



OPCITO TECHNOLOGIES

Configuration Management using HashiCorp Vault

About The Customer

The customer is a leading business and data analytics service provider. These services enable businesses to understand various business operations, customer needs, and future requirements and help them build online reputation and reviews.

Business Challenge

The application used by the client has more than 20 microservices that continuously analyze real-time and historical data. Each microservice has its vital configuration files. The secret configuration is maintained in YAML files (around 30+ files). These configuration files are part of the application source code. Storing credentials in the YAML file is insecure and maintaining the configuration files across the environment (development, staging, pre-production, production, etc.) is a difficult task with a risk of mistakes while copying the files manually.

How Opcito Helped

After careful analysis of the microservices network, functional aspects, and interdependencies, the Opcito team suggested a solution that used HashiCorp's Vault. HashiCorp Vault is an open-source tool that supports Docker containers, which helps to achieve availability, scaling, and monitoring.

The Opcito team reviewed all the configuration files and designed a scalable and modular configuration management solution. Configuration is structured based on an environment; all standard configurations are maintained globally.

We leveraged the vault authentication mechanism to use the existing Lightweight Directory Access Protocol (LDAP). As a result of this integration, a centralized user management system is created, which will help the admin control the access of different users to the vault and assign the required roles and policies.

All configuration files are moved to the vault in a secret backend in the form of a key/value. We have designed environment-wise vault backend paths – separate global paths for development, staging, testing, production, etc.



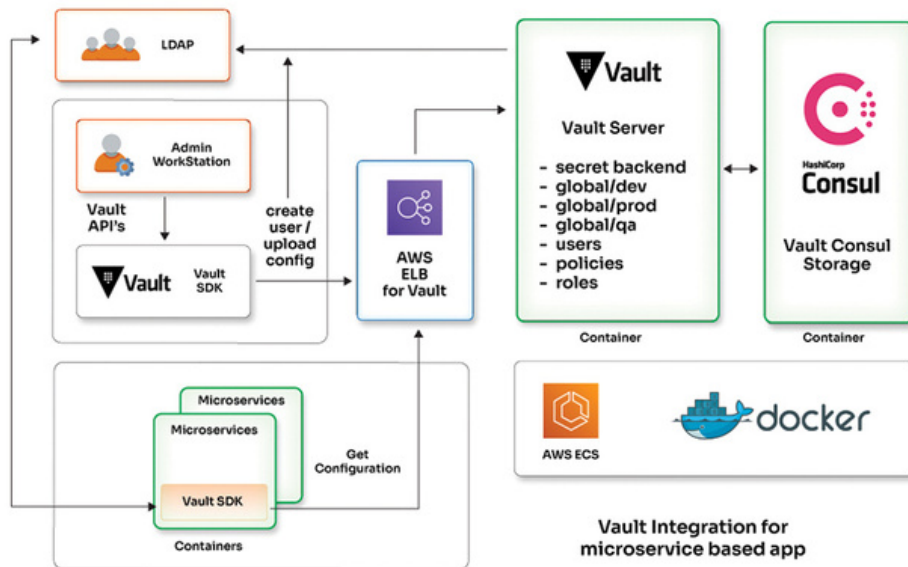
This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Opcito Technologies.

India office +91 (20) 6712 4100

US office +1 (650) 772 4442

The vault admin will run the command exposed by the ruby library to create the user and copy the configuration from global to the required user's environment with assigned roles and policies. The user can only see and update the configuration uploaded on the dedicated user's path using their credentials.

We removed all config files from microservices. The implemented vault library is used to get the required configuration from the vault using the vault user's credentials.



Technologies, Tools, and Platforms used

AWS ECS

AWS ELB

HASHICORP CONSUL

HASHICORP VAULT

DOCKER

Benefits

SECURE RBAC MANAGEMENT

Provided a secure centralized management system with Role Based Access Control (RBAC) list, to control user accessibility

ENVIRONMENT CONFIGURATION

Easy management configuration across the environments (Development, Production, Staging, etc.)

SCALABILITY

Centralized AWS ECS, which is used for vault and consul container for scalability and durability of the application

CREDENTIAL SECURITY

Eliminated the need to store YAML files, enabling developers to start their service without worrying about credentials security

About Opcito

At Opcito, we believe in designing transformational solutions for our customers, start-ups, and enterprises, with our ability to unify quality, reliability, and cost-effectiveness at any scale. Our core work culture focuses on adding material value to your products by leveraging best practices in DevOps, like continuous integration, continuous delivery, and automation, coupled with disruptive technologies like containers, serverless computing, and microservice-based architectures. We also believe in high standards for quality with a zero-bug policy and zero downtime deployment approach.



This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Opcito Technologies.

India office [+91 \(20\) 6712 4100](tel:+912067124100)

US office [+1 \(650\) 772 4442](tel:+16507724442)