Token Transition update

GDB, 27 March 2024

M. Litmaath

v1.1

Computing (1)

More details in Dec GDB update

- Campaign to have HTCondor CEs upgraded to maintained versions
  - Intermediary version: v9.0.20
    - Supports tokens, SSL (no VOMS mapping) and GSI (with VOMS mapping)
  - Versions >= v23.x
    - Support tokens and SSL without VOMS mapping
  - Versions >= v23.5.2
    - Support tokens and SSL with VOMS mapping! (release notes)
  - To use SSL mappings with proxies, clients must also run **recent** versions!
  - All versions support *delegation* of VOMS proxies to be used by jobs and APEL
    - Mind this setting for APEL: USE_VOMS_ATTRIBUTES = True
  - 53 tickets, 14 solved
  - Many sites prefer upgrading to **EL9** at the same time, but APEL client, parsers and python-argo-ams-library (GGUS:165910) not yet available for that platform
    - Expected soon, possibly from the WLCG repository temporarily

Computing (2)

- APEL support for *tokens* is discussed separately between concerned parties
  - APEL, HTCondor, ARC, several sites, EGI Ops, WLCG Ops Coordination
  - Stopgap approaches for the time being
    - Map token issuers / subjects / … to **pseudo** VOMS FQANs
    - The rest of the machinery can stay unchanged
  - Medium-term solution expected from the GUT Profile WG (see later)

IAM service developments (1)

- All production instances at CERN were upgraded to 1.8.3 still in Dec
  - The services have been running OK
  - Upgrades to 1.8.4 are planned for this Wednesday!

- The “dteam” instance is already used for service monitoring with tokens
  - Users are imported from the VOMS-Admin service until its retirement
  - VO membership is managed by EGI Operations and WLCG Ops Coordination

- The 3 small community VOs at CERN have instances since March 20

- The instance for the “ops” VO will be announced in the coming weeks

IAM service developments (2)

- New instances for the LHC experiments will be created on **Kubernetes**
  - For better **load-balancing**, **logging**, **monitoring**, **GitOps** and **HA** options
  - They will eventually replace the current production instances on *OpenShift*
  - Sites have been ticketed to add support for the future VOMS endpoints and token issuers

- A timeline with tentative milestones for the transition from VOMS-Admin to full dependence on IAM has been agreed for the LHC experiments
  - Some IAM code improvements should still happen beforehand
  - VO admin training material will be provided e.g. for secretariats
  - **Supported use cases** for the time being are:
    - VO management
    - VOMS proxies
    - **Low-rate** token issuance for pilot jobs, SAM tests etc.

Data Challenge 2024 (1)

- DC24 was a **major** milestone in the WLCG transition to tokens
- It has allowed **scale tests** with tokens of services involved in data management
  - Rucio (ATLAS & CMS) and DIRAC (LHCb)
  - FTS
  - IAM

ALICE use "*access envelope*'' tokens with XRootD services since 20 years, but a future switch to WLCG tokens is an option being investigated

- Preliminary reports by ~all stakeholders were presented and discussed in two DOMA meetings on March 6 and March 13
- Full analyses will be presented and discussed in the Data Challenge sessions during the WLCG/HSF Workshop in May

Data Challenge 2024 (2)

- DC24 was a **big success** overall and allowed us to draw conclusions from **millions** of transfers done with tokens!
- It already looks clear that some ways in which tokens were used are not advisable for the long term
  - FTS and IAM instances got overloaded in various ways, requiring interventions
- Several ideas for more **sustainable** use of tokens will be discussed between experts of the services involved
  - Concerning audiences, scopes, lifetimes, exchanges, refreshing, ...
- For the time being, we keep relying on VOMS proxies for most data management

AuthZ WG items (1)

- Various IAM code changes are needed or desirable in the short term
  - For example, fixing VO admin-related issues
  - Lessons learned from DC24 should also be taken into account
    - In particular, stop storing access tokens in the DB
  - However, **no high-rate usage** is foreseen for the time being
    - First, **sustainable** token usage patterns have to be agreed between the parties involved in data management

- Version 2.0 of the **WLCG token profile** is expected this spring
  - Fixing a number of issues encountered with v1.0
    - In the description and/or implementation
  - MW products must at least not reject v2.0 in tokens
    - Nor any future v2.x minor revisions!
  - There may be very few other code changes needed at this time

AuthZ WG items (2)

- The **Grand Unified Token (GUT) Profile WG** has met a few times (agendas)
  - Good progress with its current main challenge: how to determine the VO for the token profiles and the various use cases we need to handle
    - WLCG tokens, SciTokens, EGI Check-in tokens
  - A **new, common attribute** will be defined with practical semantics
    - Details TBD in upcoming meetings

- The **Token Trust & Traceability WG** has also met a few times
  - Aiming to equip site admins, VO experts, … with “tips & tricks” for tokens
    - Recipes, tools, log mining, testing, debugging, monitoring, banning, ...
  - For example, to prevent exposure of tokens through logs!
  - Or how to use the “dteam” VO for monitoring with tokens
    - See next page

Auxiliary services

- The March 7 Ops Coordination meeting had a presentation on **MyToken**
  - Used at KIT e.g. to monitor dCache services with “dteam” tokens
  - Further details are expected to be presented in a future meeting
- At FNAL, a solution based on **Vault** and the ***htgettoken*** and ***httokensh*** clients is in production for various communities since >1 year
- Such auxiliary services are expected to facilitate various use cases
  - Production workflows
  - Monitoring
  - User workflows
    - To help avoid that users need to know anything about tokens!

Conclusions and outlook

- A number of items will keep many parties busy in the next months:
  - VOMS-Admin EOL
  - IAM usability for VO administration by LHC experiments
  - HA options for LHC experiment IAM instances
  - Data management - lessons learned from DC24
  - HTCondor CE versions that no longer support GSI
  - APEL adjustments for tokens
  - GUT Profile WG progress toward a new VO attribute
  - Version 2.0 of the WLCG token profile
  - More deployment and operations know-how
  - More use of auxiliary services

- And a steadily increasing experience with tokens all around !