GNU/Linux Administration - Support #326

Managing User Information From Active Directory Using nslcd on Debian

02/04/2014 12:23 AM - Daniel Curtis

Status:	Closed	**Start date:**	02/03/2014
Priority:	Normal	**Due date:**	
Assignee:	Daniel Curtis	**% Done:**	100%
Category:	Domain Controller	**Estimated time:**	1.00 hour
Target version:		**Spent time:**	2.00 hours

Description

While migrating my centralized user information server from an OpenLDAP/Kerberos to a Samba4 Active Directory, I needed a method to integrate using my existing server baseline, which is Debian 7. The method I previously used was very similar to this method in that I get a Kerberos keytab from my Kerberos authentication server and I use that keytab file as the authentication token to do user information lookups on the OpenLDAP server. This guide is to show how I connected an example server to a Samba4 Active Directory Domain Controller.

Example machines:

- dc.example.com: 192.168.1.200
- server.example.com: 192.168.1.33

Make sure /etc/resolv.conf points to the Active Directory Domain Controller's IP address:

```
search example.com
nameserver 192.168.1.200
```

To start, install some required packages:

```
apt-get install krb5-user nslcd samba libnss-ldapd libpam-ldapd libsasl2-modules-gssapi-heimdal ks
tart
```

Make sure to copy the **/etc/krb5.conf** and **/usr/local/samba/etc/smb.conf** files from the Domain Controller to the **/etc/krb5** and **/etc/samba/smb.conf**. If these files are not present, joining the domain will fail.

Join the Active Directory Domain

```
net ads join -U administrator@EXAMPLE.COM
```

Once the machine is joined to the domain, a keytab is generated at /etc/krb5.keytab. Now edit the /etc/default/nslcd file and make the following changes:

```
vi /etc/default/nslcd
```

```
K5START_START="yes"

#!# Options for k5start.
K5START_BIN=/usr/bin/k5start
K5START_KEYTAB=/etc/krb5.keytab
K5START_CCREFRESH=60
K5START_PRINCIPAL="SERVER$"
```

Note: Make sure the K5START_PRINCIPAL is set to the Active Directory machine name, which is appended with a *$*.
This will automatically authenticate the keytab generated while joining the domain. This is necessary to allow access to the directory information on the domain controller.

Reboot the machine to enable k5start:

```
reboot
```

After reboot, there should be a krb5cc_0 file in /tmp:

```
ls -l /tmp
```

```
-rw------- 1 nslcd nslcd 2296 Feb  3 23:25 krb5cc_0
```

Configure nslcd

Edit the /etc/nslcd.conf file and change the configuration as needed:

```
vi /etc/nslcd.conf
```

```
uid nslcd
gid nslcd

#!# LDAP/AD server settings
uri ldap://192.168.1.200:389
base dc=example,dc=com

#!# Some settings for AD
pagesize 1000
referrals off

#!# Filters (only required if your accounts doesn't have objectClass=posixAccount
#!# and your groups haven't objectClass=posixGroup. This objectClasses won't be added
#!# by ADUC. So they won't be there automatically!)
filter  passwd  (objectClass=user)
filter  group   (objectClass=group)

#!# Attribute mappings (depending on your nslcd version, some might not be
#!# necessary or can cause errors and can/must be removed)
map     passwd  uid             sAMAccountName
map     passwd  homeDirectory      unixHomeDirectory
map     passwd  gecos             displayName
map     passwd  gidNumber         primaryGroupID
#map     group   Member           member

#!# Kerberos
sasl_mech GSSAPI
sasl_realm EXAMPLE.COM
krb5_ccname /tmp/krb5cc_0
```

And restart nslcd:

```
service nslcd restart
```

Update the authentication services

Once nslcd is configured, edit the /etc/nsswitch.conf and modify it to look similar to the following:

```
vi /etc/nsswitch.conf
```

```
passwd:         compat ldap
group:          compat ldap
shadow:         compat
```

Run the PAM configuration tool:

```
pam-auth-update
```

[*] Unix authentication
[*] LDAP Authentication

This will make the following changes, if you ran the above command then you do not need to make these changes:

- /etc/pam.d/common-auth

  ...
  auth [success=2 default=ignore] pam_unix.so nullok_secure
  auth [success=1 default=ignore] pam_ldap.so minimum_uid=1000 use_first_pass
  ...

- /etc/pam.d/common-account

  ...
  account required pam_permit.so
  account [success=ok new_authtok_reqd=done ignore=ignore user_unknown=ignore authinfo_unavail=ignore default=bad] pam_ldap.so minimum_uid=1000
  ...

- /etc/pam.d/common-session

  ...
  session required pam_unix.so
  session [success=ok default=ignore] pam_ldap.so minimum_uid=1000
  ...

- /etc/pam.d/common-password

  ...
  password [success=2 default=ignore] pam_unix.so obscure sha512
  password [success=1 default=ignore] pam_ldap.so minimum_uid=1000 try_first_pass
  ...

At this point, I was able to run getent and get user information from the domain controller:

```
getent passwd
getent group
```

History

#1 - 02/04/2014 12:31 AM - Daniel Curtis

- Description updated

#2 - 02/05/2014 12:43 PM - Daniel Curtis

- Description updated

Currently the nslcd service does not automagically set the correct GECOS parameters. I found a simple layout of the NIS parameters, which can be mapped accordingly in /etc/nslcd.conf.

SFU Attributes for User and Group Objects

- **NIS Domain** -> msSFU30NisDomain
- **Username** -> msSFU30Name
- **UID** -> msSFU30UidNumber
- **Password** -> msSFU30Password

- **GID** -> msSFU30GidNumber
- **Login Shell** -> msSFU30LoginShell
- **Home Directory** -> msSFU30HomeDirectory
- **Group Members** -> msSFU30PosixMemberOf

Edit the /etc/nslcd.conf file and change the configuration as needed to map the necessary attributes:

```
vi /etc/nslcd.conf
```

```
uid nslcd
gid nslcd

#!# LDAP/AD server settings
uri ldap://192.168.1.200:389
base dc=example,dc=com

#!# Some settings for AD
pagesize 1000
referrals off

#!# Filters (only required if your accounts doesn't have objectClass=posixAccount
#!# and your groups haven't objectClass=posixGroup. This objectClasses won't be added
#!# by ADUC. So they won't be there automatically!)
filter  passwd  (objectClass=user)
filter  group   (objectClass=group)

#!# Attribute mappings (depending on your nslcd version, some might not be
#!# necessary or can cause errors and can/must be removed)
map     passwd  uid             msSFU30UidNumber
map     passwd  homeDirectory   msSFU30HomeDirectory
map     passwd  gecos           msSFU30Name
map     passwd  gidNumber       msSFU30GidNumber
map     group   uniqueMember    msSFU30PosixMemberOf

#!# Kerberos
sasl_mech GSSAPI
sasl_realm EXAMPLE.COM
krb5_ccname /tmp/krb5cc_0
```

#3 - 02/05/2014 01:13 PM - Daniel Curtis

- Description updated

#4 - 02/05/2014 01:14 PM - Daniel Curtis

- Description updated

#5 - 02/10/2014 08:13 AM - Daniel Curtis

When using multiple domain controllers, specify the addressing in a single uri, similar to the following example.

```
#! User/group with which the daemon should run (must be a local account!)
uid nslcd
gid nslcd

#! LDAP/AD server settings
uri ldap://192.168.0.38:389 ldap://192.168.0.89:389
base dc=example,dc=com

#! Some settings for AD
pagesize 1000
referrals off

#! Filters (only required if your accounts doesn't have objectClass=posixAccount
#! and your groups haven't objectClass=posixGroup. This objectClasses won't be added
#! by ADUC. So they won't be there automatically!)
filter  passwd  (objectClass=user)
filter  group   (objectClass=group)

#! Attribut mappings (depending on your nslcd version, some might not be
#! necessary or can cause errors and can/must be removed)
map     passwd  uid             sAMAccountName
```

```
map     passwd  homeDirectory      unixHomeDirectory
map     passwd  gecos              displayName
#!map    passwd  gidNumber         primaryGroupID
map     group   Member             member

#! Kerberos
sasl_mech GSSAPI
sasl_realm EXAMPLE.COM
krb5_ccname /tmp/krb5cc_0
```

If using Active Directory, make sure to have an associated PTR record of the backup domain controller in the reverse DNS zone.

#6 - 02/10/2014 08:13 AM - Daniel Curtis

- Status changed from Resolved to Closed

#7 - 02/16/2015 02:07 PM - Daniel Curtis

- Project changed from 79 to GNU/Linux Administration

- Category set to Domain Controller