Base site planning: Implications for Kerberos, LDAP, and IAM

Alex Withers

LSST authn/z bi-weekly meeting, 3/10/2016

- Information distilled from various talks, sessions, etc. at the Joint Technical Meeting this February.
- Much of the discussion taking place here:
  - https://confluence.lsstcorp.org/pages/viewpage.action?pageId=16908452
- What follows is a list of requirements from DM, Camera and T&S that may impact LSST IaM efforts

- Summit needs to operate independently in the event it's cutoff from base and wider world
- Common accounts across all machines
- Restricted access to nodes for the **camera control system**
  - Nodes accessed through bastion hosts (access probably means two jumps, see last bullet below)
- Shared file systems needed for sharing various files (i.e. calibration constants)
  - Not sure if this has implications for authn/z
- Remote access into the base site and summit (VPN and SSH)
  - Restrict remote access to subset of users
  - Access for both service and personal accounts

- Source code and configuration repositories
  - Probably using git and stash
  - May contain sensitive LSST data
- SMTP services for sending mail (i.e. alerts, reports)
  - Strongly advise that this requires authentication *even from internal users and services*
- Internal facing web services
  - OCS and TCS monitoring and *operator interactions*
- DM also requires common accounts across all machines, further more to quote Don:
  - “DM would like to have common identity manager to proxy for administrative access. DM would like root-levet trust to extend to Apropos DPPD staff no matter where located.”