NMS Version 2.2.25

Network Management Software (NMS) DATASHEET

1 General NMS Features

- Provides hierarchical multiple thresholds configuration option for each parameter being monitored.
- Has the option to export the views into PDF, Word, Excel, HTML etc. formats depends on the need.
- Provides Role and grouping level based viewing and user management; Role based authorization.
- Stores data for a minimum duration of time configurable by the user, default is 1 year. Flexibility to store the Raw polled points to summarized data reduction based on the storage availability without any restriction.
- System has Node Tags for device grouping and resource/interface tagging for element grouping. Apart from Node Tags additionally system should have options to do device grouping based on default fields and customer fields .
- The solution is a unified system which can monitor networks, servers, apps and any IT or Non-It Communicable device.
- The solution will be able to stop SLA calculation for every node in case of known downtimes with a one click alarm masking capability in the system.
- The solution provides views for any type of device including Networking devices, firewalls, servers, applications , IP Cameras, Wi-Fi, VSAT's, RF devices.
- The system will be able to set minute level configuration to the element level. Polling interval, hierarchical thresholds, report dashboards should be configurable to very component in a single node or across nodes.
- The system is capable of retrieving and showing fault, performance , inventory and SLA data in a single dynamic view.
- The System has proper segregation of admin users and portal users via separate logins and authentications.

2 Discovery

- The system can fetch topology via SNMP for ARP tables from routers , MAC tables from layer 2 switches, cisco Discovery Protocol, Link Layer Discovery Protocol and other standard network discovery protocols. The discovery should be automated and continuous.
- Discovery option works intelligently by identifying the device in the network by the given IP range and categorize into network devices and servers with vendor and model details.
- The system has capability to manually add any additional topology in the network and also allow downloading of topology connections.

3 Polling

- System is capable of configuring business , non-business hours or custom time polling. These configurations are available for every device as well as every component in the device.
- System has capability to configure the maintenance period for any device. When device is in maintenance period there is no polling done and the SLA clock on the device is stopped.

4 Flow Management

- Will be able to associate traffic coming from different sources to application names.
- Will be able to receive flows from non-SNMP-enabled devices, like VMware vSwitch.
- Has options to specify data retention periods .
- Will highlight the IP addresses of the top bandwidth consumers on the network and find out unwanted bandwidth usage.
- Identifies which users, applications, protocols,top routers, and top interfaces are consuming the most bandwidth.
- Monitors Class-Based Quality of Service (CBQoS) to find out if traffic prioritization policies are effective and if business-critical applications have network traffic priority. Also support CBQoS Nested policies.
- Will be able to monitor network traffic by capturing flow data from network devices, including Cisco Netflow v5 or v9, Juniper J-Flow, IPFIX, sFlow, NetStream data and also sampled Netflow data. System has capability to alternatively capture flow data .

5 Alerts, Fault Management & Reporting

- Provide Alarms Suppression capabilities so that any duplicated events can be tracked to provide just a single event notification
- Provides alarm suppression with hold time and aid in prevention of flooding
- Sends alert via E-mail, SMS, Execute Batch file, SNMP Trap.
- Monitor VMWare ESXi servers, Hyper-v Servers, Xen servers, KVM and all market standard virtualization environment
- System covers geographically distributed networks through multi-level scalable distributed deployment architecture
- Cover geographically distributed networks through multi-level scalable distributed deployment architecture
- Supports Real-Time report generation for checking continuous reachability of target device
- Supports instant diagnosis of the node status through Ping, Telnet and SNMPwalk
- System has capability to create a user level repository of all the issued being faced. Users will have the rights to add data to this repository and system should be intelligent to automatically retrieve back information from here based if same issue re-occurs
- Detects & highlight faults (abnormal situations) occurring anywhere within the network
- System has customisable multi-level Severity definition, handles events automatically and informs the designated person as per operational requirement
- System supports separate Rule Engine based alarms apart from the generic threshold.

  a. Has the capability to configure Device Group based, Node Based, Resources/Interface based, Aggregation link based.
  b. On Selection of Nodes/Resources/Aggregation links it have flexibility to filter based on fields available in node information.
  c. Rules will have option to apply configuration on top of performance value or based on configured threshold alarms .
  d. Rules will have option to configure the breach based on min, max and average values .
  e. Has the option to configure rules n repeat counters.
  f. Has the options to select custom alarm and clear alarm messages for individual configured rules.
  g. Has the option to send severity levels like error, warning and information .
  h. Notifications support are based on configured rules.

- Any graph or network diagram configured will have functions to associate every component in the diagram to an existing node or resource.
- Provides provision to draw & map user specific network diagram. System should support Drag & Drop based Network Diagram builder.
- Will provide a notification mechanism that allows administrator to define what notification channel to be used in different time of days, and able to trigger multiple notifications to alert multiple person and actions.
- Will provide escalation and acknowledgement function to provide the mechanism to ensure alternative personnel will be alerted when there is a critical situation and acknowledgement mechanism for generated alerts. The escalation will be available for any number of hierarchical sequence.
- Monitors all traffic from all the interfaces of the network device. Provides traffic Utilization based on individual interface level, nodes level or based on the group by location, branch, departments etc. as an Avg, Min and Max bandwidth, utilization, throughput or any custom monitoring parameters.
- Provision to change the polling interval to any frequency depending on the priority till the individual component / resource level like each interface might have the different polling interval in the same device based of the criticality and importance of service customer
- Has provision to change the polling interval to any frequency depending on the priority till the individual component / resource level like each interface might have the different polling interval in the same device based of the criticality and importance of service customer
- Allows end-users to browse all reports using any web browser like Internet Explorer, Mozilla Firefox, Google Chrome etc. without the need to install any report specific software
- Provides online and offline reports that allow the user to view the present usage of their devices. Reports generated will be exportable in the format of HTML, PDF, Excel and CSV
- Provides standard reports that display current status of nodes and interfaces. Reports can be viewed on daily graph (5 minute average), weekly graph (1 hour average minute average), monthly graph (1 hour average) and yearly graph (1 day average)
- Provides the option to get the required report as an all hours, business and non business hours for detailed analysis. Also provides report on single or multiple statistical split based on the operation need as option during the configuration
- The system will have a integrated service management tool from the same OEM

- The system has exhaustive threshold defining capabilities for various monitored parameters. All thresholds should have set point , reset point, set point message and reset point message for ease of use.

- Automatically learns IP Networks and their segments, LANs, hosts, switches, routers, firewalls etc. and establishes the connections and to correlate

- Filter topology view based on device group, node tag, vendor, model, IP address, host name etc.

- The system has provision to search specific device or resources in a view

- **System provides many different types of topology representation. based on :**

  1. Display physical connections of the different devices being monitored in the system
  2. Display maps of the entire network or networks in a single view
  3. Display customer maps based on user configurations
  4. Display maps based on geo locations

- Measures & monitors the following QoS parameters :Latency, Packet Loss,Probes,Packets,Delay,MOS,Jitter,RTT (Round-Trip-Time) and Detect quality deterioration by tracking QoS parameters

6 Configuration Management

- Alerts user on any changes made to the current running configuration file of any monitored device

- Allows scheduling of automatic download of the configuration file from the network devices

- Downloads current running configuration file from the network devices

- Maintains/stores the configuration files of all the monitored devices for reference

- Provides a web base and intuitive user interface that showcases the list of devices whose configuration file got changed with option to highlight the changes