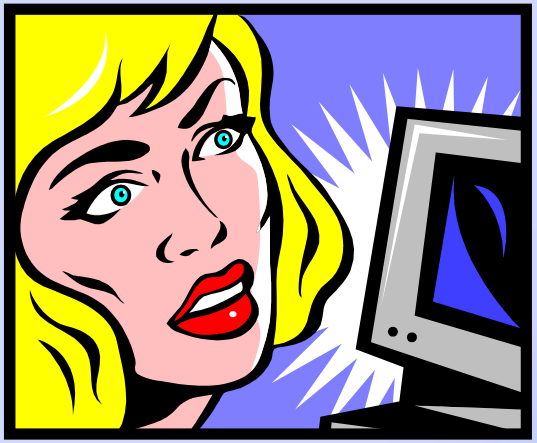
Proactively Managing Your NT Infrastructure with Event Log Monitor™



TNT Software

Challenges of Administering Windows NT/2000

- Single system providing critical services
  - Internet server in DMZ (e.g., FTP, HTTP, SMTP)
  - Corporate File & Print, Email or Database Server
  - Other critical island server
- Multiple systems providing critical services
- Monitoring Flat Files
- Cross-platform monitoring (Unix/Linux)

Challenges of Administering Windows NT/2000

- Managing Events
  - Security Log – Authentication and Auditing
  - Application Log – Application events
  - System Log – Operating System events
  - Additional Windows 2000 Event Logs
- Performance Data – Regular collection and alarm monitoring
- Gathering System Configuration Data

Challenges of Administering Windows Clusters

- Logging turned off by default in NT 4.0 clusters. When turned on, the log is not very readable.
- Windows 2000 cluster logging is on by default. Logs to a flat file (cluster.log) that is difficult to monitor manually.

Event Log Monitor Features

- Centralized monitoring, collection, processing and archiving of Windows NT/2000 events and Unix/Linux Syslog events
- Centralized monitoring, collection, processing and archiving of Windows NT/2000 performance data
- Enhanced monitoring of Microsoft Cluster Server and Windows 2000 clusters
- Monitoring of NT services, TCP/IP services (HTTP, SMTP, FTP, POP3) and processes
- Monitoring of flat files (e.g., .LOG, .TXT, etc.) files

Event Log Monitor Features (cont'd)

- Notification of events or performance alarms (via email, pager, Syslog message, network message, batch file, etc.)
- Collection and comparison of system configuration data (shares, devices, drivers, accounts, etc.)
- Automatic recovery for failed services
- Console can receive traps from or send traps to other SNMP management packages (e.g., Tivoli, OpenView, SMS).

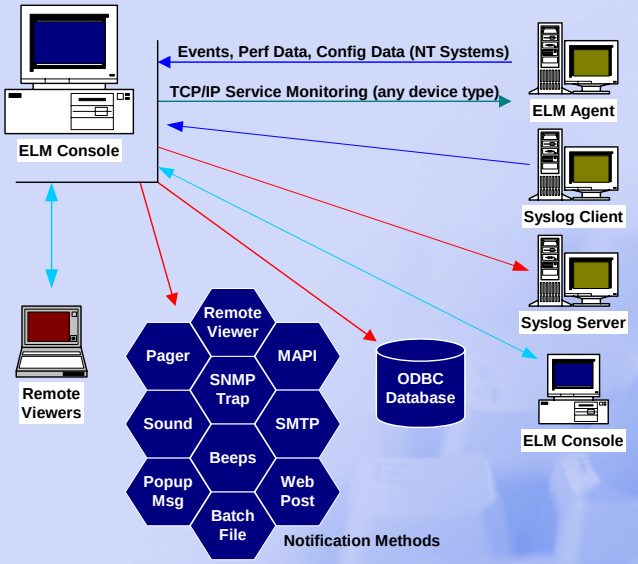
Event Log Monitor Features (cont'd)

- Agents easily installed remotely (from Console)
- Message Notes & Comments allow you to create a Knowledge Base containing events and solutions for problems.
- Automatic database management (purge events after X days, and performance data aggregation weekly, monthly or quarterly)
- Over 40 built-in reports for events and performance data
- Support for multiple database platforms:
  - Microsoft Access (runtime included)
  - Microsoft SQL Server 6.5, 7.0 or 2000
  - Oracle 8 or higher

Event Log Monitor Features (cont'd)

- Works great in a firewall environment (NetBIOS and RPCs not needed)
- Can forward events to another Console or to a Unix/Linux Syslog server
- Data can be exported to ASCII files or Windows Clipboard
- Remote Viewer and Web Viewer are remoted consoles that can run on Windows NT, Windows 2000, Win9x, Windows ME and Windows CE.

Event Log Monitor Architecture



Console: Management Console (Server)

Agent: Monitoring component (Client)

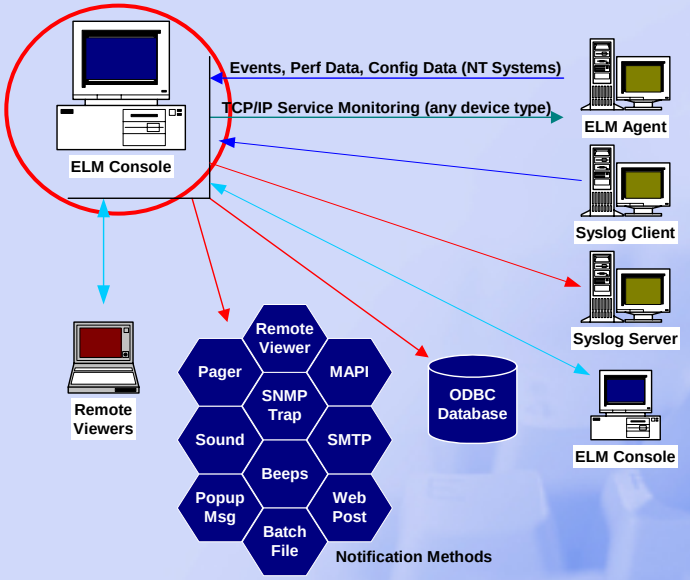
Remote Viewer: Remoted Console

Web Viewer: Web-based remoted Console

Database(s): Event/Perf Data Storage

CFG/DAT Files: System Config Data

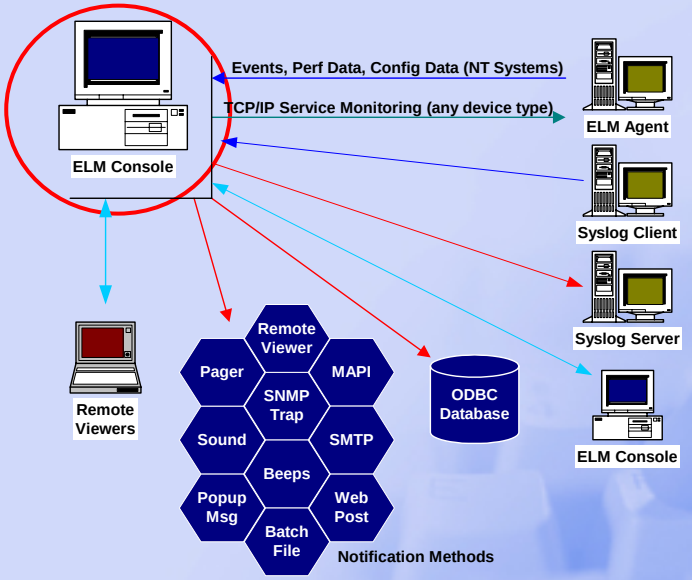
Event Log Monitor Architecture



Console: Management Console (Server)

- Install and configure agents (NT & IP)
- Configure Notification Rules
- Configure Notification Methods
- Manage Collection Sets
- Annotate Events (Notes & Comments)
- View Collected Events
- View System Configuration Data

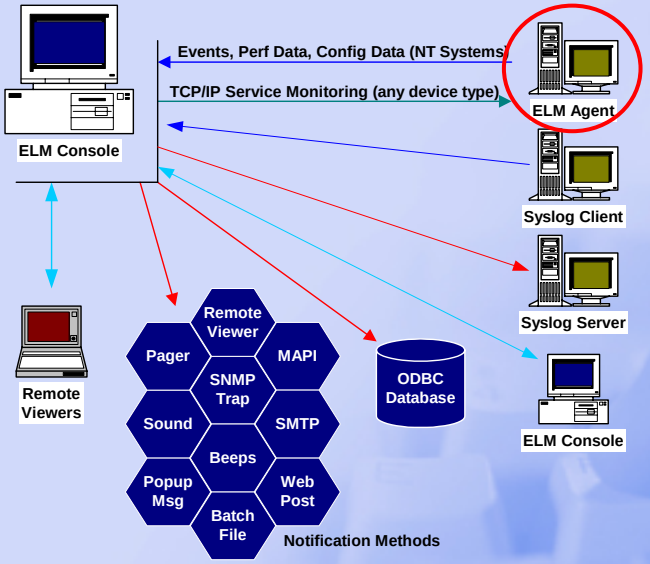
Event Log Monitor Architecture



Console: Management Console (Server)

- Runs interactively and/or as NT service
- Uses integrated NT authentication
- Customizable TCP/IP port settings for use in a firewall environment
- Utilizes system resources very efficiently
- Can receive events from Syslog clients

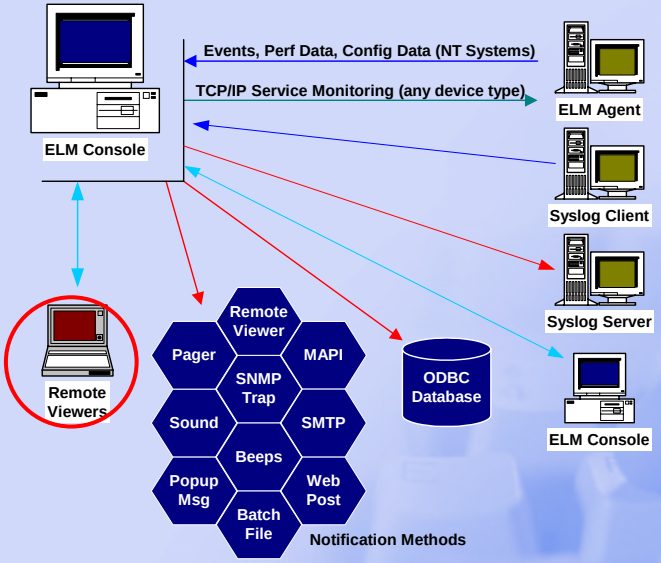
Event Log Monitor Architecture



Agent: Monitoring Component (Client)

- Listens to NT Event Subsystem
- Listens to NT Performance Subsystem
- Collects Specified Performance Counters
- Monitors Services and Processes
- FileMon Monitors Flat Files
- Collects System Configuration Data
- Enhanced Monitoring of NT/2000 Clusters

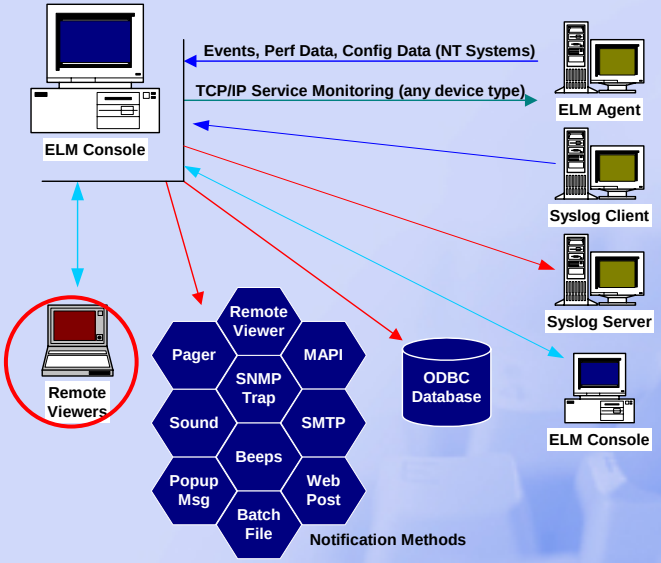
Event Log Monitor Architecture



Remote Viewer: Remoted Console

- Limited functionality
  - View Events
  - Receive Alerts
  - View Agent Status
  - View/Control Processes, Services & Devices
  - View Notes/Comments entries
- Cannot change agent settings

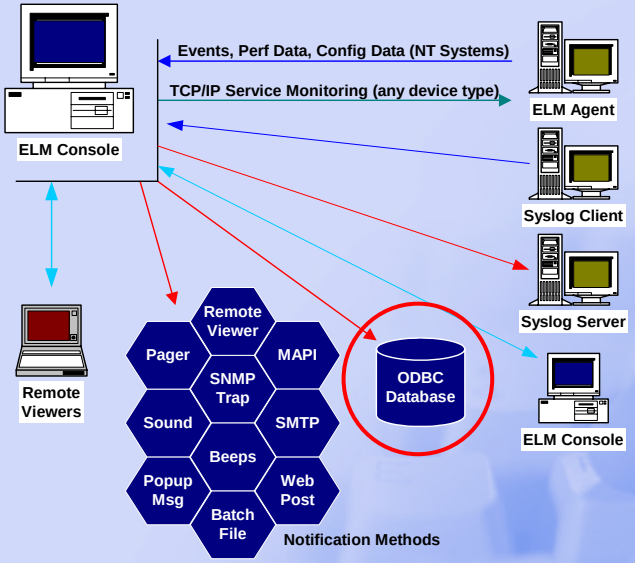
Event Log Monitor Architecture



Web Viewer: Remoted Console

- Limited functionality
  - View Events
  - View Agent Status
  - View/Control Processes & Services
  - Generate Reports
- Cannot change agent settings

Event Log Monitor Architecture



Database(s): Event/Performance Data

- Microsoft Access – runtime included!
- Microsoft SQL Server 6.5, 7.0 or 2000
- Oracle 8 or higher

Network Traffic Analysis

- Typical event generates 12 packets (381 bytes) between Console and Agent
- Remote Viewer ←→ Agent/Console < 40k
- Authentication traffic < 40k
- Network Analysis White Paper available at:
  http://www.tntsoftware.com/products/emon20/elmnetplanwp.pdf

Performance Analysis

- Console typically uses less than 10MB of physical memory and less than 10% CPU time
- Agent typically uses less than 5MB of physical memory and less than .1% CPU time
- Able to withstand severe event storms

Customers

- Microsoft
- Intel
- Compaq
- AT & T
- Texas Instruments
- Eastman Kodak
- TRW
- Federal Reserve Board
- ...and many, many, many more!

TNT Software

For more information, visit

http://www.tntsoftware.com or
http://www.eventlogmonitor.com