

Network Instruments Puts Virtualized Systems on Tap

Event

On March 23, 2009, Network Instruments® announced a new revision of their Observer® network performance management solution optimized for installation directly within a virtualized server environment. This is one of the very first network management tools that has been customized specifically for the purpose of directly monitoring traffic across the virtual switch within Virtual Machine (VM) environments that also provides a direct

Network Instruments is making a bold initial move into monitoring of virtual environments.

adaptation for reaching those traffic flows outside of the VM host. In particular, the Virtual TAP features within this release allow a complete copy of VM-to-VM virtual network traffic to be accessed and viewed outside of the VM host system for troubleshooting, security monitoring, and compliance assessment.

Network Instruments is one of a few well-established, enterprise-class players in the packet-based performance management solutions space, and is making a bold initial move into monitoring of virtual environments with this new product announcement.

Context

With the growth of server virtualization, network management technology players of all stripes are working in various ways to add support into their wares. Such announcements within the past six months alone include those by EMC, Solarwinds, OPNET, and PacketTrap. And the entry of Cisco into the blade computing marketplace, with their UCS announcement, is based heavily on more tightly integrating networking and virtual computing technologies, further driving these two worlds together.

There are a lot of new challenges around managing these environments that concern network managers. One of the biggest involves visibility. While vCenter from VMware and System Center from Microsoft for the Hyper-V provide help in configuring and basic monitoring of VMs on a host server, they fall far short of delivering the full, contextually complete visibility required to understand how VMs are working together and how they fit into the broader IT service delivery infrastructure.

Another big management challenge arises because VMs, being virtual by definition, can be moved about dynamically. Most deployments are starting to leverage the wonderful features offering resilience and flexibility, such as VMware's vMotion, HA (High Availability) and DRS (Distributed Resource Scheduler), each of which can result in frequent movements of VMs from one host system to another – sometimes even to another data center. This is really great for giving IT shops ultimate control over how best to deploy available resources to meet changing computing needs, but it's a nightmare for operations teams trying to understand just what is executing where, whether their interest is in proactive service monitoring, efficient troubleshooting, planning adequate capacity, security, or policy compliance.

There are two major approaches to delivering visibility into virtual server environments. One is to use traditional computing server monitoring agent interfaces, such as SNMP and WMI, to recognize and keep track of both host servers as well as guest virtual servers. Another is to recognize that each virtual host is a miniature network ecosystem, complete with a virtual switch (vSwitch) and virtual Network Interface Cards (vNICs) that can be accessed with packet-based monitoring technologies.

When it comes to network-based monitoring and troubleshooting, many in the industry turn to packet-based technologies to provide definitive visibility into communications traffic. Packet-based approaches not only deliver true real-time problem indications, they also offer the only true opportunity to capture full sessions and transactions, enabling forensic analysis and reconstruction and troubleshooting of the thorniest performance issues.

There have been a few attempts to apply packet-based monitoring tools into VM environments. One method is to drop packet analysis tools directly into each VM instance, and then look at each guest VM's vNIC to understand what traffic is going out to other VMs. Another option is to drop packet monitoring software on the host operating system, next to the hypervisor, and then listen to all of the traffic going across the vSwitch. The third approach is to install packet monitoring within a guest VM instance, and listen to vSwitch activity from that viewpoint.

Network Instruments is taking this third angle with their solution, allowing installation of the Expert Probe or Multi-Probe products into one VM "slot," and harvesting all of the traffic going across the vSwitch from a single location. This affords visibility for troubleshooting application traffic that is traveling between VMs. It also provides one additional differentiating capability – the opportunity to aggregate some or all of the vSwitch traffic so that it can be mirrored out one of the host's physical NICs, exposing the flows for multiple monitoring and recording purposes. Network Instruments calls this their "Virtual TAP" feature.

Key Ramifications

While Network Instruments is not the first to apply packet-based monitoring to virtual environments, this release brings some unique and innovative features along with it. Here's what the major elements mean in terms of improved ability for managing virtualized server environments:

1. By putting Observer into a VM form, operations teams will be able to gain direct visibility into the traffic that is traveling between VM guest servers on a common VM host. The pure software footprint eases deployment versus the use of physical appliance form factors. This will be of benefit for tracking and troubleshooting VM-to-VM communications and transactions – something that was not easily available before this product was released.
2. One of the other challenges for management is to gain insight into VM-to-VM communications for other management and monitoring purposes, such as security monitoring, policy compliance monitoring, resource accounting, and long-term packet capture for forensic troubleshooting. The Virtual Tap feature – a piece of software that provides a virtual equivalent to switch SPAN or port mirroring – can collect and stream a copy of all VM-to-VM traffic out one of the physical server's NICs.

Operations teams will be able to gain direct visibility into the traffic that is traveling between VM guest servers.

EMA Perspective

As with many (if not most) technological innovations in IT, server virtualization has gone through its initial growth and adoption largely without regard to or participation by networking professionals. But along the way, virtualization of servers creates yet another layer of abstraction that impedes the operational visibility which is essential for proactive, integrated service management. And so, a light must be shown on the inner workings and communications flows within virtual computing so that compliance can be enforced, problems identified and resolved, security assured, and ultimate business integrity protected.

The introduction of these new features by Network Instruments addresses this need and includes a great, innovative answer to some of the key challenges delaying many from embracing virtualization fully. In particular, making VM-to-VM communications flows visible to the outside world via the Virtual TAP feature could go a very long way in increasing the comfort level of IT security and compliance professionals, while paying additional benefits for those responsible for fixing things when performance bogs down.

EMA applauds this important step for the network management technology sector that IT shops need to fully operationalize VMs.

The ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) team applauds this move as an important step for the network management technology sector in delivering the visibility that IT shops need to fully operationalize VMs and capture the full potential that they offer for flexibility and efficiency.

Written by [Jim Frey, EMA Research Director](#)