# Pluribus Insight Analytics 2.1

## Network Performance Monitoring and Analytics

## End-to-End Network Visibility

Network visibility and analytics can often require expensive and difficult to deploy tap and probe hardware. Existing solutions to extract business value from an entire existing network in the data center, campus or branch have historically been difficult to deploy.

Pluribus Insight Analytics eliminates the economic and operational barrier associated with traditional monitoring infrastructure (based on packet brokers and expensive tools), and brings flows and packet analytics to broader enterprise networking deployments ranging from campus to data center.

Pluribus Insight Analytics is also fully interoperable with third party networks. This compatibility allows customers to extract more visibility from the network, to spot security concerns and to drastically reduce the time spent in war rooms to solve IT trouble tickets.

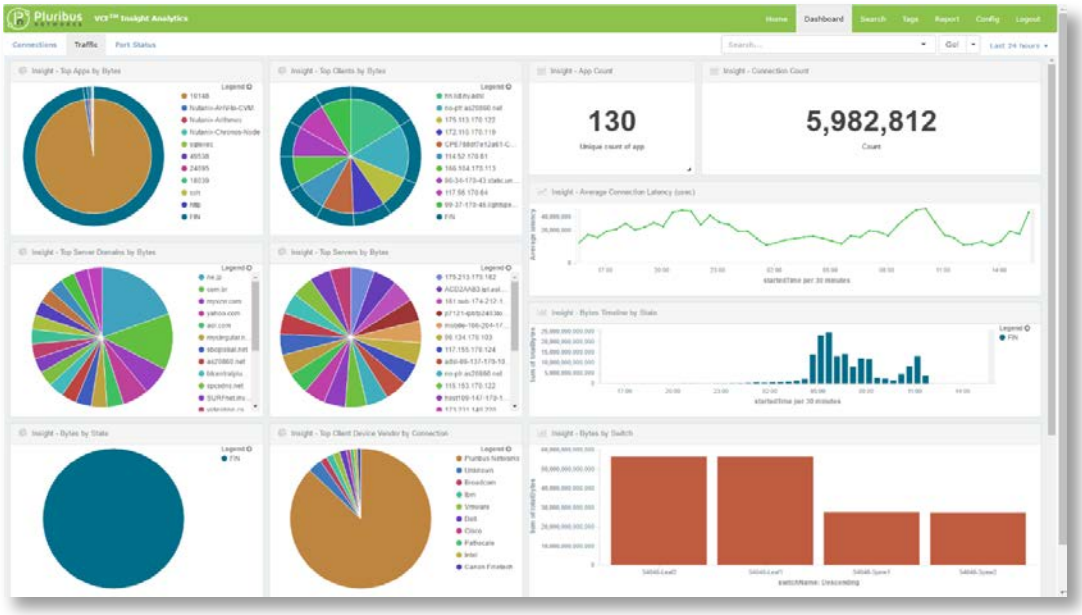
Insight Analytics is the most affordable, easiest-to-use, flow and packet analytics solution to empower Netops to extract more value from their current assets and make the network more relevant to the business.

Insight Analytics empowers Network administrators with:

- A simple to deploy and maintain tool with a single pane of glass to analyze flows or packets to drastically reduce the time troubleshoot application problems on the network
- A simple to deploy and maintain tool to enhance the security posture of the fabric with extensive forensic analysis and flow auditing capabilities
- A simple to deploy and maintain tool to gain unprecedented visibility into East-West applications flows and end-points behavior

## Pluribus Insight Analytics

Insight Analytics is a monitoring solution intended to replace the most common deployment of packet brokers and analysis tools. It provides an inexpensive means to monitor and track the performance of business application flows of information, and can be used with or without existing Pluribus Networks switching fabrics.




Dashboard – click any aspect to filter and drill-down, intuitively.

Insight Analytics (IA) is a network application built on top of the Pluribus Netvisor® (switch operating system) flow telemetry capabilities and open API and residing on an external x86 server (or cluster of servers).

The IA application relies upon an advanced search engine technology to store, aggregate, filter, correlate and visualize vast amounts of data in real-time and with a powerful “time machine” functionality.

# Flow Analytics

Pluribus Insight Analytics offers Flow Analytics with six modules through the graphical user interface: Dashboard, Report, Advanced Search, Custom Tags, Schedule Reports, Alerts.

## Dashboard

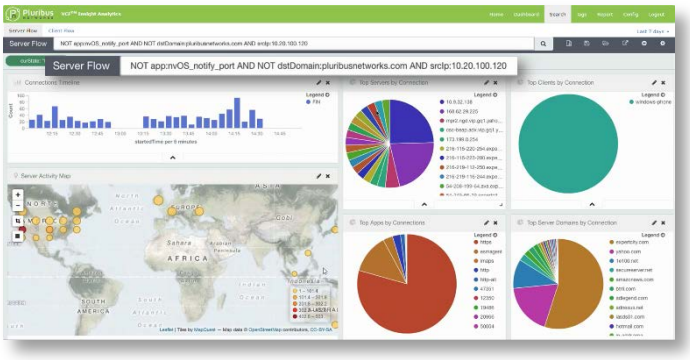
An easy-to-use, drillable dashboard to visualize key application flow metrics, with extensive filtering, and correlation capabilities.

## Features

- Live streaming of network flow data
- Selectable rolling window view from 15 minutes to 30 days
- “Quick Search” window with autocompletion to rapidly filter the entire dashboard for a specific flow, IP, hostname or VLAN traffic.
- Top Applications by total number of connections/transferred bytes with connection breakdown by TCP state (SYN, EST, FIN, RST)
- Top Clients by total number of connections/transferred bytes with connection breakdown by TCP state (SYN, EST, FIN, RST)
- Top Servers by total number of connections/transferred bytes
- Top server destination domains by total number of connections/transferred bytes
- Connection breakdown by TCP state (SYN, EST, FIN, RST)
- Top Clients by device vendor
- Total application count and flow count
- Connection and total bytes histogram by (TCP state) with selectable time window
- Top switches by total connections and total bytes transferred
- Average connection latency (proxy measurement based on SYN/SYN-ACK timestamping) with selectable time window
- Table with detailed flow information
- Intuitive dashboard filtering based on “clickable” live charted data
- Dedicated analytics dashboard for monitoring the Pluribus distributed fabric OS
- Switch port traffic statistics with unicast, multicast, broadcast breakdown. Ingress and egress.
- Switch port statistics for errored frames, congestion drops and discarded frames. Ingress and egress.
- Top switch ports by client and server number of connections

## Search

Powerful search engine UI and simple query syntax to isolate and filter specific flows among millions - in a fraction of a second.




Search – enter command line instructions for rapid filtering.

## Features

- Powerful query syntax to filter flow metadata information based on: field-based exact matches, regular expressions, ranges, boolean operators
- Selected views from the Dashboard module
- IP Geolocation for Client and Servers, with flow aggreagation by City
- Aggregated flow stats: duration, latency, total bytes per connection
- Extensive time machine with absolute or relative year-month-day-hour-minute-second granularity
- Detailed flow table comprising over 30 metadata fields associated with each flow.

## Report

A standardized view reporting high-level flow statistics over the past 7 days.

## Features

- Daily total connections
- Transferred bytes
- Daily average duration
- Daily unique client devices
- Daily unique apps
- Daily average latency
- Hourly connection activity
- Weekly top domains
- Weekly top clients
- Weekly top servers
- Weekly top apps

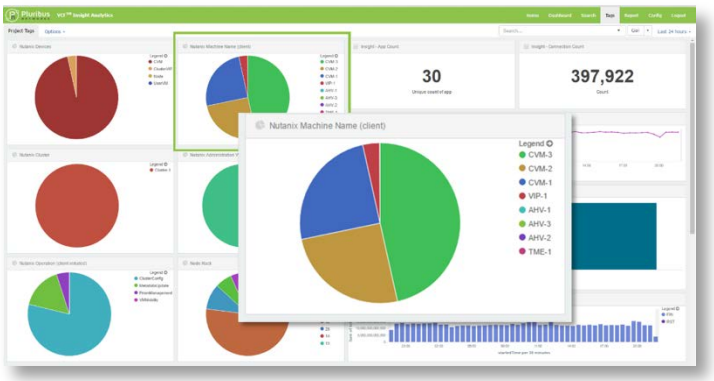
Report view (showing past seven days of flow statistics)

## Tags

With Tags customers can tag their assets (IP addresses, VLANs, MAC addresses, switch ports) with any number of metadata/context tags and then be able to aggregate and filter flows based on these programmable tags.

For example customers can look at the flows in their network by owner, by project name, by type of platform, by application or by corporate initiative etc.

The Tags dashboard offers a customizable set of widgets for customers to build their own dashboard based on the context tags they program on the flows.




Custom Dashboard – it may display predefined and/or custom tags.

## Features

- Define as many as 100 programamble tags for your flows and network assets
- Customize your dashboard to aggregate flows based on tags and any other flow metadata
- Automate the upload of the tagging profile file (CSV or XML file) via REST API
- Option for manual upload of tagging profile file via UI

## Schedule Reports

In version 2.1 of Insight Analytics, the Schedule Reports module is distributed as an early access product.

The Pluribus Insight Analytics Schedule Reports module provides a method of creating customized reports which are then sent by email to the user. Schedule Reports notifies the user of useful monitoring information, such as the information in the standardized view reporting high-level flow statistics over the past 7 days. Reports can be mailed to individual users or to mailing lists.

## Alerts

In version 2.1 of Insight Analytics, the Alerts module is distributed as an early access product.

The Pluribus Insight Analytics Alerts module provides a method of creating Alerts notifying the user of critical monitored events. Alerts Details, Alert Conditions, Schedule Details and Alert Action parameters can all be adjusted depending on the monitoring and alerting requirements. All attributes in a connection record, including any custom attributes, may be compared or counted to define the alerting condition. Multiple conditions can be combined together to create a complex match.

Conditions are of the following types:

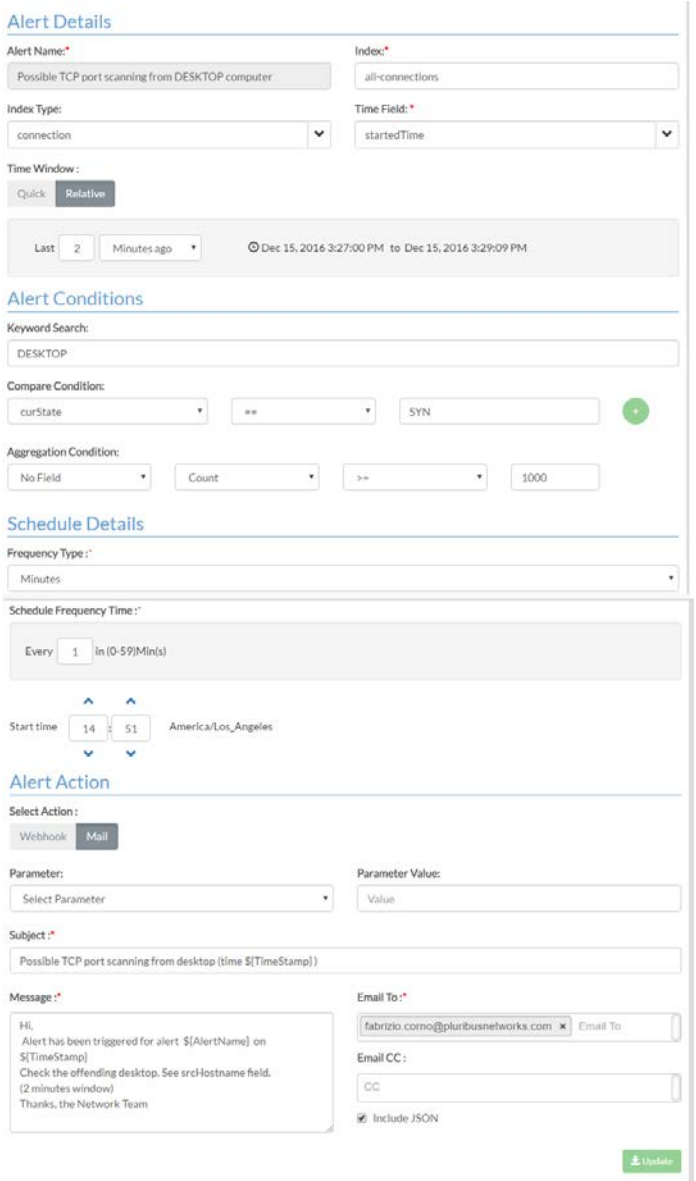
- Keyword Search: a string or a pattern matching any part of the record, according to the Elastic Search “Query String Query” (example: "this AND that OR thus")
- Compare Condition (operators: ==, <, >, =<, =>)
- Aggregation Conditions e.g. count, avg, min, max based on the selection of field.

Potential Use Cases for Pluribus Insight Analytics Alerts and programmable tagging include the detection of the following conditions:

- Port Scanning - The user computers are generating too many unsuccesfull connections per minutes and this may be sign of a port scanning in progress.
- Cluster Node Failure - When a node is unresponsive, Insight Analytics records an excessive number of connections attemps for the cluster housekeeping protocol.
- Unhautorized Access Attempt - The administrator wants to be notified of any unauthorized access attempt to access a restricted application on a server.
- Too Many Concurrent Connections - The number of established connections to an application server passes a threshold over a given time. Too many open connections may impact the server performance and user experience.
- DDOS Attack - When total number of connections in any state to a specific network service (as defined by the TCP port “domain”) pass a threshold over a given time.
- A Lost or Stolen Device Comes Online - Alert is based on MAC address of lost/stolen device.

Alert notifications can be mailed to individual users or lists. The email text can be parameterized to contain the alert name and time. The administrator can attach to the notification email a JSON file containing a set of the records which triggered the alert.

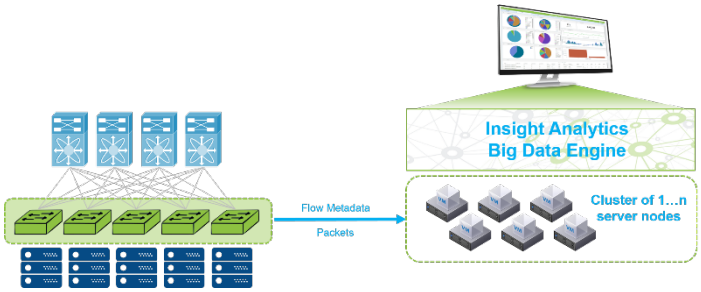
To enable automation via machine to machine communication, the Alert notification may be delivered as a Webhook message.



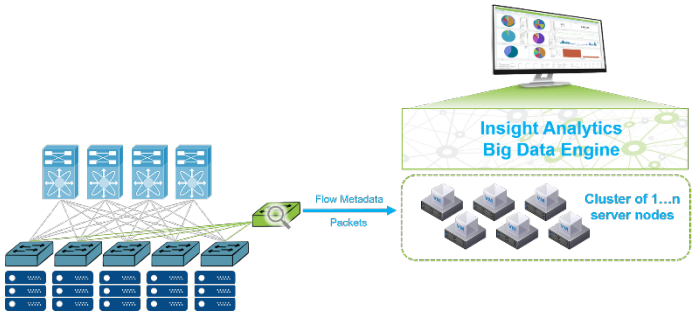

Alert – alert configuration menu showing alert conditons and email template

## Deployment Options

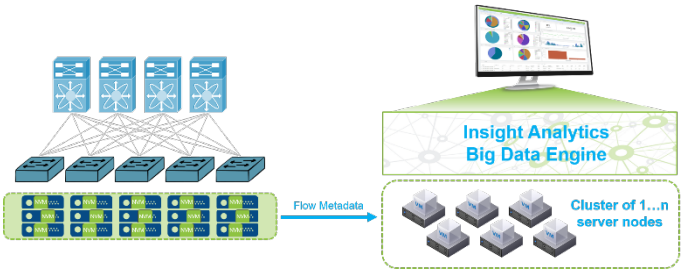
Pluribus Insight Analytics is a monitoring solution for both flows and packets which does not require a packet broker nor additional tools. Insight Analytics provides a cost-effective means to monitor and track the performance of business application flows of information, and can be used with or without existing Pluribus Networks based switching fabrics.




Deployment Option 1 - Pluribus ToR Fabric and 3rd Party Spine.



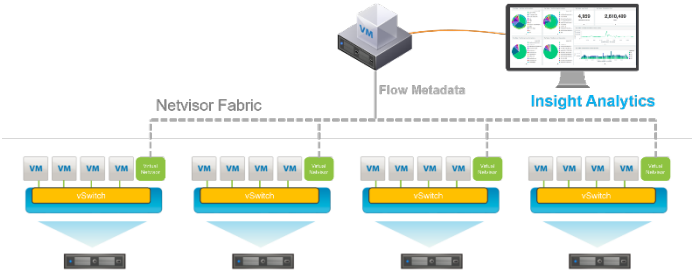

Deployment Option 2 - 3rd Party Network. Switch (or fabric of switches) with Pluribus Netvisor used in lieu of a packet broker.




Deployment Option 3 - Netvisor VM-Analytics probe to analyze virtual machines traffic directed outside or local to a VMware ESXi server.

## Netvisor VM-Analytics

Based on the Open Netvisor® Linux operating system, Netvisor VM-Analytics is a probe delivered and deployed as a VMware ESXi low footprint virtual machine in OVA format. The Netvisor VM-Analytics probe version 2.5.2 is distributed as an early access product.




Netvisor VM-Analytics – Probes fabric across multiple ESXi servers connected to Insight Analytics.

Netvisor VM-Analytics is designed to analyze the virtual machine traffic directed either outside or local to the VMware ESXi server; at least one instance of Netvisor VM-Analytics is required for each ESXi server to monitor. Each Netvisor VM-Analytics instance is connected to a Standard Virtual Switch or to a Distributed Virtual Switch in promiscuous mode. A powerful utility simplifies the provisioning of the Pluribus Fabric of up to 20 Netvisor VM-Analytics instances on multiple ESXi servers.

Use cases include:

- Analize the East/West traffic in a multi layer application deployed on a single physical server
- Report any unwanted traffic for intra local VMs
- Analize ESXi traffic related to hypervisor events such as VM mobiliy and built-in storage

Netvisor VM-Analytics enable Pluribus Insight Analytics to work in a pure virtual environment, without the need to deploy any physical switches.

## Packet Analytics

In version 2.1 of Insight Analytics, the Packet Analtyics application is distributed as an early access product.

The following modules and capabilities are supported:

### Data Broker

This module allows to orchestrate the creation of flow filters and the start and stop of packet capture operations. First the user creates a hardware-based flow filter on Netvisor switches to mirror specific packets to the capture engine of Insight Analytics. A flow rule can then be created to match against a combination of the following fields in a packet:

- Physical switch port
- VLAN
- Source IP
- Dest IP
- Dest Port
- Protocol (TCP, UDP, ICMP, IGMP, IP)

The user specifies where packets should be mirrored. There are three options: Insight Analytics server directly connected to a switch port, Insight Analytics server in a specific VLAN or across an IP network.

The PCAP Engine, which captures and analyzes the filtered packet stream, may be local to Insight Analytics or remote, on a separate virtual machine. While packets are being captured, it is possible to launch the packet analytics dashboard from the data broker to analyze in (quasi) real time the filtered packets.

### Packet Capture

This module manages the PCAP files created either through Insight Analytics or any other applications. PCAP files can be uploaded to Insight Analytics for analytics processing, while being retained in PCAP format for further analysis with third party tools.

### Dashboard

The dashboard is where the user can access the packet analysis for the selected PCAP files. Below is the list of capabilities supported by Pluribus Packet Analytics:

**Main Dashboard**

**HTTP Dashboard**

**TCP Dashboard**

**UDP Dashboard**

**Multicast (PIM/IGMP) Dashboard**

**Error Dashboard**

## Tags for Packet Analytics

The Pluribus Packet Analytics Tags module provides a convenient method of adding business and application context to packets, using user-edited custom-defined tags. The functionality is similar to the Insight Analytics Packet Analytics Tagging. For example, customers can customize a dashboard to aggregate the packet analysis results by owner, by project name, by type of platform, by application or by corporate initiative, etc.

## Integration with HP ClearPass User, Device and Location context

Hewlett-Packard Aruba® ClearPass Policy Manager is a wireless network access control and policy management infrastructure. The Pluribus Insight Analytics Tags may be enhanced with information from ClearPass Policy Manager to view user activity after a user logs into the wireless network. Network flows are associated with an individual user regardless of access method. Pluribus Insight Analytics allows users to analyze compliance, security, and IT resources utilization based on users and user groups.

The tags provided by integraton with ClearPass Policy Manager are:

- Name
- Login
- Domain
- Department
- Group (Active directory: CN, OU, DC)
- Device Family
- Device Category
- Device Name
- Location
- Access Point
- SSID

| Packet Analytics Dashboard | Capability |
|---|---|
| Main Dashboard | • Packet by Protocol over Time – displays protocol types such as TCP, PGSQL, FTP, STP, TLS, etc., over time.<br>• Top 10 Protocols – Pie chart display of top 10 protocols.<br>• Top 10 Destination Port/App – Pie chart display of top 10 protocols destinations by port number.<br>• Top 10 Destination City – Pie chart display of top 10 hosts destination city locations.<br>• Top 10 Source City – Pie chart display of top 10 hosts source city locations.<br>• Top 10 Destination Host – Pie chart display of destination host addresses.<br>• Top 10 Source Host – Pie chart display of source host addresses.<br>• Destination Geo Location – presented in a map format of captured IP traffic locations.<br>• TCP Round-Trip Delay Time – length of time for packet to be sent, acknowledged and received back.<br>• Fragmentation over Time – amount of IP fragmentation occurring over a specified amount of time.<br>• Bad TCP by Time – display of TCP data traffic failing and the specific reason why the data failed to arrive.<br>• UDP Average Jitter – average variation of latency in the packet flow between source and destination.<br>• Packet Count by DSCP Distribution – total number of packets measured by Differentiated Services Code Point<br>• Search Log – packet capture log within the specified time. |
| HTTP Dashboard | • Top 20 HTTP URI – display of Uniform Resource Identifiers listed by IP address.<br>• HTTP Request Method – type of http request; GET, POST, NOTIFY, etc.<br>• Total Packet Counts – total number of packets collected in the packet capture sample.<br>• TCP Round-trip Delay Time – length of time for packet to be sent, acknowledged and received back.<br>• Top Source Domains – display by domain name or address of HTTP connection by source.<br>• HTTP/HTTPS – type of http connects, unsecured or secured.<br>• Top Source Host – display of top TCP host sources.<br>• Top Destination Host – display of top TCP destination hosts.<br>• Top Destination City – display of traffic by name of city.<br>• Top Destination Domain – display by domain name or address of HTTP connection by destination.<br>• Top User Agents – display of user agents and devices connecting by IP address.<br>• HTTP Content Type – display of http content type headers by protocol and MIME types.<br>• HTTP Response Codes – codes by class (informational responses, successful responses, redirects, client errors, and server errors) and specific number.<br>• HTTP Response Time – display of http response times greater than 400 milliseconds.<br>• File Download Type – display of file download types, e.g. EXE, DMG, BIN, PDF, etc.<br>• PCAP Listing – Packet capture details. |

| Packet Analytics Dashboard, continued | Capability |
|---|---|
| TCP Dashboard | • Top Source Host – display of top TCP host sources.<br>• Top Destination Host – display of top TCP destination hosts.<br>• Total TCP Packet Counts – total number of packets collected in the packet capture sample.<br>• Top Source Domains – display by domain name or address of TCP connection by source.<br>• Top Destination Domain – display by domain name or address of TCP connection by destination.<br>• Total Bad TCP Counts – total number of bad packets collected in the packet capture sample.<br>• TCP Trace – timestamped trace data of TCP packets (average.tcp.seq and average.tcp.ack).<br>• TCP Round-trip Delay Time – length of time for packet to be sent, acknowledged and received back.<br>• Bad TCP by Time – count of bad TCP transmissions by type.<br>• TCP Packet Length Distribution – histogram bins showing distribution length of TCP packets.<br>• Packet Count By DSCP Distribution –<br>• Top TCP Source Port – pie chart of TCP source ports by port number.<br>• Top TCP Destination Port – pie chart of TCP destination ports by port number.<br>• All Packet Length Distribution – histogram bins showing distribution length of all packets.<br>• Top TCP Source Mac – pie chart of source MAC addresses.<br>• Top TCP Destination Mac – pie chart of top destination MAC addresses. |
| UDP Dashboard | • Top UDP Source Host – display of top UDP host sources.<br>• Top UDP Destination Host – display of top UDP destination hosts.<br>• # of UDP Packets – total number of UDP packets collected in packet capture sample.<br>• Top UDP Source Port – display of UDP ports originating from source.<br>• Top UDP Destination Port – display of UDP ports at destination.<br>• UDP Average Jitter – timestamped display of average frame time.<br>• UDP Packet Length Distribution – count and size of packet frame len ranges.<br>• Top UDP Source Mac – source MAC address.<br>• Top UDP Destination Domain – display by domain name or address of UDP connection by destination.<br>• # of UDP Packets by DSCP Distribution –<br>• Top UDP Source Domain – display by domain name or address of UDP connection by source.<br>• Top UDP Destination Mac – top destination MAC address. |
| Multicast (PIM/IGMP) Dashboard | • # of IGMPv2 Membership Report – the count of igmpv2 membership groups being reported.<br>• # of IGMPv3 Membership Report – the count of igmpv3 membership groups being reported.<br>• # of Rendezvous Points – the count of multicast rendezvous points.<br>• Total Packet Counts – total count of multicast packets traversing the switch.<br>• # of PIM Assert Messages – number of PIM election messages.<br>• # of PIM Hello Messages – number of PIM advertisement messages.<br>• # of PIM Joins – number of join messages.<br>• # of PIM Prunes – number of prune messages.<br>• Top PIM Types – top PIM types, e.g., RPF Vector or Transport Attribute<br>• Top ICMPv6 Types – top icmpv6 message types, e.g., MLDv2, Router Solicitation, etc.<br>• Top ICMP Codes – top icmp control message types, e.g., Destination Unreachable or Echo Reply<br>• Top IGMP Types – top igmp types, e.g., membership query, membership report, etc. |
| Error Dashboard | • Bad TCP by Time – display of TCP data traffic failing and the specific reason why the data failed to arrive.<br>• HTTP Response Codes – codes by class (informational responses, successful responses, redirects, client errors, and server errors) and specific number.<br>• File Download Type – display of file download types, e.g., EXE, DMG, BIN, PDF, etc.<br>• Total Bad TCP Counts – total number of bad packets collected in the packet capture sample.<br>• Total Fragmentation Counts – a total count of fragmented packets.<br>• HTTP Response Time – display of http response times greater than 400 milliseconds.<br>• Fragmentation Over Time – amount of IP fragmentation occurring over a specified amount of time.<br>• Top ICMP.Code Values – top icmp codes in descending order, e.g., Echo Reply, Destination Unreachable, etc.<br>• DNS ReturnCode Distribution – distribution to DNS return codes, e.g., SERFAIL, NXDOMAIN, etc.<br>• Top DNS Query Names – pie chart of top DNS query names.<br>• Top ICMPv6 Types – message types for icmpv6, e.g., Neighbor Advertisement or Multicast Listener Discovery<br>• Top Ten Protocols – Pie chart display of top 10 protocols.<br>• Top 10 Destination Host – Pie chart display of destination host addresses.<br>• Top 10 Source Host – Pie chart display of source host addresses.<br>• Top 10 Destination Port/App – Pie chart display of destination ports by application. |

# Product Requirements and Information

Pluribus Insight Analytics 2.1 is delivered and deployed as a VMware ESXi virtual machine compatible with vSphere 5.5 or later, in OVA format. The mimimum virtual machine configuration is:

- 128 GB of RAM
- 400 GB SSD
- 16 server class virtual CPUs

**Ingestion Rates**

- Flow Analytics – upto 1000 CPS (Connections per Second)

**Licensing and licensing levels** (Flow Analytics)

- 100M flows/30 days days of historical records (whichever comes first)
- 10M flows/7 days days of historical records (whichever comes first)

Note: Pluribus Insight Analytics Reports and Alerts are each additional licences and currently considered Early Access only.

**Netvisor VM-Analytics 2.5.2 probe**
Is delivered and deployed as a VMware ESXi virtual machine compatible with vSphere 5.5 or later, in OVA format. The mimimum virtual machine configuration is:

- 2 GB of RAM
- 40 GB HD
- 1 server class virtual CPU

A single Pluribus Insight Analytics 2.1 instance can connect to a fabric of up to 20 Netvisor VM-Analytics probes. Netvisor VM-Analytics is licensed as part of a set of 20.

**Hardware Platforms Supported**

- Pluribus: E28Q-L and E68-M
- Pluribus: 9272-X, 9372-T and 9232-Q
- Dell: S4048, S6000, S6010, S4048-T
- Edge-Core: AS5712-54X, AS5812-54-X and AS6712-32X

| Product | Part Number | Description |
|---|---|---|
| 10M Flows for Pluribus Fabric | VCFC-SSC-1YR-10M | 1 Year Subscription VCFcenter 10M flow incl. Standard Support |
| | VCFC-SSC-3YR-10M | 3 Years Subscription VCFcenter 10M flow incl. Standard Support |
| | VCFC-LIC-10M | Perpetual License VCFcenter 10M flows |
| 100M Flows for Pluribus Fabric | VCFC-SSC-1YR-100M | 1 Year Subscription VCFcenter 100M flow incl. Standard Support |
| | VCFC-SSC-3YR-100M | 3 Years Subscription VCFcenter 100M flow incl. Standard Support |
| | VCFC-LIC-100M | Perpetual License VCFcenter 100M flows |
| 10M Flows for 3rd Party Networks | VCFCE68M-LIC-10M | Perpetual License VCFcenter 10M flows and 1xE68-M |
| 100M Flows for 3rd Party Networks | VCFCE68M-LIC-100M | Perpetual License VCFcenter 100M flows and 1xE68-M |
| 100M Flows for 3rd Party Networks (Bundle) | BND-VCFC-2E68M-LIC100M1Y | Perpetual License VCFcenter 100M flows and a fabric of 2xE68-M with Fabric and Virtual Wire License + 1 Year 24x7 Software and RMA Next Business Day Shipping |
| Alerts | VCFC-ALRT | Perpetual License for VCFcenter Alerts Support included with VCFC support. |
| Reporting | VCFC-RPRT | Perpetual License for VCFcenter Reports Support included with VCFC support. |
| Netvisor VM-Analytics (20 PAK) | VCFC-NVM-20PAK | Perpetual License up to 20 Netvisor VMs (20 ESXi Host) for VCFcenter Analytics Applications. Support included with VCFC support. |

## 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 Fabric architecture provides unprecedented insight, agility and security to customers seeking to simplify operations, run more cost effectively and bring new applications online faster.

Learn more at **www.pluribusnetworks.com** and **@pluribusnet**.

Pluribus Networks, Inc., 2455 Faber Place, Suite 100, Palo Alto, CA 94303
1-855-GET-VNET / +1 650-289-4717

May 2017