Orient Overseas Container Line Limited (OOCL) Gains Improved Operational Visibility Into Infrastructure and Applications

Executive summary

Headquartered in Hong Kong, OOCL is one of the world's largest integrated international container transportation and logistics companies, with more than 320 offices in 70 countries. OOCL is also an industry leader in the use of information technology and e-commerce to manage the entire cargo process.

OOCL needed a solution that could enable it to correlate data outside system silos and link up all IT components and business processes with end-to-end visibility and near real-time analysis. Since deploying Splunk Enterprise, the company has seen benefits including:

- Enhanced logistics reliability
- Full operational visibility
- Optimized service

Why Splunk

OOCL is one of the leading international carriers serving China, providing a full range of logistics and transportation services throughout the country. There is a high volume of data exchange within OOCL's daily operations, such as transactions for bookings and container movement events. Data flows towards an integration gateway in standard EDI or in XML format and is transformed into internal XML schema before passing through various system components for further processing. At the end, the message is formulated and sent back to external parties as a "reply" or "confirmation of order." Full monitoring of this process requires OOCL to capture the events entering and leaving each system component, while correlating and analyzing system log files and database records to identify exceptional cases.

OOCL had many different proprietary solutions and open source systems running across its IT environment. The systems ran independently and were being monitored with a patchwork of self-developed tools on separate platforms, making it very time-consuming for system administrators to generate an all-in-one status report. Troubleshooting was also reactive and there was little to no visibility into "choke points" across the IT infrastructure as a whole.

Industry
- Transportation and logistics

Splunk Use Cases
- Business analytics
- IT operations

Challenges
- Needed to monitor, correlate and analyze a high volume of data across infrastructures and systems in near real time
- Numerous solution platforms made it difficult and time-consuming to create consolidated reports
- Lack of end-to-end operational visibility into IT infrastructure and "choke points"
- Troubleshooting was reactive, not proactive

Business Impact
- Enhanced logistics reliability thanks to near real-time data analysis capabilities
- Improvements to container transport and logistics services from more seamless information flow
- Full operational visibility and near real-time insights on service integrity
- Hassle-free system administration
- Effective troubleshooting capabilities thanks to big data analysis
- Better business risks management from early discovery of production problems and "choke points"

Data Sources
- Windows, Linux/Unix servers
- Application servers
- Databases
- Enterprise service bus
- Self-developed applications

Splunk Products
- Splunk Enterprise

OOCL knew it had to establish a near real-time, end-to-end monitoring framework to meet its business service requirements. After evaluating other datacenter monitoring and enterprise application integration solutions, OOCL decided to deploy Splunk Enterprise for its flexibility in correlating all the company's system and application monitoring data to meet the company's critical business needs.

Full operational visibility into information flow

The Splunk platform meets OOCL's needs by enabling system administrators to understand each "milestone" in the information flow and monitor end-to-end latency and transaction volumes. By comparing the "moving average" figures automatically calculated from historical data, potential problems can be discovered and any event stuck in any system can be flagged for attention well in advance.

Thanks to the Splunk platform, OOCL now has full end-to-end operational visibility across its infrastructure and applications, and is able to identify problems in near real time. OOCL's administrators have been able to integrate disparate systems and build dashboards to provide a single-pane-of-glass view into business operations while enjoying hassle-free systems administration convenience with intuitive, flexible and easy-to-integrate analytic tools. This efficiency has led to considerable time savings for the team and allowed OOCL to free up development resources for building the monitoring platform.

Optimized service with proactive IT monitoring

By correlating systems and business processes within Splunk Enterprise, OOCL can monitor IT health with full visibility into daily operations and end-to-end business service levels. Choke points and production problems are revealed in near real time, troubleshooting is simplified and business risks are

> "The Splunk platform offers unprecedented flexibility and ease of use. Its well-integrated big data engine not only opens up new horizons for understanding and monitoring system health but also enables near real time, end-to-end monitoring and analysis of our logistics information flow and business service levels, which we've never been able to do before."

Gen Ho
Manager – Technology
Information Services Department,
OOCL

minimized. Production problems that were previously tackled reactively (or overlooked entirely) by traditional tools are now discovered proactively where preventive measures can be taken well in advance. As a result of the more seamless information flow and reliable logistics operations, OOCL's overall container transport and logistics services have greatly improved.

Unlimited innovation, unlimited possibilities

The flexibility, scalability, ease of integration and processing power of the Splunk platform enables OOCL to correlate any text-based data sources for analytic purposes. In addition to backend systems monitoring, OOCL is now working on the extension to cover front-end applications for 100 percent client-to-server visibility. This will enable the IT team to monitor client application performance and identify any bottlenecks within the application stack. By analyzing user behavior and usage patterns, the OOCL IT team is developing innovative ideas for service optimization, with Internet of Things and mobile intelligence initiatives now in the pipeline.

Download Splunk for free or get started with the free cloud trial. Whether cloud, on-premises, or for large or small teams, Splunk has a deployment model that will fit your needs.

Learn more: www.splunk.com/asksales   www.splunk.com