Pluribus Netvisor® Fabric Visibility

Complete Network Fabric Visibility for Monitoring, Control and Analytics

April 2020

Pluribus NETWORKS

The Need for Network Visibility

Today's network architectures tend to be complex, rigid, and unable to meet the utmost levels of speed and efficiency demanded by the business. Any business applications such as Big Data, VDI or Nutanix-like storage arrays that call for deep traffic visibility are unfortunately getting addressed with separate and high cost network tap and packet broker infrastructure deployments. These infrastructures are heavily dependent upon the direct replication of desired network traffic, which in practice only provides insight into a fraction of overall and necessary East-West traffic flows. In some cases, it may even be necessary to install an agent at the hypervisor level to extract traffic from virtual machines. In addition, third-party tools are often required to extract additional packet-level information, further adding to the cost of network visibility. This cost is a large barrier to obtaining crucial information used in capacity planning, performance analysis and application workload optimization. This information could also be used for auditing and security purposes to log and report on any network event – if it weren't so insufficient.

Until now, little attention has been paid to monitoring individual flows and application dependencies residing on these networks because whatever data was available, was limited in scope as well as detail. With the introduction of Pluribus Netvisor® Fabric Visibility, these hindrances are now a thing of the past. It is now possible for companies to make intelligent business decisions based on metrics available directly from their network.

Pluribus Netvisor® Fabric Visibility

Pluribus Networks advances virtual and software-defined networking (SDN) through Netvisor, the industry's most programmable, open source-based network operating system. Netvisor is based upon the Pluribus Adaptive Cloud Fabric™ (ACF) architecture, a proven approach to understanding flow, rapidly responding to business needs and securing your data.

Netvisor combines the benefits of server clustering for networking with a distributed controller fabric. The traditional CLI (Command Line Interface) is paired with fabric-wide programmability (C, RESTful API), and DevOps tools (e.g. Ansible) for agility and automation via a single point of management.

Granular visibility is available through a fabric-wide directory that contains endpoint information (vPorts) as well as allows for granular flow filtering and control (vFlow).

In combination with Pluribus Network hardware switches, Netvisor provides best-in-class switching economics. The deployment flexibility is guaranteed by Pluribus Netvisor full L2/L3 stack providing complete interoperability with the legacy networking infrastructure, allowing for easy insertion into existing, multi-vendor deployments.

Flow Visibility

With Pluribus Netvisor running on a Pluribus switch, the network is no longer just the platform for traffic forwarding, it is now a powerful networking data platform as well. Running Pluribus Netvisor allows the network to provide rich, flow-based information on both bare-metal as well as virtualized workloads across the entire data center. Pluribus Netvisor Fabric Visibility offers unique visibility features not offered by any other datacenter platform, including:

- 100% East-West flow visibility
- Full port state information available across the entire fabric
- No need for a separate tap and packet broker infrastructure

Pluribus Netvisor Fabric Visibility Has Advanced Capabilities

Pluribus Netvisor Fabric Visibility brings unprecedented visibility to the data center with three important new concepts: Telemetry for application flow, vFlow and vPort.

Telemetry

Pluribus' application flow Telemetry is the unique ability of Netvisor to inspect every individual TCP connection and client-server aggregated connection statistics in the fabric. The unique architecture of Netvisor running on a Pluribus switch hardware opens up unmatched visibility to all connections that traverse the entire data center fabric. With Netvisor Telemetry, both virtualized as well as bare-metal workloads are now fully visible, end-to-end.

This functionality is much more powerful than sFlow and is more ubiquitous than Netflow. Application flow telemetry is not a single device hardware concept. It does not depend on dedicated hardware and is a fabric-wide software process that reads data directly from the switching chip (ASIC). Since this functionality is scalable in software by design, there is virtually no limit to how many devices can report data in the fabric.

This application-flow-centric data is unique to Pluribus Netvisor and provides the capability to quickly examine specific hosts or endpoints and instantly obtain a snapshot of current or historical traffic patterns. This enables not only application performance analysis, but also deep security visibility across all devices and endpoints throughout the entire Netvisor fabric.

vFlow

vFlow is the Pluribus Networks name for the ability to filter fabric-wide data center switching traffic on a granular flow level, and apply security/QoS (Quality of Service) actions or forwarding decision on each defined flow. Using vFlow, Pluribus Netvisor provides flow-level visibility, filtering and statistics reporting. At this level, it is possible to classify traffic for prioritization using QoS, but additionally, this data can be used for reporting and accounting purposes. Data center flows can now be grouped and classified by application VLAN, source or destination IP, physical port, or numerous other Layer 1 – 4 traffic descriptors.

Troubleshooting, reporting, monitoring or analyzing specific application flows now take seconds when utilizing Pluribus Netvisor vFlows. This can be taken further and implemented into a fabric-wide filter that can be used to redirect or drop matching traffic. Regardless of traffic protocol, TCP or UDP, vFlows can be used to analyze, filter and redirect traffic. This powerful mechanism enables users control and visibility into data center network workloads like never before.

vPort

vPort is the Pluribus Networks name for the functionality of tracking endpoints/VMs on a global, fabric-wide endpoint table. vPort data is stored in software, a superset of the information stored in a traditional switch L2 (Layer 2) hardware table. vPort is more than a simple L2 table, it is a mechanism for tracking endpoint identity, mobility and location information anywhere within a Netvisor fabric from any Netvisor switch.

In addition to L2 table information, the vPort table stores:

- switch ID and location
- host IP address
- host MAC address
- VLAN
- associated ports
- hostname
- host CPU details - memory, CPUs, disk and OS when provided by hypervisor management
- migration count

vCenter or KVM APIs can be used to populate the vPort information within ONVL. Since the vPort table is shared globally across all fabric nodes, it is now possible to create a broadcast-free network fabric. Both bare-metal and virtualized workloads can be pinpointed with a single API or CLI command. This feature can be used to locate a single host or to provide a snapshot of the current state of every device communicating across the data-center networking fabric. This valuable information is available not only in real time, but it can also be provided for any prior logged point in time, with the same information available.

"Tunnel View"

Pluribus Netvisor vPort, vFlow and application flow Telemetry seamlessly extend visibility to an existing overlay environment. When deployed alongside any VXLAN tunneled traffic, Pluribus Netvisor makes it possible to inspect the encapsulated traffic as if there was no VXLAN header present. Detailed vPort, vFlow and application flow Telemetry is provided with the same level of detail as non-VXLAN traffic, making it possible to fully examine all traffic trends, performance measurements and detailed statistics like never before.

FlowTrace

When vFlow functionality is combined with the power of the underlying Linux command prompt (Quagga direct access), users can execute an included application called FlowTrace. The FlowTrace app takes in two arguments, a source IP address and a destination IP address. It then analyzes the data provided by Netvisor and outputs the data path that is taken from switch to switch throughout the fabric, carefully detailing port and switch information at each hop. With this functionality, not only is visibility into where traffic is being sent much easier, troubleshooting is as well. What once took minutes of correlating data from multiple sources, is now provided in seconds from any point within the fabric.

WireShark

Existing monitoring solutions heavily leverage PCAP functionality, with WireShark as one of the leading open source tools used to analyze packet data. Pluribus Netvisor Fabric Visibility has built-in WireShark capabilities. vFlow capability allows packets to be sent to the CPU to be snooped in real time. From here, the data can be exported to other devices or analyzed directly on the switching platform, making troubleshooting and deep packet inspection an easy to accomplish task on Netvisor.

Summary

Pluribus Netvisor Fabric Visibility leverages unique functionality not found in any other data center platform to provide unmatched Visibility for application flow, fabric-wide endpoint visibility (vPort), flow control (vFlow) and integration into existing ecosystem tools. With these data sets, network operators, business decision makers and executives can make more intelligent decisions regarding the security and performance of their network to ensure that mission-critical business applications operate in the most optimal, secure way possible to continue to support the business mission. Pluribus Netvisor Fabric Visibility with its powerful features allows for the elimination of separate tap and packet broker infrastructure with the associated reduction of CapEx expenditures needed to purchase and maintain these additional tools.

Network Function	Challenge	Pluribus ONVL
East-West flow visibility	Current solutions require a dedicated network TAP infrastructure to obtain visibility to a subset of datacenter traffic	Provides 100% east-west traffic flow visibility natively, without additional hardware or software purchases
Endpoint Location/ VM Migration Tracking	When troubleshooting network issues, it is difficult to locate a virtual machine without additional hypervisor information	Treats every endpoint the same and makes locating any device as simple as a single management command
Traffic Statistics Reporting	Detailed traffic statistics require investment 3rd party tools to collect fabric flow data	Natively reports server-client statistics from every flow that traverses the fabric, avoiding the need for expensive tools and hardware
VXLAN Traffic Inspection	It is difficult to inspect VXLAN overlay encapsulated traffic on the network	Can inspect VXLAN traffic and report the overlay traffic patterns as if they were natively communicating across the network
Traffic Filtering	Effectively removing a particular type of traffic from an entire data center fabric is complex and difficult	Allows fabric-wide filtering to drop any type of traffic classified in a vFlow/ fabric-wide filter creation with one command

About Pluribus Networks

Pluribus Networks provides data center solutions that allow your business to run unconstrained. Our software-defined, open networking, fabric-based solutions transform existing network infrastructures into flexible and strategic assets fully aligned with today's digital business needs. Our Adaptive Cloud Fabric™ (ACF) architecture provides unprecedented insight, agility and security to customers seeking to simplify operations, run more cost effectively and bring new applications online faster.