


THE
CLIENT

Department of Health and Human Services

Our systems integration partner was in the early phases of implementing and maintaining Splunk IT Service Intelligence (ITSI) with one of the Department of Health and Human Services (HHS) agencies whose mission is to improve health care to people who are geographically isolated, economically or medically vulnerable.

The key project objective was to monitor the applications that different entities (applicants/grantees, grantors, auditors, consultants/experts, vendors, technical analysts) used to access, review and process a variety of electronic handbooks.

At the time, the project team consisted of four consultants, and our systems integration partner was looking to add a senior Splunk ITSI Developer to the team.


THE
SUPPORT

- Splunk ITSI
- Clustered Splunk
- Splunk DB Connect
- Data Ingestion
- Data Onboarding of Oracle DB
- Reports/alerts
- Java
- Python
- Windows, Linux
- Data Science


THE
CHALLENGE

One of the key responsibilities of our integration partner was to collect and monitor service intelligence for five enterprise applications. They were also in the process of adding Splunk DB Connect to monitor the performance of the structured databases.

As a result of this new effort to add Splunk DB Connect, our prime integration partner had a critical need to add a senior Splunk developer who could not only guide the junior team members, but also make an impact on new development

features and functionality.

This unique blend of technical and leadership skills required an expert who could quickly consume the system documentation, then jump right in and help develop new functionality.



THE SOLUTION

After a quick scan of our local Splunk network, our recruiting team found that there was a limited Splunk candidate talent pool with Federal experience. Therefore, our team expanded the search to identify candidates with deep commercial experience.

After an aggressive national search, we identified a strong Splunk developer with over 12 years of IT experience, which included over seven years of Splunk. What impressed us most about this candidate was his strong understanding of technology combined with his solid communication and leadership skills.

Our prime integration partner moved quickly to conduct a round of in-depth interviews. After debriefing with our team, they gave us the green light to add him to the team. After passing an agency-specific background check, our consultant was able to join the project team. As anticipated, he was quick to pick-up the scope of the project through an in-depth review of the existing documentation and was able to contribute in the following areas:

- Manage a team of three Splunk ITSI Developers
- Gather client requirements, assign to team members and monitor tasks
- Manage SLA's to prioritize and deliver tasks on time
- Plan, deploy, manage, and administer the ITSI app in a clustered Splunk environment
- Oversee the LOE/planning and conduct service decompositions, while collaborating with team lead for requirements gathering
- IT Service Intelligence (ITSI) app installation / Glass tables configuration
- Data ingestion of various data sources (app/db)
- Data onboarding of Oracle DB logs and translate/re-create the reports/alerts in SPL from SQL scripts
- Create custom apps (TA's) for data ingestion – with custom props.conf
- Manage/update forwarder configurations
- Create reports/alerts and KO's



THE SUCCESS

Our senior Splunk developer played a key role in monitoring and rolling out the database using DB Connect. He also played a key role with data ingestion of unstructured data using ITSI.

As a result of his effort and analysis, the Federal agency made the decision to scale up those areas of the infrastructure that were identified by Splunk ITSI as major bottlenecks. As a result, the user experience was completely enhanced and major reduction in application lag times were realized, especially during the peak access periods. As an additional benefit, the federal agency gained insights into the overall health of the applications and as a result, will be able to track it over time.