Storage4PUNCH and Authorisation Claims in Tokens

Oliver Freyermuth, Michael Hübner, Simon Thiele, Luka Vomberg

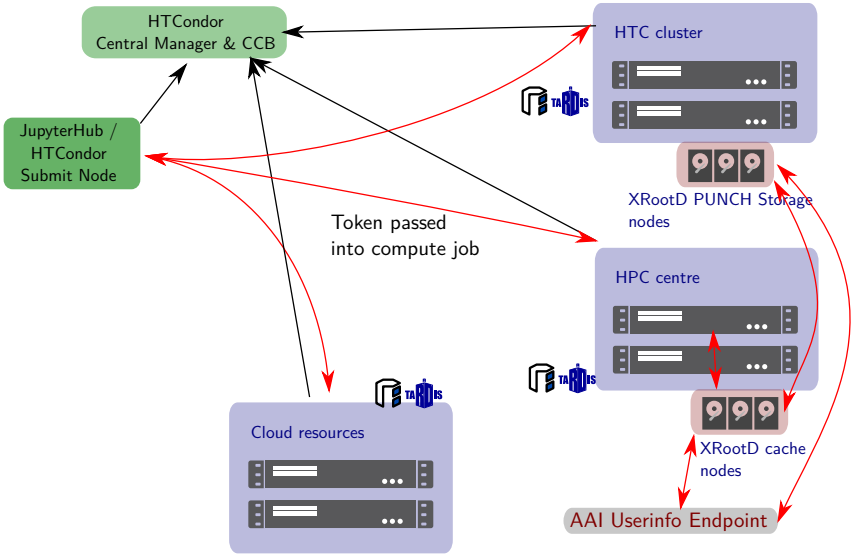
4th May, 2023

UNIVERSITÄT BONN

Limitations

- Authorization information (group membership) only available from userinfo endpoint, i.e. no authorisation in tokens
- No functional way to request a token granting access to less than ‘all’ groups
- No granular permissions (directories etc.) in tokens
- Services can not pass on tokens with reduced permissions

Operational Model



PUNCH 4NFDI

UNIVERSITÄT BONN

Example Case

Common Particle Physics case

- Several users start thousands of compute jobs
- Each job reads dozens / hundreds of files
- Files read from ‘data lake’, i.e. from dozens of sites
- Each site, experiments etc. run multiple storage servers, some sites even run a service for each worker node
- Each individual server (and each cache!) needs to check authorization for each token

$\Rightarrow$ DDoS of userinfo endpoint
$\Rightarrow$ Storage services don’t implement this, since it is bound to break

Thank you

for your attention!