IAM training for LHC VO administrators

In this document we collect input for topics to be covered in the upcoming IAM training for LHC VO administrators.

Proposed topics

- General introduction to IAM
    - How to get tokens
    - Scopes, groups, etc...
- The IAM deployment @ CERN
    - Structure
    - How to ask for support
    - How to get access if not an experiment member
- IAM-VOMS periodic sync: how it works
- Common administration tasks
    - VO membership request handling
    - Group membership request handling
    - Group management
    - Client management
    - Scope management
    - Scope policy management
- ...

Experiments input

ATLAS

- VOMS user records have a single, assignable attribute, `nickname`, which is used by ATLAS to associate a user with their CERN account name. Even though VOMS checks the CERN user database for account information and validity, this attribute is not auto-filled and must be manually entered by a VO admin. Will IAM have similar attributes? If so, regardless of whether they will not be auto-assigned, this should be included in training.
- Will there be a similar concept of group managers like in VOMS-Admin, so that VO managers may delegate the approval of some groups/roles for subgroups of people to other VO members? Would be nice to see if/how this is possible (import group managers from VOMS to IAM?)
- Does expired AUP prevents IAM to issue new VOMS X.509 proxies / tokens?
- How to create service account that doesn't require AUP signing?
- VOMS -> IAM synchronization issues (few missing users, no group removal, wrong userName and displayName, AUP) - plan to fix or we should just get rid of VOMS as fast as possible? Who is responsible / where to report issues with synchronization?
- Missing documentation for proxycert API? Should we use this API to replace MyProxy (does MyProxy have defined end-of-life / end-of-support)?

- (From Zoom chat) How do we properly request a profile change from “user” to “administrator”?

CMS

- what happens to roles ? I understand that they will have to be replaced by groups but would be nice to have examples for organizing the transition and timelines, some are used by by people not directly involved in central operations and we need to properly communicate.
- what happens to the concept of primary group ? I am told by e.g. KIT people that they rely on dCache use of primary group for properly give access to local storage.
- Why tokens ? Isn’t the current transition only about replacing VOMSAdmin servers with a different service which intefaces with CERN HR DB to create list of authorized users and act as endpoint for voms-proxy-init requests ? (yeah, and some legacy make-grid-map-like stuff which Maarten has been chasing for 1 year, thanks!)

Please cover how the relation with CERN HR and registration in experiments will be handled, that’s the most tricky and time consuming part of VOAdmin work atm

- will IAM avoid creating multiple memberships for the same physical person ? And will those be automatically cleaned when importing from current VOMSAdmin DB (consolidating all DN’s registered for same CERN HR ID into a single record) ? Would REALLY great
- will there be a “grace period” between people “disappearing” in HRDB and their suspension/removal in IAM (e.g. to not kick out people who have been accidentally removed and get re-instated a day or two later in HRDB) ? (slide 24 seems to say that this is immediate)
- sorry to add this late: what happens to “additional certificates” ? robots and service DN’s which we currently add to physical users
- The “Register at cms” page should make it clear that this is _only_ for the registration to the CMS VO, not to the experiment itself (optionally with a link to the expt. registration page) That link to the expt. registration page should also be on the error message if someone tries to connect w/o being a member (of the expt.) yet.
- voms-proxy-init should print a message warning the user that their membership is about to be suspended (AUP expiring e.g.) prompting user to take action before things stop working “please visit cms-auth.web.cern.ch to fix this” or similar

ALICE

It would be good to document how the service admins can restore VO admin access in case the admins of a VO accidentally shut themselves out (or ran into some bug or so).

LHCb