Samba and LDAP

Previous Next

This section covers the integration of Samba with LDAP. The Samba server's role will be that of a "standalone" server and the LDAP directory will provide the authentication layer in addition to containing the user, group, and machine account information that Samba requires in order to function (in any of its 3 possible roles). The pre-requisite is an OpenLDAP server configured with a directory that can accept authentication requests. See OpenLDAP Server for details on fulfilling this requirement. Once this section is completed, you will need to decide what specifically you want Samba to do for you and then configure it accordingly.

Software Installation

There are two packages needed when integrating Samba with LDAP: *samba* and *smbldap-tools*.

Strictly speaking, the *smbldap-tools* package isn't needed, but unless you have some other way to manage the various Samba entities (users, groups, computers) in an LDAP context then you should install it.

Install these packages now:

```
sudo apt install samba smbldap-tools
```

LDAP Configuration

We will now configure the LDAP server so that it can accomodate Samba data. We will perform three tasks in this section:

1. Import a schema
2. Index some entries
3. Add objects

Samba schema

In order for OpenLDAP to be used as a backend for Samba, logically, the DIT will need to use attributes that can properly describe Samba data. Such attributes can be obtained by introducing a Samba LDAP schema. Let's do this now.

For more information on schemas and their installation see Modifying the slapd Configuration Database.

1. The schema is found in the now-installed *samba* package. It needs to be unzipped and copied to the `/etc/ldap/schema` directory:

```
sudo cp /usr/share/doc/samba/examples/LDAP/samba.schema.gz /etc/ldap/schema
sudo gzip -d /etc/ldap/schema/samba.schema.gz
```

2. Have the configuration file `schema_convert.conf` that contains the following lines:

```
include /etc/ldap/schema/core.schema
include /etc/ldap/schema/collective.schema
include /etc/ldap/schema/corba.schema
include /etc/ldap/schema/cosine.schema
include /etc/ldap/schema/duaconf.schema
include /etc/ldap/schema/dyngroup.schema
include /etc/ldap/schema/inetorgperson.schema
include /etc/ldap/schema/java.schema
include /etc/ldap/schema/misc.schema
include /etc/ldap/schema/nis.schema
include /etc/ldap/schema/openldap.schema
```

```
include /etc/ldap/schema/ppolicy.schema
include /etc/ldap/schema/ldapns.schema
include /etc/ldap/schema/pmi.schema
include /etc/ldap/schema/samba.schema
```

3. Have the directory `ldif_output` hold output.

4. Determine the index of the schema:

```
slapcat -f schema_convert.conf -F ldif_output -n 0 | grep samba,cn=schema

dn: cn={14}samba,cn=schema,cn=config
```

5. Convert the schema to LDIF format:

```
slapcat -f schema_convert.conf -F ldif_output -n0 -H \
ldap:///cn={14}samba,cn=schema,cn=config -l cn=samba.ldif
```

6. Edit the generated `cn=samba.ldif` file by removing index information to arrive at:

```
dn: cn=samba,cn=schema,cn=config
...
cn: samba
```

Remove the bottom lines:

```
structuralObjectClass: olcSchemaConfig
entryUUID: b53b75ca-083f-102d-9fff-2f64fd123c95
creatorsName: cn=config
createTimestamp: 20080827045234Z
entryCSN: 20080827045234.341425Z#000000#000#000000
modifiersName: cn=config
modifyTimestamp: 20080827045234Z
```

Your attribute values will vary.

7. Add the new schema:

```
sudo ldapadd -Q -Y EXTERNAL -H ldapi:/// -f cn\=samba.ldif
```

To query and view this new schema:

```
sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b cn=schema,cn=config 'cn=*samba*'
```

Samba indices

Now that slapd knows about the Samba attributes, we can set up some indices based on them. Indexing entries is a way to improve performance when a client performs a filtered search on the DIT.

Create the file `samba_indices.ldif` with the following contents:

```
dn: olcDatabase={1}hdb,cn=config
changetype: modify
add: olcDbIndex
olcDbIndex: uidNumber eq
olcDbIndex: gidNumber eq
olcDbIndex: loginShell eq
olcDbIndex: uid eq,pres,sub
olcDbIndex: memberUid eq,pres,sub
olcDbIndex: uniqueMember eq,pres
olcDbIndex: sambaSID eq
olcDbIndex: sambaPrimaryGroupSID eq
olcDbIndex: sambaGroupType eq
olcDbIndex: sambaSIDList eq
olcDbIndex: sambaDomainName eq
olcDbIndex: default sub
```

Using the *ldapmodify* utility load the new indices:

```
sudo ldapmodify -Q -Y EXTERNAL -H ldapi:/// -f samba_indices.ldif
```

If all went well you should see the new indices using *ldapsearch*:

```
sudo ldapsearch -Q -LLL -Y EXTERNAL -H \
ldapi:/// -b cn=config olcDatabase={1}hdb olcDbIndex
```

Adding Samba LD AP objects

Next, configure the *smbldap-tools* package to match your environment. The package comes with a configuration helper script, smbldap-config.pl, that will ask questions.

The *smbldap-populate* script will then add the LDAP objects required for Samba. It is a good idea to first make a backup of your DIT using *slapcat*:

```
sudo slapcat -l backup.ldif
```

Once you have a backup proceed to populate your directory:

```
sudo smbldap-populate
```

You can create a LDIF file containing the new Samba objects by executing `sudo smbldap-populate -e samba.ldif`. This allows you to look over the changes making sure everything is correct. If it is, rerun the script without the '-e' switch. Alternatively, you can take the LDIF file and import its data per usual.

Your LDAP directory now has the necessary information to authenticate Samba users.

Samba Configuration

There are multiple ways to configure Samba. For details on some common configurations see Samba. To configure Samba to use LDAP, edit its configuration file `/etc/samba/smb.conf` commenting out the default *passdb backend* parameter and adding some ldap-related ones:

```
#   passdb backend = tdbsam

# LDAP Settings
   passdb backend = ldapsam:ldap://hostname
   ldap suffix = dc=example,dc=com
   ldap user suffix = ou=People
   ldap group suffix = ou=Groups
   ldap machine suffix = ou=Computers
   ldap idmap suffix = ou=Idmap
   ldap admin dn = cn=admin,dc=example,dc=com
   ldap ssl = start tls
   ldap passwd sync = yes
...
   add machine script = sudo /usr/sbin/smbldap-useradd -t 0 -w "%u"
```

Change the values to match your environment.

Restart *samba* to enable the new settings:

```
sudo systemctl restart smbd.service nmbd.service
```

Now inform Samba about the rootDN user's password (the one set during the installation of the slapd package):

```
sudo smbpasswd -w password
```

If you have existing LDAP users that you want to include in your new LDAP-backed Samba they will, of course, also need to be given some of the extra attributes. The *smbpasswd* utility can do this as well (your host will need to be able to see (enumerate) those users via NSS; install and configure either *libnss-ldapd* or *libnss-ldap*):

```
sudo smbpasswd -a username
```

You will prompted to enter a password. It will be considered as the new password for that user. Making it the same as before is reasonable.

To manage user, group, and machine accounts use the utilities provided by the *smbldap-tools* package. Here are some examples:

1. To add a new user:

   ```
   sudo smbldap-useradd -a -P username
   ```

   The *-a* option adds the Samba attributes, and the *-P* option calls the *smbldap-passwd* utility after the user is created allowing you to enter a password for the user.

2. To remove a user:

   ```
   sudo smbldap-userdel username
   ```

   In the above command, use the *-r* option to remove the user's home directory.

3. To add a group:

   ```
   sudo smbldap-groupadd -a groupname
   ```

As for *smbldap-useradd*, the *-a* adds the Samba attributes.

4. To make an existing user a member of a group:

```
sudo smbldap-groupmod -m username groupname
```

The *-m* option can add more than one user at a time by listing them in comma-separated format.

5. To remove a user from a group:

```
sudo smbldap-groupmod -x username groupname
```

6. To add a Samba machine account:

```
sudo smbldap-useradd -t 0 -w username
```

Replace *username* with the name of the workstation. The *-t 0* option creates the machine account without a delay, while the *-w* option specifies the user as a machine account. Also, note the *add machine script* parameter in `/etc/samba/smb.conf` was changed to use *smbldap-useradd*.

There are utilities in the *smbldap-tools* package that were not covered here. Here is a complete list:

```
smbldap-groupadd
smbldap-groupdel
smbldap-groupmod
smbldap-groupshow
smbldap-passwd
smbldap-populate
smbldap-useradd
smbldap-userdel
smbldap-userinfo
smbldap-userlist
smbldap-usermod
smbldap-usershow
```

Resources

1. For more information on installing and configuring Samba see Samba of this Ubuntu Server Guide.
2. There are multiple places where LDAP and Samba is documented in the upstream Samba HOWTO Collection.
3. Regarding the above, see specifically the passdb section.
4. Although dated (2007), the Linux Samba-OpenLDAP HOWTO contains valuable notes.
5. The main page of the Samba Ubuntu community documentation has a plethora of links to articles that may prove useful.

Previous Next