iris

IRIS PAM module

Jens Jensen, STFC, IRIS collaboration

www.iris.ac.uk

08 Nov 2021

UKRI Science and Technology Facilities Council

History

- Forked from ICS-MU (Masarykova Univerzita)
- Cloud authorisation features by Will Furnell
- Prod’n refactor/hardening plus a few features – Jens Jensen
- Additional contributions from Brian Bockelman

Why the fork?

- Needed extra features for “cloud authorisation”
  - Project/group access
  - Cambridge wanted a bypass feature (see later)
- Currently it’s in the ‘jens’ branch
  - Need to merge into main as people often check out main

Refactoring

- Server certificate is checked
  - CA location configurable but defaults to /etc/grid-security/certificates
- Removing C-isms
  - C-style casts, NULL, unsafe printfs
  - C code (LDAP) builds as C, not as C++ (safer)
- General refactoring
  - curl, logging
  - More things are configurable
- More regression/unit tests
- Improved error handling/logging

Principles

- Refactor & harden
  - Modern C++ features for correctness and maintainability
- Staying close to upstream
  - Stayed with C++11
  - Stayed with JSON configuration file
  - Stayed with make as build (as opposed to switching to cmake)

Δfeatures list

- New authorisation methods (cloud/project) – Will Furnell
- Config debug, HTTP basic auth, QR optional – Brian Bockelman
  - `Debug' is now superseded by loglevel or PAM params
- Cambridge's bypass feature
  - LDAP lookup will bypass module (not a failure)
  - In which case PAM config falls back to password
  - (the fed PAM module must be *above* the password module)

Current Authorisation

- cloud:
  - A “project id” file is read from the IAM server
  - This file contains groups which should match one of the user’s groups
  - And the PAM user plus configurable suffix must equal OIDC user id
  - (Suffix allows all mapped users to be jjensen_iris, say, locally)
- group:
  - User must be member of specific group
  - And the PAM user plus suffix must match as before
- local:
  - PAM user and OIDC user id match explicit local mapping
- LDAP:
  - Configurable LDAP query using OIDC user id is successful

To do

- Rethink authorisation?
  - Refactoring kept functionality but some bits won’t scale well
  - More sophisticated local user mapping?
- Upstream (ICS-MU) has moved forward as well
  - Would be worth comparing and sharing
- Updated EOSC/appint interoperation guidance
  - Expressions of group memberships and roles
  - Make use of LoA
- Fix remaining tests
- Make build to RPM/DEB easier
- Incorporate major update of JSON submodule

Current Testing

- DiRAC test (www.dirac.ac.uk, part of IRIS)
  - Cambridge and Durham were volunteered to go first
- SCARF (STFC Scientific Computing HPC cluster) trial mooted
- Further deployment in IRIS
  - (Optional live demo here, if there's time)

- https://github.com/stfc/pam_oauth2_device/tree/jens
  - (eventually we will get round to merge with main branch)

Science and Technology Facilities Council