Realtime
publishers

The Essentials Series: Solving Network Problems Before They Occur

How to Use WMI in Network Problem Resolution

by Greg Shields

Copyright Statement

How to Use WMI in Network Problem Resolution

I've found myself constantly amazed at the language barrier we experience in the world of IT. I'm not talking here about the barrier between the technologists and the non-technologists, the geek and non-geek. I'm speaking about the language barrier we've all experienced between an organization's "server" administrators and their "network" administrators.

You've probably been in the same situation as you've been called in to work together on a big problem. Your network team sits at one side of the conference table, while the server admins take over the other. Although some problem is preventing your users from getting their job done, the two opposing teams pull out domain-specific vocabulary the other doesn't understand in an effort to prove that the problem isn't their fault.

This circle-the-wagons approach to solving IT problems has been around as long as the problems themselves. When a major problem occurs in the environment, a common approach is to gather everyone that is potentially involved and focus them on today's firefight. Yet solving problems in this way is expensive in terms of people's time and in cost to your business. There's got to be a better way.

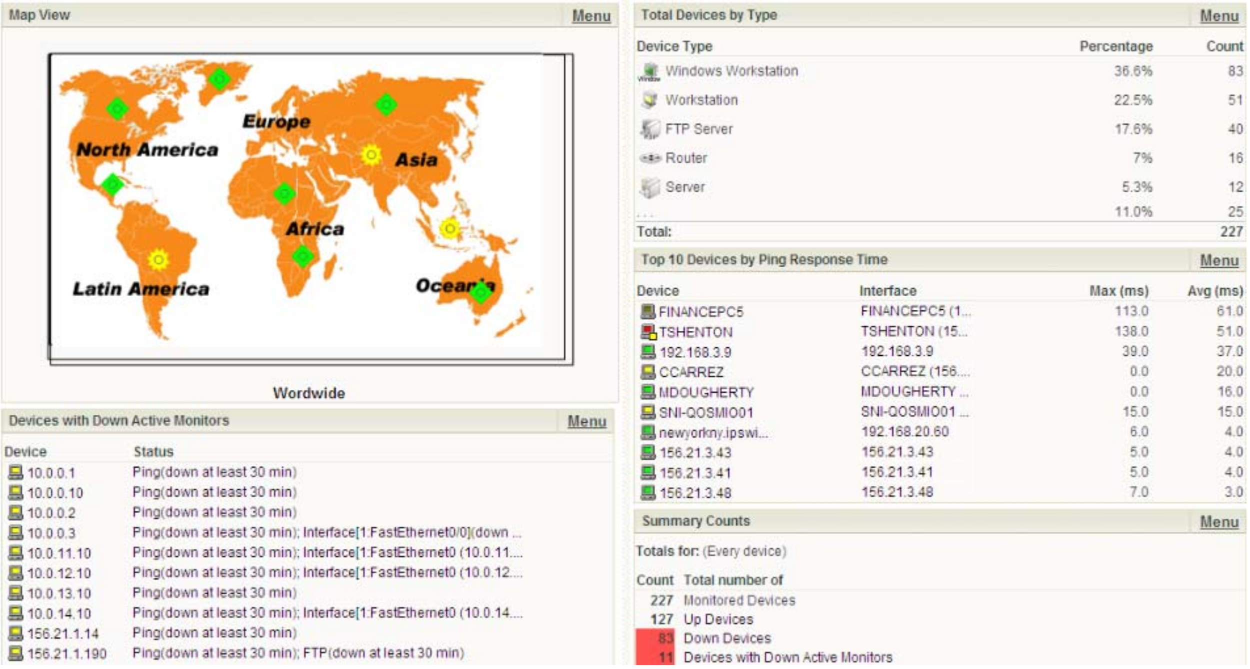
The Network Rosetta Stone

With the right Network Management Solution (NMS) solution in place, it is possible to improve your resolution of large-scale problems without the finger pointing. The right solutions leverage integration to servers and applications as well as network components to provide complete visibility into your operating environment. The result is that your NMS becomes a kind of Rosetta Stone or universal translation device between IT teams; the NMS helps the network team understand the impact of servers and applications, while giving systems administrators a perspective on the network infrastructure.

One way in which an NMS, acting as a Rosetta Stone, translates your Microsoft Windows computers is through Windows Management Instrumentation (WMI) integration. Microsoft's WMI is a platform-specific service that enables third-party devices to query the Microsoft OS for details about its behaviors. As a rough analogy, if you consider the Simple Network Management Protocol (SNMP) the request/response tool for network device monitoring, WMI performs the same actions within the Windows OS. A typical WMI query might look like this:

```
Select FreeSpace from Win32_LogicalDisk
```

In this query, the targeted machine is asked to provide the amount of free space on its installed volumes. This process looks different than SNMP's numerical Object Identifier (OID) approach, but the result is the same. An NMS queries for information across multiple Windows machines, storing the results into its local database and reporting them along its management consoles. Because multiple Windows machines can be queried by a central monitoring server, that server becomes the locus of analysis for behaviors across servers and network devices (see Figure 1). As a result, it becomes dramatically easier to locate or prevent network problems because their root cause can be tracked to very specific endpoints and behaviors.



Device Type	Percentage	Count
Windows Workstation	36.6%	83
Workstation	22.5%	51
FTP Server	17.6%	40
Router	7%	16
Server	5.3%	12
...	11.0%	25
Total:		227

Device	Interface	Max (ms)	Avg (ms)
FINANCEPC5	FINANCEPC5 (1...	113.0	61.0
TSHENTON	TSHENTON (15...	138.0	51.0
192.168.3.9	192.168.3.9	39.0	37.0
CCARREZ	CCARREZ (156....	0.0	20.0
MDOUGHERTY	MDOUGHERTY ...	0.0	16.0
SNI-QOSMIO01	SNI-QOSMIO01 ...	15.0	15.0
newyorkny.ipswi...	192.168.20.60	6.0	4.0
156.21.3.43	156.21.3.43	5.0	4.0
156.21.3.41	156.21.3.41	5.0	4.0
156.21.3.48	156.21.3.48	7.0	3.0

Device	Status
10.0.0.1	Ping(down at least 30 min)
10.0.0.10	Ping(down at least 30 min)
10.0.0.2	Ping(down at least 30 min)
10.0.0.3	Ping(down at least 30 min); Interface[1:FastEthernet0/0](down ...
10.0.11.10	Ping(down at least 30 min); Interface[1:FastEthernet0 (10.0.11....
10.0.12.10	Ping(down at least 30 min); Interface[1:FastEthernet0 (10.0.12....
10.0.13.10	Ping(down at least 30 min)
10.0.14.10	Ping(down at least 30 min); Interface[1:FastEthernet0 (10.0.14....
156.21.1.14	Ping(down at least 30 min)
156.21.1.190	Ping(down at least 30 min); FTP(down at least 30 min)

Totals for: (Every device)

Count	Total number of
227	Monitored Devices
127	Up Devices
83	Down Devices
11	Devices with Down Active Monitors

Figure 1: A unified dashboard that displays information about servers, applications, and network devices in one place.

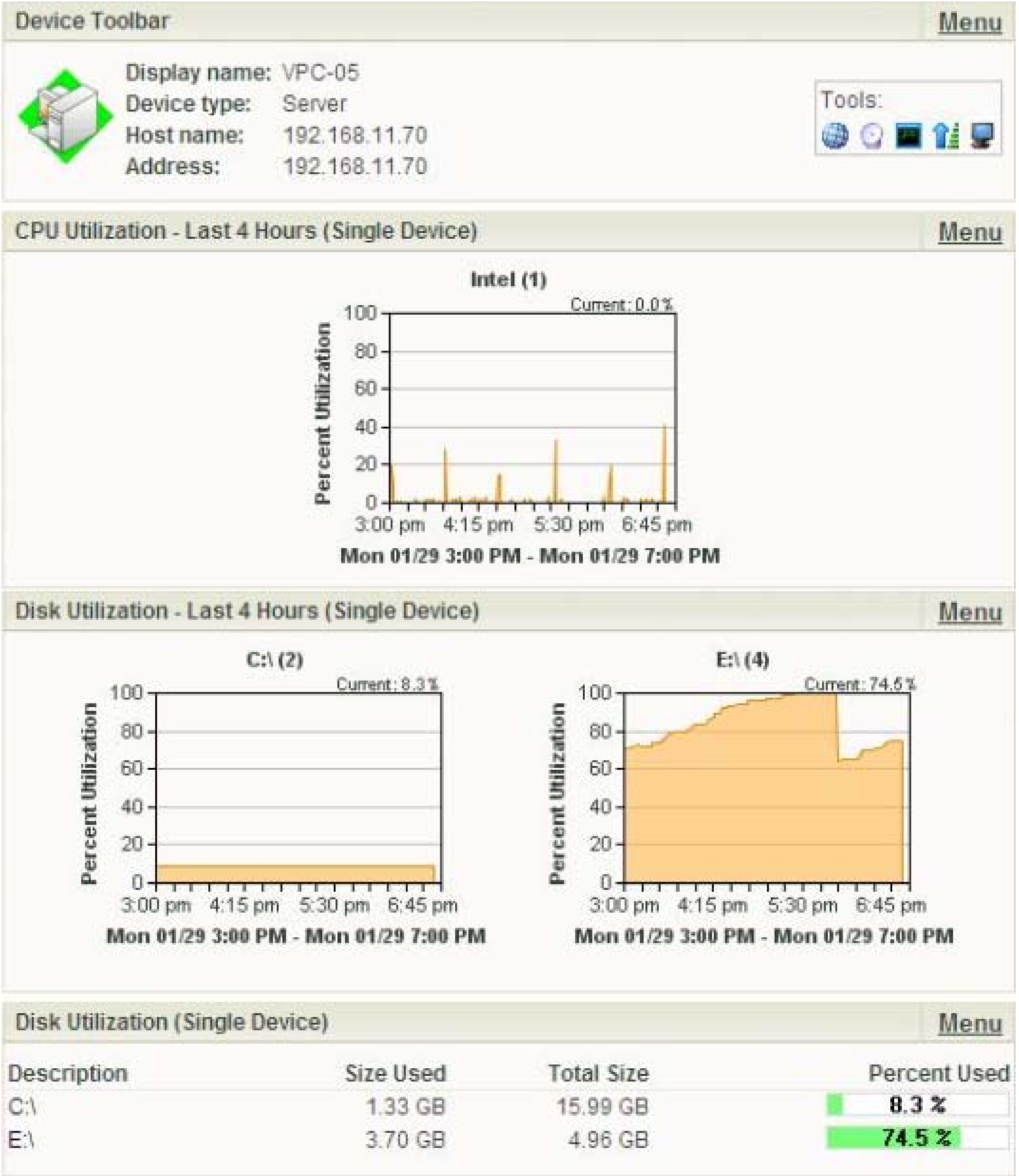
WMI, Finger-Pointer Preventer

It is the intersection of WMI and SNMP monitoring where an NMS provides great value. It also helps out with the historical problem of teams pointing fingers at each other. Consider another situation I experienced not long ago with one of my consulting clients. At this client, a particular Windows virtual machine was experiencing an intermittent problem with its network connection. That network problem would occur only irregularly; however, when it did occur, it impacted a large number of users. Thus, resolving this problem was extremely important for this client.

The client was very focused on the perceived network source for this problem, pointing their attention and resources to the network and its behaviors. "There must be something wrong with the network cards, their drivers, or their firmware," they would tell me.

Yet what they did not recognize was how virtualization tends to significantly increase the complexity of troubleshooting these types of problems. With multiple virtual machines co-located atop a single virtual host, a simple network problem's root cause can be something as seemingly-unrelated as a shortage of system memory or too much consumption of processor cycles.

To resolve the situation, a unified NMS was implemented that enabled the collection and reporting on metrics through SNMP and WMI statistics. This same solution integrated with the virtualization platform to provide additional data about its processing as well (see Figure 2). The solution to the problem was immediately discovered the very next time it occurred. WMI queries to the virtual host discovered that the virtual host's processor utilization experienced a dramatic spike in use at the very moment the networking problem occurred. The solution was to offload some of that virtual host's workload to other servers to prevent the resource-overuse situation.



Device Toolbar — Menu

Display name: VPC-05
Device type: Server
Host name: 192.168.11.70
Address: 192.168.11.70

Tools:

CPU Utilization - Last 4 Hours (Single Device) — Menu

Disk Utilization - Last 4 Hours (Single Device) — Menu

Disk Utilization (Single Device) — Menu

Description	Size Used	Total Size	Percent Used
C:\	1.33 GB	15.99 GB	8.3 %
E:\	3.70 GB	4.96 GB	74.5 %

Figure 2: A single view with SNMP, WMI, and even virtualization counters provides a holistic view of the entire environment.

WMI, Keeping Email Operational

Another averted crisis that may strike home in your own network environment has to do with keeping email servers up and running. Although most businesses can endure the loss of file servers for a day, or even a few databases for a few hours, the loss of the email system usually sends a business' executives into orbit.

That's why in organizations both large and small, the email system is often considered one of the most important services to remain up and operational. Email at the same time can be one of the most dynamic data processing systems in your data center. Handling thousands of messages a day in even the smallest of environments, email systems must effortlessly deal with large attachments, malware, and addressing failures while preserving the users' experience within their desktop email clients.

I was once called in to architect a monitoring solution for a company in the financial services industry. Although this client needed the monitoring solution for their entire multi-site infrastructure, the real reason for its implementation was due to regular and painful problems with the email server.

Implementing the right kind of tools for this small business of less than 100 employees was a trivial installation. Connecting it to network devices, identified servers, and even a few clients was not difficult because the system included preconfigured templates for each type of device. We completed the installation and initial configuration in less than a day.

The next morning, I returned to the client to find an extremely tired but extremely happy systems administrator sitting at his desk. It turns out that the majority of the problems with the email system were related to users overfilling it with data to the point where it would consume all its available disk space. That very night after the installation of this monitoring system, the administrator received an alert notifying him that the email server's disk drive was within a few percentage points of full consumption. Unlike in each of the previous incidents, this administrator was able to add the necessary disk space prior to the email server's database shutting down. The right level of monitoring across network, server, and even application facets of the IT environment prevented the problem from ever occurring.

WMI, Network Monitoring for Servers and Applications

As with the previous article in this series, these stories are told to explain why effective monitoring goes far in preventing problems. With the right monitoring that spans every part of an IT environment, you gain much-needed visibility into areas where you otherwise would have none. By integrating the network focus traditionally associated with SNMP with the server and application focus commonly used with WMI, that vision spans the entire environment. In the end, it may bring your network and server teams closer together as a cohesive unit for better managing your IT infrastructure.