Seamlessly Migrating to Splunk Cloud

CUSTOMER OVERVIEW

One of Australia's leading banking and financial institutions, servicing over 10 million customers and employing more than 30,000 workers.

Industry:
Banking & Finance

Primary Software/Solution:

- Splunk Cloud
- Splunk Enterprise Security

THE SITUATION

JDS was engaged by the customer to assist with a complex Splunk Cloud migration which was encountering complications and missing milestones. JDS has existing experience with, and knowledge of the customer's environment, and their expertise was pivotal in the design, strategy, scoping and migration of the on-premise platforms to a single Splunk Cloud instance.

THE SOLUTION

JDS worked with Splunk architects and the client to design a strategy to migrate the customer's on-premise Splunk environments to Splunk Cloud. This involved:

- Vetting 400 apps to ensure supportability with Splunk Cloud
- Re-architecting the customer’s index structure to improve search performance and promote cross-functional team collaboration
    - Developing automation scripts to deploy Splunk Forwarders on all Windows and Linux servers
- Creating a framework for detecting and removing Personally Identifiable Information (PII) data from being ingested into Splunk
- Developing a custom alert action to tightly integrate Splunk and the client’s existing ITSM environment

> "The JDS team were constructive, supportive and provided all the technical leadership and acumen necessary to shape up this work. Having JDS involved from the beginning was instrumental as they led the outcomes based on Splunk best practices and industry wide knowledge and experience."

THE PROCESS

JDS & Splunk held frequent workshops with the customer to gather requirements and agree on the scope. From the requirements provided, JDS created a project plan, using collaborative daily stand-ups with the customer, to discuss progress and blockers. As well as working with the customer’s Splunk engineers and project team, JDS worked with SMEs & support staff from various departments across the enterprise to ensure a successful plan was implemented.

KEY CHALLENGES

- A number of legacy applications required analysis and updating prior to being migrated to Splunk Cloud.
- Sophisticated automation recipes were needed to deploy Splunk to every Windows and Linux server.
- Production and non-production on-premises platforms had to be consolidated into a single cloud instance.
- Over 450 indexes to be consolidated into 65 indexes with updated Splunk searches to reference new index names.
- A large, complex enterprise environment with up to 750 daily users.

> "With the team of experts from JDS, we could safely and securely migrate over 120 applications from on-premise to Cloud in less than 3 months. This was a massive effort from the team and I would like to thank everyone involved."
>
> *- Customer Program Director*

THE OUTCOME

As a result of the successful migration efforts, the customer was able to shut down the on-premise Splunk platforms and achieve the planned savings from their hosted Splunk platform.

They were also able to realise significant savings by moving to Splunk Cloud, allowing them to rationalise other logging platforms and address a significant backlog of applications.

Due to the resulting additional capacity, the customer was able to immediately begin a number of projects to onboard new use cases, such as migrating their SIEM monitoring solution to Splunk Enterprise Security.

ABOUT JDS

Established in 2003, JDS Australia delivers specialist services and leading capabilities in a set of technologies to ensure critical IT systems work.
Employing the AIOps approach, JDS focuses on Observability, Security, Service Management, Quality Assurance and Automation in order to make sense of complex IT environments, optimise the user experience and enable positive business outcomes.
With an entirely local team of 90+ employees, JDS has the trusted skills and experience to ensure IT works and Australian business carries on.

KEY INTERACTIONS

- **Information Security** - To ensure information and infrastructure were secured according to customer & APRA requirements
- **Risk** - To ensure appropriate controls were in place to meet the customers' requirements
- **DevOps** - Provided requirements on what the Automation scripts needed to do
- **Networking** - To ensure connectivity to Splunk Cloud as well as configuring internal load balancers
- **Solutions Architects** - Worked collaboratively to design a solution that incorporated Splunk best practices while using the customer's tooling and standards.
- **Splunk Users** - Advice to users on how to create efficient, performant and engaging dashboards, compatible with Splunk Cloud.