Lab – Researching Network Monitoring Software

Objectives

Part 1: Survey Your Understanding of Network Monitoring

Part 2: Research Network Monitoring Tools

Part 3: Select a Network Monitoring Tool

Background / Scenario

Network monitoring is needed for any sized network. Proactively monitoring the network infrastructure can assist network administrators with their day-to-day duties. The wide variety of networking tools available vary in cost, depending on the features, number of network locations and number of nodes supported.

In this lab, you will conduct research on available network monitoring software. You will gather information on software products and features of those products. You will investigate one product in greater detail and list some of the key features available.

Required Resources

- PC with Internet access

Part 1: Survey Your Understanding of Network Monitoring

Describe network monitoring as you understand it. Give an example of how it might be used in a production network.

In today's world, the term network monitoring is widespread throughout the IT industry. 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.

Part 2: Research Network Monitoring Tools

Step 1: Research and find three network monitoring tools.

List the three tools that you found.

- Ip monitor
- Nagios Core
- ntop

Step 2: Complete the following form for the network monitoring tools selected.

Vendor	Product Name	Features
Solarwinds	IpMonitor	● Monitor network devices, servers, VMware hosts and applications from one console ● Receive alerts for availability and performance issues ● Monitor network status on maps and NOC view ● Minimize downtime by automating remediation actions ● Enhance monitoring with built-in reports and dashboards
Nagios	Nagios Core	● Nagios Core serves as the basic event scheduler, event processor, and alert manager for elements that are monitored. ● I t features several APIs that are used to extend its capabilities to perform additional tasks. ● implemented as a daemon written in C for performance reasons, & is designed to run natively on Linux/*nix systems.
ntop	ntopng	• Sort network traffic according to many criteria including IP address, port, Layer-7 (L7) application protocols, throughput, Autonomous Systems (ASs) • Show realtime network traffic and active hosts • Produce long-term reports for several network metrics including throughput and L7 application protocols • Top talkers (senders/receivers), top ASs, top L7 application protocols • Monitor and report live throughput, network and application latencies, Round Trip Time (RTT), TCP statistics (retransmissions, out of order packets, packet lost), and bytes and packets transmitted • Store on disk persistent traffic statistics to allow future explorations and post-mortem analyses • Geolocate and overlay hosts in a geographical map

Part 3: Select a Network Monitoring Tool

Step 1: Select one or more monitoring tools from your research.

From your research, identify one or more tools you would choose for monitoring your network. List the tools and explain your reasons for choosing them, including specific features that you consider important.

Ntopng - You can install ntopng on a server with multiple interfaces and use port mirroring or a network tap to feed ntopng with the data packets from the network for analysis. ntopng can analyze traffic even at 10G speeds; report on IP addresses, volume, and bytes for each transaction; sort traffic based on IP, port, and protocol; generate reports for usage; view top talkers; and report on AS information. This level of traffic analysis helps you make informed decisions about capacity planning and QoS design and helps you find bandwidth-hogging users and applications in the network. ntopng has a commercial version called ntopng pro that comes with some additional features, but the open-source version is good enough to quickly gain insight into traffic behavior. ntop can also integrate with external monitoring applications such as Nagios for alerting and provide data for monitoring.ntopng has some limitations, but the level of network traffic visibility it provides makes it well worth the effort.

Step 2: Investigate the PRTG network monitoring tool.

Navigate to www.paessler.com/prtg.

Give examples of some of the features that you found for PRTG in the space provided below.

Monitor Everything
Alert management & SLA modeling
Dashboard and mobile apps

Reflection

Based on your research, what conclusions have you reached regarding network monitoring software?

Based on my research I concluded that network monitoring tools are important. Because many organizations

Need their network up and functioning to generate revenue, and by having the right set of tools to monitor and manage the one you created is important.