ESCAPE

European Science Cluster of Astronomy &
Particle physics ESFRI research Infrastructures

AAI: next steps

Andrea Ceccanti - INFN

andrea.ceccanti@cnaf.infn.it

ESCAPE -The European Science Cluster of Astronomy & Particle Physics ESFRI Research Infrastructures has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement n°824064

AAI next steps

- WP5 AAI integration workshop
  - https://indico.in2p3.fr/event/22812/contributions/89052/
- Fine-grained AuthZ
  - experiment separation
- Token-based AuthN/Z
- Improved continuous monitoring
- HA IAM deployment

Funded by the European Union's
Horizon 2020 - Grant N° 824064

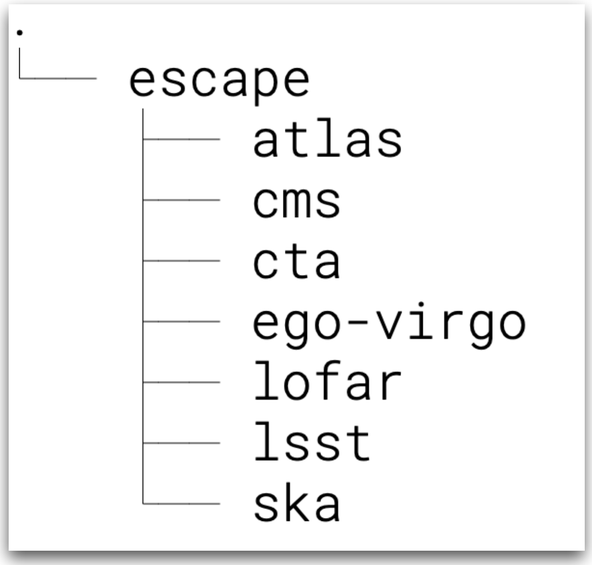
ESCAPE namespace authorization

- ESCAPE Namespace authorization proposal
  - A proposal for the organization of the storage namespace in the ESCAPE data lake to support group-based authorization for data access
  - Authorisation determined by people's membership in groups within ESCAPE IAM
- Main focus (up to now): experiment separation in open data access
  - Avoid that user for experiment A can wipe out data from experiment B
- Preliminary proposal for embargoed data handling
  - Needs more discussion

Funded by the European Union's Horizon 2020 - Grant N° 824064

The namespace structure

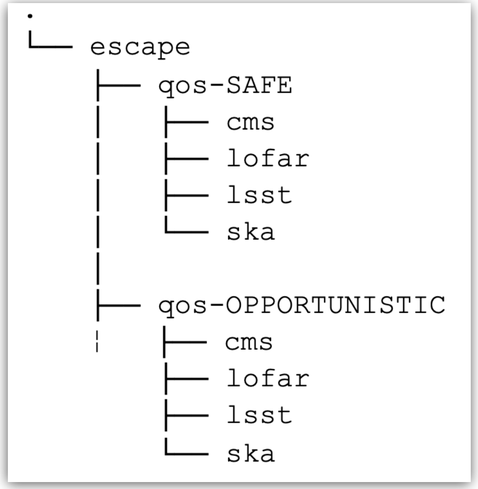
- Use a different folder for each experiment data, rooted under the ESCAPE root namespace directory (which can be different at each storage element)



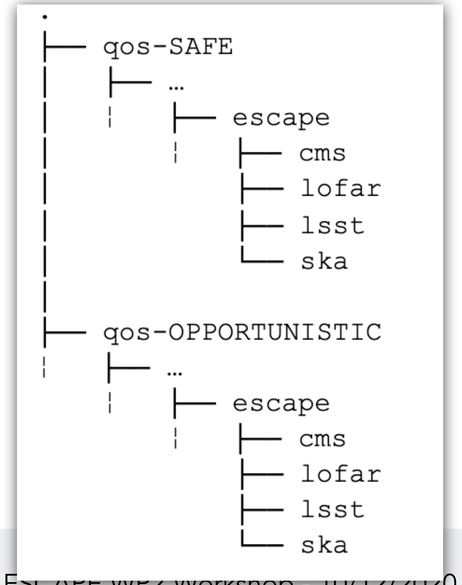
Funded by the European Union's
Horizon 2020 - Grant N° 824064

The namespace structure (multiple QoS)

post-ESCAPE approach



pre-ESCAPE approach



- SEs that support multiple QoS (dCache, EOS?) may include QoS specific directories in the ESCAPE namespace structure
  - A newly written file gets the QoS associated with the path where it is written
- Two proposed approaches
  - to be sorted out which one to use
- Is AuthZ orthogonal to QoS?
  - or we envision allowing access to certain QoSs only to selected groups of users in the context of an experiment?

Funded by the European Union's Horizon 2020 - Grant N° 824064

Namespace authorization

- ESCAPE VO members can read any data in the `/escape` namespace, also in experiment sub-folders

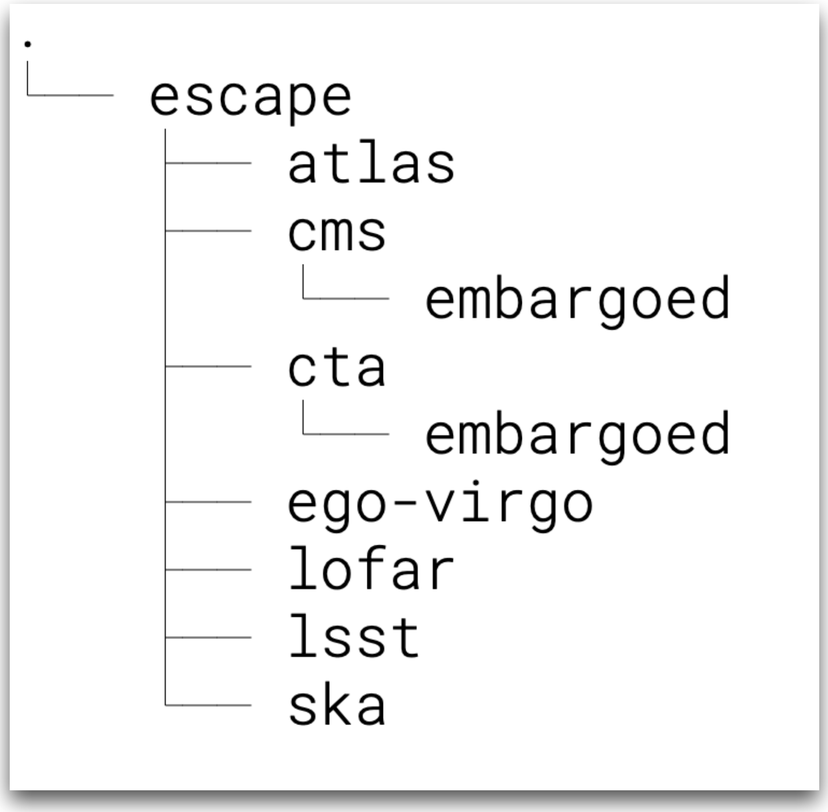
- Write access is granted in an experiment folder to members of the experiment group in ESCAPE IAM
  - e.g., write access to the `/escape/cms` part of the namespace is granted to members of the `/escape/cms` group in IAM

- A `data-manager` group is created in IAM which grants full access privileges to the whole ESCAPE namespace; access to this group will be restricted to people and services managing the namespace

- The authorization scheme above is enforced **both** for X.509/VOMS and token-based authN/Z

Funded by the European Union's
Horizon 2020 - Grant N° 824064

Embargoed and non-public data



- Initial proposal: use a folder named `embargoed` under each experiment folder for non-public data
- In this folder, read and write access is only granted to members of the experiment
- **More discussions needed** to understand if this approach works well with RUCIO

Funded by the European Union's
Horizon 2020 - Grant N° 824064

Deployment strategy

- Reach this authorization in incremental steps:
  1. Run periodic tests that check all storage systems have the desired namespace structure, without testing that fine-grain authorisation is respected
  2. In addition to the existing tests, also run periodic tests that verify that sites honour the desired fine-grained authorisation when authenticating with X.509+VOMS
  3. In addition to the existing tests, also run periodic tests that verify that sites honour the desired fine-grained authorisation when authenticating with a token

- At each step, progress onto the next step would only take place once all sites are passing all tests

Funded by the European Union's
Horizon 2020 - Grant N° 824064

Towards token-based AuthN/Z

- Enable token-based AuthN/Z support in RUCIO/FTS
  - tentative deadline: January, 15th 2021
- Require that sites configure support for token-based authN/Z
  - tentative deadline: February, 1st 2021
  - Initially ESCAPE VO-wide authorization, then incrementally move to fine-grained authZ as described in previous slides
- Data transfers use token-based authN/Z over **HTTP TPC**
  - XRoot protocol support for tokens is not there, yet
  - tentative deadline: March, 1st 2021

Funded by the European Union's
Horizon 2020 - Grant N° 824064

Thanks for your attention!
Questions?