Identity, Entitlement and Access Management Working Team

ESGF F2F Workshop,

Washington DC, December 2016

Working team leads: Rachana Ananthakrishnan, Philip Kershaw

Members: Luca Cinquini, Aashish Chaudhary, Antonio Cofino, Katharina Berger, Carsten Ehbrecht, Georgi Kostov, James McEnerney, Mark Greenslade, Sandro Fiore, Maarten Plieger, Matt Pryor, Dean N. Williams

2016 Progress & Accomplishments

- Deploy OAuth 2.0 operationally with ESGF Identity Providers (IdPs) (July 2016).
  - A **new OAuth 2.0 Django-based implementation** was made and deployed at CEDA by Matt Pryor
  - A **generic ESGF deployment package** was created derived from the CEDA version
    - This includes an Ansible Playbook for complete automation of the deployment process. It is ready for incorporation into the ESGF installer
  - OAuth 2.0 functionality integrated into CoG by Lukasz
- Pilot integration of Live Access Server (LAS) with ESGF OAuth 2.0 service deployed at CEDA. (March 2016).
  - Successfully demonstrated.
  - Implements user delegation as previously demonstrated with the *KNMI Impacts Portal*
- Implement service discovery mechanism for OAuth 2.0. (May 2016)
  - We will use the existing Yadis mechanism used with ESGF until OpenID Connect is rolled out

2016 Missed Milestones

1. Deploy OAuth 2.0 operationally with ESGF Identity Providers (IdPs) (July 2016).
   - Missed **but** the Deployment package is ready for integration into the ESGF installer
2. Integration of Globus with ESGF OAuth 2.0 service (August 2016).
   - Missed: Globus doesn't support OAuth 2.0, integration is deferred until ESGF can migrate to OpenID Connect
3. Retire MyProxyCA (October 2016).
   - CEDA HTTP-based Short-Lived Credential Service (SLCS) replaces MyProxyCA
   - Missed: This needs to wait until 1) is complete.
   - The SLCS is part of the new ESGF OAuth package. It simplifies the installation dependencies since the MyProxy software is no longer needed.
4. Implement and integrate OpenID Connect into ESGF. (ongoing to December 2016).
   - Missed **but**: Pull requests to integrate OpenID Connect with Python OAuthLib were accepted paving the way for full OpenID Connect support for the ESGF IdPs
     - (The new ESGF OAuth service can be patched to provide full OpenID Connect)

2017 Roadmap

1. Retire OpenID 2.0. OpenID Connect service replaces it (March 2017).
2. Roll out OpenID Connect in operational federation (2017)
3. Improve user interfaces for registration and management of access restrictions
4. Refactor authorisation system (stretch goal)

- To complete 1) and 2) we must first port the ORP package from OpenID 2.0 to OpenID Connect
  - The ORP is a Java package which filters requests to TDS in the Data Node. It enforces login and authorisation.
  - The current OpenID sign-in interface is part of it. This must be updated to support Oauth 2.0/OpenID Connect protocol
- The user experience should remain the same:
  - Users keep the same user id and don't need to re-register when the new changes come into place.

Additional Resources Needed

- Progress has been made this year but it is slow.
- Significant work is needed to port the ORP code. (approx. ¼ FTE)
- Support will be needed from the Installation Team to complete integration of OAuth/OpenID Connect
- Improvement work to user interfaces (1/2 FTE)
- Once OpenID Connect migration is complete attention is needed to the authorisation system (1 FTE)
  - Work needed to investigate a solution to replace the current SAML interfaces and system for authorisation policies. OAuth 2.0/OpenID Connect could provide a basis
- The system cannot stand still: continuous development effort is needed to keep the system secure, up to date and make it easy to use and maintain

Community Feedback from Survey

- Underlines the points made in the previous slide:
  - Improvements are needed to user interfaces for registration and management of access restrictions

Collaborations Needed

- CEDA, Argonne for
  - integration of Globus
  - Completion of OAuth/OpenID Connect role out
- ENES partners and Compute WT for user delegation use cases.
  - KNMI Impacts Portal, Downscaling portal (University of Cantabria)
  - Compute Node
- User interface improvements
  - Need to determine who can work on this