GigaVUE Cloud Suite for AWS QuickStart Guide

GigaVUE Cloud Suite

Product Version: 5.10

Document Version: 2.0

(See Change Notes for document updates.)

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
5.10.01	2.0	08/28/2020	Fixed formatting and cross-references issues, and streamlined instructions throughout the guide.
5.10.00	1.0	08/14/2020	Original release of this document with 5.10.00 GA.

Contents

GigaVUE Cloud Suite for AWS

GigaVUE® Fabric Manager (GigaVUE-FM) is a web-based fabric management interface that provides a single pane of glass visibility and management of both the physical and virtual traffic that form the GigaVUE Cloud Suite Cloud.GigaVUE-FM integrates with the Amazon Elastic Cloud Compute (EC2) APIs and deploys the components of the GigaVUE Cloud Suite for AWS in the Virtual Private Cloud (VPC).

The GigaVUE Cloud Suite for AWS consists of the following components:

- GigaVUE-FM
- GigaVUE V Series node
- GigaVUE V Series controller
- GigaVUE Cloud Suite G-vTAP controller

GigaVUE-FM is launched by subscribing to the GigaVUE Cloud Suite for AWS in the AWS Marketplace. Once the GigaVUE Cloud Suite for AWS instance is launched, the rest of the Amazon Machine Images (AMIs) residing in the AWS Marketplace are automatically launched from GigaVUE-FM based on the specifications in the GigaVUE-FM interface.

GigaVUE Cloud Suite is available in both the public AWS cloud and in AWS GovCloud, and supports the Bring Your Own License (BYOL) model and the hourly Pay-As-You-Go (PAYG) model that you can avail from the AWS Marketplace.

This guide describes how to deploy the GigaVUE Cloud Suite on the Amazon Web Services (AWS) cloud. For information about installing GigaVUE-FM in your enterprise data center, refer to the "Installation and Upgrade" section in the *GigaVUE-FM User's Guide* available in the Gigamon Customer Portal.

Permissions

Before you begin configuring the components, you must enable the following permissions and attach the policies to an IAM role. You must then attach this IAM role to the GigaVUE-FM instance running in AWS:

- Full EC2 Instance access
- Read-only permission for IAM role
- EC2 pass role permission
- GigaVUE-FM Instance Role Policy
- STS AssumeRole Policy

For creating an IAM role, refer to AWS identity and Access Management (IAM) service. For more information on access control of EC2 instances in AWS, refer to the AWS documentation on Controlling Access to Amazon EC2 Resources.

> **NOTE:** For VPC Traffic Mirroring, **"ec2:*TrafficMirror*"** is an additional set of permission required for the IAM role.

An example of the above permissions is to associate the following policies to your IAM role before launching the GigaVUE-FM instance (you can attach this IAM at any time the instance exists):

```
---EC2 Permissions
"ec2:Describe*",
"ec2:RebootInstances",
"ec2:RunInstances",
"ec2:StartInstances",
"ec2:StopInstances",
"ec2:TerminateInstances",
"ec2:ReportInstanceStatus",
"ec2:Disassociate*",
"ec2:CreateTags",
"ec2:AttachVolume",
"ec2:AttachNetworkInterface",
"ec2:Associate*",
"ec2:Allocate*",
"ec2:DeleteTags",
"ec2:DeleteVolume",
"ec2:DeleteNetworkInterface",
"ec2:ModifyInstanceAttribute",
"ec2:ModifyNetworkInterfaceAttribute",
"ec2:ModifyVolumeAttribute",
"ec2:ReleaseAddress",
"elasticloadbalancing:Describe*",
"autoscaling:Describe*"
```

If you choose Amazon CloudWatch integration in GigaVUE-FM, you may also associate the following optional policies to your IAM role:

```
"cloudwatch:*",
              "logs:*",

"sqs:*", "events:*"
---IAM Permissions
```

For detailed instruction on creating an IAM policy, refer to the AWS documentation on Creating Customer Managed Policies.

Amazon STS Support and AssumeRole Policies

GigaVUE-FM supports VPC connections in only one account. You can add additional accounts using *Access and Secret Keys*. From GigaVUE-FM version 5.7.01, GigaVUE-FM connections to AWS can use the Amazons STS (Secure Token Service) and Assume Role policies. Using these policies, you can attach a role to a GigaVUE-FM instance running in AWS, thus enabling GigaVUE-FM to create and monitor multiple accounts in AWS.

You can still use the *Access and Secret Keys* to create additional accounts. However, using the STS option is the recommended best practice for security reasons.

Configuration

This section provides guidance on configuring your GigaVUE-FM instance to enable Amazon STS support.

Prerequisites

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

- A policy must be created in the account in which GigaVUE-FM is running.
  - Attach the created policy to a Role.
  - Attach the same Role to GigaVUE-FM, as an IAM instance Role.
- A policy must be included in other accounts as well.
  - These policies must allow GigaVUE-FM to assume the role in that account.

Procedure

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

To configure GigaVUE-FM for Amazon STS support:

1. In each target account, create an IAM role with the source account number as a trusted entity and attach policies with permissions allowing GigaVUE-FM to perform its functions. Record the ARN of each role created.

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

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

   IMPORTANT: The following example is provided as an illustration only.

   ```
   {
      "Version": "2012-10-17",
      "Statement": {
        "Effect": "Allow",
        "Action": [
          "iam:ListPolicies",
          "iam:GetPolicy",
          "iam:GetPolicyVersion"
      ],
        "Resource": "*"
      }
   }
   ```

3. In the source account, create a new IAM policy that allows the “sts:AssumeRole” action on all role ARNs created in Step 1.

   IMPORTANT: The following example is provided as an illustration only.

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

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

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

Sizing - Recommended Instance Types

The following table lists the recommended instance type and size per V Series node for the components.

Table 1: Recommended Instance Type per V Series Node

Component	Instance Type/Size
GigaVUE-FM	m4.xlarge
G-vTAP Agent	t2.micro
G-vTAP/V-Series Controller	t2.micro **NOTE:** t2.nano instance type is not supported
GigaVUE® V Series nodes	Table 2: Recommended Instance Types for Mirrored Traffic lists the instance type and size if the GigaVUE V Series node just receives and tunnels the traffic out. **NOTE:** C5.large is the recommended instance type if the total mirrored traffic from targets is around 1.5Gbps. Table 3: Recommended Instance Types with GigaSMART Applications Running lists the instance type and size if the GigaVUE V Series node has application running on it. **NOTE:** C5.Xlarge or C5.2Xlarge instances are the recommended instance types if applications are being used. C5.Xlarge can handle around 1Gbps of masked traffic (with 79% CPU utilization) and C5.2xlarge can handle 1Gbps (with 40-50% CPU utilization).

Table 2: Recommended Instance Types for Mirrored Traffic

Instance Type	Throughput (Packets per second)	Throughput (Mbps)	Framelength (bytes)
c4.large	54308	602	1454
c4.xlarge	71110	788	1454
c4.2xlarge	175302	1944	1454
c4.4xlarge	260564	2890	1454
c5.large	270500	2900	1454
c5.xlarge	292297	3400	1454
c5.2xlarge	309491	3600	1454

Table 3: Recommended Instance Types with GigaSMART Applications Running

Instance Type	Throughput (Packets per second)	Throughput (Mbps)	Framelength (bytes)
c4.large	29372	325	1454
c4.xlarge	37736	418	1454
c4.2xlarge	145901	1618	1454

Instance Type	Throughput (Packets per second)	Throughput (Mbps)	Framelength (bytes)
c4.4xlarge	169012	1874	1454
c5.large	54160	630	1454
c5.xlarge	104023	1010	1454
c5.2xlarge	206320	2400	1454

AWS Components and Services

This guide expects the users to be familiar with the following AWS services. If you are new to AWS, then refer to the Getting Started with AWS section for more information:

Component	Description
Amazon VPC	Amazon Virtual Private Cloud A web service for provisioning a logically isolated section of the AWS cloud where you can launch AWS resource in a virtual network that you define. You control your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways. See Also https://aws.amazon.com/vpc.
SG	Security Group A named set of allowed inbound network connections for an instance. (Security groups in Amazon VPC also include support for outbound connections.) Each security group consists of a list of protocols, ports, and IP address ranges. A security group can apply to multiple instances, and multiple groups can regulate a single instance.
NACL	Network ACL An optional layer of security that acts as a firewall for controlling traffic in and out of a subnet. You can associate multiple subnets with a single network ACL, but a subnet can be associated with only one network ACL at a time.
CloudWatch	Amazon CloudWatch A web service that enables you to monitor and manage various metrics, and configure alarm actions based on data from those metrics.
CFT	CloudFormation Template AWS CloudFormation simplifies provisioning and management on AWS. You can create templates for the service or application architectures you want and have AWS CloudFormation use those templates for quick and reliable provisioning of the services or applications (called “stacks”). You can also easily update or replicate the stacks as needed.
Tags	Metadata that you can define and assign to AWS resources, such as an EC2 instance. Not all AWS resources can be tagged.

Deploying GigaVUE-FM Using CloudFormation Templates (CFT)

You can deploy GigaVUE-FM using the AWS CloudFormation Templates (CFT) found in the AWS Marketplace, or manually through the AWS console. Refer to the following sections for more details:

- Launching GigaVUE-FM from AWS Marketplace
- Initializing GigaVUE-FM

Launching GigaVUE-FM from AWS Marketplace

To launch the GigaVUE-FM instance from the AWS Marketplace:

1. Login to the AWS account.
2. Go to https://aws.amazon.com/marketplace/.
3. In the **Search** field, type Gigamon and press **Enter**.
4. Click the **GigaVUE Cloud Suite for AWS** link for complete details about the product.
5. Click **Continue**. The Launch page is displayed.
6. In the Launch on EC2 page, select the following:
    a. From the **Version** drop-down list, select the latest version.
    b. From the **Region** drop-down list, select the appropriate region.
    c. Under Deployment Options, select **Auto Deploy GigaVUE-FM using AWS CFT**.
    d. Click the **Accept Software Terms** button to subscribe to the GigaVUE Cloud Suite for AWS software. A message is displayed to confirm the subscription. Click **Return to Launch Page**.
    e. In the Launch on EC2 page, the **Launch with CloudFormation Console** button is enabled. Click this button. The Select Template page is displayed.
7. In the Select Template page, the Gigamon Fabric Manager CloudFormation template is selected by default. Click **Next**. The Specify Details page is displayed.

8. In the Specify Details page, enter the following:
    a. In the **Stack name** field, enter a stack name.
    b. From the **Instance Type** drop-down list, select m4.xlarge as the minimum instance type for GigaVUE-FM.

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

    c. From the **Key Pair** drop-down list, select the name of an existing EC2 key pair.
    d. In the **Volume Size** field, by default 40 is selected. Change the volume size based on your requirement.
    e. From the **VPC ID** drop-down list, select the appropriate VPC ID.
    f. From the **My Subnet** drop-down list, select the appropriate public subnet ID.
    g. In the **SSH Location** field, enter the IP address or subnet that requires SSH access to the GigaVUE-FM instance.
    h. In the **CIDR IP**, enter the CIDR block where GigaVUE-FM would be deployed to allow management port access to the other components.
9. Click **Next**. In the Review page, review the complete details and then select the check box to acknowledge that AWS CloudFormation might create IAM resources.
10. Click **Create** to deploy GigaVUE-FM.

Initializing GigaVUE-FM

It will take several minutes for the GigaVUE-FM instance to initialize. After the initialization is completed, you can verify the instance through the Web interface as follows:

1. Select your instance and expand the page in the **Descriptions** tab to view the instance information, if necessary.
2. Copy and paste the Public DNS value into a new browser window or tab.
3. Copy the Instance ID from the **Descriptions** tab.

If GigaVUE-FM is deployed inside AWS, use the **Instance ID** as the password for the admin user to login to GigaVUE-FM, for example, admin/i-i-079173111e2d73753. You can change the password after logging in to GigaVUE-FM.
If GigaVUE-FM is deployed outside AWS, use admin123A! as the default admin password.

Backup/Restore

GigaVUE-FM includes a backup-and-restore feature for saving configuration data. You can use the saved data to restore a GigaVUE-FM instance or provide a copy of the configuration data and have it available for the new instance of GigaVUE-FM.

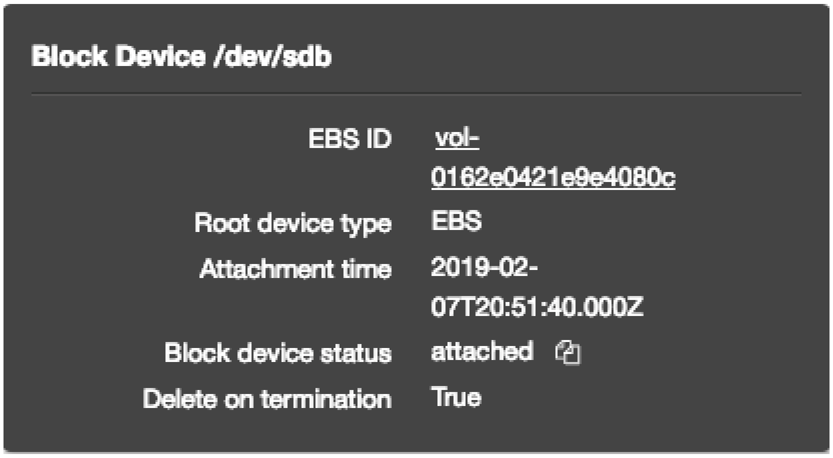
IMPORTANT:
If the GigaVUE-FM instance is in AWS, then you should back up the data periodically by creating a snapshot of the data volume and store a copy in another region. If GigaVUE-FM fails for any reason, then you must launch a new GigaVUE-FM AMI from the AWS Marketplace and attach this backup volume to resume operation.
It is recommended to back up cloud data in various availability zones and regions.

Backing Up GigaVUE-FM Configuration Data

To back up the GigaVUE-FM instance (that is, to create a snapshot of the volume of the existing version (dev/sdb) of the GigaVUE-FM instance), perform the following steps:

NOTE: It is recommended that you stop the GigaVUE-FM instance before taking a snapshot.

1. In your AWS console, locate the GigaVUE-FM instance and click the **Description** tab.
2. Scroll down and locate **Block Devices.** You will see two devices.
3. Click the second device, which is called **dev/sdb**. The **Block Device** dialog box is displayed with **EBS ID,** which is the volume ID.



Block Device /dev/sdb

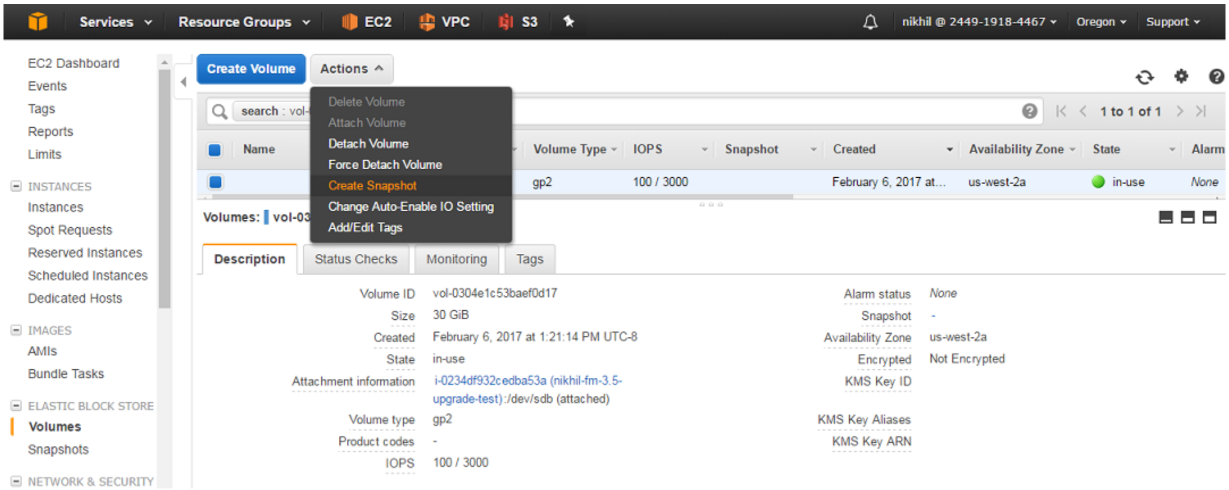
EBS ID	vol-0162e0421e9e4080c
Root device type	EBS
Attachment time	2019-02-07T20:51:40.000Z
Block device status	attached
Delete on termination	True

Figure 1 *Volume ID*

4. Click on the EBS ID link to view the volume in the **Volumes** console.

5. Click **Create Snapshot**. Depending on the size of the volume, it may take several minutes for the snapshot to be created.

> **NOTE:** The snapshot is stored in the **Snapshots** area in the console in the **Elastic Block Store** section.



Name	Volume Type	IOPS	Snapshot	Created	Availability Zone	State	Alarm
	gp2	100 / 3000		February 6, 2017 at...	us-west-2a	in-use	None

Volume ID vol-0304e1c53baef0d17
Size 30 GiB
Created February 6, 2017 at 1:21:14 PM UTC-8
State in-use
Attachment information i-0234df932cedba53a (nikhil-fm-3.5-upgrade-test):/dev/sdb (attached)
Volume type gp2
Product codes -
IOPS 100 / 3000

Alarm status None
Snapshot -
Availability Zone us-west-2a
Encrypted Not Encrypted
KMS Key ID
KMS Key Aliases
KMS Key ARN

Figure 2 *Create Snapshot*

6. Make a note of the snapshot ID, and/or tag it appropriately.

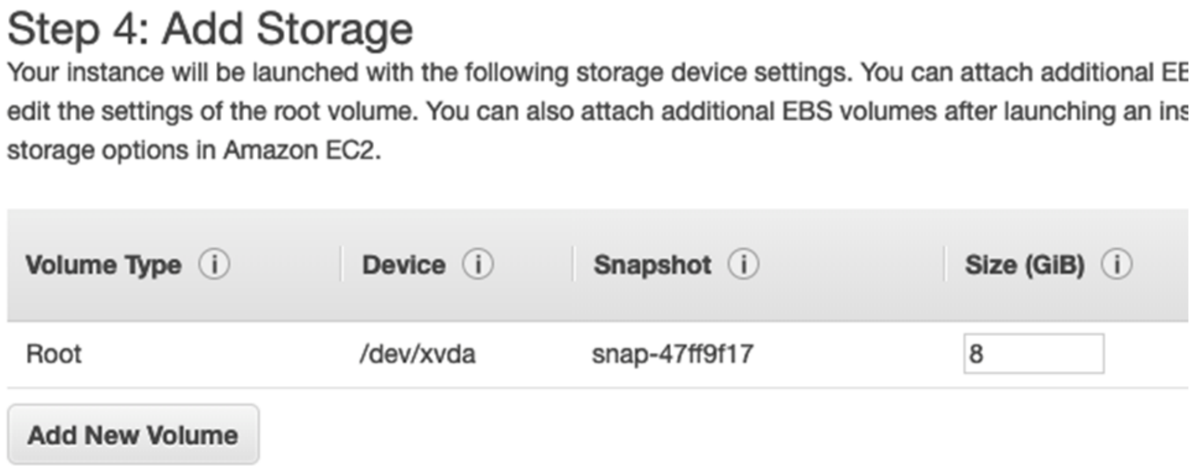
> **NOTE:** You can take snapshots as part of a regular backup process at required intervals. Snapshots can also be copied to other regions as backup in case of a regional failure.

Restoring GigaVUE-FM Configuration Data

The Amazon EBS volume must be restored with the data from the snapshot that is created in section Backing Up GigaVUE-FM Configuration Data.

1. Launch the same version of the GigaVUE-FM AMI from the AWS Marketplace in the console.
2. Choose the instance type and configure the instance details (such as network, subnet, IAM role and auto-assign public IP).

3. On the Add Storage page, click **Add New Volume** button.



Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EB
edit the settings of the root volume. You can also attach additional EBS volumes after launching an ins
storage options in Amazon EC2.

Volume Type	Device	Snapshot	Size (GiB)
Root	/dev/xvda	snap-47ff9f17	8

Figure 3 *Adding New Volume*

4. Choose **/dev/sdb** as the device name. Enter the snapshot ID of the latest snapshot taken. Make sure that the size (in GiB) is the same as the original volume.
5. Continue the launch process:
    a. Add tags.
    b. Select the right security groups.
    c. Review the instance details.
    d. Select your SSH key and click **Launch**.

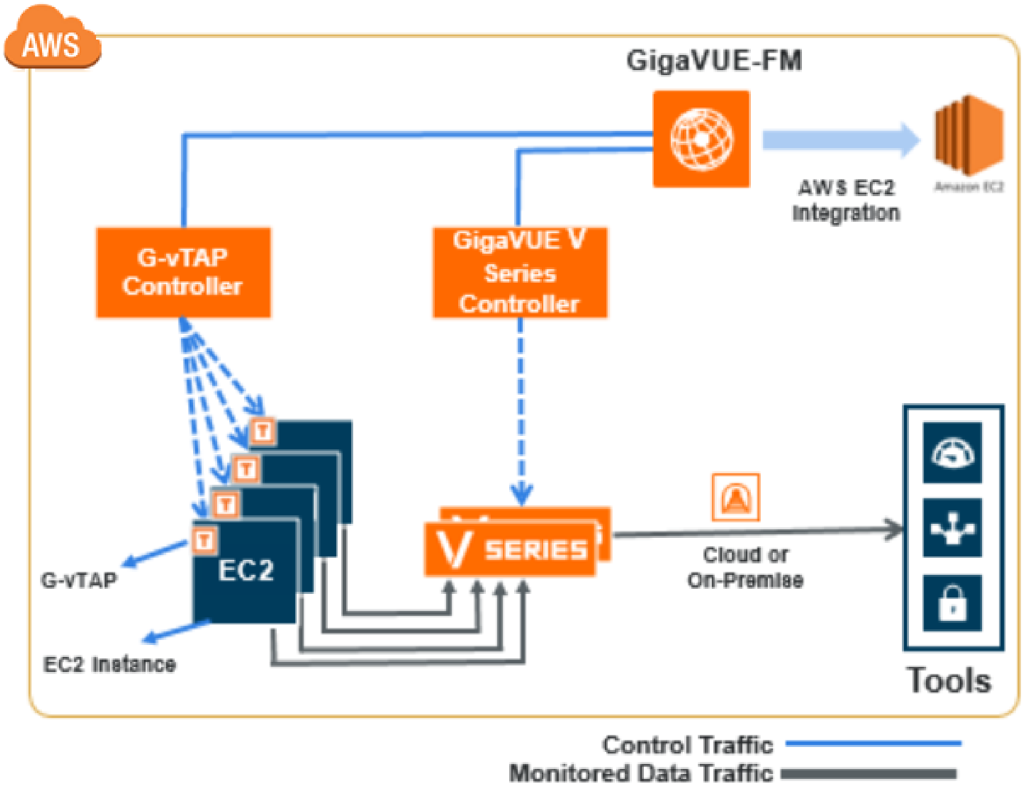
GigaVUE-FM will boot with the snapshot attached at this point and will restore itself from the data volume (snapshot) that was attached.

All fabric instances will remain running during this process and the configured traffic policies will continue to operate uninterrupted. GigaVUE-FM, once restored, will re-establish the connection to AWS and the fabric nodes.

> **NOTE:** If the GigaVUE-FM instance is configured on-site or on-premises, then refer to the 'Backup/Restore' procedure described in detail in the *GigaVUE-FM and GigaVUE-VM User's Guide* available in the customer portal.

GigaVUE Cloud Suite for AWS Components

The following image illustrates how the GigaVUE Cloud Suite for AWS components are configured within a VPC.



GigaVUE Cloud Suite for AWS includes the following components:

Component	Instance Type/Size
GigaVUE® Fabric Manager (GigaVUE-FM)	A web-based fabric management interface that provides single pane of glass visibility and management of both the physical and virtual traffic that forms the GigaVUE Cloud Suite for AWS. GigaVUE-FM can be installed on-premises or launched as an Amazon Machine Image (AMI) in AWS. GigaVUE-FM manages the configuration of the following components in your Amazon Virtual Private Clouds (VPC): • GigaVUE Cloud Suite V Series nodes • G-vTAP Controllers • GigaVUE Cloud Suite V Series Controllers To launch the AMI in AWS, refer to GigaVUE Cloud Suite for AWS Components. To install GigaVUE-FM on premise, refer to the *GigaVUE-FM and GigaVUE-VM User's Guide* available in the Customer Portal.
G-vTAP agent	An agent that is deployed in the Elastic Compute Cloud (EC2) instance. This agent mirrors the selected traffic from the instances (virtual machines) to the GigaVUE® V Series node. The G-vTAP agent is offered as a Debian or RedHat Package Manager (RPM) package. Refer to the GigaSECURE Cloud for AWS Configuration Guide for more details.

Component	Instance Type/Size
G-vTAP Controller	Manages multiple G-vTAP agents and orchestrates the flow of mirrored traffic to GigaVUE Cloud Suite V Series nodes. GigaVUE-FM uses one or more G-vTAP Controllers to communicate with the G-vTAP agents.
GigaVUE Cloud Suite V Series Controller	Manages multiple GigaVUE Cloud Suite V Series nodes and orchestrates the flow of traffic from GigaVUE Cloud Suite V Series nodes to the monitoring tools. GigaVUE-FM uses one or more GigaVUE Cloud Suite V Series Controllers to communicate with the GigaVUE Cloud Suite V Series nodes.
GigaVUE® V Series node	A visibility node that aggregates mirrored traffic from multiple G-vTAP agents. It applies filters, manipulates the packets using GigaSMART applications, and distributes the optimized traffic to cloud-based tools or backhaul to GigaVUE Cloud Suite for AWS using the standard IP GRE or VXLAN tunnels.

You can choose one of the following options for configuring the components described above:

Table 4: Configuration options for Nodes and Controllers

Option	Components
Option 1: Standard Configuration	GigaVUE® V Series nodes, GigaVUE V Series controllers and G-vTAP controllers are launched in all the VPCs.
Option 3: Shared Controller and V Series Node Configuration	GigaVUE® V Series nodes, GigaVUE V Series controllers and G-vTAP controllers are launched in a shared VPC. **NOTE:** VPC Peering must be enabled in the VPCs.

Configuring GigaVUE Cloud Suite in AWS

You can configure GigaVUE Cloud Suite for AWS using the GigaVUE-FM users interface.

Prerequisites

This section covers the following topics:

- AWS Security Credentials
- Network Requirements
- Security Group
- Key Pairs

AWS Security Credentials

When you first connect GigaVUE-FM with AWS, you need the security credentials for AWS to verify your identity and check if you have permission to access the resources that you are requesting. AWS uses the security credentials to authenticate and authorize your requests.

You need one of the following security credentials:

- **Identity and Access Management (IAM) role**—If GigaVUE-FM is running inside AWS, it is highly recommended to use an IAM role because it can securely make API requests from the instances.
  Create an IAM role and ensure that the permissions and policies listed in Permissions are associated to the role.
- **Access Keys**—If GigaVUE-FM is configured in the enterprise data center, then you need to use the access keys or basic credentials to connect to the VPC. Basic credentials allow full access to all the resources in your AWS account.
  An access key consists of an access key ID and a secret access key. For detailed instructions on creating access keys, refer to the AWS documentation on Managing Access Keys for Your AWS Account.

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

You cannot launch the GigaVUE-FM instance from the EC2 dashboard without having one of these security credentials. If you are launching the GigaVUE-FM instance from the AWS Marketplace, you need to have only the IAM roles.

> **IMPORTANT:**
>
> - Always run GigaVUE-FM inside AWS to manage your AWS workloads.
> - Always attach an IAM role to the instance running GigaVUE-FM in AWS to connect it to your AWS account.
> - Do NOT use access keys and secret keys to connect GigaVUE-FM to AWS. This requires GigaVUE-FM to store these keys and is NOT recommended.
> - Well architected guidelines highly recommend the use of IAM roles.

> **NOTE:** Running GigaVUE-FM outside of AWS requires the credentials to be stored internally. Although GigaVUE-FM encrypts access keys and secret access keys within its database, it is not recommended to connect to AWS from a GigaVUE-FM instance outside of AWS.

Network Requirements

To enable the flow of traffic between the components and the monitoring tools, your VPCs and instances should meet the following requirements:

- Subnets for VPC
- Elastic Network Interfaces (ENIs) for Instances

Subnets for VPC

Your VPC must have the following recommended subnets to configure the GigaVUE Cloud Suite for AWS components:

- **Management Subnet** that the GigaVUE-FM uses to communicate with the GigaVUE V Series nodes and controllers and G-vTAP controllers.
- **Data Subnet** that can accept incoming mirrored traffic from agents or be used to egress traffic to a tool. If a single subnet is used, then the Management subnet is also used as a Data Subnet.

Elastic Network Interfaces (ENIs) for Instances

For G-vTAP agents to mirror the traffic from the instances, you must configure one or more Elastic Network Interfaces (ENIs) on the EC2 instances.

- **Single ENI**—If there is only one interface configured on the EC2 instance with the G-vTAP agent, the G-vTAP agent sends the mirrored traffic out using the same interface.
- **Multiple ENIs**—If there are two or more interfaces configured on the EC2 instance with the G-vTAP agent, the G-vTAP agent monitors any number of interfaces but has an option to send the mirrored traffic out using any one of the interfaces or using a separate, non-monitored interface.

Security Group

A security group defines the virtual firewall rules for your instance to control inbound and outbound traffic. When you launch GigaVUE-FM, GigaVUE Cloud Suite V Series Controllers, GigaVUE Cloud Suite V Series nodes, and G-vTAP Controllers in your VPC, you add rules that control the inbound traffic to instances, and a separate set of rules that control the outbound traffic.

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

Table 5: Security Group Rules

Direction	Type	Protocol	Port	Source and CIDR, IP, or Security Group	Purpose
GigaVUE-FM Inside AWS					
Inbound	HTTPS	TCP(6)	443	Anywhere Any IP	Allows G-vTAP Controllers, GigaVUE Cloud Suite V Series Controllers, and GigaVUE-FM administrators to communicate

Direction	Type	Protocol	Port	Source and CIDR, IP, or Security Group	Purpose
					with GigaVUE-FM
G-vTAP Controller					
Inbound	Custom TCP Rule	TCP(6)	9900	Custom GigaVUE-FM IP	Allows GigaVUE-FM to communicate with G-vTAP Controllers
G-vTAP Agent					
Inbound	Custom TCP Rule	TCP(6)	9901	Custom G-vTAP Controller IP	Allows G-vTAP Controllers to communicate with G-vTAP agents
GigaVUE Cloud Suite V Series Controller					
Inbound	Custom TCP Rule	TCP(6)	9902	Custom GigaVUE-FM IP	Allows GigaVUE-FM to communicate with GigaVUE Cloud Suite V Series Controllers
GigaVUE Cloud Suite V Series node					
Inbound	Custom TCP Rule	TCP(6)	9903	Custom GigaVUE V Series Controller IP	Allows GigaVUE Cloud Suite V Series Controllers to communicate with GigaVUE Cloud Suite V Series nodes
GRE Traffic					
Inbound	Custom Protocol Rule	GRE (47)	ALL	Anywhere Any IP	Allows mirrored traffic from G-vTAP agents to be sent to GigaVUE Cloud Suite V Series nodes using the L2 GRE tunnel Allows monitored traffic to be sent from GigaVUE Cloud Suite V Series nodes to the monitoring tools using the L2 GRE tunnel
VXLAN Traffic					
Inbound	Custom UDP Rule	VXLAN	4789	Anywhere Any IP	Allows mirrored traffic from G-vTAP agents to be sent to GigaVUE Cloud Suite V Series nodes using VXLAN tunnel Allows monitored traffic to be sent from GigaVUE Cloud Suite V Series nodes to the tools using VXLAN tunnel

Creating a Security Group

To create an inbound security group for a component:

1. In the Amazon EC2 dashboard, click **Security Groups** in the navigation pane.
2. Click **Create Security Group**.
3. In the Security group name, enter a name.
4. In **Description**, specify the purpose for creating the security group.
5. In **VPC**, select the VPC ID.
6. Click **Add Rule** and enter the protocol, port, IP address, and description appropriate for the component. For information about the rules, refer to Security Group Rules.

   > **NOTE:** The Source and the CIDR must be entered based on your requirement.

7. Click **Create**. The security group is created for the respective component.
8. Repeat steps 2 to 8 to create security groups for the other components.

Key Pairs

A key pair consists of a public key and a private key. You must create a key pair and specify the name of this key pair when you define the specifications for the G-vTAP Controllers, GigaVUE Cloud Suite V Series nodes, and GigaVUE Cloud Suite V Series Controllers in your VPC.

For information about creating a key pair, refer to creating a key pair in the AWS documentation.

Pre-Configuration Checklist

The following table provides information that you must obtain to ensure a successful and efficient configuration of the GigaVUE Cloud Suite for AWS using the GigaVUE-FM user interface.

Table 6: Pre-configuration Checklist

	Pre-configuration Checklist
□	VPC ID
□	VPC Peering **NOTE:** Peering must be active between VPCs within the same monitoring domain. This is required only when shared controller/V Series node option is chosen for configuring the components.
□	Instance ID of the GigaVUE-FM
□	Public or Private IP of the GigaVUE-FM
□	Elastic IP **NOTE:** If GigaVUE-FM is installed in the enterprise data center, an Elastic IP is required for G-vTAP controllers and GigaVUE Cloud Suite V Series controllers to communicate with GigaVUE-FM

	Pre-configuration Checklist
□	Region name for the VPC
□	Availability zone of the VPC
□	IAM role name OR Access key ID and Secret Access key
□	SSH Key Pair
□	Subnets
□	Security groups

Logging in to GigaVUE-FM

To login to GigaVUE-FM, do the following:

1. Copy and paste the GigaVUE-FM instance's public or private IP address into a browser. The GigaVUE-FM login page is displayed.
2. Enter admin as the user name and Instance ID of GigaVUE-FM as the password.
3. Click **Login**.

If you want to enable CloudWatch Events to track instance state changes in GigaVUE-FM, you must enable the checkbox before connecting to AWS.

To enable **AWS Cloud Watch Event Based Inventory Refresh** for the connection, go to **AWS > Configuration > Settings** and select the **AWS CloudWatch event-based inventory refresh** check box. AWS Cloud Watch Event Based Inventory Refresh lets you create a CloudWatch Event Rule and SQS queue that sends and receives the instance state change events. The GigaVUE-FM will poll the SQS queue for instance state change events.

Connecting to AWS

GigaVUE-FM connects to the VPC through the EC2 API endpoint. HTTPS is the default protocol which GigaVUE-FM uses to communicate with the EC2 API. For more information about the endpoint and the protocol used, refer to http://docs.aws.amazon.com/general/latest/gr/rande.html#ec2_region. Once the connection is established, GigaVUE-FM launches the G-vTAP Controller, GigaVUE Cloud Suite V Series Controller, and GigaVUE Cloud Suite V Series node.

GigaVUE-FM provides you the flexibility to connect to multiple VPCs. You can choose the VPC ID and launch the GigaVUE Cloud Suite Cloud in AWS components in the desired VPCs.

To connect to AWS using GigaVUE-FM:

1. Click **Cloud** in the top navigation link.
2. Under AWS, select **Configuration > Connections**, and then click the **New** drop-down menu. You can either create a new monitoring domain or a new connection.
   - If you select **Monitoring Domain**, then the **Create Monitoring Domain** dialog box is displayed. Enter the alias that is used to identify the monitoring domain.
   - If you select **Connection**, then the AWS Connection page is displayed.

3. Enter or select the appropriate information as shown in the following table.

Table 7: AWS Connection

Field	Description
Alias	An alias used to identify the connection to AWS. For example, vpcs-48b0ac2c-Oregon.
Monitoring Domain	An alias used to identify the monitoring domain. You can either create a new monitoring domain or select an existing monitoring domain that is already created. **NOTE:** Monitoring domain consists of set of connections.
Authentication Type	The authentication type for the connection. For more information, refer to Connecting to AWS.
Region Name	The AWS region for the connection. For example, EU (London). **NOTE:** If the region you want to choose is not available in the Region Name list, you can add a custom region. **Adding a Custom Region** To add a custom region: **a.** In the Region Name drop-down list, select **Custom Region**. **b.** In the Custom Region Name field, enter the name of the region that is not available in the list.
VPC ID	The ID of the target VPC for establishing the connection.
Availability Zone	The availability zone of the VPC. For example, US-West-2c. **NOTE:** An availability zone may fail due to various reasons. To recover the availability zone, you must have another standby GigaVUE-FM instance running in another availability zone. The connections to the VPCs must be pre-configured with a GigaVUE V Series Node Spec of 0 minimum. This GigaVUE-FM instance waits for the new workloads to launch the appropriate number of V Series nodes to handle the load. You can configure GigaVUE-FM to generate an event if a connection in an availability zone goes down and the fabric controllers/nodes are unreachable. Refer to the section Setting Up Email Notifications for details on how to setup an event. GigaVUE-FM attempts to recover the fabric nodes and controllers (up to 5 times before triggering a notification).
Access Key/Secret Access Key	The access key and secret access key that are used to establish AWS connection. These keys are required when the authentication type is Basic Credentials.
Use Proxy Server	The check box to add a proxy server, if required.
Proxy Server	The list of proxy servers already configured in GigaVUE-FM. For more information on adding the proxy servers before configuring the AWS connection, refer to the GigaSECURE Cloud for AWS Configuration Guide.
Add Proxy Server	The proxy server can be configured from the AWS Connection page. Click **Add Proxy Server**.

4. Click **Save**.

If the connection is established, the status is displayed as **Connected** in the Connections page. GigaVUE-FM discovers the inventory of the VPC in the background. If the connection fails, an error message is displayed specifying the cause of failure. The connection status is also displayed in **Cloud > Audit Logs**.

Configuring the G-vTAP Controllers

A G-vTAP Controller manages multiple G-vTAP agents and orchestrates the flow of mirrored traffic to GigaVUE Cloud Suite V Series nodes.

A G-vTAP Controller can only manage G-vTAP agents that has the same version. For example, the G-vTAP Controller v1.3 can only manage G-vTAP agents v1.3. So, if you have G-vTAP agents v1.2 still deployed in the EC2 instances, you must configure both G-vTAP Controller v1.2 and v1.3.

While configuring the G-vTAP Controllers, you can also specify the tunnel type to be used for carrying the mirrored traffic from the G-vTAP agents to the GigaVUE Cloud Suite V Series nodes. The tunnel type can be L2GRE or VXLAN.

To configure the G-vTAP Controllers:

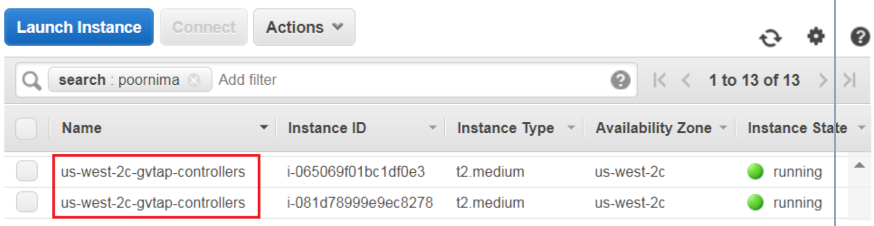
1. Click **Cloud** in the top navigation link.
2. Under AWS, click **Configuration > G-vTAP Controllers**.
3. Click **New**. The G-vTAP Configuration page is displayed.

4. Enter or select the appropriate information as shown in the following table.

Table 8: Fields for G-vTAP Configuration

Fields	Description
Connection	The name of the AWS connection. **NOTE:** For shared controller configuration, you must select the required connection for configuring the G-vTAP Controller. Peering must be active in the selected connection to allow the rest of the connections containing the V-series nodes to be monitored.
EBS Volume Type	The Elastic Block Store (EBS) volume that you can attach to a single G-vTAP Controller instance. The available options are gp2 (General Purpose SSD), io1 (Provisioned IOPS SSD), and standard (Magnetic).
SSH KeyPair	The SSH key pair for the G-vTAP Controller. For more information about SSH key pair, refer to Key Pairs
Management Subnet	The subnet that is used for communication between the G-vTAP Controllers and the G-vTAP agents. This is a required field. Every fabric node (both controllers and the nodes) need a way to talk to each other and to GigaVUE-FM. Therefore, they should share at least one management plane/subnet.
Mgmt Subnet Security Groups	The security group created for the G-vTAP Controller. For more information, refer to Security Group.
IP Address Type	The IP address type. Select one of the following: • Select **Private** if you want to assign an IP address that is not reachable over Internet. You can use private IP address for communication between the G-vTAP Controller instances and GigaVUE-FM instances in the same subnet in a VPC, or a peered VPC subnet. • Select **Public** if you want the IP address to be assigned from Amazon's pool of public IP address. The public IP address gets changed every time the instance is stopped and restarted. **NOTE:** Use this only if GigaVUE-FM cannot communicate with the controllers directly, such as outside a non-peered VPC. • Select **Elastic** if you want a static IP address for your instance. The option to select the Elastic IPs is displayed under Controller Version(s). The elastic IP address does not change when you stop or start the instance.
Controller Version(s)	The G-vTAP Controller version. The G-vTAP Controller version you configure must always be the same as the G-

Fields	Description
	vTAP agents' version number deployed in the EC2 instances. This is because the G-vTAP Controller v1.2 can only manage G-vTAP agents v1.2. Similarly, the G-vTAP Controller v1.3 can only manage G-vTAP agents v1.3. If there are multiple versions of G-vTAP agents deployed in the EC2 instances, then you must configure multiple versions of G-vTAP Controllers that matches the version numbers of the G-vTAP agents. **NOTE:** If there is a version mismatch between G-vTAP controllers and G-vTAP agents, GigaVUE-FM cannot detect the agents in the instances. To add multiple versions of G-vTAP Controllers: **a.** Under **Controller Versions**, click **Add**. **b.** From the **Image** drop-down list, select a G-vTAP Controller image that matches with the version number of G-vTAP agents installed in the instances. **c.** From the **Instance Type** down-down list, select an instance type for the G-vTAP Controller. The recommended instance type is t2.medium. **NOTE:** The instance type t2.nano is not supported. **d.** In **Number of Instances to Launch**, specify the number of G-vTAP Controllers to launch. The minimum number you can specify is 1. **e.** The Elastic IPs drop-down list appears only if the **Elastic** option is selected in the IP Address Type. From the **Elastic IPs** drop-down list, select an IP. **NOTE:** The Elastic IPs must be allocated in the EC2 management console prior to step e.
Controller Version(s) (continued)	An older version of G-vTAP Controller can be deleted once all the G-vTAP agents are upgraded to the latest version. To delete a specific version of G-vTAP Controller, click **x** (delete) next to its G-vTAP Controller image. Once you delete a G-vTAP Controller image from the G-vTAP Configuration page, all the G-vTAP Controller instances of that version are deleted from AWS.
Additional Subnet(s)	(Optional) If there are G-vTAP agents on subnets that are not IP routable from the management subnet, additional subnets must be specified so that the G-vTAP Controller can communicate with all the G-vTAP agents. Click **Add** to specify additional subnets, if needed. Also, make sure that you specify a list of security groups for each additional subnet.
Tag(s)	(Optional) The key name and value that helps to identify the G-vTAP Controller instances in your AWS environment. For example, you might have G-vTAP Controllers deployed in many regions. To distinguish these G-vTAP Controllers based on the regions, you can provide a name that is easy to identify such as us-west-2-gvtap-controllers. To add a tag: **a.** Click **Add**. **b.** In the **Key** field, enter the key. For example, enter Name. **c.** In the **Value** field, enter the key value. For example, us-west-2-gvtap-controllers.

Fields	Description
	When the G-vTAP Controllers are launched in the VPC, they appear as shown in the following figure.  Launch Instance Connect Actions Add filter 1 to 13 of 13 search : poornima Name | Instance ID | Instance Type | Availability Zone | Instance State us-west-2c-gvtap-controllers | i-065069f01bc1df0e3 | t2.medium | us-west-2c | ● running us-west-2c-gvtap-controllers | i-081d78999e9ec8278 | t2.medium | us-west-2c | ● running **Figure 4** *G-vTAP Controllers with Custom Tag Name*
Agent Tunnel Type	The type of tunnel used for sending the traffic from G-vTAP agents to GigaVUE Cloud Suite V Series nodes. The options are GRE or VXLAN tunnels.
G-vTAP Agent MTU (Maximum Transmission Unit)	The Maximum Transmission Unit (MTU) is the maximum size of each packet that the tunnel endpoint can carry from the G-vTAP agent to the GigaVUE Cloud Suite V Series node. For GRE, the default value is 9001. For VXLAN, the default value is 8951. However, the G-vTAP agent tunnel MTU should be 50 bytes less than the agent's destination interface MTU size.

5. Click **Save**.

To view the G-vTAP Controllers connection status, navigate to **Visibility Fabric > G-vTAP Controllers**. The G-vTAP Controller instance takes a few minutes to fully initialize. After the initialization is complete, the connection status is displayed as **OK**.

The G-vTAP Controller launch is displayed as an event in the **Cloud** > **Events** page.

To view the G-vTAP Controllers launched in your VPC:

1. Login to the AWS account and select **Services > EC2**.
2. In the left navigation pane, click **Instances**. The G-vTAP Controllers launched in your VPC are listed in the Instances page.

Configuring the GigaVUE Cloud Suite V Series Controllers

GigaVUE Cloud Suite V Series Controller manages multiple GigaVUE Cloud Suite V Series nodes and orchestrates the flow of traffic from GigaVUE Cloud Suite V Series nodes to the monitoring tools. GigaVUE-FM uses one or more GigaVUE Cloud Suite V Series Controllers to communicate with the GigaVUE Cloud Suite V Series nodes.

A single GigaVUE Cloud Suite V Series Controller can manage up to 100 GigaVUE Cloud Suite V Series nodes.

To configure the GigaVUE Cloud Suite V Series Controller, do the following:

1. Select **AWS** > **Configuration** > **V Series Controllers**.
2. Click **New**. The V Series Controller Configuration page opens.

   > **NOTE:** For shared controller configuration, you must select the required connection for configuring the V Series Controller. Peering must be active in the selected connection to allow the rest of the connections to be monitored.

3. Follow Step 4, Step 5 and Step 6 as described in Configuring the G-vTAP Controllers and select the appropriate information for GigaVUE Cloud Suite V Series Controllers.

To view the *GigaVUE V Series Controller* configured in your VPC:

1. Login to the AWS account and select **Services** > **EC2**.
2. In the left navigation pane, click **Instances**. The *GigaVUE V Series Controller* is configured in your VPC.

Configuring the GigaVUE Cloud Suite V Series Nodes

GigaVUE® V Series node is a visibility node that aggregates mirrored traffic from multiple G-vTAP agents. It applies filters, manipulates the packets using GigaSMART applications, and distributes the optimized traffic to cloud-based tools or backhaul to GigaVUE Cloud Suite for AWS using the standard IP GRE or VXLAN tunnels.

GigaVUE Cloud Suite V Series nodes can be successfully launched only after GigaVUE Cloud Suite V Series Controller is fully initialized and the status is displayed as OK.

To launch a GigaVUE Cloud Suite V Series node, do the following:

1. Select **AWS** > **Configuration** > **V Series Nodes**.
2. Click **New**. The V Series Node Configuration page appears.

   > **NOTE:** Make sure the GigaVUE Cloud Suite V Series node version matches with the GigaVUE Cloud Suite V Series Controller version that is already configured.

3. Enter or select the appropriate information as shown in the following table.

Table 9: Fields for GigaVUE Cloud Suite V Series Configuration

Fields	Description
Connection	The name of the AWS connection.
Image	The GigaVUE Cloud Suite V Series node image. **NOTE:** The version number of GigaVUE Cloud Suite V Series node must match with the version number of the GigaVUE Cloud Suite V Series Controller.
Instance Type	The instance type for the GigaVUE Cloud Suite V Series node. The recommended minimum instance type is c4. large.
EBS Volume Type	The Elastic Block Store (EBS) volume that you can attach to a single G-vTAP Controller instance. The available options are gp2 (General Purpose SSD), io1 (Provisioned IOPS SSD), and standard (Magnetic).
SSH KeyPair	The SSH key pair for the GigaVUE Cloud Suite V Series node. For more information about SSH key pair, refer to Key Pairs.
Management Subnet	The subnet that is used for communication between the GigaVUE Cloud Suite V Series Controller and the GigaVUE Cloud Suite V Series node. This is a required field. Every fabric node (both controllers and the nodes) need a way to talk to each other and FM. So they should share at least one management plane/subnet.
Mgmt Subnet Security Groups	The security group created for the GigaVUE Cloud Suite V Series node. For more information, refer to Security Group
Data Subnet(s)	The subnet that receives the mirrored GRE or VXLAN tunnel traffic from the G-vTAP agents. If this subnet will also egress traffic to your tools, select the 'Tool Subnet' radio button.
Tag(s)	(Optional) The key name and value that helps to identify the GigaVUE Cloud Suite V Series node instances in your AWS environment. For example, you might have GigaVUE Cloud Suite V Series node deployed in many regions. To distinguish these GigaVUE Cloud Suite V Series node based on the regions, you can provide a name that is easy to identify such as us-west-2-vseries. To add a tag: a. Click **Add**. b. In the **Key** field, enter the key. For example, enter Name. c. In the **Value** field, enter the key value. For example, us-west-2-vseries.

Fields	Description
Min Instances to Launch	The minimum number of GigaVUE Cloud Suite V Series nodes to be launched in the AWS connection. The minimum number of instances that can be entered is 0. When 0 is entered, no GigaVUE Cloud Suite V Series nodes are launched. **NOTE:** Nodes will be launched when a monitoring session is deployed as long as GigaVUE-FM discovers some targets to monitor. The minimum amount will be launched at that time.The GigaVUE-FM will delete the nodes if they are idle for over 15 minutes.
Max Instances to Launch	The maximum number of GigaVUE Cloud Suite V Series nodes that can be launched in the AWS connection. When the number of instances per V Series node exceeds the max instances specified in this field, increase the number in the Max Instances to Launch. When additional V Series nodes are launched, GigaVUE-FM rebalances the instances assigned to the nodes. This can result in a brief interruption of traffic.
Tunnel MTU (Maximum Transmission Unit)	The Maximum Transmission Unit (MTU) on the outgoing tunnel endpoints of the GigaVUE Cloud Suite V Series node when a monitoring session is deployed. The default value is 9001.

To view the *GigaVUE V Series nodes* launched in your VPC:

1. Login to the AWS account and select **Services** > **EC2**.
2. In the left navigation pane, click **Instances**. The *GigaVUE V Series nodes* launched in your VPC can be seen.
   - The recommended minimum instance type for the GigaVUE Cloud Suite V Series node is c4.large.
   - Certain availability zones may sometimes throw an insufficient instance capacity error. This is because AWS does not currently have enough capacity to service your request. When this error is displayed, you can launch the instance using a different instance type and resize at a later stage. Refer to the following link to select another instance type: https://aws.amazon.com/ec2/instance-types/
   - The insufficient instance capacity error can be viewed only on Events page. Refer to Events.
   - To change the instance type at a later stage, the active monitoring sessions must be undeployed and the GigaVUE V Series nodes must be relaunched with the new configuration settings.

Administration

This chapter describes the administration tasks that can be performed in GigaVUE Cloud Suite for AWS. Refer to the following section for details:

- Setting Up Email Notifications
- Events
- Storage Management
- Fabric Health Monitoring
- Recovery Timing

Setting Up Email Notifications

Notifications are triggered by a range of events such as AWS license expiry, VM instance terminated, connection failure in availability zone and so on. You can setup the email notification for a particular event or a number of events and the recipient or recipients to whom the email should be sent.

Gigamon strongly recommends you to enable email notifications so there is immediate visibility of the events affecting node health.

The following are the events for which you can setup the email notifications:

- AWS License Expire
- Fabric Node Down
- Fabric Node Reboot Failed
- Fabric Node Rebooted
- Fabric Node Replacement Launch Failed
- Fabric Node Replacement Launched
- Fabric Node Restart Failed
- Fabric Node Restarted
- Fabric Node Unreachable
- Fabric Node Up

To configure automatic email notifications in GigaVUE-FM:

1. On the right side of the top navigation bar, Click ⚙
2. On the left navigation pane, select **System** > **Notifications**.
3. In the Notifications page, select the event and click **Configure**.
4. In the Recipient(s) box, enter one or multiple email IDs separated by a comma.
5. Click **Save**.

Events

The Events page displays all the events occurring in the virtual fabric node, VM Domain, and VM manager. An event is an incident that occur at a specific point in time. Examples of events include:

- AWS License Expire
- G-vTAP Agent Inventory Update Completed
- AWS Connection Status Changed

An Alarm is a response to one or more related events. If an event is considered of high severity, then GigaVUE-FM raises an alarm. An example of alarm could be AWS license expiry.

The alarms and events broadly fall into the following categories: Critical, Major, Minor, or info. To configure alarms, click **Cloud** on the top navigation link. On the left navigation pane, click **Events**.

Table 10: Event Parameters describes the parameters recording for each event. You can also use filters to narrow down the results. .

Table 10: Event Parameters

Controls/ Parameters	Description
Source	The source from where the events are generated.
Time	The timestamp when the event occurred. **IMPORTANT:** Timestamps are shown in the time zone of the client browser's computer and not the timezone of the node reporting the event. The timestamp is based on the correctly configured clock on the GigaVUE-FM server and converted from UTC to the client computer's configured timezone.
Scope	The category to which the events belong. Events can belong to the following category: Virtual Fabric Node, VM Domain, VM Manager.
Event Type	The type of event that generated the events.
Severity	The severity is one of Critical, Major, Minor, or Info. Info is informational messages. For example, when GigaVUE V Series nodes are installed, such a message is displayed as Info.
Affected Entity Type	The resource type associated with the alarm or event.
Affected Entity	The resource ID of the affected entity type.
Description	The description of the event, which includes any of the possible notifications with additional identifying information where appropriate.
Device IP	The IP address of the device.
Host Name	The host name of the device.

Storage Management

GigaVUE-FM Storage Management is used to configure storage settings for the GigaVUE-FM instance.

> **NOTE:** The fabric nodes are stateless and do not store data. Therefore, fabric nodes do not have any storage issues. If fabric nodes fail due to storage issues, then GigaVUE-FM recovers or replaces the fabric nodes accordingly.

To access **Storage Management** for GigaVUE-FM:

1. On the right side of the top navigation bar, Click ⚙
2. On the left navigation pane, select **System** > **Storage Management.**
3. Click **Edit** to configure the storage settings.

For detailed information on storage management, refer to the “Storage Management” section in the *GigaVUE-FM and GigaVUE-VM User’s Guide* available in the Customer Portal.

Disk Utilization Monitor

The **Disk Utilization Monitor** displays disk usage levels over time for individual partitions and provides information about peak disk usage for GigaVUE-FM logs and data. This provides information that can help prevent outages due to disk out-of-space issues.

To set thresholds for the Disk Utilization Monitor, do the following:

1. Click **Dashboard > Health Monitor.**
2. On the Health Monitor Dashboard page, click **Settings**.
3. On the **Health Monitor Thresholds Settings** page, select the percentages for CPU, Memory and Disk Utilization. This is the threshold for the alarm.
4. Click **Save.**

After you have set the utilization thresholds, the threshold is displayed as a red line on the time chart of the monitors. The following figure shows the storage usage of the GigaVUE-FM instance.

> **NOTE:** You can also configure GigaVUE-FM to send email notifications on disk space as described in section Setting Up Email Notifications.

Fabric Health Monitoring

GigaVUE-FM monitors the health of all virtual fabric instances to maintain a highly available fabric. Fabric health monitoring involves the following:

- Monitoring the state of the nodes deployed.
- Restarting a node if it is down.
- Reconfiguring, restarting or re-deploying the nodes to restore monitoring services quickly.

Virtual fabric monitoring helps to achieve auto-scaling, fail-over and load-balancing of the fabric. GigaVUE-FM monitors both the G-vTAP controllers and the GigaVUE Cloud Suite Vseries nodes that are deployed in every connection. If GigaVUE-FM detects any failure on the controllers and nodes, then it recovers these components as described below:

- Restarts a node if it is shut down.
- Reboots an unreachable node and recovers it. If this operation fails, then GigaVUE-FM replaces the node.
- Replaces a node that is terminated by a user
- Reconfigures a node if it is rebooted and redeploys the monitoring session

If recovery is not possible, then GigaVUE-FM marks the node as 'Down' and an alert is generated in the Events page. If a node cannot be replaced, then GigaVUE-FM displays the reason in the Events page. You can set up an **E-mail notification** for the Alerts and Events generated for all these events.

NOTE: You can also enable **CloudWatch Events** to track instance state changes in GigaVUE-FM before connecting to AWS. Refer to section Logging in to GigaVUE-FM for details on how to enable AWS CloudWatch Events.

If CloudWatch is not integrated with GigaVUE-FM, then GigaVUE-FM polls the fabric every 900 seconds by default. This can be configured using the **Refresh Interval** for fabric deployment inventory in the **AWS Settings** page. You can choose the interval from 30 seconds to 86400 seconds.

Recovery Timing

GigaVUE-FM takes around 5 minutes to recover after it is launched. This might vary depending on the platform, instance type, region and other such reasons. After the GigaVUE-FM instance is launched and running, it takes 5 minutes to initialize the instance.

The fabric nodes take almost the same time as GigaVUE-FM to recover. If the fabric nodes are found to be 'Down', then GigaVUE-FM initiates a replacement. GigaVUE-FM takes the same time as that of the platform to boot the fabric nodes. Once the nodes are running in AWS, it takes less than a minute until GigaVUE-FM redeploys the configurations to the nodes and recovers.

NOTE: If GigaVUE-FM fails (in the same region/AZ where fabric is deployed), the snapshot backup can be used to replace the failed GigaVUE-FM in about 5 minutes. This can be done either:

- By manually launching GigaVUE-FM from the AWS Marketplace and attaching a backup snapshot as a second disk.
- By using AWS tools such as a CFT template to launch a new GigaVUE-FM instance, and attaching the backup volume as a data disk.

In either of these two cases, GigaVUE-FM will recover using the backup data and resume operations. Fabric nodes will remain running, and traffic flow will not be interrupted as long as they remain running. In the event of a regional or availability zone failure, it is recommended to run another GigaVUE-FM in another region/AZ, as a standby.

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 Gigamon Community

Documentation

ATTENTION: 5.10.00 was delivered as embedded software on new hardware only. The updated PDFs for the 5.10.01 software release are coming soon! Check back on 8/29/2020 for the latest.

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.

Table 1: Documentation Set for Gigamon Products

GigaVUE Cloud Suite 5.10 Hardware and Software Guides
Hardware how to unpack, assemble, rack-mount, connect, and initially configure ports the respective GigaVUE Cloud Suite devices; reference information and specifications for the respective GigaVUE Cloud Suite devices
***G-TAP A Series 2 Installation Guide**
GigaVUE-HC1 Hardware Installation Guide
GigaVUE-HC2 Hardware Installation Guide
GigaVUE-HC3 Hardware Installation Guide
GigaVUE TA Series Hardware Installation Guide *(now including TA25)*
***GigaVUE-OS Installation Guide for DELL S4112F-ON** how to install GigaVUE-OS and configure ports on COTS DELL S4112F-ON
Software Installation and Upgrade Guides
GigaVUE-FM Installation, Migration, and Upgrade Guide how to install GigaVUE-FM on VMware ESXi, MS Hyper-V, and KVM how to migrate GigaVUE-FM on VMware ESXi, Hardware Appliance, and AWS
GigaVUE-OS Upgrade Guide

GigaVUE Cloud Suite 5.10 Hardware and Software Guides
how to upgrade the embedded GigaVUE-OS on GigaVUE H Series and GigaVUE TA Series nodes
Administration
GigaVUE-OS and GigaVUE-FM Administration Guide how to administer the GigaVUE-OS and GigaVUE-FM software (note, new file name for PDF)
Fabric Management
GigaVUE-FM User's Guide how to install, deploy, and operate GigaVUE-FM how to configure GigaSMART operations includes instructions for GigaVUE-FM and GigaVUE-OS features
Cloud Configuration and Monitoring how to configure the GigaVUE Cloud Suite components and set up traffic monitoring sessions for the respective cloud platform
GigaVUE Cloud Suite for AnyCloud Configuration Guide how to deploy the GigaVUE Cloud Suite solution in any cloud platform
GigaVUE Cloud Suite for AWS Configuration Guide
GigaVUE Cloud Suite for AWS Quick Start Guide quick view of AWS deployment used in conjunction with the GigaVUE Cloud Suite for AWS Configuration Guide
GigaVUE Cloud Suite for AWS SecretRegions Configuration Guide
GigaVUE Cloud Suite for Azure Configuration Guide
GigaVUE Cloud Suite for Kubernetes Configuration Guide
GigaVUE Cloud Suite for Nutanix Configuration Guide
GigaVUE Cloud Suite for OpenStack Configuration Guide
GigaVUE Cloud Suite for VMware Configuration Guide
Gigamon Containerized Broker
Reference
GigaVUE-OS-CLI Reference Guide library of GigaVUE-OS CLI (Command Line Interface) commands used to configure and operate GigaVUE H Series and TA Series devices
GigaVUE-OS Cabling Quick Reference Guide guidelines for the different types of cables used to connect Gigamon devices
GigaVUE-OS Compatibility and Interoperability Matrix compatibility information and interoperability requirements for Gigamon devices

GigaVUE Cloud Suite 5.10 Hardware and Software Guides
GigaVUE-FM REST API Reference in GigaVUE-FM User's Guide samples uses of the GigaVUE-FM Application Program Interfaces (APIs)
Release Notes
GigaVUE-OS, GigaVUE-FM, GigaVUE-VM, G-TAP A Series, and GigaVUE Cloud Suite Release Notes new features, resolved issues, and known issues in this release ; important notes regarding installing and upgrading to this release **NOTE:** Release Notes are not included in the online documentation. **NOTE:** Registered Customers can log in to My Gigamon to download the Software and Release Notes from the Software & Docs page on to My Gigamon. Refer to .
In-Product Help
GigaVUE-FM Online Help how to install, deploy, and operate GigaVUE-FM.
GigaVUE-OS H-VUE Online Help provides links the online documentation.

How to Download from My Gigamon

Registered Customers can download software and corresponding Release Notes documents from the **Software & Docs** 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 & Documentation** 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

To send feedback and report issues in our documentation, complete the short survey at the following link:

https://www.surveymonkey.com/r/gigamondocumentationfeedback

Contact Technical Support

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

Partners: www.gigamon.com/partners.html

Premium Support

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

The Gigamon Community

The Gigamon 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 Gigamon Community site to:

- Find knowledge base articles and documentation
- Ask and answer questions and learn best practices from other members.
- Join special-interest groups to have focused collaboration around a technology, use-case, vertical market or beta release
- Take online learning lessons and tutorials to broaden your knowledge of Gigamon products.

- Submit and vote on feature enhancements and share product feedback. (Customers only)
- Open support tickets (Customers only)
- Download the latest product updates and documentation (Customers only)

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

Register today at community.gigamon.com

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