

Secure and scalable log management solution by leveraging bi-directional cross-cluster replication of Elastic for a leading German car manufacturer.

**100 GB/Day**  
Data Ingestion

**18 TB**  
Data Retention

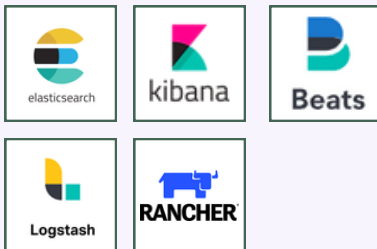
**16 Nodes**  
Cluster

## CLIENT

The client is a leading German luxury and commercial automotive manufacturer.

The client also offers digital services for fleet management, card payments and insurance brokerage.

## TECHNOLOGY STACK



## PROJECT CONTEXT

The client offers various digital services, and these services and applications used independent solutions to collect logs.

The client identified this as a potential area for improvement as the setup was not scalable and had been facing availability issues.

The team required a low-maintenance, secure log management solution to house logs from several services, applications and teams with granular role-based access control.

## PROJECT REQUIREMENTS

- On-premise Elasticsearch deployment.
- Set up ingest pipelines to ingest 100GB/day data from various digital services, applications and development teams.
- Plan for 18 TB data retention distributed across hot, warm and cold data storage tiers.
- Set up Kibana with role-based access control and develop bespoke dashboards to meet each team's requirements.
- Ensure high availability & scalability of the system.

## SOLUTION DELIVERY

- The Bi-Directional cross-cluster replication feature of Elasticsearch was leveraged to ensure high availability.
- Provided deep expertise on corporate network tools and configurations for data ingestion and ensured that all high-availability cases are covered in the setup.
- Implemented cluster design, capacity planning and role-based access control for production and non-production environments