16jul09 --siggy

sudo using LDAP

This started with the premise that as pallets are built, through automation, the corresponding LDAP, additionally sudo would need to be constructed.

Most of my time has dealt with design rather than implementation although a certain amount of experimentation is/was involved. My current design is to have a template that creates a directory structure (from a template) based on accepted pallet naming convention (palletName). Under this “palletName” will have directory frame work for hosts (palletHosts) and users (palletUser). Adding host is as what it implies. You add a host to the list and it has the “sudo” permissions set for the pallet (palletName). User permission is a little different. Single user names can be added within “palletUser” existing groups of users can be added at the “palletName” level.

Below are example of command lines I used to build (by hand) examples of the above directory structure.

&&&&&

Search paths are backwards … closest directory level is the left most entry (as a FQPN would appear)

The sudo part of LDAP is fairly straight forward. Ron had edited pl1rad740.admin.edmunds.com:/etc/ldap.conf file to include the following entry:

sudoers\_base ou=Sudoers,dc=edmunds,dc=com

via command line you can perform searches/additions/deletion with:

SEARCH

ldapsearch -h localhost -D "cn=Manager,dc=edmunds,dc=com" -x -W -b 'ou=Sudoers,ou=Services,dc=edmunds,dc=com' cn=<choice of inputs>

ADDITIONS (TOP level)

Adding a “sub-directory” to the Sudo directory level.

Additions can be performed by:

(1) edit a new file named “add-palletName.ldif” containing:

changetype: add

dn: cn=palletName,ou=Sudoers,ou=Services,dc=edmunds,dc=com

objectClass: top

objectClass: sudoRole

cn: palletName

sudoUser: %palletUsers

sudoHost: %palletHosts

sudoCommand: /usr/bin/tail /var/log/messages

sudoCommand: /usr/bin/less /var/log/messages

ldapadd -h localhost -x -D "cn=Manager,dc=edmunds,dc=com" -W -f add-palletName.ldif

Adding a “sub-sub-directory to the Sudo directory level (or a sub directory to the “palletName” directory)

(2) edit a new file named ”add-palletHosts.ldif” containing

changetype: add

dn: cn=palletHosts,cn=palletName,ou=Sudoers,ou=Services,dc=edmunds,dc=com

objectClass: sudoRole

cn: palletHosts

sudoUser: %palletUsers

sudoCommand: %palletName

sudoHost: xenrap[0-9][0-9][0-9]

ldapadd -h localhost -x -D "cn=Manager,dc=edmunds,dc=com" -W -f add-palletHosts.ldif

another example of adding to the “palletName” directory level.

(3) edit a new file named “add-palletUsers.ldif” containing:

changetype: add

dn: cn=palletUsers,cn=palletName,ou=Sudoers,ou=Services,dc=edmunds,dc=com

cn: palletUsers

objectClass: top

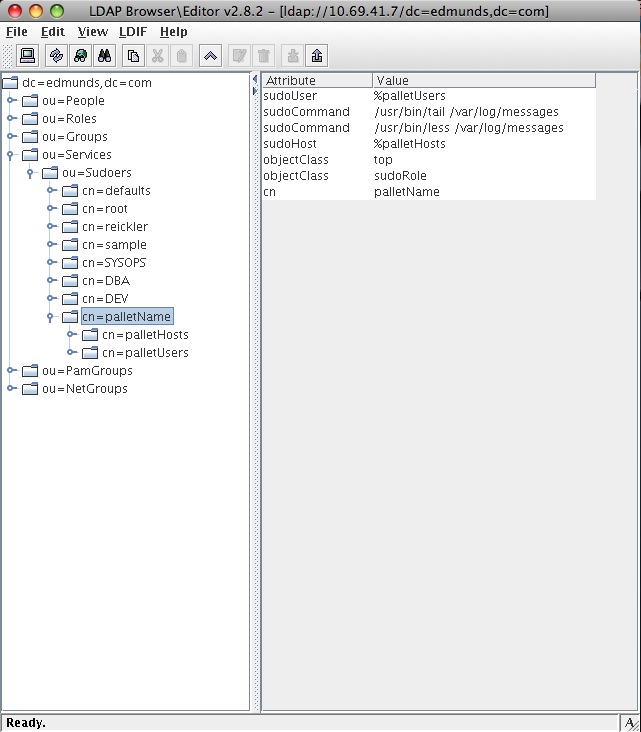
objectClass: posixGroup

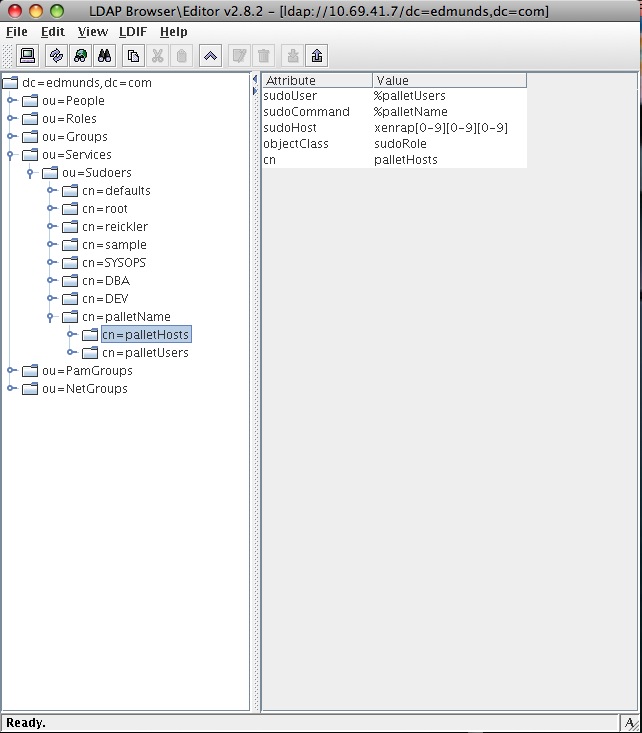
gidNumber: 666

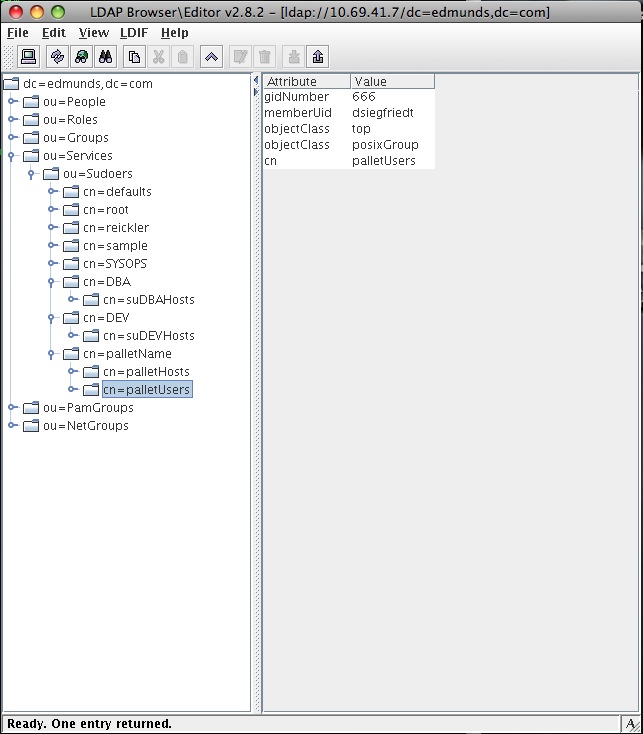
memberUid: dsiegfriedt

ldapadd -h localhost -x -D "cn=Manager,dc=edmunds,dc=com" -W -f add-palletUsers.ldif

There are multiple ways to add users to the “palletName” structure. To add single name you add the username to “palletUser” (memberid <username>). Adding a “group” would be added to the “palletName” (sudoUser %<groupname>) level







DELETION

to delete a sub-attribute.....(ie oem)

ldapdelete -v -h localhost -x -D "cn=Manager,dc=edmunds,dc=com" -W "cn=oem,cn=DBA,ou=Sudoers,ou=Services,dc=edmunds,dc=com"

ldap\_initialize( ldap://localhost )

Enter LDAP Password:

deleting entry "cn=oem,cn=DBA,ou=Sudoers,ou=Services,dc=edmunds,dc=com"