Token migration update

GDB, 22 March 2023

M. Litmaath

v1.1

Milestones

- From the Token Transition Timeline – changes w.r.t. Jan 2023:
  - M.2 (Dec 2022) DIRAC versions supporting job submission tokens deployed for concerned Vos
    - LHCb have upgraded to v8.0 and validated job submission to HTCondor and ARC CEs with tokens
    - Token configuration details to be communicated to the sites
  - M.3 (Feb 2023) VOMS-Admin is switched off for one or more experiments
    - Pushed back, but good progress in CMS
  - M.4 (Mar 2023) HTCondor installations at EGI sites have been upgraded to supported versions > 9.0.x
    - See next pages
  - M.5 (Mar 2023) End of HTCondor support for GSI Auth (link)
    - Postponed to May
    - See next pages
  - M.6 (Mar 2023) Some storage endpoints provide support for tokens
    - T2_US_Nebraska XRootD SE passes CMS SAM tests with tokens

Meetings

- AuthZ WG
  - Jan 13
    - IAM hot spare (or HA setup) desirable before VOMS-Admin is switched off
  - Jan 27
    - IGTF host certificate concerns → Resource Trust Evolution TF
      Feb GDB update
  - Feb 10
    - IAM Hackathon summary →
      see this GDB
  - Feb 24
    - XRootD transfer monitoring use case
  - Mar 09
    - Access token lifetimes and revocation
- DOMA BDT WG
  - Jan 18
    - Transfers with root:// protocol
  - Feb 15
    - FTS token improvement plans
  - Mar 01
    - ATLAS scope policies for transfer tests
    - CMS SAM tests for transfers with tokens
  - Mar 15
    - Progress with recommended storage configuration for X.509 + tokens
    - Initial discussion about *storage.stage* scope

IAM deployment news

- CERN IAM team has an extra FTE since Feb 1
  - Welcome **Berk Balcı** and thanks already!
- ATLAS instance upgraded to v1.8.0
- WLCG test instance at CNAF runs v1.8.1 released Feb 28
  - Various fixes, additions and other changes
  - Experiment instances to be upgraded soon
  - IAM developers have agreed to a faster release cycle
- ALICE
  - Token clients have been set up for normal jobs and SAM ETF tests
  - A campaign has been launched for sites to adjust the configurations of their HTCondor CE and VObox services accordingly
- LHCb
  - WIP
- CMS
  - Driving IAM contents from CRIC!

CE token support on EGI

- First deployment campaign on EGI almost done
  - HTCondor v9.0.x + HTCondor CE v5 supporting both GSI and tokens
  - ARC CE REST interface
- Second campaign TBD for v10.x when EGI Check-in tokens are sufficiently supported by HTCondor CE and DIRAC
  - See next pages
- Issues were found in HTCondor v10.x when used to submit jobs to ARC CEs
  - Incorrect RuntimeEnvironment variable name (workaround available)
  - Repeated queries about failed jobs, leading to a memory leak (ditto)

HTCondor CE legacy experiment support

- On March 16 a meeting was hosted by the HTCondor team to discuss concerns about the end of GSI support with representatives from all parties concerned
  - EGI Operations
  - EGI Check-in team
  - DIRAC team
  - Several sites
  - WLCG Operations

- A summary of the discussions is given on the following pages

HTCondor CE v6 – VOMS support

- HTCondor CE v6 can still support **X509** for job submission
- The price is a hardcoded mapping file with less flexibility
  - SSL /…….\/CN=name/ account
- DIRAC pilot factory host certificate DN could be mapped to 1 account
  - Note: a factory can only be mapped to 1 VO
- Each VOMS proxy subject DN can be mapped to its own account
  - SSL /…….\/CN=name(\/CN=[0-9]+)*/ account
  - Note: a DN can only be mapped to 1 VO
- The VOMS proxy should still be delegated as usual
- VOMS attributes will then be available in the job Class Ad
- Jobs can then be handled according to those attributes
- If the batch system is HTCondor, those mappings can work fine
- With other batch systems some flexibility will be lost

HTCondor CE – Check-in token support

- EGI Check-in tokens can be made to work as of HTCondor 10.2.0
  - More easily as of 10.4.0
- Via a simple mapping like used for SciTokens
  - SCITOKENS /^https:\/\/issuer\.host\.domain\/,subject-string$/ account
- Problem: Check-in has a single issuer for all supported VOs
  - The VO would need to be inferred from the subject string instead
- DIRAC pilot factory token subject could be mapped to 1 account
  - Note: a factory can only be mapped to 1 VO
- Any subject string could be mapped to its own account
  - Note: a subject can only be mapped to 1 VO

Common mapping plug-in call-out

- In the ARC/HTCondor CE Hackathon on Sep 15-16 at NIKHEF, a common mapping plug-in call-out design has been agreed
  - The call-out mechanism has been implemented in HTCondor and ARC
- Each plug-in is a stand-alone program that determines the mapping
- If so configured, the appropriate plug-in will be called for a given token
- The attributes found in the token are presented on *stdin*
  - In particular to allow the VO and any groups to be determined
- The plug-in then decides to which account the token shall be mapped
  - It will need its own *mapfile* machinery for that
- The result is returned via *stdout*
- A first version of the Check-in plug-in is expected in O(weeks)
  - To be implemented and packaged as an optional add-on by the Check-in team
  - It would allow avoiding the previously described, awkward mappings

Conclusions and outlook

- Though the token transition timeline has seen some delays, progress has been steady in many areas concerned

- The main milestones at this time are about the switch to HTCondor CE versions that no longer support GSI
  - Several scenarios to smooth the transition for legacy use cases
  - The next meeting with the HTCondor team is planned for April 13

- To be continued…