

Enhancing the user life-cycle management management in EGI Federated Cloud

Thursday, 12 November 2015 11:00 (20 minutes)

Basic FedCloud user access scenario is composed of a VOMS server for authentication and authorization, and the site itself. Users with valid VOMS credentials are automatically created on sites. This solution is easy to deploy and manage but has several drawbacks if you need to support the whole user life-cycle.

In this presentation we will introduce Perun as an additional component in the described scenario. Perun is EGI Core Service for VO and group management, it also provides functionality for managing access to services. It supports the whole user life-cycle from user import and enrollment through user expiration and membership renewal to complete account deletion and deprovisioning from services. In addition, it supports linking of multiple external identities (federated identities, X.509 certificates, kerberos, ...) to one user account.

As a part of its service management capabilities, Perun can propagate user accounts to both VOMS and sites. VOMS will still be used as the authentication and authorization service. User data is managed centrally and then distributed to VOMS. For example, if the user wants to change her/his certificate, she or he is able to do it in one place even though he is a member of several VOs.

Active propagation of user data to sites enables users to change their preferences (e.g. contact e-mail) in one place, then the information is distributed to all sites without any further action required from the users. More importantly, it enables sites to know about expired or suspended users and take appropriate action, such as suspending or stopping their virtual machines. That substantially enhances security of Federated Cloud sites.

Primary authors: PROHAZKA, Michal (CESNET); LICEHAMMER, Slavek (CESNET)

Co-authors: PARAK, Boris (CESNET); SUSTR, Zdenek (CESNET)

Presenter: LICEHAMMER, Slavek (CESNET)

Session Classification: Current status and evolution of the EGI AAI