NSX-T Edition of vSTREAM

NSX Edition of vSTREAM Overview

The NSX-T edition of vSTREAM™ virtual appliance (or simply vSTREAM), certified by VMware, revolutionizes how applications are monitored and analyzed in NSX software defined networks (SDN) and beyond. It is an advanced service assurance solution that delivers affordable, optimized monitoring of east-west traffic in NSX environments. Complementing existing Adaptive Session Intelligence™ (ASI)-based instrumentation, vSTREAM offers the same smart data visibility consumers have come to expect. vSTREAM eliminates blind spots and provides a seamless view for complete visibility and monitoring, using packet data, across VMware ESX, NSX, and SD-WAN deployments alongside multi-cloud and legacy data center environments.

Deployment

The NSX-T edition of vSTREAM is a service virtual machine (SVM) that can be installed on every hypervisor in a VMware cluster and leverages the NSX NetX API to process copies of packets flowing into and out of VMs on the same ESX host (see Figure 1).

Packet forwarding to the NSX-T edition of vSTREAM is simple and easily controlled using an NSX security group. Any VM that belongs to the vSTREAM security group will automatically be monitored by it. NSX provides various means of defining membership rules for security groups. Using a security group to control packet forwarding allows IT to align their application visibility and assurance with their security policies and practices.

Figure 1: NSX-T Edition of vSTREAM with nGeniusONE Service Assurance platform which improves collaboration among all members of the IT team from NetOps to DevOps, AppOps, SecOps and CloudOps.
The analysis performed locally by ASI in the NSX-T edition of vSTREAM generates KPIs for correlation and presentation in nGeniusONE. This has the benefit of avoiding over-burdening the network with added load from sending copies of packets to external data sources.

If direct access to packet data is required, vSTREAM can be configured to perform on-demand packet captures for in-depth analysis when necessary.

Smart Data and Smarter Analytics Overview
Only NETSCOUT can leverage the power of packet data through its patented ASI technology and is designed to scale to the needs of the world’s largest enterprises and service providers supplying smart data for service and security assurance. The NSX-T edition of vSTREAM is unique in delivering Layer 7 application visibility directly from the hypervisor. nGeniusONE Service Assurance platform, with industry-leading support for more than 1000 applications including voice, video and data, uses smart data from vSTREAM to pinpoint the source of application disruptions impacting the user community. All of NETSCOUT’s ASI-based monitoring platforms are integrated with the nGeniusONE platform to provide a common set of metadata analytics.

SPECIFICATIONS

**NSX-T Edition of vSTREAM**

- **vCenter Server**: v5.X, v6.X
- **Hypervisor**: VMware vSphere ESXi Standard, Enterprise, or Enterprise Plus running ESXi v5.5, v6.0, v6.5, or v6.7 on a 64-bit Intel platform
- **NSX**: NSX-T – 2.5 (vCenter compute targets only)
- **vSphere**: 5.5, 6.0, 6.5, 6.7
- **vCenter**: 5.x, 6.x
- **vSwitch**: VMware vSphere VDS
- **Virtual Interfaces**: Up to 1 Management & 4 Monitoring
- **vCPUs**: 2 or more
- **Memory**: 2 GB or more
- **vSTREAM Disk**: 100 GB
- **Packet Capture Disk**: Configurable

nGeniusONE Service Assurance Platform
nGeniusONE is a real-time information platform that provides a single pane of glass to view the data, voice, and video service delivery performance to manage both the availability and quality of the user’s experience.

Available on both hardware and virtual platforms, nGeniusONE leverages NETSCOUT smart data as a universal source for providing smarter analytics for end-to-end visibility throughout private, virtualized, public, and hybrid cloud environments.

ASI Technology
ASI technology transforms wire traffic into smart data, providing real-time visibility into user experience for the most advanced and adaptable information platform to ensure security, manage risk, and drive service performance.