Contribution ID: **5** Type: **Practical Demonstration (15')**

Secret management service for EGI infrastructure

Thursday 13 October 2022 14:45 (15 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 by IISAS in cooperation with INFN and CSIC to solve the issues.

The Secret management service is designed as follows:

- **Usability:** A dedicated module of FedCloud client is developed to make the service works out of the box with very simple syntax. Authentication is realized via OIDC tokens from EGI Check-in, no additional registration, no extra credentials are required.
- **Advanced features:** Built-in support for secret values from files, export/import secrets to/from files in YAML/JSON formats. Encrypting/decrypting secret values on the fly on the client side greatly improves security and trust of the service.
- **Compatibility:** The service is based on Hashicorp's Vault which is well-known in industry, with many client tools and libraries. Software for service and clients are open-sourced with strong support from communities.
- **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.

The full documentation of the Secret management service is available at https://vault.docs.fedcloud.eu/.

Primary author: TRAN, Viet (Institute of Informatics SAS Slovakia)

Presenter: TRAN, Viet (Institute of Informatics SAS Slovakia)

Session Classification: IBERGRID Contributions

Track Classification: Development of innovative software services