



GigaMon's GigaVue: Monitoring Azure with MistNet NDR

April 07, 2022

© LogRhythm, Inc. All rights reserved.

This document contains proprietary and confidential information of LogRhythm, Inc., which is protected by copyright and possible non-disclosure agreements. The Software described in this Guide is furnished under the End User License Agreement or the applicable Terms and Conditions (“Agreement”) which governs the use of the Software. This Software may be used or copied only in accordance with the Agreement. No part of this Guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than what is permitted in the Agreement.

Disclaimer

The information contained in this document is subject to change without notice. LogRhythm, Inc. makes no warranty of any kind with respect to this information. LogRhythm, Inc. specifically disclaims the implied warranty of merchantability and fitness for a particular purpose. LogRhythm, Inc. shall not be liable for any direct, indirect, incidental, consequential, or other damages alleged in connection with the furnishing or use of this information.

Trademark

LogRhythm is a registered trademark of LogRhythm, Inc. All other company or product names mentioned may be trademarks, registered trademarks, or service marks of their respective holders.

LogRhythm Inc.
4780 Pearl East Circle
Boulder, CO 80301
(303) 413-8745
www.logrhythm.com

Phone
Support (7am - 6pm, Monday-Friday)
Toll Free in North America
(MT) +1-866-255-0862
Direct Dial in the Americas
(MT) +1-720-407-3990
EMEA (GMT) +44 (0) 844 3245898
META (GMT+4) +971 8000-3570-4506
APAC (SGT) +65 31572044

Table of Contents

Overview	4
Integration Checklist.....	4
Prerequisites	5
Configuration Steps	5
Integration Installation.....	5
Configure MistNet Sensor	8
Troubleshooting.....	9
Resources	9

Overview

To capture network traffic in Azure, a 3rd party network traffic capture solution, such as GigaMon's GigaVue, must be used. By leveraging GigaMon's technology in Azure, the LogRhythm MistNet NDR can successfully capture network activity and detect threats in the monitored Azure environment.

Integration Checklist

Device/Application Name	GigaVue Cloud Suite for Azure
Vendor	GigaMon
Device/Application Type	Network Traffic Capture Solution
Supported Model Name/Number	Cloud Suite for Azure
Supported Software Version	5.14.00 or newer
Collection Method	
Configurable Log Output	
Log Source Type	
Log Processing Policy	
Exceptions	
Additional Information	
Document Status	FINAL
Document Owner	Jake Haldeman - Channel Sales Engineer Ewa Sobon - Technical Writer

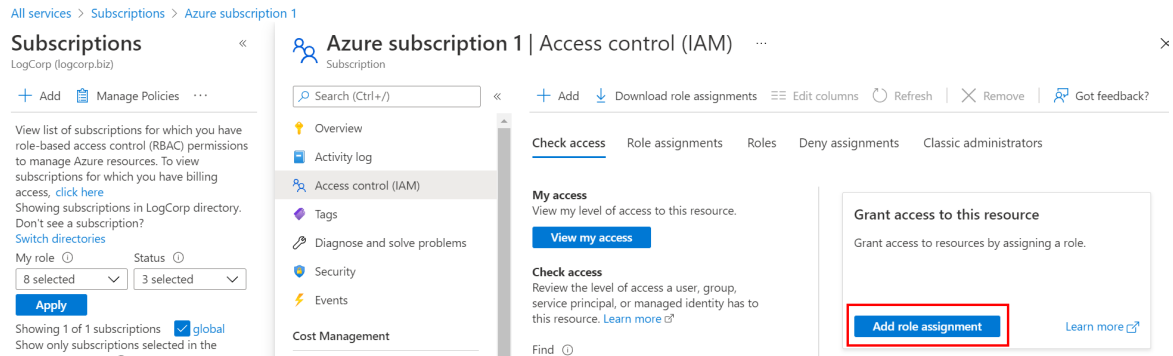
Prerequisites

Prerequisite	Details	Link
Type of Integration		
Supported Operating Systems		
Supported Software & Versions		
Authentication Credentials		
Required Software Prior to Integration	<ul style="list-style-type: none">• GigaMon G-vTAP on each host to monitor traffic• MistNet NDR	

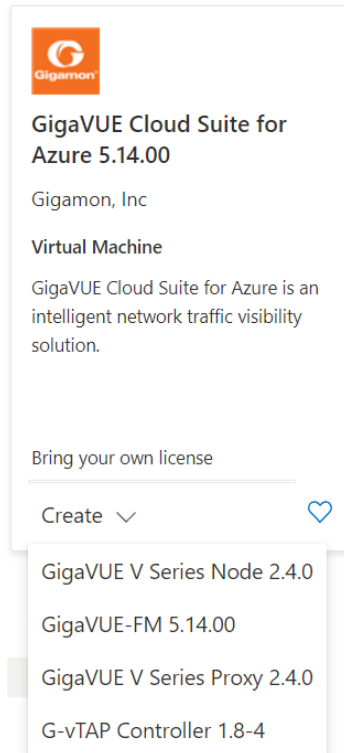
Configuration Steps

Integration Installation

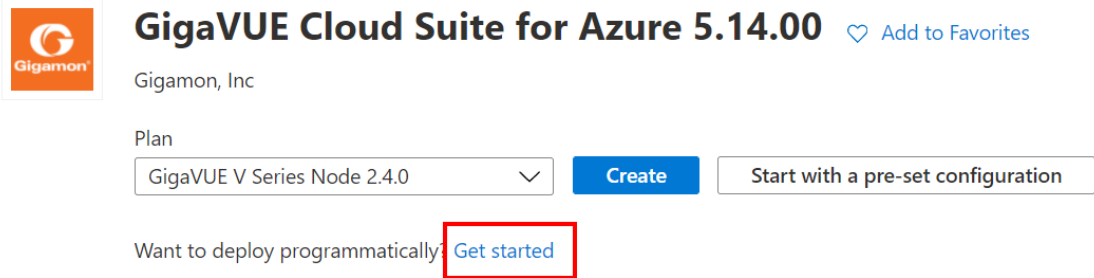
1. Deploy GigaVue-FM.
 - a. Deploy GigaMon's GigaVue Cloud Suite for Azure 5.14.00's GigaVue-FM from the Azure Marketplace.
 - b. Refer to GigaMon's documentation for proper sizing - in this evaluation, the suggested default virtual machine (VM) sizes were used.
2. Once the VM has been deployed, the permissions to access details within the Azure Subscription or Resource Group will be needed.
 - a. In the Azure Portal, navigate to the **Subscription** or **Resource Group** to which access is needed.
 - b. Select the **Access control (IAM)** section and select **Add role assignment** to assign permissions to the VM.



- c. In this configuration, the GigaMon-FM instance was given "Owner" level access to the subscription. For hardening guidance, refer to the GigaMon documentation.
- 3. Power on the GigaVue-FM instance (if not already powered up).
- 4. Enable Programmatic Deployments of the g-vTap controller and GigaVue V Series Node.
 - a. Locate the GigaVue Cloud Suite for Azure in the Marketplace.
 - b. Select the component that programmatic deployments must be enabled for (Node, G-vTap Controller).



- c. On the details page, select **Get Started**.



GigaVUE Cloud Suite for Azure 5.14.00 [Add to Favorites](#)

Gigamon, Inc

Plan

GigaVUE V Series Node 2.4.0

Want to deploy programmatically? [Get started](#)

d. Change the **Status** to **Enabled** for the areas where GigaMon will be deployed.

Choose the subscriptions

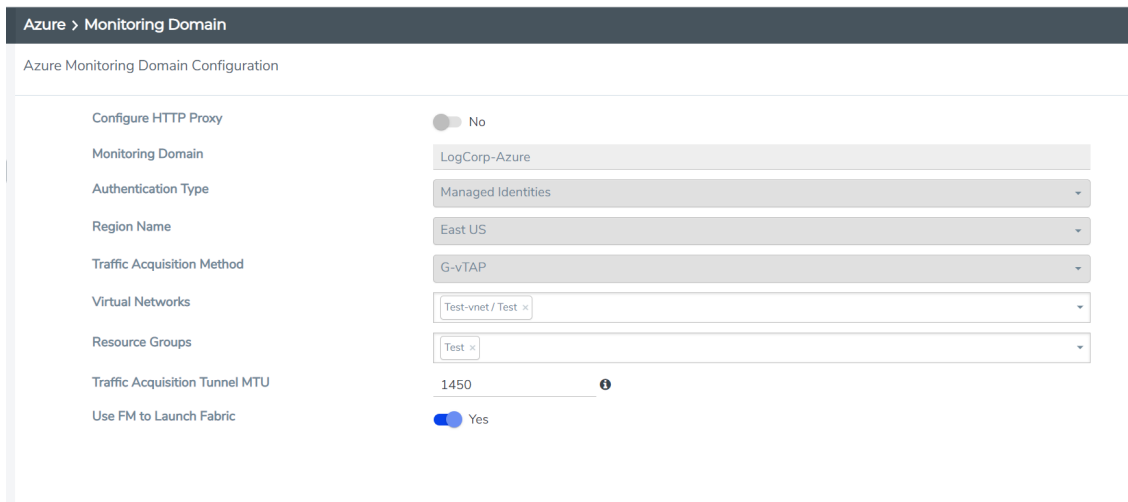
Select the Azure subscriptions for which you would like to enable programmatic deployments of the above offering(s)

Subscription Name	Subscription ID	Status
Azure subscription 1	69b25131-7007-4abc-b952-cae4ebb6...	<input type="button" value="Enable"/> <input type="button" value="Disable"/>

e. Repeat this for the services components described above.

Configure GigaVue-FM

1. Create a **Monitoring Domain** under the Azure section
2. Settings used for this instance are seen below.



Azure > Monitoring Domain

Azure Monitoring Domain Configuration

Configure HTTP Proxy No

Monitoring Domain LogCorp-Azure

Authentication Type Managed Identities

Region Name East US

Traffic Acquisition Method G-vTAP

Virtual Networks Test-vnet / Test

Resource Groups Test

Traffic Acquisition Tunnel MTU 1450 ⓘ

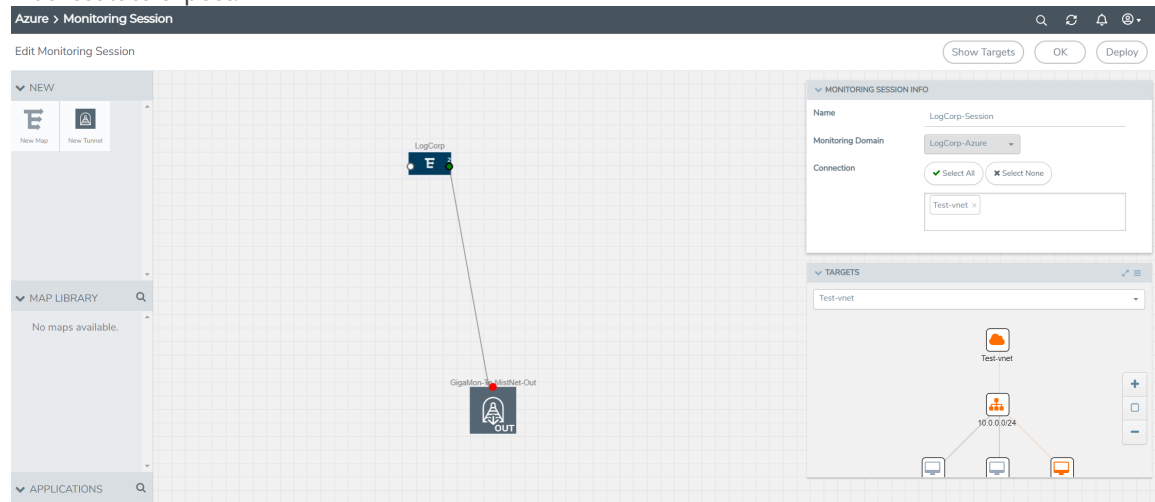
Use FM to Launch Fabric Yes

- a. Ensure the Virtual Networks and Resource Groups that were selected are the ones that will be included in the traffic capturing and the VM has permission to see those segments.
 - b. In the process of setting up the Monitoring Domain, the GigaVue-FM will attempt to deploy a vTap and Node to capture and manage the traffic. Depending on the Azure configuration, CPU quotas may need to be increased to run these servers.
3. Install the vTap agent on the servers that traffic will be captured from - this is an agent that must be installed on the operating system to properly capture the network traffic.
 4. To setup a Monitor Session in GigaVue-FM,

- Navigate to **Azure Orchestration** and create a new **Monitoring** session
- Drag a **New Map** to the working space and configure the include filters to meet the needs of the session. For this testing session, all IPv4 traffic was sent.
- Drag a **New Tunnel** to the working space to configure. The following represents what configurations were used for this instance. (Note: Update the Remote Tunnel IP to be the IP of the MistNet server being used.)

X Tunnel	
Alias	GigaMon-To-MistNet-Out
Description	Description (optional)
Type	VXLAN
Traffic Direction	Out
Remote Tunnel IP	10.0.0.9
MTU	1500
Time to Live	64
DSCP	0
Flow Label	0
VxLan Network Identifier	100
Source L4 Port	8080
Destination L4 Port	4789

- Once created, drag a line from the map to the tunnel. Refer to the following screenshot for an example of what result to expect.



- Note: The **Targets** section on the right will highlight in **orange** what is being seen by the GigaMon deployment. If nothing is **orange**, the GigaMon deployment will need to be reviewed for errors.

Configure MistNet Sensor

- SSH into the sever that will host the Mistnet NDR software.
- Referencing the settings used to create the Tunnel (Configure GigaVue-FM 4c), run the following commands making sure to change the VXLAN ID and port to what was configured.


```
sudo ip link add vxlan100 type vxlan id 100 dstport 4789
sudo ip link set up dev vxlan100
```

3. To test and confirm that traffic is being received to the MistNet sensor, run the following command:

```
sudo tcpdump -i vxlan100
```

4. If traffic being generated on the hosts is seen with the vTap software installed, then the GigaMon product to forward traffic to LogRhythm's MistNet NDR was successfully configured. Confirm that MistNet setup, as defined in the documentation, has been completed prior to handing off to the LogRhythm SRE team to onboard the new sensor.

Troubleshooting

Resources