Realtime
publishers

The Shortcut Guide™ To

Smart Network Management for the SMB

sponsored by

IPSWITCH
WhatsUpGold
Network Management Software

Chris Hampton

Copyright Statement

Chapter 4: Four Must-Have Features for a Smart Network Management Solution

In a small to midsize business, you are faced with making tough decisions every day: how to control cost, how to increase revenue, and which technologies will really help your business. Technology is transforming the way business is conducted, and the technology trends faced by an SMB are numerous:

- Flexible workforce—Users are demanding remote access to network resources from anywhere, anytime
- Internet access—Fast and reliable access to the Internet is no longer a luxury; it is vital to any business model
- Virtualization—Virtualization of the server infrastructure and network appliances is spreading like wildfire across the data center
- Complex applications and systems—More complex multi-tiered systems are being introduced into the network requiring advanced performance monitoring and troubleshooting

Each of these technology trends presents a significant challenge to any SMB. How can your business make smart technology decisions that will be effective in meeting these challenges?

Core to each of these technology trends is the network, making this the logical place to start when evaluating technologies that can really have an impact on your business. Throughout this guide, there has been much discussion around the topic of network management. When you look across the breadth of network management, there are core functions that must exist in any solution: discovery, mapping, monitoring, alerting, and reporting to name a few. To address the previously presented challenges, the network management solution must extend beyond these core functions and provide truly intelligent features.

This final chapter will focus on four must-have features that take the network management solution beyond basic requirements and provide a truly smart network management solution:

- Real-time troubleshooting and analysis—Troubleshooting capabilities are at the heart of a smart network management solution. By leveraging the richness of the discovery, mapping, and monitoring data, real-time troubleshooting becomes a reality.
- System event log management—With the addition of each new system or device into the network comes a plethora of log data, application events, system events, error logs, and Syslog data. Without a way to intelligently manage the overwhelming amount of data generated by each system or device, the data becomes useless.
- Virtual infrastructure monitoring and management—Monitoring and managing a virtual infrastructure presents different challenges than does a physical environment. For example, virtualized systems typically do not support standard Simple Network Management Protocol (SNMP) mode of data collection and often the performance or monitoring data collected directly from a virtualized system is inaccurate due to the underlying hypervisor integration. What is needed is a virtualization-aware management solution that fully integrates with the virtual infrastructure.
- Network traffic monitoring and management—Consistent performance of the network is vital to any business and is even more important for an SMB because many aspects of an SMB's business model rely on the Internet. From key business-to-business partnerships to an ever-growing telecommuting workforce, network utilization and performance must be closely monitored and maintained.

Get Answers When You Need Them

When a business experiences a network outage, a device failure, application performance loss, or a sudden bandwidth constraint, the consequences can be costly. For an SMB, interruptions such as these can impact the business at a much faster pace. SMBs need a way to quickly detect the impending problem before it effects the business as well as to accurately troubleshoot the problem when it does occur.

Real-Time Troubleshooting—System and Device

As discussed in previous chapters, the use of proactive monitoring of all systems and devices ensures the network administrator is notified when a problem occurs on the network. Once a problem is identified, the network administrator must take immediate action to resolve the problem to minimize the impact on the business. A smart network management solution must provide a rich set of real-time troubleshooting and analysis tools to assist the network administrator.

By leveraging the richness of the discovery and mapping tools within a smart network management solution, troubleshooting system and device connectivity failures is greatly enhanced. Intelligent discovery of systems and devices at layer 2 and layer 3 of the network means the network management solution is fully aware of how each system and device is connected to the network and, more importantly, how each system and device is interconnected. Figure 4.1 highlights an example of a network topology map generated during the discovery process of a smart network management solution. With the ability to automatically enable active monitoring of each discovered system and device interface, the network management solution can provide proactive notification of any connectivity failure.

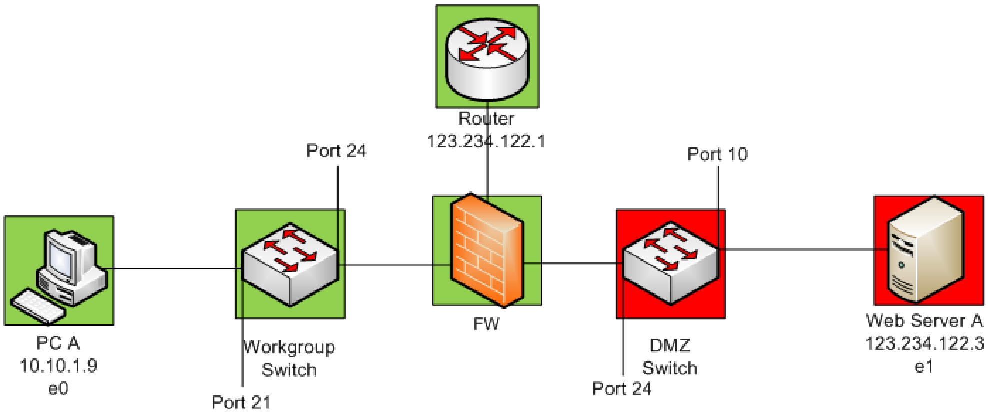


Figure 4.1: Network active monitor map.

The active monitoring in Figure 4.1 indicates a connectivity alarm for the DMZ switch and Web server A. At this point, more information is required to determine the actual cause of the connectivity failure. By drilling down into the active monitor map, the cause of the failure is quickly discovered when the layer 2 switch port data for the DMZ switch is reviewed.

Figure 4.2 indicates port 10 on the switch has failed, causing the connectivity alarms seen on the initial network monitor map. The power of using the topology maps in combination with the active monitoring data for real-time troubleshooting is evident.

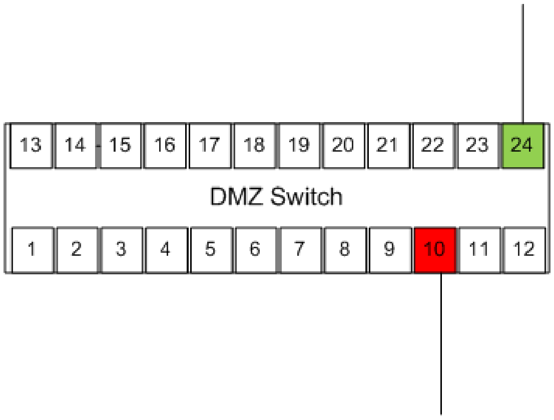


Figure 4.2: DMZ switch port monitor.

Layer 2 vs. Layer 3 Addressing

An IP address is a layer 3 (network layer) address. The MAC address is a layer 2 (data link) address. Layer 3 addresses are logical addresses that pertain to a single protocol (such as IP, IPX, or AppleTalk). Layer 2 addresses are physical addresses that pertain to the actual hardware interface (NIC) in the computer. A computer can have any number of layer 3 addresses, but it will only have one layer 2 address per LAN interface. At layer 3, the data is addressed to the host for which the data is destined. At layer 2, though, the data is addressed to the next hop.

Real-Time Troubleshooting—Applications

Although immediate response and resolution of connectivity issues is important, application access and performance is really the key to any business. Without reliable access to core point-of-sale Web applications, customers will quickly move onto competitors sites. If employees cannot access company resources when needed, critical business transactions are delayed. An SMB must have the ability to quickly detect and resolve any application failure or performance loss.

Smart network management solutions incorporate a number of features to assist with detection of application-related issues: IP services monitoring, Microsoft Exchange Monitoring, SQL Database Performance Monitoring, and Windows Process Monitoring, to name a few. These features were detailed in Chapter 2 and a short summary of the benefit of each feature with regard to application failure detection follows:

- IP services monitoring—Provides broad support for monitoring IP services and Web applications
- Microsoft Exchange monitoring—Allows for monitoring and tracking of Exchange 2007/2010 server roles including all related Exchange services
- SQL database performance monitoring—Provides real-time SQL-based queries against monitored databases and integrated SQL Server monitoring of key internal processes
- Windows process monitoring—Provides preconfigured and custom Windows Management Instrumentation (WMI) monitors for broad support of process monitoring

When it comes to troubleshooting application performance in real-time, a must-have feature is *synthetic transaction monitoring.* This feature was also introduced in Chapter 2 but is worthy of additional attention.

The idea behind synthetic transactions is to allow the network administrator to fully simulate a prospective Web transaction against a production Web server environment in real-time. This ability provides immediate feedback into the performance and status of critical Web server farms. In Figure 4.3, an example of a synthetic transaction is shown; a typical user transaction is completed by accessing the default home page, navigating to the Contact Us page, and completing data entry in a form for submission.

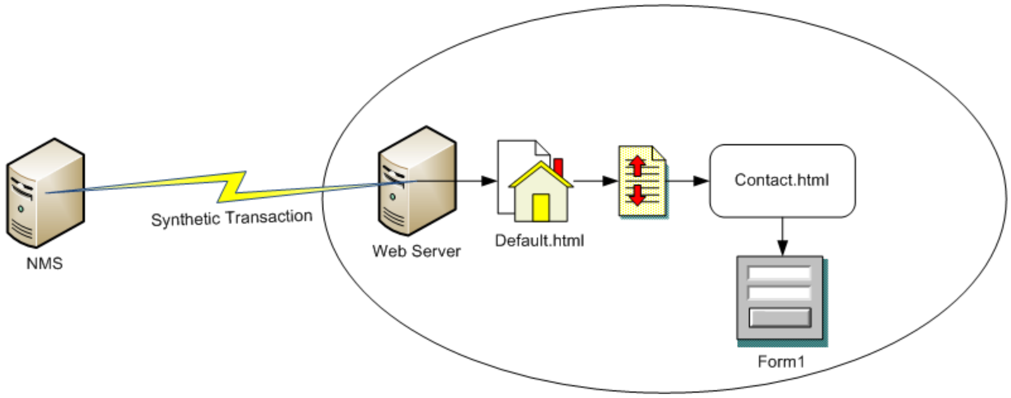


Figure 4.3: Synthetic transaction.

If a failure occurs along the prescribed transaction path, an alert monitor can be triggered providing notification of the failure. By utilizing real-time troubleshooting features such as layer 3 protocol addressing and layer 2 MAC or port-level addressing, network connectivity monitoring, and application-level synthetic transaction monitoring, an SMB can achieve a higher level of network performance and readiness.

Finally realize the value of log data

As your network environment grows with the addition of new devices, systems, and applications, so does the amount of log data. Each device, system, or application generates a large amount of logging and event data. In a typical network environment, this data is decentralized and resides on each individual device or system—making it very difficult to realize the value of the data.

Who has time to visit each device or system and open every log file? Not many administrators make this task a top priority and most often only review log files after an outage or failure has occurred. Even if this was a top priority, the vast amount of log data generated in a typical environment makes the task of analyzing the data virtually impossible. For example, in a large SMB with 20 Microsoft Windows servers (assuming three log file types per server) multiplied by the amount of log data generated over a 24 hour period by each server, times the number of total log files, the amount of data to review for a single day can be overwhelming.

The process of manually reviewing log data may be overwhelming, but there is enormous value in gaining visibility of log data across the entire network. Windows event log files and device Syslog information files hold very valuable information. Complete historical records for each system and device can be constructed from these log files and used during forensic analysis after a major outage or failure. More importantly, these log files can provide critical proactive information to help avoid a major outage.

For example, within a Microsoft Exchange 2010 environment, the Client Access Server (CAS) role utilizes the Autodiscover service to provide Microsoft Outlook 2007 with configuration information that's needed to connect to Exchange. If this service were unavailable, users' Outlook clients would fail to connect to Exchange. By proactively monitoring the Windows Application event log for any *MSExchange Availability* related events, the administrator will be made aware of a potential failure of this important service.

System Event Log Management

The previous example highlights the importance of proactive event log management and real-time monitoring. Being able to monitor event logs gives an administrator a substantial advantage in identifying failures early on—rather than investigating them after the fact. The presence of a well-planned event log monitoring strategy is the cornerstone to a proactive network management plan.

To establish an event log monitoring strategy, the current problem inherent with traditional event logging must be addressed—most notably, the decentralization of the log file data. By centralizing the collection of log files from each server and device within the network management solution, the first hurdle in log file management is overcome. Centralizing all log file data in a secure database within the network management solution ensures visibility across all logging data for every Windows system on the network.

Collecting Log Files

To accomplish the centralization of log data, the network management solution must have support for the collection of multiple types of Windows event log data.

> **Log File Types**
>
> When looking for a log management solution, ensure the solution has visibility and collection capabilities into the following types of log data: system, security, administrative, operational, and application logs across both EVT formatted logs (Windows NT, 2003, XP) and EVTX formatted logs (Windows Vista, Windows 7, Windows 2008) for Microsoft Windows servers.

A manual solution for the collection of log data across multiple Windows servers is difficult to achieve using manual scripting, and the storage options do not scale very well, making the task of centralization of log data difficult. Additionally, the very nature of manual script creation and management is proprietary to the specific administrator, and when the SMB experiences turn over, often the knowledge of administrating the manual scripts is lost.

What is needed is a more consistent and reliable method of collection—look for a solution that provides the following capabilities:

- Automated collection and storage of Windows event log data—Enables the scheduling, collection, and centralized storage of Windows event log data; also provides the ability to leave and active copy of the log data on the source server
- Flexible remote and agent-based collection of Windows event log data—Provides collection of Windows event log data from both local LAN-based and remote WAN-based systems. Also provides support for agent-based architectures within restricted security environments
- Automatic database maintenance—Automates the process of managing quickly-growing Windows event log data collection utilizing built-in database maintenance capabilities to archive files and purge data

Syslog data residing on Linux, Unix, and network devices such as routers is equally important in the overall log management solution. The centralization of Syslog data relates to the ability to centrally analyze and monitor the data along with Windows event log data but does not pertain to the collection of Syslog data in a centralized database.

> **What Is Syslog Data?**
>
> Syslog is a client-server protocol with an associated logging application used to transmit a small text message to a Syslog receiver or server. These messages may be sent via the User Datagram Protocol (UDP) or the Transmission Control Protocol (TCP).

Analyzing Log Files

The second hurdle to overcome with regards to log file management is the centralization of log data analysis. As mentioned earlier, system and device log file data holds a wealth of information that is crucial to the proactive management of the network. Once the Windows log file data has been collected and normalized, you need a tool that allows filtering, correlation, and reporting on log data across all Windows systems and Syslog information devices.

The normalization of Windows event log data refers to the process of providing consistent field-level data representation in the generated event logs between Windows EVT and EVTX formatted files. An example of this type of normalization can be seen when comparing Windows 7 Security event log entries with Windows XP. The Windows 7 security log does not provide information about the user performing the action or affected by the action in the User field, as was the case with Windows XP. Instead, the information is placed in the Description field of the event. The technology used for the normalization of Windows event log data adds the ability to place the most relevant user information back into the User field as the logs are processed. This helps to maintain consistency across all log data for quicker analysis.

The log management solution should provide the ability to easily filter through the vast amounts of log file data for specific logs and then provide the ability to view and further filter at the specific event level. Some of the key features to look for in a log file management solution with regard to analysis are:

- Event log correlation and analysis—Provides a powerful 'windowing' technology that gives network administrators the ability to correlate different cross sections of event log records from multiple sources; also allows administrators to quickly jump to specific dates, event IDs, and source types
- Prepackaged and custom event log reporting—Allows network administrators to quickly produce HTML or CSV formatted reports based on multiple types of event log entries—providing immediate feedback to the business on network issues and security compliance.

Real-Time Monitoring of Log Files

The final hurdle is the ability to provide real-time visibility of Windows event log and Syslog file entries across the entire network. The real power in a centralized log file management solution lies in its ability to provide targeted monitoring of event log data across multiple Windows systems or network devices using a single alarm setting. Think back to our example regarding Microsoft Exchange 2010 CAS; in a larger Exchange environment that spans multiple locations, an SMB will have an Exchange 2010 CAS installed at each location in-line with the Active Directory (AD) site architecture. To proactively monitor the Exchange 2010 Autodiscover Service, an alarm must be created to monitor each server's Application event log for MSExchange Availability event entries.

In an environment that does not have a centralized log management solution, the network administrator would have to visit each Exchange 2010 CAS manually and review the Application event logs on a regular basis to determine the health of the Autodiscover service. Utilizing the real-time monitoring capabilities of a centralized log file management solution, the network administrator can create a single alarm that polls every Exchange 2010 CAS on a regular basis for a Warning or Error event entry with the Source type of *MSExchange Availability* (see Figure 4.4). In this example, three Exchange 2010 CAS are monitored for an MSExchange Availability warning or error event entry. The CAS at AD Site 1 has logged an Event Error with the Event ID of 4002, matching the alarm source type set on the network management system.

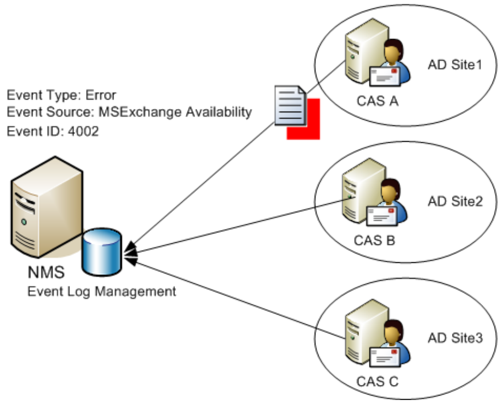


Figure 4.4: Exchange 2010 CAS event log monitoring.

The log file management solution must provide for the real-time automation of log file monitoring across Windows event logs and Syslog files with key capabilities in the following areas:

- Broad range of event notification types—Including options for email alerts, network popups, pager calls, Syslog server forwarding, database insertion, and broadcast notifications to administrators
- Combined Windows event and Syslog support—The ability to monitor standard Windows event logs for application, security, system, and Syslog files generated by network devices, Unix, and Linux systems
- Dual mode support for remote and agent-based monitoring—Provides the flexibility to monitor remote systems and devices without the requirement for agent-based installs; when necessary, due to security compliance restrictions, allow for full agent-based monitoring of remote systems and devices.

When evaluating a network management solution, consideration of an event log management feature must be high on the list.

Server Virtualization Creates a New Problem

Virtualization is sweeping across data centers. SMBs are seeing the value in making the move to server virtualization for the reduction in hardware cost and maintenance. Although server virtualization and consolidation make perfect sense for most SMBs, there are common pitfalls related to network management and server virtualization.

Some of the common difficulties experienced by SMBs that attempt to utilize legacy network management software include hardware inventories that do not accurately reflect the environment, server performance monitoring data that is skewed, automated alerting and remediate tasks that fail or cause virtual infrastructure host issues, no reporting of virtual machine placement within the virtual infrastructure, and lack of visibility into virtual infrastructure host performance. This list highlights just a few of the problems legacy network management software encounters due to its lack of virtualization awareness.

One good example of the difficulties encountered by SMBs when attempting to utilize traditional methods of network monitoring and management of a virtualized server environment is the shortcomings of SNMP monitoring as it relates to virtual machines. SNMP was originally designed to manage hardware devices with a well-defined MIB structure and definitive resource capacities. In a virtualized infrastructure, capacities are elastic (they can be made to grow or shrink dynamically) and full virtual machines can be started/stopped or migrated from one hardware to another while maintaining their system state. In this dynamic environment, the rigid MIB and OID structure of SNMP is not suitable.

Virtual Infrastructure Monitoring and Management

To overcome these issues, an SMB needs to ensure the network management solution incorporates a fully integrated virtual server monitoring and management feature. By providing a virtualization-aware solution, the network management environment gains visibility at the hypervisor level of the virtual infrastructure. This is critical for accurate awareness of the virtualized servers and associated applications.

> **What Is a Hypervisor?**
>
> A hypervisor, also called virtual machine monitor (VMM), allows multiple operating systems (OSs) to run concurrently on a single host computer—a feature called hardware virtualization. The hypervisor presents the guest OSs with a virtual platform and monitors the execution of the guest OSs. In that way, multiple OSs, including multiple instances of the same OS, can share hardware resources.

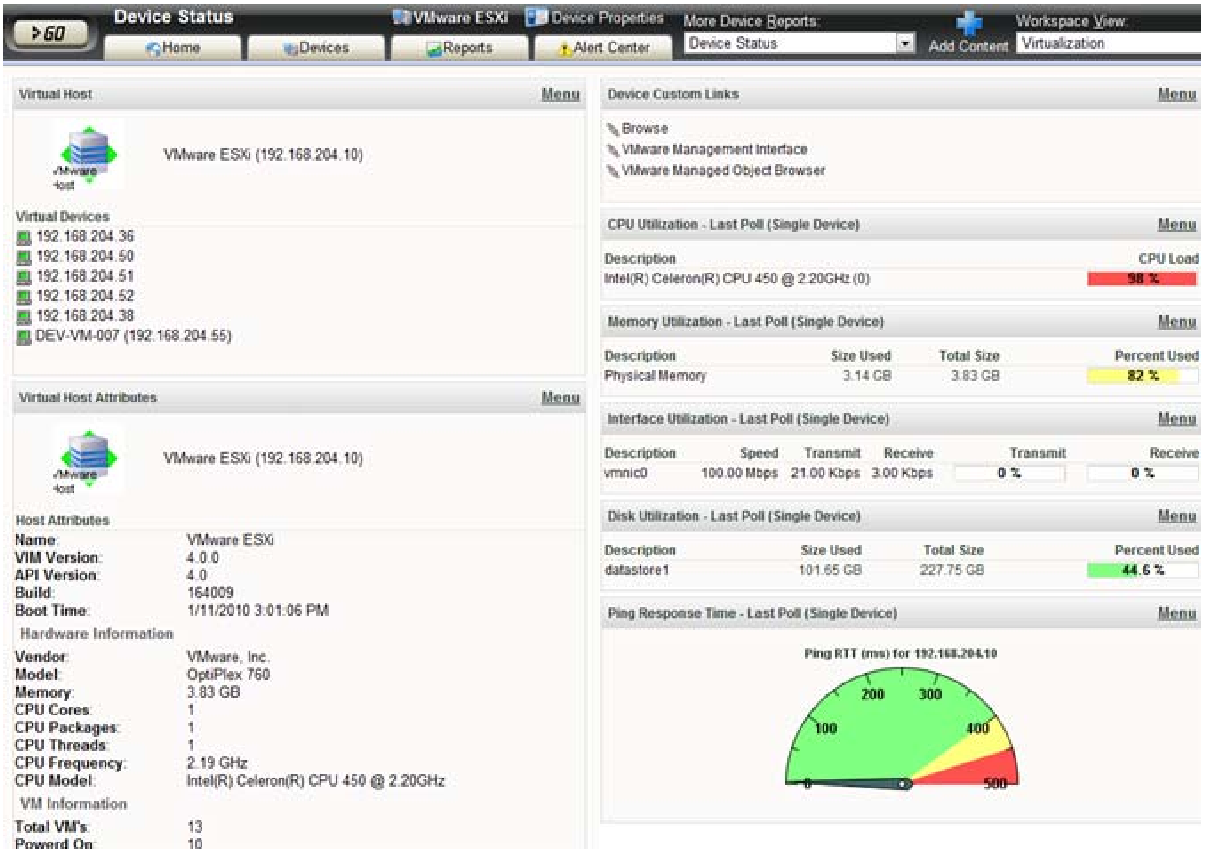
By integrating the monitoring and management of the virtual infrastructure into the network management solution, the SMB can utilize a single solution to discover, map, and monitor both physical and virtual server and network resources. One of the top vendors in the virtualization space is VMware Inc.; according to IDC's Q4 2009 reporting (IDC, 2010), VMware's ESX and ESXi hypervisors continue to hold the number one position across virtualization platforms. Because of the large market share, it is very important that the network management solution fully supports integration with VMware's hypervisors.

VMware with the release of vSphere and the associated ESX 4 and ESXi 4 hypervisors has moved to a new open Application Programming Interface (API) architecture. This new Web service, running on vSphere server systems, provides direct access to the ESX management components. The management components can be used to manage, monitor, and control virtual machine operations and other virtual infrastructure components (data stores, networks and, appliances).

A smart network management solution should make full use of the API architecture within vSphere and should provide a rich set of tools for virtual machine management and monitoring. The advantages of a network management solution that integrates at this level are many:

- Discovery and mapping—Automatically discover and map VMware ESX and ESXi hosts and their associated guest systems
- Resource utilization—Collect accurate utilization and resource consumption metrics from the virtual infrastructure
- Real-time alerting—Receive real-time alerts when utilization on host systems or virtual machines reach established thresholds
- Management integration—Utilize VMware tools to actively manage virtual machines on demand or on a scheduled basis
- Centralized management—Manage the entire data center infrastructure including; hosts, virtual machines, virtual appliances and, applications all from a single console

Figure 4.5 details the visibility a smart network management solution can provide when supporting direct integration with the hypervisor's API architecture. This figure presents the performance visibility into a VMware ESXi environment provided by the network management system.



More Device Reports: Device Status

Workspace View: Virtualization

Virtual Host

VMware ESXi (192.168.204.10)

Virtual Devices

192.168.204.36
192.168.204.50
192.168.204.51
192.168.204.52
192.168.204.38
DEV-VM-007 (192.168.204.55)

Virtual Host Attributes

VMware ESXi (192.168.204.10)

Host Attributes

Name:	VMware ESXi
VIM Version:	4.0.0
API Version:	4.0
Build:	164009
Boot Time:	1/11/2010 3:01:06 PM
Hardware Information	
Vendor:	VMware, Inc.
Model:	OptiPlex 760
Memory:	3.83 GB
CPU Cores:	1
CPU Packages:	1
CPU Threads:	1
CPU Frequency:	2.19 GHz
CPU Model:	Intel(R) Celeron(R) CPU 450 @ 2.20GHz
VM Information	
Total VM's:	13
Powerd On:	10

Device Custom Links

Browse
VMware Management Interface
VMware Managed Object Browser

CPU Utilization - Last Poll (Single Device)

Description	CPU Load
Intel(R) Celeron(R) CPU 450 @ 2.20GHz (0)	98 %

Memory Utilization - Last Poll (Single Device)

Description	Size Used	Total Size	Percent Used
Physical Memory	3.14 GB	3.83 GB	82 %

Interface Utilization - Last Poll (Single Device)

Description	Speed	Transmit	Receive	Transmit	Receive
vmnic0	100.00 Mbps	21.00 Kbps	3.00 Kbps	0 %	0 %

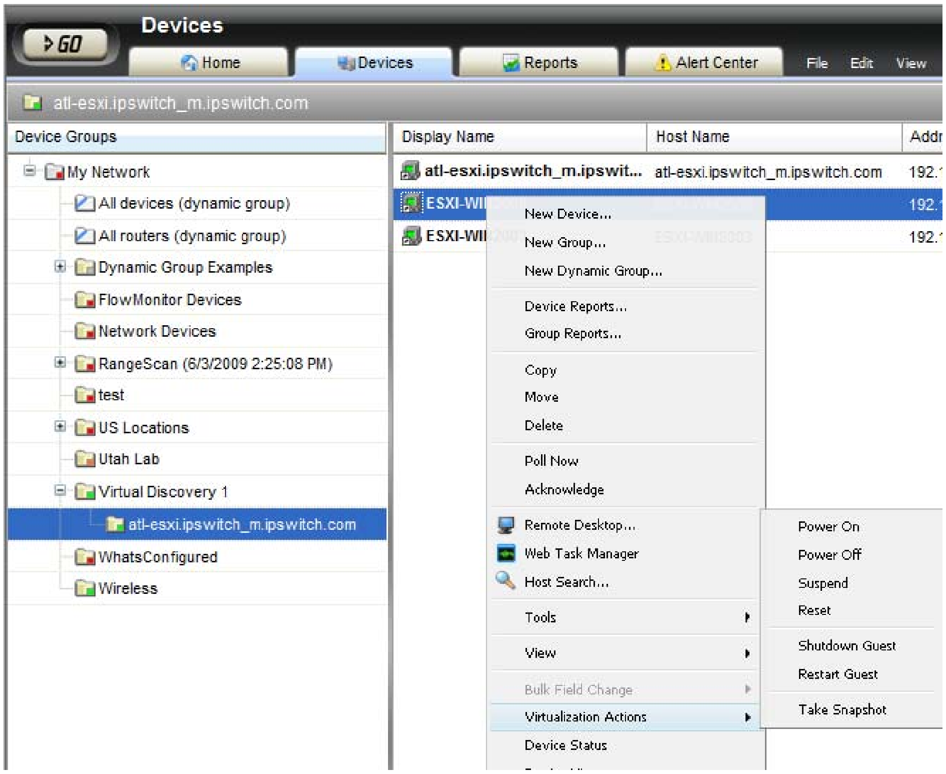
Disk Utilization - Last Poll (Single Device)

Description	Size Used	Total Size	Percent Used
datastore1	101.65 GB	227.75 GB	44.6 %

Ping Response Time - Last Poll (Single Device)

Figure 4.5: Manage virtualized servers' performance.

Figure 4.6 highlights the type of powerful integration and control a network management solution can provide when able to utilize the VMware API architecture. This image shows the virtual machine management options accessible from within the network management console. This ability allows the network administrators to work within a single pane of glass for all server management (physical and virtual).



Display Name	Host Name	Addr
atl-esxi.ipswitch_m.ipswit...	atl-esxi.ipswitch_m.ipswitch.com	192.1
ESXI-WI		192.1
ESXI-WI		192.1

Figure 4.6: Virtual machine management.

Equally important in today's virtualization landscape is the ability to support multiple vendors' hypervisor products. Referencing the same IDC report from Q4 2009, Microsoft's Hyper-V and Citrix's XenServer platforms are also showing impressive growth: 200% and 300%, respectively, year-over-year. When evaluating a network management solution, planning for the management and monitoring of a multi-vendor virtual infrastructure makes sense.

The Network Is Always Open

Much like the corner convenience store in your local neighborhood, the network within your SMB is always expected to be available and ready for business. With current trends towards telecommuting and a geographically dispersed workforce, your business resources must be accessible over the Internet 24 hours a day, 365 days a year. Combine this requirement with the increasing dependence on high-speed access to the Internet from within your business for access to critical business-to-business partner Web sites, and the need to closely monitor and manage your SMB's network utilization and bandwidth is apparent.

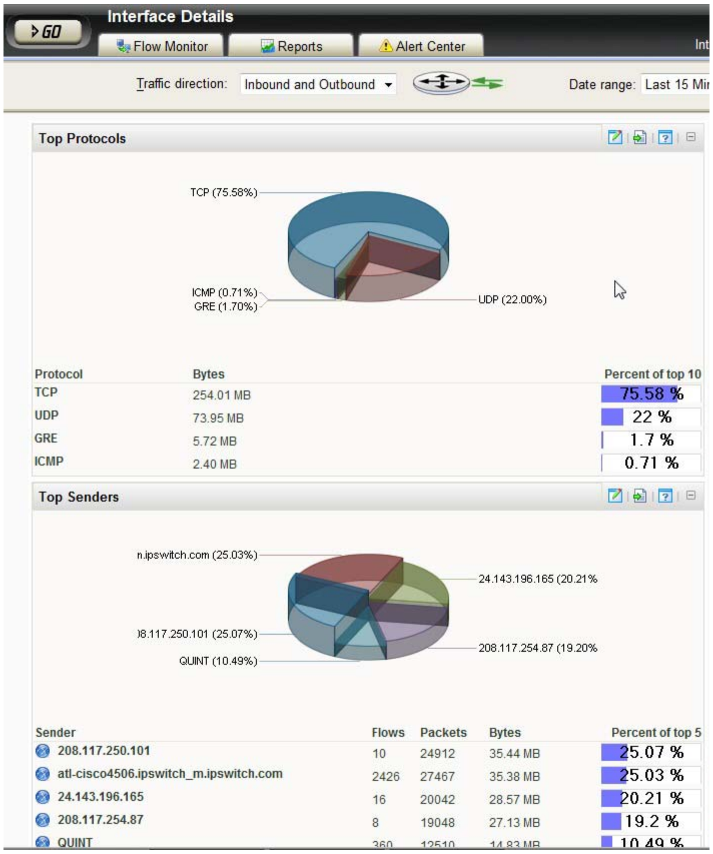
When evaluating a network management solution, a must-have feature that provides the ability to gain insight into the utilization and performance of network bandwidth is *network traffic monitoring and management*.

Network Traffic Monitoring and Management

The key technology underlying a network traffic monitoring solution is flow-level visibility. In a packet switching network such as TCP /IP, network traffic is comprised of a sequence of packets traveling from a source to a destination. This sequence of packets is termed network flow. Network traffic monitoring tools allow for the gathering, analyzing, and reporting of the network flow data or IP packets passing from the source to the destination.

The power of this feature is the ability to analyze and report on network traffic patterns and bandwidth utilization in real-time. With network flow monitoring, the network administrator can quickly determine overall utilization for the LAN or WAN and specific devices or interfaces. Network flow monitoring also indicates users, applications, and protocols that are consuming abnormal amounts of bandwidth.

In Figure 4.7, an example of a network flow monitor console is highlighted, providing visibility of inbound and outbound traffic across the edge router's external interface. By utilizing easy to understand top-based graphs, the network administrator can identify those protocols, applications, and users that are consuming bandwidth and causing performance issues.



Traffic direction: Inbound and Outbound

Date range: Last 15 Mi

Top Protocols

Protocol	Bytes	Percent of top 10
TCP	254.01 MB	75.58 %
UDP	73.95 MB	22 %
GRE	5.72 MB	1.7 %
ICMP	2.40 MB	0.71 %

Top Senders

Sender	Flows	Packets	Bytes	Percent of top 5
208.117.250.101	10	24912	35.44 MB	25.07 %
atl-cisco4506.ipswitch_m.ipswitch.com	2426	27467	35.38 MB	25.03 %
24.143.196.165	16	20042	28.57 MB	20.21 %
208.117.254.87	8	19048	27.13 MB	19.2 %
QUINT	360	12510	14.83 MB	10.49 %

Figure 4.7: Network flow monitor.

To accomplish the level of visibility required into the network, the network flow monitoring solution must support a wide variety of flow protocols including NetFlow, sFlow, and J-Flow. The flow monitor works by collecting and summarizing data that is carried over a device and then transmitting that summary to a centralized collector for storage and analysis.

> **What Type of Flow Protocol Do I Need?**
>
> Flow protocols such as NetFlow and J-Flow track every packet as it travels across the monitored interface, while sFlow protocol uses a sampling algorithm where every *n*th packet is recorded. Which type should you use? For high security and compliance environments, NetFlow and J-Flow is where you need to be. If all you need is a way to determine who is hogging the network bandwidth, the sFlow protocol will suffice.

Some key use cases for a network flow monitoring and management solution are:

- Maintain required level of network capacity—Review network usage trends and determine when to increase the network capacity to maintain the required level of performance
- Identify network configuration issues—Recognize and correct configuration issues that are consuming network resources or introducing security vulnerabilities
- Target unwanted traffic—Identify traffic patterns that may indicate undesired network usage, such as peer-to-peer file-sharing applications
- Proactive bandwidth management—Troubleshoot and correct bandwidth spikes in network traffic before they become a major problem

Network management solutions incorporating network flow monitoring and management take management of the network to a new level.

These four must-have features greatly enhance a network management solution by providing capabilities that extend the basic requirements of a network management system. When evaluating a network management solution for your SMB, ensure these features are included and take the management of your network to a new level.

SMBs Need Smart Network Management

Over the past four chapters, a clear vision has been established of what is required by SMBs in today's economy with regard to network management. Gone are the days of simple peer-level networks that safely operate within the confines of a business' brick walls. Today SMBs, much like their corporate counterparts, are having to build and maintain very complex network environments including high-speed Internet, advanced routing, layer 2 and layer 3 switching, VLANS, multi-tiered applications, virtualization of servers and network appliances, and an ever demanding flexible workforce.

The monitoring and management of these complex networks requires a robust network management solution that can provide a rich set of features and tools to address the challenges inherent in a complex network. The blueprint for such a network management solution focuses on four key features: *complete visibility*, *sophisticated monitoring*, *integrated configuration and change management*, and *real-time troubleshooting, trending, and flow analysis*. Together these features form the foundation of what is called a smart network management solution.

Download Additional Books from Realtime Nexus!