LSST IAM Technical Demonstration

The LSST IAM Technical Demonstration evaluates authentication, authorization, and identity management technologies for use by LSST and documents their recommended configuration.

Current status:

- Using NCSA Kerberos and NCSA LDAP
- SSH configured using pam_sss and sssd
  - SSH authentication via NCSA Kerberos password
  - SSH logins obtain a Kerberos ticket for single sign-on to other Kerberos-enabled services
  - SSH logins have UNIX groups set according to LDAP group memberships
- MariaDB configured for Kerberos password authentication
- HTTPD configured for Kerberos password (HTTP Basic Auth) and Kerberos ticket (GSSAPI/SPNEGO) authentication using mod_krb5
- Configuration documented at https://goo.gl/sdZiwD

Activities:

- **DM-4313** - Configure sshd with pam_krb5 and document DONE
- **DM-4314** - Configure DAX web app with Kerberos authentication in IAM test VM DONE
- **DM-4316** - Set up test IAM MariaDB instance with Kerberos DONE
- **DM-4316** - Configure sssd with NCSA LDAP for accounts in test IAM VM DONE
- **DM-4317** - Configure httpd with SSL and mod_krb5 in IAM test VM DONE
- **DM-4674** - Configure WebDAV with Kerberos/LDAP on lsst-auth1 DONE
- **DM-4674** - Prototype web SSO server DONE
- **DM-4675** - Prototype web SSO client (service provider) DONE
- **DM-4676** - Demonstrate InCommon authentication DONE

Task list (from LSSTIdentityandAccessManagementDesign.docx):

- Deploy Kerberos and LDAP for authentication and authorization to OpenStack containers at NCSA and the services running in the containers (e.g., SSH)
- DAX integration with Kerberos/LDAP
- User/Group manager initial availability
- MariaDB integration with Kerberos/LDAP
- WebDAV integration with Kerberos/LDAP
- Web SSO identity provider and service provider
- Integration with InCommon federated authentication