

EXPERIMENT NO 1

Exercise 1.1 : Instance Creation in IBM Security Directory Server (SDS)

1. Aim: To create a new instance in IBM Security Directory Server (SDS) 6.4.0.20, enabling secure directory management and understanding the setup process.

2. Objective:

1. To learn how to set up and configure a new directory instance in SDS.
2. To understand the tools and commands used for instance creation.
3. To validate the successful creation and operation of the instance.

3. Tools and Requirements

1. Software Required:

- IBM Security Directory Server 6.4.0.20.
- IBM Directory Server Administration Tool.

2. System Requirements:

- Operating system: Linux/Windows.
- VM ware Workstation Player 17 pro.

4.Theory:

1. What is Instance Creation?

Instance creation refers to the process of setting up and configuring multiple independent directory server environments within the IBM Security Directory Server (SDS) on a single machine. Each instance operates as a separate server with its own configuration, port assignments, and data storage.

2. What is SDS Version 6.4.0.20

IBM SDS 6.4.0.20 supports running multiple directory server instances on a single machine. It is secure, scalable, and used for centralized authentication and directory-based management.

3. What is idslsap1?

The idslsap1 is the name assigned to the primary directory server instance in this lab. It is configured to run on port 1389 and is the main instance used for LDAP queries and authentication in this setup.

4. What is idslsap2?

The idslsap2 is the name assigned to the secondary directory server instance. It operates on port 2389 and provides an additional directory.

Steps :

Step1: Command Explanation: `/opt/ibm/ldap/V6.4/sbin/idsilist -a`

-This command is used in IBM Security Directory Server (SDS) to list all the directory server instances configured on the machine, along with their detailed information.

-a (All flag): When used, this flag displays detailed information about each instance, such as:

- Instance name
- Configuration path
- Ports in use (LDAP, admin, etc.)
- Current status (running/stopped).

Output:

```
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
```

Step2: Open Terminal from Desktop and navigate to the SDS folder as below:

```
cd /opt/ibm/ldap/V6.4/sb
```

Output :

```
File Edit View Search Terminal Help
root@isim ~]# cd /opt/ibm/ldap/V6.4/sbin/
root@isim sbin]#
```

Step 3 : This command is used to create two new users, idslldap1 and idslldap2, as owners of two separate SDS instances :

```
./idsadduser -u idslldap1 -w P@ssw0rd -l /home/idsldap1 -g idslldap -
```

- -u idslldap1: Specifies the username to be created (e.g., idslldap1).
- -w P@ssw0rd: Sets the password for the user (P@ssw0rd).
- -l /home/idsldap1: Specifies the home directory for the user (/home/idsldap1).
- -g idslldap: Assigns the user to the group idslldap.
- -n: Prevents interactive prompts during execution, making it a non-interactive command.

Output :

```
root@isim:/opt/ibm/ldap/V6.4/sbin
File Edit View Search Terminal Help
[root@isim ~]# cd /opt/ibm/ldap/V6.4/sbin/
[root@isim sbin]# ./idsadduser -u idsldap1 -w P@ssw0rd -l /home/idsldap1 -g ids
dap -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'.
```

Step4 : Similarly, add the second user idsldap2. This command is used to create new users, idsldap2, as owners of two separate SDS instances :

```
./idsadduser -u idsldap2 -w P@ssw0rd -l /home/idsldap2 -g idsldap -n
```

- -u idsldap2: Specifies the username to be created (e.g., idsldap1).
- -w P@ssw0rd: Sets the password for the user (P@ssw0rd).
- -l /home/idsldap1: Specifies the home directory for the user (/home/idsldap1).

Output:

```
[root@isim sbin]# ./idsadduser -u idsldap2 -w P@ssw0rd -l /home/idsldap2 -g ids
dap -n
GLPWRP123I The program '/opt/ibm/ldap/V6.4/sbin/64/idsadduser' is used with the
following arguments '-u idsldap2 -w ***** -l /home/idsldap2 -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 'idsldap2' will be created.
GLPGRP021I The user's primary group 'idsldap' will be created.
GLPGRP022I The home directory for user 'idsldap2' will be '/home/idsldap2'.
GLPGRP024I The user 'idsldap2' will be a member of group 'idsldap'.
GLPGRP025I The user 'root' will be a member of group 'idsldap'.
GLPGRP005I The password for user 'idsldap2' will be set.
GLPGRP034I The group 'idsldap' already exists.
GLPGRP029I The user 'idsldap2' was created successfully.
GLPGRP030I The user 'idsldap2' was added to group 'idsldap' successfully.
GLPGRP047I The user 'root' is already a member of group 'idsldap'.
GLPGRP006I Setting the password for user 'idsldap2'
GLPGRP007I Successfully changed password for user 'idsldap2'.
[root@isim sbin]# █
```

Step5 : Create the instance for the idsldap1 user using idsicrt command as below :

```
./idsicrt -I idsldap1 -e encryptionseed -l /home/idsldap1 -n
```

Here in the command :

- -I: Specifies the name of the instance to be created.
- -e: Provides the encryption seed for the SDS instance.
- -l: Defines the location where the instance will be stored.
- -n: Ensures the command runs without any prompts in the console.
- -idsicrt : The idsicrt command is used to add a DB2 instance for the SDS in the backend and create the instance.

Output:

```
root@isim:/opt/ibm/ldap/V6.4/sbin
File Edit View Search Terminal Help
[root@isim ~]# cd /opt/ibm/ldap/V6.4/sbin/
[root@isim/sbin]# ./idsicrt -I idsldap1 -e encryptionseed -l /home/idsldap1 -n
GLPICR076E The directory server instance 'idsldap1' already exists.
GLPICR024W The program did not complete successfully. View earlier error messages for information about the exact error.
[root@isim/sbin]# ./idsicrt -I idsldap2 -e encryptionseed -l /home/idsldap2 -n
GLPWRP123I The program '/opt/ibm/ldap/V6.4/sbin/64/idsicrt' is used with the following arguments 'idsicrt -I idsldap2 -e ***** -l /home/idsldap2 -n'.
You have chosen to perform the following actions:

GLPICR020I A new directory server instance 'idsldap2' will be created.
GLPICR057I The directory server instance will be created at: '/home/idsldap2'.
GLPICR013I The directory server instance's port will be set to '2389'.
GLPICR014I The directory server instance's secure port will be set to '2636'.
GLPICR015I The directory instance's administration server port will be set to '3542'.
GLPICR016I The directory instance's administration server secure port will be set to '3543'.
GLPICR019I The description will be set to: 'IBM Security Directory Server Instance V6.4'.
GLPICR021I Database instance 'idsldap2' will be configured.
GLPICR028I Creating directory server instance: 'idsldap2'.
GLPICR025I Registering directory server instance: 'idsldap2'.
GLPICR026I Registered directory server instance: : 'idsldap2'.
GLPICR049I Creating directories for directory server instance: 'idsldap2'.
GLPICR050I Created directories for directory server instance: 'idsldap2'.
GLPICR043I Creating key stash files for directory server instance: 'idsldap2'.
GLPICR044I Created key stash files for directory server instance: 'idsldap2'.
GLPICR040I Creating configuration file for directory server instance: 'idsldap2'.
GLPICR041I Created configuration file for directory server instance: 'idsldap2'.
GLPICR034I Creating schema files for directory server instance: 'idsldap2'.
GLPICR035I Created schema files for directory server instance: 'idsldap2'.
GLPICR037I Creating log files for directory server instance: 'idsldap2'.
GLPICR038I Created log files for directory server instance: 'idsldap2'.
GLPICR088I Configuring log files for directory server instance: 'idsldap2'.
```

Step6 : Similarly, create the instance for the idsldap2 user using idsicrt command as below : `./idsicrt -I idsldap2 -e encryptionseed -l /home/idsldap2 -n`

```
File Edit View Search Terminal Help
GLPCTL017I Cataloging database instance node: 'idsldap2'.
GLPCTL018I Cataloged database instance node: 'idsldap2'.
GLPCTL008I Starting database manager for database instance: 'idsldap2'.
GLPCTL009I Started database manager for database instance: 'idsldap2'.
GLPCTL049I Adding TCP/IP services to database instance: 'idsldap2'.
SGLPCTL050I Added TCP/IP services to database instance: 'idsldap2'.
GLPICR081I Configuring database instance 'idsldap2' for directory server instance: 'idsldap2'.
GLPICR082I Configured database instance 'idsldap2' for directory server instance: 'idsldap2'.
GLPICR052I Creating DB2 instance link for directory server instance: 'idsldap2'.
GLPICR053I Created DB2 instance link for directory server instance: 'idsldap2'.
GLPICR032I Added database instance 'idsldap2' to directory server instance: 'idsldap2'.
[root@isim/sbin]#
```

Step7: So, to check the details of the new instances idsldap1 and idsldap2, you can use the following command in the terminal:

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

- The -a flag stands for "all."
- It provides detailed information about each instance, such as:
- Instance name
- Port numbers
- Configuration paths
- Status (running/stopped)

Note : We can see that ports 1389 and 2389 are by default assigned to idsldap1 and idsldap2, respectively. This is the standard behavior of SDS. You can also specify a custom port using the -p argument with the idsicrt command if needed.

Output:

```
[root@isim sbin]# /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: idslldap2

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

Step8: Once the instances are created, we will configure the DB2 database for the SDS instance. The DB2 database serves as the backend to store all LDAP entries securely.

```
./idscfgdb -l idslldap1 -w P@ssw0rd -a idslldap1 -t idslldap1 -l /home/idsldap1 -n
```

Note: Here in the command

- -l is the instance name.
- -w is the password for the instance owner.
- -a is the database admin user.
- -t is the database name.
- -n prevents any prompts during execution.

Output :

```

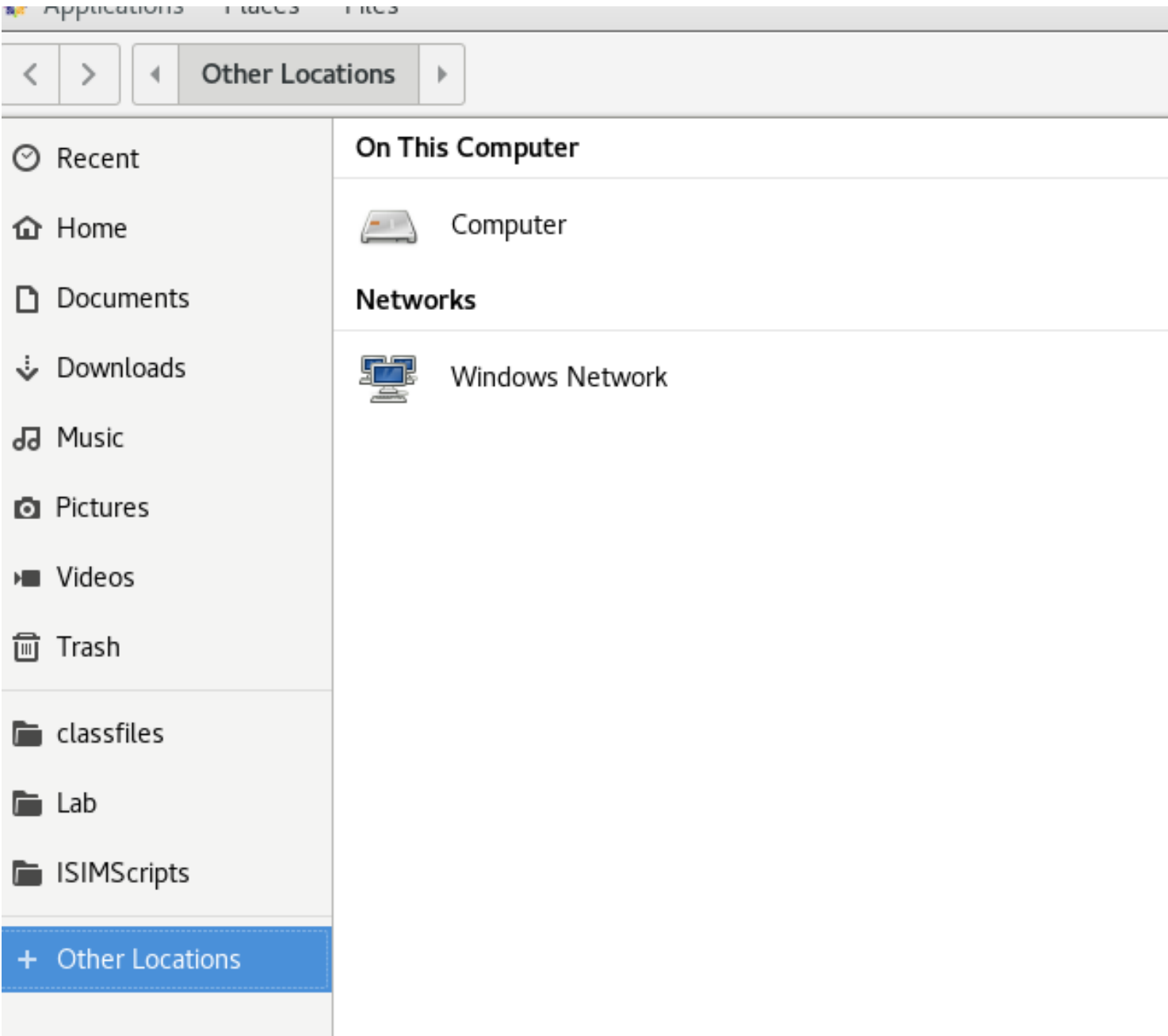
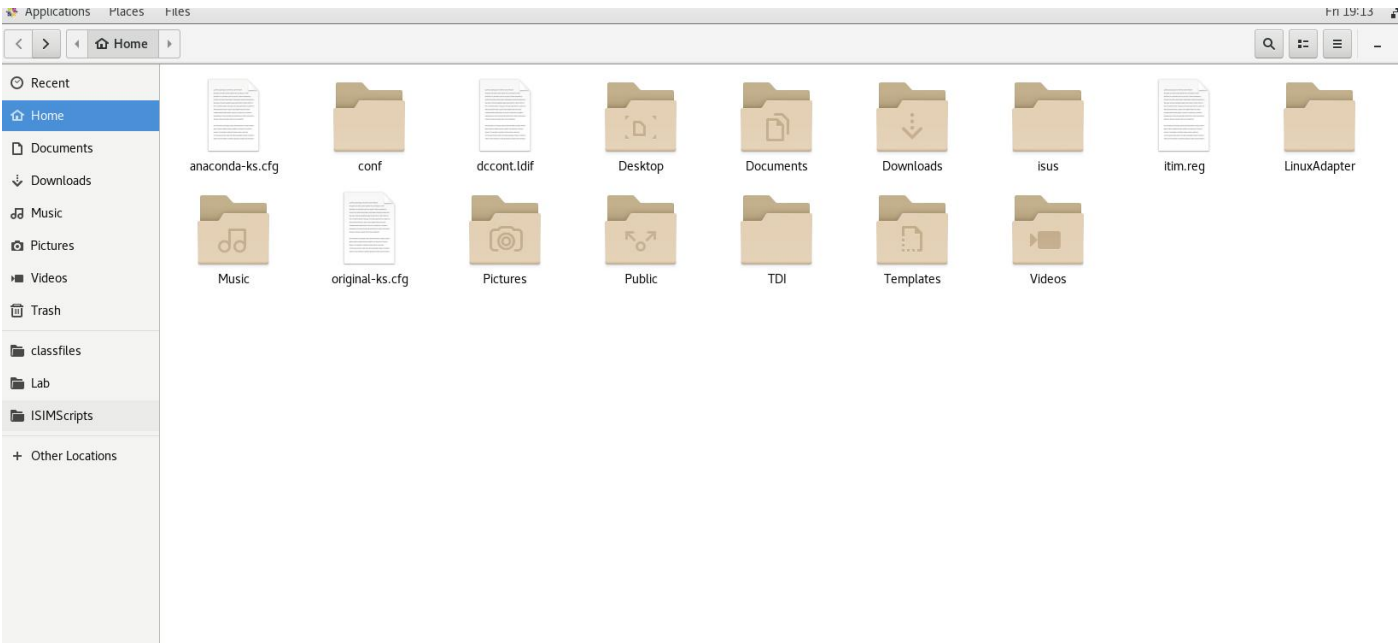
-k backup_dir      Backup location for the database.
                    If this argument is passed, online backup for the database will be configured.
-l db_location     DB2 database location.  For AIX, Linux, Solaris, and HP-UX systems,
                    this is a directory name (i.e., /home/ldapdb2).
                    For Windows systems, this must be a drive letter.
                    There must be at least 80 Megabytes free.  Additional
                    disk space should be available to accommodate growth
                    as directory entries are added.
-n                Run in no-prompt mode. All output is generated except for
                    messages requiring user interaction. The -w option must
                    be used with this option.
-q                Run in quiet mode. All output except errors is suppressed.
                    If the -d option is also specified, trace output
                    is not suppressed.
-s storage_loc     TABLESPACE container location.
-t db_name         DB2 database name.
-v                Prints the version information about the command.
-w db_admin_pw     DB2 administrator password.
-x                Create the DB2 database in a local codepage.
-z ext_size        Tablespace extension size in pages.
                    The default value for extension size is 8192 pages.
-?                Displays the usage.
```

Step9 : Similarly, to configure the database for the second instance idslldap2, use the following command:

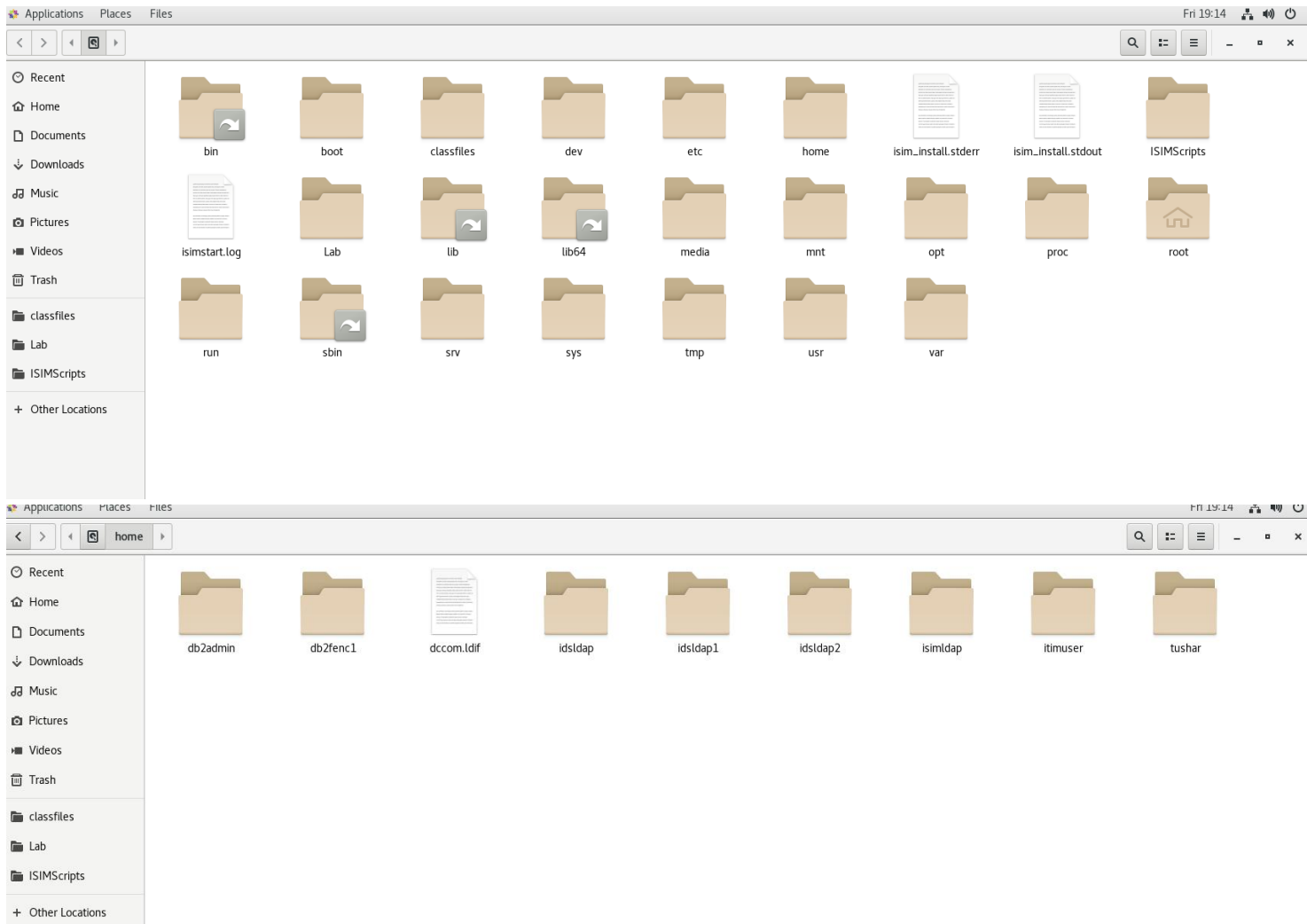
```
./idscfgdb -l idslldap2 -w P@ssw0rd -a idslldap2 -t idslldap2 -l /home/idsldap2 -n
```

The database idslldap2 is created in the idslldap2 DB2 instance. After that, all the default SDS tables are added to this database.

Output:



Step10 : Minimize the Terminal window, then double-click the Home icon on the Desktop. In the left pane, click Other Locations, then double-click Computer and Home. You'll see two folders: idslsap1 and idslsap2, which are the home directories for the SDS instance owners.



Step11 : Double-click idslsap1 directory and you can see idsslapd-idslsap1 folder which have all instance related configurations and log files.

```
[root@isim sbin]# ./idsnpw -I idslsap1 -u cn=root -p P@ssw0rd -n
GLPWRP123I The program '/opt/ibm/ldap/V6.4/sbin/64/idsnpw' is used with the
following arguments '-I idslsap1 -u cn=root -p ***** -n'.
You have chosen to perform the following actions:
```

```
GLPDPW004I The directory server administrator DN will be set.
GLPDPW005I The directory server administrator password will be set.
GLPDPW009I Setting the directory server administrator DN.
GLPDPW010I Directory server administrator DN was set.
GLPDPW006I Setting the directory server administrator password.
GLPDPW007I Directory server administrator password was set.
[root@isim sbin]#
```

Step12:Create admin user (cn=root) who can be used to do the administrative task on the ldap instances

```
./idsnpw -I idslsap1 -u cn=root -p P@ssw0rd -n
```

Note : Here in the command

- -l is instance name
- -u user name of the instance admin
- -p for password of admin use
- -n for no prompt.

Output :

```
[root@isim sbin]# ./idsdnpw -I idslldap2 -u cn=root -p P@ssw0rd -n
GLPWRP123I The program '/opt/ibm/ldap/V6.4/sbin/64/idsdnpw' is used with the
following arguments '-I idslldap2 -u cn=root -p ***** -n'.
You have chosen to perform the following actions:

GLPDPW004I The directory server administrator DN will be set.
GLPDPW005I The directory server administrator password will be set.
GLPDPW009I Setting the directory server administrator DN.
GLPDPW010I Directory server administrator DN was set.
GLPDPW006I Setting the directory server administrator password.
GLPDPW007I Directory server administrator password was set.
[root@isim sbin]# █
```

Step 13: Similarly, for the idslldap2 instance, create the admin user cn=root using the following command:

```
/idsdnpw -l idslldap2 -u cn=root -p P@ssw0rd -n
```

```
[root@isim sbin]# ./idsdnpw -I idslldap2 -u cn=root -p P@ssw0rd -n
GLPWRP123I The program '/opt/ibm/ldap/V6.4/sbin/64/idsdnpw' is used with the
following arguments '-I idslldap2 -u cn=root -p ***** -n'.
You have chosen to perform the following actions:

GLPDPW004I The directory server administrator DN will be set.
GLPDPW005I The directory server administrator password will be set.
GLPDPW009I Setting the directory server administrator DN.
GLPDPW010I Directory server administrator DN was set.
GLPDPW006I Setting the directory server administrator password.
GLPDPW007I Directory server administrator password was set.
[root@isim sbin]# █
```

The user is successfully created. This admin user will be used to connect to the LDAP and perform administrative tasks.

Step 14 Close terminal .

Learning outcomes :

- -We gained an understanding of how to create and configure directory server instances in IBM Security Directory Server (SDS).
- We learned how to use commands like idsadduser, idsicrt, idscfgdb, and idsdnpw to create instances, configure databases, and handle administrative tasks.
- -We successfully created and set up idslldap1 and idslldap2 instances with unique configurations such as ports, encryption seeds, and database settings.
- We also understood how to link and configure DB2 databases for SDS instances, allowing efficient management of LDAP entries.

