


Globus Authentication

 [NDS-1040](#) - Discuss Workbench Globus Auth integration **RESOLVED**

Notes from 10/17 meeting with Kyle Chard

Use case

A central goal is to make Workbench easy to install and work with existing system. One

One driving use case is TERRA-REF, where Workbench runs along with Clowder near the ROGER system. ROGER uses NCSA LDAP for authentication /authorization. In this case, Workbench might use the UID/GID from LDAP for the container context to ensure correct filesystem ownership /permissions. While this likely won't be possible with Globus auth, we want to understand what kind of cases we might be able to support.

Summary

We should look at Globus Auth seriously for Workbench, since it covers the CILogon case. Whole Tale is already using it. They have a few examples that we could look at immediately.

The MRDP <https://docs.globus.org/modern-research-data-portal> is an example intended to demonstrate a very common case of a portal that has an analysis service that can do computations. This includes an example of using the transfer scope to initiate a transfer on the user's behalf.

Globus implemented an authenticator for Jupyterhub. We could easily set it up.

Whole Tale is already integrating with Globus and we have access to the developers.

The one snag is groups: they are planning a new feature and are limiting who can use Globus groups. If we can find another option, great. If not, then we can contact them if we can make a compelling case to use it.

May need to look at <https://www.internet2.edu/products-services/trust-identity/grouper/>

Notes

We're looking at adding OAuth support in Workbench and are considering Globus auth specifically. We'd like to hear about existing examples of use, particularly when integrating with existing infrastructure (e.g., HPC systems, initiating transfer, etc). This may be as simple as a list of examples (e.g., <https://docs.globus.org/modern-research-data-portal/mrdp-description/>).

We're also concerned about authorization -- controlling who has access to what in Workbench. In talking with Kacper, it sounds like Globus uses scopes to issue tokens for different purposes and that we might be able to use Globus groups for this purpose.

- This is a common request
- Running JupyterHub: Needs to change into the user
- Running Globus endpoint: Maps the user to the machine that it's on
- Most often, they're setting policy on Globus auth
 - I'll only accept 1 identity provider
 - They'll use that identity as the globally unique name
- For example:
 - Restrict to an identity provider
 - JupyterHub, let anyone in
 - Set ID = globusID only
 - Provision user account on system
 - MRDP
 - That code essentially does the "can transfer on my behalf"
 - Token delegation
 - Also has an analysis service that can do computations as well
 - Saw lots of people building these types of web services
 - Also has a running instance
 - At Argonne
 - Only people at Argonne
 - Globus auth client
 - User must have an Argonne account
 - Use the username that comes with the Argonne
- Discussion of groups
 - Groups -- old way
 - They are planning to re-write globus groups
 - At the moment, they're quite complex, built with Biomedical use cases in mind
 - Everyone needs group-based authentication
- Scopes
 - If you define a resource server (e.g., you are a service that provides a random capability, e.g., transfer)
 - Can define a number of scopes
 - User can approve those scopes so other people can use those scopes
 - "Can perform a transfer on my behalf"

- Maybe something in NDS world is scopeable
 - View running containers
 - Deploy running containers
 - Whole tale could ask for permission to deploy in NDS
 - There is a scope to use the groups
 - Can engage Ian to make Globus more integral
 - Otherwise, we're waiting for the groups refactor
- Kyle says that next groups system may be built on Grouper
 - Need to extend grouper to be a resource server in the Globus
 - User's can approve seeing groups in Group
- For a while, Globus exported LDAP
- Get JupyterHub running with GlobusAuth
- This is a good use case and one they're seeing
 - You need UID, groups, scopes for services
- Make the case for groups
- Has professional services to help with setup