tunnel when you configure the traffic policy.	To create and add the secure tunnel while configuring in , in UCT Container refer to the <a href="#">Configure Traffic Policy</a>						

## Configure Secure Tunnel from GigaVUE Cloud Suite V Series Node 1 to GigaVUE Cloud Suite V Series Node 2

You can create secure tunnel in the following ways:

- Between GigaVUE Cloud Suite V Series Node 1 to GigaVUE Cloud Suite V Series Node 2
- From GigaVUE Cloud Suite V Series Node 1 to multiple GigaVUE Cloud Suite V Series nodes.

You must have the following details before you start the configuration of secure tunnel from GigaVUE Cloud Suite V Series Node 1 to GigaVUE Cloud Suite V Series Node 2:

- IP address of the tunnel destination endpoint (GigaVUE Cloud Suite V Series Node 2).
- SSH key pair (pem file).

To configure secure tunnel from GigaVUE Cloud Suite V Series Node 1 to GigaVUE Cloud Suite V Series Node 2, refer to the following steps:

S · N O	Task	Refer to						
1.	Upload a Custom Authority (CA) Certificate	<p>You must upload a Custom Certificate to UCT-V Controller for establishing a connection between the GigaVUE Cloud Suite V Series node.</p> <p>To upload the CA using GigaVUE-FM follow the steps given below:</p> <ol style="list-style-type: none"> <li>1. Go to <b>Inventory &gt; Resources &gt; Security &gt; CA List</b>.</li> <li>2. Click <b>New</b>, to add a new Custom Authority. The <b>Add Custom Authority</b> page appears.</li> <li>3. Enter or select the following information.</li> </ol> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: center;">Field</th> <th style="text-align: center;">Action</th> </tr> </thead> <tbody> <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> </tbody> </table> <ol style="list-style-type: none"> <li>4. Click <b>Save</b>.</li> <li>5. Click <b>Deploy All</b>.</li> </ol> <p>For more information, refer to the section <a href="#">Adding Certificate Authority</a>.</p>	Field	Action	Alias	Alias name of the CA.	File Upload	Choose the certificate from the desired location.
Field	Action							
Alias	Alias name of the CA.							
File Upload	Choose the certificate from the desired location.							
2.	Uploading a SSL Key	<p>You must add a SSL key to GigaVUE Cloud Suite V Series node. To add SSL Key, follow the steps in the section <a href="#">Upload SSL Keys</a>.</p>						
3	Creating a secure tunnel between UCT-V and GigaVUE Cloud Suite	<p>You should enable the secure tunnel feature to establish a connection between the UCT-V and GigaVUE Cloud Suite V Series node 1. To enable the secure tunnel feature follow these steps:</p> <ol style="list-style-type: none"> <li>1. In the Edit Monitoring Session page, click <b>Options</b>. The <b>Apply template</b> page appears.</li> <li>2. Enable the <b>Secure Tunnel</b> button. You can enable secure tunnel for both mirrored and preencrypted traffic.</li> </ol>						

S · N O	Task	Refer to
	V Series Node 1.	
4.	Selecting the added SSL Key while creating a monitoring domain and configuring the fabric components in GigaVUE-FM in GigaVUE Cloud Suite V Series Node 1	You must select the added SSL Key in GigaVUE Cloud Suite V Series Node 1. To select the SSL key, follow the steps in the section <a href="#">Configure GigaVUE Fabric Components in GigaVUE-FM</a> .
5.	Selecting the added CA certificate while creating the monitoring domain	<p>You should select the added Certificate Authority (CA) in UCT-V Controller. To select the CA certificate, follow the steps in the section <a href="#">Configure GigaVUE Fabric Components in GigaVUE-FM</a>.</p> <p>You can also push the CA manually by editing CA in Monitoring Domain page. To edit CA, go to <b>Monitoring Domain &gt; Actions &gt; Edit CA</b>.</p>

S · N O	Task	Refer to														
6	Creating an Egress tunnel from GigaVUE Cloud Suite V Series Node 1 with tunnel type as TLS-PCAPNG while creating the monitoring session.	<p>You must create a tunnel for traffic to flow out from GigaVUE Cloud Suite V Series Node 1 with tunnel type as TLS-PCAPNG while creating the monitoring session. Refer to <a href="#">Create a Monitoring Session</a> to know about monitoring session.</p> <p>To create the egress tunnel, follow these steps:</p> <ol style="list-style-type: none"> <li>1. After creating a new monitoring session, or click <b>Actions &gt; Edit</b> on an existing monitoring session, the GigaVUE-FM canvas appears.</li> <li>2. In the canvas, select <b>New &gt; New Tunnel</b>, drag and drop a new tunnel template to the workspace. The <b>Add Tunnel Spec</b> quick view appears.</li> <li>3. On the New Tunnel quick view, enter or select the required information as described in the following table:</li> </ol> <table border="1" data-bbox="341 798 1442 1816"> <thead> <tr> <th data-bbox="341 798 535 877">Field</th> <th data-bbox="535 798 1442 877">Action</th> </tr> </thead> <tbody> <tr> <td data-bbox="341 877 535 919">Alias</td> <td data-bbox="535 877 1442 919">The name of the tunnel endpoint.</td> </tr> <tr> <td data-bbox="341 919 535 961">Description</td> <td data-bbox="535 919 1442 961">The description of the tunnel endpoint.</td> </tr> <tr> <td data-bbox="341 961 535 1003">Type</td> <td data-bbox="535 961 1442 1003">Select TLS-PCAPNG for creating egress secure tunnel</td> </tr> <tr> <td data-bbox="341 1003 535 1696">Traffic Direction</td> <td data-bbox="535 1003 1442 1696">                     Choose <b>Out</b> (Encapsulation) for creating an egress tunnel from the V Series node to the destination. Select or enter the following values:                     <ul style="list-style-type: none"> <li>o MTU- The default value is 1500.</li> <li>o 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.</li> <li>o DSCP - Enter the Differentiated Services Code Point (DSCP) value.</li> <li>o Flow Label - Enter the Flow Label value.</li> <li>o Source L4 Port- Enter the Souce L4 Port value</li> <li>o Destination L4 Port - Enter the Destination L4 Port value.</li> <li>o Flow Label</li> <li>o Cipher- Only SHA 256 is supported.</li> <li>o TLS Version - Select TLS Version1.3.</li> <li>o Selective Acknowledgments - Choose Enable to receive the acknowledgments.</li> <li>o Sync Retries - Enter the value for number of times the sync has to be tried. The value ranges from 1 to 6.</li> <li>o Delay Acknowledgments - Choose Enable to receive the acknowledgments when there is a delay.</li> </ul> </td> </tr> <tr> <td data-bbox="341 1696 535 1738">IP Version</td> <td data-bbox="535 1696 1442 1738">The version of the Internet Protocol. Only IPv4 is supported.</td> </tr> <tr> <td data-bbox="341 1738 535 1816">Remote Tunnel IP</td> <td data-bbox="535 1738 1442 1816">Enter the interface IP address of the GigaVUE Cloud Suite V Series Node 2 (Destination IP).</td> </tr> </tbody> </table> <ol style="list-style-type: none"> <li>4. Click <b>Save</b>.</li> </ol>	Field	Action	Alias	The name of the tunnel endpoint.	Description	The description of the tunnel endpoint.	Type	Select TLS-PCAPNG for creating egress secure tunnel	Traffic Direction	Choose <b>Out</b> (Encapsulation) for creating an egress tunnel from the V Series node to the destination. Select or enter the following values: <ul style="list-style-type: none"> <li>o MTU- The default value is 1500.</li> <li>o 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.</li> <li>o DSCP - Enter the Differentiated Services Code Point (DSCP) value.</li> <li>o Flow Label - Enter the Flow Label value.</li> <li>o Source L4 Port- Enter the Souce L4 Port value</li> <li>o Destination L4 Port - Enter the Destination L4 Port value.</li> <li>o Flow Label</li> <li>o Cipher- Only SHA 256 is supported.</li> <li>o TLS Version - Select TLS Version1.3.</li> <li>o Selective Acknowledgments - Choose Enable to receive the acknowledgments.</li> <li>o Sync Retries - Enter the value for number of times the sync has to be tried. The value ranges from 1 to 6.</li> <li>o Delay Acknowledgments - Choose Enable to receive the acknowledgments when there is a delay.</li> </ul>	IP Version	The version of the Internet Protocol. Only IPv4 is supported.	Remote Tunnel IP	Enter the interface IP address of the GigaVUE Cloud Suite V Series Node 2 (Destination IP).
Field	Action															
Alias	The name of the tunnel endpoint.															
Description	The description of the tunnel endpoint.															
Type	Select TLS-PCAPNG for creating egress secure tunnel															
Traffic Direction	Choose <b>Out</b> (Encapsulation) for creating an egress tunnel from the V Series node to the destination. Select or enter the following values: <ul style="list-style-type: none"> <li>o MTU- The default value is 1500.</li> <li>o 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.</li> <li>o DSCP - Enter the Differentiated Services Code Point (DSCP) value.</li> <li>o Flow Label - Enter the Flow Label value.</li> <li>o Source L4 Port- Enter the Souce L4 Port value</li> <li>o Destination L4 Port - Enter the Destination L4 Port value.</li> <li>o Flow Label</li> <li>o Cipher- Only SHA 256 is supported.</li> <li>o TLS Version - Select TLS Version1.3.</li> <li>o Selective Acknowledgments - Choose Enable to receive the acknowledgments.</li> <li>o Sync Retries - Enter the value for number of times the sync has to be tried. The value ranges from 1 to 6.</li> <li>o Delay Acknowledgments - Choose Enable to receive the acknowledgments when there is a delay.</li> </ul>															
IP Version	The version of the Internet Protocol. Only IPv4 is supported.															
Remote Tunnel IP	Enter the interface IP address of the GigaVUE Cloud Suite V Series Node 2 (Destination IP).															

S · N O	Task	Refer to
7.	Selecting the added SSL Key while creating a monitoring domain and configuring the fabric components in GigaVUE-FM in GigaVUE Cloud Suite V Series Node 2	You must select the added SSL Key in GigaVUE Cloud Suite V Series Node 2. To select the SSL key, follow the steps in the section <a href="#">Configure GigaVUE Fabric Components in GigaVUE-FM</a> .
8	Create an ingress tunnel in the GigaVUE V Series node 2 with tunnel type as TLS-PCAP	<p>You must create a tunnel for traffic to flow out from GigaVUE Cloud Suite V Series Node 2 with tunnel type as TLS-PCAPNG while creating the monitoring session. Refer to <a href="#">Create a Monitoring Session</a> to know about monitoring session.</p> <p>To create the ingress tunnel, follow these steps:</p> <ol style="list-style-type: none"> <li><b>1.</b> After creating a new monitoring session, or click <b>Actions &gt; Edit</b> on an existing monitoring session, the GigaVUE-FM canvas appears.</li> <li><b>2.</b> In the canvas, select <b>New &gt; New Tunnel</b>, drag and drop a new tunnel template to the workspace. The <b>Add Tunnel Spec</b> quick view appears.</li> <li><b>3.</b> On the New Tunnel quick view, enter or select the required information as described in the following table:</li> </ol>

S · N O	Task	Refer to	
		Field	Action
	NG while creating the monitoring session for GigaVUE V Series node 2.	Alias	The name of the tunnel endpoint.
		Description	The description of the tunnel endpoint.
		Type	Select TLS-PCAPNG for creating egress secure tunnel
		Traffic Direction	Choose <b>in</b> (Encapsulation) for creating an egress tunnel from the V Series node to the destination. Select or enter the values as described in Step 6:
		IP Version	The version of the Internet Protocol. Only IPv4 is supported.
		Remote Tunnel IP	Enter the interface IP address of the GigaVUE Cloud Suite V Series Node 1 (Destination IP).
		4. Click <b>Save</b> .	

# Upgrade UCT-C

To upgrade UCT-C, you must perform the following steps:

1. **Upgrade to GigaVUE-FM 6.4.00:** Before upgrading GigaVUE-FM from 6.3.00 or earlier versions with UCT\_C deployed, delete the container tapping solution, and then upgrade GigaVUE-FM to 6.4.00. To upgrade the GigaVUE-FM in respective cloud platforms, refer to [GigaVUE-FM Installation and Upgrade guide](#).
2. **Upgrade to UCT-C 6.4.00:** To upgrade UCT-C to 6.4.00, you must delete the older versions and deploy UCT-C 6.4.00 version. To deploy UCT-C, refer to [Steps to Delete and Redeploy UCT-C](#).

GigaVUE-FM 6.4.00 is compatible only with UCT-C 6.4.00.

## Steps to Delete and Redeploy UCT-C

1. Delete the UCT Controller deployment.
 

```
kubectl get deployment -A
kubectl delete deployment <uct-controller name> -n <namespace>
```
2. Delete the UCT Tap daemonset.
 

```
kubectl get daemonset -A
kubectl delete daemonset <uct-tap-name> -n <namespace>
```

3. Delete the UCT controller service.

```
kubectl get services -A
kubectl delete services <uct-cntlr-service-name> -n <namespace>
```

4. Deploy the UCT controller/UCT Tap using helm chart or YAML file.

- a. To install using Helm chart:

```
helm install uctc-cntlr uctc-cntlr/
helm install uctc-tap uctc-tap/
```

- b. To install using YAML.

```
kubectl apply -f <uctc_controller_yaml_file>
kubectl apply -f <uctc_tap_yaml_file>
```

5. Delete the ingress rule and redeploy it using YAML to point to the right service (uctc-cntlr-service).

```
kubectl get ingress -A
kubectl delete ingress <uct-cntlr-ingress-name> -n <namespace>
uctc-ingress.yaml
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  annotations:
    kubernetes.io/ingress.class: nginx-uct-ns
    nginx.ingress.kubernetes.io/backend-protocol: HTTPS
    nginx.ingress.kubernetes.io/proxy-connect-timeout: "360000"
    nginx.ingress.kubernetes.io/proxy-read-timeout: "360000"
    nginx.ingress.kubernetes.io/proxy-send-timeout: "360000"
    nginx.ingress.kubernetes.io/rewrite-target: /
    nginx.ingress.kubernetes.io/secure-backends: "false"
    nginx.ingress.kubernetes.io/ssl-passthrough: "true"
  generation: 1
  name: uctc-cntlr-ingress
  namespace: uct-ns
spec:
  rules:
    - http:
        paths:
          - backend:
              service:
                name: uctc-cntlr-service
                port:
                  number: 8443
            path: /
            pathType: ImplementationSpecific
  status:
    loadBalancer: {}
    kubectl apply -f <ingress_rule_yaml_file>
```

6. Restart the nginx controller and backend.

```
kubectl get pods -A
kubectl rollout restart deployment nginx-controller -n <namespace>
kubectl rollout restart deployment nginx-ingress-default-backend -n
<namespace>
```

7. Redeploy the policy.



# 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 6.4 Hardware and Software Guides
<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.
<b>Hardware</b> how to unpack, assemble, rack-mount, connect, and initially configure ports the respective GigaVUE Cloud Suite devices; reference information and specifications for the respective GigaVUE Cloud Suite devices
<b>GigaVUE-HC1 Hardware Installation Guide</b>
<b>GigaVUE-HC2 Hardware Installation Guide</b>
<b>GigaVUE-HC3 Hardware Installation Guide</b>
<b>GigaVUE-HC1-Plus Hardware Installation Guide</b>
<b>GigaVUE-TA25 Hardware Installation Guide</b>
<b>GigaVUE-TA25E Hardware Installation Guide</b>

<b>GigaVUE Cloud Suite 6.4 Hardware and Software Guides</b>	
<b>GigaVUE-TA100 Hardware Installation Guide</b>	
<b>GigaVUE-TA200 Hardware Installation Guide</b>	
<b>GigaVUE-TA200E Hardware Installation Guide</b>	
<b>GigaVUE-TA400 Hardware Installation Guide</b>	
<b>GigaVUE-OS Installation Guide for DELL S4112F-ON</b>	
<b>G-TAP A Series 2 Installation Guide</b>	
<b>GigaVUE M Series Hardware Installation Guide</b>	
<b>GigaVUE-FM Hardware Appliance Guide for GFM-HW1-FM010 and and GFM-HW1-FM001-HW</b>	
<b>Software Installation and Upgrade Guides</b>	
<b>GigaVUE-FM Installation, Migration, and Upgrade Guide</b>	
<b>GigaVUE-OS Upgrade Guide</b>	
<b>GigaVUE V Series Migration Guide</b>	
<b>Fabric Management and Administration Guides</b>	
<b>GigaVUE Administration Guide</b>	covers both GigaVUE-OS and GigaVUE-FM
<b>GigaVUE Fabric Management Guide</b>	how to install, deploy, and operate GigaVUE-FM; how to configure GigaSMART operations; covers both GigaVUE-FM and GigaVUE-OS features
<b>Cloud Guides</b>	
how to configure the GigaVUE Cloud Suite components and set up traffic monitoring sessions for the cloud platforms	
<b>GigaVUE V Series Applications Guide</b>	
<b>GigaVUE V Series Quick Start Guide</b>	
<b>GigaVUE Cloud Suite Deployment Guide - AWS</b>	
<b>GigaVUE Cloud Suite Deployment Guide - Azure</b>	
<b>GigaVUE Cloud Suite Deployment Guide - OpenStack</b>	
<b>GigaVUE Cloud Suite Deployment Guide - Nutanix</b>	
<b>GigaVUE Cloud Suite Deployment Guide - VMware</b>	
<b>GigaVUE Cloud Suite Deployment Guide - Third Party Orchestration</b>	
<b>GigaVUE Cloud Suite Deployment Guide Universal Cloud Tap - Container</b>	

<b>GigaVUE Cloud Suite 6.4 Hardware and Software Guides</b>	
<b>Gigamon Containerized Broker Deployment Guide</b>	
<b>GigaVUE Cloud Suite for Nutanix Guide—GigaVUE-VM Guide</b>	
GigaVUE Cloud Suite Deployment Guide - AWS Secret Regions	
<b>Reference Guides</b>	
<b>GigaVUE-OS CLI Reference Guide</b>	
library of GigaVUE-OS CLI (Command Line Interface) commands used to configure and operate GigaVUE HC Series and TA Series devices	
<b>GigaVUE-OS Security Hardening Guide</b>	
<b>GigaVUE Firewall and Security Guide</b>	
<b>GigaVUE Licensing Guide</b>	
<b>GigaVUE-OS Cabling Quick Reference Guide</b>	
guidelines for the different types of cables used to connect Gigamon devices	
<b>GigaVUE-OS Compatibility and Interoperability Matrix</b>	
compatibility information and interoperability requirements for Gigamon devices	
<b>GigaVUE-FM REST API Reference in GigaVUE-FM User's Guide</b>	
samples uses of the GigaVUE-FM Application Program Interfaces (APIs)	
<b>Release Notes</b>	
<b>GigaVUE-OS, GigaVUE-FM, GigaVUE-VM, G-TAP A Series, and GigaVUE Cloud Suite Release Notes</b>	
new features, resolved issues, and known issues in this release ; important notes regarding installing and upgrading to this release	
<b>NOTE:</b> Release Notes are not included in the online documentation.	
<b>NOTE:</b> Registered Customers can log in to <a href="#">My Gigamon</a> to download the Software and Release Notes from the Software & Docs page on to <a href="#">My Gigamon</a> . Refer to <a href="#">How to Download Software and Release Notes from My Gigamon</a> .	
<b>In-Product Help</b>	
<b>GigaVUE-FM Online Help</b>	
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		
<b>About You</b>	<b>Your Name</b>	
	<b>Your Role</b>	
	<b>Your Company</b>	
<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 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)