Edison Group Technology Spotlight

Extending Service Assurance into VMware NSX Environments

Digital disruption is real and Software Defined Networking (SDN) and Network Function Virtualization (NFV) are part of it. But what does losing control mean to your business? IDC says 75% of the S&P 500 will be replaced by 2027.

NETSCOUT provides a natural starting point to solve service performance problems in physical, virtual and hybrid IT environments.

Virtualization has changed everything for service delivery as well as the IT organization tasked with its implementation and operation. Virtualized servers and now the virtual network are required to smoothly deliver Microsoft Exchange, Oracle, Citrix, Unified Communications and a lot more. Essentially, VMware has extended the advantages of server virtualization to the network. VMware's NSX framework is gaining popularity within IT teams for its data center and cloud advantages and the huge OPEX savings it brings to business, up to 30% in most cases according to IDC.

However, adding a complete suite of logical networking elements and services managed by the NSX controller also adds a level of complexity and a new dimension to tackling service delivery problems. Gartner estimated service disruptions can cost a company $5,000 to $10,000 a minute. Things can go wrong anywhere in the IT environment, inside or outside the NSX deployment, making service assurance a challenge. Traditional performance monitoring tools simply can't see the whole picture with disparate data sets and when users and customers experience service degradations IT teams tend to respond with finger pointing and wasting time in the war room looking for the root cause of the problem.

NETSCOUT provides a holistic view of the entire data center – including VMware NSX resources. NETSCOUT's nGeniusONE Service Assurance platform provides continuous monitoring and real-time analysis of the East-West and North-South traffic traversing the data center physical and Software Defined Network environments. Its patented Adaptive Service Intelligence (ASI) technology is used to collect, correlate, analyze and contextualize traffic data to understand the interrelationship and dependencies of the physical and virtual service delivery environment.

ASI technology runs on NETSCOUT's physical and virtual Intelligent Data Sources and generates highly scalable metadata in real time as the IP traffic traverses physical or virtual links. Administrators can gather significant insights from this metadata, including application traffic volumes, server response times and throughputs, aggregate error counts, and error codes specific to the various applications and servers active in the environment.

According to a recent survey by [TechValidate](#), NETSCOUT customers use this insight for rapid service triage to identify the root-cause of service issues and to significantly reduce Mean Time to Knowledge (MTTK).
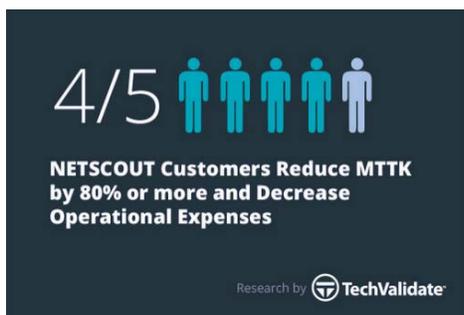
The nGeniusONE platform and ASI technology provide a natural starting point to solve service performance problems, foster collaboration between the different IT teams, and reduce time in the war room by providing situational awareness and a consistent view.

NETSCOUT's products were designed to be both flexible and scalable so that variations in virtual environment configurations can be accommodated. The nGeniusONE platform works with different VMware configurations and provides a comprehensive service assurance solution for a wide range of virtual environments through:

- **Traffic between VMs on the same hypervisor** is monitored by integrating NETSCOUT's ASI technology into a virtual machine (VM), functioning as a virtual Intelligent Data Source. NETSCOUT's VM either analyzes the intra-VM traffic in a self-contained virtualized mode or redirects the traffic to an external NETSCOUT Intelligent Data Source for analysis.

- **Traffic between VMs in different hypervisors** is monitored by the NETSCOUT Intelligent Data Sources, which decode the VXLAN encapsulation and access the original packet flow data between the VMs.

- **Multi-tier East-West and North-South Data Center traffic** is monitored by collecting data from a combination of multi-tier physical and virtual service delivery environments. All the interrelationships and dependencies across all monitored service delivery components are

correlated and analyzed contextually. These include n-tier applications, workloads, protocols, servers, databases, users, and devices.

Virtualization provides significant business benefits, but it also makes service delivery significantly more complex. As long as the VMware environment is healthy, corporate networks experience impressive efficiencies. When issues occur, it is important to have the right solution built around effective methodologies to quickly discover and resolve these issues. NETSCOUT's nGeniusONE platform and ASI technology are designed to address the unique operational problems of virtualized and hybrid environments. NETSCOUT offers customers a way to accelerate their migration to virtualized infrastructures with confidence and without compromising end user or customer experience, and reduce capital and operational expenses. As such they need to be seriously considered when looking for a solution that provides end-to-end visibility into multi-tier physical, virtual, and hybrid service delivery environments, as well as proactive service triage.