**Network Administrators Need to See Inside the Private Cloud**

The network was built to connect users and applications. Applications have become modular and distributed, creating more traffic. With the massive migration of applications to the virtual server, and today's modular and distributed application architecture, network administrators continue to seek ways to direct virtual server network traffic to their existing monitoring, analysis and security tools. The network administrator is challenged to get east/west traffic out of the virtual switch to the tools attached to the physical network. When the applications were running on dedicated servers, inter-application communications always hit the physical wire, where it was easily captured using TAP, SPAN or mirror port techniques.

**Monitoring VM Environments Is About More than CPU, Memory, and Storage**

While solutions for virtual machine monitoring are comprehensive, they focus almost entirely on the availability of hardware resources by reporting on utilization of available CPU, memory, storage, and overall north/south network bandwidth. Very little insight into VM to VM traffic is being offered by today’s VM monitoring tools. Network administrators rely heavily on visibility of network traffic for comprehensive analysis of network performance, health and early-detection of faults, and security incidents. In the absence of visibility into packets flowing east/west from one virtual machine to another, the virtual infrastructure may become an invisible silo of IT that is left dark when server physical to virtual migration occurs.

Businesses are looking for deeper insight into customer experience, more comprehensive security and forensic capabilities, and better analytics for application traffic using their existing commercial off the shelf tools. These tools include NPM, DLP, Compliance Monitoring, IDS/IPS, and APM. While some of these tools include monitoring beyond vCOPS for CPU, memory and storage availability on the hypervisor, their deep analysis capabilities rely on examining network packets.

**Gaining Visibility of VM Traffic with GigaVUE-VM**

The GigaVUE-VM virtual fabric node is one of Gigamon's latest product innovations that expand pervasive visibility for monitoring, analysis and security tools into the virtual environment and private cloud. GigaVUE-VM is a native VMware virtual machine. GigaVUE-VM currently supports the vNetwork Distributed Switch and Standard Switch, as well as the Cisco Nexus1000V for vSphere 5.x environments. Leveraging VMware’s native APIs, the GigaVUE-VM solution is able to virtually TAP, or port mirror, specific vNICs of virtual machines. The mirrored traffic is directed to an inbound vNIC on the GigaVUE-VM, where it is filtered before being encapsulated on a tunnel and sent to a destination tool on the physical network via a physical fabric node with Gigamon’s GigaSMART® technology enabled. GigaVUE-VM can also use the Gigamon patented Flow Mapping® engine and packet slicing operations prior to encapsulating traffic onto the tunnel, reducing the amount of overhead on the network related to monitoring features.

![Diagram](image-url)

**Figure 1:** The GigaVUE-VM enables visibility for Virtual Machine Traffic transiting the Virtual Switch and directs the traffic to destination tools
Many tools are now available as virtual instances, enabling organizations to avoid costly server hardware. However, except in the most minimal cases, deploying a virtualized data analysis appliance onto the same hypervisor as production applications can compromise the availability of production applications. The GigaVUE-VM solution is an agnostic approach, enabling a single VM to broker network packets for multiple tools on the physical network.

Because the Gigamon solution optimizes traffic for tools, it may also extend the life of the tools currently in use. Best practices dictate that tools adapted to run as VMs be allocated 100% of available host server resources, maintain connectivity on the physical management network, and use an agnostic solution like the GigaVUE-VM to send a single copy of interesting traffic from the virtual machines to a Gigamon physical fabric node which is able to replicate the packet stream to each tool in the environment.

**Delegate Change Control without Risking Availability**

Network administrators are generating an increasing number of requests for visibility from the virtual server administration team. Typical environments restrict administrative access for the vCenter server to a limited number of VM administrators. Failure to maintain a separation of duties can risk business SLAs. The GigaVUE-VM solution is managed by Gigamon's Fabric Manager, or GigaVUE-FM. GigaVUE-FM is a VMware native virtual machine and centrally manages up to five vCenter instances. The VMware admin can assign a low-privileged user account for use by the GigaVUE-FM, enabling the network administrator to centrally manage tightly-controlled packet filtering for VM traffic, where the GigaVUE-FM limits packet mirror destinations only to the GigaVUE-VM virtual machine. This management solution can alleviate concern of the VM administration team around enabling unfettered access to the environment.

**Maintaining Visibility During Virtual Machine Migration**

Another issue facing VM administrators is enabling constant visibility to the tools being used to monitor, analyze, and secure the entire data center infrastructure. Virtual Servers have become the platform of choice for application deployment because of their dynamic nature. However, their dynamic nature makes them very difficult to monitor, especially when a vMotion even occurs. When a VM is moved from one hypervisor to another, the only way to maintain visibility is for the VM admin to go through a long list of configuration items to manually disable existing vSwitch port mirror sessions and create a new port mirror session on the destination hypervisor where the VM in motion has landed.

The GigaVUE-VM solution for monitoring of VM traffic, along with the GigaVUE-FM fabric manager, monitors the vCenter server alert function for vMotion events. When a VM is moved, the GigaVUE-VM visibility policy moves with it to the new hypervisor, thus providing continuous visibility of the VM traffic before and after a vMotion event occurs.

Gigamon solutions have been deployed globally across enterprise, data centers and service providers, including over half of the Fortune 100 and many government and federal agencies.

For more information about the Gigamon Visibility Fabric architecture visit: [www.gigamon.com](http://www.gigamon.com)