ELM Enterprise Manager

Feature Summary

Sy System Lg Log Cr Core Ev Event Nt Network

THE TRUSTED SOLUTION FOR EVENT LOG COLLECTION, SERVER & DEVICE MONITORING, REAL-TIME NOTIFICATIONS AND REPORTING.

EVENT & LOG MANAGEMENT FEATURES

Event Collector

Sy Lg Cr Ev

The Event Collector monitors all Windows event logs. When an event matching a specified filter is determined it is transferred to the ELM Server and then stored in the database.

ELM will run queries against the database to populate Event Views and trigger notifications as well as generate reports.

Unlike some event log products, ELM provides the ability to collect ALL events by default and filter them down accordingly for your specific needs.

Event File Collector

Sy Lg

Event File Collectors do just that – collect raw .evtx logs on Windows desktop and server operating systems. You can specify which logs to collect, and optionally clear the Event Logs at each collection interval. Collected .evtx files can be compressed and signed if a signing certificate is available.

The Event File Collector operates at a scheduled interval you determine. At each interval, the Event File Collector will attempt to talk with the Log service, select the appropriate log files and then copy the specified Event Log Files from the assigned Agents to a defined storage location.

The files are be stored by default on the ELM Server in a sub folder.

File Monitor

Sy Lg Cr

The File Monitor scans ASCII or plain text files or groups for files on a scheduled basis for a specific character string.

When a match is found, and an action can be triggered such as writing an event to the database that a can start a correlation sequence or launch an alert.

Commonly monitored files include:

- Custom Application Logs (non circular)
- IIS log files
- SQL Server error logs
- Backup software log files
- Anti-virus software log files

Event Monitor

Sy Lg Cr Ev

The Event Monitor compares new events against a set of Include and Exclude Event Filters. If an event matches or fails to match these criteria within the specified interval, a local Action is executed under the local administrator account.

Actions include writing an event to the database when an event is found, or not found, so that the occurrence can be queried against for a view or to trigger a notification.

A command script can also be launched to perform a corrective action.

Syslog Receiver

Sy Lg Nt

The Syslog Receiver is configured to process and parse Syslog messages from network devices and Linux/UNIX systems. Supporting both UDP and TCP, these messages are converted to the standard Windows event log format.

Like Windows events, they are stored in the database and queried against to create concise views and trigger alerts or notifications.

The Syslog Receiver is a valuable tool for supporting firewalls and the security of Windows networks.

SNMP Receiver

Sy Lg Nt

The SNMP Receiver is configured to accept SNMP v1, v2, and v3 Traps from network devices. These traps can be translated against stored .MIBS and converted into a standard Windows event log format.

Like Windows events, they are stored in the database and queried against to create views and to trigger alerts or notifications.

The SNMP Receiver allows for real-time monitoring, alerting and reporting of Windows and non-Windows systems together on a single platform.

SNMP Monitor

The SNMP Monitor includes a MIB browser that queries a SNMP Object ID (OID) and triggers an Action if the value is greater than, less than, or equal to a specified value for warnings, success, or failure.

Events generated can be written to the ELM database or to an Application log.

It extends the status monitoring of ELM beyond Windows systems and into SNMP supported network devices.

SNMP Collector

The SNMP Collector monitors the SNMP Object IDs by polling devices on a scheduled basis, much like a performance collector, and returns the values to the ELM Server.

It will display the OID, Translated Name, and the Community fields.

These values are stored in the database for reporting and trending analysis.

PERFORMANCE & STATUS MONITORING FEATURES

Ping Monitor

The Ping Monitor sends custom ICMP echo requests to verify TCP/IP connectivity and the Quality of Service.

It provides an early warning alert of a problem with the remote system's status.

You may specify the size of the echo request packets and the number of packets that are sent. The Ping Monitor will execute the configured Actions, depending on the results of the Ping. When enabled:

- The Success Action will be executed if all echo requests succeed.
- The Warning Action will be executed if at least one echo request fails and at least one succeeds.
- The Failed Action will be executed if all echo requests fail.

Even though the Ping Monitor is assigned to Agents, it is always executed by the ELM Server and can be run at a pre-defined schedule that you determine.

Performance Monitor

Performance Monitors can be used to monitor any published performance counter for a condition that is greater than, less than or equal to a threshold value you determine for the specified duration that is appropriate for your server's function.

By using Performance Alarms, you can be alerted when disk space, memory or CPU has reached unexpected or out-of-bound levels.

Performance Collector

The Performance Collector supports proactive system management and resource monitoring by passing collected data to the Dashboard and comparing against pre-determined thresholds for bottleneck status displays. Any published performance objects, counters and/or instances can be collected at a set frequency on a scheduled basis.

- Disk Performance
- Free Disk Space
- Memory Usage
- Network Performance
- Processor Performance

Process Monitor

The Process Monitor provides a comprehensive view of a system's process activity. The Process Monitor is multi-functional; it can notify you when a process has exceeded the threshold of CPU usage you specify and it can track when processes are started or terminated.

It can also generate a Warning or Error when the number of instances of a process exceeds your specified value.

Service Monitor

The Service Monitor detects and responds to changes to the service status. It monitors changes into the conditions:

- Starting
- Started
- Paused
- Stopping
- Stopped

It is commonly used with the Command Script notification to restart a failed service. Alerts can be triggers that confirm a service has stopped and was successfully restarted. This empowers administrators to combine monitoring with automated corrective actions.

Script Monitor

The Script Monitor, first introduced in ELM Enterprise Manager 7.5, allows the ELM Agent to run virtually any PowerShell, VB, or CScript on a remote system on any schedule that is configured.

It operates like a distributed task scheduler providing administrators with great control and precision for automating jobs.

WMI Monitor

If you are using Windows Management Instrumentation (WMI) — the Microsoft implementation of Web-Based Enterprise Management (WBEM) — you can use WMI Monitors to query a WMI namespace and database.

The WMI Monitor queries the WMI namespace (typically rootcimv2) and generates Events when the results of the query change that you can be notified on. Common applications include detection of new external drives and file changes.

It's a powerful tool for expanding the data sources available to identify system changes or activities.

Inventory Collector

The Inventory Collector gathers data about what is installed on each Windows-based system. You can collect data on the Windows operating systems, installed services, and applications that have been installed and added to the Programs and Features applet in the Windows Control Panel.

The Inventory Collector also allows you the flexibility to add specific services to the Inventory or exclude certain products (by default all products are included in the inventory).

APPLICATION & NETWORK MONITORING FEATURES

TCP Monitor

The TCP Port Monitor allows you to monitor virtually any TCP Port. The ELM Server (not an Agent) makes the actual connection to the port, allowing you to monitor TCP port availability on any operating system.

- Unix
- Linux
- Novell
- Solaris
- Windows

And more provided that you have TCP/IP connectivity to that system from the ELM Server. Each TCP Port Monitor can poll a single port and you can have numerous TCP Port Monitors enabled.

It evaluates the port's availability and Quality of Service. Different actions can be triggered if it succeeds, fails, or the response time is slower than expected.

FTP Monitor

The FTP Monitor item monitors the status and availability of an FTP site – any valid and accessible FTP server on your network.

An application-layer FTP connection to the FTP Server is made at your specified interval and anonymous or authenticated connections are supported. By default, port 21 is used, but the Monitor can be configured to use any port.

Because the ELM Server (not an Agent) makes the FTP connection, you can monitor FTP server availability and Quality of Service (QOS) on any operating system running FTP server software such as Unix, Linux, Novell, Solaris, etc.

SMTP Monitor

SMTP Monitors watch SMTP hosts, gateways and services. They can be used with Service Agents or Virtual agents and will periodically establish an SMTP connection to the server and port specified

The SMTP Monitor connects to the SMTP Server and times the initiating conversation from “EHLO” to “250 OK.”

Enabled Actions are executed depending on successful, slow, or failed responses. Negative or slower-than-expected responses trigger a variety of notification options.

Web Page Monitor

Web Page Monitors are used to monitor HTTP or HTTPS URLs. The ELM Server periodically establishes an HTTP connection to the server and port specified. If the response is negative, slower than expected, or if the content has been changed, a variety of notification options can be triggered.

Note that multiple Web Page Monitors can be assigned to the ELM Server or to Service Agents. This means you can create Web Page Monitors independent of the number of Agent licenses you have purchased.

FAULT TOLERANCE FEATURES

Agent Monitor

The Agent Monitor performs periodic checks on ELM Service Agents. ELM is able to check on its own Agents reporting back. If communication fails unexpectedly they can automatically cycle themselves. If the Service Agent does not respond or is slow responding, notifications can be triggered to carry out corrective actions.

Event Writer

The Event Writer is designed to ensure events are being collected and the monitored system is sending events to the ELM Server. This type of point-to-point verification goes beyond a simple Ping and ensures that the system is actually reporting as expected.

At the Agent level, the Event Writer publishes a pre-configured event on a schedule into the local Application Event Log. ELM can be configured to look for this event, ensuring events are being collected and the system is functioning correctly. This fault tolerance feature tests the entire loop from event generation, to collection to filtering and notification.

EVENT VIEWS & FILTERS

Event Views

These are ELM’s defaults and some of the most commonly used views of data as well as specialized views for default monitoring items in ELM.

- All Events
- Dashboard Status
- Server & Agent Specific Events
- PING Activity
- Syslog and SNMP

Security Views

Specialized for security event activity with display columns customized to show important security information that can be buried in event data.

- Audit Activity & Failures
- Computer Account Changes
- Logon/Logoff Activity
- Network Logons
- User Accounts

Correlation Views

Designed to monitor for unique event sequences including start and end events as well as start and time-out activity.

- Point-to-Point Verification
- Service Restart to Slow
- Windows Reboot too Long

Filtering

ELM’s powerful filtering capability allows you to collect and view the data you want without spending ridiculous amounts of time sifting through thousands and thousands of records looking for the needle in the haystack.

Include and Exclude filters can be used together to support very complex situations and needs. Each of the filter types can be built from an existing event that will pre-populate fields for you or they can be built from scratch if desired. Filters in ELM apply to both Monitors and Views and can be reused throughout the product.

Filter Types

There are three types of filters used through ELM.

- **Include Filters** – Utilize a "Whitelist" approach and only collect or display matching events.
- **Exclude Filters** – Utilize a "Blacklist" approach and collect or display everything except matching events.
- **Correlation Filters** – Specialized format for matching event sequences and timeout options in Correlation Views.

Fields

Filters utilize can any / all of these event fields:

- Computer Name
- Log Name
- Username
- Event Source
- Event ID
- Event Category
- Message contains – (free form text) Save

Wild card operators (AND, OR, NOT) and partial matches are also supported.

ALERTING & NOTIFICATION METHODS

Command Script

The Command Script Notification Method is an automated response or corrective action tool that can execute a command, a command line application, a batch file, or a script. You may pass event information in the form of variables, leveraging information in the event, such as the computer name or the message details field in any batch files or scripts that are executed.

ELM supports the Windows Script Host (cscript.exe), command line (cmd.exe), or any executable, including custom-written programs in Perl or PowerShell.

Dashboard

The Dashboard View is a quick at-a-glance display of monitored systems' health and status. It provides a combination of performance data collected as well as availability and system function (point-to-point verification). Utilizing ELM's Performance Collectors, displays include "bottlenecks" for:

- Processor
- Memory
- Disk
- Free Disk
- Network

Thresholds for each metric or bottleneck can be customized and displays allow drill-down to specific performance details for each monitored system.

ELM Advisor

The ELM Advisor is a popup up message type of notification that lives in the taskbar. It provides end users with an instant notification of event activity without disrupting work flow.

Thresholds can be set to determine how many times identical events occur before the Advisor notification is triggered, preventing an overload of bubbles repeatedly popping up.

Forward Events

ELM Servers have the ability to forward events on to another ELM Server, allowing you to link and build an n-Tier type of monitoring structure across different networks or even different locations. Events can be forwarded "upstream" from several servers to one centralized server where notifications can be generated from.

This feature is very valuable with Managed Service Providers who are monitoring a number of different sites to centralize their views and notifications of event activity in order to meet SLAs.

Many Public Safety Service providers utilize this feature as well to centralize their monitoring while providing site specific real-time notifications and alerts.

Email Notification

Email messages utilize SMTP and are fully customizable with any fields available from an event as well as custom text. Messages can be sent to multiple addresses and scheduling can be used to send email notifications to different addresses at different times of the day for the same event occurring.

This is a handy feature for situations such as after-hours support.

SNMP V1/V2 Traps

Any event received by the ELM Server can be repackaged and transmitted as an SNMP Trap or Inform to any SNMP management systems in the organization.

SNMP V3 Trap

Events received by the ELM Server can be transmitted as SNMP V3 Traps or Informs and utilize different authentication, encryption protocol.

Syslog Message

ELM can send native, integrated and customizable Syslog Messages for centralized support of cross-platform environments.

PRECONFIGURED REPORTS

Data Profile Reports Include:

- Data Profile – Partitions
- Data Profile – SQL Server
- Data Profile – Various

Event Summary Reports Include:

- Events by Computer
- Events by Source
- Events by Type

Standard Reports for Installed Applications

- Application Inventory by Computer
- Application Inventory by Product Name
- Application Inventory by Publisher

Standard Reports for Installed Operating Systems

- Operating Systems by Computer
- Operating Systems by Product
- Operating Systems by Version

Standard Administrative Security Reports Include:

- Computer Account Change
- Computer Account Management
- Group Account Management
- Group Policy – Critical
- User Account Change
- User Account Management

Standard Security Logon Activity Reports Include:

- Activity by Server
- Activity by User
- Activity by Workstation
- Audit Failures
- Terminal Services Activity

Standard Security Object Access Reports Include:

- Object Access Detail
- Object Access Summary
- Object Access Type

Standard Security Privilege Use Reports Include:

- Privilege Use by Date
- Privilege Use by Server
- Privilege Use by User

2001 Main Street
Vancouver, WA 98660

TNT Software

(360) 546-0878
sales@tntsoftware.com