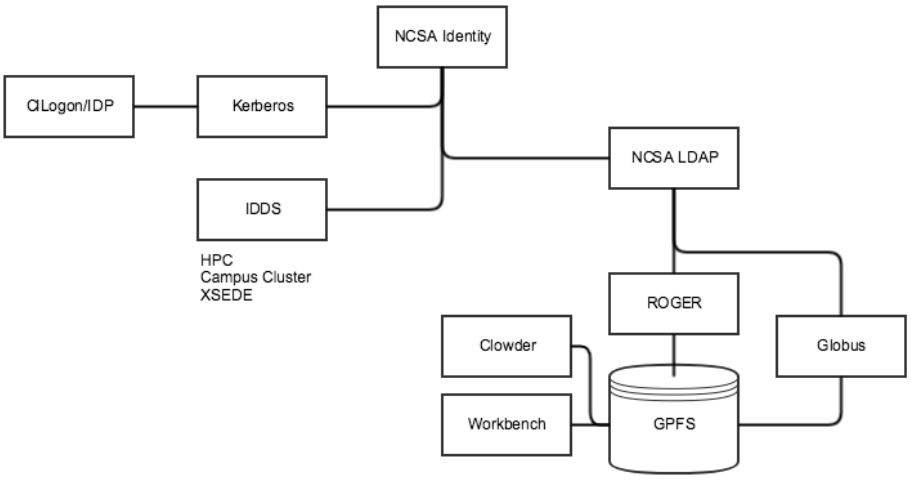
Workbench LDAP OIDC SSO

Per ~~NDS-1005~~ - Discuss LDAP integration options RESOLVED

NCSA LDAP

The following diagram is from a discussion with Nathan Tolbert (ITS) about integrating with NCSA LDAP system. This is driven by the usual TERRA-REF use case: we want users of the TERRA-REF system (Workbench, Clowder, ROGER, Globus) to have a single identity with shared UID/GID for filesystem access across all three systems. ROGER currently uses NCSA LDAP for authentication and authorization (via groups)



Notes from discussion:

- NCSA identity allows anyone to sign-up, access to resources is controlled through internal tools (e.g., Savannah).
    - Because of this, authentication is not sufficient for authorization (same as any Oauth provider)
    - There is a group called all_disabled_users that contains users that should not have access to anything for one reason or another
- Kerberos supports authentication only
- LDAP implements two standard models: inetOrgPerson and groupOfUniqueNames
- LDAP delegates authentication to Kerberos and provides Linux UIDs and GIDs, but cannot provide detailed ACLs
- There are many many users, so filters/paging are essential when querying
- Many systems tie directly to LDAP, e.g., Atlassian suite. These use LDAP for users and groups that can be mapped to application-specific ACLs
- For TERRA-REF case, LDAP integration would be sufficient (no need for OIDC/SSO as long as all services use LDAP

CILogon/CoManage

Notes from ad-hoc meeting with Jim Basney on 9/29

- There is no standard to support group membership via Oauth/OIDC. Scopes are available but inconsistent
- CILogon can provide isMemberOf scopes from LDAP providers, if available on a per-client basis
- Globus Auth has better documentation about use of scopes and groups