Perun VOMS provisioner

Slávek Licehammer

5th AARC Meeting, Athens

21. 03. 2017
Pilot

- Provide X.509 authentication for service
  - Utilize VOMS extensions in certificates
- Do not force users to manage X.509 certificates
- RCAuth.eu + Master Portal
  - Generates user certificates on the fly
  - Can include VOMS extension to the certificate
- Missing piece -> Get user DN to VOMS server
- RCAuth.eu generates user DNs with known algorithm
- Perun can compute RCAuth.eu DNs and provision them to VOMS server
• Built-in support for virtual organizations
  • Configurable application form
  • Delegation of rights to the end users
  • Access management for resources

• Group management
  • Configurable application form
  • Group manager role

• User management
  • Identities
  • Attributes
Push mechanism

- Provisioning tool
  - Way to deliver information about authorized users to the service
- Perun monitors changes within itself -&gt; push data to affected services
- Using standard format
  - SCIM, LDAP, JSON, XML, ...
- Using standard delivery protocol
  - SSH, HTTP, ...
- Benefits of push mechanism
  - Deliver data upfront first usage
  - Deprovisioning capabilities
VOMS provisioner

- Generate data in XML format
  - Complete state of users for VOMS server
- Send to VOMS server using SSH protocol
  - SSH key for authentication
  - Limited to only one command on the receiving side
- Script on VOMS server side to process the data
  - Read state of users from VOMS server using CLI interface
  - Parse XML and compare it with VOMS state
  - Change user stated accordingly using VOMS CLI interface
• Use of ELIXIR AAI infrastructure
  • Registration of users without X.509 certificates

• Access EGI Fedcloud infrastructure
  • Require X.509 certificate with VOMS extensions
  • Access using web portal
Demo - components

- RCAuth.eu Master Portal (elixir-cilogon-mp.grid.cesnet.cz)
- RCAuth.eu MyProxy (elixir-cilogon-myproxy.grid.cesnet.cz)
- CESNET VOMS server (voms1.grid.cesnet.cz)
- ELIXIR Perun Identity and Access Management system (perun.elixir-czech.cz)
- ELIXIR Proxy IdP (login3.elixir-czech.org)
- EGI FedCloud Demo portal (wuotan.ics.muni.cz)
(Show of the demo)

Described on: https://wiki.geant.org/display/AARC/PerunVOMSCILogonPilot
Thank you for attention