

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 article, 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 &nbsp; &nbsp; ldap1
2 10.20.30.41 &nbsp; &nbsp; 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*:

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

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

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

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

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

Now, again on both servers:

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

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

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

7 EOF

To get the replication running for the config database, we run the following on both servers:

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

```
1 cat &lt;&lt;EOF | ldapmodify -Y EXTERNAL -H ldapi:///
2 dn: olcDatabase={0}config,cn=config
3 changetype: modify
4 add: olcSyncRepl
5 olcSyncRepl: rid=001 provider=ldap://ldap1/ binddn="cn=config"
6   bindmethod=simple credentials=h.TDVyELBjm0g
7   searchbase="cn=config" type=refreshAndPersist
8   retry="5 5 300 5" timeout=1
9 olcSyncRepl: rid=002 provider=ldap://ldap2/ binddn="cn=config"
10  bindmethod=simple credentials=h.TDVyELBjm0g
11  searchbase="cn=config" type=refreshAndPersist
12  retry="5 5 300 5" timeout=1
13 -
14 add: olcMirrorMode
15 olcMirrorMode: TRUE
16 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!**

```
1 cat &lt;&lt;EOF | ldapmodify -Y EXTERNAL -H ldapi:///
2 dn: olcDatabase={1}hdb,cn=config
3 changetype: modify
4 add: olcLimits
5 olcLimits: dn.exact="cn=admin,dc=nodomain" time.soft=unlimited
6   time.hard=unlimited size.soft=unlimited size.hard=unlimited
```

```
7 -
8 add: olcSyncRepl
9 olcSyncRepl: rid=004 provider=ldap://ldap1/ binddn="cn=admin,dc=nodomain"
10 bindmethod=simple credentials=04PbI0zA9gvEQ searchbase="dc=nodomain"
11 type=refreshOnly interval=00:00:00:10 retry="5 5 300 5" timeout=1
12 olcSyncRepl: rid=005 provider=ldap://ldap2/ binddn="cn=admin,dc=nodomain"
13 bindmethod=simple credentials=04PbI0zA9gvEQ searchbase="dc=nodomain"
14 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;&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>

Share this:





Barry O'Donovan / January 28, 2013 / News / [addressbook](#), [ldap](#), [openldap](#)

[BarryODonovan.com](#) / Proudly powered by [WordPress](#)