

How Tivoli Manages Windows 2000 on Dell Systems

By Sabrena McBride

Tivoli Distributed Monitoring for Windows NT/Windows 2000 exploits the new features of Windows 2000 to ensure the availability and performance of mission-critical business applications running on Dell systems. This article explains how the Tivoli product can help users to meet the challenges of data analysis and operating system upgrades.

The cost of managing and supporting distributed computing environments is rising astronomically. For every dollar spent on technology, many more are spent on management costs. Moreover, as business-critical distributed applications continue to be deployed, the business risks associated with application downtime, inconsistent data, and poor reliability will become even more pronounced. With the rapid increase of business transactions taking place over the Internet, for example, it is not uncommon for companies to calculate and closely measure the costs of downtime for their e-business servers.

Windows-based servers are increasingly becoming the platform of choice for running mission-critical applications. Users and business processes depend on workstations and workgroup servers. Even applications that are based on midrange systems or mainframes may require components to run on Windows NT.

Servers running Windows NT are often the platform for firewalls, gateways, and other middleware applications. Any malfunction or degraded performance of these servers may have a direct effect on business operations. To ensure the availability of business resources, they must be intelligently and proactively managed to recognize problems before they affect end users. Ideally, problems would be diagnosed locally and

automatically corrected, thus reducing network traffic, shortening the time it would normally take to identify the problem, and freeing human resources to perform more important tasks.

The Challenge with Data Analysis

The challenge with today's management tools is making sense of the volume of raw data presented. It can be difficult to draw any conclusion about a single system or even a group of machines from the raw data provided by most monitoring tools. Possibly only a Windows NT expert could analyze such data to diagnose the real problem.

On the Microsoft platform, for example, everyone is familiar with Performance Monitor and Event Viewer. These tools are often useful, but they can sometimes be confusing. After looking at the Event Viewer and the data captured from the Performance Monitor for a perfectly working machine, an experienced administrator might need at least a few minutes to diagnose a *no problem* situation. This example illustrates the difference between providing data and information.

Today's Management Tools

A large percentage of the management tools available today provide administrators with data, not information. The

administrator must use the data and probe the troubled machine to establish the problem. For example, a Dell machine is running out of paging space. The majority of management tools would highlight three bottlenecks:

- Physical memory is 100 percent utilized.
- Logical disks have application queuing and are probably performing poorly.
- Excessive paging is occurring on all paging spaces.

To prevent system administrators from wasting time to relieve all three symptoms, the management tools would have to correlate this information to understand the real problem that must be resolved.

Tivoli's Built-in Intelligence

The need to solve such problems is not news to Tivoli, which has always had the intelligence to correlate, filter, and diagnose problem situations automatically using the powerful correlation features of Tivoli Enterprise Console™ (TEC). But the administrator has had to send the data across the network to the TEC server for intelligent diagnosis. If a correctable solution were discovered, the administrator would then trigger an action from the TEC server back to the troubled machine.

It would be more useful to diagnose the problem automatically on the local machine. If the best-practice correlation actually occurred on the machine that is experiencing problems, the upstream correlator could be dedicated to handling out-of-bound and enterprise correlations. Figure 1 shows an intuitive interface for correlating multiple indications to identify critical problems on a server running Windows NT.

In the example of paging space, the ideal solution is for one event to highlight both the paging problems and the root cause. As available memory declines, Windows systems

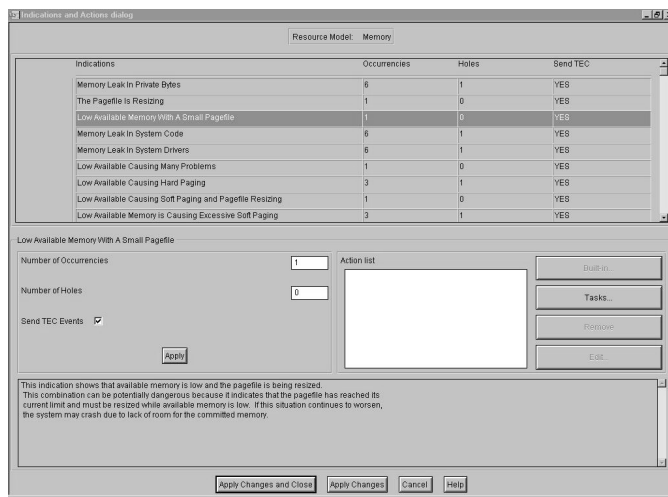


Figure 1. Autodiscovery and Correlation of Multiple Resource Indications

Windows-based servers are increasingly becoming the platform of choice for running mission-critical applications.

work hard at keeping the available memory above 4 MB. If memory falls below 4 MB, it is too low and the operating system (OS) spends more time keeping memory available than it does processing requests. High paging also begins to occur, and the pagefile will reach its maximum size.

Tivoli Distributed Monitoring for Windows NT/Windows 2000 associates *low available memory* indication with a small pagefile. This indication shows that available

memory is low and the pagefile is being resized. This combination is potentially dangerous because it indicates that the pagefile has reached its current limit and must be resized while available memory is low. If this situation continues to worsen, the system may crash because there is not enough space for the committed memory.

To determine the best way to handle problem situations, Tivoli performs analysis against various metrics and preset thresholds to determine the situation, whether or not to trigger an alert and when, and whether it can take an action to correct the problem. This ready-to-use, best-practice approach for setting threshold parameters is critical to managing a Dell system efficiently. If thresholds are too low, Tivoli would alert administrators to a problem when none really exists. If the thresholds are too high, the target machine might become inoperable before the administrators are notified to react to and solve a problem.

Figure 2 shows an intuitive interface that allows administrators to define frequency of occurrences of indications in a set time period to determine whether or not to trigger an alert or automatically define corrective actions in response to an alert.

The Challenge with OS Upgrades

Although it is becoming easier to install an OS, every fix or new release increases OS complexity with hundreds to thousands of lines of code changes. The count for lines of code in Windows 2000 is already in the millions.

The changes in the new OS are often incompatible with the software being used to manage the system because that software was purchased from a different vendor. The fixes required to support OS changes can take months to complete, and the delay can prevent users from upgrading their management tools in a timely fashion to handle OS changes.

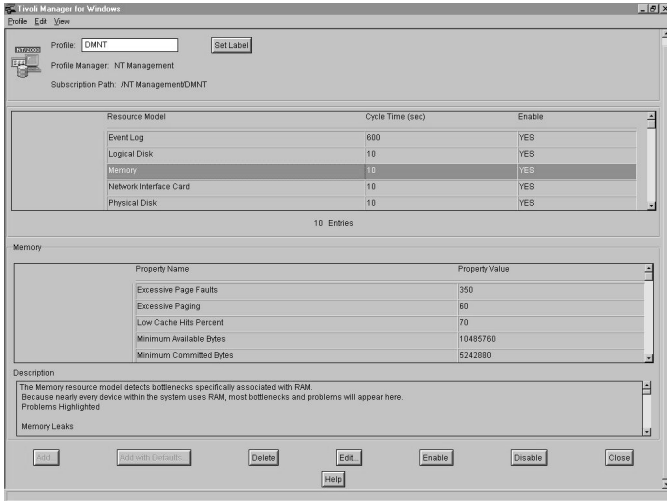


Figure 2. Intuitive Interface That Defines Responses and Automated Actions Based on the Severity of the Situation

Web-Based Enterprise Management and CIM

To make it easier to implement management functions and allow management tools to remain robust despite device or OS changes, the Distributed Management Task Force (DMTF) introduced Web-Based Enterprise Management (WBEM).

WBEM offers universal access to management information for the enterprise by providing a consistent view of the managed environment. WBEM encompasses a multitude of tasks ranging from simple workstation configurations to full-scale enterprise management across multiple platforms.

Central to this initiative is the Common Information Model (CIM), which provides a standard for obtaining hardware and software status information from servers, desktops, workstations, and portables. The basic idea is that the creator of any component, such as a new adapter card, supplies information relevant to managing the system in a well-defined, formal way, and adds the implementation of a certain functionality (such as power management or gathering of performance data) along with the device driver.

On the other end, systems management tools can query what is in the system and determine what properties and functions are supported. Because these tools can operate independently from the operating platform of the managed components, management functions can be easily implemented, and management tools that exploit the architecture can remain robust despite device or OS changes.

Management of Windows 2000

Microsoft Corporation has created the Windows Management Infrastructure (WMI) as the WBEM services implementation for Windows-based systems. As an early adopter of WMI, Tivoli exploits this implementation in Tivoli Distributed

Monitoring for Windows NT/Windows 2000 for optimal management of the Microsoft Windows platform. Tivoli's transparent management also insulates customers from OS changes that have conflicted with management tools in the past.

With the release of Windows 2000 and Dell's increasing support of CIM instrumentation, Dell customers will benefit from Tivoli's ability to obtain Dell hardware information instantly through the CIM instrumentation. Tivoli offers two products suitable for this purpose:

- **Tivoli Enterprise** is used by customers for managing over 3,000 *endpoints*, defined as a network, application, middleware, database, the Internet, hardware (server, desktop, workstation, or portable), or OS. Tivoli Enterprise consists of over 50 management applications running on a common framework.
- **Tivoli Distributed Monitoring for Windows NT/Windows 2000** is a Tivoli Enterprise application. It is pre-configured to address specific availability and performance problems that can arise in a Windows NT system. Its exploitation of WMI gives it the ability to manage the business rather than just the individual components. This solution models critical system paths inside Windows servers to evaluate the quality of an object against predefined service levels. Once a problem is diagnosed, it offers methods for automatically recovering from critical situations.

To maximize the availability and performance of Dell systems running Windows 2000, users must have the following:

- Tivoli Enterprise 3.6.1 or above; Tivoli Enterprise Console 3.6.1 is optional
- Tivoli Management Agent (TMA) installed on systems (servers, desktops, workstations, or portables) to be managed by Tivoli
- Tivoli Distributed Monitoring for Windows NT/Windows 2000 3.6.2 or above
- CIM-instrumented Dell systems

Management of Dell Systems Running Windows 2000

As a CIM-instrumented management application, Tivoli Distributed Monitoring for Windows NT/Windows 2000 sits on top of the WMI core and uses the WMI application programming interface (API) to access the relevant information. It acts as a consumer of the objects and properties provided by CIM. CIM objects represent the current state of the system. Each object contains a number of properties that reflect the status of the system in terms of its performance, throughput, and other metrics.

Tivoli adds value by compiling these objects into resource models with built-in decision-tree logic for processing relevant information. These resource definitions are formal descriptions of managed objects written as

managed object format (MOF) files, and they contain all the properties of the objects defined by Microsoft. Events that are sent to the central management site also are defined within CIM-compliant MOF files.

Local Correlation

Decision trees are a Tivoli-specific extension that is not part of the CIM specification or WMI. The decision tree contains the knowledge necessary to assess critical situations by retrieving information from the underlying resources and applying a number of rules to determine whether or not to trigger an indication.

Decision trees are provided in the form of DEC files. Each resource model has one DEC file. The decision tree implements what the resource model formally defines.

Decision trees are visited at regular intervals. That is, the engine behind the resource model collects the information from resources associated with the resource model and feeds it to the decision tree. Depending on the thresholds (resource model properties) and rules (decision trees) defined for the model, *indications* may be triggered.

An indication represents the occurrence of a possible system problem. Tivoli Distributed Monitoring for Windows NT introduces an additional layer to avoid overflowing the management system with notifications for short-time, out-of-bound events. Therefore, indications are generated and collected at the next level, the *event aggregator*, which collects indications on behalf of resources. As a result, a logical connection exists between resources and the event aggregator. Depending on the indication settings for Number of Occurrences and Number of Holes, the event aggregator will create and forward an *event* or it will dismiss indications in order to filter out-of-bound values. An event will only reach the TEC server when the problem persists for a certain period.

Enterprise Alerts

When an event is generated, it contains additional information about the system and the referred resource to provide meaningful information to the administrator. It is then forwarded to the Tivoli Enterprise Console for further processing and analysis using rules for correlation with other enterprise events, filtering or automated actions, or automatically opening trouble tickets in Tivoli Service Desk.

Figure 3 shows examples of resource models that ship with Tivoli Distributed Monitoring for Windows NT/Windows 2000. Each resource model contains the knowledge to correlate properties from different resource classes. This feature eliminates the need to send redundant alerts for each class defined by Microsoft.

Correlated events are generated from two or more indications originating in different resource models.

SELECTED RESOURCE MODELS SHIPPED WITH TIVOLI DISTRIBUTED MONITORING FOR WINDOWS NT/2000

Resource Model	Functionality
TMW_EventLogModel	Forwards some specific Windows NT System Log entries
TMW_LogicalDiskModel	Detects critical situations concerning disk use and low capacity
TMW_MemoryModel	Detects critical situations concerning memory use and low capacity
TMW_NetworkIntCardModel	Detects critical situations concerning device use of network adapters
TMW_PhysicalDiskModel	Detects critical situations concerning DASD device use
TMW_PrintModel	Detects critical situations concerning printing

Figure 3. Selected Resource Models Shipped with Tivoli Distributed Monitoring for Windows NT/Windows 2000

For example, Event(7):Busy Drive from High Paging (TMW_BusyDriveFromPaging) is triggered by correlating the following indications:

- TMW_HighLogicalPercentDiskTime (Logical Disk resource model)
- TMW_HighPaging (Memory resource model)

The Tivoli Solution

Tivoli Distributed Monitoring is a powerful tool that will save time and effort and increase efficiency in managing Dell systems running Windows 2000. This tool specializes in detecting resource problems and bottlenecks as quickly as possible as they appear on a system.

The exploitation of CIM and WMI enables Tivoli Systems and Dell Computer to decrease the maintenance and life-cycle costs associated with managing Windows systems, and thus reduces the total cost of ownership to our customers. ♦

Additional Resources

For additional information, please consult the Tivoli Redbook: *Implementing Tivoli Manager for Windows NT* (SG24-5519-00) or contact Kathy Makgill (kathy_makgill@tivoli.com).

Sabrina McBride (sabrena_mcbride@tivoli.com) is a product marketing manager for Tivoli Systems who focuses on managing availability solutions and Microsoft applications management initiatives. She has previously been a systems engineer specializing in availability and performance, a database administrator, a systems analyst, and an applications developer. Sabrina frequently represents Tivoli Enterprise Management solutions as a speaker at public forums.