Realtime
publishers

The Shortcut Guide™ To

Smart Network Management for the SMB

sponsored by

Chris Hampton

Copyright Statement

Chapter 2: The Importance of Proactive Monitoring and Alerting

I have spent a good portion of my career as a consultant working with businesses both large and small. One consistent problem I have seen is the inability of network administrators to focus and dedicate the necessary time to the project at hand. The projects are fully funded and backed by the correct stakeholders, yet the designated administrators are missing in action for a large portion of the project.

As I worked alongside these administrators on projects, I began to understand the core problem. Many spend the majority of their day jumping from support call to support call. They are constantly interrupted by having to chase down system- or network-related issues. These minor interruptions cause delays and often the entire project is put on hold to address a major IT crisis. The issues commonly begin as a small blip on the network radar, but as they go unnoticed, that small blip grows into a major outage.

The cost to the business for these delays can be critical to the project timeline and achieving planned milestones. The cost to the administrator is manifested in frustration that they cannot focus on key project tasks and they find themselves missing opportunities for knowledge transfer and training during the project.

The fault is not with the administrator for a lack of skills or knowledge; the problem is the network itself and how minor issues are reported. In network environments that lack an intelligent network management solution, key server metrics and network device alerts never leave the confines of the individual system or device. This means the administrator has no visibility into the issue.

In such an environment, the administrator is required to log in to each system or device, review event logs, and manually monitor each system metric. Multiply this process times 10 or 20 systems, and the time to undertake such tasks is impractical. With pressure from the company to do more with less, administrators fall back into a pattern of break-fix administration. This is due to a lack of time to properly monitor the network.

In Chapter 1, the importance of *complete visibility* was outlined—speaking to overall awareness of every system and device on the network. Although awareness is important, without the ability to reach into each device and monitor key metrics and alerts, the administrator is still left in the dark with regard to specific issues.

What's needed is a network management solution that closely watches individual systems and devices looking for minor threshold changes or event entries that indicate a potential problem. The individual changes and entries are then pooled together, prioritized, and reported to the administrator in a central console. This functionality is referred to as *sophisticated monitoring*.

Stop Fighting Fires

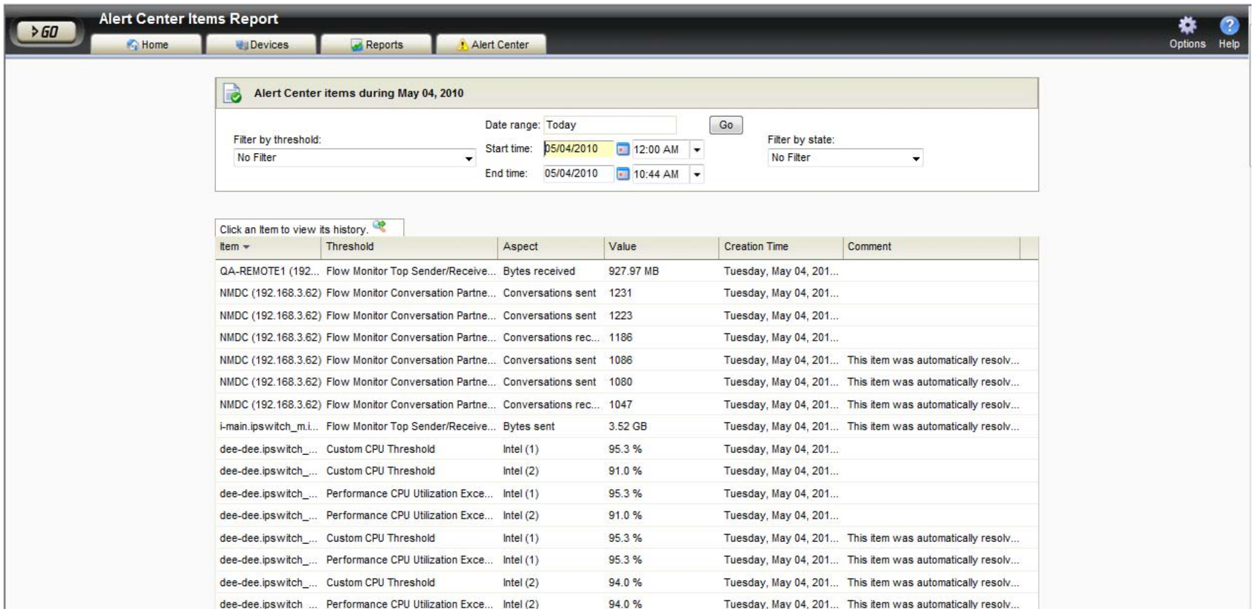
How are the network administrators within your SMB spending their days? Do they find themselves pulled in multiple directions attempting to respond to the most recent pressing issue? Have you been forced to delay important internal projects because your IT staff does not have the time to dedicate to new initiatives? Are you tired of constantly working in a reactive mode and being interrupt driven?

Unfortunately, this is how a large number of SMBs operate. With limited time and budgets, along with an increasing number of IT projects, SMB's demand more from their network administrators. If there was a "wonder product" out there to give back control of their day to the network administrator, the product name would include the word *proactive*.

In Chapter 1, survey data from a 2007 study by the Strategy Group of 173 SMBs was reviewed. Almost half of the SMBs surveyed (46 percent) had a reactive approach to network monitoring and problem solving. It is interesting to note that companies with a more proactive or strategic approach spend a smaller percentage of their budget just keeping things running (60 to 65 percent) compared with those with a reactive or chaotic approach (75 to 80 percent). SMBs need a network management solution that allows them to become more proactive in support of their network.

Proactive management of the network also requires a change in mindset. For the business, this requires a structural change in the way IT approaches network monitoring. Within most SMBs today, the network administrators often wear many hats—they are required to cover tasks ranging from hooking up a new printer to deploying a company-wide messaging system. In this busy environment, the administrator does not have the time to spend establishing a planned monitoring, alerting, and reporting system.

The network management solution needs to align with this model by providing a number of time-saving features such as single pane of glass alerting across all devices, automated monitor creation based on discovered devices, and built-in tracking and reporting of performance trend data. Figure 2.1 presents the concept of a single pane of glass for all notifications, alerts, and acknowledgements within a network management system.



Alert Center items during May 04, 2010

Filter by threshold: No Filter

Date range: Today

Start time: 05/04/2010 12:00 AM

End time: 05/04/2010 10:44 AM

Go

Filter by state: No Filter

Click an Item to view its history.

Item	Threshold	Aspect	Value	Creation Time	Comment
QA-REMOTE1 (192...	Flow Monitor Top Sender/Receive...	Bytes received	927.97 MB	Tuesday, May 04, 201...	
NMDC (192.168.3.62)	Flow Monitor Conversation Partne...	Conversations sent	1231	Tuesday, May 04, 201...	
NMDC (192.168.3.62)	Flow Monitor Conversation Partne...	Conversations sent	1223	Tuesday, May 04, 201...	
NMDC (192.168.3.62)	Flow Monitor Conversation Partne...	Conversations rec...	1186	Tuesday, May 04, 201...	
NMDC (192.168.3.62)	Flow Monitor Conversation Partne...	Conversations sent	1086	Tuesday, May 04, 201...	This item was automatically resolv...
NMDC (192.168.3.62)	Flow Monitor Conversation Partne...	Conversations sent	1080	Tuesday, May 04, 201...	This item was automatically resolv...
NMDC (192.168.3.62)	Flow Monitor Conversation Partne...	Conversations rec...	1047	Tuesday, May 04, 201...	This item was automatically resolv...
i-main.ipswitch_m.i...	Flow Monitor Top Sender/Receive...	Bytes sent	3.52 GB	Tuesday, May 04, 201...	This item was automatically resolv...
dee-dee.ipswitch_...	Custom CPU Threshold	Intel (1)	95.3 %	Tuesday, May 04, 201...	
dee-dee.ipswitch_...	Custom CPU Threshold	Intel (2)	91.0 %	Tuesday, May 04, 201...	
dee-dee.ipswitch_...	Performance CPU Utilization Exce...	Intel (1)	95.3 %	Tuesday, May 04, 201...	
dee-dee.ipswitch_...	Performance CPU Utilization Exce...	Intel (2)	91.0 %	Tuesday, May 04, 201...	
dee-dee.ipswitch_...	Custom CPU Threshold	Intel (1)	95.3 %	Tuesday, May 04, 201...	This item was automatically resolv...
dee-dee.ipswitch_...	Performance CPU Utilization Exce...	Intel (1)	95.3 %	Tuesday, May 04, 201...	This item was automatically resolv...
dee-dee.ipswitch_...	Custom CPU Threshold	Intel (2)	94.0 %	Tuesday, May 04, 201...	This item was automatically resolv...
dee-dee.ipswitch_...	Performance CPU Utilization Exce...	Intel (2)	94.0 %	Tuesday, May 04, 201...	This item was automatically resolv...

Figure 2.1: Consolidated notifications, alerts, and acknowledgements.

Network Monitoring

To make the transition from a reactive approach to more proactive network monitoring, the network management solution you implement must provide the ability to gain immediate insight into the health, status, and performance of every device on the network. With today's complex networks, not every device has the same priority; from high-profile messaging systems to low-priority test labs, your network requires specific levels of monitoring. High-profile systems and devices have a high level of visibility and any downtime is unacceptable, while the lower-priority lab devices are important but can tolerate more downtime.

In addition to the level of monitoring required, the systems and devices on your network require different monitoring technologies and speak different languages. The routers and switches need to speak Simple Network Management Protocol (SNMP) while the Windows-based hosts require Windows Management Instrumentation (WMI) interrogation; Unix and Linux systems will require communication via SSH protocol.

What Is WMI?

WMI is the underlying protocol for publishing management and operations data on Windows-based operating systems (OSs) and applications. WMI is a specific set of extensions to the Windows Driver Model that provides an OS interface through which instrumented components provide information and notification.

The network management solution selected should incorporate multiple types of monitors that give the administrator the flexibility to select the right monitoring level for the right device at the right time. The monitors also must support a broad set of network technologies allowing visibility into all systems and devices.

The following list highlights the specific types of network monitors to look for:

- Active monitors have the ability to communicate with, track, and alert you in real time when devices or systems are down.
- Passive monitors "listen" for external signals such as SNMP traps or log messages, allowing network issues to be identified and altered.
- Performance monitors track the health of the network devices and systems over time, and are crucial to proactive troubleshooting and planning.
- Custom monitors can be configured to track individual performance metrics for network devices and systems as required.
- Threshold monitors alert you when minimum or maximum values have been reached on a specific device or system.
- Active script performance monitors support additional customization through JScript and VBScript.

To better understand how these network monitors can be used within a proactive network monitoring solution, it helps to see them in action. Figure 2.2 highlights a high-profile application server; this server is very important to the operation of the business and any un-alerted interruption or downtime would be costly.

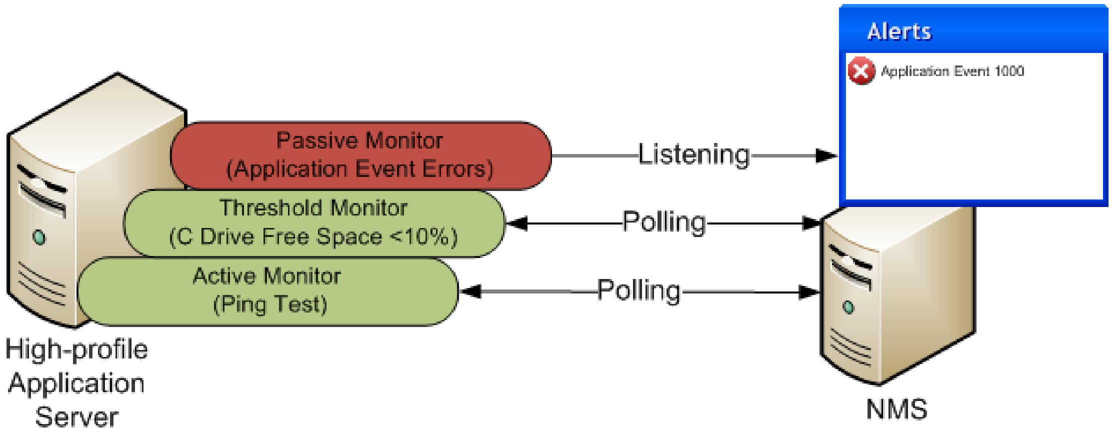


Figure 2.2: Proactive network monitors.

The SMB in this example has employed three network monitors for a critical application server. Individually, each of these network monitors provides important feedback into the health of the application server:

- Active monitor (ping test)—A simple ping test can confirm basic network connectivity with the host system.
- Threshold monitor (C drive free space)—A threshold monitor provides polling of the free drive space on the system partition.
- Passive monitor (application event errors)—A passive monitor listens for specific application log event errors, indicating an issue with the application.

Although each of these individual monitors provides key metric data with regard to the application, the power is in grouping these individual monitors to create a proactive monitoring set. To highlight the benefits of grouping monitors, first think about what type of overall system status profile can be attained by using each monitor separately.

If only one of these monitors were employed, for example the active monitor ping test, a false positive monitoring profile would be generated for the application server. The ping test would be successful, and the flagged application event error would go unnoticed within the network management console.

Together these three network monitors can provide a full picture of the profile status for the critical application server. Use of a well-planned grouping of individual monitors provides a complete proactive monitoring solution for the application server.

Additional extensibility of network monitoring really comes into play when active script monitors are incorporated with traditional monitoring. These powerful monitors allow the introduction of specific customized checks of a device or system that can provide deeper visibility into the status of the device.

Active script monitors allow the use of custom code written in a variety of scripting languages such as JScript or VBScript. In the following example, a script excerpt shows a database being opened and the number of rows being checked. If the SELECT statement returns more than 0 rows, the database is considered available.

```
objConnection.ConnectionString = "Driver={SQL Server};" & _

      "Server=SQLSERVER;" & _

     "Database=DBName;" & _

     "uid=username ;"&_

     "pwd=password;"
objConnection.Open

objRecordset.CursorLocation = adUseClient

objRecordset.Open "SELECT * FROM TableName" , objConnection

 'adOpenStatic, adLockOptimistic

If objRecordset.recordcount < 1 Then

 'Set the result code of the check (0=Success, 1=Error)

Context.SetResult 1, "Error"

Context.LogMessage "Checking Address=" & Context.GetProperty("Address")
```

As powerful as these network monitors are, they still fall short of providing the SMB the ability to understand the ebb and flow of the network. SMBs in today's economy are under pressure to cut expenses—IT budgets are being tightened and CIOs and directors within SMBs are having a difficult time justifying additional purchases. Many business owners are demanding detailed capacity and forecasting reports, requiring detailed return on investment (ROI) information before IT budget dollars are spent.

Network monitoring alone cannot provide the required information for these types of reports. What is needed is a network management solution that offers an integrated systems monitoring capability.

Systems Monitoring

Chapter 1 discussed the importance of network discovery. The ability to know when a new device or system comes onto the network is important. Although important, discovery of the device is really just the beginning—smart network management solutions extend the discovery process by including the ability to establish automated monitoring of each device's Layer 2 connectivity. Beyond this functionality, smart network management solutions ensure the health and performance of each system is tracked through its life cycle.

What Is Layer 2?

Layer 2 refers to the data link layer of the commonly-referenced multilayered communication model, Open Systems Interconnection (OSI). The data link layer is concerned with moving data across the physical links in the network. In a network, the switch is the device that redirects data messages at the layer 2 level, using the Media Access Control (MAC) address for each device to determine where to direct the message. Layer 2 monitoring and management within a network management system focuses on the basic connectivity of each device to the network.

Systems monitoring extends beyond the initial discovery process and Layer 2 connectivity monitors to provide full life cycle management of the system. Think for a moment about the cycle a new system follows within your network environment (see Figure 2.3).

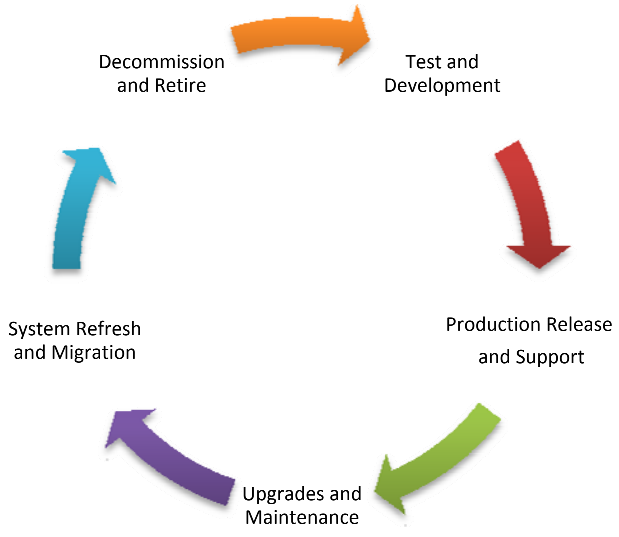


Figure 2.3: System life cycle.

As a system moves from development into production, its monitoring requirements change. The priority of the system is elevated, calling for additional system-level monitoring to ensure performance is maintained. As new upgrades are applied or maintenance patches are released, the monitoring profile must be adjusted and key metrics need to be tracked to validate the upgrade benefits. Trending data becomes important as the system ages to determine system refresh intervals and to contrast performance after a migration to new a platform. Once a system is prepared for decommissioning, active monitoring must be removed and alert priorities adjusted.

At each stage of the life cycle, systems monitoring utilizes key features that provide the required level of monitoring for the specific system. In addition to the monitoring requirements for an individual system's life cycle, the systems management solution also needs to address the different types of systems within the network. From demanding database systems spanning clustered server nodes to virtual hypervisors hosting numerous virtual machines, the challenges of monitoring a diverse systems environment are many. SMBs need a holistic systems monitoring option that includes resource monitoring, process monitoring, hardware monitoring, file system monitoring, and virtual machine monitoring. In today's SMB environment, many technologies that were once only attainable at the large corporate level are now making their way into the SMB network. One example of this progression is server virtualization. With the huge cost advantage of consolidation through virtualization, many SMBs are introducing this technology into the data center.

Resource Monitoring

Utilizing application layer protocols like WMI and SNMP among others, the basic systems monitoring capability is extended into the Windows or Linux OSs allowing availability monitoring of system and application services. Additionally, performance monitoring of CPU, memory and disk statistics can help to identify under or over utilized systems, easing capacity planning initiatives.

A prime example of the power of implementing a resource monitor is the use of SNMP to reference the management information base (MIB) of a router to monitor the port link status for a critical Internet-facing port.

> **How Does SNMP Monitoring Work?**
>
> SNMP does not define which information or variables are available from a network device. Rather, SNMP uses an extensible design that allows the reading or setting of a variable as defined within the MIB for the specific device. SNMP is the protocol used to access the information on the device.

Process Monitoring

Further insight into system availability can be tracked by monitoring the individual processes associated with a specific service. Each application and service that is running on a system spans an individual process that can be monitored by a defined process monitor. This is helpful when a system service is not exposed within the vendor's MIB. For example, in the case of the antivirus software installed on a critical email server, there is no defined MIB to reference. With a process monitor, the antivirus' executable can be monitored to ensure it is running on the email server.

Hardware Monitoring

Often, early indications of a system failure come in the form of hardware-level warnings. Hardware monitors that provide visibility into fan, power supply, and temperature status can give the administrator the advanced notice needed to proactively avoid a system failure.

File System Monitoring

Many applications utilize temporary directories or cache directories during application execution. The presence of files within these directories often indicates the health of the application. By using file system monitoring, key directories can be watched and alerts can be set indicating a hung or failed application. Specific tracking of file- and folder-level information enhances the basic systems monitoring capability. By monitoring file existence, file size changes, or file counts within important log directories, proactive management of applications can be provided. For example, with Microsoft Exchange Server 2010, a large file count of transaction log files for a specific mailbox database can indicate an issue with the backup environment for the entire Exchange messaging system.

Virtual Machine Monitoring

With the wider adoption of virtual infrastructures, many SMBs are facing a new problem with regard to virtual machine or server sprawl. With the ease of server creation offered by virtualization, many businesses have the tendency to create additional virtual machines with little thought as to the performance monitoring of each virtual host and its related virtual machines.

The systems monitoring solution must extend into the virtual environment to provide the same level of granular performance monitoring capabilities delivered at the physical server level. Key to the SMB is a network management solution that provides a single pane of glass for monitoring the virtual infrastructure and the physical network.

To accomplish this, a network management system must support direct connectivity at the hypervisor level using technologies such as VMware's vSphere application programming interface (API). Through the integration with the hypervisor's API, the network management system provides full visibility into monitoring metrics at both the virtual machine and host level.

With advanced visibility at the vendor-specific hypervisor level, important performance thresholds can be monitored on host and virtual machines. Real-time alerts can be set for notification of utilization breaches across virtual machines and hosts. An important monitoring change to understand with regard to virtualization vendors is the lack of support for SNMP data collection within the virtual infrastructure. Vendors such as VMware are moving away from providing any level of performance information via SNMP (one reason for doing so is security considerations). This makes the search for a smart network management solution that provides full system monitoring of the virtual infrastructure that much more critical.

In addition, industry analyst are calling for the growth in multi-vendor virtualization environments due to the cost advantage and differing performance profiles for the application workloads across the business. The systems monitoring solution must support multiple hypervisors.

When these systems monitoring options are used together, the complete life cycle of each device and system is monitored and tracked. Within a smart network management solution, the systems monitoring data is pooled into a central database. The use of historical trending of all monitoring data allows SMBs to gain access to the information required to compile detailed performance trending reports and build capacity planning forecasts.

Application Monitoring

Applications make your business work—users rely on consistent performance across an ever-growing set of applications. Because of the high-visibility aspect of applications, if there is an outage or degradation of performance,. your users will be knocking on your door.

When it comes to proactive monitoring and awareness, application monitoring is at the top of the list of importance. Your SMB needs a network management solution that gives you visibility into application performance and provides advanced notification of stability issues before they affect the end users.

Another problem facing SMBs is the introduction of more complex applications. These applications span multiple servers each with critical services and processes. For example, take the recent change in architecture introduced within Microsoft Exchange 2010. As Figure 2.4 shows, Exchange 2010 utilizes a distributed role architecture, which separates key mail flow, processing, and storage into designated components. These components are modular, allowing the use of multiple server platforms to provide more flexibility in performance, availability, and scalability.

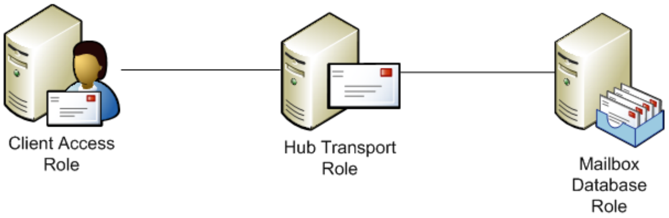


Figure 2.4: Microsoft Exchange 2010 tiered architecture.

You need a way to tie these tiered applications together and bring them under the network management environment. Smart network management solutions utilize a combination of IP service monitors with application monitors to tie everything together within a tiered application architecture. Looking at the Microsoft Exchange 2010 example again, you can see how the use of each type of monitor enhances the overall application monitoring of the Exchange 2010 architecture:

- IP services HTTPS monitor—By monitoring the health and status of the HTTPS services on the Client Access role server, Outlook Web Access (OWA) availability can be closely tracked.
- Application threshold monitor—By utilizing a specific Exchange 2010 Hub Transport threshold monitor for the Active Mailbox Delivery queue, delivery issues can be quickly alerted and acted upon.
- Application service monitor—By utilizing a specific Exchange 2010 Mailbox service monitor for the MAPI Information Store service, critical mailbox database access can be monitored.

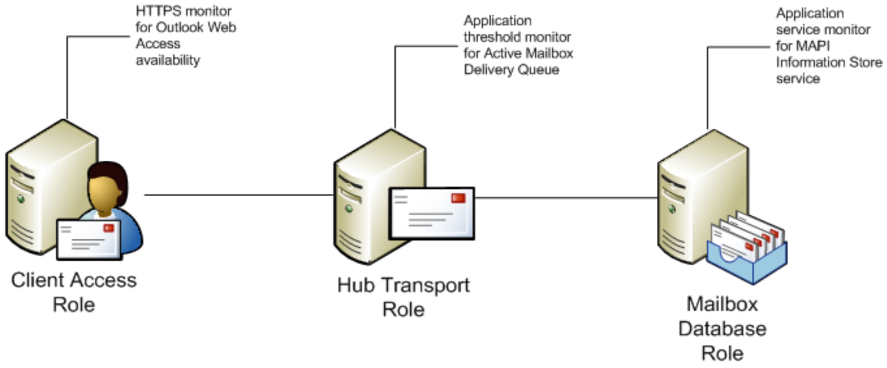

HTTPS monitor for Outlook Web Access availability
Application threshold monitor for Active Mailbox Delivery Queue
Application service monitor for MAPI Information Store service
Client Access Role
Hub Transport Role
Mailbox Database Role

Figure 2.5: Microsoft Exchange 2010 tiered monitoring.

When evaluating a network management solution, be sure to check for a solution that provides a good contrast of basic IP services monitors including FTP, HTTP, telnet, and SMTP as well as complex application monitors such as Microsoft Exchange or SQL Server. This richness in application monitoring features will give you the tools needed to closely monitor each application.

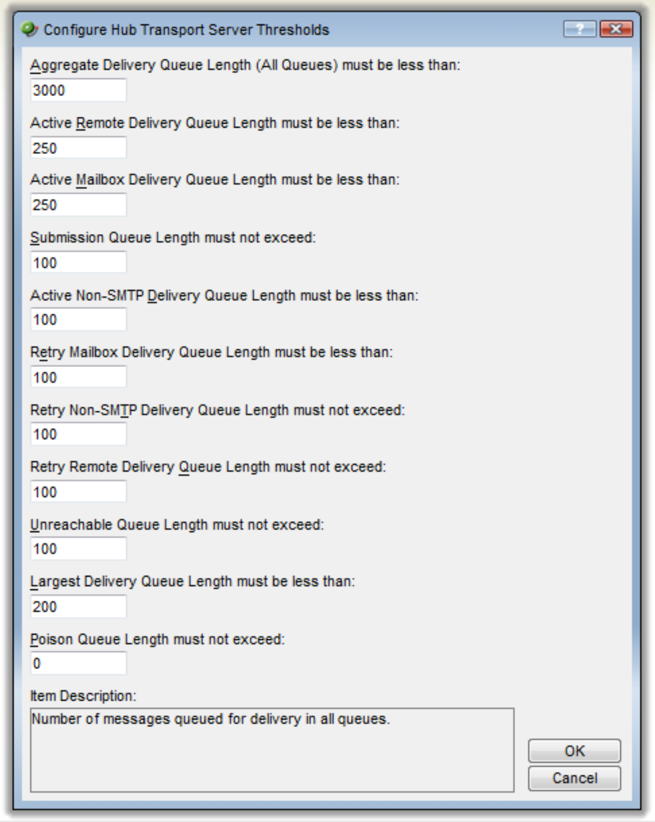
IP Services Monitors

IP service monitors play an important role in the ability to proactively monitor the network. To track and confirm access to important FTP sites across your business, utilize an FTP service monitor for upload, download, and deletion of test transactions.

You can also ensure critical Web sites are responding and correct content is returned by using HTTP monitors. Further validation of your businesses messaging system can be accomplished by implementing an SMTP monitor to test send and receive request.

Microsoft Exchange Monitors

Of all the applications running in your environment, the messaging system has the highest visibility to the user community. Beyond simple SMTP testing, application-specific monitors like MS Exchange can provide complete monitoring coverage of key messaging application roles and features. Exchange 2007 server roles such as Hub Transport Server, Client Access Server, and Mailbox Server each have unique monitoring requirements. The network management solution should address each of these roles and provide the ability to test mail flow, monitor delivery queues, and track performance.



Configure Hub Transport Server Thresholds

Aggregate Delivery Queue Length (All Queues) must be less than:
3000

Active Remote Delivery Queue Length must be less than:
250

Active Mailbox Delivery Queue Length must be less than:
250

Submission Queue Length must not exceed:
100

Active Non-SMTP Delivery Queue Length must be less than:
100

Retry Mailbox Delivery Queue Length must be less than:
100

Retry Non-SMTP Delivery Queue Length must not exceed:
100

Retry Remote Delivery Queue Length must not exceed:
100

Unreachable Queue Length must not exceed:
100

Largest Delivery Queue Length must be less than:
200

Poison Queue Length must not exceed:
0

Item Description:
Number of messages queued for delivery in all queues.

Figure 2.6: Rich Exchange Role-based threshold monitoring.

SQL Database Performance Monitors

Larger enterprise-level applications use a tiered application architecture. Many of these complex applications are making their way into the SMB network. These applications typically incorporate a multi-tier approach. The tiered approach to application architecture allows for better scalability and distribution of application workloads across more platforms. The tiered architecture is commonly made up of a number of Web-based tiers, application services tiers, and backend database tiers. The key component in a multi-tiered architecture is the database tier. SQL databases dominate the x86 server space and as such you will need a solution that provides monitoring capability deep within the SQL platform.

SQL database monitors give you the ability to configure SQL query monitors that can execute active queries against a SQL database using known record values to ensure database integrity and performance. Thus, you will be able to go beyond simply knowing the SQL service is running and ensure that critical application databases are accessible and returning valid data.

Synthetic Transactions

In the realm of application monitoring, there is key technology to look for in your network management solution: synthetic transactions. Synthetic transactions are actions, run in real time, that are performed on monitored objects. You can use synthetic transactions to measure the performance of a monitored object and to see how the object reacts when synthetic stress is placed on your monitoring settings.

For example, for a Web site, you can create a synthetic transaction that performs the actions of a customer connecting to the site and browsing through its pages. For databases, you can create transactions that connect to the database. You can then schedule these actions to occur at regular intervals to see how the database or Web site reacts and to see whether your monitoring settings also react as expected.

Application monitoring is all about ensuring you can achieve greater visibility into application performance and provide reliable access to your business applications. By using a combination of IP services monitors, vendor-specific monitors, and supported MIB files, you will be able to deliver higher service levels across all your applications.

Alerting

So far in this chapter, the discussion has focused heavily on the types of monitoring capabilities that a smart network management solution should provide. Although monitoring is very important, without a way to aggregate the flow of information into a usable tool that centralizes all notifications and alerts, the collected performance data or captured events are wasted.

The alerting component of the network management solution is there to provide you with that centralized tool—a tool that informs you of real-time failures and impending issues. The goal behind a well-designed alerting component is to provide you timely information in an easy-to-understand format on which you can take immediate action.

Remember, the word of the day is *proactive*. The purpose of spending all this time researching and implementing a network management solution is to change the way your SMB addresses network management—by giving your business the ability to move away from a reactive chaotic method of troubleshooting to a proactive method of intelligent management of the network. Alerts and notifications are the frontline of network management. To be proactive, you must have timely and accurate data with regard to the state of devices and systems on your network.

To start with, you need a solution that delivers all notifications, alerts, and alert acknowledgements into a single pane of glass. This means that with a quick glance, at a single screen, you have immediate feedback on the health of your network. Additionally, *flexible alerting* and *notification policies* are important when it comes to proactive management of the network.

Flexible Alerting

No two devices or systems are alike; thus, you need an alerting tool that offers a high amount of flexibility in the types of alerting options supported. The flexibility you should look for in a smart network management solution allows for alerting based on multiple metrics such as configurable thresholds, specific monitors, traffic flows, and configuration changes.

For example, you can configure a threshold alert for a critical point-of-sale Web server that is triggered based on a maximum CPU value over 80% for specified timeframe and a configurable traffic flow alert for increased HTTP traffic flow. This will give you the ability to build an intelligent alert that helps you proactively manage the performance of the point-of-sale Web server.

Notification Policies

The second component of proactive management relates to the notification framework within the network management solution. As a device or system alert is received by the alerting tool, you need an intelligent way of deciding the importance of that alert and what the response should be. Notification policies provide a framework that allows you to define the severity level of an alert, then create a workflow for notification of the alert to the correct individuals within your IT organization and ultimately resolution of the event(s) generating the alert.

The network administrators within your SMB are spread across multiple tasks each day. With a shortage of time, you may have elected to delegate the job of managing the response of network alerts to a tier-1 Help desk technician. Although this is fine for low-level systems or informational-type alerts, when it comes to a critical system or device failure, the alert requires a higher level of attention and response.

For these types of alerts, a notification policy should be created that includes multiple levels of escalation based on determined intervals. This setup will ensure the alert is getting the attention it demands and a small issue does not grow into major outage. Notification policies should also integrate with existing Help desk systems to allow for automatic ticket generation.

After an alert has been handled and the issue addressed, the notification policy can also include a process of updating the effected users, notifying them that the issue has been corrected as well as providing acknowledgement that the alert can be completed, halting further escalation. And notifications framework should support critical monitors that prevent alert storms from occurring by only alerting on critical monitors and not all downstream monitors.

Reporting

Some would say that the way to judge the power of a network management solution is by its reporting capabilities. Taken a step further, you could say that the success of a network management solution is dependent on the depth and quality of the reports and reporting options included.

Few businesses have the time to dedicate to collating and analyzing the vast amount of monitoring data captured by the network management solution. The reporting tool of a smart network management solution must include a broad set of built-in reports broken into usable categories. The reports themselves should also provide dynamic data with drill-down support and interactive metrics.

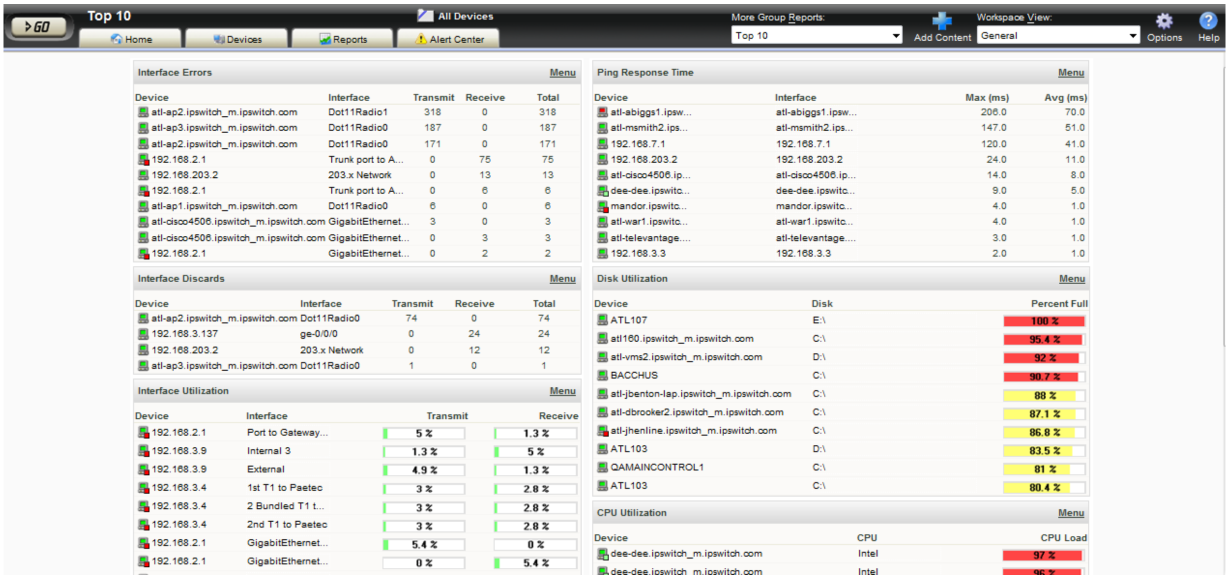
Think of the power of having a report that lists the memory utilization across each of your data center servers in an interactive bar chart. With a single click, you can see in real time the systems that are under a heavy load that may require immediate action to ensure performance levels remain high.

The same reporting tool can provide detailed trending data on that same set of data center servers. You can run historical reports spanning the past 6 months, enabling you to quickly know which systems are consistently overloaded and recognize potential targets for load balancing or clustering. Just as important, you will uncover those under-utilized systems that are taking up valuable rack space and heating and cooling costs; these systems become great targets for server consolidation through virtualization.

Top-10 Reports

This category of network monitor reporting will become invaluable to the business owner, CIO, or IT director within the SMB. Top-10 reports are a great way to quickly contrast your network systems and devices across a set of standard metrics. You can select a subset of similar servers in your environment and measure the utilization of key metrics—such as processor, memory, network, and disk utilization—across the selected set. This will give you insight into potential configuration issues, under- or over-utilization, and unbalanced application usage.

Top-10 reports are also great for gaining visibility into network bandwidth issues by observing the amount of data each user's workstation is transmitting or receiving. You will be able to see what system is monopolizing the bandwidth. When looking for a network management solution, make sure top-10 reports are high on your priority list. Figure 2.7 highlights an example of a top-10 report, showing the power of contrasting a set of metrics across multiple devices on the network.



Interface Errors

Device	Interface	Transmit	Receive	Total
atl-ap2.ipswitch_m.ipswitch.com	Dot11Radio1	318	0	318
atl-ap3.ipswitch_m.ipswitch.com	Dot11Radio0	187	0	187
atl-ap2.ipswitch_m.ipswitch.com	Dot11Radio0	171	0	171
192.168.2.1	Trunk port to A...	0	75	75
192.168.203.2	203.x Network	0	13	13
192.168.2.1	Trunk port to A...	0	6	6
atl-ap1.ipswitch_m.ipswitch.com	Dot11Radio0	6	0	6
atl-cisco4506.ipswitch_m.ipswitch.com	GigabitEthernet...	3	0	3
atl-cisco4506.ipswitch_m.ipswitch.com	GigabitEthernet...	0	3	3
192.168.2.1	GigabitEthernet...	0	2	2

Ping Response Time

Device	Interface	Max (ms)	Avg (ms)
atl-abiggs1.ipsw...	atl-abiggs1.ipsw...	206.0	70.0
atl-msmith2.ips...	atl-msmith2.ips...	147.0	51.0
192.168.7.1	192.168.7.1	120.0	41.0
192.168.203.2	192.168.203.2	24.0	11.0
atl-cisco4506.ip...	atl-cisco4506.ip...	14.0	8.0
dee-dee.ipswitc...	dee-dee.ipswitc...	9.0	5.0
mandor.ipswitc...	mandor.ipswitc...	4.0	1.0
atl-war1.ipswitc...	atl-war1.ipswitc...	4.0	1.0
atl-televantage....	atl-televantage....	3.0	1.0
192.168.3.3	192.168.3.3	2.0	1.0

Interface Discards

Device	Interface	Transmit	Receive	Total
atl-ap2.ipswitch_m.ipswitch.com	Dot11Radio0	74	0	74
192.168.3.137	ge-0/0/0	0	24	24
192.168.203.2	203.x Network	0	12	12
atl-ap3.ipswitch_m.ipswitch.com	Dot11Radio0	1	0	1

Disk Utilization

Device	Disk	Percent Full
ATL107	E:\	100 %
atl160.ipswitch_m.ipswitch.com	C:\	95.4 %
atl-vms2.ipswitch_m.ipswitch.com	D:\	92 %
BACCHUS	C:\	90.7 %
atl-jbenton-lap.ipswitch_m.ipswitch.com	C:\	88 %
atl-dbrooker2.ipswitch_m.ipswitch.com	C:\	87.1 %
atl-jhenline.ipswitch_m.ipswitch.com	C:\	86.8 %
ATL103	D:\	83.5 %
QAMAINCONTROL1	C:\	81 %
ATL103	C:\	80.4 %

Interface Utilization

Device	Interface	Transmit	Receive
192.168.2.1	Port to Gateway...	5 %	1.3 %
192.168.3.9	Internal 3	1.3 %	5 %
192.168.3.9	External	4.9 %	1.3 %
192.168.3.4	1st T1 to Paetec	3 %	2.8 %
192.168.3.4	2 Bundled T1 t...	3 %	2.8 %
192.168.3.4	2nd T1 to Paetec	3 %	2.8 %
192.168.2.1	GigabitEthernet...	5.4 %	0 %
192.168.2.1	GigabitEthernet...	0 %	5.4 %

CPU Utilization

Device	CPU	CPU Load
dee-dee.ipswitch_m.ipswitch.com	Intel	97 %
dee-dee.ipswitch_m.ipswitch.com	Intel	96 %

Figure 2.7: Top-10 reports quickly contrast network device metrics.

Report Subscriptions

It is getting tougher to justify additional spending because business owners are tightening the belt and reviewing every request for funding with more scrutiny. Many IT directors within SMBs have recently found themselves on the losing end of a budget debate. They did their due diligence and crossed all the Ts and dotted all the Is, yet the answer was no.

If only the business owner had seen the trending data across the messaging systems over the past months, she would have understood the need for additional memory and storage capacity or bandwidth. What about that virtualization project that is currently being proposed? Does the business owner have a historical understanding of the under-utilization being seen across many of the development and test lab servers?

With a network management solution that offers *report subscriptions* and *report exporting,* business owners will have access to key reports that highlight the trending data and performance data needed to make a more informed decision. With report subscriptions, the owner's email address can simply be added to a key report and an interval can be selected for when the report will run and be delivered. The next time a budget request occurs, the owner will already have knowledge of key monitoring and bandwidth utilization data, which provides additional leverage during negotiations. Using options like report subscriptions and report exporting, you can give non-technical users and management direct access to valuable data that can immediately effect business decisions.

Dynamic Workspaces

When it comes to reporting, SMB's administrators and IT staff have different ways they consume data. Some administrators prefer to have a narrow focus on a specific system with details on every metric under monitoring; others prefer to contrast a broad set of systems with a single metric.

This requirement changes as your priorities change for availability and performance. The network management solution should provide a reporting tool that offers a dynamic capability of selecting and grouping the various report displays. The idea is to have a dynamic workspace where each administrator can drag and drop selected report data to organize the report console in the way that makes sense to them. This gives each user a personalized view into the network management environment and allows them to focus on the report data that is relevant to their position and areas of responsibility. Once a specific workspace is created, the user can save the view and create additional workspaces that logically group related report data by business unit, applications, or device types.

Security Information and Event Monitoring

More businesses are coming under some type of industry-based compliance requirement; from PCI, HIPAA, or Sarbanes Oxley, many SMBs are having to align their security practices with the requirements of a given compliance standard. To meet the ever-rising demand on businesses for security compliance, there is a need to aggregate, display, and alert key security logs across all systems and devices on the network.

Security Information and Event Management (SIEM) automates the analysis process of security, network, and application logs. A SIEM solution provides the foundation for establishing processes for linking system access to individual users. According to most of today's regulations, tracking and reviewing access is a primary audit requirement, especially concerning access granted with administrative privileges. The current trend across many businesses implementing SIEM technologies is to leverage the log collection and log management features of the network management solution. Log management and SIEM-correlation technologies can work together to provide more comprehensive views to help your company satisfy regulatory compliance requirements.

When looking for a network management solution that supports SIEM technology, the following features are critical:

- Event archiving for automated collection, centralization, and secure storage of log data
- Event analysis for event examination, correlation, and comprehensive reporting for audit and compliance
- Event alarms for monitoring, alerting, and notification on key defined events
- Event crawling for on-the-fly forensics and log data mining

In addition to these advanced features, ensure the network management solution can capture and aggregate security logs from both Windows systems and Syslog supported devices.

In short, by integrating SIEM and log management, it is easy to see how a business can save by de-duplicating efforts and functionality. The functions of collecting, archiving, indexing, and correlating log data can be collapsed into a single solution, which will also lead to savings in the resources required for the maintenance of the tools.

Self Monitoring

Due to the importance of network management with regards to security, compliance, performance, and health monitoring, the network management system should be considered a highly critical component in the organization's infrastructure. A key monitoring feature in a smart network management solution is the ability for self monitoring. By incorporating key service monitors and alerts along with database-specific queries, the health and performance of the network management system can be monitored at the same level as any other critical component.

High availability is also very important; consider a solution that incorporates advanced database clustering and automated failover technologies.

Sophisticated Monitoring Changes the Game

In today's volatile economy, SMBs are looking for ways to cut costs and increase the value derived from the current technologies within the business. At the same time, more complex applications are being introduced that require advanced monitoring. As the business owner for an SMB, you are faced with a challenge: how do you provide a higher level of service to the business while operating under a constrained budget with less IT staff and more complex applications to manage?

A network management solution that incorporates a sophisticated framework of monitoring technologies can dramatically affect the operation of key systems and devices within your network. Sophisticated monitoring includes technologies that provide a proactive response to network issues. Instead of waiting for end users to report issues, your IT staff can proactively manage the performance and availability of every device and system on the network.

Sophisticated monitoring options allow you to gain immediate visibility into the status of every device and application. With advanced alerting and notification policies, no issue will go unnoticed. You will also be able to look at your network in a whole new light: with historical trending, you will be able to produce accurate capacity planning reports and detailed forecasting. With this information, as you plan your technology budget for the coming quarter or year, you will have accurate and detailed data with regard to the utilization, performance, and capacity of every system and device on your network.

Download Additional Books from Realtime Nexus!

Realtime Nexus—The Digital Library provides world-class expert resources that IT professionals depend on to learn about the newest technologies. If you found this book to be informative, we encourage you to download more of our industry-leading technology books and video guides at Realtime Nexus. Please visit http://nexus.realtimepublishers.com.