Multi-Master Replication

Delta-Syncrepl

READ FIRST: In the following lab the two servers have the fqdns producer.ldap and consumer.ldap. These servers can ping each other by hostname and IP address. Name resolution is handled via the /etc/hosts file. Adjust these values to match your environment and ensure name resolution succeeds **before** proceeding.

1. Delete and recreate the slapd.d directory. Then convert slapd.conf to slapd.d on both VMs

```
rm -rf slapd.d

mkdir slapd.d

slaptest -f slapd.conf -F slapd.d

service solserver restart
```

2. Use the following commands to configure delta-syncrepl replication:
   Configure the **1st Producer** server
   In the CN=Config section include the following:
   Server ID (place as the first line of the file)

```
ldapmodify -x -H ldap://producer.ldap -D cn=config -w secret
dn: cn=config
changetype: modify
add: olcServerID
olcServerID: 001 ldap://producer.ldap/
```

   SyncProv and Accesslog Modules

```
ldapmodify -x -H ldap://producer.ldap -D cn=config -w secret
dn: cn=module{0},cn=config
changetype: modify
add: olcModuleload
olcModuleload: syncprov.la
-
add: olcModuleload
olcModuleload: accesslog.la
```

   In the Database={1}MDB section include the following:
   Indexing

```
ldapmodify -x -H ldap://producer.ldap -D cn=config -w secret
dn: olcDatabase={1}mdb,cn=config
changetype: modify
add: olcDbIndex
olcDbIndex: entryCSN eq
-
add: olcDbIndex
olcDbIndex: entryUUID eq
```

   Syncrepl (note: the olcSyncrepl stanza is one continuous line that has been word-wrapped)

```
ldapmodify -x -H ldap://producer.ldap -D cn=config -w secret
dn: olcDatabase={1}mdb,cn=config
changetype: modify
add: olcSyncrepl
olcSyncrepl: rid=001 provider=ldap://consumer.ldap bindmethod=simple
binddn="dc=example,dc=com" credentials="secret"
searchbase="dc=example,dc=com" type=refreshAndPersist retry="60 +"
```

```
logbase="cn=accesslog"
logfilter="(&(objectClass=auditWriteObject)(reqResult=0))"
syncdata=accesslog schemachecking=on network-timeout=30
keepalive=180:3:60
-
add: olcMirrorMode
olcMirrorMode: TRUE
```

SyncProv Overlay

```
ldapadd -x -H ldap://producer.ldap -D cn=config -w secret
dn: olcOverlay={1}syncprov,olcDatabase={1}mdb,cn=config
objectClass: olcSyncProvConfig
objectClass: olcOverlayConfig
olcOverlay: {1}syncprov
olcSpCheckpoint: 100 10
olcSpSessionlog: 10000
```

Create a new database that includes the following:

Accesslog database

```
ldapadd -x -H ldap://producer.ldap -D cn=config -w secret
dn: olcDatabase={2}mdb,cn=config
objectClass: olcMdbConfig
objectClass: olcDatabaseConfig
olcDatabase: {2}mdb
olcDbDirectory: /var/symas/openldap-data/accesslog
olcAddContentAcl: FALSE
olcDbIndex: default eq
olcDbIndex: objectClass eq
olcDbIndex: entryCSN eq
olcDbIndex: reqDN eq
olcDbIndex: reqStart eq
olcDbIndex: reqEnd eq
olcDbIndex: reqResult eq
olcDbMaxEntrySize: 0
olcDbMaxReaders: 0
olcDbMaxSize: 5120000
olcDbMode: 0600
olcDbMultivalHi: 4294967295
olcDbMultivalLo: 4294967295
olcDbNoSync: FALSE
olcDbRtxnSize: 10000
olcDbSearchStack: 16
olcLastMod: TRUE
olcMaxDerefDepth: 15
olcMonitoring: TRUE
olcReadOnly: FALSE
olcRootDN: cn=config
olcSuffix: cn=accesslog
olcSyncUseSubentry: FALSE
```

Define only the syncprov overlay for the Accesslog database

```
ldapadd -x -H ldap://producer.ldap -D cn=config -w secret
```

```
dn: olcOverlay={0}syncprov,olcDatabase={2}mdb,cn=config
objectClass: olcSyncProvConfig
objectClass: olcOverlayConfig
olcOverlay: {0}syncprov
olcSpNoPresent: TRUE
olcSpReloadHint: TRUE
```

Add the AccessLog Overlay to the MDB database

```
ldapadd -x -H ldap://producer.ldap -D cn=config -w secret
dn: olcOverlay={0}accesslog,olcDatabase={1}mdb,cn=config
objectClass: olcAccessLogConfig
objectClass: olcOverlayConfig
olcAccessLogDB: cn=accesslog
olcOverlay: {0}accesslog
olcAccessLogOps: writes
olcAccessLogPurge: 24:00 1+00:00
olcAccessLogSuccess: TRUE
```

Remove and recreate a new database directory

```
rm -rf /var/symas/openldap-data/accesslog/

mkdir /var/symas/openldap-data/accesslog
```

Configure the **2nd Producer** server

In the CN=Config section include the following:

Server ID (place as the first line of the file)

```
ldapmodify -x -H ldap://consumer.ldap -D cn=config -w secret
dn: cn=config
changetype: modify
add: olcServerID
olcServerID: 002 ldap://consumer.ldap/
```

SyncProv and Accesslog Modules

```
ldapmodify -x -H ldap://consumer.ldap -D cn=config -w secret
dn: cn=module{0},cn=config
changetype: modify
add: olcModuleload
olcModuleload: syncprov.la
-
add: olcModuleload
olcModuleload: accesslog.la
```

In the Database={1}MDB section include the following:

Indexing

```
ldapmodify -x -H ldap://consumer.ldap -D cn=config -w secret
dn: olcDatabase={1}mdb,cn=config
changetype: modify
add: olcDbIndex
olcDbIndex: entryCSN eq
-
add: olcDbIndex
olcDbIndex: entryUUID eq
```

Syncrepl (note: the olcSyncrepl stanza is one continuous line that has been word-wrapped)

```
ldapmodify -x -H ldap://consumer.ldap -D cn=config -w secret
dn: olcDatabase={1}mdb,cn=config
changetype: modify
add: olcSyncrepl
olcSyncrepl: rid=001 provider=ldap://producer.ldap bindmethod=simple
binddn="dc=example,dc=com" credentials="secret"
searchbase="dc=example,dc=com" type=refreshAndPersist retry="60 +"
logbase="cn=accesslog"
logfilter="(&(objectClass=auditWriteObject)(reqResult=0))"
syncdata=accesslog schemachecking=on network-timeout=30
keepalive=180:3:60
-
add: olcMirrorMode
olcMirrorMode: TRUE
```

SyncProv Overlay

```
ldapadd -x -H ldap://consumer.ldap -D cn=config -w secret
dn: olcOverlay={1}syncprov,olcDatabase={1}mdb,cn=config
objectClass: olcSyncProvConfig
objectClass: olcOverlayConfig
olcOverlay: {1}syncprov
olcSpCheckpoint: 100 10
olcSpSessionlog: 10000
```

Create a new database that includes the following:

Accesslog database

```
ldapadd -x -H ldap://consumer.ldap -D cn=config -w secret
dn: olcDatabase={2}mdb,cn=config
objectClass: olcMdbConfig
objectClass: olcDatabaseConfig
olcDatabase: {2}mdb
olcDbDirectory: /var/symas/openldap-data/accesslog
olcAddContentAcl: FALSE
olcDbIndex: default eq
olcDbIndex: objectClass eq
olcDbIndex: entryUUID eq
olcDbIndex: entryCSN eq
olcDbIndex: reqStart eq
olcDbIndex: reqEnd eq
olcDbIndex: reqResult eq
olcDbIndex: reqDN
olcDbMaxEntrySize: 0
olcDbMaxReaders: 0
olcDbMaxSize: 5120000
olcDbMode: 0600
olcDbMultivalHi: 4294967295
olcDbMultivalLo: 4294967295
olcDbNoSync: FALSE
olcDbRtxnSize: 10000
olcDbSearchStack: 16
olcLastMod: TRUE
olcMaxDerefDepth: 15
olcMonitoring: TRUE
```

```
olcReadOnly: FALSE
olcRootDN: cn=config
olcSuffix: cn=accesslog
olcSyncUseSubentry: FALSE
```

Define only the syncprov overlay for the Accesslog database

```
ldapadd -x -H ldap://consumer.ldap -D cn=config -w secret
dn: olcOverlay={0}syncprov,olcDatabase={2}mdb,cn=config
objectClass: olcSyncProvConfig
objectClass: olcOverlayConfig
olcOverlay: {0}syncprov
olcSpNoPresent: TRUE
olcSpReloadHint: TRUE
```

Add the AccessLog Overlay to the MDB Database

```
ldapadd -x -H ldap://consumer.ldap -D cn=config -w secret
dn: olcOverlay={0}accesslog,olcDatabase={1}mdb,cn=config
objectClass: olcAccessLogConfig
objectClass: olcOverlayConfig
olcAccessLogDB: cn=accesslog
olcOverlay: {0}accesslog
olcAccessLogOps: writes
olcAccessLogPurge: 24:00 1+00:00
olcAccessLogSuccess: TRUE
```

Remove and recreate a new database directory

```
rm -rf /var/symas/openldap-data/accesslog/

mkdir /var/symas/openldap-data/accesslog
```

3. Run a slaptest on the slapd.conf file on both VMs to test for potential failures before starting the solserver (slapd service)

```
slaptest -F slapd.d -d stats,sync
```

4. On the **2nd Producer** server, search for the description attribute of a single entry and save it to a file.

```
ldapsearch -x -H ldap://consumer.ldap -D dc=example,dc=com -w secret -b "cn=Bruce
Crowe,ou=Peons,dc=example,dc=com" -LLL description | tee toModify.ldif
```

5. Edit the toModify.ldif file to this:

```
sudo vi toModify.ldif
```

6. Insert the following:

```
dn: cn=Bruce Crowe,ou=Peons,dc=example,dc=com
changetype: modify
replace: description
description: This is the new delta-syncrepl description
ESC :wq        (Save changes and quit)
```

7. Modify the entry with ldapmodify on the **2nd Producer** (to ensure changes are referred to the **1st Producer** server).

```
ldapmodify -x -H ldap://consumer.ldap -D dc=example,dc=com -w secret -f
toModify.ldif
```

8. Verify the modify worked and was referred correctly by performing the following search on the **1st Producer** server:

```
ldapsearch -x -H ldap://producer.ldap -D dc=example,dc=com -w secret -b "cn=Bruce
Crowe,ou=Peons,dc=example,dc=com" -LLL description
```

9. On the **1st Producer** server delete the user La Valko

```
ldapdelete -x -H ldap://producer.ldap -D dc=example,dc=com -w secret "cn=Bruce
Crowe,ou=Peons,dc=example,dc=com"
```

10. Verify the entry was deleted successfully and replication is working by running the following command on the **2nd Producer** server.

```
ldapsearch -x -H ldap://consumer.ldap -D dc=example,dc=com -w secret -b "cn=Bruce
Crowe,ou=Peons,dc=example,dc=com" -LLL dn
```

The result should be `"No such object (32)"`.