ALTOROS™

Kubernetes | Microservices

Enabling Security Compliance for a Kubernetes Cluster Behind an Insurance App

One of the world's oldest insurers turned to Altoros to validate an architecture of a Kubernetes cluster underlying existing applications.

6
nodes

3
masters

CIS
security

The Customer

Based in Switzerland, the company is an insurer with 100+ years in the global market. The customer serves multiple lines of insurance: health, travel, property, life, etc. The organization employs thousands of employees in 200+ countries with billions in total revenue.

The Need

Considering to implement Kubernetes as a container orchestration platform, the customer wanted to validate its architectural approach behind the cluster. Collaborating with Altoros, the company sought an independent review of the architecture developed, as well as consultancy around enabling logging/monitoring and security across the Kubernetes cluster.

The Challenges

Under the project, the team at Altoros had to address the following issues:

- The Kubernetes cluster had to comply with the CIS security guidelines. However, the chosen implementation setup was not mature enough to conform with the practices outlined;
- The logging/monitoring functionality across the cluster had to be automated.

The Solution

With reference architecture supported by exhaustive recommendations as a deliverable, the team at Altoros provided extensive consultancy across four major topics: **microservices** development, **best practices** for Kubernetes implementation, cluster **logging/monitoring**, and **security**. Microservices. Our engineers introduced the customer to the concept of 12-factor app principles used for building microservices. Outlining the difference from a monolith architecture, developers at Altoros delivered an overview of concepts such as stateless services, lightweight/loosely coupled communication, persistence, etc.

Kubernetes best practices. Initially, the customer wanted to deploy Kubernetes on a 4-node cluster with a single master node, while the official documentation of the platform recommends to have at least 3 masters to achieve high availability. Experts at Altoros elaborated an installation of 6 nodes with 3 masters to ensure cluster failover. Our team also exemplified how to deploy services in seconds instead of hours to days when done manually.

Cluster logging/monitoring. Suggesting the ELK stack (Elasticsearch, Logstash, and Kibana), engineers at Altoros demonstrated how to automate logging and monitoring across the Kubernetes cluster. Through multiple technical sessions, our developers mentored the customer's in-house team on such practical issues as how much memory to assign to a logging/monitoring component, how to size it, and how to troubleshoot the installation.

Security. To comply with the CIS security guidelines, the consultants at Altoros detected the noncompliant parts under the developed architecture, prioritized them by severity, and worked out an optimization strategy. In iterations, our developers assisted the customer in implementing the necessary changes related to container scanning, securing configurations, etc.

Finally, the team at Atoros delivered a set of recommendations on further improvements related to enabling scalability, continuous integration/delivery, advanced configuration management, and more.

The Outcome

Partnering with Altoros, the customer has got an independent validation of the architecture behind a 6-node Kubernetes cluster to be implemented. Introduced to the best practices, the company was able to elaborate a security strategy compliant with the CIS guidelines, to enable automated logging and monitoring across the cluster, and to troubleshoot installation issues. Finally, the organization got exhaustive recommendations on the overall Kubernetes implementation, as well as on how to enable scalability and continuous integration/delivery.

Brief results of the collaboration

- With a developed architectural approach, the customer implemented a production-grade Kubernetes cluster of 6 nodes and 3 masters compliant with the CIS security guidelines.
- The company achieved automation across cluster logging and monitoring.
- With extensive recommendations, the organization worked out a roadmap for improving scalability, managing configurations, and enabling continuous integration/delivery.

Technology stack

Platform	Kubernetes
Frameworks and tools	Docker, Elasticsearch, Kibana, Logstash, Puppet, Ansible, Chef, Terraform, Jenkins, Istio