Data & Log Analytics

PROJECT SPECS

PROJECT TYPE: Data Analytics

TECHNOLOGIES: Splunk

SERVICES PROVIDED: Data & Log Analytics

TEAM:

Data Analytics Engineer
Project Manager/ Business Analyst

Duration: 6 months

TESTIMONIAL

"Riverstone is a professional business partner of exceptional quality. They provided several talents over the course of a few years and each one of them were a great fit for our needs. I would look to Riverstone to raise the bar in any QA organization, no matter how big or small."

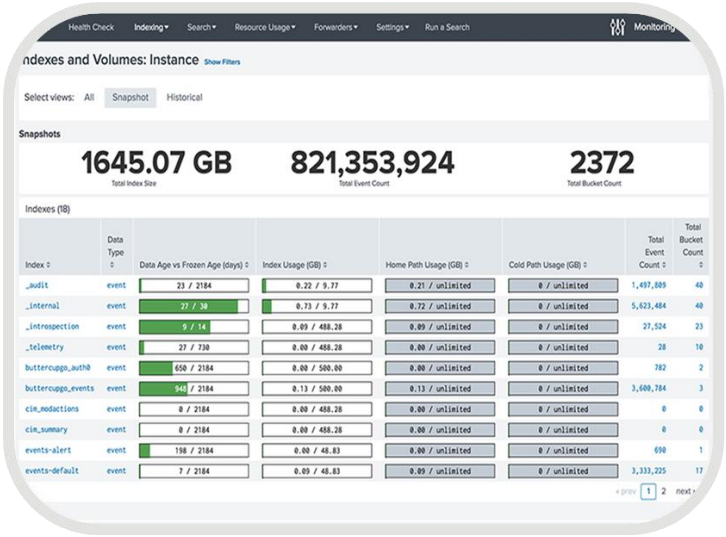
Muthu Arumugam,
VP of Engineering
Cambridge Blockchain

Client: WANdisco

Industry: Distributed Computing

Website: https://www.wandisco.com/

WANdisco, plc. is a public software company specialized in the area of distributed computing. WANdisco is also a corporate contributor to Hadoop, Subversion and other open source projects.



BUSINESS CHALLENGE

- To build data processing pipelines that ingest, validate, transform and load data quickly and efficiently
- To build a system which expose intuitive APIs and interfaces for querying and investigating large data sets
- To build a system to process data with high peak traffic and short SLAs

OBJECTIVE

To provide Splunk development services to prototype, document and deploy a Splunk log ingest and analysis solution that will include automation of log collection, filters, and a dashboard for per-case management, drill-down, and efficient identification of errors or anomalies via log searching.

U.S. Office:
5890 Stoneridge Dr. #209
Pleasanton, CA, 94588
1 - 925 -218 -0669

www.riverstonetech.com

Software@riverstonetech.com

KEY ACHIEVEMENTS

- Developed a log analytics application in ~6 sprints
- Data ingestion of large datasets & dashboards
- Created 5 different dashboards including performance analysis
- Introduced Auto-analysis feature for indexed logs
- Reduced trouble shooting time & effort significantly

SCOPE OF WORK

- Prerequisites and testing on log ingestion
- Automated log ingestion
- Creating dashboards & Use cases
- Identifying files not being ingested in Splunk
- Automated talkbacks and data ingestion
- Parsing & field extraction
- Performance analysis
- Dashboards/UI
- Platform upgrade

SOLUTION

- Real-time logs and with faster speed
- Generate report and alerts for the desired search
- Auto-analysis of indexed logs
- Detect when a critical system stops working
- Create knowledge objects for Operational Intelligence
- Visualize the graph based on actions
- User Monitoring
- Data and Application Monitoring
- Advanced Analytics
- Instant Reporting and Visualization

KEY MILESTONES

- Designed and built a **Network dashboard** to provided summary of network issues observed in log
- Observed REST API connection exception on UI Server
- **Transfer dashboard**: Creating a panel on file transfers with file size and transfer duration
- Included a drilldown to showcase reason behind the exception in transfer
- **Task Executions Dashboard:** To summarize and list down all the tasks with task type
- **Repair Dashboard:** Created a drill down from failed repairs and co-relate the same with proposal IDs
- Splunk app for **Slack**

U.S. Office:
5890 Stoneridge Dr. #209
Pleasanton, CA, 94588
1 - 925 -218 -0669

www.riverstonetech.com

Software@riverstonetech.com