New Replication Features in OpenLDAP

Howard Chu
CTO, Symas Corp.  hyc@symas.com
Chief Architect, OpenLDAP  hyc@openldap.org
2019-11-06
Context

- Syncrepl has been in OpenLDAP since 2003
  - Open spec, but still not widely implemented
  - ApacheDS appears to be the only other
- Migration from other servers has become more urgent
  - SunDS has reached end of life
  - Microsoft AD doesn’t perform well enough to be a primary LDAP server
Approach

- Small extensions to the existing Syncrepl consumer
  - Stubs for SunDS retro-changelog replication already existed
  - Never got fleshed out before due to lack of demand
  - The demand exists today
  - Needs 11 new attributes, 1 new objectclass (in schema/dsee.schema)
  - Supports refreshOnly and refreshAndPersist with syncdata=changelog
Changelog Config

- See test072 and test075 in the test suite
- Simple setup of DSEE

```bash
# Test replication:
#   - start provider
#   - start consumer
#   - populate over ldap
#   - perform some modifies and deleted
#   - attempt to modify the consumer (referral)
#   - retrieve database over ldap and compare against expected results

DSEEPr#="secret21"
DSEEEN="cn=Directory Manager"
DSEEFPW="$TESTDIR/dseepw"

echo "secret21" > $DSEEFPW

echo "Setting up DSEE provider slapd on TCP/IP port $PORT1..."
dsadm create -p $PORT1 -w $DSEEFPW $DBDIR1
dsadm start $DBDIR1
dconf create-suffix -c -p $PORT1 -w $DSEEFPW $BASEDN
dconf set-server-prop -p $PORT1 -w $DSEEFPW moddn-enabled:on
dconf set-server-prop -p $PORT1 -w $DSEEFPW retro-cl-enabled:on
dsadm restart $DBDIR1
KILLPIDS='basename $DBDIR1/locks/server/*'
```
Changelog Config

- See test072 and test075 in the test suite
  - Syncrepl stanza

```bash
syncrep1
  rid=1
  provider=@URI1@
  binddn="cn=Directory Manager"
  bindmethod=simple
  credentials=secret21
  searchbase="dc=example,dc=com"
  filter="(objectClass=*)"
  schemachecking=off
  scope=sub
  type=refreshOnly
  logbase="cn=changelog"
  syncdata=changelog
  retry="3 + " interval=00:00:00:03
  @URI1@
```

MSAD DIRSYNC

- For sites that only need user/group info, and not full AD compatibility (use Samba for that)
- Slightly less convenient, requires loading ~1000 attributetypes and a few objectclasses (in schema/msuser.schema)
- Only works with scheduled polling, no persist support
MSAD Config

- See test071 in the test suite
- Configure type=dirSync
Caveats

- Both MSAD DirSync and DSEE changelog replication use host-specific changeNumbers
  - Not valid if you switch to a different provider server
  - Unlike Syncrepl contextCSNs / entryCSNs
- Replication to MSAD or DSEE not supported