Second Token-based AuthN/Z Hackathon

Andrea Ceccanti
INFN CNAF

GDB
October 14th, 2020

The Second token-based AuthN/Z hackathon

https://indico.cern.ch/event/953075/

When: 16-17-18 September 2020, 15-18 CEST

Focus on DOMA TPC use cases and JWT profile compliance

Good and active participation:

- 27 persons on day one, ~22 on average each day

Many thanks to everyone for their work!

Objectives

DOMA HTTP TPC smoke tests supporting JWT authN/Z

WLCG JWT profile compliance test suite

- Audience restriction enforcement etc…

Group-based authorization flows for DOMA TPC

Discuss key topics

- local user mapping
- scope-based authZ policy management
- token handling in XRootD
- simplifying VO enrolment flows
- transitioning IAM in production for LHC VOs

DOMA HTTP TPC Smoke tests using JWT

https://github.com/paulmillar/http-tpc-utils

Checks that HTTP data management and TPC work as expected for a configurable set of endpoints and sends a daily report on the DOMA-TPC WG list

Extended to support fully X509-free auth

https://github.com/paulmillar/http-tpc-utils/pull/17

TODO:

Get daily report using WLCG VO token for authN/Z

WLCG JWT profile conformance test suite

A JWT profile compliance test-suite to assess conformance with the profile

- Check that issuer checks, signature checks, temporal validity, audience restrictions, path constraints, … are honoured by the implementations

The **token factory** (a mock token issuer) has been deployed at

https://tf.cloud.cnaf.infn.it

This gives the ability to create potentially malformed/expired tokens and will be used by the test suite to check JWT profile compliance (tokens are issued only to authenticated clients)

Requires integration at the SEs to assess compliance

WLCG JWT profile compliance test suite

First incarnation lives at:

https://github.com/indigo-iam/wlcg-jwt-compliance-tests

Implemented tests for:

- Audience restrictions
- Scope-based authorization
- Group-based authorization

TODO:

- Integrate token-factory for in depth testing of token validation
- Run in CI on GH actions
- Include RUCIO and FTS checks in the test suite

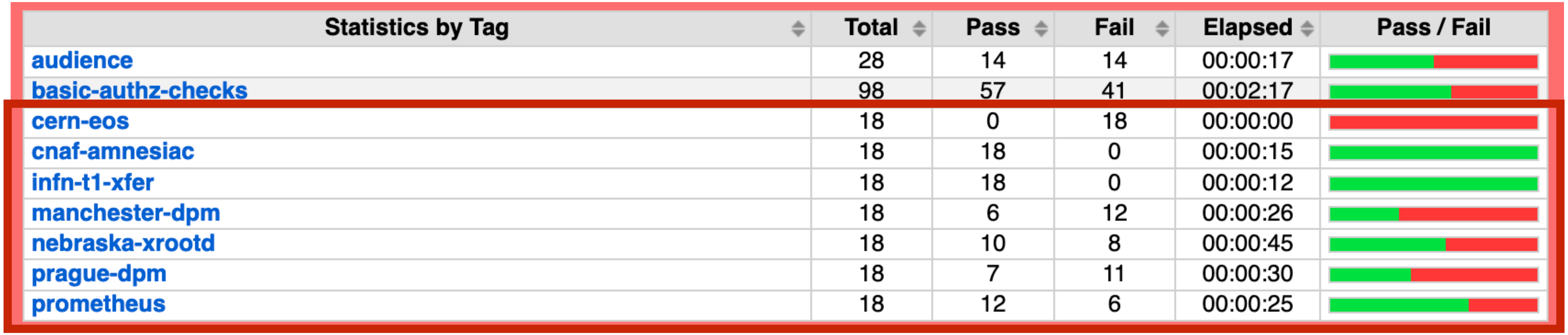
WLCG JWT profile compliance test suite: results

https://amnesiac.cloud.cnaf.infn.it:8443/wlcg/jwt-compliance-reports/

Access to results requires WLCG VO membership

Latest run results:

- https://amnesiac.cloud.cnaf.infn.it:8443/wlcg/jwt-compliance-reports/20201014_120115/joint-report.html



Statistics by Tag	Total	Pass	Fail	Elapsed	Pass / Fail
audience	28	14	14	00:00:17	🟩🟥
basic-authz-checks	98	57	41	00:02:17	🟩🟥
cern-eos	18	0	18	00:00:00	🟥
cnaf-amnesiac	18	18	0	00:00:15	🟩
infn-t1-xfer	18	18	0	00:00:12	🟩
manchester-dpm	18	6	12	00:00:26	🟩🟥
nebraska-xrootd	18	10	8	00:00:45	🟩🟥
prague-dpm	18	7	11	00:00:30	🟩🟥
prometheus	18	12	6	00:00:25	🟩🟥

JWT compliance failure analysis

Audience checks are correctly enforced by StoRM and XRootD (the test fails for XRootD since 403 is returned instead of 401, minor issue)

Only StoRM correctly implements group-based authorization (configuration issue at the other endpoints?)

Scope-based path authorization is not correctly enforced by most storage elements (configuration issue?)

storage.create and storage.modify semantics is correctly enforced by StoRM and dCache

Local user mapping: discussion

Provide a mechanism based on tokens ~ equivalent to what we have for X.509 certificates.

Agree on token claims used to drive the mapping:

- “issuer” + “sub” claim
- “wlcg.groups” for groups

Subject-based mapping is necessary to handle the home-directory use case

An MkGridmap-like utility integrated with IAM is still needed by some software

- EOS, DPM, Echo

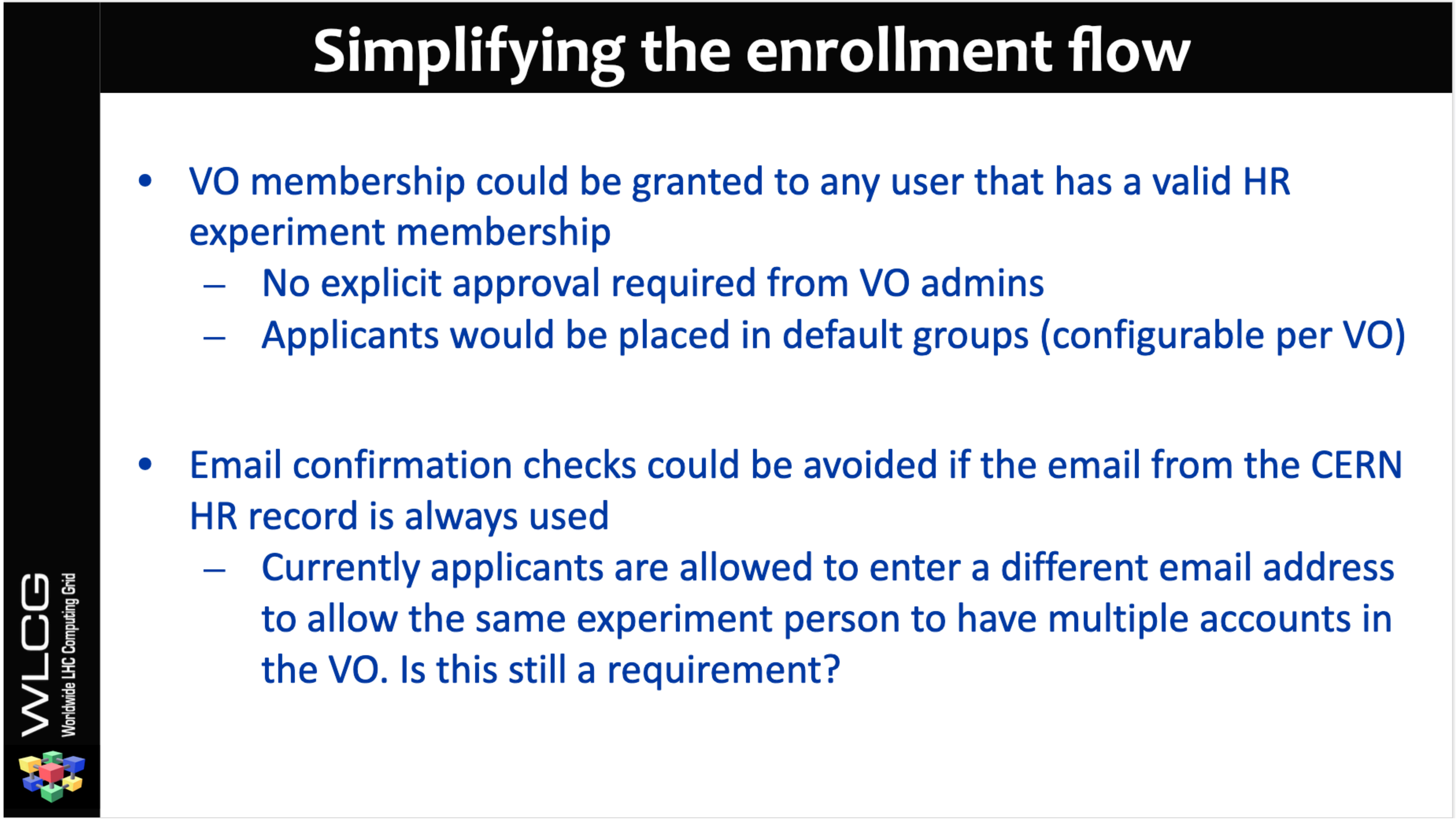
Local user mapping: Scitokens library implementation

Proposal described in the Hackathon google doc

First implementation by Brian in the XRootD Scitokens library

- https://github.com/scitokens/xrootd-scitokens/pull/32

Simplifying VO enrolment discussion



Simplifying the enrollment flow

- VO membership could be granted to any user that has a valid HR experiment membership
  - No explicit approval required from VO admins
  - Applicants would be placed in default groups (configurable per VO)
- Email confirmation checks could be avoided if the email from the CERN HR record is always used
  - Currently applicants are allowed to enter a different email address to allow the same experiment person to have multiple accounts in the VO. Is this still a requirement?

Simplifying VO enrolment discussion

CMS would like to have automatic onboarding, as the VO Admin doesn't do much more than click yes to approve membership requests, given that all the policy aspects are sorted out by IAM (HR membership check, AUP etc.). There's no bootstrap/configuration besides the membership request approval

Other VOs (e.g. ALICE) may have different requirements

Transitioning IAM in production discussion

Devise a plan (and present it at the GDB) to “deprecate” VOMS and move to IAM

- activity started in the context of the WLCG AuthZ WG

Requires ability to migrate VO membership data from VOMS Admin to IAM and have the services run in parallel

- This should be already technically possible, but must be investigated in detail

Other achievements

Improved scoped-based authZ and token validation in DPM

GlideIn WMS/HTCondor integration with the IAM WLCG token issuer

Working token-exchange support in Vault supporting audience restrictions

Improved audience validation in RUCIO

Group-based authorization support in RUCIO

Token-exchange support with audience restrictions in FTS against WLCG IAM

Improved JWT validation compliance in FTS

… and more!

Next steps

Improve JWT compliance in SEs, RUCIO and FTS

- a third hackathon focused on this?

More testing for Group-based authorization

More endpoints in the JWT testbed

Move focus from data to compute

- *WMS and HTCondor integration

WLCG AuthZ WG

Token-based AuthN/Z discussions mostly happen in the context of the WLCG AuthZ WG, so join us on the calls!

https://indico.cern.ch/category/68/

https://twiki.cern.ch/twiki/bin/view/LCG/WLCGAuthorizationWG

Thanks for your attention.

Questions?