



PROACTIVE MANAGEMENT
OF THE
MICROSOFT WINDOWS SERVER 2003 PLATFORM

CONTENTS

Introduction	1
Windows Server 2003	3
ELM Enterprise Manager 4.0	4
Real-time and Scheduled Monitoring	5
Rules-Based Management System	5
Rich Notification and Corrective Action	5
ELM Server Database and Reporting Engines	5
Full range of technologies integrated into a full-featured monitoring system	6
Scalability, Availability and Reliability	7
Secure by Design	8
Secure by Default	8
Resilient by Default	9
ELM Economy	10
Conclusion	11
Appendix	12

INTRODUCTION

Administrators continue to need a way to proactively manage their Windows Server infrastructure in real time without adding a lot of overhead to the system. Tools that are comprehensive but easy to use are a necessity in the well-run IT space.

ELM Enterprise Manager™ (EEM) from TNT Software is that tool. EEM is a multithreaded, COM-based client/server application specifically designed for minimal system overhead, minimal network impact and maximum visibility and monitoring. Using ELM Enterprise Manager, Windows Server administrators can proactively monitor their server event logs, send and receive alerts when specified events occur, collect and monitor health and performance data, and automatically take corrective action with run commands when problems arise.

Traditionally, the IT staff learns of system problems by:

- waiting for users, managers, or customers to report problems,
- trying to monitor all aspects of system performance manually or
- using a variety of tools to monitor the discrete parts of a system and then trying to coordinate the data,

ELM Enterprise Manager alerts administrators in real-time, automating the management of their Windows Server infrastructure.

Whether they use EEM in an out-of-the-box configuration or customize it for specific concerns, administrators rely on ELM Enterprise Manager to notify them of activity or problems using an array of methods, some of which are:

- Customizable beeps
- Multimedia sound files
- Network pop-up messages
- SMTP or MAPI email
- Instant messaging
- Posting to Web forms
- Alpha-numeric and numeric pagers
- SNMP traps
- User-written batch files
- Command files, or applications

New in EEM 4.0 is the innovative ELM Advisor, a desktop notification that displays an unobtrusive text balloon in the desktray. Now administrators can see notifications as they arrive, without workflow interruption. Opening ELM Advisor, a list of alerts is displayed. This list can be used as a checklist with the ability to mark each alert as “read”, helping administrators keep track of to-dos.

EEM supports SNMP, enabling interoperability with other enterprise management systems and syslog messaging for platform extension.

ELM Enterprise Manager:

- Monitors Windows Server event logs, processes, and services in real time,
- Collects and stores event log entries for analysis, auditing, alerting and compliance requirements,

- Collects and stores published performance counters, including published performance counters, for base lining, trending, and capacity planning,
- Creates reports of event and performance data,
- Sends and receives alert notifications when events occur, services fail, or performance exceeds thresholds,
- Automatically restarts failed services,
- Stops and starts services locally and remotely,
- Kills processes locally and remotely,
- Processes and forwards SNMP traps from network devices,
- Monitors non-Windows systems using syslog monitoring,
- And more...

ELM Enterprise Manager 4.0, ELM Log Manager 4.0, ELM Performance Manager 4.0, and ELM Event Log Monitor 4.0 - have earned the Windows Server 2003 certification from Microsoft Corporation through VeriTest, the testing division of Lionbridge. This certification is awarded to software applications meeting a rigorous technical standard that identifies software applications that are secure and manageable, and that run reliably on the Microsoft Windows family of operating systems.

”This certification through VeriTest provides TNT Software customers added confidence in their purchase of ELM Enterprise Manager 4.0, ELM Log Manager 4.0, ELM Performance Manager 4.0 or ELM Event Log Monitor 4.0,” said Steve Nemzer, IT, Global Development and Testing Solutions of Lionbridge. “Confirming that the product meets Microsoft’s stringent standards assures end-users that they can experience a higher level of reliability and a lower total cost of ownership than if they were to purchase a non-certified product.”

The full certification results earned by TNT Software’s ELM Solutions may be viewed at www.veritest.com.



WINDOWS SERVER 2003

Windows Server 2003 is designed to help customers do more with less. It builds on the strengths of the Windows 2000 Server family to take application and hardware performance to new levels of scalability and availability, while at the same time providing new opportunities for server consolidation. In December 2005, Standard, Enterprise, and Datacenter editions of Windows Server 2003 R2 were released, offering Active Directory, storage, and branch office enhancements for customers.

Windows Server 2003 offers:

- **Availability** - The Windows Server 2003 operating system provides improved availability through enhanced clustering support.
- **Scalability** - Windows Server 2003 scales from single processor solutions all the way up to 64-way systems. It supports both 32-bit and 64-bit processors.
- **Security** - Windows Server 2003 provides many important new security features and improvements including the common language runtime and Internet Information Services 6.0.

Windows Server 2003 comes in four editions:

- **Standard Edition.** The reliable network operating system that delivers business solutions quickly and easily—the ideal choice for small business, workgroup, departmental, and team use.
- **Enterprise Edition.** The platform of choice for applications, Web services, and infrastructure, delivering high-availability, increased reliability and performance, and a strong ROI.
- **Datacenter Edition.** The platform for business-critical and mission-critical applications that demand the highest levels of scalability and availability.
- **Web Edition.** The platform for Web serving and hosting.
 - Windows Storage Server 2003 is a dedicated file and print server providing dependable storage while integrating seamlessly with existing IT infrastructure. Microsoft has optimized this server to simplify file serving, backup, and data replication.

Those editions are provided in 10 architectures:

- 64 bit:
 - Windows Server 2003 R2 Standard x64 Edition
 - Windows Server 2003 R2 Enterprise x64 Edition
 - Windows Server 2003 Datacenter x64 Edition
 - Windows Server 2003 Enterprise Edition for Itanium-based Systems
 - Windows Server 2003 Datacenter Edition for Itanium-based Systems
- 32 bit:
 - Windows Server 2003 Web Edition
 - Windows Server 2003 Standard Edition
 - Windows Server 2003 R2 Standard Edition
 - Windows Server 2003 R2 Enterprise Edition
 - Windows Server 2003 R2, Datacenter Edition

ELM Enterprise Manager 4.0

TNT Software's ELM Enterprise Manager™ (EEM) is a comprehensive solution to monitor the health and status of distributed systems by combining the following core functions into a feature-packed, reliable, and scalable application:

- Real-Time and Scheduled Monitoring
- Rules-Based Management System
- Rich Notification and Corrective Action
- Data Collection, Archiving and Reporting

As illustrated in Figure 1, ELM Enterprise Manager provides real-time monitoring, event collection and consolidation, health and performance monitoring and data collection, service and process monitoring, log file monitoring, enhanced cluster monitoring, availability and quality of service monitoring for Microsoft Exchange Server, and query-based monitoring of Microsoft SQL Server. In addition, ELM Enterprise Manager includes enhanced monitoring of Internet Information Services, can receive SNMP Traps and Syslog messages, and can monitor IP-based services and applications such as HTTP, POP3, SMTP, and FTP.

ELM Enterprise Manager uses Microsoft's COM architecture, enabling administrators and developers to extend ELM using any COM-supported language (e.g., VBScript, Visual Basic, Visual C++, C#, and others).

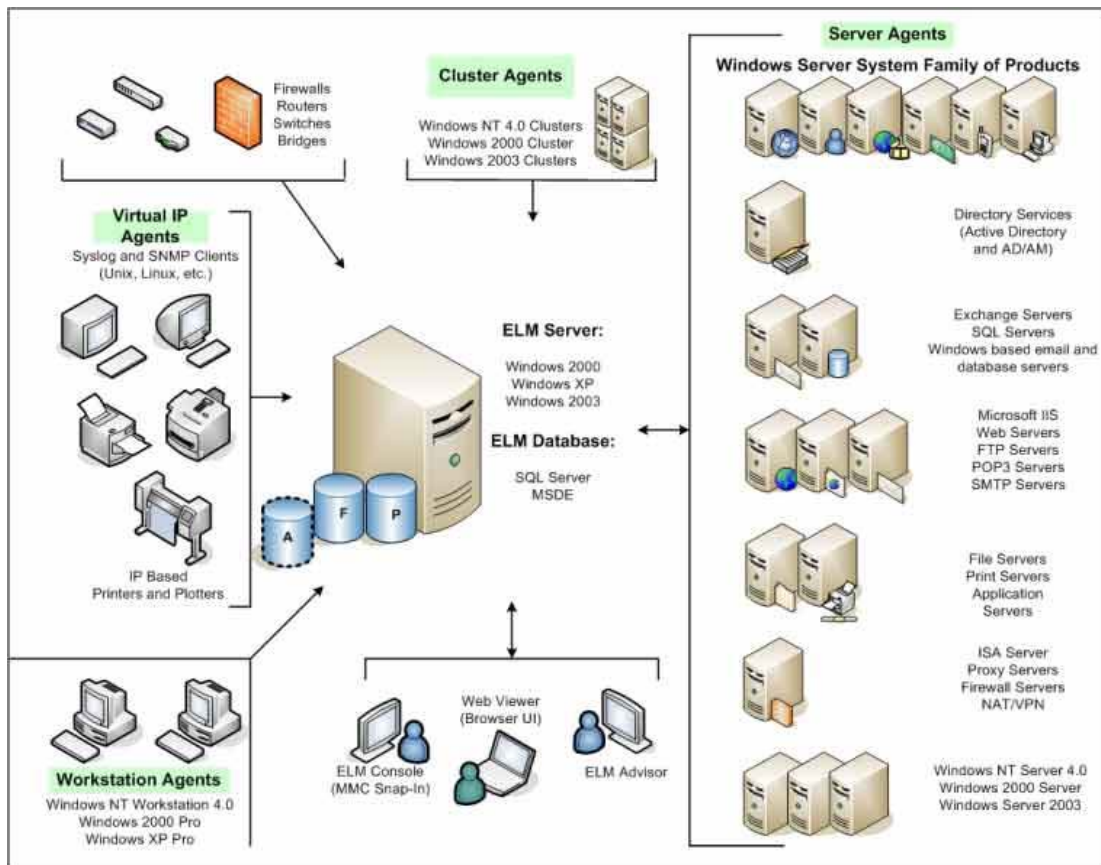


Figure 1. ELM Enterprise Manager's broad array of monitored systems

REAL-TIME AND SCHEDULED MONITORING

EEM can monitor systems and collect data in real time or at scheduled intervals. Each Monitor Item has a schedule component that enables you to tailor it to each system's monitoring needs:

- A scheduled interval, which determines how frequently the monitor item is executed – e.g. every 10 minutes, every 24 hours, every 7 days, etc.
- Scheduled hours, which specify the days and hours the monitor item should run

Real-time monitoring requires the installation of an Agent on the monitored system. Scheduled monitoring can be performed with an Agent or without an Agent (i.e., Agentless monitoring).

RULES-BASED MANAGEMENT SYSTEM

EEM is a rules-based Management System. Rules tie Event Filters and Notification Methods together. Using Event Filters and Rules, you decide which events and conditions trigger notification or corrective action. The ELM Server component has a sophisticated Event Filter engine that creates and customizes Event Views and selectively triggers notification. Using Event Filters, you can define which events are important without having to define each individual event by using wildcards and Boolean logic on any information in the event.

EEM comes pre-populated with a number of rules that help you manage your environment. These rules enable you to manage your Windows workstations and servers out-of-the-box, without requiring any additions, scripts, or other software.

RICH NOTIFICATION AND CORRECTIVE ACTION

When problems occur, it's important for administrators to be notified as soon as possible so that they can correct the problem quickly. EEM includes a rich, robust Notification Engine that enables you to customize notification and corrective action to suit your organizational needs. Different events can trigger different Notification Methods, or a single Notification Method can be used for all similar events. For example, you can use an email notification method to notify a database administrator about important database related events, and a beeper notification method for notifying a security administrator about important security related events. You can have yet another method for notifying Help Desk technicians when a critical server is down. If desired, you can completely customize the message sent via the Notification Method. This is helpful if there are any restrictions on message size, as in the case of a pager, PDA or cell phone. Customizable messages are also a convenient way of making the notification more meaningful.

EEM also includes a Command Script Notification Method that enables you to automate corrective action using batch files, command scripts, and Windows Script Host scripts.

ELM SERVER DATABASE AND REPORTING ENGINES

ELM stores a variety of information in its database:

- Event Log Records
- SNMP Traps
- Syslog Messages
- ELM Alerts

- Performance Data
- Events generated by ELM Server and Agents

After installation, you may launch a wizard to step you through the creation of an archive database, specifying event, alert and performance data retention periods (i.e., how long collected events remain in your database).

EEM includes a Reporting Engine for the creation and scheduling of an impressive array of reports. All reports are stored in the Reports container in the ELM Console. This container, as well as each individual report, supports the application of Windows Access Control Lists (ACLs). You can secure the entire container or secure individual reports. Reports can be scheduled to run automatically at periodic intervals.

Reports included with ELM Enterprise Manager 4.0 are listed in the Appendix.

FULL RANGE OF TECHNOLOGIES INTEGRATED INTO A FULL-FEATURED MONITORING SYSTEM

ELM products use proven, extensible technologies providing comprehensive, robust, scalable, and reliable enterprise management solutions. All ELM products are based on the common set of ELM Technologies; ELM Log Manager™, ELM Performance Manager™ and ELM Event Log Monitor™ are common-code subsets of ELM Enterprise Manager™.

ELM integrates deeply with Windows and leverages Microsoft technologies, APIs, and features. ELM also provides full support for a wide variety of Internet and other standards-based protocols and technologies. Listed below are brief descriptions of the technologies (in alphabetical order) that are combined to create the ELM set of products.

- COM/DCOM
- Internet Protocols (TCP/IP, HTTP/HTTPS, SMTP, POP3, FTP, and PING)
- Messaging API (MAPI)
- Microsoft Management Console (MMC)
- OLE DB
- Simple Network Management Protocol (SNMP)
- Speech API (SAPI)
- SQL Server
- Syslog
- Windows Clusters and Cluster APIs
- Windows Installer
- Win32 APIs
- Windows Management Instrumentation (WMI)
- Windows Script Host (WSH)
- Extensible Markup Language (XML)

A description of these technologies and details on how they are implemented in ELM can be found at <http://www.tntsoftware.com/Products/Technologies>.

SCALABILITY, AVAILABILITY AND RELIABILITY

ELM Enterprise Manager is designed for scalability, availability, and reliability. EEM is *secure by design*, *secure by default* and *resilient by default*. ELM uses an n -tier architecture that enables administrators to distribute secure, real-time monitoring on public, private, federated, and demilitarized networks. Figure 2 illustrates a distributed two-tier architecture (i.e., two ELM Server layers) with multiple slave ELM Servers reporting to a master ELM Server.

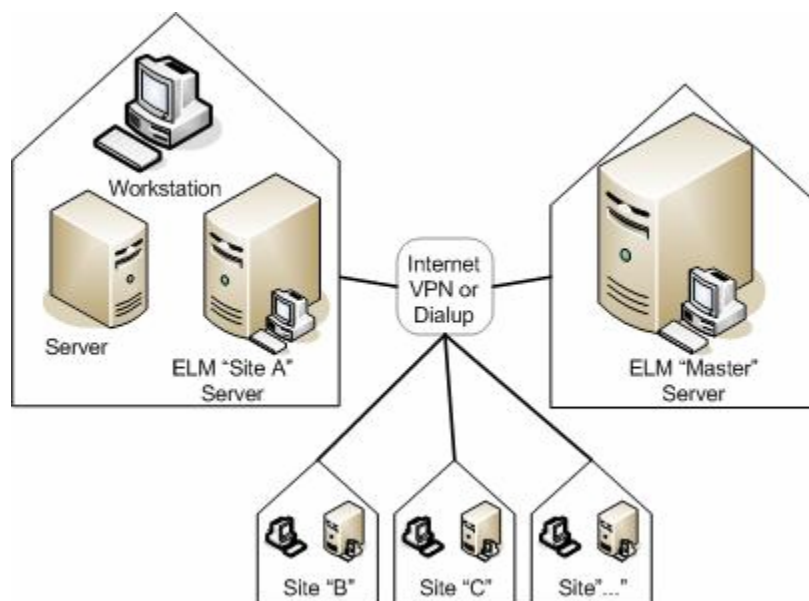


Figure 2. ELM Enterprise Manager Sample Architecture for Multiple Locations

In the above example, the company headquarters and each branch office include a local ELM Server. The branch office ELM Servers can act as slave servers, securely forwarding some or all of the collected event data to a master ELM Server. Each branch office ELM Server monitors the local directory, database, email, file and Web servers using Service Agents. Each Service Agent transmits data to its local ELM Server using a single encrypted and authenticated socket. The local ELM Server then forwards the event data to the master ELM Server using a single encrypted and authenticated socket.

Another configuration is illustrated in Figure 3, which illustrates how a central ELM Server can monitor both local and remote systems. In this example, Service Agents are installed on each Help Desk ELM Server, which in turn is monitoring its local environment. Those Service Agents transmit all collected data from the local ELM Servers to the Central ELM Server using a single encrypted and authenticated socket.

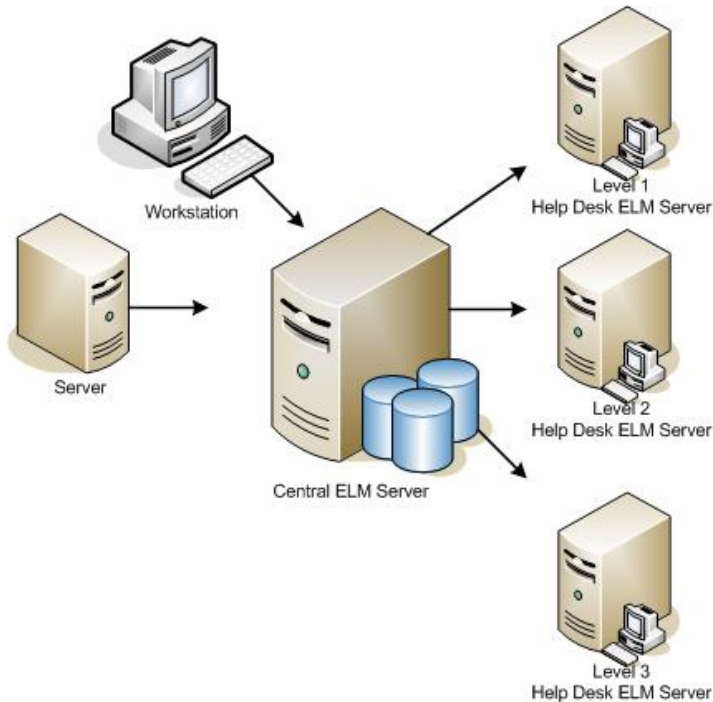


Figure 3. ELM Enterprise Manager Sample Tiered Helpdesk Architecture

There are many available variations of this architecture. No matter how many systems you have to monitor, or how they are distributed, there is an ELM architecture design to fit your needs. ELM can scale-out and scale-up to handle the most demanding environments.

SECURE BY DESIGN

Like Windows Server 2003, ELM Enterprise Manager has been designed with security in mind. EEM leverages many of the security features in Windows 2003, including integrated authentication, item-level security using Windows ACLs, support for Windows auditing, socket encryption, and DCOM authentication and encryption.

SECURE BY DEFAULT

Like Windows Server 2003, ELM Enterprise Manager is secure out of the box. Initial deployment of ELM Enterprise Manager allows only administrators access to EEM objects and features. Whether they access EEM using the ELM Console or through the ELM Web Viewer, the authenticated user accessing EEM without administrative rights on the ELM Server will not be able to edit, change, add, delete or in any way manipulate ELM configuration objects.

RESILIENT BY DEFAULT

ELM Enterprise Manager includes features such as Agent cache mode, database failover, streamlined backup, and recovery and support for Windows Clustering, designed specifically to provide high availability and resiliency of the ELM infrastructure.

Agent Cache Mode

ELM Service Agents include built-in caching functions, so that they continue collecting data, monitoring system health and performance, and executing configured corrective actions even when communication or connectivity between a Service Agent and an ELM Server is interrupted. The Service Agent will go into Cache Mode, saving collected data until connectivity is restored.

Database Failover

The ELM Server has built-in database failover protection to reduce the chances of data loss if the ELM Server's primary database is unavailable. When this happens, ELM invokes database failover and all incoming data is stored in a local database. When the primary database becomes available, ELM will merge the data into the primary database and remove the tables from the temporary database.

Streamlined Backup & Recovery

The ELM Server stores its configuration data in a .DAT file that resides in the directory in which the ELM Server is installed. Every ten seconds, a thread that looks for configuration changes runs in the ELM Server process. When configuration changes are made to ELM Server Objects, the configuration data (.DAT) file is updated and saved. When ELM Server service starts and the .DAT file is successfully loaded, a backup of the current configuration data is created and stored in a .BAK file. Recovery is as simple as reinstalling ELM and restoring this file from backup.

Support for Windows Clusters

In addition to providing powerful monitoring of Windows Clusters, the ELM Server is cluster aware and can be deployed in a cluster for high availability. EEM supports the Active/Passive cluster model and can be clustered on Windows Server 2003 Standard and Enterprise Editions.

ELM ECONOMY

Because Windows Server 2003 enables you to do more with less, especially where server consolidation opportunities exist, deploying Windows Server 2003 can reduce infrastructure.

The primary value for deployment of ELM Enterprise Manager exists in reduction of TCO. This includes reduction in OpEx through automation of IT tasks, reducing downtime and mean-time-to-repair (MTTR), coupled with much deeper and proactive monitoring of critical business processes. The collection of IT performance data provides significant value through the reduction of CapEx, enabling IT to consolidate servers and more effectively plan the deployment of new applications, often using existing hardware.

Deployment of ELM Enterprise Manager further reduces costs by providing a quick Return on Investment (ROI). Below is a sample ROI analysis:

Assume: 20 Windows Server 2003 computers
10 minutes/day/server manually reviewing audit records & diagnosing system problems.
Total: 200 minutes/day (3.3 man hours/day)

Assume: \$65.00/hour for IT personnel
Cost of manually monitoring servers: $3.3 \times \$65.00 = \$214.50/\text{day}$

Assume: 20-server license for ELM Enterprise Manager, eliminating manual processes.
Cost of 20 Server licenses: \$8,500.00

$\$8,500.00 / \$214.50/\text{day} = 39.6 \text{ days ROI}$

Often the actual ROI using this simple calculation is just over a month after deploying ELM Enterprise Manager. Folding in TCO considerations, the ROI could be significantly shorter.

Using ELM Enterprise Manager IT executives can reduce TCO and increase ROI, which translates to faster time to value.

CONCLUSION

Because Windows Server 2003 does not manage itself, Windows administrators must find a way to proactively manage their Windows Server infrastructure in real time without adding significant amounts of overhead to the system using tools that are complete and not overly complex. ELM Enterprise Manager enables administrators to take a proactive and automated approach to managing their Windows Server infrastructure.

Problem management can be divided into three areas: problem detection, problem notification, and problem resolution. ELM Enterprise Manager plays an important role in all three areas: it can detect a wide variety of problems, it can notify the appropriate personnel that a problem exists, and it can automatically correct problems. ELM Enterprise Manager is a scalable, reliable and secure solution for enterprises of all sizes. Its flexible architecture makes it possible to deploy a monitoring and management infrastructure that satisfies any organization's requirements.

Like Windows Server 2003, ELM Enterprise Manager plays a significant role in reducing costs. By automating a Windows administrator's most critical and time-consuming tasks, ELM Enterprise Manager makes the IT day significantly less interrupt-driven, freeing IT staff to proactively manage their systems and delivering an enviable ROI.

APPENDIX

Reports available in ELM Enterprise Manager 4.0

- Active Directory
 - Health
 - Search
- Exchange Server
 - Antivirus Activity
 - Client Performance and Logon Activity
 - Internet Protocol Use
 - Message Activity
 - Public Folder Replication
 - Queues
 - System Resource Utilization
 - 2003 – Mobility
- IIS Server Report
- IIS Server 2000
- IIS Server 2004
- Microsoft Identity Integration Server 2003
- Sharepoint Portal Server 2003
- SQL Server Performance Report
- Windows – Microsoft Message Queue Report
- Windows DNS Server
- Windows Server System – Rights Management Services
- Audit
 - Computer Account Management
 - Logon Activity
 - Object Access
 - Privilege Use
 - User Account Management
- Windows Group Policy
- Installed Applications
- Operating Systems
- Server Reliability
- Event Summary
- Network Health and Performance
- Process performance
- Server Performance