

### Logging In Depth

EventTracker is a Security Information and Event Management (SIEM) solution designed to enhance the security of critical systems, ensure confident compliance and improve overall performance and availability

### LAWRENCE LIVERMORE NATIONAL LABORATORY

Science in the National Interest

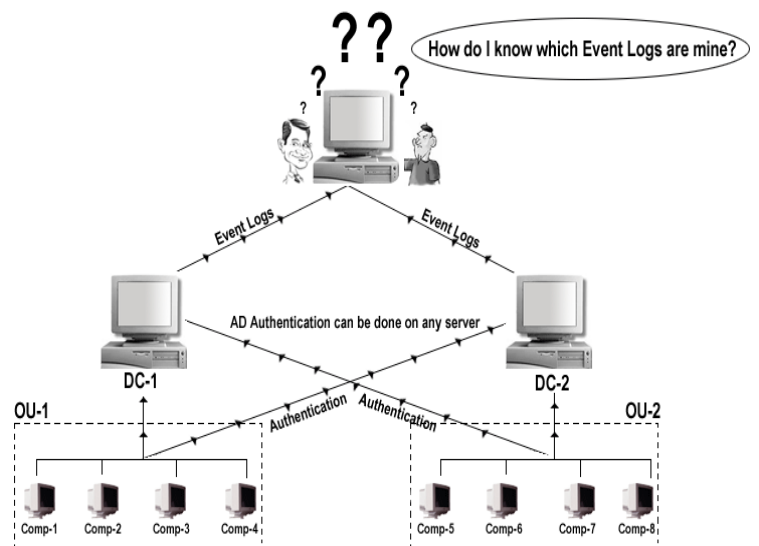
#### Drivers

- Consolidate logs from multiple locations for audit and security requirements
- Identify and redirect event logs to specific organizational Units

As a national security laboratory, Lawrence Livermore National Laboratory (LLNL) is responsible for ensuring that the nation's nuclear weapons remain safe, secure, and reliable through application of advances in science and technology. The Laboratory's special capabilities have led to expanding responsibilities to meet other pressing national security needs, which include countering the proliferation of weapons of mass destruction and strengthening homeland security against the terrorist use of such weapons. LLNL has an annual budget of about \$1.6 billion and a staff of over 8,000 employees. It is home to over 3,500 scientists, engineers, and technicians together with professionals in many other disciplines that keep the Laboratory running in a safe, secure and efficient manner.

LLNL is moving to an Active Directory (AD) implementation using Microsoft Windows. One single top level domain replaces multiple NT 4.0 domains. As part of their security requirement, they required a central logging facility with event correlation. Individual labs (each an Organizational Unit (OU)) within the LLNL environment maintain a high degree of autonomy and are responsible for their own IT infrastructure including security. This business requirement is contrary to the Active Directory model recommended by Microsoft, where a high degree of centralization is presumed. Typically Microsoft AD implementations are company wide – not department specific.

This business problem at LLNL therefore was to **a)** consolidate event logs from multiple locations; **b)** identify event logs (via correlation rules) as related to a given OU; and **c)** redirect event logs related to a particular OU to the corresponding OU-Admin Console. This is shown as follows:

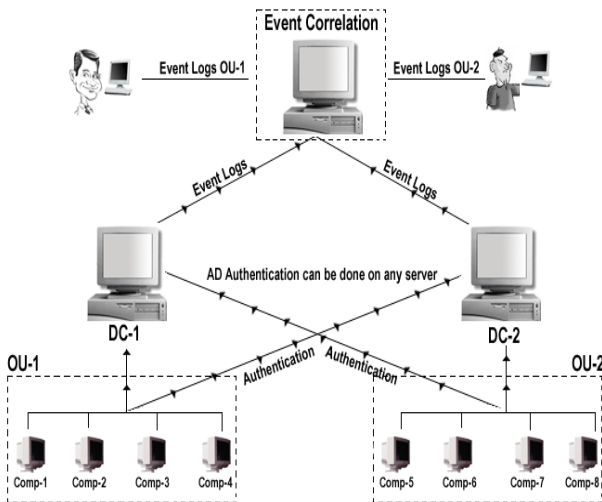


Eric Eichenlaub is the System Architect - Active Directory with the SMSG/ICCS Group at LLNL. His mission was to design and implement a secure and robust solution for LLNL so that the benefits of Active Directory could be leveraged over the older NT domain technology.

Eichenlaub started looking for solutions that would allow him to satisfy the audit requirements for a high security installation, as well as provide tools to manage the lab's infrastructure and servers farms. He needed an automated way to record all the events generated by the servers, and issue alerts on any external and/or internal intrusions into the servers. Additionally, OU Administrators needed to be notified of any performance issues to maintain their SLAs. Eichenlaub spent many months evaluating various solutions, but none of them had the capabilities and efficiency that his organization needed.

Eichenlaub identified EventTracker as a possible candidate for the labs to deploy and contacted Prism to discuss his specific requirements including correlation rules. A requirements document was created to capture the various scenarios that needed to be satisfied. These were initially drawn up assuming Windows Server 2000 but were later changed to accommodate Windows Server 2003.

Working with LLNL, Prism developed a set of correlation rules that are at the heart of the EventTracker Correlation Engine. This engine resides behind the EventTracker console and sifts the incoming event stream to recognize patterns. When a pattern is recognized, the corresponding action is fired. Actions include log separation and redirection, alerts etc. Correlation rules identify many security concerns including User Logon failure, Account Lockout, OU Audit Policy changes, Add/Delete resources including OUs, Users, Printers, Shares etc. This solution is shown in the following figure:



EventTracker gives LLNL control over their infrastructure because they know everything that's occurring on mission-critical workstations and servers. Customizable automated reports are produced in the background, sending consolidated information to concerned persons on a regular basis. EventTracker enables administrators to choose what kind of data is reported on, by using customizable Event Categories. The correlation rules route relevant events to designated persons which decreases exposure time to potential threats.

Support for guaranteed delivery of events between agents and the central console was important in the LLNL environment. In the case of network or computer failure, events are cached against loss and delivered in sequence. LLNL also required support for Oracle 9 as the backend relational database where events are stored.

EventTracker has allowed LLNL to deploy Active Directory in their distributed enterprise while satisfying regulations and honoring organizational boundaries on ownership and control. In addition, LLNL can centrally monitor and manage events generated by their distributed servers. All event data is organized in relevant databases. Beyond basic firewall functions, EventTracker provides security for the "last mile"; it detects intrusions within the network. For example, if an employee tried to access a server he or she did not have permission to, EventTracker will alert the administrator. Another security feature, which must be addressed for regulatory compliance, is encryption of log data. EventTracker archives and stores all logs in a tamper-proof "vault" for future analysis. All these security precautions are necessary. CERT data shows that there are hundreds of attacks mounted everyday. EventTracker provides a detailed audit trail that can be followed if required.

In conclusion, LLNL was able to effectively implement Active Directory in their complex, distributed and highly secure environment and has gained control and insight into their growing infrastructure. LLNL met their requirement to migrate smoothly from NT4.0 domains to Active Directory using Windows Server 2003. LLNL has satisfied regulatory compliance auditors and increased their security forensic capabilities through the deployment of EventTracker.