Network Management & Monitoring

1. Introduction

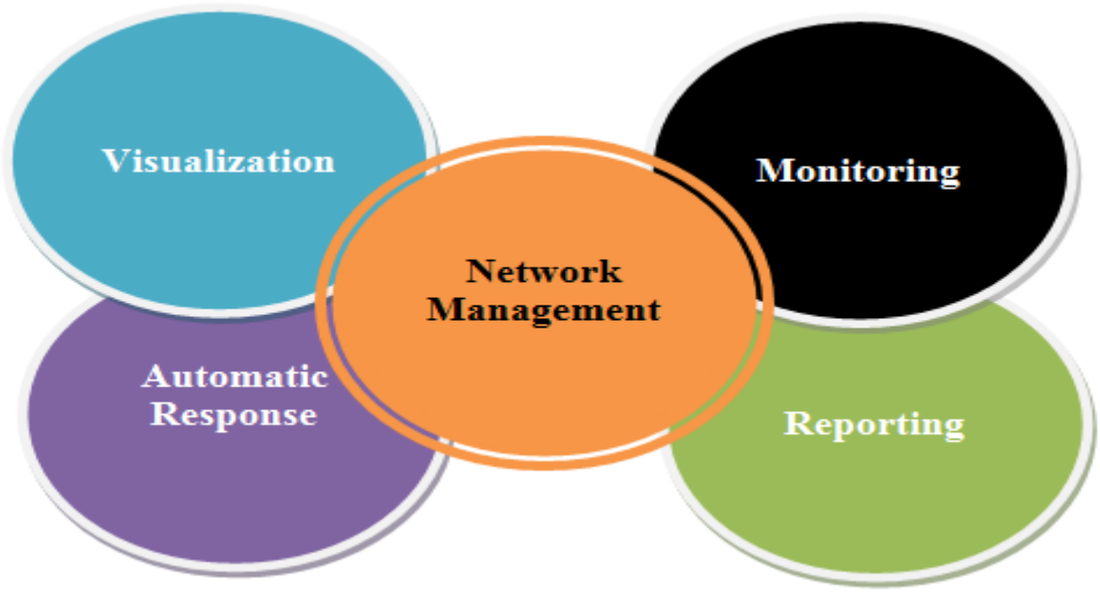
This document describes the project undertaken by PalC Networks for developing a network Management and Monitoring solution for our client -IP Infusion

1.1. Introduction to Network Management and Monitoring

In today's world, the term network management and monitoring are widespread throughout the IT industry. Network management is the process of administering and managing computer networks. Services provided by this discipline include fault analysis, performance management, provisioning of networks and maintaining the quality of service. Software that enables network administrators to perform their functions is called network management software. Network monitoring is a critical IT process where all networking components like routers, switches, firewalls, servers, and VMs are monitored for fault and performance and evaluated continuously to maintain and optimize their availability. One important aspect of network monitoring is that it should be proactive. Finding performance issues and bottlenecks proactively helps in identifying issues at the initial stage. Efficient proactive monitoring can prevent network downtime or failures.

2. Network Management and Monitoring Solution

The below diagram represents the high-level overview of the Network Management solution



2.1. Network Management

The following features are usually requested and seen on most of the network management solutions.

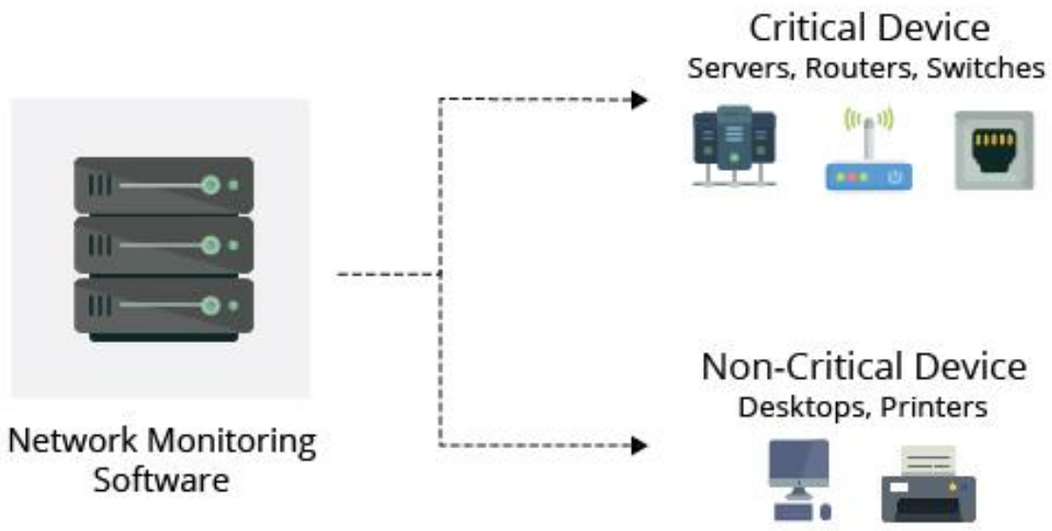
- End-to-end visibility into the health and performance of on-premises, hosted, and cloud infrastructure
- Easily understand the delivery health of cloud services with visualization all along the delivery path
- Quickly see maps of network connections, dependency relationships, and topology information—built automatically. This also lets us know who and what's connected to your network, and when and where they're connected
- Gain better understanding of whether complex network devices are performing as expected
- Be prepared to recover quickly from hardware faults and human errors with automatic backups

- Help ensure devices are configured and operating in compliance with regulatory standards or open standards.
- Plan for the future with capacity forecasting and EOS/EOL tracking

2.2. Network Monitoring

2.2.1. Essential Monitoring

Faulty network devices impact network performance. This can be eliminated through early detection and this is why continuous monitoring of network and related devices is essential. In effective network monitoring, the first step is to identify the devices and the related performance metrics to be monitored. The second step is determining the monitoring interval. Devices like desktops and printers are not critical and do not require frequent monitoring whereas servers, routers and switches perform business critical tasks but at the same time have specific parameters that can be selectively monitored.



2.2.2. Protocols

When monitoring a network and its devices, a common good practice is to adopt a secure and non-bandwidth consuming network management protocol to minimize the impact it has on network performance. Most of the network devices and Linux servers support SNMP (Simple Network Management Protocol) and CLI protocols and Windows devices support WMI protocol. SNMP is one of the widely accepted protocols to manage and monitor network elements. Most of the network elements come bundled with a SNMP agent. They just need to be enabled and configured to communicate with the network management system (NMS). Allowing SNMP read-write access gives one complete control over the device. Using SNMP, one can replace the entire configuration of the device. A network monitoring system helps the administrator take charge of the network by setting SNMP read/write privileges and restricting control for other users.

2.2.3. Proactive monitoring and Thresholds

Network downtime can cost a lot of money. In most cases, the end-user reports a network issue to the network management team. The reason behind this is a poor approach to proactive network monitoring.

The key challenge in real time network monitoring is to identify performance bottlenecks proactively. This is where thresholds play a major role in network monitoring. Threshold limits vary from device to device based on the business use case.

Instant alerting based on threshold violations.

Configuring thresholds helps in proactively monitoring the resources and services running on servers and network devices. Each device can have an interval or threshold value set based on user preference and need. Multi-level threshold can assist in classifying and breaking down any fault encountered. Utilizing thresholds, alerts can also be raised before the device goes down or reaches critical condition.

2.2.4. Dashboards and Customization

Data becomes useful only when it is presented clearly to the right audience. It is important for IT administrators and users to know about critical metrics as soon as they log in. A network dashboard should provide an at-a-glance overview of the current status of your network, with critical metrics from routers, switches, firewalls, servers, services, application, URLs, printer, UPS and other Infrastructure devices. Support for widgets to monitor the required specifics and real-time performance graphs can help administrators quickly troubleshoot problems and monitor devices remotely.

2.3. Requirement

The requirement is to build a comprehensive, proactive network management and monitoring solution ready for deployment in a datacenter.

3. Features to be supported

- Topology discovery
- Interactive dashboard
- Node details
- Topology viewer

4. Approach

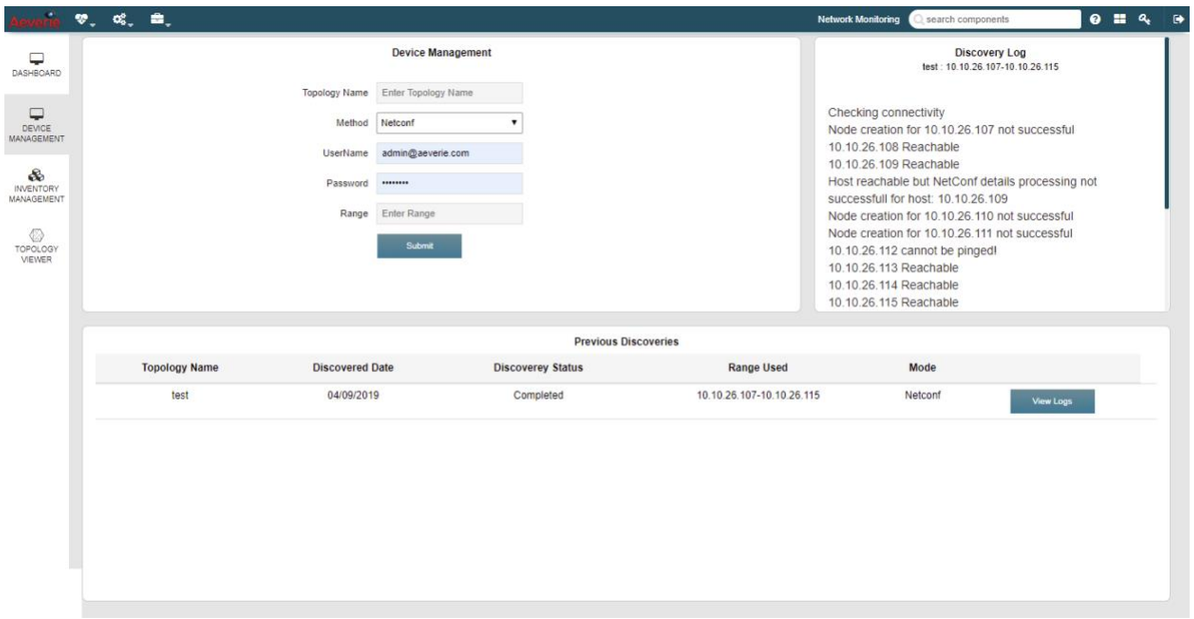
Network management solutions can cater to a large set of appliances and needs. The requirement from our client identified a certain set of features to be supported and how they interplay with each other thereby bringing meaningful insight to the data collected.

Using the network monitoring system we have enabled the following:

- collect detailed information about the network to produce a detailed network inventory.
- can automatically map network topology.
- obtain fault, availability, and performance metrics.

Topology Discovery

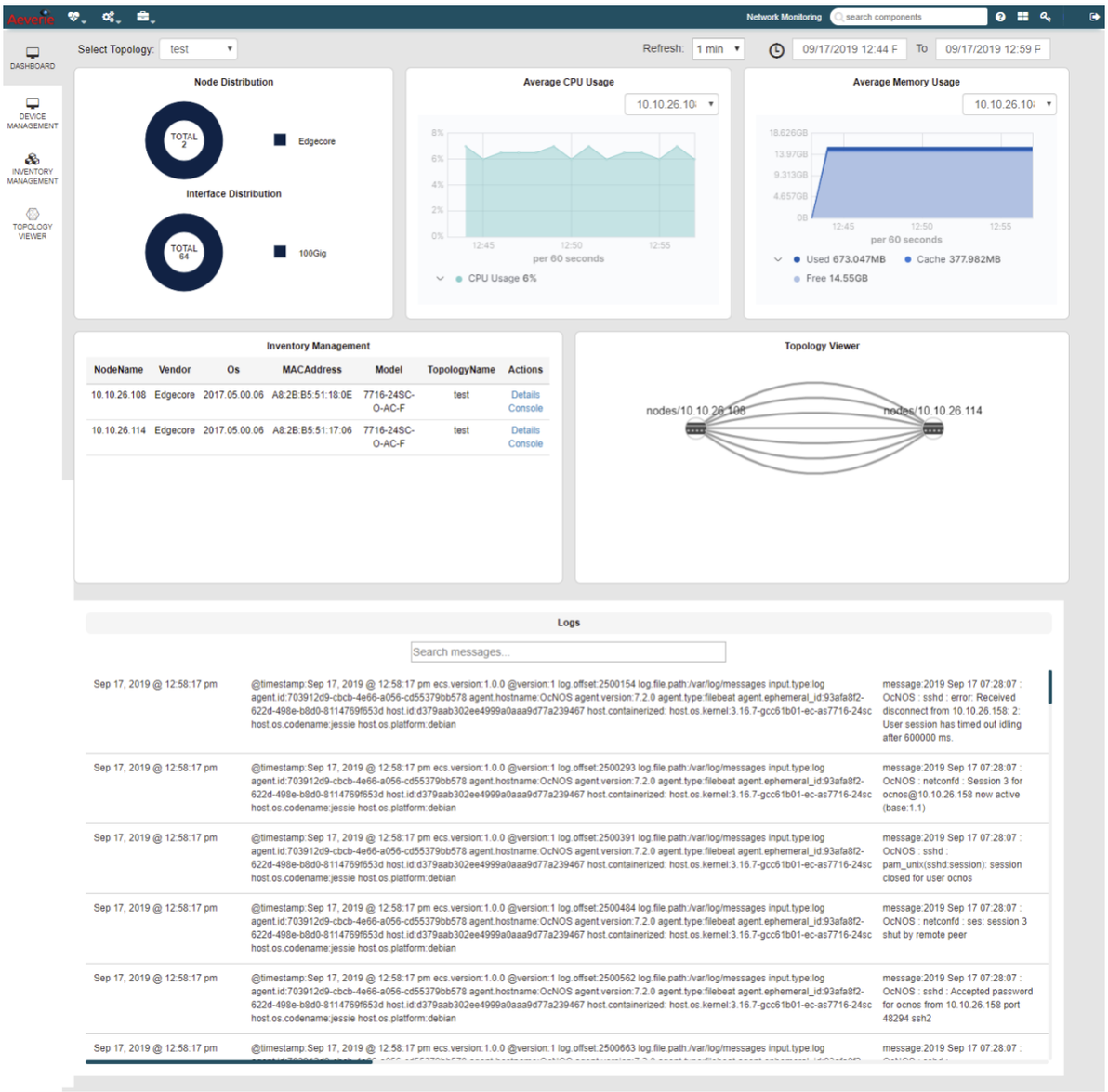
Topologies can be discovered using multiple methods – Netconf, SNMP etc. While logging in, one can enter the range of IP address subnets and the topology matching this subnet will be discovered.



Once the topology is discovered and Netconf or SNMP connectivity is established, the collected logs can be seen below under the tab of “Previous discoveries”. The current discovery log will indicate which devices have responded and what is the status of each device.

Interactive Dashboard

The interactive dashboard will provide the network administrator with one page view of the entire system/topology with each tab having its own GUI. The current details of the topology under purview with alerts and status of the system will be displayed.

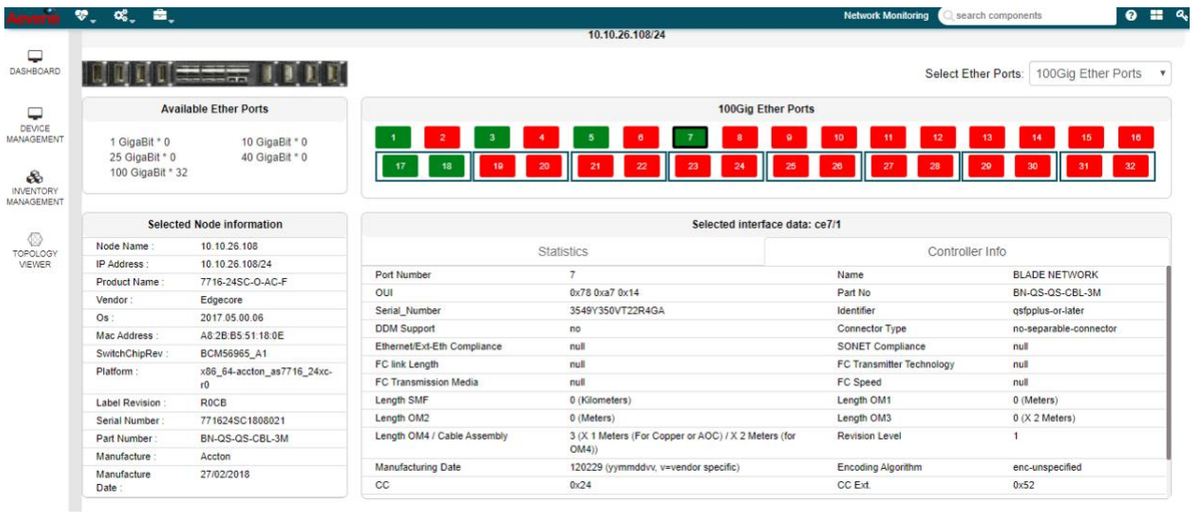


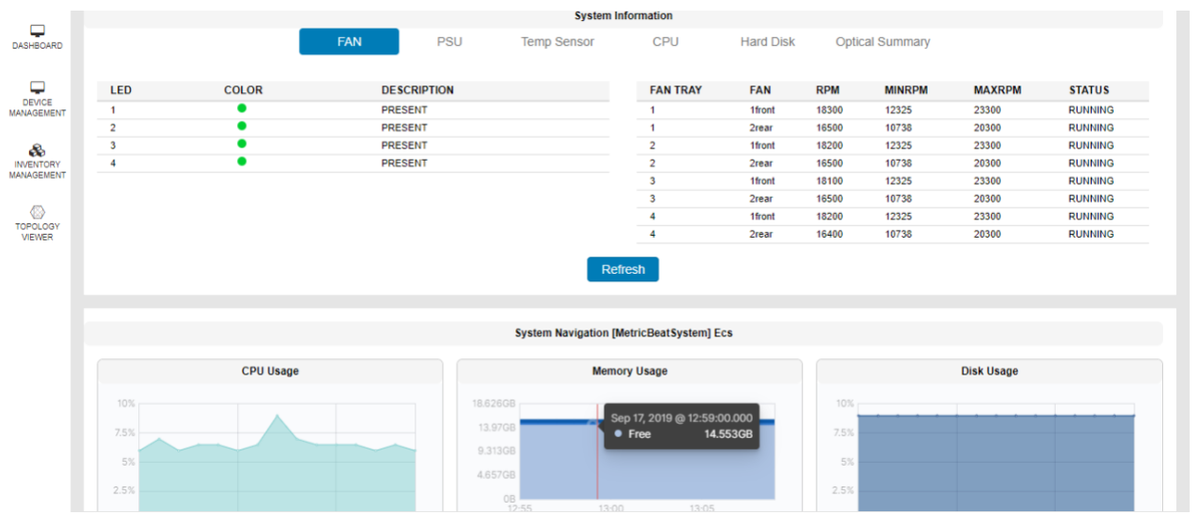
It provides the following:

- Node & Interface Distribution: Node indicates the different components in the system – routers, switches, firewalls etc. The distribution will indicate the classification of the components and the interface distribution will indicate the how the interfaces are classified in the system.
- Average CPU usage: Based on each node which is chosen, the average CPU usage is indicated as a graph. If the CPU usage crosses a certain threshold, an alarm will be raised to the network administrator.
- Average Memory usage: Based on the node chosen, the average memory consumption is displayed as a graph over time and when it crosses a certain threshold, an alarm will be raised to the network administrator.
- Inventory Management: This tab details the specifics of each node/inventory from learnt from the topology discovery. The network administrator can perform actions on individual nodes if there are any alarms.
- Topology viewer: It shows a graphical view of the nodes and the interconnections between them. This is displayed after topology is learnt.
- Logs: This tab details all the logs from each of the node in the topology and the network administrator can search for errors or specific error codes.

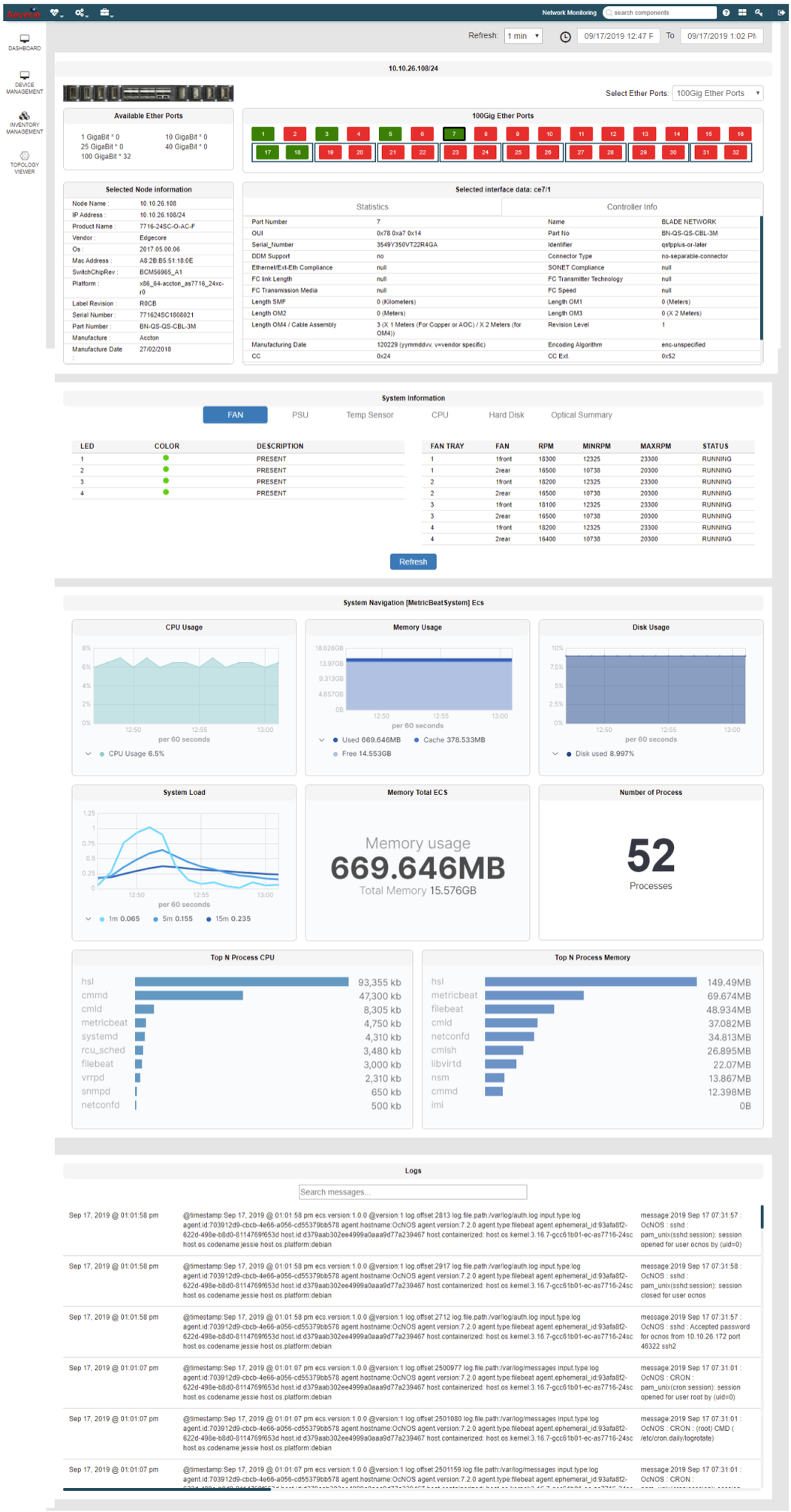
Node details

The GUI indicating Node details are expansive and covers every aspect of the node from the network administrator point of view. It details the topology, IP address, vendor details, port configuration, the current status of the free/used ports, software information ranging from OS details, version, MAC address, platform, Manufacturer details and position in the data center.





If a particular interface is chosen, the details of that interface will be displayed in the GUI. The statistics ranging from Port number, serial number, DDM support, length, manufacturing date to the controller information of name, identifiers, encoding algorithms in use etc will be displayed.


Aeverie
Network Monitoring
search components
DASHBOARD
DEVICE MANAGEMENT
INVENTORY MANAGEMENT
TOPOLOGY VIEWER
Refresh: 1 min
09/17/2019 12:47 F
To 09/17/2019 1:02 PM
10.10.26.108/24
Select Ether Ports: 100Gig Ether Ports
Available Ether Ports
1 GigaBit * 0
10 GigaBit * 0
25 GigaBit * 0
40 GigaBit * 0
100 GigaBit * 32
100Gig Ether Ports
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32
Selected Node information
Node Name : 10.10.26.108
IP Address : 10.10.26.108/24
Product Name : 7716-24SC-O-AC-F
Vendor : Edgecore
Os : 2017.05.00.06
Mac Address : A8:2B:B5:51:18:0E
SwitchChipRev : BCM56965_A1
Platform : x86_64-accton_as7716_24xc-r0
Label Revision : R0CB
Serial Number : 7716245C1808021
Part Number : BN-QS-QS-CBL-3M
Manufacture : Accton
Manufacture Date : 27/02/2018
Selected interface data: ce7/1
Statistics
Controller Info
Port Number 7
OUI 0x78 0xa7 0x14
Serial_Number 3549Y350VT22R4GA
DDM Support no
Ethernet/Ext-Eth Compliance null
FC link Length null
FC Transmission Media null
Length SMF 0 (Kilometers)
Length OM2 0 (Meters)
Length OM4 / Cable Assembly 3 (X 1 Meters (For Copper or AOC) / X 2 Meters (for OM4))
Manufacturing Date 120229 (yymmddvv, vv=vendor specific)
CC 0x24
Name BLADE NETWORK
Part No BN-QS-QS-CBL-3M
Identifier qsfpplus-or-later
Connector Type no-separable-connector
SONET Compliance null
FC Transmitter Technology null
FC Speed null
Length OM1 0 (Meters)
Length OM3 0 (X 2 Meters)
Revision Level 1
Encoding Algorithm enc-unspecified
CC Ext 0x52
System Information
FAN
PSU
Temp Sensor
CPU
Hard Disk
Optical Summary
LED COLOR DESCRIPTION
1 PRESENT
2 PRESENT
3 PRESENT
4 PRESENT
FAN TRAY FAN RPM MINRPM MAXRPM STATUS
1 1front 18300 12325 23300 RUNNING
1 2rear 16500 10738 20300 RUNNING
2 1front 18200 12325 23300 RUNNING
2 2rear 16500 10738 20300 RUNNING
3 1front 18100 12325 23300 RUNNING
3 2rear 16500 10738 20300 RUNNING
4 1front 18200 12325 23300 RUNNING
4 2rear 16400 10738 20300 RUNNING
Refresh
System Navigation [MetricBeatSystem] Ecs
CPU Usage
CPU Usage 6.5%
Memory Usage
Used 669.646MB
Cache 378.533MB
Free 14.553GB
Disk Usage
Disk used 8.997%
System Load
1m 0.065
5m 0.155
15m 0.235
Memory Total ECS
Memory usage
669.646MB
Total Memory 15.576GB
Number of Process
52
Processes
Top N Process CPU
hsl 93,355 kb
cmmd 47,300 kb
cmld 8,305 kb
metricbeat 4,750 kb
systemd 4,310 kb
rcu_sched 3,480 kb
filebeat 3,000 kb
vrrpd 2,310 kb
snmpd 650 kb
netconfd 500 kb
Top N Process Memory
hsl 149.49MB
metricbeat 69.674MB
filebeat 48.934MB
cmld 37.082MB
netconfd 34.813MB
cmlsh 26.895MB
libvirtd 22.07MB
nsm 13.867MB
cmmd 12.398MB
imi 0B
Logs
Search messages...
Sep 17, 2019 @ 01:01:58 pm
@timestamp:Sep 17, 2019 @ 01:01:58 pm ecs.version:1.0.0 @version:1 log.offset:2813 log.file.path:/var/log/auth.log input.type:log agent.id:703912d9-cbcb-4e66-a056-cd55379bb578 agent.hostname:OcNOS agent.version:7.2.0 agent.type:filebeat agent.ephemeral_id:93afa8f2-622d-498e-b8d0-8114769f653d host.id:d379aab302ee4999a0aaa9d77a239467 host.containerized: host.os.kernel:3.16.7-gcc61b01-ec-as7716-24sc host.os.codename:jessie host.os.platform:debian
message:2019 Sep 17 07:31:57 : OcNOS : sshd : pam_unix(sshd:session): session opened for user ocnos by (uid=0)
Sep 17, 2019 @ 01:01:58 pm
@timestamp:Sep 17, 2019 @ 01:01:58 pm ecs.version:1.0.0 @version:1 log.offset:2917 log.file.path:/var/log/auth.log input.type:log agent.id:703912d9-cbcb-4e66-a056-cd55379bb578 agent.hostname:OcNOS agent.version:7.2.0 agent.type:filebeat agent.ephemeral_id:93afa8f2-622d-498e-b8d0-8114769f653d host.id:d379aab302ee4999a0aaa9d77a239467 host.containerized: host.os.kernel:3.16.7-gcc61b01-ec-as7716-24sc host.os.codename:jessie host.os.platform:debian
message:2019 Sep 17 07:31:58 : OcNOS : sshd : pam_unix(sshd:session): session closed for user ocnos
Sep 17, 2019 @ 01:01:58 pm
@timestamp:Sep 17, 2019 @ 01:01:58 pm ecs.version:1.0.0 @version:1 log.offset:2712 log.file.path:/var/log/auth.log input.type:log agent.id:703912d9-cbcb-4e66-a056-cd55379bb578 agent.hostname:OcNOS agent.version:7.2.0 agent.type:filebeat agent.ephemeral_id:93afa8f2-622d-498e-b8d0-8114769f653d host.id:d379aab302ee4999a0aaa9d77a239467 host.containerized: host.os.kernel:3.16.7-gcc61b01-ec-as7716-24sc host.os.codename:jessie host.os.platform:debian
message:2019 Sep 17 07:31:57 : OcNOS : sshd : Accepted password for ocnos from 10.10.26.172 port 46322 ssh2
Sep 17, 2019 @ 01:01:07 pm
@timestamp:Sep 17, 2019 @ 01:01:07 pm ecs.version:1.0.0 @version:1 log.offset:2500977 log.file.path:/var/log/messages input.type:log agent.id:703912d9-cbcb-4e66-a056-cd55379bb578 agent.hostname:OcNOS agent.version:7.2.0 agent.type:filebeat agent.ephemeral_id:93afa8f2-622d-498e-b8d0-8114769f653d host.id:d379aab302ee4999a0aaa9d77a239467 host.containerized: host.os.kernel:3.16.7-gcc61b01-ec-as7716-24sc host.os.codename:jessie host.os.platform:debian
message:2019 Sep 17 07:31:01 : OcNOS : CRON : pam_unix(cron:session): session opened for user root by (uid=0)
Sep 17, 2019 @ 01:01:07 pm
@timestamp:Sep 17, 2019 @ 01:01:07 pm ecs.version:1.0.0 @version:1 log.offset:2501080 log.file.path:/var/log/messages input.type:log agent.id:703912d9-cbcb-4e66-a056-cd55379bb578 agent.hostname:OcNOS agent.version:7.2.0 agent.type:filebeat agent.ephemeral_id:93afa8f2-622d-498e-b8d0-8114769f653d host.id:d379aab302ee4999a0aaa9d77a239467 host.containerized: host.os.kernel:3.16.7-gcc61b01-ec-as7716-24sc host.os.codename:jessie host.os.platform:debian
message:2019 Sep 17 07:31:01 : OcNOS : CRON : (root) CMD (/etc/cron.daily/logrotate)
Sep 17, 2019 @ 01:01:07 pm
@timestamp:Sep 17, 2019 @ 01:01:07 pm ecs.version:1.0.0 @version:1 log.offset:2501159 log.file.path:/var/log/messages input.type:log agent.id:703912d9-cbcb-4e66-a056-cd55379bb578 agent.hostname:OcNOS agent.version:7.2.0 agent.type:filebeat agent.ephemeral_id:93afa8f2-
message:2019 Sep 17 07:31:01 : OcNOS : CRON :

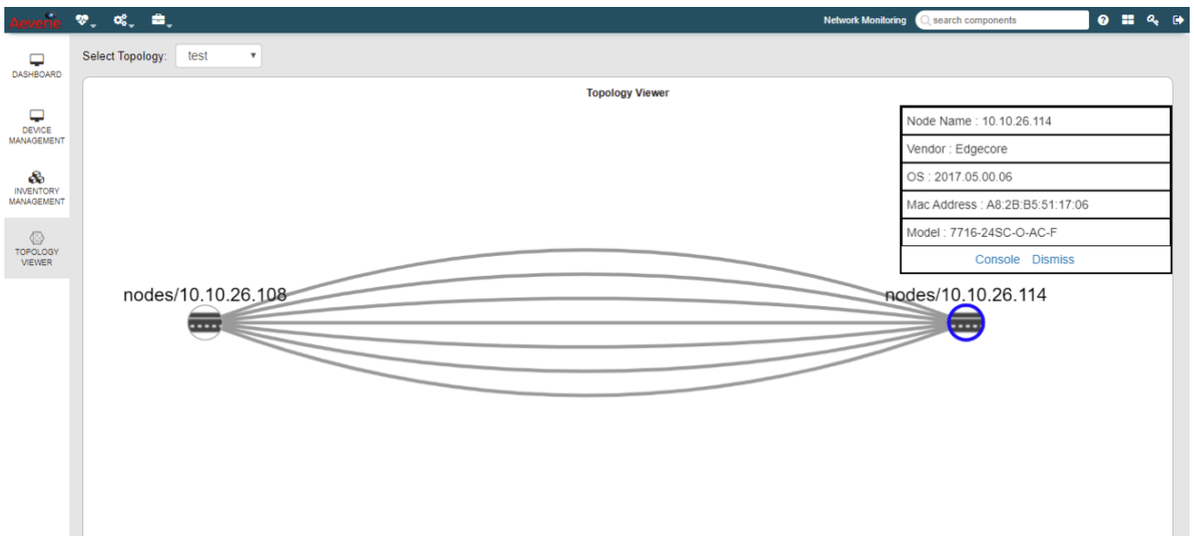
Below this would be system information indicating Fan details, PSU, Temp sensor details, CPU, Hard disk and Optical summary (if available) will be displayed in its own tab. The following metrics will be displayed:

- CPU metrics,
- memory usage,
- disk usage,
- system load ,
- total memory consumed
- and the total number of processes in the node.

The logs of the node will be displayed at the bottom.

Topology Viewer:

The topology viewer displays the entire topology and the connectivity from each node to another.



Clicking on a node will display the details of the node such as the node name, vendor, OS information, Mac address and will also give the administrator an option to open a console to that node for either configuration or verification.

5. GLOSSARY

CPU Central Processing Unit

SNMP Simple Network Management Protocol

CLI Command Line Interpreter

EOL End of Life

NMS Network Management System