splunk> listen to your data™

CASE STUDY

Splunk® at Manitoba Hydro

Exchange App Helps Power Data Convergence

Manitoba Hydro

"With Splunk you can create scripts and indexes to capture any data or output, and then do whatever you want with that data. It's the unlimited flexibility that really sets Splunk apart."

James Klassen
Exchange Administrator, Manitoba Hydro

OVERVIEW

INDUSTRY
- Power utility

SPLUNK USE CASES
- Data Convergence for 360° View
- Exchange Monitoring
- Exchange Reporting
- Exchange Security and Alerting
- Compliance Management
- Troubleshooting and Analysis

BUSINESS IMPACT
- Avoiding up to $50,000 in licensing and maintenance costs over five years by eliminating legacy tools
- Avoiding additional software licensing related to clean-up of Public folders and other projects
- Enabling Exchange administrators to focus on value-added projects by reducing time spent on mundane troubleshooting from hours to minutes
- Correlation of data among multiple, mission critical servers now done from single system

DATA SOURCES
- Applications logs: Microsoft Exchange 2010, Blackberry Enterprise Server
- Security logs: Cisco IronPort

SPLUNKBASE APPLICATIONS
- Splunk App for Microsoft Exchange
- Splunk Cisco Security Suite
- Splunk App for Cisco IronPort
- PowerShell Search Cmdlet

The Business

Manitoba Hydro® is the electric power and natural gas utility for the province of Manitoba, Canada, serving more than 543,000 electric and 267,000 natural gas customers. Approximately 98% of the electricity it produces each year is clean, renewable power generated at 14 hydroelectric generating stations.

Challenges

Manitoba Hydro is a Crown Corporation and closely regulated by the provincial government. The company is the sole commercial provider of electrical power to the province and is an integrated operation, combining generation, transmission and distribution. Manitoba Hydro is also a major exporter of power to other Canadian provinces and the United States.

With 6,300 employees distributed across multiple locations throughout the province, communications applications and systems are mission critical. Among the most critical of these systems are the company's Microsoft® Exchange and Blackberry® Enterprise Server messaging environments.

Responsive monitoring, alerting, reporting and troubleshooting have long been a priority for Manitoba Hydro's messaging team. Before discovering Splunk® Enterprise™, the messaging team relied on several tools and homegrown scripts to help reduce the time required to solve system problems.

In early 2010, in the midst of its transition from Exchange 2003 to Exchange 2010, the Exchange administration team discovered some shortcomings in their monitoring solutions. "We were using another tool for monitoring and alerting," notes James Klassen, Exchange administrator for Manitoba Hydro. "However, the vendor moved some of the features we were dependent upon from the original tool to a new product, which would have required us to purchase this new product as well. Also, I wasn't happy with the rising software maintenance costs."

Enter Splunk

Klassen and his team saw in Splunk Enterprise a single system that could encompass all of the company's current needs and accommodate any additional data going forward. Soon after Klassen began experimenting with Splunk software he learned of a new beta test program for the Splunk App for Microsoft Exchange. The new app, in combination with Splunk Enterprise, promised to allow Manitoba Hydro to index, search and analyze in real time unlimited amounts of data from Exchange servers as well as other systems.

"I submitted many feature requests and even my own code as part of the beta program," Klassen notes. "The Splunk development team incorporated much of our input into the final product. There's even a management report built into the App that is modeled on one of our monthly reports, which is very nice for us and others."

Breakthroughs

Data convergence leads to rapid ROI

Manitoba Hydro deployed Splunk Enterprise and the Splunk App for Microsoft Exchange as its central system for collecting, indexing, searching and reporting on machine data from virtually any and every source. By eliminating three previous tools and the need for additional solutions, Manitoba Hydro estimates it will avoid nearly $50,000 over the next five years in software licensing and maintenance costs.

The Splunk App for Exchange includes more than 50 dashboards and reports, including a built-in dashboard for monitoring public folders within Exchange 2010. Klassen and his team plan to use this dashboard to help phase out public folders.

"Splunk and the Splunk App for Exchange tell us exactly where data are located, when it was last accessed and other statistics. In fact, we expect that Splunk will save us from having to purchase another product to help us find obsolete public folder data that can be deleted—that was one of the first features I noticed and it really blew me away."

Message tracking made easy

The Manitoba Hydro messaging environment includes more than two dozen Exchange servers, Blackberry Enterprise servers and Cisco IronPort Email Security Appliances (ESA). The firm leverages Splunk, the Splunk App for Exchange, Splunk Cisco Security Suite and the Splunk App for Cisco IronPort ESA to provide a single, cohesive view that cuts troubleshooting from hours to minutes.

"We used to have to go to many different application and server system logs trying to figure out patterns or track messages," Klassen says. "It's a time-consuming pain to do Exchange hub tracking and log into each server separately. Now, all of those logs are in Splunk and we can search them quickly in one place.

Alerts, reports and dashboards

Using a mix of both homegrown and built-in alerts, reports and dashboards, Klassen and his team save time and have improved overall reliability in keeping with the mission critical status of the messaging environment.

Alerts and reports include:

- A script that pings Exchange every 30 seconds to ensure availability
- Backup reports every morning list completions and failures
- Summaries of hourly, daily, weekly and monthly performance monitoring
- Alerts for database dismounts, disk space, reputation status, server reboots, database failures and RBAC group changes

Custom applications

Klassen and his team are also using Splunk to help the Manitoba Hydro IT support group solve Blackberry user problems. The team built an application using .Net and the Splunk PowerShell Search Cmdlet that initiates a remote connection to gather statistics on users and public folders from Exchange and Blackberry servers into a dashboard.

Free Download

Download Splunk for free. You'll get a Splunk Enterprise license for 60 days and you can index up to 500 megabytes of data per day. After 60 days, or anytime before then, you can convert to a perpetual Free license or purchase an Enterprise license by contacting sales@splunk.com.

250 Brannan St, San Francisco, CA, 94107 info@splunk.com | sales@splunk.com 866-438-7758 | 415-848-8400 www.splunkbase.com