Contribution ID: **464** Type: **oral**

Log Mining with Splunk

Thursday 26 March 2009 18:10 (20 minutes)

Robust, centralized system and application logging services are vital to all computing organizations, regardless of size. For the past year, the RHIC/USATLAS Computing Facility (RACF) has dramatically augmented the utility of logging services with Splunk. Splunk is a powerful application that functions as a log search engine, providing fast, real-time access to data from servers, applications, and network devices. Splunk at the RACF is configured to parse system and application log files, script output, snmp traps, alerts, and has been integrated into our Nagios monitoring infrastructure.

This work will detail our central log infrastructure vis-‘a-vis Splunk, examine lightweight agents and example configurations, consider security, and demonstrate functionality. Distributed Splunk deployments or clusters between institutions will be discussed.

Presentation type (oral | poster)

Oral

Primary author: PETKUS, Robert (Brookhaven National Laboratory)

Co-authors: SMITH, Jason (Brookhaven National Laboratory); RIND, Ofer (Brookhaven National Laboratory)

Presenter: PETKUS, Robert (Brookhaven National Laboratory)

Session Classification: Software Components, Tools and Databases

Track Classification: Software Components, Tools and Databases