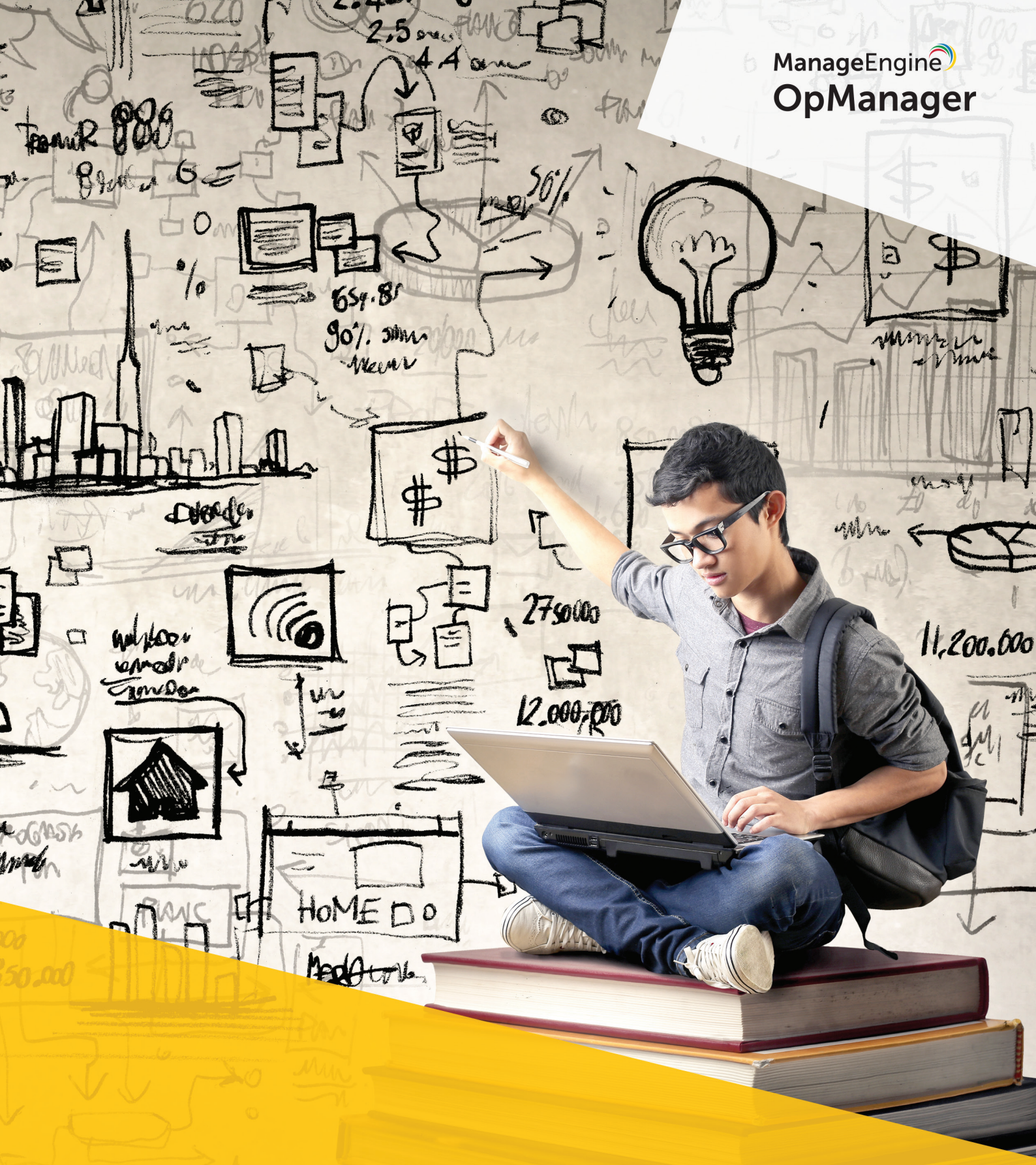
ManageEngine
OpManager



The Basics of Network Monitoring

Network Monitoring Basics Every IT Professional Should Know.

-Nithin.S

www.opmanager.com

Introduction

As business and organizations grow, the size of their network grows not only in size, it becomes more complex and an integral part of the establishment. Irrespective of the size of an organization, the network becomes a repository of data and information. Understanding the network, its complexity and being informed about the availability at all times is a key factor in maintaining the integrity of the network and invariably, the organization. This is where network monitoring plays a critical role.

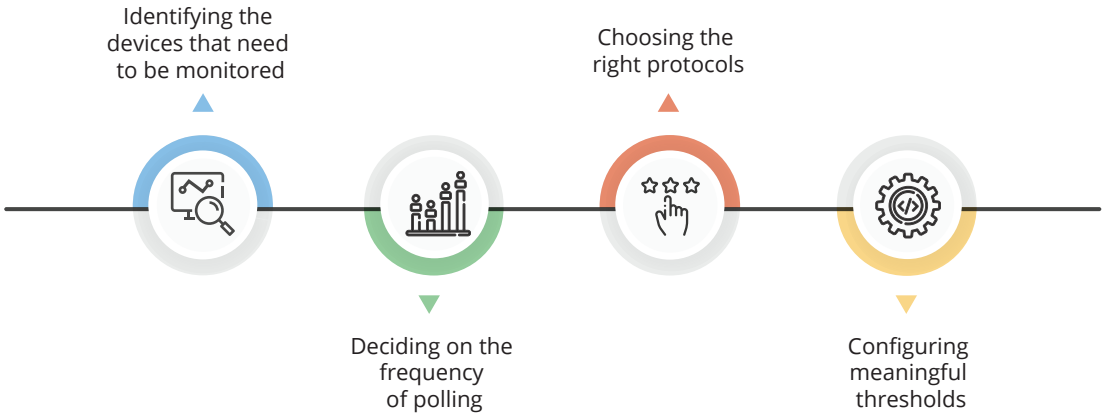
What is network monitoring?

In today's world, the term network monitoring is well-known in 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, as well as evaluated continuously to maintain and optimize their availability.

One important aspect of exceptional network monitoring is being proactive. Finding performance issues and bottlenecks proactively helps with identifying issues before they cause network downtime or complete network failures.

Important aspects of network monitoring:

- Monitoring the essentials
- Optimizing the monitoring interval
- Selecting the right protocol
- Setting thresholds



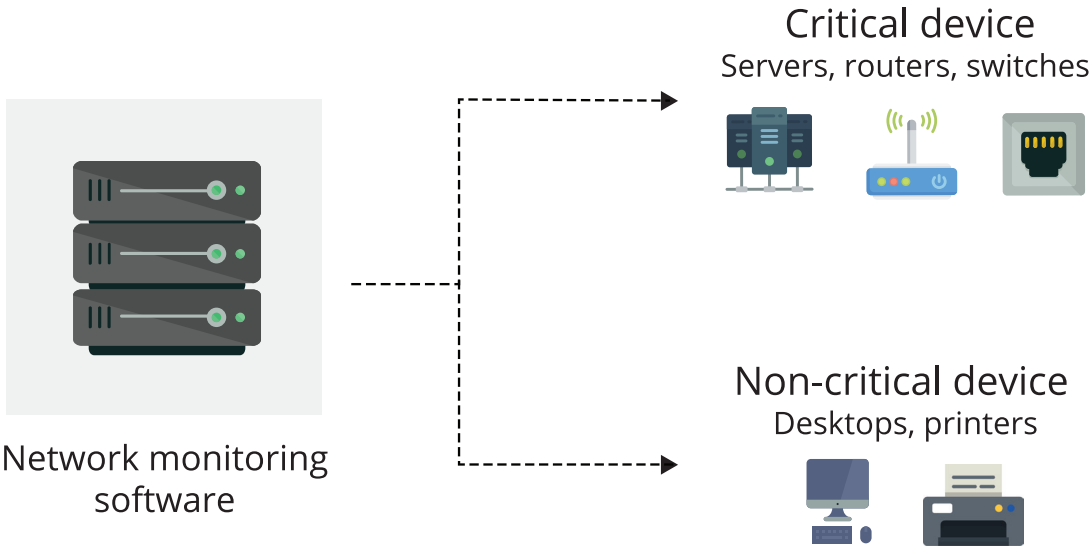
Did you know?

- Industry surveys estimate the cost of a network outage at around $5,600 per minute. This sums up to over$300,000 per hour which is a heavy price for several business organizations.
- Only 2% of organizations recover from downtime within an hour. The majority have to wait longer - the average is 4.78 hours

Monitoring the essentials

Faulty network devices impact network performance, but this can be eliminated through early detection, which highlights the importance of continuously monitoring your network and its related devices. Device availability is a major factor when it comes to network monitoring. Apart from knowing the availability of devices, there are several other specifics that affect the proper functions of a network.

The first step toward effective network monitoring is to identify which devices and related performance metrics need to be monitored. Devices like desktops and printers are not critical and do not require frequent monitoring whereas servers, routers, and switches perform business-critical tasks and require constant monitoring.



Monitoring interval

A monitoring interval determines the frequency at which network devices and their related metrics are polled to identify the performance and availability status. Setting up monitoring intervals can help take the load off the network monitoring system and, in turn, your resources.

The monitoring interval depends on the type of network device or parameter being monitored. Availability statuses of devices should be monitored every minute, CPU and memory stats should be monitored every five minutes, and disk utilization should be monitored once every 15 minutes. Monitoring every device at the shortest interval will only add unnecessary load to the network and isn't necessary for detecting critical aspects of network performance.

Types of protocol

When monitoring a network and its devices, a common good practice is to adopt a secure and non-bandwidth consuming protocol to minimize the impact the protocol has on network performance. Most network devices and Linux servers support SNMP and CLI protocols, while Windows devices support WMI protocol.

SNMP is a widely accepted protocol to manage and monitor network elements. Most network elements are bundled with an SNMP agent, they just need to be enabled and configured to communicate with the network management system (NMS). Allowing SNMP read-write access on a device gives you complete control over that device. Using SNMP, you can replace the entire configuration of a device. A network monitoring system helps administrators take charge of the network by setting SNMP read/write privileges and restricting control for other users.

Proactive monitoring and thresholds

Network downtime can cost a lot of money. In most cases, end-users report network issues to the network management team. This is a reactive approach to network

monitoring. The key challenge in network monitoring is proactively identifying performance bottlenecks. 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. A 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.

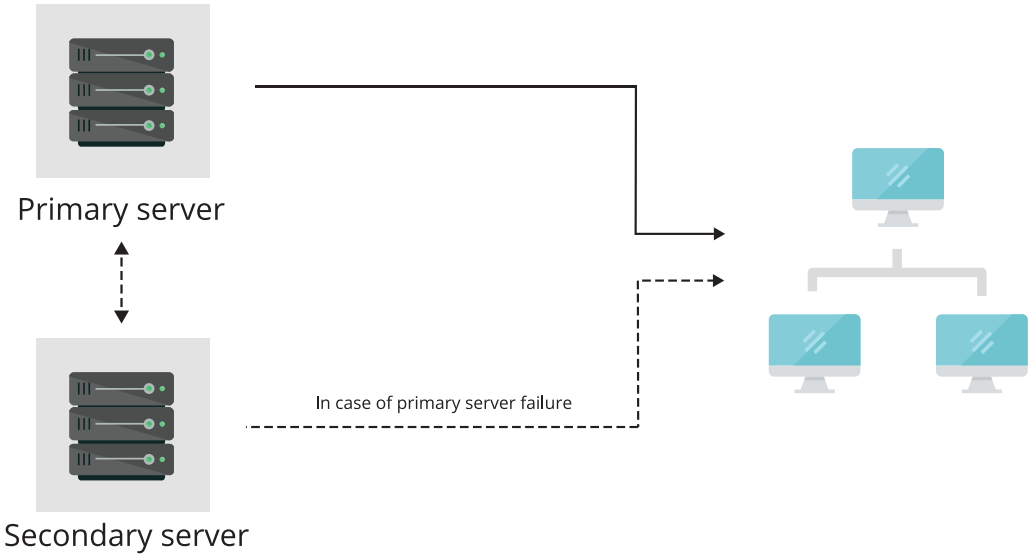
Dashboards and customization

Data becomes useful only when it is presented clearly to the right audience. It's 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 network devices like routers, switches, firewalls, servers, services, printers, and UPSs, as well as from applications and URLs. Support for widgets to monitor the required specific and real-time performance graphs can help administrators quickly troubleshoot problems and monitor devices remotely.

High availability and failover

What happens when your trusted network monitor is running on a server that crashes or loses network connection? You would want to receive instant alerts on this and you'd probably want the situation automatically remedied using a stand-by network monitor. High availability refers to the continuous availability of a monitoring system. Every single network incident—device sickness, unhealthy bandwidth levels, DoS attacks, etc.—should be immediately brought to your attention so that counter-measures can be quickly taken.

Failover and fail-back functionality ensures network environments are always monitored by utilizing a secondary standby server. If a failure occurs in the primary server, the secondary server is ready to take over so the database remains secure. This ensures total network and device uptime.



Benefits of a failover system:

- Instantly recognize primary server failure.
- Immediate notification via email in event of a primary server failure.
- 100 percent uptime and uninterrupted network management.
- Automated, seamless switching from the primary server to the standby server, and vice versa.

Choosing the right network monitoring tool

Artificial intelligence and machine learning

Network monitoring tools have the potential to incorporate artificial intelligence (AI) and machine learning (ML) as both thrive on data. With machine learning, network monitoring tools can adapt to the networking environment and provide suggestions based on the data available.

Possibilities of network monitoring with AI and ML:

- Load sharing based on usage.
- Smarter notification profiles.
- Network adaptation and the ability to automatically take corrective actions.
- Forecasting.

Automation

With rapid development in AI, automation is at a tipping point. Automation helps network monitoring tools react based on thresholds or a set of rules/criteria being met. With automation, a monitoring tool can automatically detect and troubleshoot problems (proactive monitoring), send alert notifications, and provide suggestions for better network performance and maintenance based on usage and priority.

Benefits of automation in network monitoring:

- The ability to automate repetitive tasks.
- Automated configuration and backup deployment across devices.
- Automatic discovery and monitoring of new devices.
- Proactive troubleshooting and efforts to take corrective measures.
- Scheduled report generation.

Features

Every network monitoring solution provides monitoring for basic core requirements like bandwidth, availability, and usage. An efficient network monitoring tool should support common protocols (SNMP, WMI, and CLI) and technologies (NetFlow, sFlow, jFlow, and packet sniffing). Configurable alert notifications, reporting capabilities, and customizable dashboards are features that make a network monitoring tool easy to use as well as accessible. Understanding your basic requirements and considering the essential network monitoring features is necessary when it comes to choosing the right network monitoring solution. But apart from the features, there are several more critical aspects to keep in mind when selecting the right network monitoring tool.

Distributed networks

Often, two companies will merge together or one company may buy out another, expanding the size of the network considerably. The greatest challenge is merging the corporate cultures and, of course, the two computer networks. When this happens, the new network grows considerably in a short amount of time and is distributed over new local networks, branch offices, customer networks (in case of MSP), data centers, and in the cloud. Robust networks can be costly to manage and difficult to troubleshoot. Steadily monitoring the availability and bandwidth utilization of distributed networks is a necessity.

Challenges in distributed monitoring:

- Centralized control: Monitoring multiple remote sites from a central location with probe-specific control to visualize performance hiccups.
- Network maintenance: Maintaining the network and troubleshooting network issues.
- Language barrier: Viewing language-specific stats across the probe site in a central location.

Scope

A common problem faced by IT operators and system administrators is the lack of visibility. A network monitoring tool that provides comprehensive, consolidated, detailed visibility into various monitoring aspects of the network as well as the flexibility of choosing what you want to see, will help you to stay on top of your network. The information from these various tools needs to be available on a single screen with at-a-glance charts and intuitive graphs. Some network monitoring tools can be enhanced to perform more advanced operations, which means it's important for the tool you choose to offer support for add-ons and integrations so you can monitor a wider aspect of your network.

Scalability

Network scalability is an important aspect when it comes to selecting an efficient network monitoring tool. A network monitoring tool is considered scalable when it's

more adaptable to the changing needs and demands of a business and its users. Scalability helps a network stay on par with increased productivity, trends, changing needs, and new adaptations to ensure that the overall network performance doesn't degrade, regardless of the network's size.

Recognition

When selecting a network monitoring tool, a common best practice is to analyze and familiarize yourself with the solutions in the marketplace. Review sites simplify this job by providing insights on various aspects of each tool and how specific features stand out from the rest. Analysts conduct in-depth primary and secondary research for which they draw from a vast network of sources, including end-user clients, technology providers, and industry leaders. They may also incorporate content from academic, journalistic, and scientific sources. Recognition from established review sites like Gartner and EMA can be beneficial in ascertaining the right network monitoring tool for your business.

Pricing

There are different licensing models available in the market based on the number of devices, nodes, or servers. The appropriate license scheme can be determined based on the size of the network, the type of solution (monitoring or management), and the scalability of the network. It's important to consider both the cost of the product (including things like annual maintenance, time spent on set up, add-ons, integrations, and training), and the potential savings. A transparent pricing policy ensures that there are no hidden costs.

Evaluation

Many software vendors provide a free trial to give you a firsthand experience with the product, so you know exactly what you're getting. It's crucial that you trial and demo the product to familiarize yourself with the features and get a feel for the user interface.

How OpManager performs network monitoring

OpManager is a proactive network monitoring solution loaded with powerful features that help IT administrators resolve network outages quickly and take control of their network.

With OpManager, it's easy to:

- Monitor the health and performance of all network devices.
- Gain visibility on network traffic patterns.
- Monitor your network proactively with multi-level thresholds.
- Automate network change and configuration management.
- Analyze and troubleshoot WAN issues and VoIP performance.
- Get detailed network insights with customizable dashboards.
- Keep on top of alerts thanks to OpManager's advanced fault monitoring and alert management system.
- Ensure business continuity with high availability and failover support.