

What Systems and Network Professionals Need in Automated Monitoring Solutions – A TechRepublic Survey Sponsored by MKS Software.

Are you expected to keep mission-critical, information technology resources available 24x7? Do you seek the “peace of mind” of knowing your websites, email servers, e-commerce applications and other crucial systems and applications are running smoothly? You’re not alone.

In order to understand the availability monitoring needs of those supporting Windows and other platforms, we asked TechRepublic to conduct a survey of network and system administrators and managers. The outcome of this survey shows what over 650 IT professionals feel they need in order to meet availability expectations in our non-stop world.

We believe MKS AlertCentre, a point-and-click solution for automating availability monitoring, alerting, escalation and corrective actions, is just what these professionals are looking for.

AlertCentre is affordable, powerful and easy-to-use and it comes bundled with MKS Toolkit for System Administrators, which provides a rich set of tools such as Secure Shell and Telnet for remote administration, and hundreds of other tools for automating repetitive tasks such as: data replication, performing daily back-ups across machines, deploying software and much more. Best of all, MKS Toolkit for System Administrators is the systems management solution platform that AlertCentre was built on, and it is at your disposal for customizing AlertCentre to handle your unique monitoring and automation requirements.

We hope this survey is valuable to you. Please visit our Web site at <http://www.mkssoftware.com>, or call us today at (800) 637-8034 or +1 (703) 803-3343.

MKS Software
www.mkssoftware.com
Email: tk_info@mkssoftware.com

What Systems and Network Professionals Need in Automated Monitoring Solutions

January 31, 2002

Executive summary

Automated monitoring is essential for maintaining high-availability of mission-critical systems and applications. Monitoring also insures crucial applications are running efficiently, and producing high-quality output. Today's network and systems professionals are faced with the challenge of maintaining high-availability for a multitude of applications and Internet/intranet-based systems that operate across an infrastructure of various platforms and a wide array of technologies. Given the urgency for businesses to perform, it is becoming increasingly important for IT professionals to look for systems management solutions that provide "peace of mind" by automatically monitoring networks, applications, and Internet/intranet-based systems that are involved in revenue generation.

To explore key areas of network and systems management, and to identify the relevant issues faced by network managers and administrators, TechRepublic recently conducted a survey of these IT professionals. The study examined several facets of network and systems monitoring, including current practices and the benefits of automated monitoring tools.

The results of the survey demonstrate that current systems monitoring practices center on the reactive approach to systems management, which is not monitoring in the true sense, specifically:

- Over 60 percent report they monitor or respond to support calls only when an issue arises.
- Only a small portion of respondents' workdays, in the range of 6–10 percent, is spent monitoring systems status and performance (reported by 36 percent of participants).
- When daily monitoring does take place, only basic IT performance factors are checked—monitoring system disk space (80 percent of responses), and CPU utilization (58 percent of responses).

In terms of available management tools, around 65 percent of respondents found existing network management tools lacking in some way. Thirty-five percent see the current market as offering large frameworks that are too expensive and difficult to deploy. Another 30 percent indicate that point solutions would be ideal if they could be customized.

Not surprisingly, the overwhelming majority of network and systems professionals surveyed have a preference for network management solutions that integrate with or extend their existing management solutions easily and readily (81 percent overall). The largest number, 43 percent, prefer having the same administration tools used by their systems management solution vendors, and nearly equal numbers endorse a semi-open environment that can be extended/integrated with easy-to-use prefabricated modules (38 percent of responses).

Almost 70 percent of survey participants rely on Telnet for remote administration. Even though this technology is adequate in many respects, since Telnet doesn't provide secure connections, administrators and managers who are concerned about secure communications might consider the advantages of other technologies that provide this capability, for example, Secure Shell (SSH).

The data show that even though the majority of respondents are in a Windows environment, 43 percent of survey participants still prefer a browser-based interface, versus traditional Windows or command line interfaces. Browser-based interfaces provide the mobility and flexibility to take administrative action from any location.

The study also highlights areas where the ability to manage and administer the availability of the enterprise's networks and systems would benefit from automated systems monitoring solutions. Nearly 70 percent of respondents identified systems monitoring of malfunctions and systems resource monitoring as the job functions or tasks that would most benefit from automation.

Additionally, 50 percent or more of respondents indicated there were other critical administrative tasks that would also benefit from automated solutions, including:

- Automated daily back-ups of all machines
- Automated replication of data (including data synchronization) on a regular basis
- Automated back-ups across UNIX, Linux, and Windows platforms
- Automated user/group administration

Network and systems professionals also report a need for automated monitoring tools that readily support multiple scripting languages in order to customize management solutions for specific situations and tasks. Such a feature enables them to automate corrective actions identified through monitoring, and is clearly a necessary component of any effective automated monitoring solution.

Introduction

Today's business environment requires that mission-critical systems and applications are running continuously, efficiently and reliably. To provide this level of service to the enterprise, network and systems professionals must monitor applications and Internet/intranet-based systems that operate across a variety of platforms, technologies, and programming languages.

Given this formidable task, it is becoming increasingly important for IT professionals to look for systems management solutions that provide reliable and accurate monitoring of the organizations networks, systems, and applications.

This research explores some of the key aspects of systems monitoring, including:

- Current systems monitoring practices and demands on staff time
- Current opinions on network monitoring tools
- Preferred notification modes and interface
- Benefits of automated monitoring tools

The results of the study are highlighted in the following sections.

Research methodology

A survey invitation was sent to a highly targeted group of TechRepublic members during the period of January 7, 2002 through January 15, 2002. The Web-based survey consisted of 19 closed-ended questions designed to explore and identify the key issues and current practices in enterprise system monitoring. The results reported here are based on the 683 completed surveys collected during the study.

Key findings

Respondent demographics

Survey respondents were selected from among TechRepublic members who met certain selection criteria, specifically those IT professionals who are based in the United States, Canada or Europe, and who:

- Are affiliated with organizations of various sizes
- Have primary job roles in:
 - Network or systems administration
 - Network or systems management

The tables and charts below contain the summary demographics of the survey respondents by job role, organization size, and industry category. In addition, the distribution of system managers/administrators at respondents' organizations, as well as the operating system platforms supported in these organizations are highlighted in this section.

Job role distribution

Job role	Percentage of respondents
Network/Systems Administration	69%
Network/Systems Management	16%
Other	15%

Size of organizations sampled

Organization size (all locations combined)	Percentage of respondents
<100 employees	30%
100-999 employees	31%
1,000-9,999 employees	24%
10,000 or more employees	15%

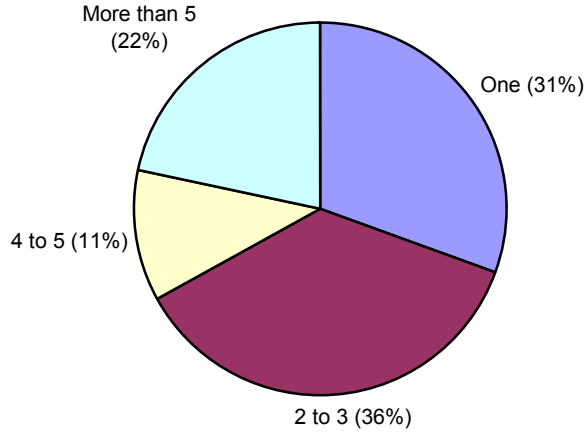
Geographical distribution

Geographical area	Percentage of respondents
United States	68%
Canada	7%
Europe	25%

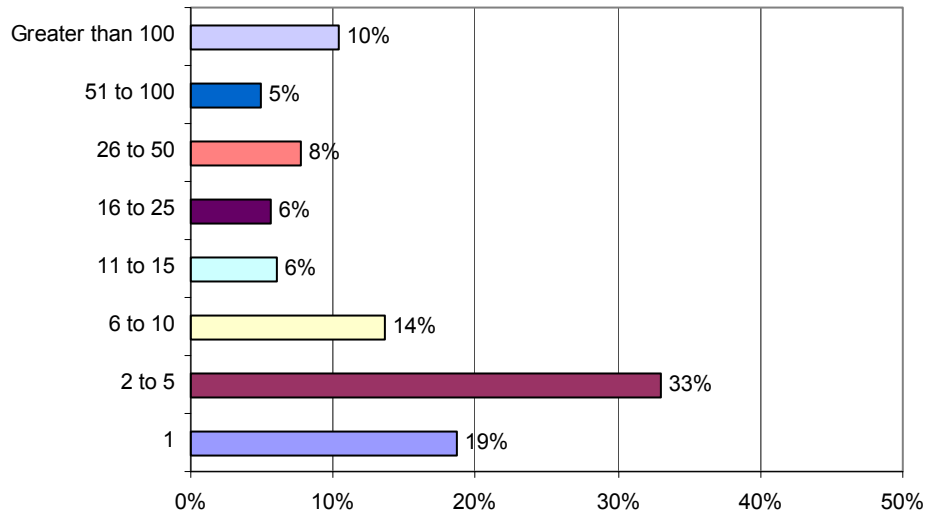
Industry distribution

Industry category	Percentage of respondents
Computer-related businesses and services	21%
Non-computer related businesses and services	65%
Government, and regulated businesses and services	14%

Number of systems managers/administrators at respondent's location

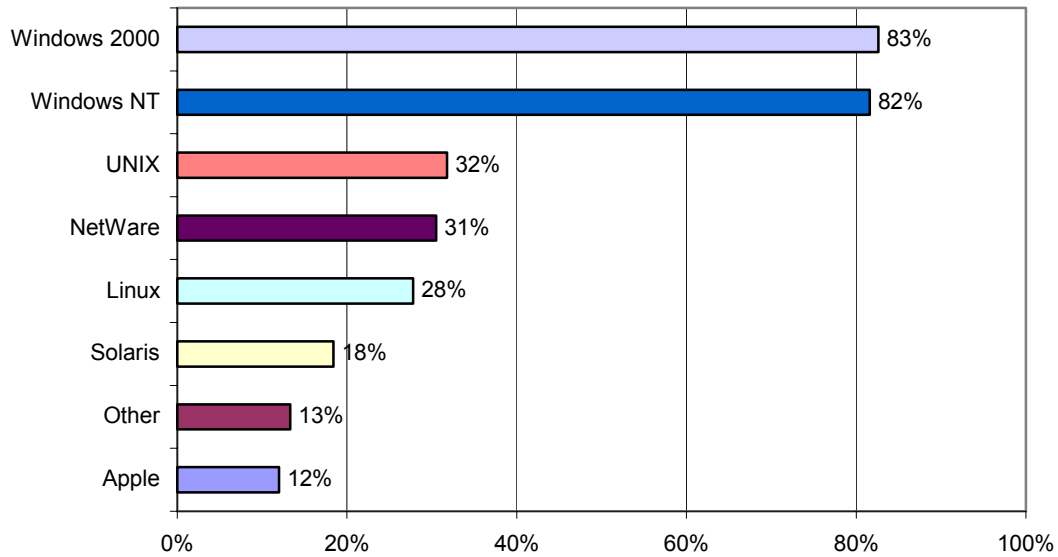


Number systems managers/administrators in respondent's entire organization



Respondents were asked to identify the OS platforms they currently support. Not surprisingly, Windows and Windows NT were the most frequently listed operating systems supported by over 80 percent of respondents, respectively.

What OS platforms do you currently support? (Choose all that apply.)



Other operating systems noted were Windows XP and VMS.

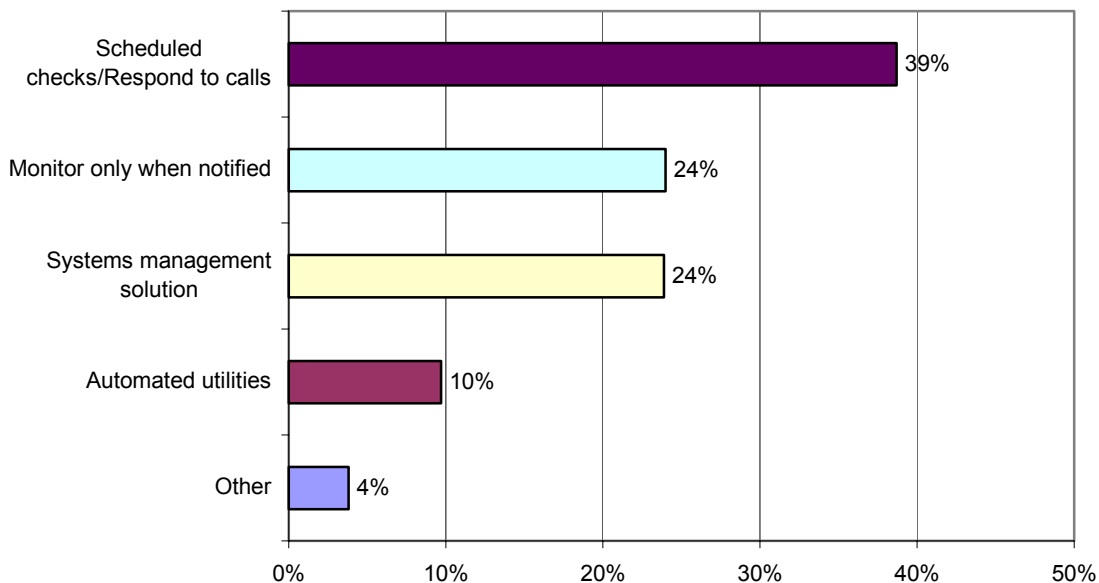
Systems monitoring: Current practices

The research presented in this section addresses general approaches to system monitoring as reported by survey respondents. Particular emphasis is placed on network and systems professionals' approaches to monitoring critical systems. The questions posed to participants explored several key aspects of network and systems management, including:

- The types of utilities used
- The scripting languages employed
- The number and type of applications used to monitor network/systems
- The most frequently monitored network/systems performance parameters
- Type of network connectivity used most frequently
- The time demands associated with network/systems monitoring

In terms of the respondents' primary approach to systems monitoring, the survey data show that less than 40 percent perform scheduled checks of crucial systems, and respond to support calls. About 25 percent indicate that they monitor systems only when an issue is brought to their attention. Only about one-fourth of respondents (24 percent) use a systems management solutions platform that automatically conveys the status on different systems. Less than 10 percent of respondents rely on automated monitoring utilities provided by vendors.

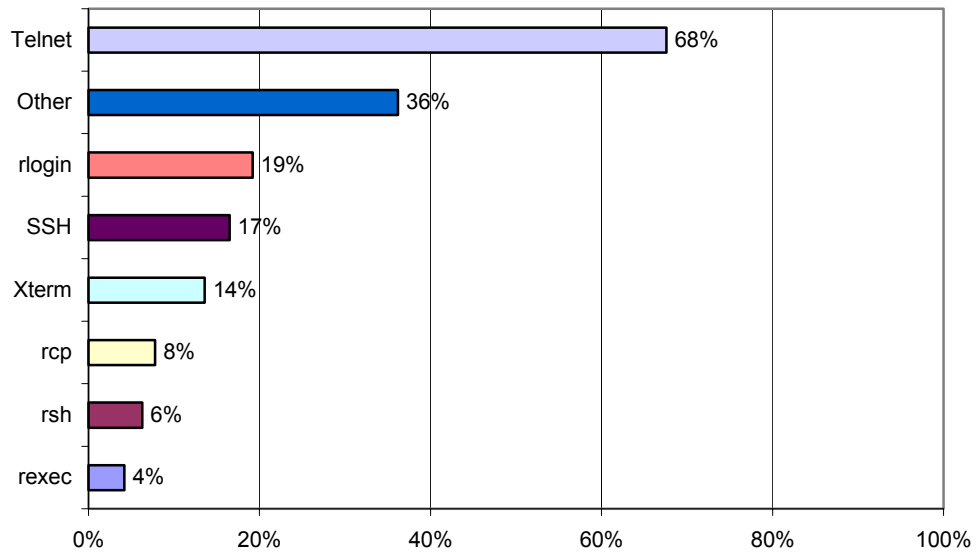
What is your primary approach to monitoring the availability of mail servers, Web servers, databases and other crucial systems? (Choose the most critical approach.)



“Other” responses included reliance on custom monitoring utilities, and development of in-house applications.

Survey respondents were asked to identify the utilities they use for remote systems administration. The results are shown below.

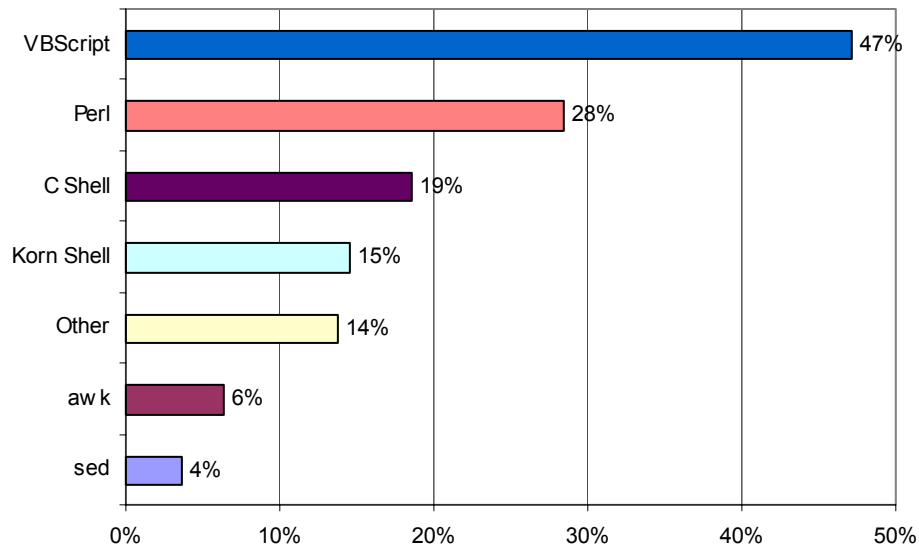
Which utilities do you use for remote systems administration? (Choose all that apply.)



The vast majority of respondents (nearly 70 percent) indicated that they use Telnet for remote systems administration. Data show that rlogin, Secure Shell (SSH), and Xterm were used by less than 20 percent of respondents, respectively. Among the least used utilities are rcp, rsh, and rexec. "Other" responses included RCONSOLE, Terminal Server Win2000, NetOp, and pcAnywhere utilities.

Respondents were also asked to identify the most frequently used scripting languages. The data show that VBScript is most often used by nearly half of respondents (47 percent). Other more commonly used scripting languages were Perl (28 percent), C Shell (19 percent), and Korn Shell (15 percent). Less than 10 percent of survey participants reported using awk and sed most often (6 percent and 4 percent, respectively). These data are presented below.

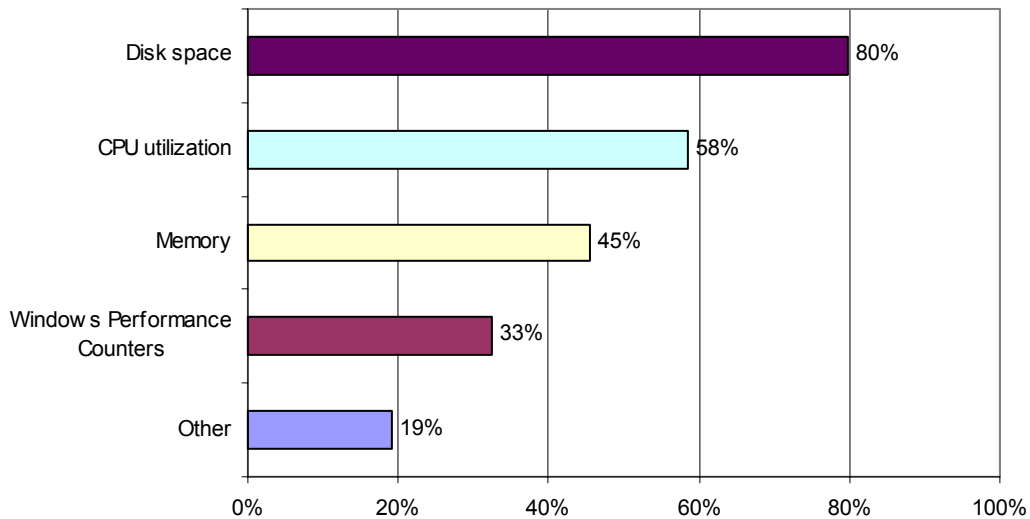
Which scripting languages do you use most often? (Choose all that apply.)



“Other” responses were Java, bash scripts, and .bat scripts.

The study also examined which systems are regularly monitored, and how many different applications are used to monitor key systems.

Which of the following do you monitor daily? (Choose all that apply.)

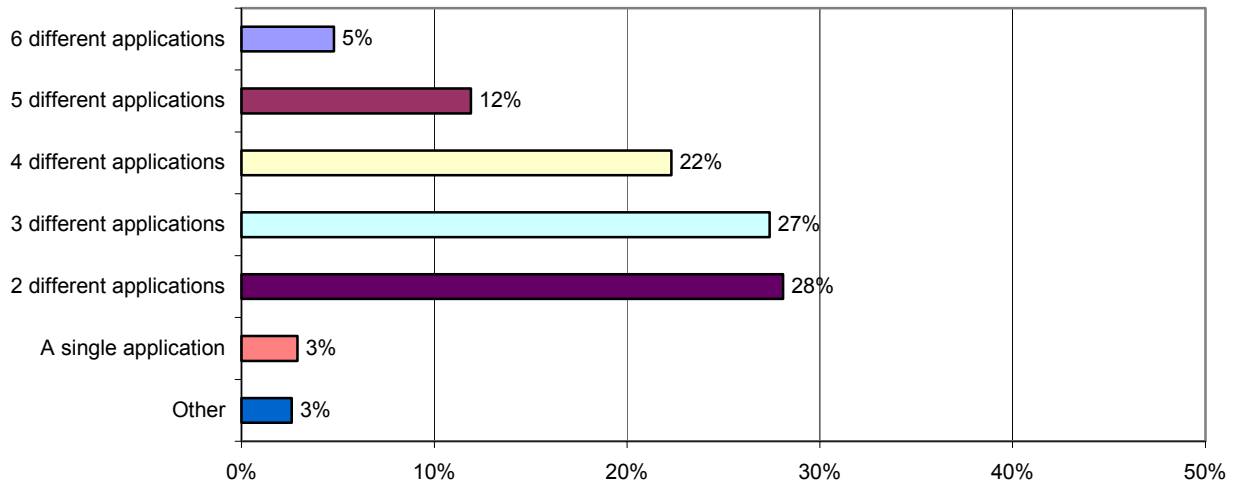


The data, presented above, show that 80 percent of respondents monitor disk space on a daily basis, and almost 60 percent indicated that they also monitor CPU utilization. Memory is regularly monitored by slightly less than half of respondents (45 percent), and Windows Performance Counters are monitored by about one-third of respondents.

“Other” responses indicate that disk cue length, and event logs are also monitored regularly.

Taken together, over half of respondents indicate that they use two or three different applications to monitor critical systems applications. Few respondents (less than 5 percent) monitor with more than four different applications. These data are presented below.

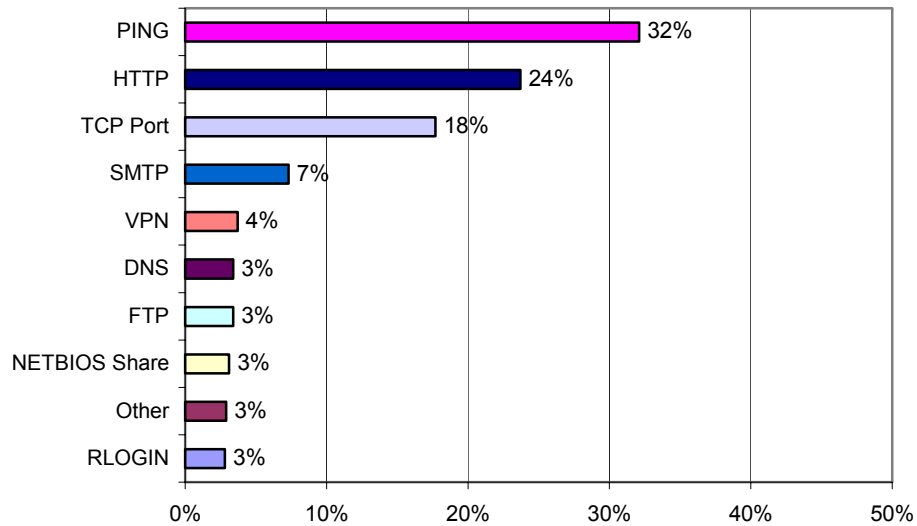
How many different applications do you use to monitor Web sites, email servers, Internet connections, disk space, CPU utilization, memory, and Windows Performance Counters?



“Other” responses included system tools, single-solution sets, and instances where there were too many applications used to accurately count them.

Respondents were asked to identify the category of network connectivity they use most frequently. The results reveal that 30 percent use Ping, and almost one-fourth identifies HTTP as the most frequently used category of network connectivity. Over 15 percent of respondents also rely on TCP Port.

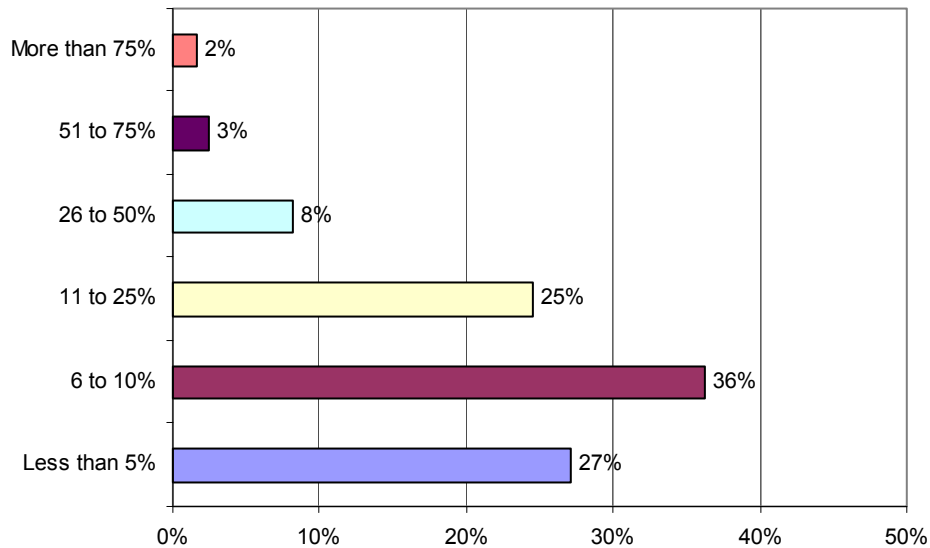
Please select the category of network connectivity monitoring that you use most frequently? (Choose one.)



“Other” responses included IPX sockets, SNMP, SSH, Telnet, RAS, ReachOut and VPN, and NetWare.

Respondents were asked to estimate the amount of time allocated daily to monitoring system status and performance. They were also queried about the management of routine activities (for example, moving data between machines, synchronizing passwords, managing users and groups, and setting up machines). These data are presented below.

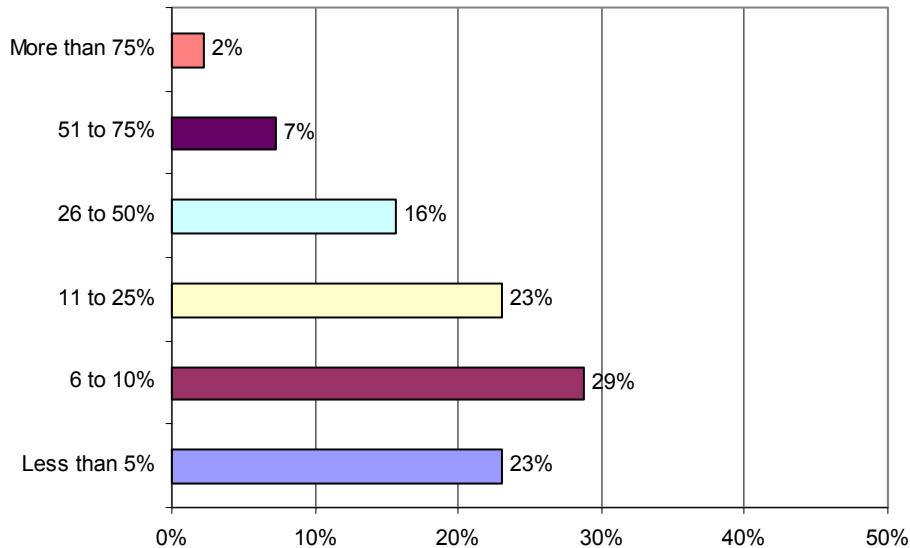
How much of your daily time would you estimate that you spend monitoring the status and performance of your systems? (Choose one.)



Less than 40 percent of respondents indicate that they spend an estimated 6 to 10 percent of their time monitoring system status and performance. Over one-quarter reported that they spend less than 5 percent of their time doing so. Few respondents indicate spending over half of their time monitoring system status and performance. Only 3 percent indicate 51 to 75 percent of their time is spent monitoring status and performance, while less than 2 percent indicate they spend over 75 percent of their time monitoring.

Participants were also asked to estimate the time they spend executing several routine administrative functions.

How much of your daily time would you estimate that you spend doing all of the following: moving data between machines, synchronizing passwords, managing users and groups, and setting up machines? (Choose one.)

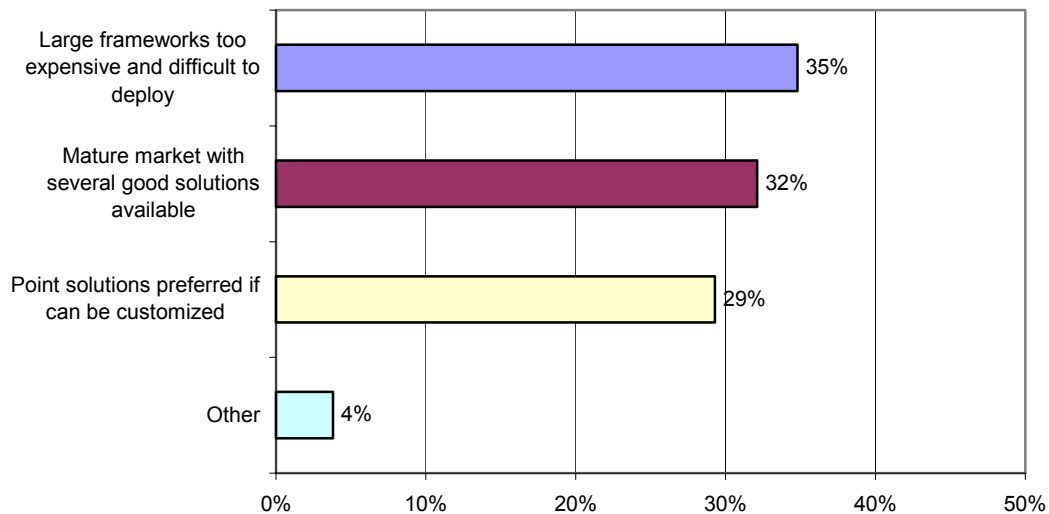


The data show that almost 30 percent of respondents spend 6 to 10 percent of their time performing such functions as moving data between machines, synchronizing passwords, managing users and groups, etc. Just over 15 percent spend from 26 to 50 percent of their time performing these management functions, and over 20 percent indicate that 11 to 25 percent of their time is spent doing so.

Network management tools: Current views

This section of the study details the current opinions of IT professionals on the state of the network management tools market, and the ability to extend or integrate network management solutions with their existing solutions.

Which statement best describes your view of the state of the Network and Systems Management tools market? (Choose one.)

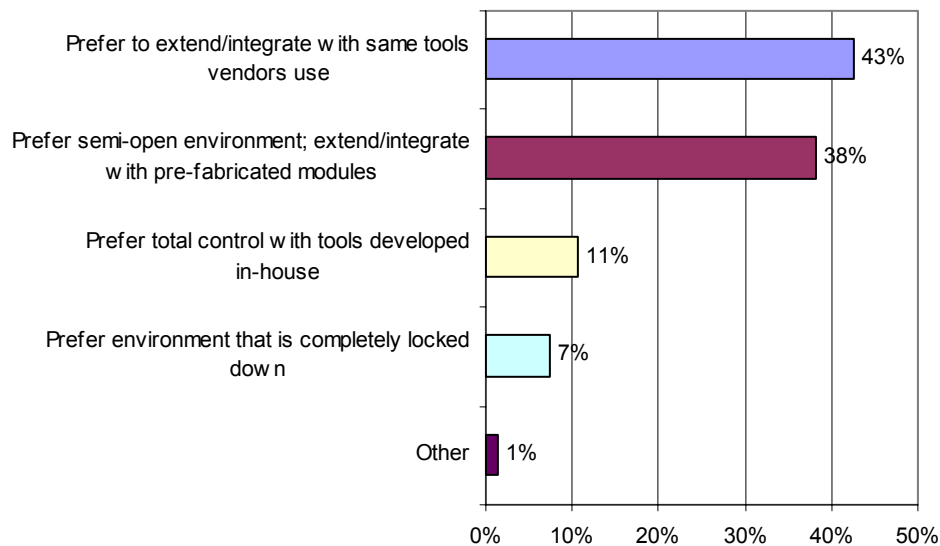


Survey respondents are nearly equally split in their current opinions of the network management solutions market. Thirty-five percent of respondents view the current market as offering large frameworks that are too expensive and difficult to deploy. Thirty-two percent of respondents indicate that the network management solutions market is mature with several good options from which to choose. Almost 30 percent of respondents indicated that point solutions would be ideal if they could be customized.

“Other” responses included the observation that no single solutions are available, and that most existing solutions are unreliable, overly expensive, and do not perform as advertised.

The network and systems professionals surveyed in this study show a strong preference for being able to easily and readily extend their current solutions or integrate new or additional network management solutions with their existing solutions (over 80 percent of respondents). This is evidenced by the preference of 43 percent who want the flexibility and capability provided by vendor-quality tools, and the 38 percent who prefer a semi-open environment that can be extended/integrated with prefabricated modules.

Which statement best describes your view regarding your ability to extend and integrate new or additional network management solutions with your existing solutions? (Choose one.)



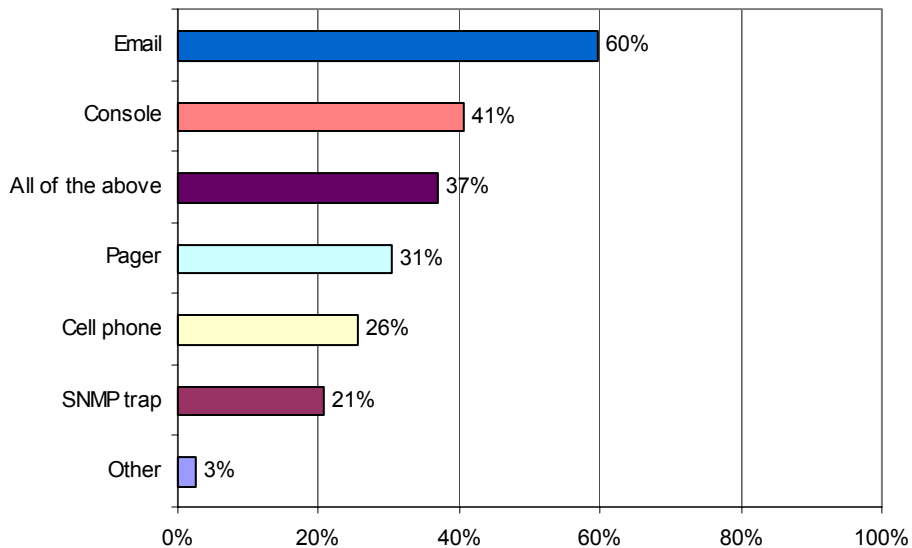
Around 10 percent of respondents prefer having total control with tools developed in-house. Few respondents (7 percent) prefer an environment that is completely locked down. “Other” responses indicate that respondents prefer whatever is cost effective, and produces high-quality results.

Preferred notification mode and interface

Respondents were asked their opinion about how a system monitoring utility should notify them of systems availability issues, and which mode of notification would be preferred if it were the only available mode. In addition, respondents were asked which interface they preferred to work with on network administration tasks. This section presents these results.

By far, the most popular notification mode for respondents was e-mail (almost 60 percent), followed by console notification (40 percent), and pager (30 percent). Twenty-six percent of respondents preferred to be notified by cellular phone, and 20 percent indicated that SNMP trap was their preferred notification mode.

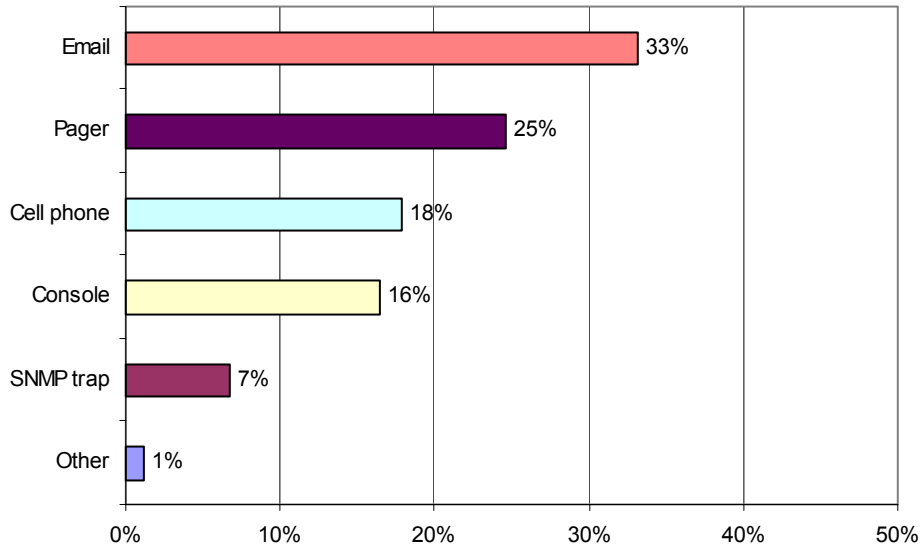
In your opinion, how should a system monitoring utility notify you of systems availability issues? (Choose all that apply.)



Nearly 40 percent of respondents would like to be notified by all these modes. Among other preferred notification modes were fax, integrated alarm-telephone paging system, and MSN messenger.

Respondents were asked to choose the most preferred notification mode if only one were available. These data are presented below.

If only one notification mode was available, which would you prefer as a means of notifying you of systems availability issues?

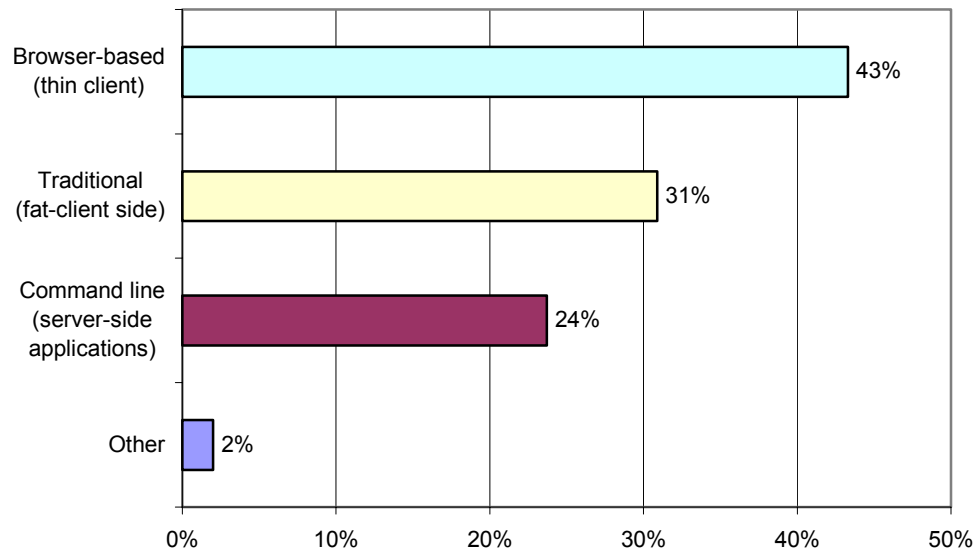


E-mail and pager were the two notification modes chosen by almost 35 percent and 25 percent of respondents, respectively, which together account for over half of the responses. Cellular phone notification was chosen by 18 percent of respondents, and console notification followed closely, endorsed by 16 percent of respondents. SNMP trap was the least preferred mode.

Other modalities included audio system notifications (system “beeps”), and broadcast network messages.

Data presented below reveal that the preferred user interface for system administration tasks is browser-based (thin client), chosen by over 40 percent of respondents. The traditional client/server (fat-client side) followed, endorsed by slightly over 30 percent of respondents. Command line (server-side applications) was chosen by nearly 25 percent of respondents. The heavy preference for browser-based interface suggests that administrators rely on Web-enabled access to be able to take administrative action at any location without the need for special software installed locally.

*Which user interface do you prefer to work with for systems administration tasks?
(Choose one.)*

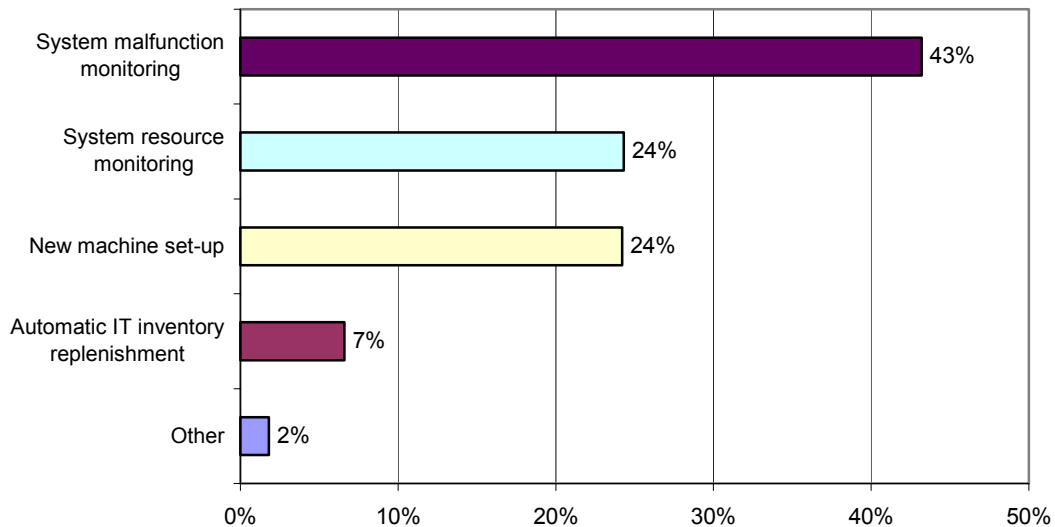


Other user interface preferences included remote desktop, server direct interface, Telnet, and Cisco Works.

Benefits of automated systems monitoring tools

This section of the paper presents data on the benefits of automated monitoring tools. Respondents were asked which aspect of their job would benefit most from automated tools. In addition, to automated monitoring availability, respondents were asked to identify other systems and administrative functions they thought would be useful to automate.

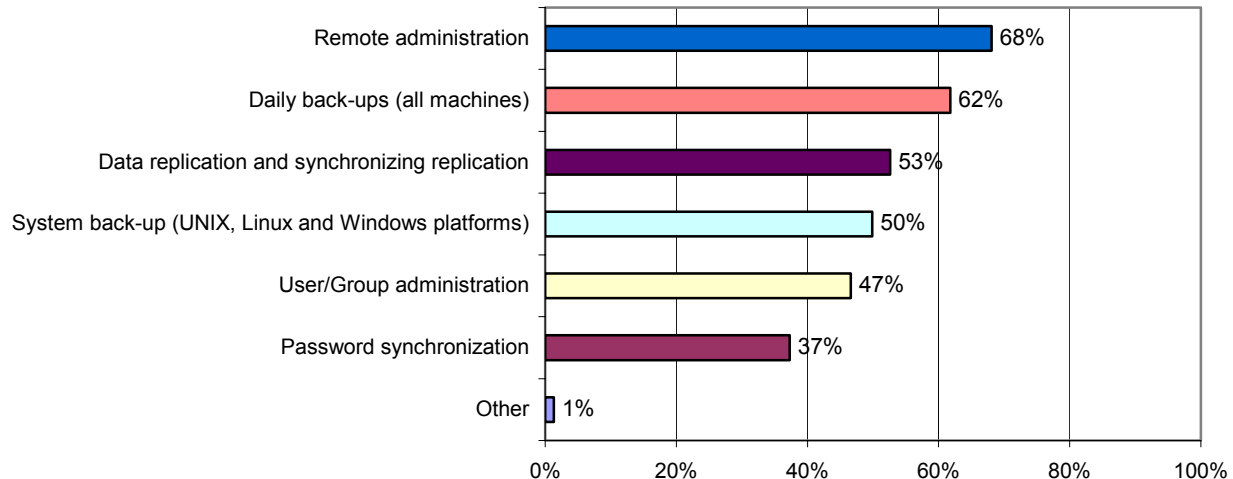
Which aspect of your job would benefit most from automated tools? (Choose one.)



In aggregate, 67 percent of respondents indicated that their job would most benefit from automated monitoring of basic system operations—43 percent stated that automated system resource monitoring of malfunctions would benefit them most, and 24 percent endorsed automated system resource monitoring as most beneficial for their job. Another 24 percent seek automated set-up for new machines as a means to enhance their ability to do their job, while less than 10 percent of participants view automated replenishment of IT inventory as most beneficial. Among other job aspects that would benefit most from automation were monitoring network traffic, monitoring network intrusion attempts, and application of OS patches.

In order to gauge respondents' needs, we asked them about other systems management and administrative tasks they thought might benefit from automation. These data are presented below.

In addition to monitoring availability, what other system management and administration functions would be useful to automate? (Choose all that apply.)



Enabling remote administration was selected by nearly 70 percent of respondents as an aspect of management and administration they would like to see automated. Over 60 percent of respondents also indicated that they would like automation for performing daily back-ups of all machines. Over 50 percent of respondents would like to see replication of data automated, which includes synchronizing the replication.

Half of respondents chose performing back-ups across UNIX, Linux, and Windows platforms as a management/administrative task they would like to have automated. User/group administration was chosen by nearly 50 percent, followed by password synchronization (nearly 40 percent). Among "other" responses were automated filtering, and re-imaging of desktops.

Key insights

This study uncovered several important issues surrounding systems management solutions. These findings may assist administrators and managers as they evaluate the contributions automated systems monitoring solutions make to improved network and systems performance. These key insights are highlighted below.

Systems monitoring: not standard practice

The survey data indicate that the need for systems monitoring is appreciated by the majority of respondents, but current practices center on the reactive approach to systems management, which is not monitoring at all. In fact, respondents report that very little of their day is spent actually monitoring the status and performance of crucial systems. The key findings that support these observations are:

- The majority of respondents respond to support calls or monitor only when an issue is brought to their attention (63 percent).
- Only 6–10 percent of respondents' workdays are spent monitoring systems status and performance (reported by 36 percent of participants).

These data suggest that today's IT operations are likely functioning in a crisis mode where network and systems professionals are required to prioritize their administration duties throughout the day to deal with the most pressing issues first. This modality may effectively relegate monitoring to a lower priority, such that monitoring or checks only occur when some triggering event occurs. When monitoring does take place, it appears that only basic IT performance factors are checked on a daily basis—monitoring system disk space (80 percent of responses), and CPU utilization (58 percent of responses).

Today's network management tools

About 65 percent of respondents find existing network management tools lacking in some way:

- 35 percent see the current market as offering large frameworks that are too expensive and difficult to deploy.
- Almost 30 percent indicate that point solutions would be ideal if they could be customized.

In addition, the overwhelming majority of network and systems professionals surveyed have a preference for network management solutions that integrate with or extend their existing management solutions easily and readily (81 percent overall). These conclusions are based on several findings:

- Most prefer having the same administration tools used by their systems management solution vendors (43 percent of respondents)
- A nearly equal number advocate a semi-open environment that can be extended/integrated with easy-to-use prefabricated modules (38 percent).
- Less than 20 percent desire an environment that is totally controlled by either lock-down or one that requires in-house tools.

These data suggest that network and systems professionals are looking for solutions that can be deployed quickly, and that can be customized readily to meet their unique requirements.

In terms of remote administration capabilities, almost 70 percent of survey participants rely on Telnet. While this technology is adequate in many respects, the fact that Telnet doesn't provide secure connections is clearly one important issue that administrators and managers should reconsider in light of the increasing need for heightened network and systems security. Due to the increased concern for security, Secure Shell (SSH), the secure equivalent of Telnet, will likely experience significantly increased demand in the coming years.

Notification mode and interface preferences

The results of this study indicate that even though the majority of respondents are in a Windows environment, they still seek interfaces that afford them mobility and flexibility. Since network and systems professionals don't know where they'll be moment-to-moment during the workday, they need to be able to take administrative actions from any location or desktop. Hence their pronounced preference for a browser-based interface for systems administration tasks, versus traditional Windows or command line interfaces.

And while respondents indicate a preference for a systems monitoring utility that notifies them of availability issues through a variety of means—email, console, pager, cell phone—if limited to only one notification modality, most preferred email (35 percent of responses). This is understandable. With the spread of wireless email devices, many network and systems professionals are never far from their inbox.

The need for automated systems monitoring tools

This study highlights several critical areas where the ability to manage and administrate the availability of the enterprise's networks and systems would benefit from automated systems monitoring solutions. The job functions that would benefit most from such solutions include:

- Automated system monitoring of malfunctions (40 percent of responses)
- Automated system resource monitoring (24 percent of responses)

The study also reveals other network and systems management and administrative tasks that 50 percent or more of respondents believe could benefit from automated monitoring, including:

- Automated daily back-ups of all machines
- Automated replication of data (including data synchronization) on a regular basis
- Automated back-ups across UNIX, Linux, and Windows platforms
- Automated user/group administration

When viewed along with the finding that only 6–10 percent of the administrators' or managers' day is spent monitoring, it is easy to see why these IT professionals value the benefits of automated monitoring technologies. Today, they have little time to devote to monitoring and this constraint may be confounded by the fact that many do not have the right tools to help them do the job properly and efficiently. Recall, most companies are not proactively monitoring the availability of their networks and systems, and again, this may be due to the lack of adequate resources—tools and staff.

In addition, network and systems professionals need automated monitoring tools that readily support multiple scripting languages that permit customization of tools for specific situations. This feature enables them to automate corrective actions found or identified through monitoring, a critical component of an effective automated monitoring solution.

The importance of supporting multiple scripting languages is also confirmed by the finding that after monitoring availability, survey participants think that remote administration is clearly the second most important systems management/administration function that should be automated. Obviously, remote administration cannot be automated without the ability to work in a variety of scripting languages.

In summary, these results highlight the critical need that IT professionals have for monitoring solutions that will alert them to potential system malfunctions automatically, and solutions that will also insure that adequate systems resources are available to meet user demand. Moreover, due to the diverse operating systems and other technologies that reside in today's network and systems infrastructure, for a monitoring solution to be useful it must support a wide variety of scripting languages.

TechRepublic Community Research Programs

The Community Research team conducts surveys of the TechRepublic membership on a project basis. Projects are funded by TechRepublic and in some cases by vendors who have particular interests in topical areas. In cases where the project has been sponsored by a third party, the Community Research team leads the effort in developing survey questions and has final approval of all questions. The Community Research team conducts all analyses and writes the final report that is subject to TechRepublic editorial review. Funding for this project was provided by MKS, Inc. If you have a topic of interest for either editorial or sponsored research, please e-mail us at research@techrepublic.com.

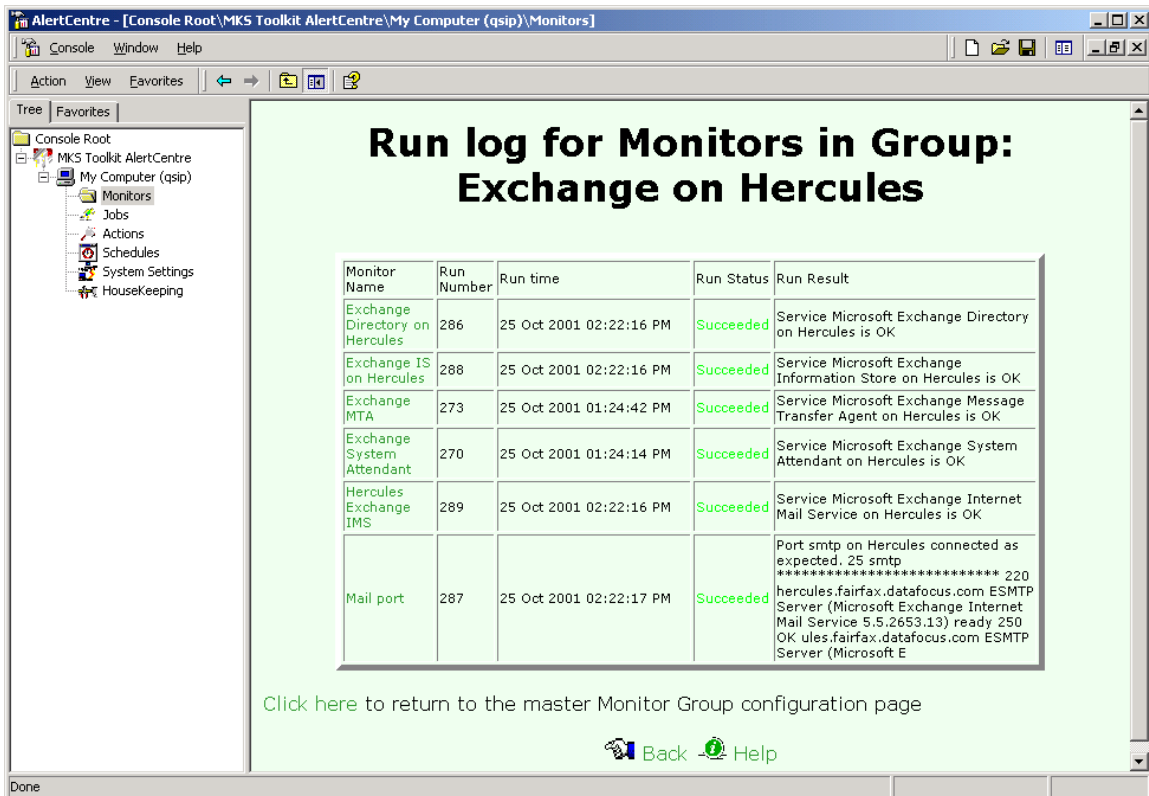
Appendix

MKS AlertCentre

Automated Monitoring, Alerting, and Corrective Action Solution for Windows

MKS AlertCentre™ is an exciting new solution for monitoring, alerting, escalation and corrective action automation. AlertCentre can monitor your mission-critical systems and applications 24x7 to provide you with the “peace of mind” of knowing that your network, applications, and Internet/Intranet-based information systems are running normally. Things do occasionally go wrong; when they do, AlertCentre ensures that you are the first to know so you can minimize any detrimental effects on your business.

AlertCentre is available in a specially packaged bundle with MKS Toolkit for System Administrators 8.0 and as an add-on to other MKS Toolkit 8.0 products.



What is AlertCentre?

AlertCentre (www.alertcentre.com) is a monitoring solution for System Manager, System Administrators and other IT professionals that need to ensure the high availability of network-based resources such as Web sites and email servers as well as disk space and remote access facilities. AlertCentre enables System Administrators to define monitors that can observe, report on, and control the activities of other programs or devices on your network so that you can be sure that mission-critical applications are up and running at all times. AlertCentre gives you and your colleagues the ability to be notified in a timely fashion if anything on your network is malfunctioning.

How can AlertCentre help System Managers and System Administrators?

AlertCentre is a cost-effective, easy to use point solution and provides System Managers and System Administrators with availability monitoring that is built on an integrated foundation for scheduling, alerting, and automating repairs. Unlike the large, monolithic monitoring solutions in the marketplace, AlertCentre is easy-to-install and enables you to improve availability without having to wrestle with the solution itself. If the availability of information resources is important to your organization, then you need MKS Toolkit for System Administrators 8.0 with AlertCentre.

AlertCentre enables system administrators and other IT professionals to:

- Monitor the availability of:
 1. Individual physical and virtual IT resources such as URLs, CPUs, system services, mail ports, etc. through the use of a wide variety of monitor types.
 2. Complex applications such as mail servers and Web sites that require a host of underlying hardware or software resources to be functioning normally in order to minimize downtime for you and your customers.
- Monitor remote devices and IT resources from any workstation or Web-aware device with access to your network.
- Implement an escalation process to notify the right people and take appropriate action based on the severity of a problem.
- Be notified through various media including e-mail, cell phone, pager, SNMP trap, or through the execution of an error recovery script that can leverage the full power of MKS Toolkit scripting to maximize your responsiveness to critical issues whether you are in or out of the office.
- Extend the power of AlertCentre through the powerful MKS Toolkit scripting languages including Perl, KornShell, awk, C Shell; as well as Windows Script Host to customize and evolve your Network, Systems, and Application Administration within your organization.
- Schedule Batch Jobs to automate the timely execution of processes.
- Measure performance through Windows Performance Counters including scriptable access to the counters via Perl and Windows Script Host (using either VBScript, PScript™ or JScript) for complete awareness of the health of your network.
- Limit access to only authorized AlertCentre users.

Flexible Architecture

AlertCentre is built on an integrated platform that includes a powerful scheduling engine, an action engine to drive notification, and automated recovery actions, in addition to the robust scripting engines of MKS Toolkit for System Administrators. MKS Toolkit for System Administrators also includes many tools and utilities for comprehensive system and network administration. Move data and files between machines, remotely administer systems, and perform backups across UNIX, Linux, and Windows platforms. Increase productivity and automate repetitive tasks like password synchronization, adding users and groups, setting up new machines, cloning a system file or a document tree on local or remote systems. Script and execute repetitive tasks that you could only do previously one-at-a-time using graphical Windows utilities. Perform complex file searches and copy permissions between objects from a single desktop.

Monitor Groups

AlertCentre Monitors can be organized into groups for ease of administration. Groups are handy when monitoring complex applications such as Web sites that require constant vigilance at the network, system, application and content levels. One Web site may require multiple monitors at each level such as monitors for both Web system services as well as database system services.

Admin Process Automation

AlertCentre provides you with workflow capabilities for integrating system administration procedures with other functional areas within your organization. It enables you to create Batch Jobs that execute scripts based on defined events or schedules and provide verification that the scripts execute correctly. Jobs can conditionally execute other actions or jobs based on their success or failure. Jobs extend the use of AlertCentre's integrated scheduling, alerting and scripting platform beyond monitoring to administrative process automation and provide a glimpse of how additional functionality will be able to be integrated in the future.

Built-in Redundancy

AlertCentre allows you to define a backup monitoring station in addition to your primary. The backup monitoring station is regularly synchronized with the primary to insure they both have identical monitoring configurations so if the primary station fails for any reason the secondary station automatically picks up where the primary left off to insure your networks, systems and applications are running smoothly. The AlertCentre license allows you to install one primary and one backup station.

Custom Monitors

AlertCentre allows you to define custom monitors to handle any specialized monitoring that you need to do. And, because AlertCentre is part of MKS Toolkit for System Administrators (TKSA), you have the full resources of TKSA to build scripts for your custom monitors. As an example, you may want to define a custom monitor to check inventory levels on your web store and define a batch job to automatically re-order a given product when the inventory falls below the re-order point.

AlertCentre Monitor Types

Monitor Type	Description
Network Connectivity	Network Connectivity Monitors enable you to ensure your network is connected and available to authorized users and devices from all appropriate access points.
HTTP	The HTTP Monitor insures that specified URLs, and therefore your business critical Web content, are available. AlertCentre supports both HTTP and HTTPS addresses on the Windows platform.
FTP	The FTP Monitor insures that you can connect to and retrieve a file from your FTP server.
SMTP	The SMTP Monitor insures that your mail server can send and accept requests and messages.
TCP Port	The TCP Port Monitor determines whether a service on a TCP port is connectable.
NetBIOS Share	A NetBIOS Share Monitor verifies that files are accessible over the network to any network mounted drive.
DNS	The DNS Monitor insures that domain names and addresses can be found and that the DNS server itself can accept requests.

Monitor Type	Description
Remote Access	The Remote Access Monitor attempts to make a dial-up connection with an ISP or Remote Access/VPN server.
Ping	The Ping Monitor insures the continuous availability of specified hosts via the network.
Resource Availability	Resource Availability Monitors enable you to ensure your systems infrastructure is available with adequate capacity and performance.
Disk Space	The Disk Space Monitor insures that you are aware of and can control disk space utilization.
CPU Utilization	The CPU Utilization Monitor insures that your systems are not CPU-bound by reporting and acting on CPU use percentage data.
Memory Utilization	The Memory Utilization Monitor insures that your virtual memory use falls within acceptable tolerance levels.
Performance Counter	The Windows Performance Counter Monitor is a generalized way to monitor any Windows Performance Counter and measure it against an expected state. AlertCentre automatically enumerates the Windows Performance Counters that are available on the machine you need to monitor.
Application Availability	Application Availability Monitors enable you to ensure your mission-critical applications are available to authorized users and that the content has not been tampered with.
Windows Service	The Service Monitor insures that ANY Windows service, such as DNS, TCP/IP, Telnet and even application services like Microsoft® Exchange®, IIS®, or SQL Server® are up and running.
Web Page	The Web Page Monitor retrieves a selected URL, checking for regular expressions within the page. The use of regular expressions provides much more power and flexibility than using plain text search strings.
ODBC Database	The ODBC Database Monitor insures that your ODBC-capable database system can successfully process a query.
Windows Event Log	The Windows Event Log Monitor triggers alerts when specific entries are added to one of the Windows NT Event Logs (System, Application, Security, DNS, or IExplore). Event log monitoring can be used to control remote logons and other security-sensitive events. It can also be used to execute custom actions when remote logons occur such as disabling accounts or downloading software updates to remote systems.
Application Log	The Application Log Monitor reads any flat file application log, such as a Web server log, and reports or triggers alerts based on content.

Download MKS Toolkit for SysAdmin with AlertCentre today: <http://www.mkssoftware.com/eval/>

MKS, Toolkit, and Integrity are registered trademarks and AlertCentre is a trademark of MKS Inc. All other trademarks mentioned in this release are the property of their respective owners.



MKS Contact Information
800-637-8034 +1(703) 803-3343 www.mkssoftware.com