Contribution ID: **62** Type: **Lightning Talk 8 mins**

Secret management service for EGI Infrastructure

Tuesday, 20 September 2022 17:30 (8 minutes)

Applications in EGI Infrastructure may need different secrets (credentials, tokens, passwords, etc.) during deployments and operations. The secrets are often stored as clear texts in configuration files or code repositories that expose security risks. Furthermore, the secrets stored in files are static and difficult to change/rotate. The secret management service for EGI Infrastructure is developed to solve the issues.

The secret management service is designed as follows:

- Non-intrusion: Operates as a stand-alone service, no extra efforts from site admins to support the service, no additional permissions are needed for users.
- Simple usage: Authentication via OIDC tokens from EGI Check-in, no extra credentials are required. The service is based on Hashicorp's Vault which is well-known in industry, with many client tools and libraries.
- High-availability: Service instances are distributed on different sites, without single point of failure. A generic endpoint https://vault.services.fedcloud.eu:8200 is dynamically assigned to a healthy instance via Dynamic DNS service.

At the moment, the service is in public beta testing, full production operation is expected in September 2022.

The service is available at the generic endpoint https://vault.services.fedcloud.eu:8200/. The detailed designed of the service is available at [1], and user guide is available at [2].

1. https://docs.google.com/document/d/18uqpZ2AkdAm9WMsDfQgDnv4Y4qMyoUpBilsLiHPrfvk/edit?usp=sharing
2. https://docs.google.com/document/d/11QKGQjJFGiTYCrs2fLazrFBEg2lfOgzpcJIuIKq02CE/edit?usp=sharing

Any relevant links

Service endpoint: https://vault.services.fedcloud.eu:8200/
Service design: https://docs.google.com/document/d/18uqpZ2AkdAm9WMsDfQgDnv4Y4qMyoUpBilsLiHPrfvk/edit?usp=sharing
User guide: https://docs.google.com/document/d/11QKGQjJFGiTYCrs2fLazrFBEg2lfOgzpcJIuIKq02CE/edit?usp=sharing

Topic

A Federated Compute Continuum

Primary authors: TRAN, Viet (IISAS); ANTONACCI, Marica (INFN); LOPEZ GARCIA, Alvaro (CSIC)

Presenter: TRAN, Viet (IISAS)

Session Classification: Lightning Talks: Security, Trust & Identity

Track Classification: Security, Trust & Identity