Data Lake Migration from Elastic Stack (ELK) to Search Anywhere Framework

business intelligence · cybersecurity · IT operations

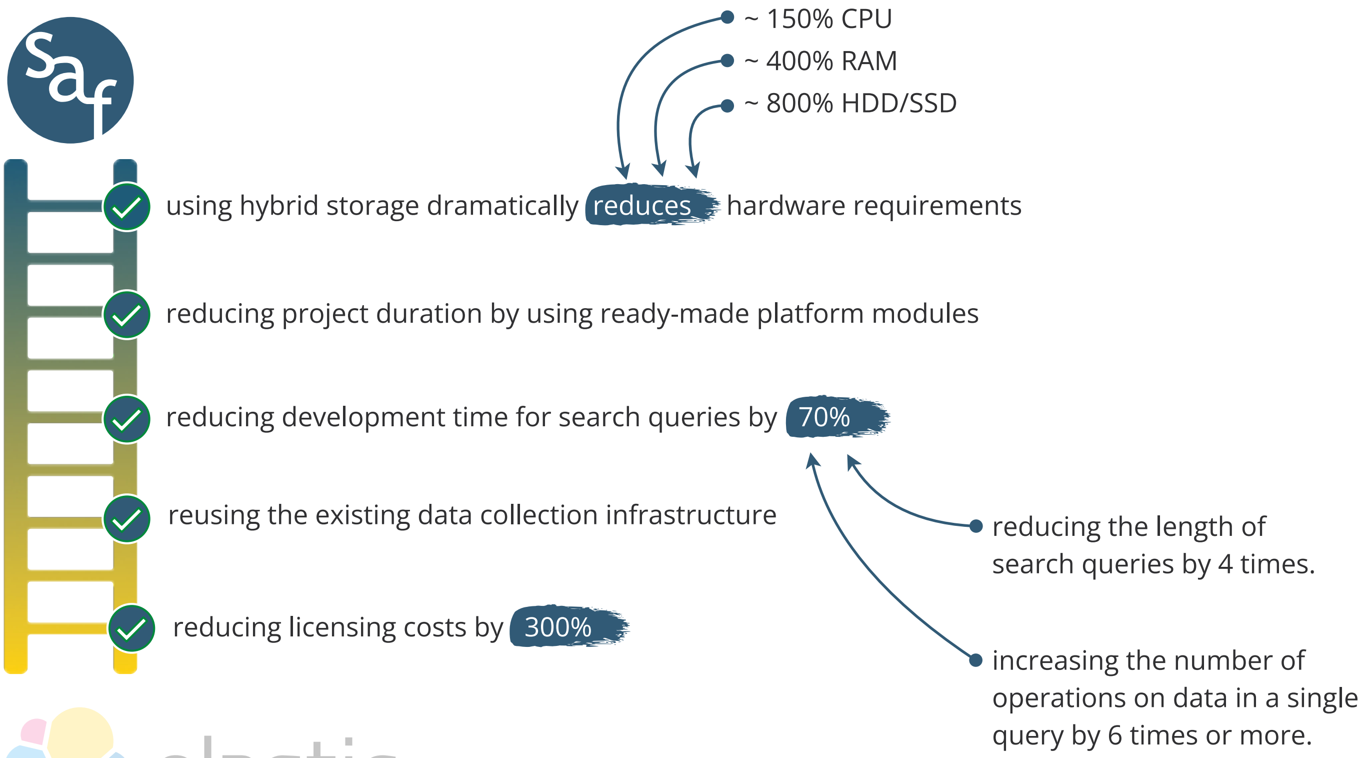
Goals

reduction of Total Cost of Ownership (TCO) for the monitoring system, enhanced search analytics capabilities for the data lake. Decreased time and costs for development and enhancement of machine data analysis projects.

Tasks

- hardware requirements reductions
- monitoring system licensing costs optimization
- reuse of data collection infrastructure and data model/schema
- reduction of staff workload by simplifying the data analysis process
- combining events from different data stores in a single query with complex logic
- post-processing of events during the request process through pipelined execution

Results



~ 150% CPU

~ 400% RAM

~ 800% HDD/SSD

✓ using hybrid storage dramatically reduces hardware requirements

✓ reducing project duration by using ready-made platform modules

✓ reducing development time for search queries by 70%

reducing the length of search queries by 4 times.

increasing the number of operations on data in a single query by 6 times or more.

✓ reusing the existing data collection infrastructure

✓ reducing licensing costs by 300%