NIT No: AEML/ MDB/2019-20/39

Supply, Installation & Commissioning of SCADA & ADMS System at Adani Electricity, Mumbai Ltd.

Generic Specification of NMS for Network Management

Description

Network management software for monitoring of IT networks viz. Routers, Switches, Firewalls, Wireless devices, Servers, Workstations, Other SNMP-enabled devices and should be vendor agnostic.

Software License

1. License should be perpetual
2. Licenses for 200 devices which should be perpetual.
3. The license has to be one integrated package with Database, HA and load balancing clusters, Network Scalability, Built in Ticketing system, Syslog server, Customizable Dashboard / Map designer, NetFlow/Jflow / Sflow as part of single license.
4. Should provide horizontal / vertical scalability as the network expands.
5. Software has to be windows based.

Monitoring Capabilities

1. Should automatically provide real-time, in-depth network performance statistics after discovery/configuration of devices, including but not limited to:(a) CPU load (b) Memory utilization (c) Interface utilization (d) packet loss. Should be capable of monitoring varied parameters available as part of MIB definition of the monitored device.
2. Graphical status representation for devices, optical links, ethernet links, power supplies, fans, and any other device sub-component.
3. Should show statistics like interface bandwidth, current traffic in bps, total bytes received/transmitted etc.

4. Should be able to discover and troubleshoot network paths hop-by-hop for both on premises and cloud environment for specific TCP connections
5. Should display information including alerting for major routing protocols (BGP, OSPF, RIP, EIGRP).
6. Should help with multicast traffic information monitoring, Packet drops, Ping jitter, VoIP jitter.
7. Should display device status and interface status by different colors to represent warning and critical status.
8. Should monitor hardware health for popular vendors like Cisco, DELL, F5, Juniper, HP, Fortinet etc. and should allow alerting and reporting on hardware health monitoring
9. Should show both real-time details and historical details in form of charts with option to choose the time periods
10. Should be able to discover and monitor both IPv4 and IPv6 devices
11. Should have options to specify data retention periods.
12. Should have the option to determine device availability using SNMP V1, V2C & V3.
13. Should have feature to access dashboard using Mobile App (for iOS, Android or Windows Phone operating systems).
14. Customize event actions. Viz Reporting tool, Project setup wizard, Hierarchical supervision structure, Task scheduler, Network Dashboard, Configuration Signature Check, Configuration File Compare.

Network Discovery

1. The proposed monitoring solution should be able to discover devices in the network with SNMP and ICMP capabilities automatically, on input of (a) IP address ranges (b) subnets (c) individual IP addresses (d) Active Directory
2. Should allow interface filtering on discovery results to exclude virtual interfaces and access ports and select interfaces based on pattern matching.
3. Should have option to automate and schedule discovery process
4. Graphical User Interface and Customization

Graphical User Interface and Customization

1. The proposed management solution should provide a high-quality graphical user interface.
2. This web console should be accessible centrally or remotely
3. The web console should allow multiple users to log in at the same time
4. It should have load-balancing options available if too many users login at same time
5. It should provide a unified view of alerts, traps, events, syslog messages in a single page
6. It should quickly highlight devices with issues, based on different properties like response time, cpu load, memory usage, high interface usage etc.
7. It should allow creation of custom dashboards and restrict views for users based on devices or interfaces, i.e. it should have role-based access
8. It should log user actions and events in the web console for audit purposes and they should be available for alerting and reporting
9. It should allow interactive charting for node, interface, volume charts etc.
10. It should provide a dynamic dashboard that allows in-depth visibility and correlates disparate historical data points across different part of the infrastructure. The result should be exportable with a tabular format.

Advanced Reporting

1. The proposed monitoring solution should provide current and historical out-of-the-box reports for various statistics monitored.
2. Should be able to generate / create the report via the web console
3. Should be able to generate statistical reports that can be used as reference for future planning or troubleshooting
4. Should allow customization of reports by adding/removing columns, setting filters, specifying timeframes, grouping columns etc.
5. Should allow advanced customization by providing options to enter custom queries to query the database directly
6. Should have options to save the customized reports permanently and have them accessible in web console

7. Should allow reports to be sent out on schedule as daily, weekly, monthly, Qtrly, Yearly report.
8. Should allow emailing of dashboards created in web console
9. Should be able to configure both charts and tables into a single report.
10. Should have options to import/exports reported created by other users
11. Should support multiple formats such as pdf, XML, HTML and CSV.

Advanced Alerting

1. The proposed monitoring solution should be able to manage and display events/alerts in the web console
2. The alerts and events information should be logged into the database for future reference
3. The alerting mechanism should allow complex conditions and condition groups to be specified for narrowing down the alert condition.
4. It should allow custom queries to be entered to create rules against the database
5. It should allow creation of new alerts from scratch and also customizable threshold limits.
6. Should have support for variables in alert email message to make the content more self-explanatory.
7. Should allow alerts suppression during scheduled maintenance

Grouping

1. The proposed monitoring solution should allow grouping of devices by various properties -- by department, by location, by name and by other properties gathered
2. Should be able to define dependencies and relationships between connected devices and interfaces to avoid false-positive email alerts in case of outage.

Network Maps

1. The proposed monitoring solution should be able to represent the network pictorially and display performance details of devices in real time
2. Should allow customization of background, icons etc. and should allow multiple network maps to be nested with drill-down capabilities.

3. Should be able to display not just the device status on the map but also status of any other detail obtained.
4. Should have the ability to show the link utilization.

Support

1. The proposed monitoring solution should not be vendor-specific
2. Traffic and bandwidth usage monitoring, internet usage monitoring, free upgradation to higher version within support period
3. With a centralized operations console view, alert acknowledgement and reporting interface

Antivirus Solution

Description

The antivirus solution shall have one central server for management of antivirus from central location. The central server shall be connected to the internet for getting the updates. Once the updates are available the server shall push the updates to the antivirus client machines based on the set schedule and based on user demand. Further details shall be as follows:

Software License.

1. The license for Management console: Validity shall be till the end of FMS
2. The license for all the physical and VM servers and workstations as per the architecture of system at MCC & BCC. The validity of these licenses shall be till the end of FMS.

Solution Capabilities:

1. Advanced Malware Protection using Machine Learning.
2. Antivirus management console:
    a. From the management console, it shall be possible for administrators to view and manage the entire security landscape and apply the defined and chosen security policies to every endpoint in SCADA MCC and BCC. This

helps deploy security rapidly and with minimum interruption, using a wide range of preconfigured scenarios.

b. It shall be possible for administrator using management console to define the various security profiles and apply them to a single or group of servers/workstations.

3. Exploit Prevention: Prevents malware executing and exploiting software, delivering an extra layer of protection against unknown, zero-day threats.
4. Behavioral Detection and Automatic Rollback: Identifies and protects against advanced threats, including ransomware, fileless attacks and admin account takeovers. Behavior Detection blocks attacks, while Automatic Rollback reverses any changes already made.
5. Protection against encryption for shared folders: A unique anti-Cryptor mechanism can block the encryption of files on shared resources conducted by a malicious process running on another machine on the same network.
6. Network Threat Protection: Malware using a buffer-overrun attack can modify a process already running in the memory and in this way execute malicious code. Network Threat Protection identifies network attacks and stops them in their tracks.
7. Web console: To improve fault-tolerance web console to centrally manage both physical and virtual machine environments
8. Application Control: Reduces exposure to attack, giving total control over what software can run when on SCADA servers/workstations.
9. Dynamic whitelisting: For a better applications categorization, Application Control uses a Dynamic Whitelisting Database.
10. Device Control: This feature allows users to set, schedule and enforce data policies that control removable storage and other peripheral devices – connected to a USB or any other bus type.
11. Host Intrusion Prevention (HIPS): Regulates access to sensitive data and recording devices, without affecting the performance of authorized applications.
12. Protection for

    • Windows and Linux
    • Windows and Linux servers

- Windows Server containers
- Android and other mobile devices
- Removable storage

13. Unparalleled defense against

- Software exploits
- Mobile malware
- Advanced threats
- Fileless threats
- PowerShell & script-based attacks
- Web threats

14. Features should include

- Anti-Malware
- Vulnerability Management
- Security Policy Adviser
- AI-based learning
- AMSI support
- Encrypted traffic scanning
- Process isolation
- Firewall and OS firewall management
- Integrated EDR agent
- Adaptive Anomaly Control
- Server and containers protection
- Protection for terminal servers
- Windows Linux Subsystem support
- Mobile Threat Defense
- OS encryption management
- System configuration & deployment
- Patch Management
- Reporting