



Science and
Technology
Facilities Council

Scientific Computing

Accounting of Jobs Submitted with Tokens

Update from the WLCG AuthZ WG & APEL

Tom Dack
Federating Services Group Leader
Scientific Computing, STFC UKRI

Introduction & Landscape

- For jobs submitted with VOMS, the communication of VO for accounting purposes was well understood – and consistent
- In a token authenticated world, the process requires some reconsideration
 - The [WLCG Token profile v1](#) defines a token issuer per VO, asserting that the issuer token claim can be used to communicate VO
 - However, this does not work for all issuers – especially those which serve several communities, such as EGI Check-in
- Therefore, the method through which the association between VO and Job can be established needed to be revisited.

ARC CEs

- Due to ARC having its own internal accounting, associating tokens and VOs is already implemented, and complete job records are sent directly to APEL.
- Two methods to map tokens to jobs are supported in ARC v7:
 - The `usetokenforvoms` option maps token claims directly as VOMS attributes, with use of the `wlcg.groups*` claim currently supported.
 - This option is disabled by default
 - The `vomsless_vo` option supports manual admin-defined maps of tokens to an appropriate VO.
 - The token is first mapped to an authgroup through the standard ARC methods, and then the `vomsless_vo` config is used to assign this authgroup to a VO.
 - Manual admin-defined maps in this way is the preferred method
- Documentation available in the [ARC v7 release notes](#)

HT Condor CEs

- HT Condor code currently relies on the presence of *x509UserProxyFirstFQAN* in the history record of each job
- The proposed implementation for HT Condor is one resembling the configuration present in ARC config
- Implementation of a flexible expression, which could also work when only a token is present, and establishing VO from token claims
 - If present, `wlcg.groups` can be used
 - The union of `issuer` and `subject*` claims are expected to be sufficient for most use-cases

HT Condor CEs cont.

- Following the WLCG AuthZ WG meeting on 24/04, and coordination with HT Condor team, a basic implementation of this expression has been prototyped and tested
- This enables HTCondor CE to support the same accounting options as the ARC v7
 - Currently works only with HTCondor as LRMS
 - Similarly to ARC, a mapfile is preferred over `wlcg.groups` mapping
- Petr Vokac, Maarten Litmaath, & Adrian Coveney are coordinating with the HT Condor development team



Commit ed0a146

 Petr Vokac committed 2 days ago

```
Basic APEL accounting for job submitted with tokens
```

```
Accounting for jobs without delegated VOMS proxy
```

```
Provide similar accounting options implemented in ARC-CE 7
```

```
(https://bugzilla.nordugrid.org/show\_bug.cgi?id=4236).
```

```
* no changes for jobs with delegated VOMS proxy (x509UserProxyFirstFQAN)
```

```
* optionally use first wlcg.groups with APEL_USE_WLCG_GROUPS enabled
```

```
* mapfile for remaining job using Owner or AuthTokenIssuer,AuthTokenSubject
```

```
 apel_token_accounting
```

Conclusions

- Token Accounting is closer to being implemented than anticipated two weeks ago
- If CEs can be configured to use tokens to map VOs, this avoids significant changes to accounting workflows
 - Steps to be taken to verify that alternate clients – such as AUDITOR – can operate in the same manner
- Solution for HTCondor CE with Slurm LRMS still to be investigated
- It is important to ensure that sufficient information is communicated in tokens
 - Of note are workflows where the subject & issuer union may not uniquely identify a VO
 - An example is that it is currently impossible to distinguish Femilab jobs submitted for the "small experiment" VOs.
 - NoVA, Mu2e, Minerva, ... rely on indistinguishable tokens:
"sub": "fermilabpilot@fnal.gov",
"iss": "https://cilogon.org/Femilab",



Science and
Technology
Facilities Council

Scientific Computing

Questions?





Science and
Technology
Facilities Council

Scientific Computing

Thank you

sc.stfc.ac.uk

ARC Mapping example

```
# /etc/arc.conf
# ...
[authgroup: wlcg_group]
authtokensgen = (iss=https://wlcg.cloud.cnaf.infn.it/)

[authgroup: egi_auger_group]
authtokensgen = (iss=https://aai.egi.eu/auth/realms/egi) & (sub=85ff127e07ea6660c727831b99e18e4e96b319283f8d2cc8113f405bad2ba261@egi.eu)

[authgroup: atlasprd_group]
authtokensgen = (iss=https://atlas-auth.cern.ch/) & (sub=7dee38a3-6ab8-4fe2-9e4c-58039c21d817)

[authgroup: atlasplt_group]
authtokensgen = (iss=https://atlas-auth.cern.ch/) & (sub=750e9609-485a-4ed4-bf16-d5cc46c71024)

[authgroup: atlas_group]
authtokensgen = (iss=https://atlas-auth.cern.ch/)

[arex/jura]
vomsless_vo wlcg_group /wlcg/Role=NULL/Capability=NULL
vomsless_vo egi_auger_group /auger/Role=NULL/Capability=NULL
vomsless_vo atlasprd_group /atlas/Role=production/Capability=NULL
vomsless_vo atlasplt_group /atlas/Role=pilot/Capability=NULL
vomsless_vo atlas_group /atlas/Role=NULL/Capability=NULL
#...
```

HTCondor-CE+HTCondor Mapping example

```
# /etc/condor/apel_acct_group.map
# map local job owner "dteam" to APEL accounting group /dteam
* dteam /dteam
# map all local owners starting with "ops" to the APEL accounting group /ops
* /^ops.*$/ /ops
# map ATLAS token issuer and subject to the APEL accounting group
* /^https:\/\/atlas\(-auth\.cern\.ch\/,7dee38a3\(-6ab8\(-4fe2\(-9e4c\(-58039c21d817$/ /atlas/Role=production/Capability=NULL
* /^https:\/\/atlas\(-auth\.cern\.ch\/,5c5d2a4d\(-9177\(-3efa\(-912f\(-1b4e5c9fb660$/ /atlas/Role=lcgadmin/Capability=NULL
* /^https:\/\/atlas\(-auth\.cern\.ch\/,750e9609\(-485a\(-4ed4\(-bf16\(-d5cc46c71024$/ /atlas/Role=pilot/Capability=NULL
* /^https:\/\/atlas\(-auth\.cern\.ch\/,.*$/ /atlas/Role=NULL/Capability=NULL
# map DUNE token issuer and subject to the APEL accounting group
* /^https:\/\/cilogon\.org\/dune,dunepilot\@fnal\.gov$/ /dune/Role=pilot/Capability=NULL
* /^https:\/\/cilogon\.org\/dune,.*$/ /dune/Role=NULL/Capability=NULL
# no way to map individual Fermilab experiments hidden behind one token identity
#* /^https:\/\/cilogon\.org\/fermilab,fermilabpilot\@fnal\.gov$/ NoVA? Minerva? Mu2e? ...
```