Gigamon Validated Design

GigaVUE Cloud Suite for Nutanix

Organizations have heterogeneous workloads in the form of physical, virtual, cloud containers, and more specifically the adoption of cloud has been a drastic and ever-increasing due to various advantages. Cloud provides scaling, faster provisioning, elastic computing based on varying loads, almost non-existent capital expense to name a few in the case of Public Cloud; total control over data security and availability in case of Private cloud. There are some inhibitors to adopt cloud on all the considerations before deciding the right form of workload and security, thus visibility is a major factor. Security infrastructure is usually deployed in a layered approach often referred as “defense in depth” to both safeguard their assets and meet regulatory requirements, resulting in deployment of tools such as IDS, DLP, APM etc.

GigaVUE® Cloud Suite for Nutanix provides a centralized platform that lets network and security teams acquire, optimize and deliver the right kind of traffic to one or many tools for data deployed within Nutanix HCI implementation on acropolis hypervisor (AHV).

With the Gigamon solution ecosystem, you can:

- **Acquire:** Extending visibility across virtual environments and eliminating traffic blind spots across the enterprise resulting in pervasive visibility by acquiring and forwarding VM network traffic to the existing security and network monitoring tools, regardless of the location.
- **Optimize:** Leverage the GigaVUE HC Series appliances to supplement your Network and Security functions with rich insights using GigaSMART Application and Traffic intelligence.

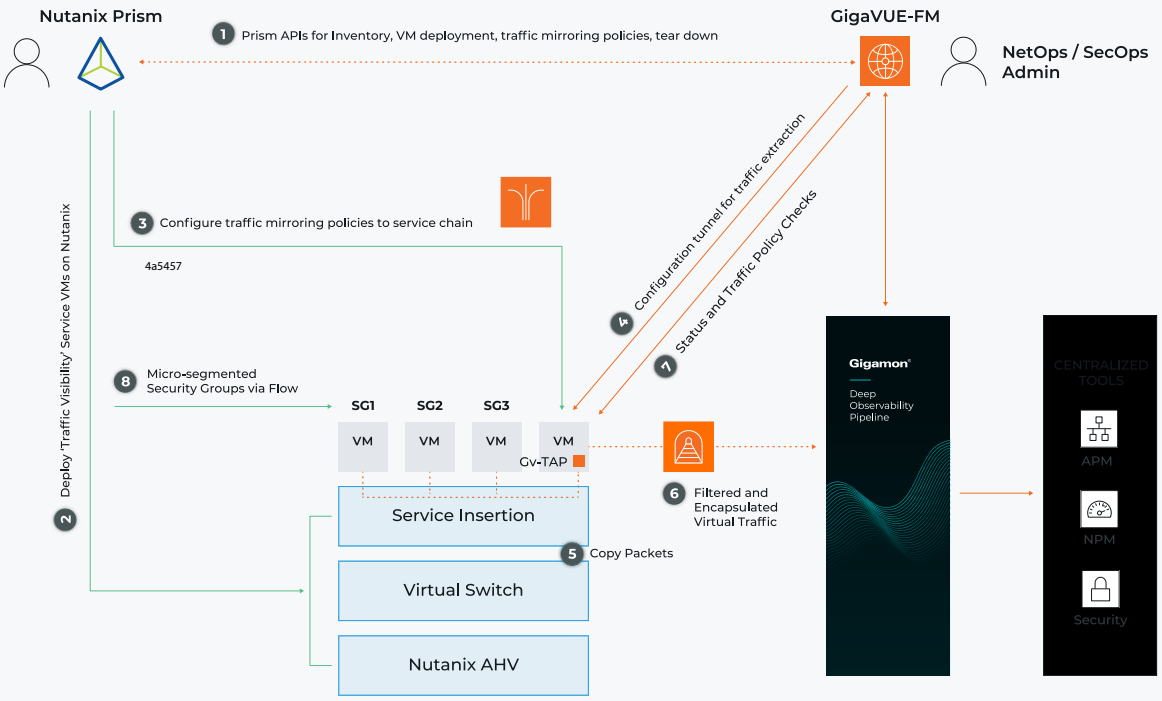

Figure 1. The Gigamon Deep Observability Pipeline is integrated with Nutanix-based private clouds to mirror traffic from all sources, then optimally process and distribute to the appropriate tools.

Design Overview

The design illustrates the unified joint solution has certified integration with Nutanix's Prism and Flow management automation suite for comprehensive insight and control. Further, leverage advanced capabilities with the Gigamon Deep Observability Pipeline such as GigaSMART® intelligence — includes application intelligence, packet slicing, data de-duplication, masking, decapsulation, header stripping, and more.

Before you Begin

- The traffic mirroring is done using G-TAP VM developed specifically for Nutanix-AHV platform.
- If any Gigamon fabric VM is deployed on multiple clusters, the management network selected during configuration must have the same name on all clusters, the CIDR may differ though.
- Assignment of Static IP for Gigamon Fabric Nodes is not supported at the moment, make sure the management subnet chosen is DHCP enabled.
- Only one G-TAP VM can be deployed per Nutanix Node, one Fabric Controller per Cluster.
- The G-TAP VM in its current form doesn't support any GigaSMART apps.
- For GigaVUE-FM to orchestrate the solution, the Nutanix admin account should be of at the minimum of "Prism Central Admin" on Prism Central and "Cluster Admin" on individual clusters. The password should be set to be same across the environment if they are locally management, alternatively external authentication like AD/LDAP could be used.
- The file names of the Fabric images shouldn't be altered while uploading to the Nutanix image repository.
  - For Fabric Controller retain "gigamon-fabric-cntlr" as the prefix for filename.
  - For G-TAP VM retain "gigamon-G-TAP VM-nutanix" as the prefix for the filename.
- The Fabric images can be downloaded from Gigamon Community portal.
- Refer the following GigaVUE-FM and Fabric images minimum hardware requirements.

GigaVUE-FM

SPECIFICATION	MINIMUM RECOMMENDATION
Memory	8GB
vCPU	4 vCPU
Virtual storage	2 x 40 GB
vNIC	1 (management)
Hypervisor	Nutanix AHV 5.5 and above

Fabric Images

Fabric Controller

SPECIFICATION	MINIMUM RECOMMENDATION
Memory	1GB
vCPU	1 vCPU
Virtual storage	1 x 10 GB
vNIC	1 (management)

G-TAP VM

SPECIFICATION	MINIMUM RECOMMENDATION
Memory	4GB
vCPU	2 vCPU
Virtual storage	1 x 12 GB
vNIC	1 (management) + vTAP interface

Deployment Steps

To achieve visibility for Nutanix AHV, the below sequence needs to be followed:

1. Deploy GigaVUE-FM
2. Defining Monitoring Domain
3. Fabric Launch configuration
4. Defining Tunnel Endpoint
5. Configuring Monitoring Session

Before installation, the respective images/disks are to be uploaded to Nutanix-AHV image repository. You can view the uploaded images/disks through Menu > Virtual infrastructure > Images.

Step 1: Deploy GigaVUE-FM

This step assumes there is no other existing GigaVUE-FM in the environment, else you can use any existing GigaVUE-FM v5.8 or later and skip to Step 2.

The GigaVUE-FM software for Nutanix-AHV is available as QCOW2 file. The following sections describes how to deploy a fresh installation of GigaVUE-FM and perform its initial configuration:

1. In GigaVUE-FM, navigate to Menu > Virtual infrastructure > VMs.
2. Click Create VM, select the Cluster where the GigaVUE-FM needs to be deployed.
3. Provide the following customary details, with the computing requirement is taken into consideration.
   - Name
   - Description (optional)
   - Timezone (org standard)
   - Compute and Disks with consideration on minimum requirement
   - Map the QCOW2 disk as boot disk with additional storage drive of minimum 40GB.
   - Network Adapters (NIC)
   - VM Host Affinity (optional)
   - Save the requirements and power-on the machine. Wait for about 10 minutes to complete the installation.
4. Proceed with initial configuration and login using the initial password as admin/admin123A! and change the CLI password upon prompt driven by the wizard. Note: Default Web console credentials are admin/admin123A!!, and you are recommended to change it.

Step 2: Defining Monitoring Domain

1. Navigate to Cloud > Nutanix > Monitoring Domain, and click New.
2. Update the required information in the following fields:
   - **Monitoring Domain:** Any identifiable name tag.
   - **Connection Alias:** Any identifiable name tag.
   - **Nutanix Prism Central IP:** Provide the Nutanix Prism Central IP address.
   - **Nutanix Prism Central Username:** This is the user account GigaVUE-FM uses to orchestrate the deployment, refer the prerequisite section for further details.
   - **Nutanix Prism Central Password:** This is the user account GigaVUE-FM uses to orchestrate the deployment, refer the prerequisite section for further details.
3. Click Save, this navigates to the Nutanix Fabric Launch Configuration window.

Step 3: Nutanix Fabric Launch Configuration

The other fabric images such as Fabric Controller, G-TAP VM are launched based on the inputs in this window.

Note: The QCOW2 images for Fabric Controller and G-TAP VM are to be previously uploaded to images repository with the filename convention.

1. Update the required information in the following fields:
   - **Management Subnet:** This is populated from all the clusters registered under the Prism central, chose the management subnet which the specification mentioned in the prerequisites.
   - **Fabric Controller:**
     - **Version:** Select the corresponding version from the repository
     - **Clusters:** Select the cluster you would want the Fabric controller (FC) to be deployed, max. one per Cluster, while a single FC could be shared with multiple clusters.
   - **G-TAP VM:**
     - **Version:** Select the corresponding version from the repository.
     - **Clusters:** Select the cluster you would want the traffic Mirroring to be configured thus G-TAP VM to be deployed.
     - **Hosts:** The customer has the option to chose nodes or specific nodes from the selected cluster.
     - **Memory, Disk Size, Number of vCPUs:** The values are set to default as shown in the screenshot, it can be amended based on the perceived load or changed in run-time once deployed.
     - **Data Subnet:** Select subnet based on interesed VM's vNIC's (IP address of VMs being monitored), could go on to add multiple subnet with "Add Subnet" option. You would notice on the Nutanix console that with each subnet added here would correspondingly add a vNIC to G-TAP VM. One of the added vNIC would also be used to route/export the mirrored traffic to tunnel endpoint based on the selection in definition of tunnel endpoint.
2. Click Save, this initiates the deployment of Fabric images based on the section. Give it time for it to be completed. The status can also be checked in the Prism Central task status. (The below screenshot is based on the selection of 1 Cluster for FC and 2 nodes for G-TAP VM.)

Step 4: Defining Endpoint Tunnel

Traffic from each G-TAP VM is tunneled out to the Tunnel endpoint directly. A Tunnel Endpoint can be created using a standard L2 Generic Routing Encapsulation (GRE) tunnel or a Virtual Extensible LAN (VXLAN) tunnel.

1. In GigaVUE-FM, on the top navigation bar, select Cloud.
2. On the left navigation pane, select Nutanix > Settings.
3. Select the Tunnel Spec Library tab. The Tunnel Library page appears.
4. Click New. The Edit Tunnel page appears.
5. On the Edit Tunnel page, select or enter the appropriate information in the fields.
   - **Alias:** The name of the tunnel endpoint, do not enter spaces in the alias name.
   - **Description:** The description of the tunnel endpoint.
   - **Type:** The type of the tunnel. Select L2GRE or VXLAN to create a tunnel.
   - **Traffic Direction:** The direction of the traffic flowing through the Gv-TAP-VM. By default the value is set as OUT.
   - **Remote Tunnel IP:** The IP address of the tunnel destination endpoint.
   - **Network CIDR for Egress Interface:** Specify the CIDR of the egress interface through which the mirrored traffic has to be exported (routed) to reach the tunnel endpoint. Example: G-TAP VM has 1 vNIC from Data Subnet definition (aside from the TAP vNIC for mirroring) with IP 10.10.10.10 on network /24, and the remote tunnel is configured with IP 11.11.11.11 on network /24. The egress interface CIDR should be configured as 10.10.10.0/24 provided the 11.11.11.0/24 is reachable.
6. Click Save.

Step 5: Configuring Monitoring Sessions:

1. Navigate to Cloud > Nutanix > Monitoring Session, and click New.
2. Provide the following details:
   - **Alias:** Enter an unique alias for monitoring session
   - **Monitoring Domain:** Select an applicable monitoring domain for this session entity
   - **Connection:** Select the applicable connection
   - Click Create, the session canvas is now brought up to configure new map for the session.
3. Drag-drop the New Map into the canvas and provide the details for the new map.
4. Click Add a Rule for further criteria to load.
5. Select the specific map rule criteria, based on traffic origin/destination IP, VM name, Subnet etc.
6. Click Save.
7. Drag-drop the Tunnel tile, as previously created and connect them by conduit.
8. Click Deploy, for the traffic mirroring policy to be configured and this is denoted by on-screen messages on GigaVUE-FM.
9. When the deployment is completed, the monitoring session picks up the agents within the scope of the subnet/ip-range defined in the Monitoring Domain configuration.

Verification Steps

After you deploy the monitoring session, if the status don't reflect success, troubleshoot some of the following aspects:

1. Check the status of the service of each fabric image on GigaVUE-FM and the reach-ability from each other.
2. Check the topology to verify the agents/vNIC detected and their status.
3. Verify the TEP status and interface stats on G-TAP VM.
4. Initiate test traffic from monitored VM and check the traffic at the tunnel endpoint.

Fabric Manager	5.8 GA
Prism Central	5.11.1
Nutanix AOS	5.11
Fabric Images	• gigamon-fabric-centlr-1.7.1 • gigamon-G-TAP VM-nutanix-1.7.1
Tool	Wireshark

About Gigamon

Gigamon offers a deep observability pipeline that harnesses actionable network-level intelligence to amplify the power of observability tools. This powerful combination enables IT organizations to assure security and compliance governance, speed root-cause analysis of performance bottlenecks, and lower operational overhead associated with managing hybrid and multi-cloud IT infrastructures. The result: modern enterprises realize the full transformational promise of the cloud. Gigamon serves more than 4,000 customers worldwide, including over 80 percent of Fortune 100 enterprises, nine of the 10 largest mobile network providers, and hundreds of governments and educational organizations worldwide. To learn more, please visit gigamon.com.

References

Refer to the GigaVUE Documentation Library and Guides.

Refer to the GigaVUE Cloud Suite for Nutanix Configuration Guide.

Gigamon®

Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | gigamon.com

04.23_v2