1 Introduction to IBM Security Directory Server 6.4.0.20 exercises

The purpose of this lab is to demonstrate the basic features of the IBM Security Directory Server(SDS) and setup replication between two SDS servers.

This lab will consist of the following activities.

1. Create 2 IBM SDS instances
2. Import the sample data using LDIF.
3. Configure Master – Master replication within IBM Security Directory Servers.

The following lab environment has been configured:

1. Operating System – CentOS 7.7 installed on a VMware Workstation VM.

2. IBM Security Directory Server – version 6.4.0.20 x64 Linux. IBM Security Directory Server 6.4.0.20 includes the following middleware:

    - DB2® Universal Database version 11.1.4 Enterprise Server Edition (DB2) with FixPack 5
    - Global Security Kit (GSKit) Version 8.0.50
    - IBM Websphere ND 9.0.1

You have worked on LDAP in above exercises for ISIM. We will learn more things about IBM Security Directory Server(SDS) in below exercises

Installation Paths :

1.SDS - /opt/ibm/ldap/V6.4/
2. DB2 - /opt/ibm/db2/V11.1/
3. WAS - /opt/IBM/WebSphere/AppServer/

1.1 Exercise 1 – Instance Creation in SDS

Instance Creation

SDS version 6.4.0.20 allows for multiple directory server instances to be run per machine. In this lab 2 instances will be used on a single VM. The instances are to be created. The instances to be created are:

- **idsldap1** – This instance will run on port **1389** (At places this instance is also referred to as **Primary** Server in this document)

- **idsldap2** – This instance will run on port **2389** (At places this instance is also referred to as **Secondary** Server in this document)

For ISIM, we have already created on instance by default while installing ISIM, you can check the instance details using the below command in terminal:

```
/opt/ibm/ldap/V6.4/sbin/idsilist -a
```

```
Name: isimldap
Version: 6.4
Location: /home/isimldap
Description: IBM Security Directory Server Instance V6.4
IP Addresses: All available
Port: 389
Secure Port: 636
Admin Server Port: 3538
Admin Server Secure Port: 3539
Type: Directory Server
```

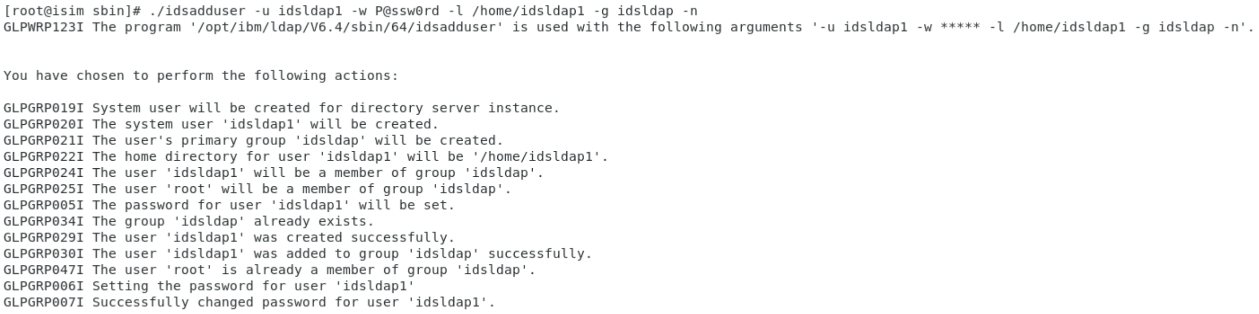
You can observe ISIM SDS instance uses the port **389** which is default LDAP port. Create the two new instances using below steps :

1. Open **Terminal** from **Desktop** and navigate to the SDS folder as below
   `cd /opt/ibm/ldap/V6.4/sbin/`

2. Create two new users **idsldap1** and **idsldap2** as the owner of two new instances using :
   `./idsadduser -u idsldap1 -w P@ssw0rd -l /home/idsldap1 -g idsldap -n`

> **Note :** Here in the command -u stands for **username**, -w for **password**, -l is home directory **location** of user, -g is the **secondary group** for user, -n for No Prompt and command will run without any prompt in console.

You can check the user is created successfully



```
[root@isim sbin]# ./idsadduser -u idsldap1 -w P@ssw0rd -l /home/idsldap1 -g idsldap -n
GLPWRP123I The program '/opt/ibm/ldap/V6.4/sbin/64/idsadduser' is used with the following arguments '-u idsldap1 -w ***** -l /home/idsldap1 -g idsldap -n'.


You have chosen to perform the following actions:

GLPGRP019I System user will be created for directory server instance.
GLPGRP020I The system user 'idsldap1' will be created.
GLPGRP021I The user's primary group 'idsldap' will be created.
GLPGRP022I The home directory for user 'idsldap1' will be '/home/idsldap1'.
GLPGRP024I The user 'idsldap1' will be a member of group 'idsldap'.
GLPGRP025I The user 'root' will be a member of group 'idsldap'.
GLPGRP005I The password for user 'idsldap1' will be set.
GLPGRP034I The group 'idsldap' already exists.
GLPGRP029I The user 'idsldap1' was created successfully.
GLPGRP030I The user 'idsldap1' was added to group 'idsldap' successfully.
GLPGRP047I The user 'root' is already a member of group 'idsldap'.
GLPGRP006I Setting the password for user 'idsldap1'
GLPGRP007I Successfully changed password for user 'idsldap1'.
```

3. Similarly, add the second user **idsldap2**
   `./idsadduser -u idsldap2 -w P@ssw0rd -l /home/idsldap2 -g idsldap -n`

4. Create the instance for the idsldap1 user using **idsicrt** command as below :
   `./idsicrt -I idsldap1 -e encryptionseed -l /home/idsldap1 -n`

> **Note :** Here in the command -I stands for **instance name** which we want to create, -e for **encryption seed** for SDS instance, -l is instance **location**, -n for No Prompt and command will run without any prompt in console.

The idsicrt command adds DB2 instance idsldap1 for the SDS in the backend and creates the instance.

5. Similarly, create the instance for the **idsldap2** user using idsicrt command as below :
   `./idsicrt -I idsldap2 -e encryptionseed -l /home/idsldap2 -n`

6. Now you can check the instance details using the below command in terminal and check the new instance idsldap1 and idsldap2 created:
   `/opt/ibm/ldap/V6.4/sbin/idsilist -a`

```
Directory server instance(s):

--------------------------------------
Instance 1:

Name: isimldap
Version: 6.4
Location: /home/isimldap
Description: IBM Security Directory Server Instance V6.4
IP Addresses: All available
Port: 389
Secure Port: 636
Admin Server Port: 3538
Admin Server Secure Port: 3539
Type: Directory Server

--------------------------------------
Instance 2:

Name: idsldap1
Version: 6.4
Location: /home/idsldap1
Description: IBM Security Directory Server Instance V6.4
IP Addresses: All available
Port: 1389
Secure Port: 1636
Admin Server Port: 3540
Admin Server Secure Port: 3541
Type: Directory Server

--------------------------------------
Instance 3:

Name: idsldap2
Version: 6.4
Location: /home/idsldap2
Description: IBM Security Directory Server Instance V6.4
IP Addresses: All available
Port: 2389
Secure Port: 2636
Admin Server Port: 3542
Admin Server Secure Port: 3543
Type: Directory Server
```

Note : We can see the the ports **1389** and **2389** are by default assigned to **idsldap1** and **idsldap2** respectively. It is default SDS behavior. You can also specify custom port using -p argument to **idsicrt** command.

7. Once the instances are created we will configure the DB2 database for the SDS instance, the DB2 database acts as the backend to **store** all the ldap entries.

   ```
   ./idscfgdb -I idsldap1 -w P@ssw0rd -a idsldap1 -t idsldap1 -l
   /home/idsldap1 -n
   ```

Note : Here in the command -I is **instance name** -w **password** of the instance owner -a is **database admin user** -t is the **database name** and -n for **no prompt.** We keep the database name and database admin user name similar to instance name (idsldap1) for convenience.

   The database idsldap1 is created in the idsldap1 DB2 instance after this command and all the SDS default **tables** are loaded into this **database**.

8. Similarly, configure database for the second instance idsldap2 with below command

   ```
   ./idscfgdb -I idsldap2 -w P@ssw0rd -a idsldap2 -t idsldap2 -l
   /home/idsldap2 -n
   ```

9. Minimize the **Terminal** window, **Double-click** the **Home** icon from **Desktop**. Click **Other Locations** in the left pane double-click **Computer** and then home and you can see the below 2 folders. The **idsldap1** and **idsldap2** are the SDS instance owner home directories.

10. **Double-click** idsldap1 directory and you can see **idsslapd-idsldap1** folder which have all instance related configurations and log files.

11. **Minimize** the **Files** window and go back to **Terminal** window. Create admin user (**cn=root**) who can be used to do the administrative task on the ldap instances

    ```
    ./idsdnpw -I idsldap1 -u cn=root -p P@ssw0rd -n
    ```

Note : Here in the command -I is **instance name** -u **user name** of the instance admin -p for **password** of admin user -n for **no prompt.**

12. Similarly, for **idsldap2** instance create the admin user cn=root as below:

    ```
    ./idsdnpw -I idsldap2 -u cn=root -p P@ssw0rd -n
    ```

    The user is successfully created. We will use this user to connect to the ldap and perform admin tasks.

13. Close **Terminal**.

1.2 Exercise 2 –Start and Stop IBM SDS instances

To start and stop IBM SDS instances follow below steps:

1. Open **Terminal** from Desktop.

2. **Start** the newly created SDS instance **idsldap1** using below command:
```
/opt/ibm/ldap/V6.4/sbin/ibmslapd -I idsldap1 -n -t
```

Note : Here in the command -I is **instance name** -n is to start -t to tail logs in console.

You can see the server is started.

3. Similary, start the **idsldap2** instance using :
```
/opt/ibm/ldap/V6.4/sbin/ibmslapd -I idsldap2 -n -t
```

4. To **stop** the instance idsldap1 enter the below command :
```
/opt/ibm/ldap/V6.4/sbin/ibmslapd -I idsldap1 -k
```

5. Similarly, to **stop** the idsldap2 instance enter below command:
```
/opt/ibm/ldap/V6.4/sbin/ibmslapd -I idsldap2 -k
```

6. **Start** both the instances again :
```
/opt/ibm/ldap/V6.4/sbin/ibmslapd -I idsldap1 -n -t
```
After startup is completed
```
/opt/ibm/ldap/V6.4/sbin/ibmslapd -I idsldap2 -n -t
```

Note : Start and Stop SDS instances using above commands for all the exercises below.

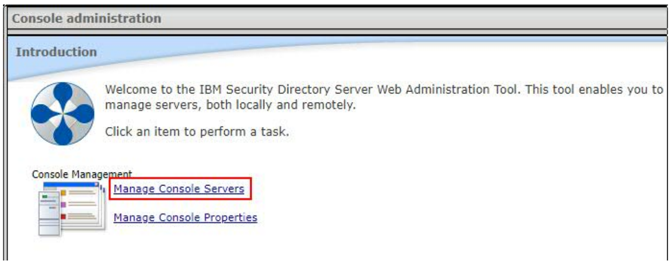
1.3 Exercise 3 – SDS Web Admin tool

The Web admin tool(WAT) is already installed on the WAS (Websphere) server. We will verify the instances using the WAT.

1. Open the Firefox browser from the task bar and enter the below URL or Click the **Web Admin Tool Bookmark** in the Bookmark bar.
https://isim.test:9444/IDSWebApp/

2. Click on **Login to Console admin**. Enter the credentials as **superadmin** using the password **secret**. This is default password for WAT superadmin.

3. Click on **Manage Console Servers.**



Console administration

Introduction

Welcome to the IBM Security Directory Server Web Administration Tool. This tool enables you to manage servers, both locally and remotely.

Click an item to perform a task.

Console Management

Manage Console Servers

Manage Console Properties

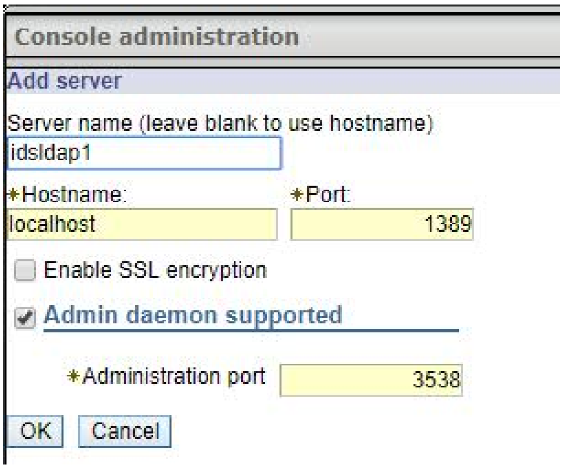
4. Click on **Add.**

   Enter the following details -

   Server name **- idsldap1**

   Hostname : **localhost**

   Port : **1389**



Console administration

Add server

Server name (leave blank to use hostname)

idsldap1

*Hostname: localhost

*Port: 1389

□ Enable SSL encryption

☑ Admin daemon supported

*Administration port 3538

Click **OK and OK on next screen.**

5. Click on **Add.**

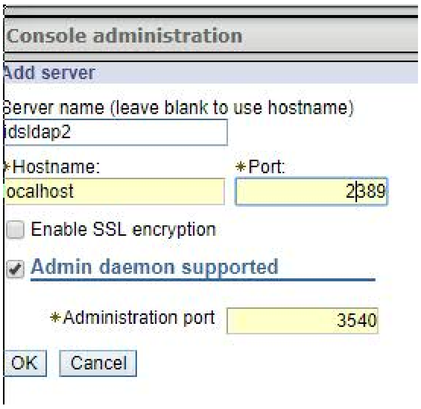
   Enter the following details -

   Server name **- idsldap2**

   Hostname : **localhost**

   Port : **2389**

   Administration port: **3540**



Console administration

Add server

Server name (leave blank to use hostname): idsldap2

*Hostname: ocalhost

*Port: 2389

☐ Enable SSL encryption

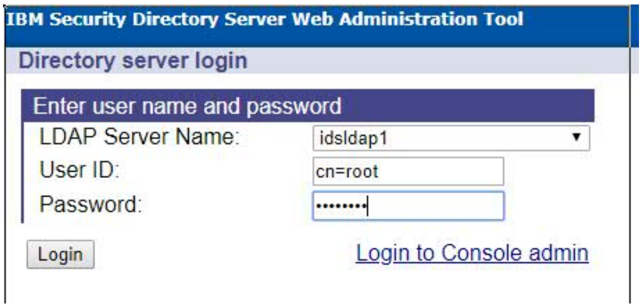
☑ Admin daemon supported

*Administration port: 3540

Click **OK and OK on next screen.**

6. Click on **Logout** in the left pane and then on next screen press on **here.**

7. Now we will get the LDAP Server Name. Select idsldap1 and enter the credential cn=**root/P@ssw0rd**



IBM Security Directory Server Web Administration Tool

Directory server login

Enter user name and password

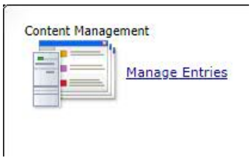
LDAP Server Name: idsldap1

User ID: cn=root

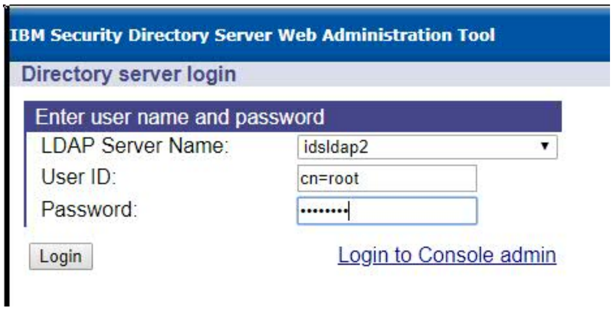
Password: ••••••••

Click on **Login.**

8. Click **Manage Entries** in the Content Management Section . There are few default entries created by SDS when the instance is created.



9. Press **Logout** in Left Pane and login with **idsldap2** with Userid **cn=root/P@ssw0rd**



IBM Security Directory Server Web Administration Tool

Directory server login

Enter user name and password

LDAP Server Name: idsldap2

User ID: cn=root

Password: ••••••••

Click **Login**.

10. Click **Manage Entrie**s as above steps and similar data will be shown as idsldap1.

> **Note :** Always check the **top bar** after login if you login using idsldap1 it should be **localhost:1389** and if using idsldap2 it should be **localhost:2389**. Sometimes due to caching other server page can be open. In that case, clear the browser cache. **(Ctr+Shift+Del) Clear Data**

1.4 Exercise 4 – Create Suffix and Load Organization data

You must create and configure at least one suffix before you add an LDAP entry to a directory server instance.

1. To add the suffix **stop** both the SDS instances. Open **terminal** and enter command:

   ```
   /opt/ibm/ldap/V6.4/sbin/ibmslapd -I idsldap1 -k
   ```
   and then for idsldap2,
   ```
   /opt/ibm/ldap/V6.4/sbin/ibmslapd -I idsldap2 -k
   ```

2. Since we will be loading data into the directory servers, it is necessary to **add** the **base suffix** into the directory server configuration. We will be using the “**o=jke**” suffix. In **terminal** enter the commands:

   ```
   /opt/ibm/ldap/V6.4/sbin/idscfgsuf -I idsldap1 -s "o=jke" -n
   ```

   and then for idsldap2,

   ```
   /opt/ibm/ldap/V6.4/sbin/idscfgsuf -I idsldap2 -s "o=jke" -n
   ```

   The suffix are added.

3. Start the IBM SDS instances using below commands:

   ```
   /opt/ibm/ldap/V6.4/sbin/ibmslapd -I idsldap1 -n -t
   ```
   for idsldap2,
   ```
   /opt/ibm/ldap/V6.4/sbin/ibmslapd -I idsldap2 -n -t
   ```

4. Now that the suffix information has been added, and the directory server instances have been started – it is necessary to add the “**o=jke**” organization information to the directory tree.

5. In the **terminal** enter below command for **idsldap1**,

   ```
   /opt/ibm/ldap/V6.4/bin/idsldapadd -D cn=root -w P@ssw0rd -p 1389
   ```

<press **enter**, and then enter the following data, enter each line one by one>

```
dn: o=jke

objectclass: organization

objectclass: top

o: jke
```

<press **enter** twice, a message saying the entry has been added>

hit <control C> to quit the ldapmodify command.

> **Note :** Here in the command idsldapadd is used to add entry in LDAP. **-D** specifies the binding user we use **cn=root,** the admin user. -p **1389** defines port in our case it is for idsldap1 instance and tries to modify idsldap1 instance.
> Objectclass defines what kind of object o=jke is, in our case it is type '**organization**'.

6. Similarly, for idsldap2 add the o=jke entry as organization, we use 2389 port to imply the idsldap2 instance in the command

```
/opt/ibm/ldap/V6.4/bin/idsldapadd -D cn=root -w P@ssw0rd -p 2389
```

<press **enter**, and then enter the following data, enter each line one by one>

```
dn: o=jke

objectclass: organization

objectclass: top

o: jke
```

<press **enter** twice, a message saying the entry has been added>

hit <control C> to quit the ldapmodify command.

> **Note :** The organization information is added in the o=jke suffix and now we can create entries in this suffix. **In the commands we have used -p 1389 and -p 2389 to identify the two different instances.**

7. Minimize **Terminal**. Open **Firefox** and click **Web Admin Tool Bookmark**. Login to **idsldap** using cn=root/P@ssw0rd.

8. Click **Manage Entries** from Content Management section on Homepage. You can see the organization information o=jke is added. **Logout** from idsldap1.

9. Login to **idsldap2** using **cn=root/P@ssw0rd** and you can see similar entries in idsldap2 instance.

10. **Logout**. Close **Firefox**.

1.5 Exercise 5 – Import LDIF

The LDAP Data Interchange Format (LDIF) is a standard plain text data interchange format for representing LDAP (Lightweight Directory Access Protocol) directory content and update requests.

We will see the two ways of importing LDIF :

- Import LDIF using Command Line
- Import LDIF using LDAP Browser.

Import LDIF using Command Line in Terminal

1. We will import user data into the organization **“o=jke”** using LDIF file. Open **Terminal**. Navigate to /classfiles

   ```
   cd /classfiles
   ```

2. Create the file **User1.ldif** in this folder. Use **gedit** to open

   ```
   gedit User1.ldif
   ```

3. Copy or type the below ldif entries into the file:

LDIF Entries

```
dn: cn=joe, o=jke
objectclass: person
objectclass: top
sn: walter

dn: cn=carry, o=jke
objectclass: person
objectclass: top
sn: jones
```

4. **Save** the file and **Close**.

5. In the terminal enter the idsldapadd command as below for idsldap1 :

   ```
   /opt/ibm/ldap/V6.4/bin/idsldapadd -D cn=root -w P@ssw0rd -p 1389 -i /classfiles/User1.ldif
   ```

   You can see the output as below:

   ```
   Operation 0 adding new entry cn=joe, o=jke

   Operation 1 adding new entry cn=carry, o=jke
   ```

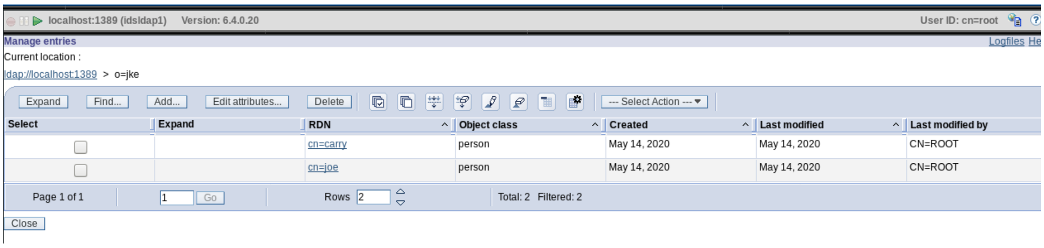
   Two users are added **successfully**.

Note : Users are currently only added in **idsldap1** instance as we have hit the command specifying the -p **1389** port which is for **idsldap1**

6. Verify if the users are added into the **idsldap1** instance of SDS using WAT. Open **Firefox**. Click **Web Admin Tool** bookmark.

7. Login to **idsldap1** using **cn=root/P@ssw0rd.**

8. Click **Manage Entries** in Content Management section. Click the plus (+) sign near o=jke and you can see two users **joe** and **carry** are displayed.



localhost:1389 (idsldap1) Version: 6.4.0.20 User ID: cn=root

Manage entries

Logfiles He

Current location :

ldap://localhost:1389 > o=jke

Select	Expand	RDN	Object class	Created	Last modified	Last modified by
□		cn=carry	person	May 14, 2020	May 14, 2020	CN=ROOT
□		cn=joe	person	May 14, 2020	May 14, 2020	CN=ROOT

Page 1 of 1 1 Go Rows 2 Total: 2 Filtered: 2

9. You can **click** cn=joe and see some extra details. Click **Cancel** and then Close. Click **Logout** in left pane.

10. Open the **Terminal** window and repeat the above step of **idsldap2** using the port **2389**. Enter the command as below

```
/opt/ibm/ldap/V6.4/bin/idsldapadd  -D  cn=root  -w  P@ssw0rd  -p  2389  -i
/classfiles/User1.ldif
```

11. Similar output window will be shown, now open **Firefox** and login to **idsldap2** into (Web Admin Tool) WAT in Firefox. Verify the same data on **idsldap2** on the same lines we check for idsldap1.

Import LDIF using LDAP Broswer

12. We will import user data into the organization "o=jke" using LDIF file. Open Terminal. Navigate to /classfiles

```
cd /classfiles
```

13. Create the file **User2.ldif** in this folder. Use **gedit** to open

```
gedit User2.ldif
```

14. Copy or type the below ldif entries into the file:

LDIF Entries
dn: cn=dan, o=jke objectclass: top objectclass: person sn: smith cn: dan dn: cn=bob, o=jke objectclass: top objectclass: person sn: bolter cn: bob

15. Open **LDAP Browser** by double-click on LDAP Browser of **Desktop**.

16. To add new connection of idsldap1 instance Click **New**.

17. Enter name : **IDSLDAP1**. Click the **Connection** tab.

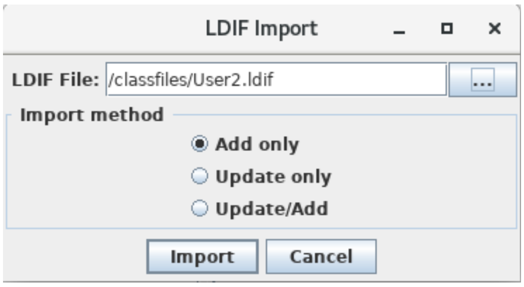
18. Enter the details as below

Field	Value
Host	localhost
Port	1389
Version	3
Base DN (Click Fetch DN)	o=jke
Anonymous Bind	Uncheck
User DN	cn=root
Password	P@ssw0rd

19. Click **Save**. Select **IDSLDAP1** and Click **Connect**.
    You will be able to see the entries in the IDSLDAP1.

20. Click **o=jke** and in **Menu Bar** Click **LDIF**. Click **Import**.

21. **Browse** to /classfiles, click **User2.ldif.** Click **OK**. Select **Add Only.**



LDIF Import

LDIF File: /classfiles/User2.ldif

Import method

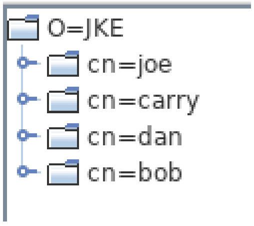
● Add only

○ Update only

○ Update/Add

22. Click **Import**. Click **Ok** on success message.

23. You can see users **bob** and **dan** are imported in LDAP. Click on o=JKE and Click the refresh icon ⟳



O=JKE
- cn=joe
- cn=carry
- cn=dan
- cn=bob

24. Repeat similar steps for IDSLDAP2. From **Menu bar→ File → Disconnect**

25. Menu bar→ File → Connect

26. Create connection for IDSLDAP2. Click **New**.

27. Enter name : **IDSLDAP2**. Click the **Connection** tab.

28. Enter the details as below

Field	Value
Host	localhost
Port	2389
Version	3
Base DN (Click Fetch DN)	o=jke
Anonymous Bind	Uncheck
User DN	cn=root
Password	P@ssw0rd

29. Click **Save**. Select **IDSLDAP2** and Click **Connect**.

30. You will be able to see the entries in the **IDSLDAP2**. We will import the **User2.ldif** in the similar fashion. Repeat above steps 20 to 22 to import the ldif and verify.

31. **Close** the LDAP Browser.

1.6 Exercise 6 – Replication

Replication is a technique used by Directory Servers to improve performance, availability, and reliability. The replication process keeps the data in multiple Directory Servers synchronized.

Here we replicate data between SDS instance idsldap1 and idsldap2 as we do not have 2 servers we will use 2 instances to act as 2 servers one services running on port 1389(idsldap1) and other on 2389(idsldap2).

Create Replication Credentials on IDSLDAP1

1. Open **Firefox**. Click on the **Web Admin Tool SDS bookmark** on bookmark toolbar.

2. Login to LDAPServer **idsldap1** using **cn=root/P@ssw0rd.**

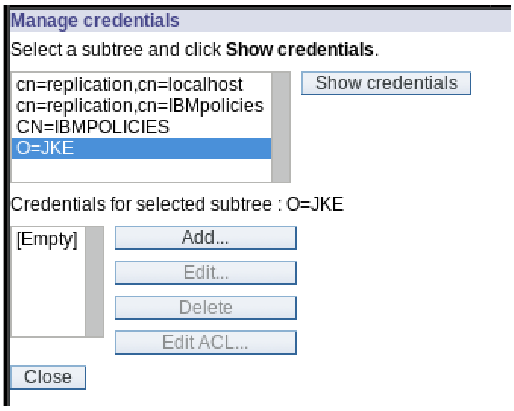
> **Note :** Always check the top bar after login if you login using idsldap1 it should be localhost:1389 and if using idsldap2 it should be localhost:2389. Sometimes due to caching other server page can be open. In that case, clear the browser cache. **(Ctr+Shift+Del) Clear Data**

3. Select **Replication Management** on left pane. Click **Manage Topology.**

4. Click the **Add** subtree button
   a. Select **o=jke** in the Subtree DN box from **Browse**.
   b. Check to ensure **ldap://localhost:1389** is in the **Master server referral URL** box

5. Click the **OK** button to **save** the changes

6. In **Replication Management,** click **Manage credentials.**
   a. **Select** O=JKE from the subtree list
   b. Click the **Show Credentials** button – there should be no credentials listed for the O=JKE tree
   The following screen capture shows what these steps should look like:



Manage credentials

Select a subtree and click **Show credentials**.

cn=replication,cn=localhost
cn=replication,cn=IBMpolicies
CN=IBMPOLICIES
O=JKE

Credentials for selected subtree : O=JKE

[Empty]

7. Click the **Add** button - to add the credentials for the replicated subtree

8. Add the credential information
   Credential Name – **cn=replicamanager**
   Authentication method – **Simple bind**

9. Click the **Next** button.

10. Enter the Simple Bind information
    Bind DN – **cn=replicamanager,o=jke**
    Bind password – **P@ssw0rd**
    Confirm password – **P@ssw0rd**
    Description – leave blank

11. Click the **Finish** button to save the changes

12. On next screen click the **Close** to complete this step.

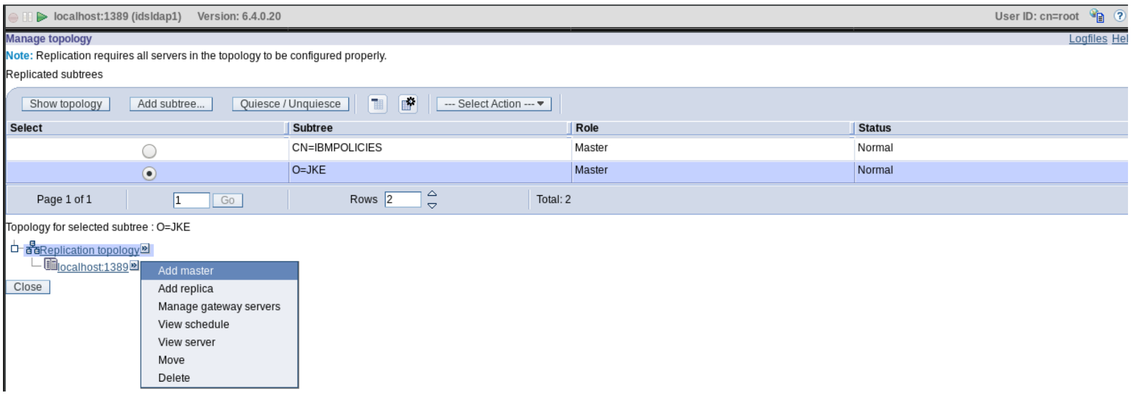
Define Replica Server

13. Now that the credentials are configured for the **O=JKE** subtree, it is time to configure the **replication topology**. This section defines the server that will be the replica of the Master server – i.e, localhost:2389 server.

14. Under **Replication management** select **Manage topology**.

15. With the **O=JKE** subtree **selected**, click the **Show topology** button.

16. From the “Topology for the selected subtree” section, click on **localhost:1389**



localhost:1389 (idsldap1) Version: 6.4.0.20 User ID: cn=root

Manage topology

Note: Replication requires all servers in the topology to be configured properly.

Replicated subtrees

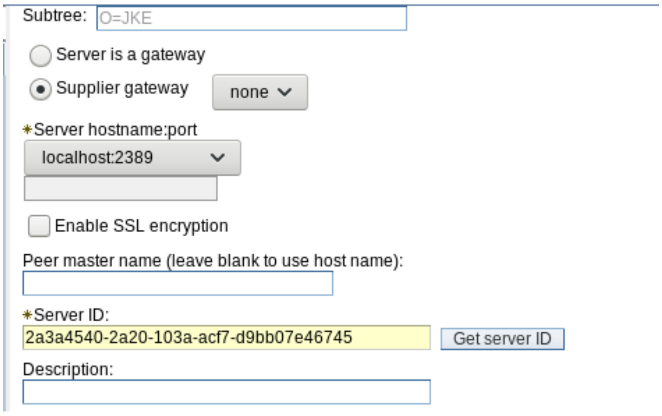
Select	Subtree	Role	Status
○	CN=IBMPOLICIES	Master	Normal
●	O=JKE	Master	Normal

Page 1 of 1 Rows 2 Total: 2

Topology for selected subtree : O=JKE

17. Click the **Add master.**

18. On the Add master screen enter the following information:
Server Hostname:port – Select **localhost:2389** as below
Enable SSL – **leave unchecked**
Peer Master – **leave blank**
Server ID – **click the Get server ID button**
(This would fetch ID for server localhost:2389)
Description – **leave blank**



Subtree: O=JKE

○ Server is a gateway

● Supplier gateway none

*Server hostname:port localhost:2389

☐ Enable SSL encryption

Peer master name (leave blank to use host name):

*Server ID: 2a3a4540-2a20-103a-acf7-d9bb07e46745

Description:

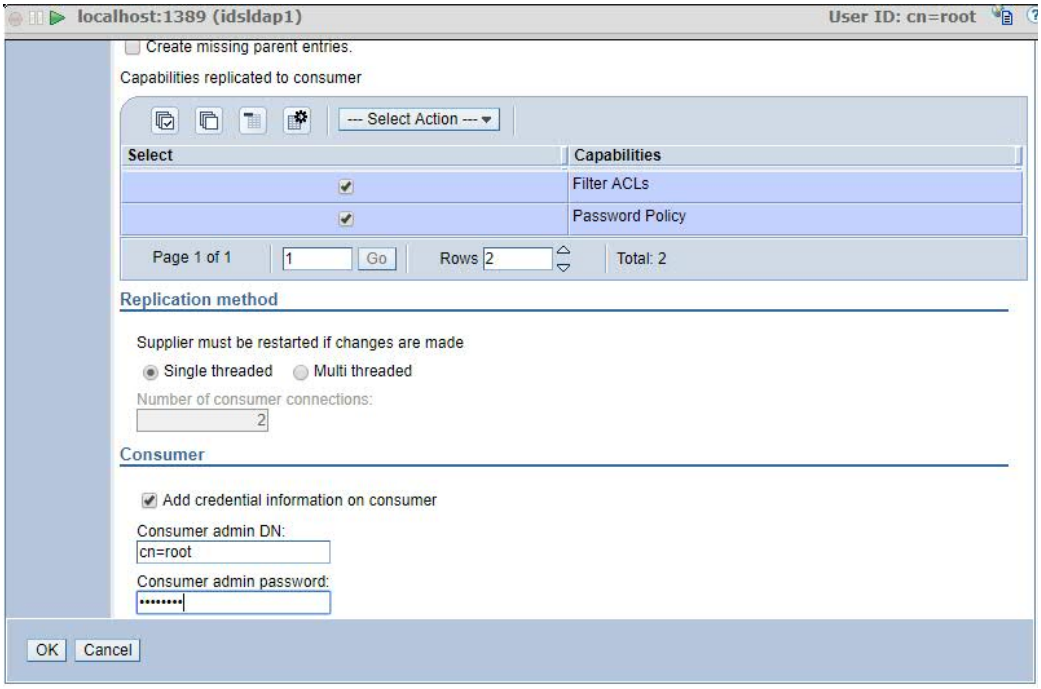
19. **Credential Object** – click the **Select** button, which will then open up a new window.

20. In the Select Credential screen, select the **radio button** next to the **O=JKE** entry. Click the **Show Credentials** button, to show the previously configured credential information. With the **replicamanager** credential displayed, click the **OK button.**

21. Click the **Additional** menu tab to continue to the next step.

22. The Add Replica – Additional screen allows the administrator to add further details about the replica - including the new feature of allowing for multi-threaded replication, to help with replication performance. **On this screen, the only change that will be made for this lab is to add the credentials to the consumer machine.**

23. Select the **checkbox** next to "Add credential information on consumer"
Consumer admin DN – **cn=root**
Consumer admin password – **P@ssw0rd**
The following screen capture shows the filled in values:



localhost:1389 (idsldap1) User ID: cn=root

□ Create missing parent entries.

Capabilities replicated to consumer

--- Select Action ---

Select	Capabilities
☑	Filter ACLs
☑	Password Policy

Page 1 of 1 [1] Go Rows [2] Total: 2

Replication method

Supplier must be restarted if changes are made

● Single threaded ○ Multi threaded

Number of consumer connections: 2

Consumer

☑ Add credential information on consumer

Consumer admin DN: cn=root

Consumer admin password: ••••••••

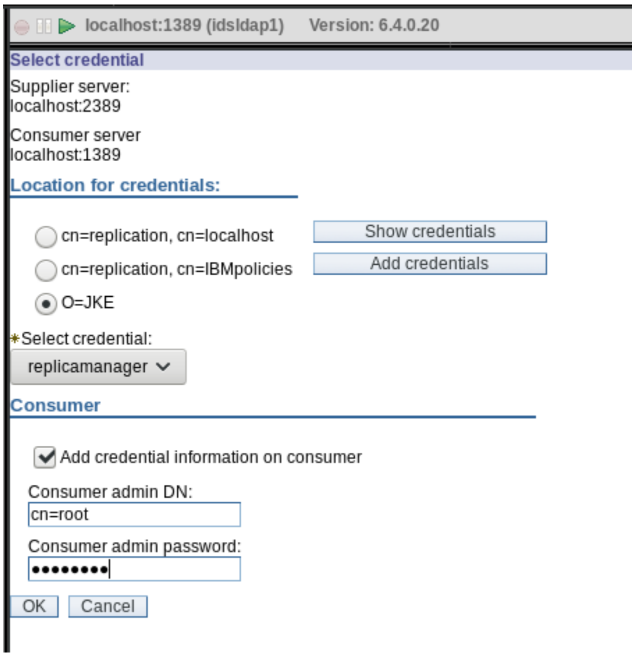
OK Cancel

24. Click the **OK** button to continue. Click **OK** again and you will get the **credential screen again.**

25. Select O=JKE **radio button** and press **Show Credentials**, in select credential section **replicamanger** will be shown.

26. Select the **checkbox** next to “Add credential information on consumer”
    Consumer admin DN – **cn=root**
    Consumer admin password – **P@ssw0rd**

27. Following image shows the operation :



localhost:1389 (idsldap1) Version: 6.4.0.20

Select credential

Supplier server:
localhost:2389

Consumer server
localhost:1389

Location for credentials:

○ cn=replication, cn=localhost
○ cn=replication, cn=IBMpolicies
● O=JKE

Show credentials
Add credentials

*Select credential:
replicamanager

Consumer

☑ Add credential information on consumer

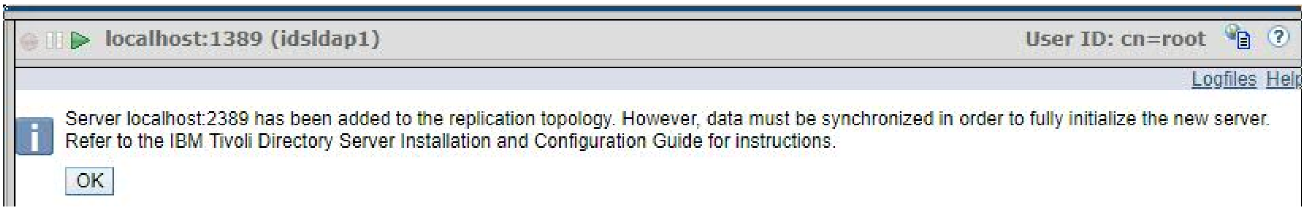
Consumer admin DN: cn=root

Consumer admin password: ••••••••

OK Cancel

28. Click **OK**

29. You will get the following message



Server localhost:2389 has been added to the replication topology. However, data must be synchronized in order to fully initialize the new server. Refer to the IBM Tivoli Directory Server Installation and Configuration Guide for instructions.

OK

30. Click **OK**

Note : As we have similar data on both the servers we **do not need to synchronize the data again**. If data is different we need to export ldif from primary server and import it to secondary.

31. In Replication Management go to **Manage Queues** .The queue is in **supended** state, select the **Radio button** and Click **Suspend/Resume.**

32. Click **Refresh**. The queue will be in **Ready** state.

33. The replication is now started from **IDSLDAP1** to **IDSLDAP2**

34. Click **Logout** from left pane.

Start the queue on IDSLDAP2

Note : As we have already **pushed credentials** to the IDSLDAP2 the topology is created in the IDSLDAP2 server. We just need to **start the queue** which is in Suspended state by default.

35. Login to **idsldap2** in WAT using the user **cn=root/P@ssw0rd**

36. In Replication Management go to **Manage Queues**.

37. The queue is in supended state, select the **Radio button** and Click **Suspend/Resume.**

38. Click **Refresh**. The queue will be in **Ready state.**

39. Replication from IDSLDAP2 to IDSLDAP1 is **started**.

40. **Logout** from WAT.

Verifying Replication

41. In this we will check if replication works fine for modifications. n the SDS Web Administration Tool, Login to **idsldap1** server and Click **Directory management** in left pane.

42. Select **Manage entries**. Select the **radio button** next to the **o=jke** branch. Click the **Expand** button.

43. Select user **cn=joe** from the list, and click the **Edit attributes** button

44. Modify the sn attribute to some new value , say “walter” to “**Hayden**”.Click **Next** and then **Finish.**

45. **Logout** from leftpane.

46. Login using **idsldap2**. Verify from the top bar its **localhost:2389**

47. Select **Manage entries**. Select the radio button next to the **o=jke** branch. Click the **Expand** button.

48. Select user **cn=joe** from the list, and click the **Edit attributes** button

49. Now you can see sn as **Hayden** which we changed on **IDSLDAP1**. The changes got replicated.

50. Press **Cancel** and **Logout** from leftpane.

Note : You can also verify by opening the **LDAP Browser tool** and login to IDSLDAP2 connection that we created previously. Also try to create the replication between the subtree **CN=IBMPOLICIES** as similar method as above. Check if changes get replicated.