Token Transition update

WLCG / HSF Workshop, 14 May 2024

M. Litmaath

v1.0

Computing (1)

More details in
[March 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 HTCondor (CE) setting for APEL: USE_VOMS_ATTRIBUTES = True
  - 53 tickets, >= 16 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 very 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 are on 1.8.4 since March 27
  - One was finally done on April 4 because of an issue with cloning its DB
  - The services have been running OK
  - It fixed a long-standing security concern about anonymous clients

- The “dteam” instance is usable 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

- 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, >= 95 solved

IAM service developments (2)

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

- 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 in May and/or June
  - VO admin training material has been provided, still to be improved further
  - **Supported use cases** for the time being are:
    - VO management
    - VOMS proxies
    - **Low-rate** token issuance for pilot jobs, SAM tests etc.

VOMS-Admin phaseout snapshot

- April 29
  - Remove legacy VOMS servers from “vomses” – in production for Puppet at CERN as of **May 7**
    - *Many tickets from users who were disabled in IAM due to sync issues, all* ***fixed*** *manually*
    - Versions 2.0.0 of the wlcg-voms rpms only contain the LSC files, no “vomses” files
    - Broadcast sent to wlcg-operations list
    - Not critical: voms-proxy-init would fail over to a VOMS server that works
- May 06
  - VOMS-Admin switched off for first VO → delayed until after the WLCG workshop
    - No VOMS-Admin service is deleted yet
- May 31
  - Deadline for sites to have configured support for the Kubernetes instances, *including “ops”*
  - Start considering switching off OpenShift instances – unlikely to happen before July → September…
    - Possibly depending on HA situation on Kubernetes
    - Ultimately also the oidc-agent menu listing IAM instances should be updated accordingly
- June 03
  - VOMS-Admin switched off for last VO – *some may need a bit more time (final deadline June 30)*

Data Challenge 2024 (1)

- 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

- The Data Challenge sessions of this workshop also feature observations and discussions about the use of tokens

Data Challenge 2024 (2)

- DC24 has allowed us to draw conclusions from **millions** of transfers done with tokens!

- It is 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, causing failures and requiring interventions

- Several ideas for more **sustainable** use of tokens will be discussed in the next months between experts of the services involved
  - Concerning token audiences, scopes, lifetimes, exchanges, refreshing, ...

- For the time being, we keep relying on VOMS proxies for most of our data management

AuthZ WG items (1)

- Various IAM code changes are desirable in the short term
  - In particular to fix VO admin-related issues in view of VOMS-Admin EOL
    - Main focus of an IAM Hackathon at CNAF, May 29-30
  - Lessons learned from DC24 will be taken into account later
    - In particular, stop storing access tokens in the DB
  - **No high-rate usage** is foreseen for the time being
    - First, **sustainable** token usage patterns have to be agreed and tested between the parties involved in data management

- Version 2.0 of the **WLCG token profile** is under preparation
  - Fixing a number of issues encountered with v1.0
    - In the description and/or implementation
  - Most PRs have been merged and the corresponding issues closed
    - A few open cases need to be discussed in AuthZ or DOMA BDT WG meetings
    - More difficult cases will be postponed for future revisions

AuthZ WG items (2)

- The **Grand Unified Token (GUT) Profile WG** has met 5 times already (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** will meet again this month
  - 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 available here

- The May 2 Ops Coordination meeting had a presentation on ***htgettoken*** + ***HashiCorp Vault*** as a Service for Managing Grid Tokens
  - In production at FNAL 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

- Various items related to tokens concern many of us in the next months
  - VOMS-Admin EOL – final deadline June 30
  - IAM usability for VO administration by LHC experiments
    - High-priority issues are being worked on for a **next release** in June
  - HA options for LHC experiment IAM instances – not to be rushed
  - 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 no longer support GSI – along with moving to **EL9**
  - APEL adjustments for tokens – short vs. medium term
  - GUT Profile WG progress toward a new VO attribute – for accounting and more
  - Version 2.0 of the WLCG token profile – to signal where we intend to go
  - More deployment and operations know-how – with IAM being in the center
  - More use of auxiliary services – gradually benefiting more use cases

- … while we keep gaining experience with tokens everywhere!