From: **Balazs Konya** balazs.konya@hep.lu.se
Subject: WLCG JWT schema: ARC feedback
Date: 8 April 2019 at 16:41
To: project-lcg-authz@cern.ch

BK

hi all,

Maarten asked us to look at the JWC document [1] and provide feedback from the ARC developer community point of view. You can read a bit longer text below.

cheers,
Balazs Konya

ARC feedback on the JWT draft

Technically document is well written. But different parts are probably written by different persons with different goals.

Purpose of scope "upload" is not clear. Is it meant for service which will perform data upload on behalf or is it for storage which will accept the data?

In short, definitions of scopes could benefit from examples.
Paths in scope could benefit from more strict and more flexible matching. Maybe shell patterns or regex could be used. Otherwise giving write access to single file /path/file may have unintended result of client creating folder /path/file and multiple files inside it.

It looks like there is no benefit to have scope as space delimited strings. It would be easier to process them if JSON array is used. Unless there is some implementation which somebody is trying to push through.

There is something wrong with description of the groups scope. It first says
"To request multiple groups, multiple groups:<group_name> scopes are included in the authorization request" followed by example
"scope=groups:/cms/uscms groups:/cms/ALARM"

When it comes to the CE related scopes, "execute" and "queue" are not clear and they even may have overlaps. Is it about execution in batch/cluster? How immediate is immediate execution supposed to be?

We think that CE related control should be based on howto control jobs.
It would be really important to define how to identify specific jobs on CE through scopes in order not to have multiple incompatible solutions one year later. Following REST approach jobs could be paths (first level folder named after identifiers of the job) with deeper paths representing data inside jobs.

As an example, the A-REX (ARC CE) authorization model could be used:
Currently A-REX internally defines 3 access control groups - "Create", "Modify" and "Read". "Create" was meant for job submission. "Modify" for allowing
other people to control your jobs (in case group of people are working on same set of jobs). "Read" is mostly for other services which monitor jobs and CEs.
We think that those 3 groups are enough for basic CE control. If job identification is well defined that should be mostly enough. IMO job is as top level folder could be good enough approach. If applied to A-REX that can be even extended to controlling access to each file inside session directory.

Rest of the document is also very clear and defines authorization process quite well. There is a small concern about how short-lived access tokens to be refreshed on CE. Will WLCG adopt one of existing protocols or shall we have to invent own?

[1] https://docs.google.com/document/d/1cNm4nBl9ELhExwLxswpxLLNTuz8pT38-b_DewEyEWug/edit?usp=sharing

--
Balázs Kónya

Technical Coordinator
NorduGrid Collaboration www.nordugrid.org

Lund University balazs.konya@hep.lu.se
Department of Physics phone: +46 46 222 8049
BOX 118, S - 221 00 LUND, Sweden fax: +46 46 222 4015