Cost Effective Network Management For Today's SMEs.

A ManageEngine White Paper

Summary

Ensuring optimal network performance 24/7 is critical to business success, irrespective of whether you are small or big. This paper examines the basic functionality of any network management solution required to achieve the optimal network performance goal. And we will also focus on how ManageEngine OpManager provides these essential functionalities at low cost.

SME Network Management Needs

Network management software is getting more expensive and complex, and at the same time network management challenges are becoming more demanding and complicated as well. In such scenario, what the IT managers of small and midsized organizations should do is to prioritize their network management needs and implement solutions that offer these basic functions exceptionally well. Some of the basic network management functions that are critical for SMEs are:
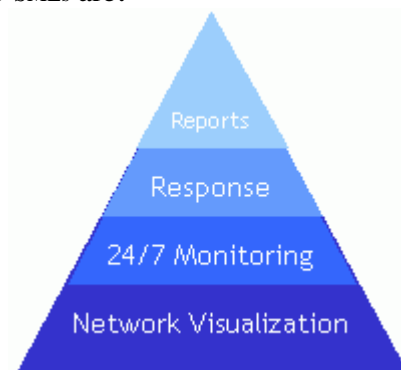
Network Visualization: Auto-discovery and mapping of all critical network elements such as mail servers, WAN links, business applications, and entire LAN infrastructure including switches, printers, wireless routers, load balancers, and non-standard devices if any.

Proactive Monitoring: 24/7 network surveillance for detecting network faults. Monitoring critical resources for availability, threshold violations, host resource (CPU, Disc space, Memory) utilizations, service availability, service response times etc.

Automated Response: Ability to send notifications and take automated remedial actions by executing custom scripts.

Flexible Reporting: Reports that help answer questions such as how many service outages occurred for all systems monitored that provide service to Atlanta branch office? What's the percentage of free space on all file servers across the entire network? And so on.

Network Visualization

To manage any network, first you must be able to identify and group network elements into different views that represent your deployment. For example if you are the IT manager responsible for managing the network infrastructure of your organization, then you would want the following in your management tool

> Automated discovery and grouping of all elements across the offices,
> Grouping of devices into routers, wireless, switches, servers etc.
> Custom maps that show branch office status at-a-glance

Network Discovery

Network discovery automates the process of identifying each manageable element of your network and adding it to the monitoring software for further monitoring. Every network monitoring software offer Network discovery, a basic functionality. But do checkout how much of information your network monitoring tool collects during this discovery process. Does it discover your most critical server as just another IP device? Or does it identify it as a Dell Server, connected to port 21 of Switch 2 in second floor, running oracle and http, with temperate of x degrees, CPU utilization of 70%, free disc space of 30% , transporting data at x kbps per second etc. Knowing what is actually happening under the hood gives you better visibility into the root cause of problems when they occur.

Grouping of Devices

The second important aspect of discovery is grouping the discovered devices into routers, switches, servers etc., separately. This helps network engineers to quickly access the relevant groups while troubleshooting.

Custom Maps

Maps or custom views help get the big picture of your network. For example, imagine a small business enterprise headquarter in California with branch offices in Texas and Atlanta. The graphic below illustrates how a network management tool helps in visualizing such a scenario. The icons as well as the links shown here reveal real-time status and provide instant information on what is up and what is down right at the moment. Moreover, these icons and links can be clicked to drill down for more details.
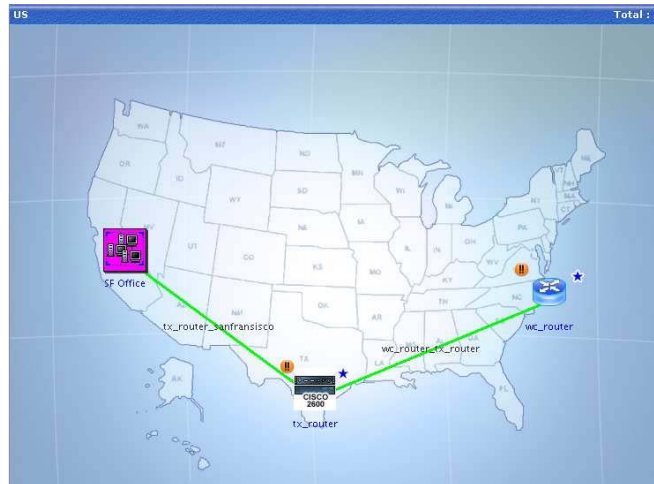
Proactive Network Monitoring

Even though hardware vendors offer management tools to every type of devices, these tools become a source of confusion when you deploy more than one. To ensure availability, proactive network monitoring is essential, but that doesn't mean you should use several tools. For an effective monitoring experience you should look for a network monitoring tool that can do the following:

Allow you to monitor your entire infrastructure components
Perform availability monitoring on all these devices
Perform proactive health monitoring using thresholds

Ability To Monitor Your Entire Infrastructure Components

Different organizations have different network components installed. As an IT Manager, the first thing that you should do is to prepare a checklist of devices that need monitoring. Then look for a network monitoring software that helps you monitor all these from a central console.

	OS		Network Components					DB Servers		
	Windows	Linux	Routers	Switches	Servers	Wireless	DNS	SQL	MySQL	Oracle
CA	x	x	x	x	x	x	x	x		x
ATLANTA	x		x	x	x					
TX	x	x	x	x	x					x

You should also look for software that allows custom device monitoring. For example your UPS devices or any other IP based device.

Availability Monitoring

Availability monitoring tells you which devices are up and which are not. This is very basic to an extent that there is no point discussing it further.

Proactive Health Monitoring

The statement below from an IT Manager captures the essence of proactive health monitoring.

"I don't want your software to tell me when my exchange server crashed; I have got users for that"

Every IT Manager wants to know failures in advance so that it can be prevented. A good network monitoring tool should help in monitoring the health of critical devices and alert the operators when health deteriorates. Automated polling of various devices for multiple health parameters is essential. For example: You can configure your network monitoring software to continuously monitor the free space available in a file server so that the users don't suffer when it runs out of disk space.

Automated Response

Ensuring optimal network performance not only depends on how quickly you identify a failure, but also on how quickly you resolve that. A good monitoring solution should allow you to respond to a failure in any of the following ways:

Generate Email/SMS notifications
Execute custom remedial scripts
Generate a ticket in your trouble ticketing software

Email/ SMS notifications

This is the second most basic functionality in any network monitoring software. As an IT manager you should look for software that can help you send emails to the right person at the right time. Say all SQL related notifications should be sent to John and all servers' related notifications should be sent to Alan.

If notification is very critical to your business, you should also look for software that can integrate with SMS engines that help you continue the notifications even if the mail server goes down.

OpManager supports integration with major SMS engines that allow SMS notifications to be sent directly to your phones without requiring your company mail server.

Execute Custom Remedial Scripts

Though notifications are effective, it's not always the best solution. For many situations it is preferred that you let the monitoring system attempt to remedy the problem on its own before involving a human.

For example, a service might fail often and would require a simple restart every time. Suppose that you have a printer server on which a particular service hangs. Each time it hangs someone should restart the service. The right network monitoring solution might be able to perform the restart for you. Automated remedial action is the next level of maturity and sophistication in a network monitoring system.

Today, most IT teams have in-house programming expertise, to write custom scripts on VB or Perl. Clubbed with their knowledge of API and COM interfaces to various system management technologies such as Windows Management Instrumentation (WMI), Active Directory Service Interfaces (ADSI) these IT pros can write scripts that ease the job of administrators when they have to repeat lengthy procedures in fixing a problem every time.
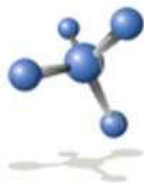
OpManager enables executing such custom scripts on the occurrence of network trouble. You can assign a script to a particular event so that OpManager triggers the script and eliminates the need for manual intervention.

Generate A Ticket In Your Trouble Ticketing Software

IT services teams rely on Help Desk or trouble ticketing software to streamline their work. Tickets raised for various problems are assigned to respective operators and are tracked for closure.

As an IT Manager you can also make use of this process and configure your network monitoring software to automatically generate tickets to the appropriate resource. This saves time and also helps in knowledge sharing. For ex: How do you free up your most experienced resources from troubleshooting ordinary problems? The simple way is to document the procedures to fix the problem once so that next time it can be done by junior level technicians. Few trouble ticketing software help you build an effective knowledge base over a period of time.

ManageEngine ServiceDesk Plus – A web based help desk tool meant for IT services pros. You can automatically generate a ticket in ServiceDesk Plus by integrating it with ManageEngine OpManager. With this duo in action, you can free up your critical resources to take up larger and strategic projects leaving behind network monitoring related problems to juniors.

Flexible Reporting

To achieve the goal of optimal network performance 24/7 you should continuously measure key parameters through reports. Questions such as how many service outages happened in the past 90 days? How many times did exchange server crashed in the past 6 months, what is the % of network availability in the past 1 month? How many failures happened in the peak hours in the last 3 months? etc... These help IT Managers to identify the trend and plan for optimization.

ManageEngine OpManager helps IT Managers to generate numerous reports for different time periods e.g. the server availability report for a month, the utilization pattern on Atlanta office for the past 6 months, the availability report on Texas office for the past 3 months etc.

Conclusion

To manage your network you must first monitor it. Network monitoring is essential to ensure high availability of your networks and applications. A comprehensive network monitoring software such as ManageEngine OpManager could save you from network outages and help saving lot of IT dollars.

OpManager offers a free edition which manages a maximum of 10 network devices. For bigger organizations there is a 30-day trial edition to try. No license required. Visit http://www.opmanager.com to download the free edition or the trial edition. OpManager starts at $595.

****

For more details on ManageEngine OpManager visit http://www.opmanager.com and to understand how it can help you manage your network, systems, and applications seamlessly, please contact sales@manageengine.com. For comments on this article contact opmanager-marketing@manageengine.com