BarryODonovan.com
Thoughts, ramblings and rants...

Multi-Master LDAP Replication

Following up from my articles on Creating an LDAP Addressbook / Directory and then Securing LDAP with TLS / SSL, I'll now focus on multi-master replication. Actually, this example will focus on master-master but it can easily be extended out to multi-master.

If you've been reading the other articles, then **some caveats and differences apply here:**

- if you plan to set up replication, I recommend you do it from the beginning which is what this article looks at;
- in the Addressbook articale, we created a new dedicated database for the addressbook. Herein however, I replicate the default database. I'll explain how to replicate any given database below too.

For your environment, ensure you have DNS names registered or that you are using named hosts defined in the */etc/hosts* file. For our case, let's assume we have a *hosts* file entry as follows:

```
1 10.20.30.40    ldap1
2 10.20.30.41    ldap2
```

and, for each of the two hosts, we have respectively included the following in the *SLAPD_SERVICES* variable in */etc/defaults/slapd* of each host (change for ldap2):

```
1 SLAPD_SERVICES="ldap://ldap1/ ...."
```

I'm going to write each of the following LDIFs as commands you can copy and paste.

We're going to start by setting server IDs, loading the *syncprov* module and creating a user for syncing the config database. On *ldap1*:

```
cat &lt;&lt;EOF | ldapmodify -Y EXTERNAL -H ldapi:///
dn: cn=config
changetype: modify
add: olcServerID
olcServerID: 1
EOF
```

Repeat above on *ldap2* but change the server ID to 2. Then, on both:

```
cat &lt;&lt;EOF | ldapmodify -Y EXTERNAL -H ldapi:///
dn: cn=module{0},cn=config
changetype: modify
add: olcModuleLoad
olcModuleLoad: {1}syncprov.la
EOF
```

On the above, ensure *{1}* is the next available module sequence by running the following first:

```
ldapsearch -Y EXTERNAL -H ldapi:/// -b cn=module{0},cn=config
```

Now, again on both servers:

```
cat &lt;&lt;EOF | ldapmodify -Y EXTERNAL -H ldapi:///
dn: olcDatabase={0}config,cn=config
changetype: modify
add: olcRootPW
olcRootPW:&amp;nbsp;h.TDVyELBjm0g
EOF
```

We now need to update the server IDs and those of our peers. So, on both servers, run:

```
cat &lt;&lt;EOF | ldapmodify -Y EXTERNAL -H ldapi:///
dn: cn=config
changetype: modify
replace: olcServerID
olcServerID: 1 ldap://ldap1/
olcServerID: 2 ldap://ldap2/
EOF
```

To get the replication running for the config database, we run the

following on both servers:

```
cat &lt;&lt;EOF | ldapmodify -Y EXTERNAL -H ldapi:///
dn: olcOverlay=syncprov,olcDatabase={0}config,cn=config
changetype: add
objectClass: olcOverlayConfig
objectClass: olcSyncProvConfig
olcOverlay: syncprov
EOF
```

```
cat &lt;&lt;EOF | ldapmodify -Y EXTERNAL -H ldapi:///
dn: olcDatabase={0}config,cn=config
changetype: modify
add: olcSyncRepl
olcSyncRepl: rid=001 provider=ldap://ldap1/ binddn="cn=config"
  bindmethod=simple credentials=h.TDVyELBjm0g
  searchbase="cn=config" type=refreshAndPersist
  retry="5 5 300 5" timeout=1
olcSyncRepl: rid=002 provider=ldap://ldap2/ binddn="cn=config"
  bindmethod=simple credentials=h.TDVyELBjm0g
  searchbase="cn=config" type=refreshAndPersist
  retry="5 5 300 5" timeout=1
-
add: olcMirrorMode
olcMirrorMode: TRUE
EOF
```

You now have 2-way master-master replication of the configuration database. Make sure you check the logs for any issues and you can easily test by changing a config option on first, verifying on the second, reverting on the second and verifying again on the first.

We can now replicate any other database by using similar changes to the above. Let's say we want to replicate the database *olcDatabase={1}hdb,cn=config*, then execute the following **on one server – remember, your configuration is now replicated!**

```
cat &lt;&lt;EOF | ldapmodify -Y EXTERNAL -H ldapi:///
dn: olcDatabase={1}hdb,cn=config
changetype: modify
add: olcLimits
olcLimits: dn.exact="cn=admin,dc=nodomain" time.soft=unlimited
  time.hard=unlimited size.soft=unlimited size.hard=unlimited
-
add: olcSyncRepl
olcSyncRepl: rid=004 provider=ldap://ldap1/ binddn="cn=admin,dc=nodomain"
  bindmethod=simple credentials=O4PbIOzA9gvEQ searchbase="dc=nodomain"
  type=refreshOnly interval=00:00:00:10 retry="5 5 300 5" timeout=1
olcSyncRepl: rid=005 provider=ldap://ldap2/ binddn="cn=admin,dc=nodomain"
  bindmethod=simple credentials=O4PbIOzA9gvEQ searchbase="dc=nodomain"
  type=refreshOnly interval=00:00:00:10 retry="5 5 300 5" timeout=1
```

```
15 -
16 add: olcDbIndex
17 olcDbIndex: entryUUID  eq
18 -
19 add: olcDbIndex
20 olcDbIndex: entryCSN  eq
21 -
22 add: olcMirrorMode
23 olcMirrorMode: TRUE
24 EOF
```

NB: ensure you change the admin user and password above as appropriate for your database. Specifically, it should be the *olcRootDN* and *oldRootPW* as listed in the *olcDatabase={1}hdb,cn=config* object. Finally, execute the following on **one server**.

```
1 cat &lt;&lt;EOF | ldapmodify -Y EXTERNAL -H ldapi:///
2 dn: olcOverlay=syncprov,olcDatabase={1}hdb,cn=config
3 changetype: add
4 objectClass: olcOverlayConfig
5 objectClass: olcSyncProvConfig
6 olcOverlay: syncprov
7 EOF
```

References

- http://www.openldap.org/doc/admin24/replication.html#N-Way Multi-Master
- https://help.ubuntu.com/10.04/serverguide/openldap-server.html

Barry O'Donovan / January 28, 2013 / News / addressbook, ldap, openldap