UC San Diego

Token Transition Report: CMS

Marco Mascheroni

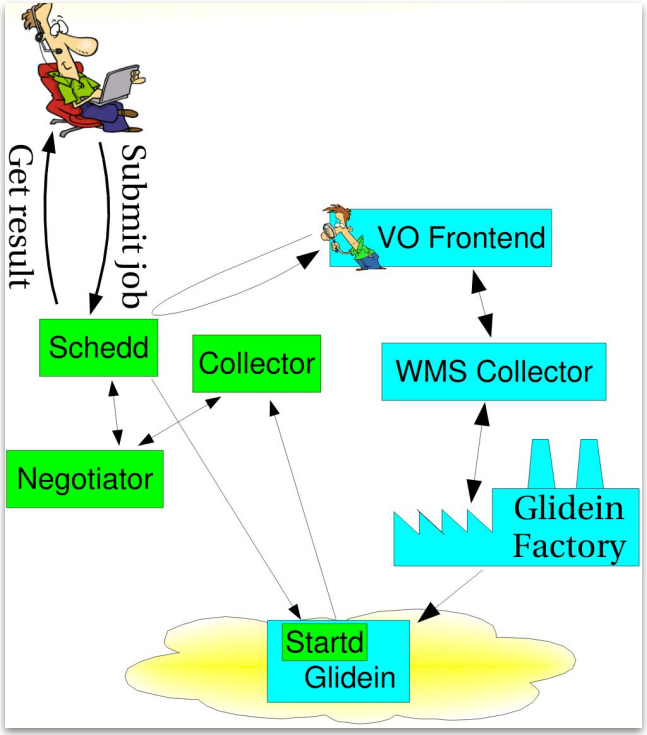
Motivations

- Globus free release of OSG (3.6): **No more GSI and GridFTP**
- **Need a replacement** for parts of the computing infrastructure that depends on those technologies, for example:
  - Dataset movement (GridFTP)
  - Pilot factories to CE communication (GSI and GridFTP)
  - Condor daemons authentication in the CMS Global Pool (GSI)
  - …
- Particular attention to transitions that involve sites
  - **Migration campaigns always time consuming**

Ongoing transitions to tokens

- Workload management
  - Pilot proxy to SCITONENS
  - Global Pool to IDTOKENS
- Data management
  - GridFTP to WebDav-TPC

GWMS and the CMS Global pool



GlideinWMS components

Vanilla HTCondor pool

- **User jobs** submitted to condor schedulers
- VO Frontend looks at “user jobs” and calculates “pilot job” **pressure**
- Glidein factory submits **pilot jobs** to CEs
- **Pilot job runs on the WN** and launch the startd
- The **startd connects to the collector** and is ready to **accept user jobs** from the CMS Global pool

- The VO Frontend generates **Pilot Proxies**
  - **Currently used both for *Factory<->CE authentication* and for *startd<->collector***

Replacing proxy with SCITOKENS for CE auth/authz

Proxy approach:

```
voms-proxy-init -voms cms:/cms/Role=pilot -valid 72:0
voms-proxy-init -voms cms:/cms/local/Role=pilot -valid 72:0
```

- Two proxy generated and renewed through custom cronjob
  - Special proxy to be used to match “extra pledge” resources to local users
- Proxy copied to the Glidein factory and used for submission co CEs
  - Same proxy used for WN to Condor central manager communication.
- Mapping on the CE (through Argus or lcmaps):

```
"/cms/Role=pilot/Capability=NULL" cmspilot
"/cms/local/Role=pilot/Capability=NULL" cmslocal
```

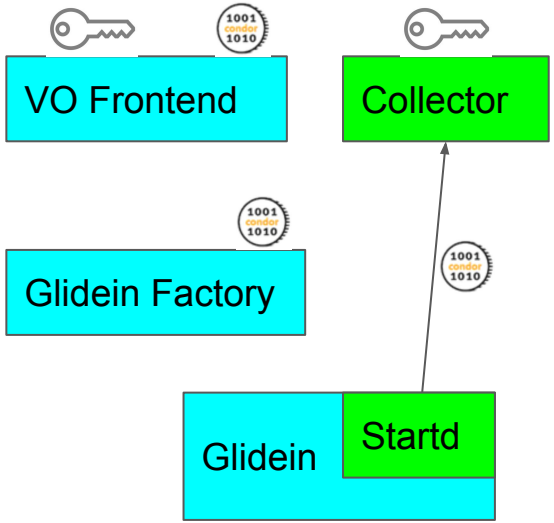
Token approach (tested in ITB):

```
oidc-token cern-itb
oidc-token cern-itb-local
```

- Tokens generated with OpenID Connect, and refreshed with osg-token-renewer
  - `cern-itb` and `cern-itb-local` are client registrered with oidc-gen
- Token copied to the Glidein factory and used for submission co CEs
  - A different token has to be used for WN to Condor central manager communication. More later
- Mapping on the CE (through condor_mapfile):

```
SCITOKENS
/^https:\/\/wlcg\.cloud\.cnaf\.infn\.it\/,6e0ebc78-7015-45cc-88e0-7
bb4683b02a6/ pilcms001
```

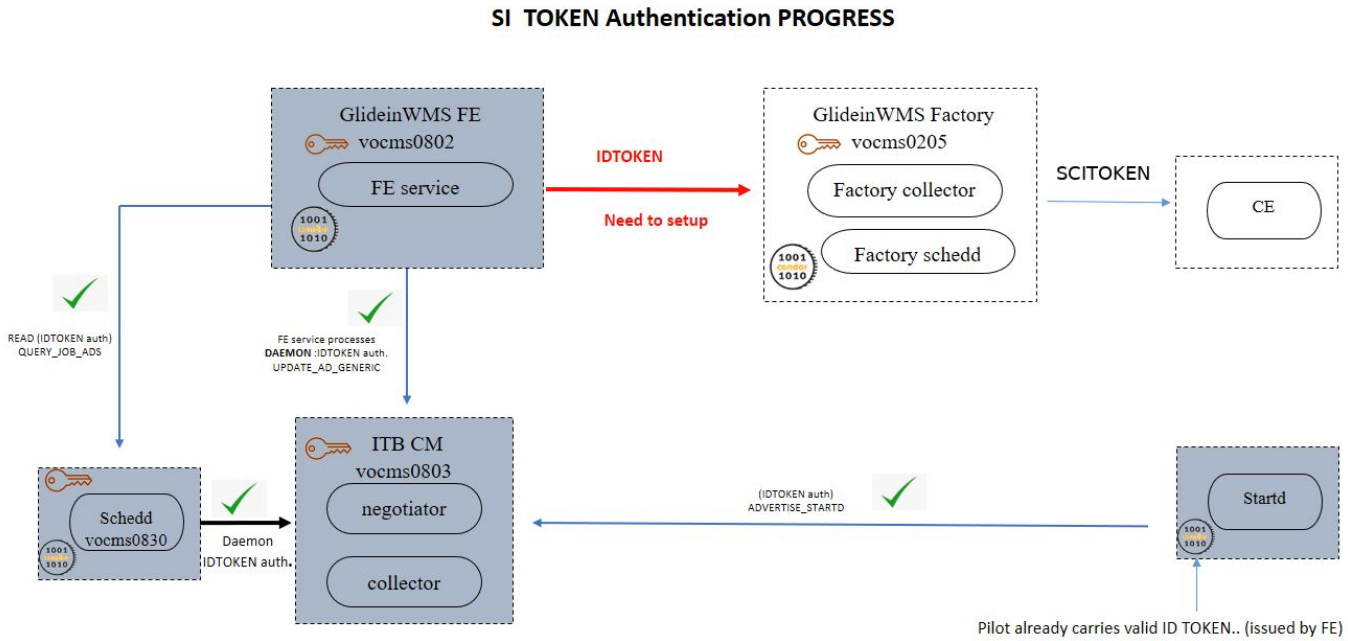
Replacing proxy with IDTOKEN for CM auth/authz



- **Same signing key** placed on both **Frontend** and **Collector**
- Frontend generates an IDTOKEN
- **IDTOKEN is transfered to** the factory, the CE, Batch System, **WN** (as pilot proxy before)
- **Startd can be authenticated and authorized** by the collector

Other HTCondor related auth/authz that have been successfully tested

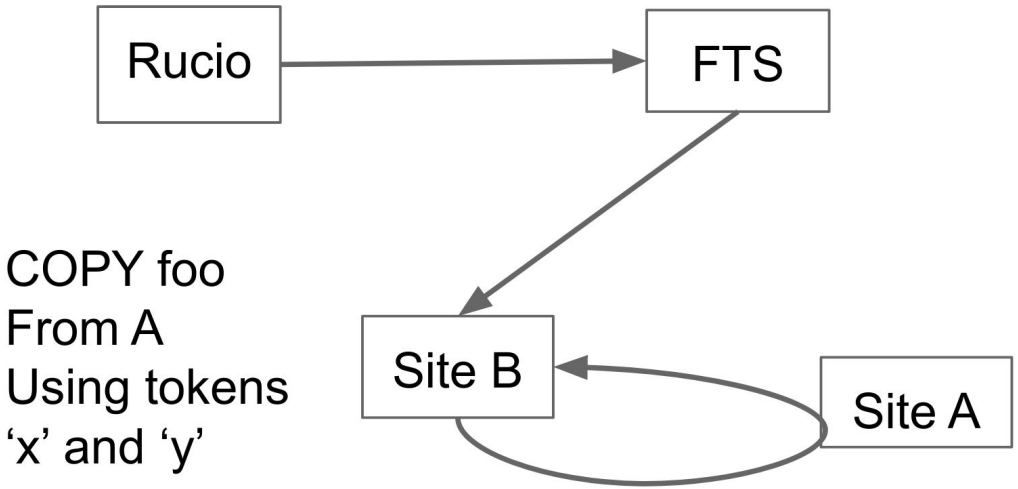
IDTOKENS: Overall test in ITB



Credits to Saqib Haleem for the picture!

GridFTP to WebDav-TPC transition

- WebDAV allows us to use tokens instead of x509 certificates for third-party transfers
  - Extension of HTTP to allow Third Party copy (TPC)
  - Macaroons (bearer token) and SciTokens (OAuth2 token) implementations available
  - Transition focused on Macaroons



Transitions status

SCITOKENS transition status

- **SCITOKEN generation** and refresh **set up** in the frontend
- **Successfully tested SCITOKENS** for Factory/HTCondorCE communication
  - Both with US sites (Wisconsin, Nebraska) and EU (CNAF)
- Using one one token for all CEs for the time being
  - Having a token per CE requires changes in GWMS
- GridFTP is still used to transfer files to ARC-CEs
  - HTCondor 9.0 includes support for ARC-CE's REST interface (but GWMS needs some changes to support it)
  - X509 certs will still be used for auth/authz since oauth token support is not there yet
  - Timeline for deployment of the new ARC-CE REST interface on sites not clear (non-US)
- Tomorrow hands-on session ad an opportunity to bootstrap a token transition campaign with US CE admins
  - Argus replacement for role mapping on non-US HTCondor-CE sites?

IDTOKENS transition status (for the Global pool)

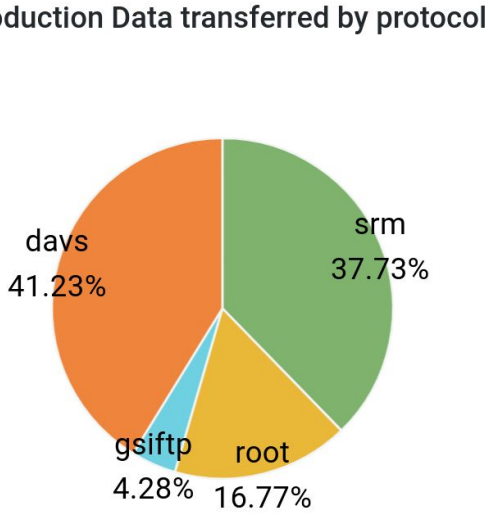
- Advanced testing phase in ITB
  - Only few demons have not been tested yet, most notably frontend to WMS (factory) collector
- Handled centrally
  - Does **not require a long campaign** with site admins
- CRAB uses GSI authentication and Argus to **map CMS users to a pool account** (cms001 to cms1999).
  - Alternative technical solution has not been identified yet

GridFTP to WebDav-TPC transition status

- **Long process** that requires all sites to enable WebDAV endpoint
  - Conversation initiated by CMS opening a ticket to site
  - **Manual tests** + manual **verification** of storage.json
  - **LoadTests** on a _Test instance has to **succeed** before **production** instance is **configured**

Results:

- **WebDAV** has been deployed at **all T1** Disk endpoints
- **38 out of 47 T2s** has completed the transition
- **Few T3s** out of ~27 has started working on it
- **SAM** tests **waiting** for **fixes** on gfal python interface



Conclusions

- (At least) **Three main areas** undergoing important changes in auth/authz due to GSI/GridFTP retirement
- **WebDAV endpoints** for HTC transfers are being deployed
  - Campaign is in a **good shape**
  - Solution for **T1 TAPE transfers** with srm+http is **being tested** and verified
- **Ready** to start campaign for migration to **SCITOKEN for HTCondorCEs**
  - **Hopefully not an invasive campaign**: update software to the latest version and add mapping for CMS SCITOKENS
  - Maybe a bit more difficult for EU sites (usage of Argus for mapping and software not taken from OSG repo)
- Migration of **Global pool to IDTOKENS** also on our radar
  - CRAB server (TaskWorker) still uses GSI and the Argus server for mapping purposes.