Deploying the Visibility Platform for AWS

This guide describes how to deploy the Gigamon Visibility Platform solution on the Amazon Web Services (AWS) cloud.

Refer to the following sections for details:

- Licensing Information on page 5
- Introduction to GigaVUE-FM on page 5
- Architecture on page 6
- Before You Begin on page 7
- Launching the GigaVUE-FM Instance on page 12
- Installing the G-vTAP Agents on page 17

Licensing Information

Gigamon lets you purchase a license that is based on the number of TAP points and the term of the license. There are two types of licenses you can purchase:

- Traffic visibility for up to 100 virtual TAP points (ENIs)
- Traffic visibility for up to 1000 virtual TAP points (ENIs)

**NOTE:** The ENIs are selected randomly.

The minimum term for the license is 3 months and the maximum term is up to 12 months.

To purchase a new license, contact the Sales Department at Gigamon. For more information, refer to Contacting Sales on page 20.

Introduction to GigaVUE-FM

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 Gigamon Visibility Platform.
GigaVUE-FM integrates with the Amazon Elastic Cloud Compute (EC2) APIs and deploys the components of the Visibility Platform for AWS in the Virtual Private Cloud (VPC).

The Visibility Platform for AWS consists of the following AMIs:
- GigaVUE-FM
- GigaVUE V Series node
- GigaVUE V Series controller
- GigaVUE G-vTAP controller

This Visibility Platform is launched by subscribing to the Gigamon Visibility Platform for AWS in the AWS Marketplace or by launching the AMI from the Community AMIs. Once the Gigamon Visibility Platform for AWS instance is launched, the rest of the AMIs residing in the Community AMIs are automatically launched from GigaVUE-FM.

For detailed information about the components, refer to *Gigamon Visibility Platform for AWS Configuration Guide* in the Customer Portal.

This guide provides instructions on launching the GigaVUE-FM instance in AWS. For information about installing GigaVUE-FM in your enterprise data center, refer to the “Installation and Upgrade” section in the *GigaVUE-FM and GigaVUE-VM User’s Guide* available in the Customer Portal.

## Architecture

The Visibility Platform for AWS solution supports the following cloud deployment models:
- *Hybrid Cloud* on page 6
- *Multi-VPC Cloud* on page 7

### Hybrid Cloud

In the hybrid cloud deployment model, you can send the customized traffic to the tools in AWS as well as the tools in the enterprise data center.
Multi-VPC Cloud

In the public cloud deployment model, you can send the customized traffic from a single VPC to the tools residing in the same VPC or from multiple VPCs to the tools residing in a different VPC.

Before You Begin

You must create an account and configure a VPC as per your requirements. This section describes the requirements for launching the GigaVUE-FM AMI.

- **AWS Permissions and Policies** on page 7
- **AWS Security Credentials** on page 9
- **Network Requirements** on page 9
- **Security Group** on page 10
- **Key Pairs** on page 12

**AWS Permissions and Policies**

Before you begin configuring the components, your AWS account must have the following permissions and policies assigned to your account:

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

In addition, you must associate the following policies to your account:

---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*",
"cloudwatch:*",
"logs:*",
"sns:*",
"sqs:*",
"events:*

--- S3 Permissions
"s3:CreateBucket",
"s3:DeleteBucket",
"s3:DeleteObject",
"s3:DeleteObjectVersion",
"s3:Get",
"s3:ListAllMyBuckets",
"s3:PutBucketNotification",
"s3:PutBucketTagging",
"s3:PutBucketVersioning",
"s3:PutObject",
"s3:PutObjectTagging",
"s3:ReplicateDelete",
"s3:ReplicateObject",
"s3:RestoreObject"

--- IAM Permissions
"iam:PassRole"

**AWS Security Credentials**

You must have IAM role for GigaVUE-FM to connect to AWS. AWS uses IAM role to authenticate and authorize your requests. To obtain the IAM role, contact your AWS administrator.

**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

Table 1-1 on page 10 lists the three recommended subnets that your VPC must have to configure the Visibility Platform components in AWS.

Table 1-1:  Types of Subnets

<table>
<thead>
<tr>
<th>Subnet</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management Subnet</td>
<td>Subnet that the GigaVUE-FM uses to communicate with the GigaVUE V Series nodes and controllers.</td>
</tr>
<tr>
<td>Tunnel Subnet</td>
<td>Subnet that the GigaVUE V Series node uses to communicate with the monitoring tools that reside inside or outside of AWS, or GigaVUE H Series node that resides in your enterprise data center. The tunnel subnet can be the same as the management subnet.</td>
</tr>
<tr>
<td>Data Subnet</td>
<td>Subnet that receives the mirrored GRE tunnel traffic from the G-vTAP agents.</td>
</tr>
</tbody>
</table>

Elastic Network Interfaces (ENIs) for Instances

EC2 instances require a minimum of two Elastic Network Interfaces (ENIs). One ENI is used for carrying the traffic that you wish to monitor and the other ENI is used for mirroring the traffic to the GigaVUE V Series node.

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 V Series Controllers, GigaVUE 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.

Table 1-2 on page 10 lists the rules and port numbers for each component.

Table 1-2:  Security Group Rules

<table>
<thead>
<tr>
<th>Direction</th>
<th>Type</th>
<th>Protocol</th>
<th>Port Range</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>GigaVUE-FM Inside AWS</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inbound</td>
<td>HTTPS</td>
<td>TCP(6)</td>
<td>443</td>
<td>Used to communicate with GigaVUE-FM</td>
</tr>
<tr>
<td>G-vTAP Controller</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inbound</td>
<td>Custom TCP Rule</td>
<td>TCP(6)</td>
<td>9900</td>
<td>Used to communicate with GigaVUE-FM</td>
</tr>
<tr>
<td>G-vTAP Agent</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inbound</td>
<td>Custom TCP Rule</td>
<td>TCP(6)</td>
<td>9901</td>
<td>Used to communicate with G-vTAP agents</td>
</tr>
<tr>
<td>GigaVUE V Series Controller</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inbound</td>
<td>Custom TCP Rule</td>
<td>TCP(6)</td>
<td>9902</td>
<td>Used to communicate with GigaVUE V Series Controllers</td>
</tr>
<tr>
<td>GigaVUE V Series node</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inbound</td>
<td>Custom TCP Rule</td>
<td>TCP(6)</td>
<td>9903</td>
<td>Used to communicate with GigaVUE V Series nodes</td>
</tr>
</tbody>
</table>
NOTE: You must add the above port numbers as ranges when you are creating a security group. Refer to Figure 1-3 on page 12.

Creating a Security Group

To create an inbound security group:

1. In the Amazon EC2 dashboard, click Security Groups in the navigation pane.
2. Click Create Security Group.
3. Enter a name and description in the respective fields.
4. Select the ID of your VPC.

Table 1-2: Security Group Rules

<table>
<thead>
<tr>
<th>Direction</th>
<th>Type</th>
<th>Protocol</th>
<th>Port Range</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>GRE Traffic</td>
<td>Custom Protocol Rule</td>
<td>GRE (47)</td>
<td>ALL</td>
<td>Used to communicate with L2 GRE Tunnel to send monitored traffic</td>
</tr>
</tbody>
</table>
5. Click **Add Rule** and enter the details as shown in Figure 1-3 on page 12.

**NOTE:** The Source and CIDR must be entered according to your requirement.

![Table of Security Group Rules](image)

**Figure 1-3: Creating an Inbound Security Group**

6. Click **Create**.

**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 launch the G-vTAP Controllers, GigaVUE V Series nodes, and GigaVUE V Series Controllers in your VPC. Then, you must provide the private key to connect to these instances.

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

**Launching the GigaVUE-FM Instance**

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

1. Login to the AWS account.
3. In the **Search** field, type Gigamon and press **Enter**. Refer to Figure 1-4.

![Search for Gigamon on AWS Marketplace](image)

**Figure 1-4: Searching for Gigamon on AWS Marketplace**
4. Click the **Gigamon Visibility Platform for AWS** link to view the complete details about the product. Refer to **Figure 1-5**.

**Figure 1-5: Gigamon Visibility Platform for AWS page in AWS Marketplace**

5. Click **Continue**. The Launch page is displayed. Refer to **Figure 1-6**.

**Figure 1-6: Launch on EC2 Page**
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. By default, the Deploy a VPC for Gigamon Fabric Manager option is selected.

d. Click the Accept Software Terms button to subscribe to the Gigamon Visibility Platform for AWS software. A message is displayed to confirm the subscription. Refer to Figure 1-7. Click Return to Launch Page.

![Subscription Confirmation Page]

**Figure 1-7: Subscription Confirmation 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. Refer to Figure 1-8.

Figure 1-8: Select Template Page
7. In the Select Template page, the Gigamon Fabric Manager CloudFormation template is selected by default. Click Next. The Specify Details page is displayed. Refer to Figure 1-9.

![Figure 1-9: Specify Details Page]

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: The t2 instance types 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 SSH to lock down the SSH access to the Gigamon FM instance.
   h. In the CIDR IP, enter a CIDR block to associate with the instance and click Next.

9. 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.
    Wait for few minutes for the GigaVUE-FM instance to launch in the VPC.
Installing the G-vTAP Agents

G-vTAP agent is an agent that is deployed in the Elastic Compute Cloud (EC2) instance. This agent mirrors the selected traffic from the instances to the GigaVUE® V Series node.

Before installing the G-vTAP agents, launch an AMI with at least two Elastic Network Interfaces (ENIs). The AMI must have sudo/root access. You may need to modify the network configuration files to make sure that the extra ENI will initialize at boot time.

You can install the G-vTAP agents either from Debian or RPM packages as follows:

- *Installing from an Ubuntu/Debian Package*
- *Installing from an RPM package*

Installing from an Ubuntu/Debian Package

To install from a Debian package:

1. Download the G-vTAP Agent Debian (.deb) package from the following location:
   
   https://s3.amazonaws.com/gvtap-agent/1.2-1/gvtap-agent_1.2-1_amd64.deb

2. Copy this package to your instance. Install the package with root privileges, for example:

   ```
   ubuntu@ip-10-0-0-246:~$ ls gvtap-agent_1.2-1_amd64.deb
   ubuntu@ip-10-0-0-246:~$ sudo dpkg -i gvtap-agent_1.2-1_amd64.deb
   ```
3. Once the G-vTAP package is installed, modify the file /etc/gvtap-agent/gvtap-agent.conf to configure and register the source and destination interfaces. The file contains an example, which you can use by uncommenting the last two lines. The following example registers eth0 as the mirror source for both ingress and egress traffic and eth1 as the destination for this traffic:

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

4. Save the file.

5. Reboot the instance.

The instance should have two interfaces. The G-vTAP agent status will be displayed as running. Check the status using the following command:

```
ubuntu@ip-10-0-0-246:~$ sudo service gvtap-agent status
G-vTAP Agent is running
```

### Installing from an RPM package

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

1. Download the G-vTAP Agent RPM (.rpm) package from the following location: https://s3.amazonaws.com/gvtap-agent/1.2-1/gvtap-agent_1.2-1_x86_64.rpm

2. Copy this package to your instance. Install the package with root privileges, for example:

   ```
   [ec2-user@ip-10-0-0-214 ~]$ ls
   gvtap-agent_1.2-1_x86_64.rpm
   [ec2-user@ip-10-0-0-214 ~]$ sudo rpm -i gvtap-agent_1.2-1_x86_64.rpm
   ```

3. Modify the file /etc/gvtap-agent/gvtap-agent.conf to configure and register the source and destination interfaces. The file contains an example, which you can use by uncommenting the last two lines. The following example registers the eth0 as the mirror source for both ingress and egress traffic and registers eth1 as the destination for this traffic as follows:

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

4. Save the file.

5. Reboot the instance.

Check the status with the following command:

```
[ec2-user@ip-10-0-0-214 ~]$ sudo service gvtap-agent status
G-vTAP Agent is running
```

If you want to avoid downloading and installing the G-vTAP agents every time there is a new instance to be monitored, you can save the G-vTAP agent running on an instance
as a private AMI. When a new G-vTAP agent is launched in an instance, GigaVUE-FM automatically updates the number of monitoring instances in the monitoring session.

To save the G-vTAP agent as an AMI:
1. From the EC2 console, right click the instance.
2. Click **Image > Create Image**.

Launch the G-vTAP agent AMI with **t2 medium** as the instance type. Also, add a second ENI which will be used as a mirror subnet. For more information, refer to *Gigamon Visibility Platform for AWS Configuration Guide*.

**Pre-Configuration Checklist**

Table 1-3 on page 19 provides information that you must obtain to ensure a successful and efficient configuration of the Visibility Platform for AWS using the GigaVUE-FM user interface:

<table>
<thead>
<tr>
<th>Required Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPC ID</td>
</tr>
<tr>
<td>Instance ID of the GigaVUE-FM</td>
</tr>
<tr>
<td>Public or Private IP of the GigaVUE-FM</td>
</tr>
<tr>
<td>Elastic IP</td>
</tr>
<tr>
<td><strong>NOTE:</strong> This is required only if GigaVUE-FM is in the enterprise data center.</td>
</tr>
<tr>
<td>Region name for the VPC</td>
</tr>
<tr>
<td>Availability zone of the VPC</td>
</tr>
<tr>
<td>IAM role name OR Access key ID and Secret Access key</td>
</tr>
<tr>
<td>SSH Key Pair</td>
</tr>
<tr>
<td>Subnets</td>
</tr>
<tr>
<td>Security groups</td>
</tr>
</tbody>
</table>

**Next Steps**

After launching the GigaVUE-FM AMI in your VPC, you can use the GigaVUE-FM user interface for configuring the Visibility Platform for AWS components and setting up the monitoring sessions for filtering the traffic. For detailed information, refer to *Gigamon Visibility Platform for AWS Configuration Guide*.
Documentation

Gigamon provides additional documentation for this solution on the Gigamon Customer Portal.

<table>
<thead>
<tr>
<th>Document</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gigamon Visibility Platform for AWS Configuration Guide</td>
<td>Provides information about configuring the Visibility Platform for AWS and its components, and setting up the monitoring sessions.</td>
</tr>
<tr>
<td>GigaVUE-FM and GigaVUE VM User’s Guide</td>
<td>Describes how to install, deploy, and operate the GigaVUE® Fabric Manager (GigaVUE-FM) and GigaVUE® Virtual Manager (GigaVUE-VM) from Gigamon® Inc.</td>
</tr>
</tbody>
</table>

Contacting Sales

Table i shows how to reach the Sales Department at Gigamon.

Table i: Sales Contact Information

<table>
<thead>
<tr>
<th>Telephone</th>
<th>+1 408.831.4025</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sales</td>
<td><a href="mailto:inside.sales@gigamon.com">inside.sales@gigamon.com</a></td>
</tr>
</tbody>
</table>