Perun VOMS CILogon pilot

- Introduction
- Detailed description
- Demonstrator Workflows

Introduction

If the infrastructure would like to provide services using X.509 authentication to the users without forcing users to have and manage their own X.509 certificates the CILogon service can be used. One of the AARC pilot deployed CILogon service under the RCAuth.eu label. RCAuth.eu service is able to request group membership and roles from VOMS service and inject them into the X.509 proxy certificate which is generated for the user. RCAuth.eu generates the X.509 certificates for the users on the fly, so there is no possibility to provision users' information into VOMS in advance. We have setup pilot which demonstrates combination of Perun, RCAuth.eu and VOMS to provide X.509 proxy certificates from RCAuth.eu with VOMS extensions. We have selected ELIXIR AAI infrastructure (https://www.elixir-europe.org/services/compute/aai) to pilot that use case.

Detailed description

You can find detailed information about RCAuth.eu in CILogon-like pilot. What is needed is to provision information about the users into the VOMS service. Perun (https://perun.cesnet.cz) as an IAM system is the core component which manages users, groups and resources. Users register into the Perun system where they are organised into the groups and also roles can be assigned to them. VOMS service uses X.509 DN as an identification of the users, so we need to know how the DN will look like of every registered user. Because the algorithm how the RCAuth.eu generated the DN is known we have configured Perun to be able to generate exactly the same DN for every registered user. Perun is then actively provision using push to the VOMS service all registered users and their group membership and roles information. When the user would like to request X.509 proxy certificate from RCAuth.eu, the RCAuth.eu contacts the VOMS service which already know the user, so it can reply with all the information about the user. User then have the X.509 proxy certificate with VOMS extensions which can be used for example in EGI fedCloud where user's membership is used for authorisation decision.

Demo consists of these 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)
- fedCloud Demo portal (wuotan.ics.muni.cz)

Demonstrator Workflows

<table>
<thead>
<tr>
<th>Accessing the fedCloud demo UI</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Initial page of the demo EGI fedCloud UI. User selects ELIXIR GUOCCI (w/ CILogon)</td>
</tr>
</tbody>
</table>

![WUOTAN](image_url)
2. User is requested to authenticate with ELIXIR Proxy IdP. User selects his/her home organisation from the list.

3. User authenticates with his/her home organisation.
User is asked to consent attribute release to the RCAuth.eu service.

User ends on the EGI fedCloud UI where he/she can manage virtual machines. EGI fedCloud UI calls remote cloud infrastructures and uses X.509 proxy certificate which was obtained in previous steps. X.509 proxy certificate contains VOMS extensions, therefore cloud infrastructures can do the authorisation decision based on the user VO membership.

Service definition in Perun system
EGI VOMS server (voms1.grid.cesnet.cz) is defined in ELIXIR Perun system.

We can see successful propagation of users from VO vo.elixir-europe.org to the EGI VOMS servers.

Technical details
Via VOMS admin UI we can check that it contains information about users propagated by the Perun system.

Detailed view on the X.509 proxy with VOMS extensions which is stored on the wuotan.ics.muni.cz, machine which hosts EGI fedCloud UI.