LIGOProvisioningUseCase

The Grouper Developers are seeking practical use cases that will contribute to the development and enhancement of the Grouper product, in turn benefiting those institutions that plan to deploy Grouper.

To participate in the development of this work, we ask that you add details of your proposed use case below, as thoroughly as possible.

LIGO provisioning Use Case

Institution: LIGO

Author: Scott Koranda

Brief Description of the LIGO VO

LIGO, the Laser Interferometer Gravitational-wave Observatory seeks to detect gravitational waves--ripples in the fabric of spacetime. The LIGO Scientific Collaboration (LSC), a self-governing collaboration, was founded in 1997
and currently has more than 800 members from 70 institutions worldwide. LIGO is the funded by the NSF.

Sketch of LIGO provisioning

Consider the case of a new data analyst, named Scott Koranda, joining the collaboration by joining the LSC group at the University of Wisconsin-Milwaukee. The following types of resources must be provisioned:

- the Kerberos principal scott.koranda@LIGO.ORG is created in the master KDC and replicated to the slave KDCs
- in the LIGO master LDAP server the following dn is created:

```
dn: employeeNumber=882,ou=people,dc=ligo,dc=org
cn: Scott Koranda
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: eduPerson
objectClass: posixAccount
objectClass: krbPrincipalAux
objectClass: eduMember
objectClass: x-LIGO-TWikiObject
objectClass: qmailUser
uidNumber: 40882
street: UWM Physics Department$P.O. Box 413
uid: scott.koranda
employeeType: Faculty, Sr. Sci/Eng
facsimileTelephoneNumber: +1 414 229 5589
x-LIGO-TWikiLoginName: scottkoranda
postalCode: 53201
postalAddress: UWM Physics Department$P.O. Box 413$Milwaukee$WI$53201$US
telephoneNumber: +1 414 229 5056
description: /DC=org/DC=LIGO/OU=People/CN=Scott Koranda
gidNumber: 40882
employeeNumber: 882
krbPrincipalName: scott.koranda@LIGO.ORG
x-LIGO-TWikiName: ScottKoranda
l: Milwaukee
st: WI
eduPersonAffiliation: University of Wisconsin at Milwaukee
sn: Koranda
homeDirectory: /home/scott.koranda
givenName: Scott
mail: scott.koranda@ligo.org
mailAlternateAddress: skoranda@gmail.com
mailForwardingAddress: skoranda@gravity.phys.uwm.edu
```

- Additionally the following dn is created:

```
dn: cn=scott.koranda,ou=group,dc=ligo,dc=org
objectClass: top
objectClass: posixGroup
gidNumber: 40882
cn: scott.koranda
```

- the subject (in Grouper terms) `scott.koranda@LIGO.ORG` is added in Grouper to the Group `Communities:LVC:LSC:MOU:UWM:` `UWMGroupMembers` and because of that becomes a member of a number of composite groups. These are provisioned into LDAP so that the dn above also has attributes

```
isMemberOf: Communities:LVC:LVCGroupMembers
isMemberOf: Communities:LVC:LSC:MOU:UWM:UWMGroupMembers
isMemberOf: Communities:LVC:LSC:LSCGroupMembers
isMemberOf: Communities:LSCVirgoLIGOGroupMembers
```

- since `scott.koranda@LIGO.ORG` is in the LDAP then that Kerberos principal can be used to login to various SSH servers that have been configured appropriately to pull uids and gids from LDAP.
- newer version control systems like git do not require any further provisioning in order for the user to push into the central repository since they can ride over SSH...
- but a legacy CVS system requires provisioning an account in the CVS writers file in various places
- a login account for a Linux cluster at each of the 10 LIGO Data Grid computing sites is provisioned, usually the account is hosted on storage exposed via NFS. These are separate logins managed by 10 distinct sets of administrators.
- each of the computing sites provisions some type of local storage on each of the cluster head nodes and also a user-dedicated local scratch space on each of the cluster worker nodes. For example on the cluster at Milwaukee we would have `/people/scott.koranda` on the head node(s) and `/localscratch/scott.koranda` on each of the worker nodes.
- a number of grid tools including GridFTP, Grid-enabled OpenSSH, and others use a type of ACL file called a grid-mapfile. These files need to be provisioned with an entry like

```
/DC=org/DC=ligo/OU=People/CN=scott.koranda@LIGO.ORG scott.koranda
```

Typically there should be a grid-mapfile for each instance of each service at each site. The composition of the grid-mapfiles could depend on the groups to which a user belongs. For example, Scott Koranda only gets an entry for one particular GridFTP server because he is in the group that analyzes a particular type of data.

- Since LIGO members are automatically qualified to run on the Open Science Grid there is also a provisioning of the DN above into the LIGO VOMS server (only used for accessing OSG resources, not LIGO resources).

Unable to render {include}   The included page could not be found.