GNU/Linux Administration - Feature #165

Adding Existing Unix Users To LDAP Directory From Local Unix Password File

08/12/2013 07:52 AM - Daniel Curtis

Status:	Closed	**Start date:**	08/12/2013
Priority:	Normal	**Due date:**	
Assignee:	Daniel Curtis	**% Done:**	100%
Category:	Domain Controller	**Estimated time:**	0.50 hour
Target version:		**Spent time:**	0.00 hour

Description

Install the LDAP migration tools

```
apt-get install migrationtools
```

This will install a collection of scripts in /usr/share/migrationtools

Edit migrationtools configuration file

Edit /etc/migrationtools/migrate_common.ph by changing the lines show below. The DEFAULT_ changes are customisations for your site, while the UID/GID lines ignore system users (that is those users created and modified by debian package scripts), and the nobody user and group (65534:65534). You can find your system settings by looking in /etc/adduser.conf.

- Skeleton

  !# Default DNS domain
  !$DEFAULT_MAIL_DOMAIN = "your.domain";
  !# Default base
  $DEFAULT_BASE = ""BaseDN"";
  ...
  !# Uncomment these to exclude Debian-managed system users and groups
  $IGNORE_UID_BELOW = 1000;
  !# Don't uncomment this if you want to be able to add users to system groups
  !# $IGNORE_GID_BELOW = 1000;
  !# And here's the opposite for completeness
  $IGNORE_UID_ABOVE = 29999;
  $IGNORE_GID_ABOVE = 29999;

- Example

  !# Default DNS domain
  $DEFAULT_MAIL_DOMAIN = "example.com";
  !# Default base
  $DEFAULT_BASE = "dc=example,dc=com";
  ...
  !# Uncomment these to exclude Debian-managed system users and groups
  $IGNORE_UID_BELOW = 1000;
  !# Don't uncomment this if you want to be able to add users to system groups
  !# $IGNORE_GID_BELOW = 1000;
  !# And here's the opposite for completeness
  $IGNORE_UID_ABOVE = 29999;
  $IGNORE_GID_ABOVE = 29999;

For Samba LDAP Users

The default subtrees used for user and group information are not compatible with the smbldap-tools package which is recommended when using LDAP for Samba authentication and mapping. For that reason, if you are using Samba with LDAP you should make the following additional changes to /etc/migrationtools/migrate_common.ph.

```
$NAMINGCONTEXT{'passwd'}            = "ou=Users";
```

```
$NAMINGCONTEXT{'group'}          = "ou=Groups";
```

Note: smbldap-tools can be configured to use the migrationtool naming context defaults. Many things default to using the migrationtool naming context, such as pam_ldap and libnss_ldap. IMHO it is easier to change the smbldap-tools config than change everything else to conform to it. Note the "ldapscripts" package is an alternative to smbldap-tools that defaults to the migrationtool naming context.

Optional: Use different subtrees based on function

If you are doing more than LDAP Authentication with your LDAP server you may wish to divide the various functions of the LDAP server into different subtrees. This can also be important if you are using different LDAP servers for different functions while still having the tree look like it is coming from a single source (it can be done but is not discussed here).

In my examples, I have 'ou=dns,"BaseDN" for the DNS server, 'ou=auth,"BaseDN"' for users and groups (authentication/authorization), 'ou=mail,"BaseDN"' for email related information, 'ou=syscfg,"BaseDN"' for system configuration information (like /etc/fstab), and 'ou=net,"BaseDN"' for networking configuration info handled by NSS.

The following assumes you also need to make the changes above for smbldap-tools.

```
} else {
        $NAMINGCONTEXT{'aliases'}           = "ou=Aliases,ou=mail";
        $NAMINGCONTEXT{'fstab'}             = "ou=Mounts,ou=syscfg";
        $NAMINGCONTEXT{'passwd'}            = "ou=Users,ou=auth";
        $NAMINGCONTEXT{'netgroup_byuser'}   = "nisMapName=netgroup.byuser,ou=auth";
        $NAMINGCONTEXT{'netgroup_byhost'}   = "nisMapName=netgroup.byhost,ou=auth";
        $NAMINGCONTEXT{'group'}             = "ou=Groups,ou=auth";
        $NAMINGCONTEXT{'netgroup'}          = "ou=Netgroup,ou=auth";
        $NAMINGCONTEXT{'hosts'}             = "ou=Hosts,ou=net";
        $NAMINGCONTEXT{'networks'}          = "ou=Networks,ou=net";
        $NAMINGCONTEXT{'protocols'}         = "ou=Protocols,ou=net";
        $NAMINGCONTEXT{'rpc'}               = "ou=Rpc,ou=net";
        $NAMINGCONTEXT{'services'}          = "ou=Services,ou=net";
}
```

You will also need to makes the following changes to the sub ldif_entry function in the same file /etc/migrationtools/migrate_common.ph:

```
sub ldif_entry
{
# remove leading, trailing whitespace
        local ($HANDLE, $lhs, $rhs) = @_;
        local ($type, $val) = split(/\=/, $lhs);
        local ($dn);
        local (@newval);
        if ($val =~ /\,/) {
                @newval = split(/\,/, $val);
                $val = $newval["0"];
        }
```

Note on EXTENDED_SCHEMA = 0

Apparently EXTENDED_SCHEMA is set to '1' in many other documents. This probably will not work without modification under Debian 3.1 'Sarge'. I haven't tried going all the way, however I have looked at the ldif that would be used and appears the following note applies.

Note: Since Debian Lenny there is a kerberos.schema within 'krb5-kdc-ldap' (although the package 'heimdal-kdc' contains hdb.schema, which you may investigate using as an alternative to kerberos.schema. WFM), so one must manually edit passwd.ldif to remove the two lines refering to kerberos for every user. That is, the following two lines:

```
objectClass: kerberosSecurityObject
krbName: user@YOUR.DOMAIN
```

Where user@YOUR.DOMAIN is the username with @YOUR.DOMAIN appended.

2007-03-22: note, EXTENDED_SCHEMA = 1 is useful for adding more fields like 'mail' to ldap People records.

For this to work 2 sections of the file migrate_passwd.pl need to be commented-out. #

```
if ($DEFAULT_REALM) {
print $HANDLE "objectClass: krb5Principal\n"; #}


#

if ($DEFAULT_REALM) {

1. print $HANDLE "krb5PrincipalName: $user\@$DEFAULT_REALM\n"; # }
```

With those 2 changes the passwd.ldif file does not need to be edited in order for ldapadd to work.

Perform the Migration

If you just want LDAPAuthentication you probably want option 3, migrating only the /etc/passwd and /etc/group databases (but first using migrate_base.pl).

Notes:

- You may need to create higher-level nodes in the tree before you perform the imports.
- For example to import /etc/passwd using the settings above you would need ou=auth,"BaseDN".
- To create a node that only exists so that nodes can exist beneath it (i.e. an wiki:Self ["LDAPFormatInternalVertices" internal vertex]), you could use 'ldapadd -h localhost -x -W -D "cn=admin,{["BaseDN"]}" -c -f node.ldif' for the following node.ldif.

The migrate_base.pl and migrate_all_online.pl scripts will create most of the required internal vertices (specifically the nodes indicated by $NAMINGCONTEXT in /etc/migrationtools/migrate_common.ph. You should only need to create extra nodes if you choose to use separate subtrees for different functions (e.g. if you use ou=Users,ou=auth for /etc/passwd you will likely need to create ou=auth but not ou=Users).

Skeleton:

```
!# node, "BaseDN"
dn: ou=node,"BaseDN"
objectClass: top
objectClass: organizationalUnit
objectClass: domainRelatedObject
associatedDomain: your.domain
ou: node
```

Example;

```
!# auth, example, com
dn: ou=auth,dc=example,dc=com
objectClass: top
objectClass: organizationalUnit
objectClass: domainRelatedObject
associatedDomain: example.com
ou: auth
```

In all cases (following Options 1..3) you will need to migrate some base settings

- Execute './migrate_base.pl >base.ldif'
- Execute 'ldapadd -h localhost -x -W -D "cn=admin,{["BaseDN"]}" -c -f base.ldif'
- Example commands:

```
./migrate_base.pl >base.ldif
ldapadd -h localhost -x -W -D "cn=admin,dc=example,dc=com" -c -f base.ldif
```

- Hint: You can migrate in a single step
  You can pipe the output of migrate into ldapadd instead of redirecting to a file and using @ldapadd -f filenam@e. For example:

```
./migrate_base.pl >base.ldif
ldapadd -h localhost -x -W -D "cn=admin,dc=example,dc=com" -c -f base.ldif
```

  would become

```
./migrate_base.pl | ldapadd -h localhost -x -W -D "cn=admin,dc=example,dc=com" -c
```

Resources:
https://wiki.debian.org/LDAP/MigrationTools

Related issues:

Related to GNU/Linux Administration - Feature #162: Installing OpenLDAP with ...	**Closed**	**08/08/2013**

History

#1 - 02/16/2015 02:26 PM - Daniel Curtis

- Project changed from 22 to GNU/Linux Administration

- Category set to Domain Controller