

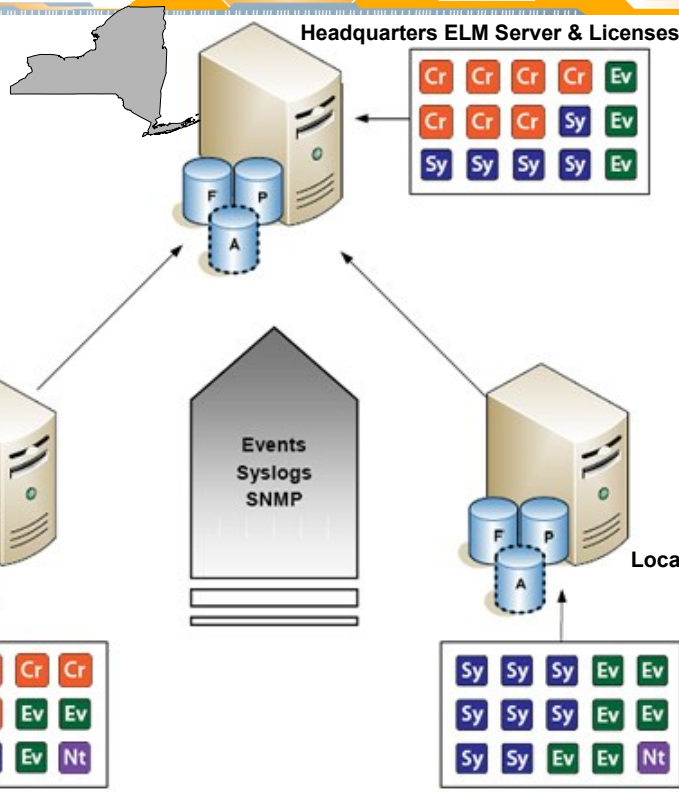
On the front end, ELM will monitor hundreds of Servers, Workstations and Devices and process tens of millions of event log entries every day, gather system performance and diagnostics information, monitor application and server availability, and send real-time notifications when conditions change that you need to be aware of. In most implementations, a single ELM server will collect, evaluate, and distribute the information as it occurs. This reduces downtime, increases security, increases server and application availability, and accelerates the return on investment.

ELM automation of these tasks frees your IT staff to manage more systems and to complete other pressing tasks required by today's regulatory and security demands.

ELM will produce meaningful Event Views of the massive amount of data collected and immediately filter it for quick analysis and decision making. All data is securely stored in Microsoft SQL Server databases. ELM requires two databases; the Primary Database (P) for real-time reporting and a Failover Database (F) to ensure data continuity should the Primary Database be unavailable. In addition, unique data retention features efficiently manage the data for long term storage needs with the use of an optional Archive database (A).

Forwarding to a Central ELM Server

An ELM Server can forward any Event, Syslog message or SNMP trap to another ELM Server. Forwarding events from one ELM Server to another enables you to design and deploy ELM in a tiered manner, or to monitor multiple locations from a centralized location. Because all data sent from one ELM Server to another is encrypted, you can safely locate ELM Servers within a DMZ, enabling real-time monitoring and notification without compromising security.

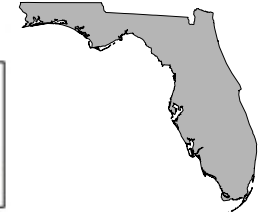


- Continuous forwarding from child ELM Server(s) to Parent ELM Server
- Filter out data that is or is not forwarded to the Parent ELM Server
- Utilize ELM Editor to generate reports for all systems at all sites.
- Provides another level of data backup & redundancy

Location 1 ELM Server & Licenses



Location 2 ELM Server & Licenses



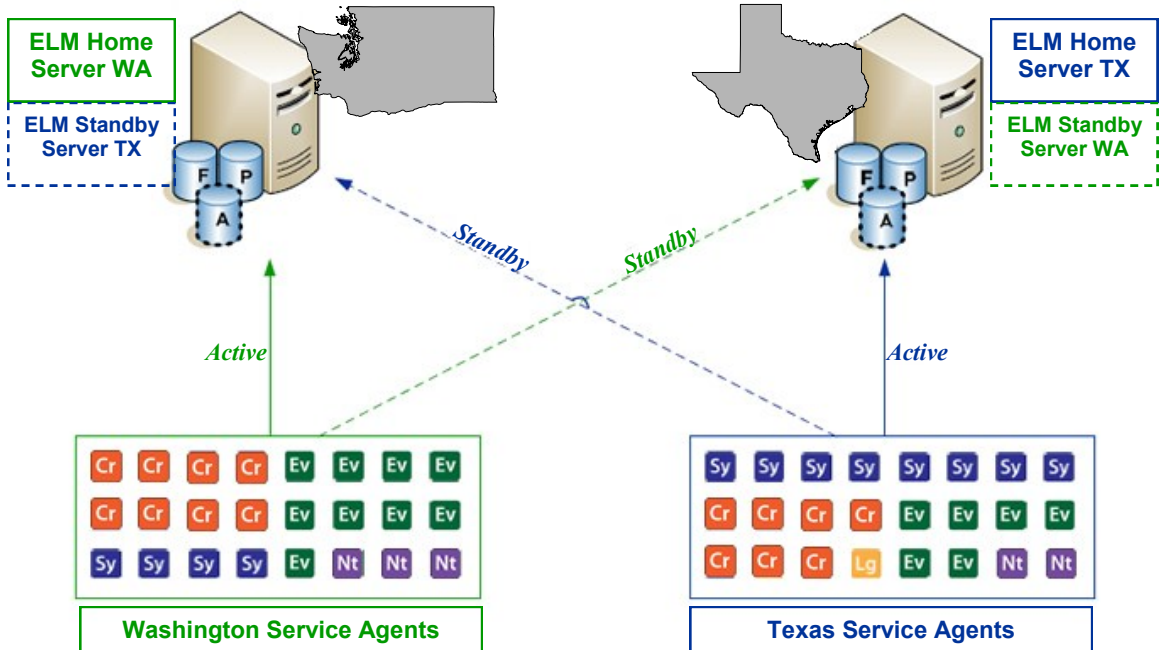
ELM is firewall friendly. Service Agents communicate with ELM Servers using a single TCP socket that is customizable. Because ELM listens on only one port by default, security implications of FTP or RPC communications through the firewall are eliminated.

You can configure the Service Agent and the ELM Server to listen on any available TCP port for communications. In addition, each Service Agent can use different ports, enabling you to customize ELM's socket usage to suit your needs.

Standby Server - Resiliency

ELM supports disaster recovery plans by providing an option for a Standby ELM Server in addition to the Home ELM Server. When the Home ELM Server is not available, select Service Agents assigned to a special category will automatically "swing over" and connect to a Standby ELM Server to continue reporting functions.

When the Home ELM Server is available again, the agents can automatically or manually be triggered to "swing back" once you determine the Home environment to be stable and ready. The Home and Standby Servers can each run their own primary database, or they could connect to the same remote database server.



In the illustration above, the ELM Home Servers at each location are also licensed to act as a Standby Server for the other location. For example, if the Washington ELM Home Server went offline due to a hardware failure, the service agents reporting to it would automatically execute their instructions to point to the Standby Server WA (TX Home Server) and begin reporting their data here until connectivity with Home Server can be restored.