Network Monitoring Tools and Technologies

[1]Bhavya Jani, [2]Kajal Jain, [3]Narendra Vishwakarma
[3]Assistant Professor
[1, 2, 3] Department of CE/IT,
[1, 2, 3] MPSTME NMIMS University, Shirpur, Maharashtra, India

Abstract: This review paper presents a detailed report of contemporary network monitoring tools and related technologies, which incorporate features such as map generation, fault detection, network configuration, device discovery, network traffic trend prediction and monitoring and alerting. The widespread class of applications are based on Simple Network Management Protocol (SNMP), Traceroute and Packet Internet Groper (PING) which are used for transmitting and receiving network performance information, searching the path from source to destination node and testing whether a node is alive respectively. Examples of numerous automated network monitoring tools are Nagios, SolarWind's Orion Network Performance Monitor, NetBrain and PRTG.

Index Terms **– Fault Detection, Network Automation, Network Configuration, Network Monitoring.**

I. INTRODUCTION

Organizations devote a considerable amount of manpower and resources on their networks. They are always trying to achieve minimum downtime for their concerned networks. Network monitoring for gathering data and improvising upon the networks is a contemporary method used to accomplish this task. This in turn has increased the formulation of various network monitoring techniques, tools, formats and standards. The most widespread tools such as network management scheme are derived from benchmark network management procedures that offer an all-encompassing outlook of the network plus each of the present devices. Evidently, there exist various other tools which may not be as complex compared to a complete network management application but prove to be equally constructive for the purpose of monitoring specific characteristics of performance of the network. This review paper will comprise of fundamentals of network monitoring, different types of monitoring tools and their highlighted features.

II. NETWORK MONITORING

Network monitoring consists of observing as well as analyzing the behavior with status of complete or partial network that comprise the devices which require monitoring and management. Information concerning the generic condition of the complete network to detect failing areas or those in need of management are collected by network monitoring tools. The tools are capable of checking the total performance of networks compared with a baseline model network in which everything functions perfectly. Using the help of such tools, network administrators effortlessly observe the performance and operation of network infrastructures. Information for network analysis is also provided by these tools. The detailed parameters of a network monitoring tool are discussed in the following phases.

II.I. MAP GENERATION

Network Maps are utilized by the monitoring tools for the ease of visualization of the entire network of an organization either as a centralized network system or as a distributed network where the maps are divided according to the logical separations of the network. Network device discovery further aids the process of map generation by identifying the devices present in the network. Hence many tools integrate device discovery and mapping in order to simplify the mapping process. The maps itself can be a logical view such as a graph of vertices and edges where the vertices represent different devices in the network and the edges represent the relations or interconnections between them or it can be a geological map with the device icons placed on actual geo map that represents its physical location and are interconnected by edges for a better visualization. There are various approaches used for network mapping: route analysis, SNMP based approaches and active probing. Route analysis gathers information from the routing protocols for building the map. The SNMP based approach retrieves data from devices such as router and switch MIBs for building the map. The active probing approach uses a series of trace-route-like probe packets for building the map.

II.II. NETWORK CONFIGURATION

Network configuration is a very important function for precise functioning of the network infrastructure of any organization. Administrators ought to be capable of configuring IP addresses of various types of devices along with other types of configurations like setting up routing protocols for layer 3 devices, updating existing configuration, adding dynamic manual routes on the fly, etc. These options offer administrators flexibility for configuring network devices on the network.

II.III.FAULT DETECTION AND ALERTING

Fault detection include finding, pinpointing and notifying the fault that can occur anywhere in the network. The fault can be in the device itself which may again be device specific such as a memory segmentation fault in a router or it can be a common occurrence such as a link failure/node failure. Alerting encompasses smart alerts that reduces unnecessary network alerts. It can allow you to create custom set of actions which can be taken when certain conditions are met. Alerts are also encapsulated and sent to specific users with further encapsulation to the levels of detail for different types of users.

II.IV.DEVICE DISCOVERY

Device discovery is done using the SNMP protocol. The devices are scanned, added to the database and imported into the monitoring tool. Device discovery identifies the type of device along with other details such as the layer in which it works, average response time, packet loss, operating-system, memory processing power, etc.

II.V. NETWORK TRAFFIC TREND PREDICTION

Network traffic analysis is very important in attaining information security while considering banking, e-commerce and business related organizations where the information communicated within the network is highly confidential. It is a proactive approach to ensure the security is not compromised within the network. Trend prediction is beneficial as it can be used for dynamic bandwidth allocation and network planning. It also avoids congestion by analysing and forecasting the traffic. It can also identify the core links of the network and notify the user so that a high alert can be placed over that link.

III. OVERVIEW OF THE EXISTING TOOLS

There exist numerous network performance application tools of different types today. Open-source and industrial products offer options for network monitoring. The aim of this review is to present a quick look into the variety of currently available tools.

SolarWinds' Orion Network Performance Monitor

SolarWinds offers an assortment of solutions for management of network and its resources varying from distinct monitoring software to full-fledged, featured network administration and monitoring platforms. Orion, SolarWinds' across the board monitoring tool is constructed on the basis of SNMP. The Orion incorporates a web technology based interface including monitoring network latency in real-time, availability, bandwidth utilization, and numerous other network performance parameter metrics. Data is summarized by the system automatically. Also, the system identifies the main events as well as alerts for straight forward troubleshooting plus monitoring [1]. Moreover, every alert, statistic, or event possesses drill-down capabilities which offer complete details of the specified information. The interface is customizable and aids in mapping the network visually along with its components and links, hence simplifying the task of finding errors and monitoring the network. In spite of variety and complexity of provided information, the application program is effortless to operate. Orion incorporates auto-configuration and auto-discovery features which shorten the task of manually inserting devices in the network that require monitoring.[2]

NetBrain

NetBrain provides a dynamic mapping feature wherein the maps created are data driven, and automatically updated to reflect changes in the network. The maps contain the detailed configuration as well as design data embedded within each dynamic diagram. It offers fault detection within the GUI with explicit annotations for different status of a network link such as red for device down, green for device up and yellow for device unstable/flapping. It also identifies status of the exact device within the network map for enhanced fault recognition. The tool presents capability to collect data over a period of time for capturing faults over transitory issues. NetBrain discovers the network in its entirety comprising of the network devices and the design of the network. This is accomplished via a patented neighbor-walking discovery engine combined with advanced network modelling. During the discovery process, NetBrain simultaneously analyses data collected from SNMP and the CLI, and decodes network design every step along the way. NetBrain includes a traffic path analysis by allowing users to visualize dynamic traffic paths across complex networks considering: dynamic and static routing, address translations, firewalls and MPLS [3]. By simply specifying IP addresses between two endpoints, it scrutinizes live gateways and routing information on each device to determine traffic.

Nagios

Nagios gives a centralized picture of the complete IT network infrastructure along with in depth status information that is accessible via a web interface. The Nagios core reads its configuration data from text files in order to configure the network devices. It allows flexibility by providing auto discovery scripts and change management interfaces. Nagios incorporates fault detection and problem remediation by implementing event handlers that permit automated rerun of devices, services and applications that have failed. It provides fast detection of infrastructure outages and alerts the users through email or SMS. Alert acknowledgements allow communication to known issues and problem response. Device discovery in Nagios is not present by default but it is an open source platform and can be easily customized by add-ons or plugins suited for the user. It analyses the traffic, trends and makes planning policies to ensure that the users are aware of the aging infrastructure. It also schedules downtimes that allows alerts to be suppressed during infrastructure upgrades. [4]

PRTG

PRTG shows devices and their connections along with their information of their status. The maps can be customized by simply using drag and drop functionality for placing the devices in the map as well as placing traffic charts and top lists. It provides monitoring in a distributed manner residing in different locations and separated within an organization. PRTG network monitor allows failover tolerant monitoring and automatic failover handling by switching over to a secondary device if the primary master of the cluster is down by immediately taking over its responsibilities. It provides numbers, graphs and statistics about the data that's monitored or configured. It also provides multiple user interfaces via Ajax web interface, enterprise console windows application with a seamless link to Ajax web interface as well as mobile apps for IOS as well as android which means that the PRTG monitoring tool is highly scalable and can be used with a variety of devices. [5]

IV. CONCLUSION

Every network must have monitoring tools. Monitoring tools are vital in every type of organization. They boost network performance, reliability, stability, while permitting the user to control the complexities in contemporary network. This review showed that there is as such no perfect tool for monitoring that meets all the needs of every organization. Each tool has its own special features that makes it different from the other and it totally depends on the requirements of the organization in order to select a monitoring tool. SolarWind's Orion network performance monitor covers all the major components required for monitoring but it has a complex GUI which needs to be learnt properly in order to use it and it is also costly. Nagios is also a very good tool and it is open source hence we can customize and personalize it according to the specific organization needs as well as we can create our own plugins of the features that we need to add and integrate it with Nagios but it needs experts and development in order to customize the tool according to the requirement which may add to the cost.. It also provides encapsulated alerting. NetBrain is also another tool that is very fit for monitoring. It is good for organization which studies the network and performs analytics on the network traffic or trend prediction as it provides all these features. NetBrain can also be used in organizations where most of the tasks are automated as it provides many automation features. PRTG can be used where distributed monitoring is required as it provides distributed form of monitoring. It can also be used where visualization of the network is required as it provides geo maps of a network in real time.

REFERENCES

[1] M. G. Nagaraja R. R. Chittal K. Kumar "Study of Network Performance Monitoring Tools-SNMP" *IJCSNS vol. 7 no. 7 pp.* 310 2007.
[2] "IT Management Software & Monitoring Tool| SolarWinds" [online] Available: https://www.solarwinds.com/.
[3] "Network Automation Software| Network Automation Tool| NetBrain" [online] Available: https://www.netbraintech.com/.
[4] "Nagios - The Industry Standard In IT Infrastructure Monitoring" [online] Available: https://www.nagios.org/.
[5] "PRTG Network Monitor » All-In-One Network Monitoring Software" [online] Available: https://www.paessler.com/prtg.