Solution Brief

Enhanced Monitoring for VMware Infrastructure

Virtual Server Monitoring is About More Than CPU, Memory and Storage

With the massive migration of applications to the virtual server, and today's modular and distributed application architecture, more and more application traffic is never hitting the physical network. While solutions for virtual machine (VM) monitoring are comprehensive, they focus almost entirely on internal server availability 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.

At the same time, businesses are looking for deeper insight into customer experience, 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. All of which go far beyond the CPU, memory, and storage availability on the hypervisor.

Increasing East/West Traffic in the Hypervisor

Gone are the days of the monolithic, large binary server-side applications running on big iron. Today's applications are lightweight, delivering optimized information to even lightest-weight client-side applications, on even the smallest mobile platforms. In order to meet the quality of service demanded by the end user, the applications are now built with modular code, and in some cases dozens of API interfaces, spread across multiple virtual machines and hosts. The result is a massive increase in East-West traffic patterns, with the modular applications now running on virtual servers that East-West traffic remains entirely inside the hypervisor.

What Happens When the Application Breaks?

Because of today's modern application architecture, monitoring has become more complex. If a client cannot access data or process an online transaction because one component of an application cannot reach a DNS server, mistakenly hard-coded in one module of the app, standard vCOPS reporting will not assist in troubleshooting the application failure. Enterprise monitoring system architects use comprehensive, agentless analysis of the applications traffic to detect the failure based on contents of individual packets flowing east/west from one virtual machine to another. Meanwhile vCOPS reporting continues to reflect that all systems are normal.

Virtualization and modernization of application architecture presents the same challenges to security and data analytic tools as it does to the application performance tools.

Administrative Control of the vSphere Environment

VMware administrators are able to deliver VM-VM packet insight on behalf of the security and monitoring teams using VMware's Port Mirroring feature for vNetwork Distributed Switch, and promiscuous mode for vNetwork Standard Switch. But two problems exist with these approaches. The first is that there exists a significant amount of complexity to enable a configuration that will not jeopardize the production application environment when a mirrored port can potentially over-utilize available network bandwidth unless port-level bandwidth enforcement policies are also enabled. The second concern is the increasing number of requests coming from other departments, not only for visibility into the hypervisor traffic, but also the requests for delegation of administrative privileges into the vCenter Server. Maintaining separation of duties is an important factor in meeting business-level SLAs.

Gaining Visibility of VM Traffic with GigaVUE-VM

The GigaVUE-VM solution is represented in Figure 1. The GigaVUE-VM virtual fabric node is a native VMware virtual machine that extends pervasive visibility for monitoring, analysis, and security tools into the virtual environment and private cloud. GigaVUE-VM currently supports the vNetwork Distributed Switch, Standard Switch, NSX vSwitch, as well as the Cisco Nexus 1000V for vSphere environments. Leveraging VMware's native vSwitch APIs, the GigaVUE-VM solution is able to virtually copy packets on ingress or egress for 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 enabled with Gigamon's GigaSMART® technology. The GigaVUE-VM can also perform packet slicing operations prior to encapsulating traffic onto the tunnel. With the Gigamon solution, tool administrators are able to greatly reduce management and monitoring overhead of virtual machine traffic that is copied and sent to destination tools in the physical network.

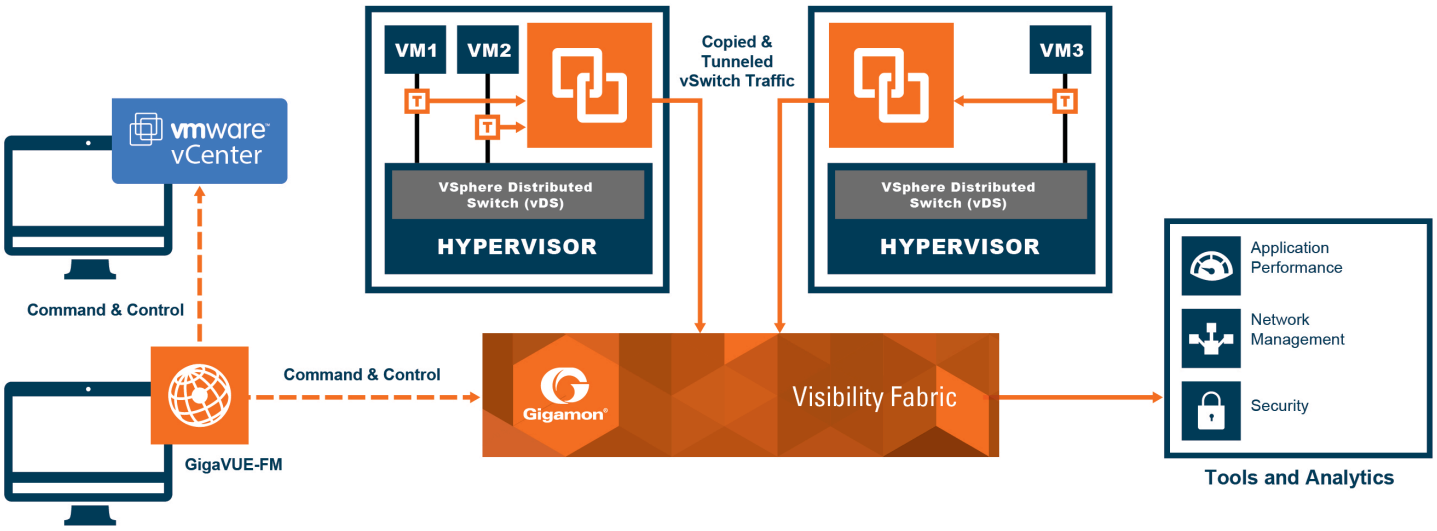

Figure 1: GigaVUE-VM enabling visibility for virtual machine traffic transiting the virtual switch and directs the traffic to destination security tools

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 deliver inter-host and intra-host network packets to multiple monitoring tools that are connected on the physical network. While some tools are available as virtual appliances, administrators generally avoid running virtual tool appliances on the same hosts that are running production applications.

Delegate Change Control without Risking Availability

VMware administrators deal with a steady stream of requests for administrative access into the vCenter server. This often interrupts smooth operational interactions with other IT departments. The GigaVUE-VM solution is managed by Gigamon's Fabric Manager, GigaVUE-FM. GigaVUE-FM is also a VMware native virtual machine and centrally manages up to 10 vCenter instances and 1000 ESXi hypervisors. The VMware administrator can assign a low-privileged user account for use by the GigaVUE-FM, allowing it to centrally manage packet mirror sessions where the GigaVUE-FM limits 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. GigaVUE-FM, that supports deploying and monitoring hundreds of GigaVUE-VM virtual fabric nodes, provides hotspot monitoring using Top-N and Bottom-N traffic widgets in the dashboards.

Maintaining Visibility during Virtual Machine Migration

Figure 2 represents monitoring in a dynamic environment where vMotion events occur. Maintaining consistent monitoring during vMotion events while enabling constant visibility to the tools being used to monitor, analyze, and secure the entire data center infrastructure is another issue facing VM administrators. 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 administrator to go through a long list of configuration items to manually disable the 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 node in conjunction 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.

Traffic Intelligence to Monitor Virtual Workload Traffic

Once GigaVUE-VM delivers the traffic to the physical GigaVUE nodes, additional GigaSMART traffic intelligence can be applied to secure and monitor the virtual workloads.

- Masking to obfuscate or mask a segment of the packet, primarily to ensure privacy and compliancy
- Decrypt SSL traffic to detect any embedded malware
- Match packets that contain known signatures or patterns using Adaptive Packet Filtering
- Remove duplicates received from physical TAPs and GigaVUE-VMs, thereby optimizing tool performance

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 Unified Visibility Fabric visit: **www.gigamon.com**

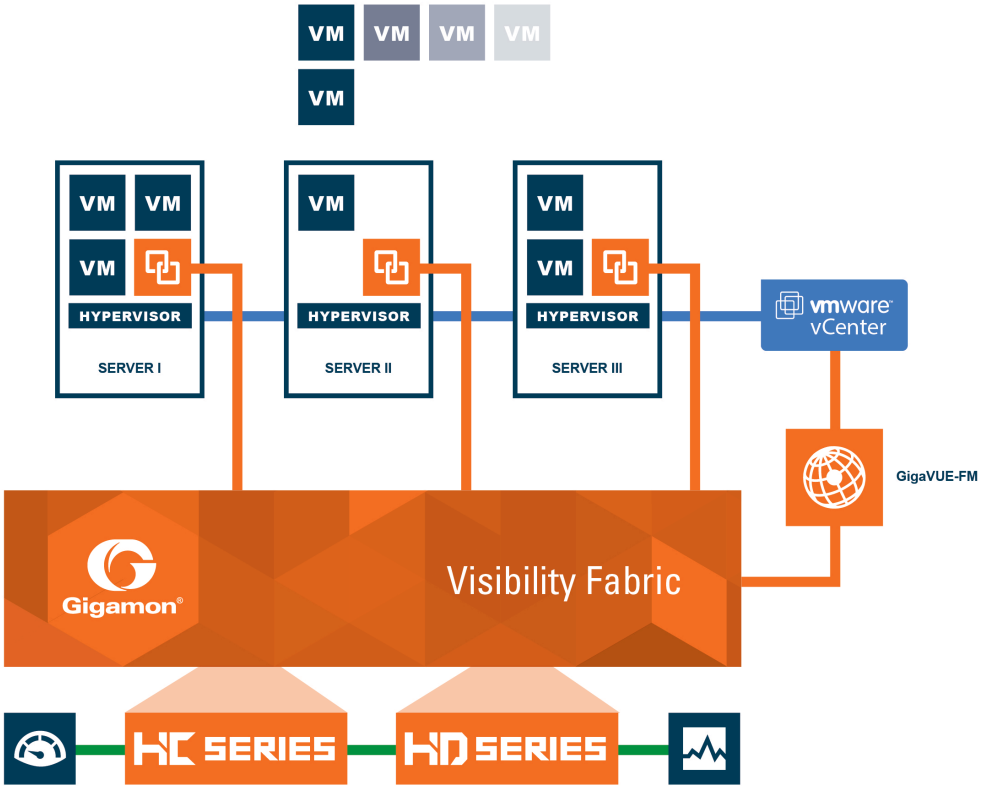

Figure 2: The GigaVUE-VM solution maintains visibility policies before and after a vMotion event occurs

3114-03 04/15

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