

What's going on with Scitokens

Diego Davila

Throughput Computing
July 12th, 2023



First of all

- Don't kill the messenger
- This is from the Facilities/SE perspective i.e. not the user's
- This is meant to be a short presentation + discussion
- If you have concerns please speak up
- Need help, let me know: didavila@ucsd.edu

Why tokens

- It all started with the end of support of Globus in 2018
- We picked https as replacement
- X509 delegation is not trivial for TPC using https
<https://twiki.cern.ch/twiki/bin/view/LCG/HttpTpcTechnical>
- So how does it work today?
 - The COPY is actually done with tokens (macaroons)
- There's also nice things about tokens:
 - Short lived (good and bad)
 - Restricted capabilities
 - Interoperability i.e. works with industry

Timeline

Next big thing

- DC24 on February: Sites must support CMS scitokens for Prod reads/writes
 - Goal: All CMS sites should support Scitokens by the end of 2023

After that (unclear when) CRAB and Prod

- Local users writes (All reads are covered by the above)
 - This is possible via scitokens mapping but not clear if that will be the standard in CMS

Finally (stolen from Jim Basney)

- **WLCG token issuers in production at CERN for Alice, Atlas, CMS, and LHCb, on track to retire proxy certificates in WLCG by March 2026**

Status

- Most of the US sites support CMS Scitokens already :)

<https://monit-grafana.cern.ch/goto/Bi1sPVjVz?orgId=20>

- Missing:
 - Purdue: waiting on a EOS version that supports scitokens
 - Caltech: already tested on 1 server
 - Vanderbilt: dealing with other fires first

Note: Actual production reads/writes with Rucio/FTS haven't been tested yet

Time for discussion



Backup slides

XrootD logs regarding scitokens

Identifying a bad user

230711 20:09:59 1789407 scitokens_Access: New valid token mapped_username=uscms,
subject=6930c7e9-441d-42b9-aa20-7aa8b6fcb6f1, issuer=https://cms-auth.web.cern.ch/,
groups=/cms,/cms/country,/cms/country/us,
authorizations=/store/mc/SAM:read,dir,stat;/store/temp/sitetest:read,dir,stat;/:read,dir,stat

230711 20:09:59 1789407 multiuser_UserSentry: Anonymous client; no user set, cannot change FS UIDs

230711 20:09:59 1789407 ofs_open: unknown.5006:38@uaf-1 Unable to create

/store/temp/user/cmssam/se_webdav_20230712-0254_etf-28_146772_tokn.txt; permission denied

230711 20:09:59 1789407 unknown.5006:38@uaf-1 Xrootd_Response: sending err 3010: Unable to create

/store/temp/user/cmssam/se_webdav_20230712-0254_etf-28_146772_t

okn.txt; permission denied