



Token Task Force Meeting

Lisa Goodenough

15th March 2023

Agenda

- **News**
- **Discussion**

News

- **Phase 3 of jobsub_lite Rollout has been postponed to April 5, 2023**
 - Jobs will no longer be submitted to jobsub_server schedds (jobsub02/03)
 - We need to understand the issues people are having
 - Please submit jobs using jsl and open a ticket if you have problems!

Token Scopes for Interactive versus Batch Jobs

Based on discussions in the Token Task Force meetings and input from Liaisons over a year-and-a-half ago, CSAID made the decision to provide the following scopes in tokens to Analysis users:

- 1.storage.create: /<experiment>/scratch/users/\${uid}
- 2.storage.modify: /<experiment>/scratch/users/\${uid}
- 3.storage.read: /<experiment>

There are a few exceptions to this rule for particular experiments, but I am not going to discuss those here.

The storage scopes are defined as follows:

- 1.storage.create: allows the user to upload data;** this includes (a) renaming files if the destination file does not already exist, (b) the creation of directories and subdirectories at the specified path, and (c) the creation of any non-existent directories required to create the path itself; this authorization does not permit overwriting or deletion of stored data; the driving use case for this scope is to enable stage-out of data from jobs on a worker node
- 2.storage.modify: allows the user to change data;** this includes (a) renaming files, (b) creating new files, and (c) writing data; this permission includes overwriting or replacing stored data in addition to deleting or truncating data; this is a strict superset of storage.create
- 3.storage.read: allows the user to read data**

In the context of the specific paths listed above, experimental Analysis users are then generally allowed

- to read data from any directory in /pnfs/<experiment> and
- to **upload and change data** in /pnfs/<experiment>/scratch/users/\${uid}, ie in their own experimental scratch area.

Token Scopes for Interactive versus Batch Jobs

The Problem:

- Tokens are currently configured so that experimental Analysis users **cannot write to their experimental dCache persistent area**, ie `/pnfs/<experiment>/persistent/users/${uid}`, using token authentication.
- The reason for this configuration is to ensure that no precious data is accidentally overwritten in a grid job.
- We have come to understand that this limitation causes many problems for interactive work in which users utilize the data handling tool `ifdhc`, which requires a token; users are accustomed to accessing and managing data in their scratch and persistent areas using `ifdhc`.

Token Scopes for Interactive versus Batch Jobs

The Solution (in progress):

We are going to **add** the following scopes in tokens for all Analysis users:

1.storage.create: /<experiment>/persistent/users/\${uid}

2.storage.modify: /<experiment>/persistent/users/\${uid}

This will allow users to **upload and change data** in /pnfs/<experiment>/persistent/users/\${uid} as well as /pnfs/<experiment>/scratch/users/\${uid}.

Through a process called “token weakening”, jobsub_lite will by default remove the storage.modify scopes in jobs. As a result, the default behavior will be that Analysis users can upload data to both persistent and scratch areas in their jobs but not change data in those areas.

A new jobsub_lite argument flag, --need-storage-modify, will be made available to enable the stronger “modify” token in jobs. One instance of the flag is needed for each path added, eg. --need-storage-modify=/path1 --need-storage-modify=/path2. In this way, users could set --need-storage-modify=/pnfs/<experiment>/scratch/users/\${uid} in their job and get the modify scope only for their persistent area.

User interactive work will have full access to dCache scratch and persistent user areas.

Discussion Points

- **What is the best way to handle refreshing of tokens during interactive sessions?**
- **Can jobsub_lite and ifdh use different environment variables for pointing to the BEARER_TOKEN so that they can be accessed separately?**
- **How does one transfer files with ifdh when using non-SLF7 containers on the grid? (ANNIE is using Centos 8 containers for much of its work; MINOS needs to remain at SL6, due to legacy code. In both cases ifdh is not available in the container.)**
- **Other?**

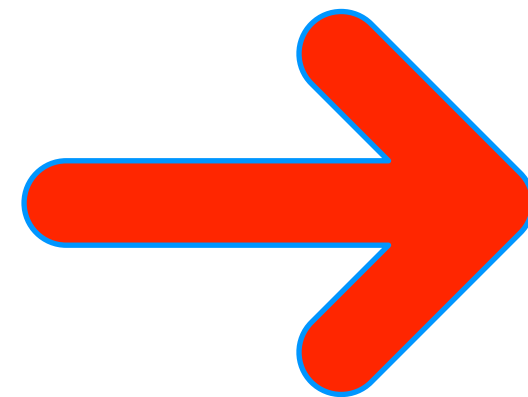
jobsub_lite and Tokens

Please use jobsub_lite!





- Instructions are here:
- https://fifewiki.fnal.gov/wiki/Getting_started_with_jobsub_lite#Authentication

If you have a problem, file a Service Desk ticket.

- [Link to Service Desk for jobsub_lite](#)



Get Help

-  [Ask a question about this service](#)
-  [Report a service outage or incident](#)
-  [Submit a request to service providers](#)
-  [Give us feedback about this service](#)