ManageEngine
Powering IT ahead

Up and Running

-you or your network?

ManageEngine OpManager

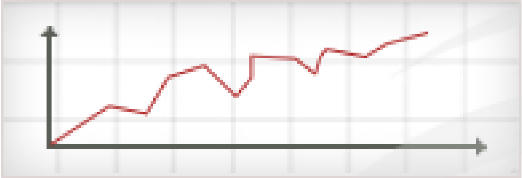
A FAULT MANAGEMENT WHITEPAPER

Up and Running - You or your network?
A Fault Management - Whitepaper

In modern day IT, it's not the network that is up and running, it's the IT administrators. Constant introduction of new devices, new technologies, patch upgrades, branch offices, etc. force the administrators to make frequent changes in the network, to include new devices and adopt new technologies. They go berserk as frequent changes affect the performance of the network, and work round the clock to fix it.

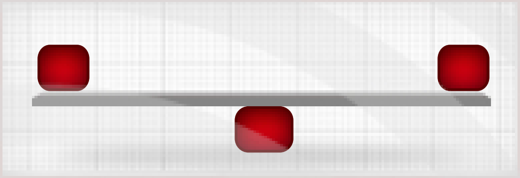
Things that make IT administrators run 24x7

Business office proliferation



Day by day your business keeps expanding, and so your networks and the complexity in managing them. It gradually transforms you from the happy guy when you were managing few devices to the-one-who-lives-with-the-blackberry-24x7 managing a multiple branch offices.

Balancing business demands & Technological advancements



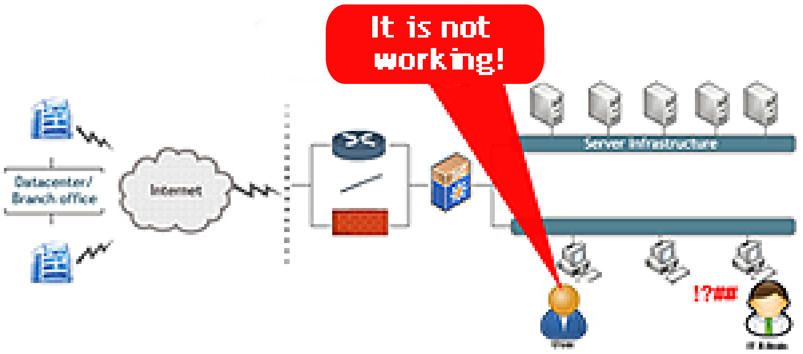
You have to constantly adopt new technologies to meet your business demands. Initially, your business demanded just the network uptime and basic ICMP ping/port check was enough. Now your entire business relies on IT network and requires SLA, SLM, BSM & more. Therefore, any problem with the network will directly affect your revenue. This has pushed companies to sign up service level agreements within their organization itself.

Aligning business and end-user preferences

As an IT administrator you are tossed between business and end-user preferences. End users never wish to compensate or get blocked for accessing Facebook or YouTube. At the same time business critical applications should not strive for bandwidth/ other resources. It is very difficult to address both the needs without buying extra bandwidth/ resources month on month.

What's needed in a modern day network?

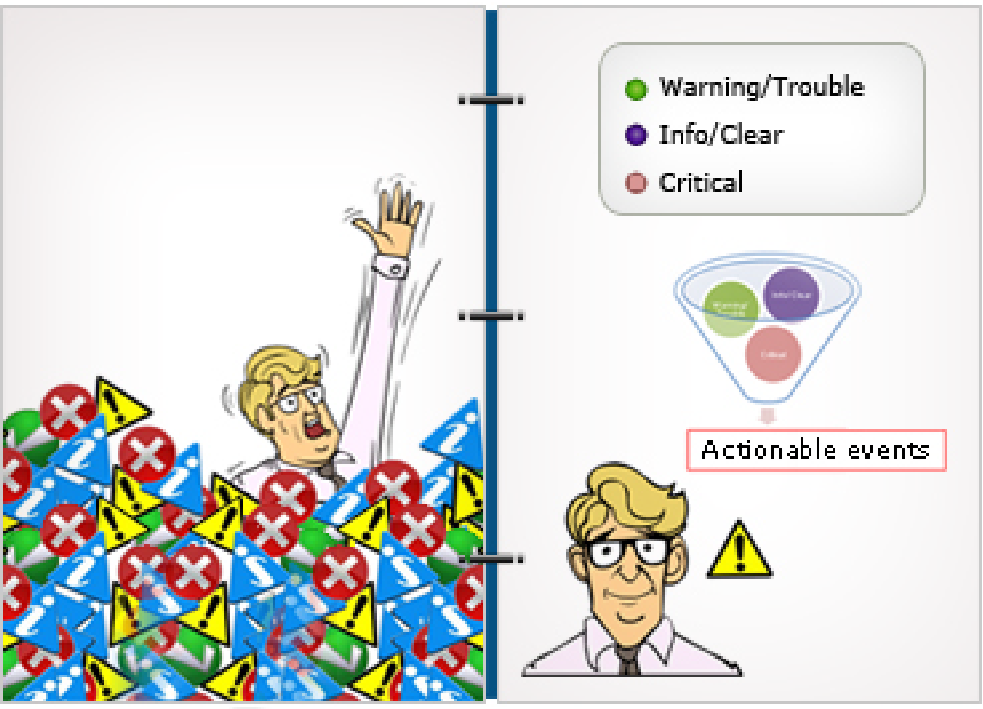
It's neither possible to stop adding new devices, adopting new technologies nor limiting the branch offices. The only solution available for today's network is 24x7 monitoring and an intelligent fault management to identify the root cause of the issue, and fix it before you feel its impact on your business.



Fault Management Perception

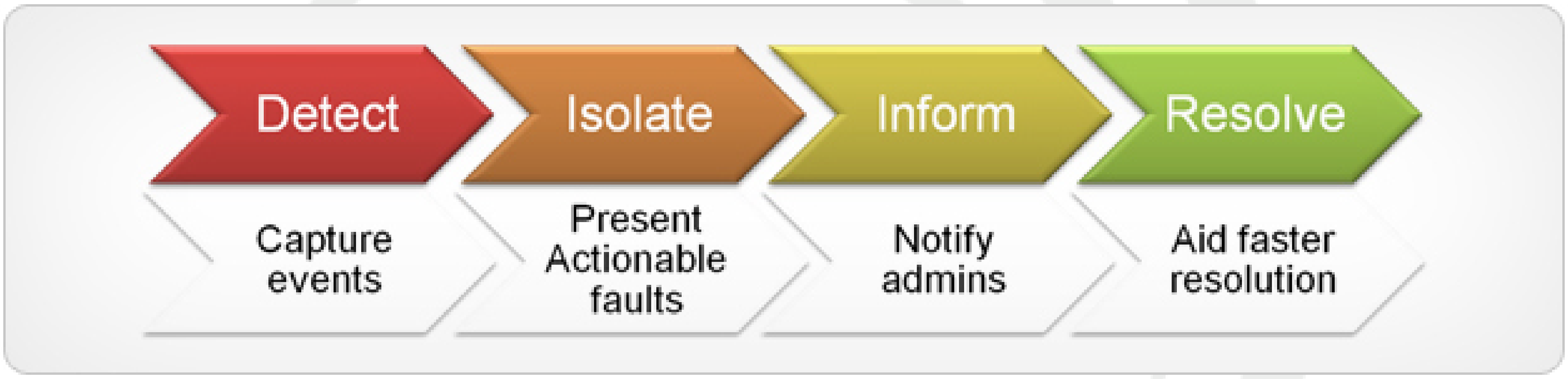
The common perception of fault management is identifying all the events. This, however, is not true. There is more to it than what meets the eye!

Any happening that has an impact on the network's performance is called an event. It can be informational in nature, a cleared event, warning message, a trouble sign or even a critical fault. If all these events are pushed to the administrator, he would be drowned and helpless. Instead, an intelligent NMS must sort the events and only actionable faults must be presented to the administrator to work on.



Fault Management – A four step process

A good fault management plan must have various mechanisms to detect the events, isolate and notify only the actionable faults to the administrators for resolution.



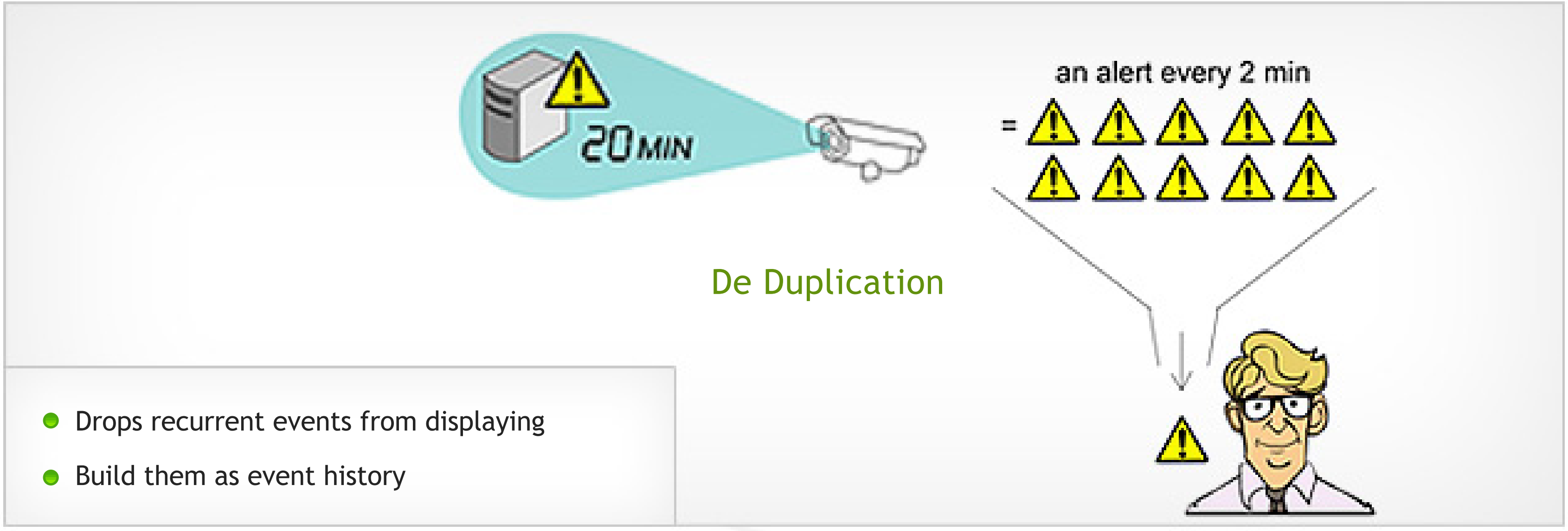
Detecting an event:

Two types of monitoring – active and passive are equally important to have responsive event detection mechanism. Active monitoring helps proactively detect an event by setting up thresholds for the monitors. Some examples of active monitoring are ICMP Ping, TCP or UDP port check and performance counters monitoring. Whereas, in passive monitoring, the NMS listens for an event for e.g. Syslogs, SNMP traps and Windows event log messages.

OpManager offers both active and passive monitoring. It monitors devices using ICMP ping, TCP & UDP ports and performance counters. It also monitors Syslogs, SNMP traps, event logs, etc.

Isolating the fault – Present an actionable fault:

Fault isolation helps identify the events that have impacted the network's performance. Fault management techniques such as De-duplication, Correlation and Automation, help in identifying the root cause.

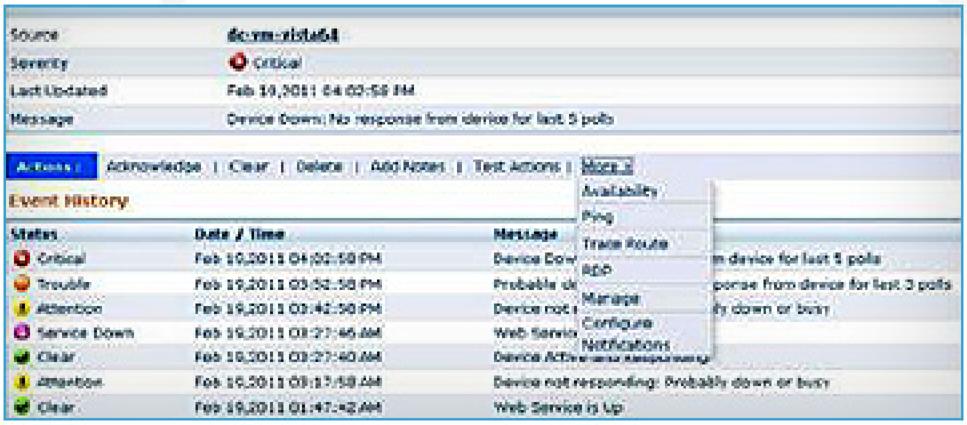


De Duplication

- Drops recurrent events from displaying
- Build them as event history

Consider a situation where a server is running at high CPU and the monitoring system polls the device for every 2 minutes. If the high CPU sustains for about 20 minutes, the monitoring system should not raise 10 alerts - a clear duplication. Instead it should show a single alert.

OpManager, for every unique event, creates a new row item with the severity color code under the Alarms tab. If the same event occurs again, it is appended to the alarm history, thereby eliminating duplication.



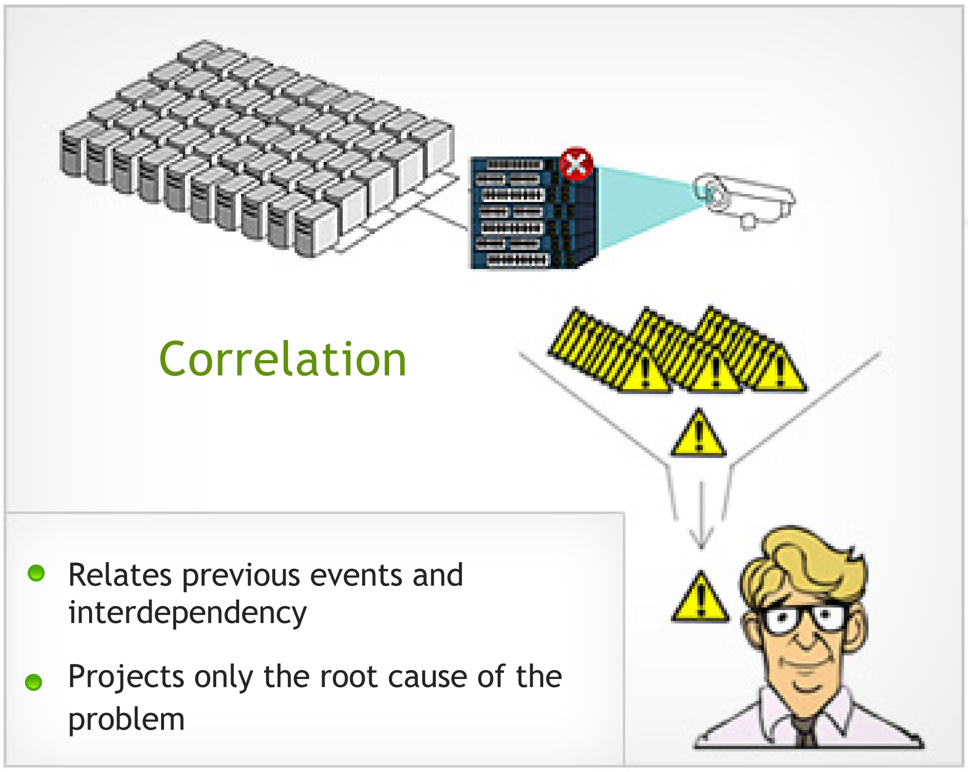
Source	dc:vm:vista64
Severity	Critical
Last Updated	Feb 19,2011 04:02:58 PM
Message	Device Down: No response from device for last 5 polls

Actions | Acknowledge | Clear | Delete | Add Notes | Test Actions | More
Availability
Ping
Trace Route
RDP
Manage
Configure
Notifications

Event History

Status	Date / Time	Message
Critical	Feb 19,2011 04:02:58 PM	Device Dow… m device for last 5 polls
Trouble	Feb 19,2011 03:52:58 PM	Probable de… ponse from device for last 3 polls
Attention	Feb 19,2011 03:42:58 PM	Device not r… ly down or busy
Service Down	Feb 19,2011 03:27:46 AM	Web Servic…
Clear	Feb 19,2011 03:27:40 AM	Device Active and Responding
Attention	Feb 19,2011 03:17:58 AM	Device not responding: Probably down or busy
Clear	Feb 19,2011 01:47:42 AM	Web Service is Up

Similarly alarms correlation also helps in showing only actionable network faults. Consider a core switch that is connected to 50 servers is down. The NMS should not raise 51 alerts, stating all the 50 servers and 1 switch, are down - Instead, the NMS should automatically map the devices and raise a single alarm for the switch.



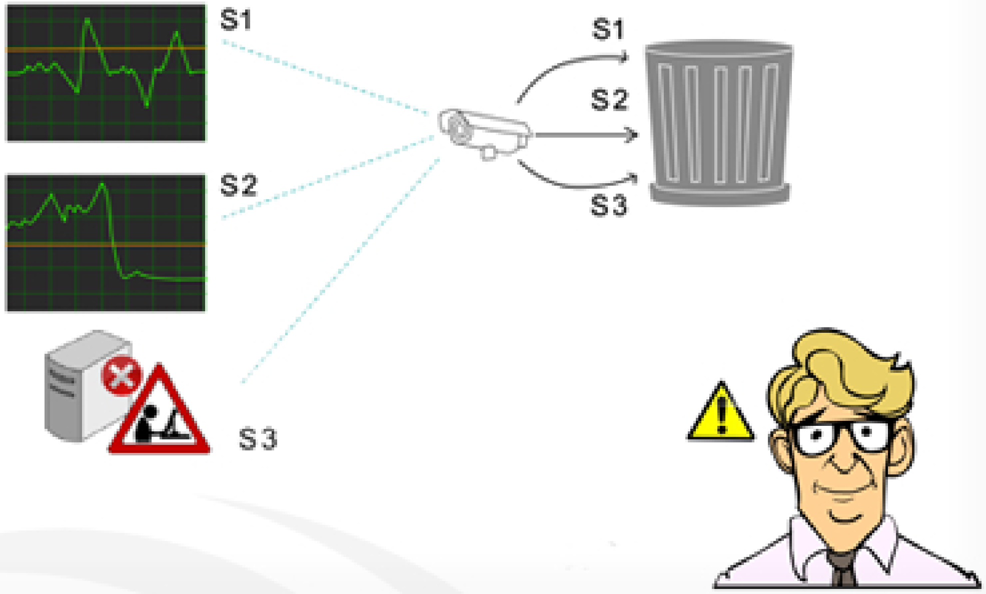
Correlation

- Relates previous events and interdependency
- Projects only the root cause of the problem

The "Device Dependency" option in OpManager helps avert such alerts. If the parent device is down, it raises alert only for the parent device. You will receive a single alert for the switch that has gone down. OpManager also automatically maps your servers to the network devices using its automated network mapping and custom network map functionality. This help the administrators see the outage or performance hiccups and troubleshoot quickly.

Automation

- Ignore incidental events
- Remove cleared faults
- Suppress known alarms (Automated/Manual Suppression)

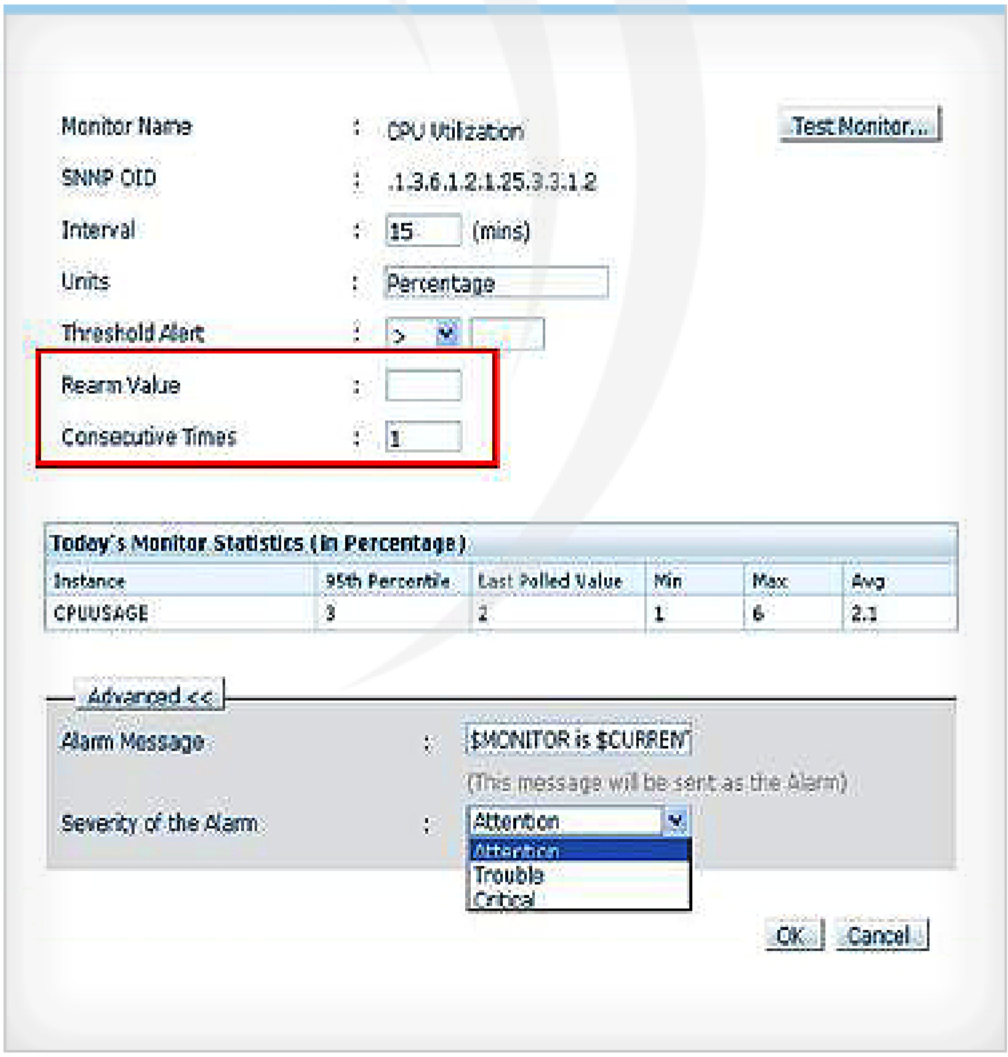


The final one, automated fault isolation, is all about dropping the unwarranted events. Negligible incidental spikes, alarm reverting to clear state, events for devices in maintenance mode, etc. are some examples of unwarranted events.

OpManager helps you ignore such unwarranted events. For active monitors, by configuring the "consecutive times" and "Re-arm value" in the threshold configuration screen, it allows you to ignore incidental spikes and clear the event. For passive monitoring, the suppression for such spikes is handled in the rules itself. For routine device maintenance, you can configure the "Downtime scheduler" in OpManager to suspend monitoring the devices during the maintenance window.

OpManager allows you to suppress alarms on need basis, using the "pause status polling" option. This option omes handy when you are working on a particular fault and want OpManager to stop polling the device, till the issue is resolved.

EDIT MONITOR - OPMSUPPORT



Monitor Name	:	CPU Utilization
SNMP OID	:	.1.3.6.1.2.1.25.3.3.1.2
Interval	:	15 (mins)
Units	:	Percentage
Threshold Alert	:	>
Rearm Value	:	
Consecutive Times	:	1

Today's Monitor Statistics (in Percentage)

Instance	95th Percentile	Last Polled Value	Min	Max	Avg
CPUUSAGE	3	2	1	6	2.1

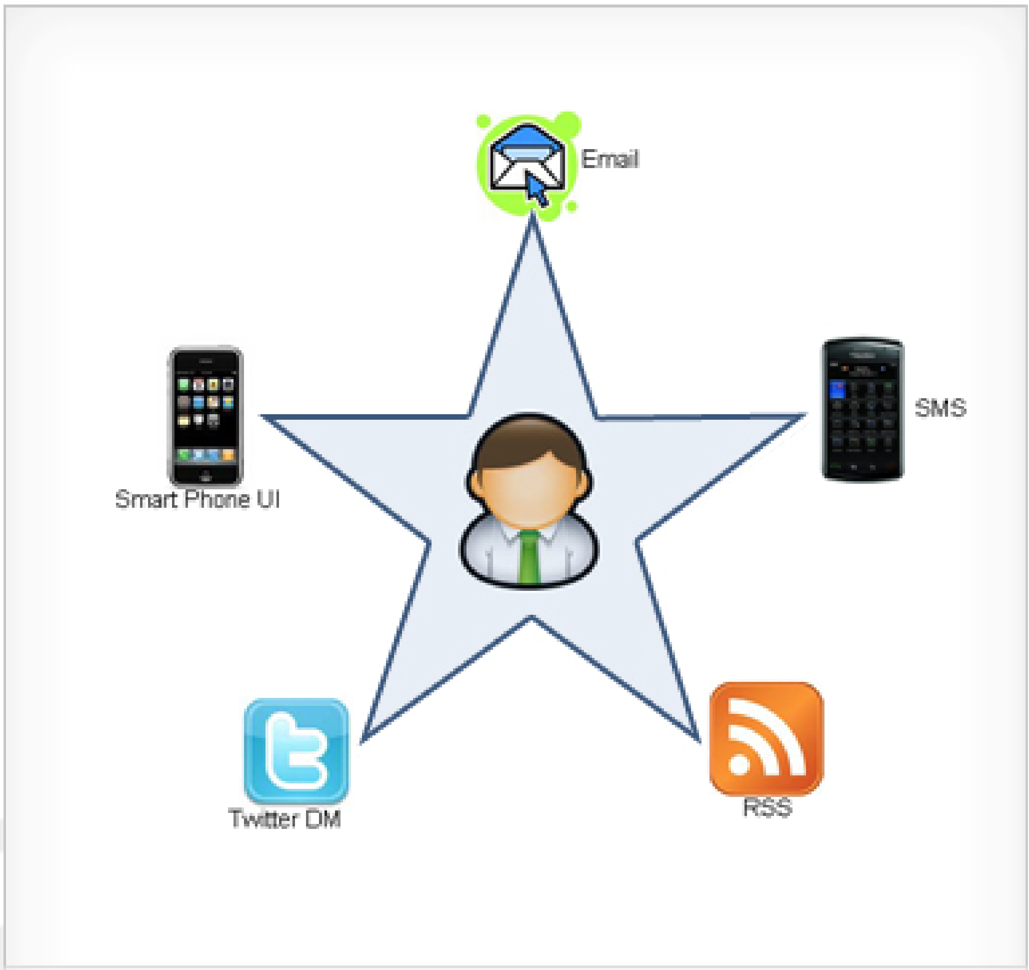
Alarm Message : $MONITOR is $CURREN
(This message will be sent as the Alarm)

Severity of the Alarm : Attention

Inform – Notify Administrators:

The core function of this process is to let you know about the actual problem. This can be through visual representation for the NOC administrators, trouble ticketing to helpdesk technicians and alerting remote administrators through Email or SMS.

To understand the issue and its root cause better, OpManager visualizes the performance bottlenecks through color coding of alarms, web alarms, dashboards, business views, etc. It also notifies the fault via Email, SMS, RSS feeds and Twitter. Its smartphone/ iPhone Graphic User Interface (GUI) helps administrators to quickly go through the alert and start troubleshooting.

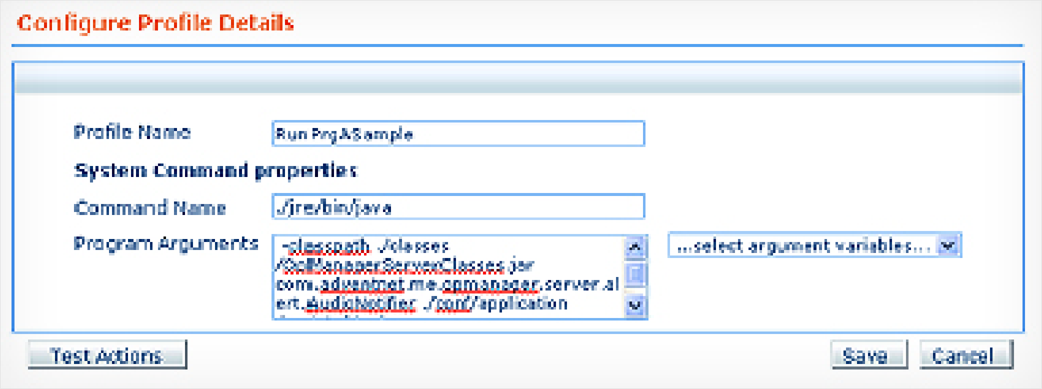


- Alert remote admins - Email, SMS, RSS feeds,Twitter Alerts, iPhone/Smartphone GUI

For trouble ticketing, OpManager integrates with ManageEngine ServiceDesk Plus. For other help desk software, OpManager can be configured to send an email with the fault message and variables.

Resolve – Aid faster resolution:

For faster fault resolution, the NMS should have a proprietary knowledge when handling faults. In case of any issue, the NMS should automatically run a particular command or program in a remote machine to fix it.



Configure Profile Details

Profile Name: Run PrgASample

System Command properties

Command Name: ./jre/bin/java

Program Arguments: -classpath ./classes /OpManagerServerClasses.jar com.adventnet.me.opmanager.server.alert.AudioNotifier ./conf/application

If it is not possible, due to some complication or error, the NMS should escalate the situation to the appropriate admin with the clear log message for next course of action.

In OpManager, for automated fault resolution, you can run self-healing scripts on the remote machine using "Run a program" or "Run a command" option. For e.g. if the hard disk is found to be running full in your MS SQL server, you can run a script to clear the transactions logs and restart the service from OpManager.

Easy Troubleshooting with OpManager

OpManager offers a wide range of troubleshooting tools that help you fix the problems in a wink. For server troubleshooting, OpManager has tools such as Remote Process Diagnostics (similar to launching a remote task manager), Device tools, ping, trace route, etc. For the network switches, OpManager provides Switch Port Mapper that maps every connected switch port. OpManager's NetFlow Traffic Analysis module helps you analyze what type of traffic is going through a particular machine.

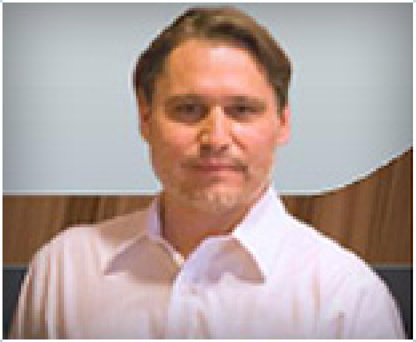
For WAN links, OpManager gives you a hop-wise visibility that lets you swiftly identify where the problem originated from. Usually, WAN link performance degradations are caused either due to high traffic or recent configuration changes done on the network device. OpManager's NetFlow Traffic Analysis module helps you solve the traffic bottlenecks. You can use the NCM plug-in for the issues arising due to configuration changes. The NCM plug-in does a side-by-side comparison with the pervious configuration and restores the configuration if needed.

OpManager also includes Syslog viewer, in-built MIB browser, real-time performance graphs, etc. to manage your network better.

Conclusion

The IT administrators are found running behind the events, literally wading through a huge pile to find the faults. An intelligent fault management system is necessary to isolate and pass-on actionable faults to the administrator. OpManager, a network and server management software, offers intelligent fault and performance management that pinpoints the root cause. Further, it notifies the appropriate administrator with all the necessary information within seconds. It's efficient and easy-to-use tools help to either automatically fix the issue or aid faster troubleshooting.

CUSTOMER'S VOICE:



"...you can't put a price on the reliability that OpManager has on the alerting capability...we've had many examples where we've had services go down where OpManager has given us the heads-up...".

Randy S. Hollaway

Senior System Administrator

Thorp Reed & Armstrong

CUSTOMERS:

L'ORÉAL SIEMENS DHL Digicel

SAINT-GOBAIN TIME WARNER CABLE The New York Times

KPMG NASA

AWARDS:

Info Security Products Guide 2011 GLOBAL EXCELLENCE FINALISTS AWARDS

Windows Networking.com

Info Security Products Guide 2010 GLOBAL PRODUCT EXCELLENCE AWARDS CUSTOMER TRUST ★★★★★

2009 SIIA //CODiE// FINALIST

About OpManager

OpManager, used by over 8500 businesses worldwide, is the flagship network monitoring and management software from ManageEngine. The 40 MB (Windows installation) software has a built-in database and Web server and delivers out-of-the-box availability and performance monitoring across any IT environment. Apart from advanced capabilities such as virtualization management, in-depth network traffic analysis, network change and configuration management, VoIP monitoring and WAN Round Trip Time monitoring, OpManager also integrates with other solutions such as ServiceDesk Plus, Applications Manager and Firewall Analyzer from the ManageEngine suite. Try it out yourself! visit our website at www.opmanager.com and download a free 30 days trial.

About ManageEngine

ManageEngine is the leader in low-cost enterprise IT management software. The ManageEngine suite offers enterprise IT management solutions including Network Management, HelpDesk & ITIL, Bandwidth Monitoring, Application Management, Desktop Management, Security Management, Password Management, Active Directory reporting, and a Managed Services platform. ManageEngine products are easy to install, setup and use and offer extensive support, consultation, and training. More than 50,000 organizations from different verticals, industries, and sizes use ManageEngine to take care of their IT management needs cost effectively. ManageEngine is a division of ZOHO Corporation. For more information, please visit www.manageengine.com.