splunk>

CASE STUDY

RIKEN Advanced Institute for Computational Science Gains Uptime, Improves Security

Executive summary

RIKEN, The Institute of Physical and Chemical Research, is Japan's only comprehensive research center for the natural sciences. Its Advanced Institute for Computational Science (AICS) relies on a complex infrastructure including the K computer, one of the world's fastest computer systems. The organization needed a solution to help it improve operations and security in computer systems that support important scientific research. Since deploying Splunk Enterprise, the organization has seen benefits including:

- Improved management of large-scale log event data
- Increased system visibility and uptime
- Real-time insights into security issues

Why Splunk

Since 2003, RIKEN has been an independent administrative corporation under Japan's Ministry of Education, Culture Sports, Science and Technology. It conducts research in a wide range of fields including physics, engineering, chemistry, biology, and medicine. Establishing the use of computer simulation for predictive science—a scientific view into the future—is a goal for RIKEN's Advanced Institute for Computational Science (AICS), with the use of the K supercomputer one important part of this mission. As one of the world's 500 fastest computer systems, the K computer is used on some 130 projects covering life sciences, weather and disaster prevention.

RIKEN's AICS generates a vast amount of machine data via three separate systems comprising the K supercomputer, the network system and the High Performance Computing Infrastructure (HPCI) server group. Operating and managing these three systems while ensuring site stability and availability presented huge operational and security challenges. Given the massive amount of data generated by these systems, the AICS chose Splunk Enterprise to analyze the logs from the disparate systems quickly and efficiently.

Industry

- Technology

Splunk Use Cases

- Security
- IT operations
- Big data
- Log management

Challenges

- Lacked visibility into voluminous internal log event data
- Required solution to provide insights into security-related attacks and unauthorized access
- Needed to improve job scheduling

Business Impact

- Improved visibility and uptime across three systems
- Increased efficiency in management of large-scale log event data
- Gained real-time insights into security issues
- Optimized job scheduling

Data Sources

- System availability logs
- K Supercomputer logs
- Network equipment logs
- HPCI server logs
- Database logs
- Data from third-party vendors

Splunk Products

- Splunk Enterprise

Full visibility into vast amounts of data

RIKEN's AICS deployed Splunk software in its three systems—K, the network system and the HPCI server group—and immediately began collecting, extracting and analyzing log event data. In addition to internal logs, security-related logs covering external attacks and unauthorized access, logs from network equipment, server loads and temperature management, and K job operational status logs are now managed via Splunk software.

According to Senior Technical Scientist Dr. Motoyoshi Kurokawa, "When the flow of logs increases rapidly, Splunk provides a structure for the delivery of an alert, which makes it very convenient for quickly understanding the problem. Also, we can monitor the work that the outside vendors responsible for network operations are doing to ensure it is done correctly. If we are in a place where we need to use CUI instead of GUI, we can do this, depending on the REST API."

Meeting security and operational challenges

The introduction of Splunk has enabled RIKEN to do high-speed searches and respond quickly to security and operational challenges. The organization is using the log data to track and analyze network failures in the server system, proactively investigate and address these issues, and improve uptime across the three different systems. In addition to this, RIKEN is using Splunk dashboards to visualize system conditions and optimize job scheduling.

"Splunk Enterprise provides the easy operability of an RDB, and because it can perform high-speed log searches, I felt it was very convenient. When I want to do a quick examination, it serves as a very useful tool. K is a huge system so we can't predict what might happen, but the introduction of Splunk allows for swift response, which gives us a good sense of security."

Dr. Fumiyoshi Shoji, Deputy Director
Operations & Computer Technologies Division
RIKEN Advanced Institute for Computational Science