Token Transition update

GDB, 10 July 2024

M. Litmaath

v1.0

Computing state of affairs (1)

- 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 HTCondor (CE) setting for APEL: USE_VOMS_ATTRIBUTES = True
  - 53 tickets, >= 21 solved
  - Many sites prefer upgrading to **EL9** at the same time
    - APEL client, parsers and python-argo-ams-library available from the WLCG repository

Computing state of affairs (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

- ARC 7 continues supporting X509 / VOMS besides tokens
  - Some VOs may prefer switching to tokens in the near future to make their job submissions more uniform

IAM service developments (1)

- All production instances at CERN are on v1.9.0 since June 25
  - Fixing various high-priority issues in the area of VO management
    - They were the main focus of an IAM Hackathon at CNAF, May 29-30
  - Other fixes are still expected in a few weeks

- The "dteam" instance is usable for service monitoring with tokens
  - Users were imported from VOMS-Admin until its retirement on July 2
  - VO membership managed by EGI Operations and WLCG Ops Coordination

- A campaign has been launched on April 19 for sites to configure support for the instance for the "ops" VO by June 1st
  - 156 tickets, >= 142 solved

IAM service developments (2)

- New instances for the LHC experiments are available on **Kubernetes**, sharing their DBs with the current production instances on *OpenShift*
  - For better **load-balancing**, **logging**, **monitoring**, **GitOps** and **HA** options
  - They will replace the current production instances in the next months
    - Dates to be decided per experiment
  - Sites have been ticketed to add support for the future VOMS endpoints and token issuers by May 31st
    - About 60 tickets still open

- A timeline with *tentative* milestones for the transition from VOMS-Admin to full dependence on IAM concerned LHC experiments & small VOs
  - All supported VOs managed to switch to IAM before the CentOS 7 EOL, June 30
    - VOMS(-Admin) was switched off for the last VO (“ops”) on **June 28**
  - **Supported use cases** for the time being are:
    - VO management
    - VOMS proxies
    - **Low-rate** token issuance for pilot jobs, SAM tests etc.

More on that on the next pages!

VOMS-Admin phaseout snapshot

- April 29
  - Remove legacy VOMS servers from “vomses” – in production for Puppet at CERN as of **May 7**
- May 06
  - VOMS-Admin switched off for first VO → delayed until after the WLCG workshop
- May 31
  - Deadline for sites to have configured support for the Kubernetes instances, *including “ops”*
- June 03
  - VOMS-Admin switched off for last VO → *was in fact the **first** VO: ATLAS !*
- June 17 – ALICE
- June 24 – LHCb
- June 27 – CMS
- June 28 – Ops

Plus:

- July 2 – DTeam

The fallout from all these changes has been minor and was dealt with as “normal” operational issues

VOMS-Admin phaseout executive summary

- Despite various delays, the transition from VOMS(-Admin) to IAM services **finished on schedule**

- This was made possible **thanks to** a **big collaborative effort** from experts of all parties concerned
  - IAM development team at CNAF
  - IAM service team and VOMS service manager
  - LHC experiments, small VOs and EGI Operations
  - WLCG Operations Coordination

Data Challenge 2024 followup

- DC24 was a **major** milestone in the WLCG Token Transition Timeline

- 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 worked on!**

- It was concluded that some ways in which tokens were used are not advisable for the long term

- Several ideas for more **sustainable** use of tokens have started being **discussed between experts** of the services involved
  - To be continued…

AuthZ WG items

- Various IAM improvements are still desirable in the short term
  - Fixes for several high-priority issues are on review, others in progress
  - Lessons learned from DC24 will be taken into account later
    - In particular, stop storing access tokens in the DB
    - But mind the work on **sustainable large-scale data management**: realistic **“mini” challenges** will require corresponding IAM improvements!

- Version 2.0 of the **WLCG token profile** is under preparation
  - Fixing a number of issues encountered with v1.0
  - A few **need to be discussed** in AuthZ or DOMA BDT WG meetings

- The **Token Trust & Traceability WG** met again on June 25
  - Aiming to equip site admins, VO experts, … with best practices for tokens, which will also provide **input for policy documents**
    - Recipes, tools, log mining, testing, debugging, monitoring, banning, ...

Conclusions and outlook

- **Collaborative** efforts will involve many of us in the next months
  - **IAM usability** for VO administration by LHC experiments and others
    - Work on high-priority issues continuing for a **1.9.1 release** in July
  - **HA options** for LHC experiment IAM instances – advancing
  - **Data management:** lessons learned from DC24
    - Aiming to reach the **next level** of token usage in the second half of this year
  - HTCondor CE versions that are fully maintained
  - **APEL** adjustments for tokens – short vs. medium term
  - GUT Profile WG progress toward a new VO attribute – for accounting etc.
  - Version 2.0 of the WLCG token profile – to signal where we intend to go
  - More **deployment and operations** know-how – also input for policies
  - More use of auxiliary services – for robustness and hiding complexity