GigaSECURE® Cloud for Azure Getting Started Guide

Version 5.3.01

DOCUMENT REVISION – 4/6/18

Contents

Deploying GigaSECURE® Cloud for Azure

This guide describes how to deploy the GigaSECURE® Cloud solution on the Microsoft® Azure cloud.

Refer to the following sections for details:

Licensing Information

The GigaSECURE® Cloud is available in both the public Azure cloud and in Azure Government, and supports the Bring Your Own License (BYOL) model and the hourly Pay-As-You-Go (PAYG) model that you can avail from the Azure Marketplace.

Bring Your Own License (BYOL)

The licenses for the BYOL option can be purchased based on the number of TAP points and the term of the license. Gigamon offers the following options for purchasing the license:

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

NOTE: Make sure you purchase a licensing option that can provide traffic visibility to all the TAP points in the VNet. If the licensing option cannot support all the TAP points, the NICs are selected randomly for monitoring the traffic.

The minimum term for the license is 3 months.

A free trial is made available in the Azure Marketplace. The trial version provides traffic visibility for up to 10 virtual TAP points for 30 days. When a

new license is purchased, the 10 virtual TAP points are replaced with how many ever TAP points the licensing option supports.

For purchasing licenses with the BYOL option, contact our Gigamon Sales. Refer to *Contacting Sales* on page 16.

Pay-As-You-Go (PAYG)

The Pay-As-You-Go (PAYG) option is available in the Azure Marketplace. The PAYG option charges the users for the Azure services availed on an hourly basis. For example, Azure charges the users for the period the GigaVUE-FM VM and the rest of the solution components are running. When the VMs stop, Azure stops charging the users. The PAYG model has no term contract.

It is a perpetual license that supports up to 100 TAP points. To support additional TAP points, licenses must be purchased from Gigamon.

For purchasing licenses with the PAYG option, contact the Gigamon Sales. Refer to *Contacting Sales* on page 16.

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. GigaVUE-FM is a key component of the GigaSECURE® Cloud solution.

GigaVUE-FM integrates with the Azure APIs and deploys the components of the GigaSECURE® Cloud in an Azure Virtual Network (VNet).

The GigaSECURE® Cloud for Azure consists of the following components:

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

This solution is launched by subscribing to the GigaSECURE® Cloud for Azure in the Azure Marketplace. Once the GigaVUE-FM VM is launched in Azure, the rest of the solution components are launched from GigaVUE-FM.

This guide provides instructions on launching GigaVUE-FM in Azure. 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 GigaSECURE® Cloud for Azure solution supports many deployment modes. The following cloud deployment models are the most common:

- *Hybrid Cloud* on page 6
- *Multi-VNet Cloud* on page 7

Hybrid Cloud

In the hybrid cloud deployment model, you can send the customized traffic to the tools in Azure as well as the tools in the enterprise data center.

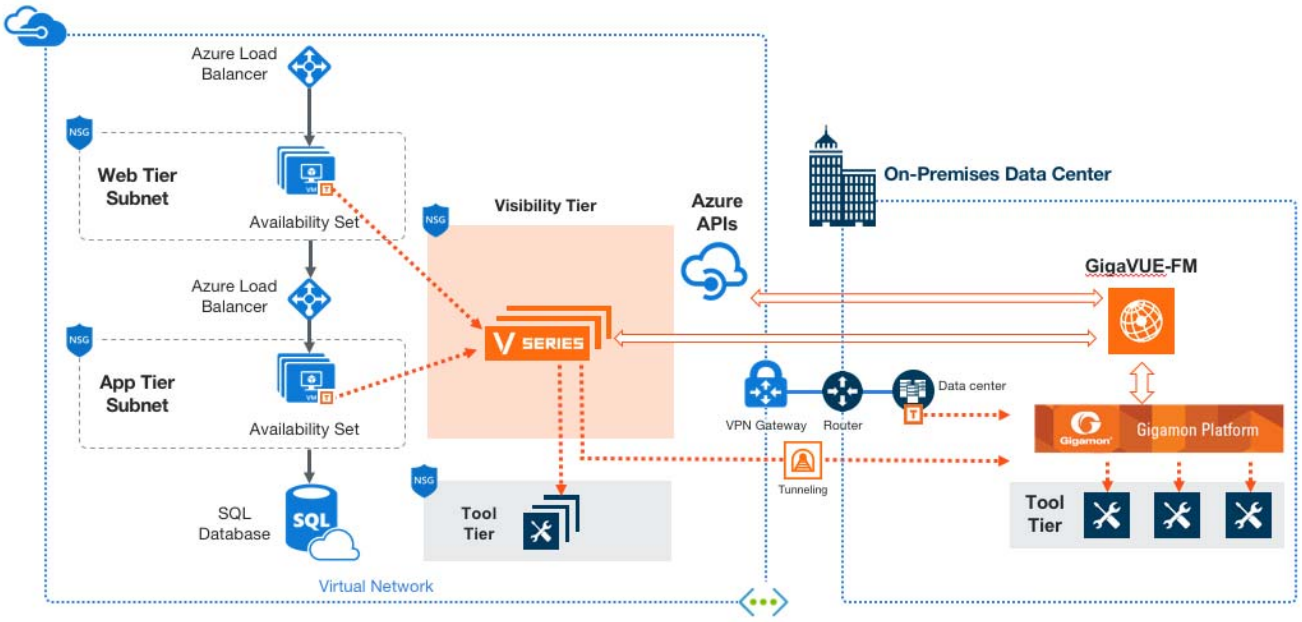

Figure 1-1: Hybrid Cloud Deployment

Multi-VNet Cloud

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

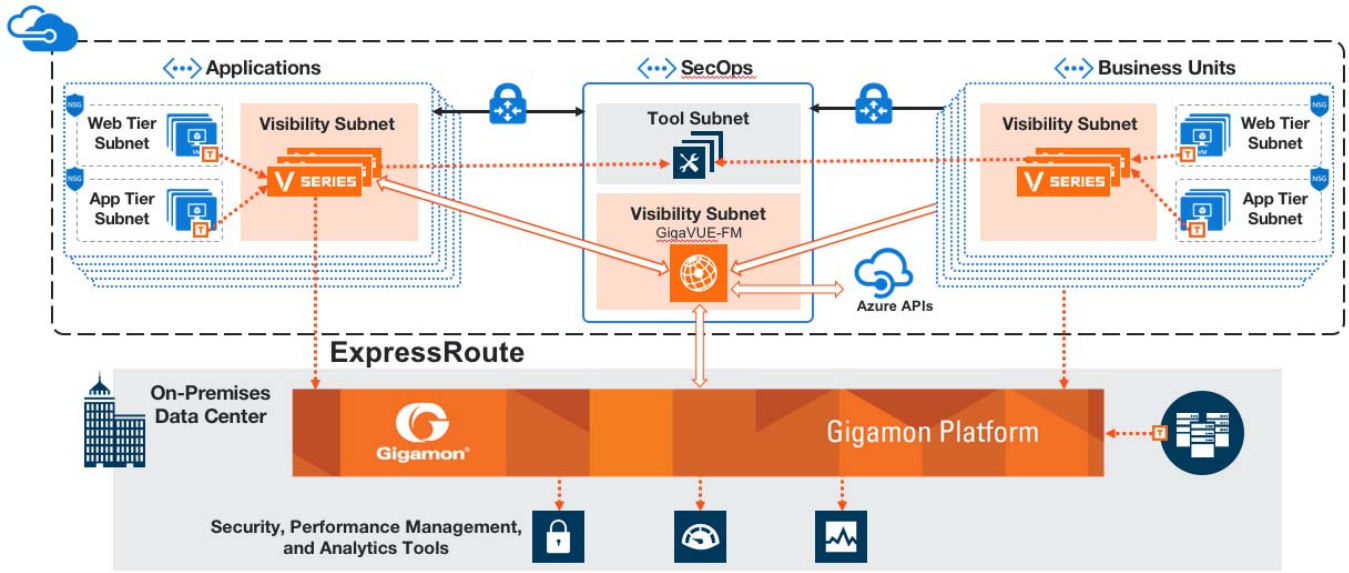

Figure 1-2: Public Cloud Deployment

Before You Begin

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

- *Network Requirements* on page 7
- *Network Security Groups* on page 8

Network Requirements

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

- *Subnets for VNet*
- *Network Interfaces (NICs) for VMs*

Subnets for VNet

Table 1-1 on page 8 lists the two recommended subnets that your VNet must have to configure the GigaSECURE® Cloud components in Azure.

Table 1-1: Types of Subnets

Subnet	Description
Management Subnet	Subnet that the GigaVUE-FM uses to communicate with the GigaVUE V Series nodes and controllers.
Data Subnet	A data subnet can accept incoming mirrored traffic from agents to the GigaVUE V Series nodes or be used to egress traffic to a tool from the GigaVUE V Series nodes. • Ingress is VXLAN from agents • Egress is either VXLAN tunnel to tools or to GigaVUE H Series tunnel port, or raw packets through a NAT when using NetFlow. **NOTE:** If using a single subnet, the Management subnet will also be used as a Data Subnet

Network Interfaces (NICs) for VMs

For G-vTAP agents to mirror the traffic from the VMs, you must configure one or more Network Interfaces (NICs) on the VMs.

- **Single** NIC—If there is only one interface configured on the VM with the G-vTAP agent, the G-vTAP agent sends the mirrored traffic out using the same interface.
- **Multiple NICs**—If there are two or more interfaces configured on the VM 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.

Network Security Groups

A network security group defines the virtual firewall rules for your VM 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 VNet, you add rules that control the inbound traffic to VMs, 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 Table 1-2 on page 8.

Table 1-2: Security Group Rules

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

Table 1-2: Security Group Rules

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

Obtaining the Image

The image for the GigaSECURE® Cloud is available in both the Azure Public Cloud and in Azure Government.

GigaSECURE® Cloud in Azure Public Cloud

GigaSECURE® Cloud is available in the Azure Marketplace for both the Bring Your Own License (BYOL) and the Pay-As-You-Go (PAYG) options.

GigaSECURE® Cloud in Azure Government

Azure Government is an isolated Azure region that contains specific regulatory and compliance requirements of the US government agencies.

To monitor the VMs that contain all categories of Controlled Unclassified Information (CUI) data and sensitive government data in the Azure Government (US) Region, the

Azure Government solution provides the same robust features in Azure Government as in the Azure public cloud.

Installing the G-vTAP Agents

A **G-vTAP agent** is an agent that is deployed in the VMs. This agent mirrors the selected traffic from the VMs (virtual machines), encapsulates it using GRE or VXLAN tunneling, and forwards it to the GigaVUE® V Series node.

A G-vTAP agent consists of a source interface and a destination interface. The network packets collected from the source interface are sent to the destination interface. From the destination interface, the packets traverse through the L2 GRE or VXLAN tunnel interface to the GigaVUE V Series node.

A source interface can be configured with one or more NICs. While configuring a source interface, you can specify the direction of the traffic to be monitored in the VM. The direction of the traffic can be egress or ingress or both.

Linux Agent Installation

Refer to the following sections for the Linux agent installation:

- *Single NIC Configuration* on page 10
- *Dual NIC Configuration* on page 11
- *Installing the G-vTAP Agents* on page 11
- *Installing the G-vTAP Debian Package* on page 11
- *Installing the G-vTAP RPM package* on page 12

Then refer to *Creating Images with the Agent Installed* on page 13.

Single NIC Configuration

A single NIC acts both as the source and the destination interface. A G-vTAP agent with a single NIC configuration lets you monitor the ingress or egress traffic from the NIC. The monitored traffic is sent out using the same NIC.

For example, assume that there is only one interface eth0 in the monitoring VM. In the G-vTAP configuration, you can configure eth0 as the source and the destination interface, and specify both egress and ingress traffic to be selected for monitoring purpose. The egress and ingress traffic from eth0 is mirrored and sent out using the same interface.

Using a single NIC as the source and the destination interface can sometimes cause increased latency in sending the traffic out from the VM.

Example of the G-vTAP config file for a single NIC configuration:

Example—Grant permission to monitor ingress and egress traffic at iface

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

Dual NIC Configuration

A G-vTAP agent lets you configure two NICs. One NIC can be configured as the source interface and another NIC can be configured as the destination interface.

For example, assume that there is eth0 and eth1 in the monitoring VM. In the G-vTAP agent configuration, eth0 can be configured as the source interface and egress traffic can be selected for monitoring purpose. The eth1 interface can be configured as the destination interface. So, the mirrored traffic from eth0 is sent to eth1. From eth1, the traffic is sent to the GigaVUE V Series node.

Example of the G-vTAP config file for a dual NIC configuration:

Example—Grant permission to monitor ingress and egress traffic at iface

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

Installing the G-vTAP Agents

You must have sudo/root access to edit the G-vTAP agent configuration file.

For dual or multiple NIC configuration, you may need to modify the network configuration files to make sure that the extra NIC will initialize at boot time.

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

- *Installing the G-vTAP Debian Package*
- *Installing the G-vTAP RPM package*

Installing the G-vTAP Debian Package

To install from a Debian package:

1. Download the G-vTAP Agent Debian (.deb) package.
2. Copy this package to your VM. Install the package with root privileges, for example:

   ```
   ubuntu@ip-10-0-0-246:~$ ls gvtap-agent_1.4-1_amd64.deb
   ubuntu@ip-10-0-0-246:~$ sudo dpkg -i
      gvtap-agent_1.4-1_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.

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

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

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

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

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

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

4. Save the file.
5. Reboot the VM.

   The G-vTAP agent status will be displayed as running. Check the status using the following command:

   ```
   ubuntu@ip-10-0-0-246:~$ sudo /etc/init.d/gvtap-agent status
   G-vTAP Agent is running
   ```

Installing the G-vTAP 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.
2. Copy this package to your VM. Install the package with root privileges, for example:

   ```
   [VM-user@ip-10-0-0-214 ~]$ ls
   gvtap-agent_1.4-1_x86_64.rpm
   [VM-user@ip-10-0-0-214 ~]$ sudo rpm -i
      gvtap-agent_1.4-1_x86_64.rpm
   ```

3. Modify the file /etc/gvtap-agent/gvtap-agent.conf to configure and register the source and destination interfaces.

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

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

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

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

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

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

4. Save the file.
5. Reboot the VM.

   Check the status with the following command:

   ```
   [VM-user@ip-10-0-0-214 ~]$ sudo /etc/init.d/gvtap-agent
   status
   G-vTAP Agent is running
   ```

Windows Agent Installation

To install the Windows agent:

1. Download the Windows agent package.
2. Extract the contents of the .zip file into a convenient location.
3. Right-click 'WinPcap_4_1_3.exe' (located in the 'winpcap' folder) and select and select **Run as Administrator**.
4. Right-click 'install.bat' and select **Run as Administrator**.
5. If you want to start the Windows G-vTAP agent, you may do one of the following:
   - Reboot the VM.
   - Run 'sc start gvtap' from the command prompt.
   - Start the G-vTAP Agent from the Task Manager.
6. If you want to build an Azure image, create the image, now.

Next, refer to *Creating Images with the Agent Installed* on page 13.

Creating Images with the Agent Installed

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

To save the G-vTAP agent as an image:

1. From the Azure console, click the VM.
2. Click **Image** > **Create Image**.
3. There may be extra steps required from Azure to deprovision the VM. Refer to Azure documentation for capturing an image: https://docs.microsoft.com/en-us/azure/virtual-machines/linux/capture-image.

Launching GigaVUE-FM

The GigaVUE-FM VM can be launched from the Azure VM dashboard or Azure Marketplace. The following instructions describe launching the GigaVUE-FM VM from the Azure VM Dashboard.

Launching the GigaVUE-FM VM from the Azure VM Dashboard

This section describes how to launch the GigaVUE-FM VM in your VNet.

To launch the GigaVUE-FM VM:

1. Login to the Azure portal and select **Virtual Machines**.

2. Click **Add** and in the Compute tile, search for Gigamon.
3. Locate the latest version of the GigaVUE-FM, click and create.
4. Enter the Basic settings.
   a. Choose either the **SSH public key** or **password authentication type for SSH access**.
   b. Select the appropriate **Subscription** and **Location**.
5. Choose the Virtual Machine size.
   a. The recommended VM type is **D4S_V3 Standard**.
   b. Click **Select**.
6. Select the appropriate **Virtual Network** (VNet), **Subnet**, and **Public IP Address**. Select the **Network Security Group** created to allow the GigaVUE-FM to communicate with the rest of the components.

   Click **Ok**.
7. Verify the summary and click **Create**.
8. It will take several minutes for the VM to initialize. After the initialization is completed, you can verify the VM through the Web interface as follows:
   a. Find your VM and expand the page in the Descriptions tab to view the VM information.
   b. Copy the Public DNS value and paste it into a new browser window or tab.
   c. If GigaVUE-FM is deployed in Azure, use admin123A! as the password for the admin user to login to GigaVUE-FM. It is highly recommended to change the password after logging in to GigaVUE-FM.

NOTE: For security reasons, it is **highly recommended** to change the password after logging in to GigaVUE-FM.

Configuring the GigaSECURE Cloud Components in Azure

You must establish a connection between GigaVUE-FM and your Azure environment before you can perform the configuration steps. After a connection is established, you will be able to use GigaVUE-FM to specify a launch configuration for the G-vTAP Controllers, GigaVUE V Series Controllers, and GigaVUE V Series nodes in the specified VNet and Resource Groups.

Pre-Configuration Checklist

Table 1-3 on page 15 provides information that you must obtain to ensure a successful and efficient configuration using the GigaVUE-FM user interface:

Table 1-3: Pre-configuration Checklist

	Required Information
☐	VNet ID(s)
☐	Resource Group ID(s)
☐	VM ID of the GigaVUE-FM
☐	Public or Private IP of the GigaVUE-FM
☐	Static Public IP **NOTE:** If GigaVUE-FM is installed in the enterprise data center, a Public IP is required for G-vTAP controllers and GigaVUE V Series controllers to communicate with GigaVUE-FM
☐	Region name for the VNet
☐	Application ID, Tenant ID, Application Secret and Subscription ID
☐	SSH Key Pair
☐	Subnets
☐	Network Security groups

Azure Connectivity for GigaVUE-FM

When you first connect GigaVUE-FM with Azure, you need the appropriate authentication for Azure to verify your identity and check if you have permission to access the resources that you are requesting. This is used for the GigaVUE-FM to integrate with Azure APIs and automate the fabric deployment and management. GigaVUE-FM supports two types of authentication with Azure:

- **Application ID with client secret**—GigaVUE-FM supports application id with client secret authentication. When using GigaVUE-FM to connect to Azure, it uses a service principal. A service principal is an account for a non-human such as an application to connect to Azure. The key fields required for GigaVUE-FM to connect to Azure are: Subscription ID, Tenant ID, Application ID and Application Secret
  - When creating the service principal using the Azure CLI, the output of that command will display the "appId" and "password" fields. These two are the Application ID and Application Secret fields that are required for GigaVUE-FM to connect to Azure. Copy them.
  - Now, using the Azure CLI again, do an ‘account show’ command and copy the Subscription ID and the Tenant ID of your subscription.
- **Managed Service Identity**—Managed Service Identity (MSI) is a feature of Azure Active Directory. When you enable MSI on an Azure service, Azure automatically creates an identity for the service VM in the Azure AD tenant used by your Azure subscription.

- Enable MSI for the GigaVUE-FM VM by using the Azure CLI command:

```
az vm assign-identity -g <Resource group where FM is deployed> -n
<GigaVUE-FM name>
```

The above command enables MSI for the GigaVUE-FM for the entire subscription. If more restrictions are needed, use "`-scope <resource group id>`" as an extension to the command to restrict the MSI permissions for GigaVUE-FM to a resource group.

Connecting to Azure

GigaVUE-FM connects to Azure using either an Application ID with the client secret or the MSI method of authentication. Once the connection is established, GigaVUE-FM launches the G-vTAP Controller, GigaVUE V Series Controller, and GigaVUE V Series node.

To connect to Azure using GigaVUE-FM:

1. Click **Cloud** in the top navigation link.
2. Under Azure, select **Configuration > Connections**, and then click **New**.
3. Enter or select the appropriate information for the VNet and one or more Resource Groups.

   If the Authentication type of Application ID with Client Secret is used, have the **Subscription ID**, **Tenant ID**, **Application ID** and **Application Secret** information ready based on the Azure connectivity section mentioned above. Click **Save**.
4. If the connection is established, the status is displayed as 'Connected' in the Connections page. GigaVUE-FM discovers the inventory of the VNet in the background. If the connection fails, a 'Connection Failed' error message is displayed when **Save** is clicked.

Once the configuration in the Connections tab is complete, the rest of the tabs under *Cloud > Azure > Configuration* can be configured so that GigaVUE-FM can deploy the rest of the solution components. As a final step, configure the monitoring session.

Contacting Sales

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

Table i: Sales Contact Information

Telephone	+1 408.831.4025
Sales	inside.sales@gigamon.com