
# Đại học Khoa học Tự nhiên – ĐHQG TP.HCM

----------□□----------

**Môn học: An toàn và bảo mật dữ liệu trong hệ thống thông tin**

# ĐỒ ÁN MÔN HỌC

# HỆ QUẢN TRỊ CƠ SỞ DỮ LIỆU ORACLE

# HƯỚNG DẪN

**Lớp: 21HTTT**

**Giảng viên phụ trách:**

Cô Phạm Thị Bạch Huệ

Thầy Lương Vĩ Minh

Cô Tiết Gia Hồng

**Thông tin sinh viên:**

21127456 – Võ Cao Trí

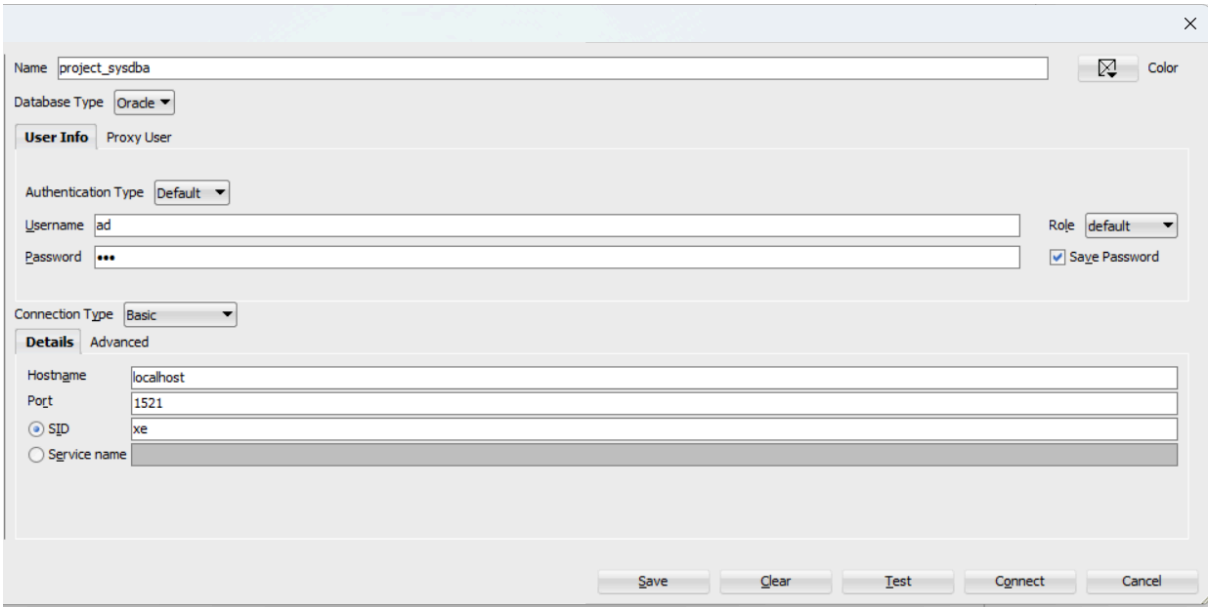
21127608 – Trần Trung Hiếu

21127668 – Đinh Quang Phong

# MỤC LỤC

# I. Hướng dẫn build và run chương trình - Phân hệ 1:

- Mở Sqldeveloper:
  - Chạy file **sys.sql** với user name là sys và quyền là SYSDBA để tạo user có quyền quản trị trong Oracle DB Server có tên là ad
  - Chạy file **table_creation.sql** với username **ad** và mật khẩu **123** vừa tạo với quyền SYSDBA để tạo cơ sở dữ liệu và chạy file **DataGen.sql** để chèn dữ liệu.
- Mở source code bằng Visual Studio thông qua file solution **ATBM-A-14.sln**
- Thay đổi config trong file **Program.cs** phù hợp với Oracle DB Server:
  Trong Sqldeveloper mục connection, chọn connection của account mà mình cần.
  Click chuột phải chọn properties




  - HOST: Trong mục Hostname
  - SERVICE: có thể chọn SID hoặc Service name đều được
  - PORT: Trong mục Port
  - SCHEMA: Là username của sysdba được tạo

```
// config here
public static string HOST = "localhost";
public static string SERVICE = "PDB_ATBMHTTT"; // SID is also fine here
public static string PORT = "1521";
public static string SCHEMA = "ad";
```

- Bấm F5 trên Visual Studio để build và run

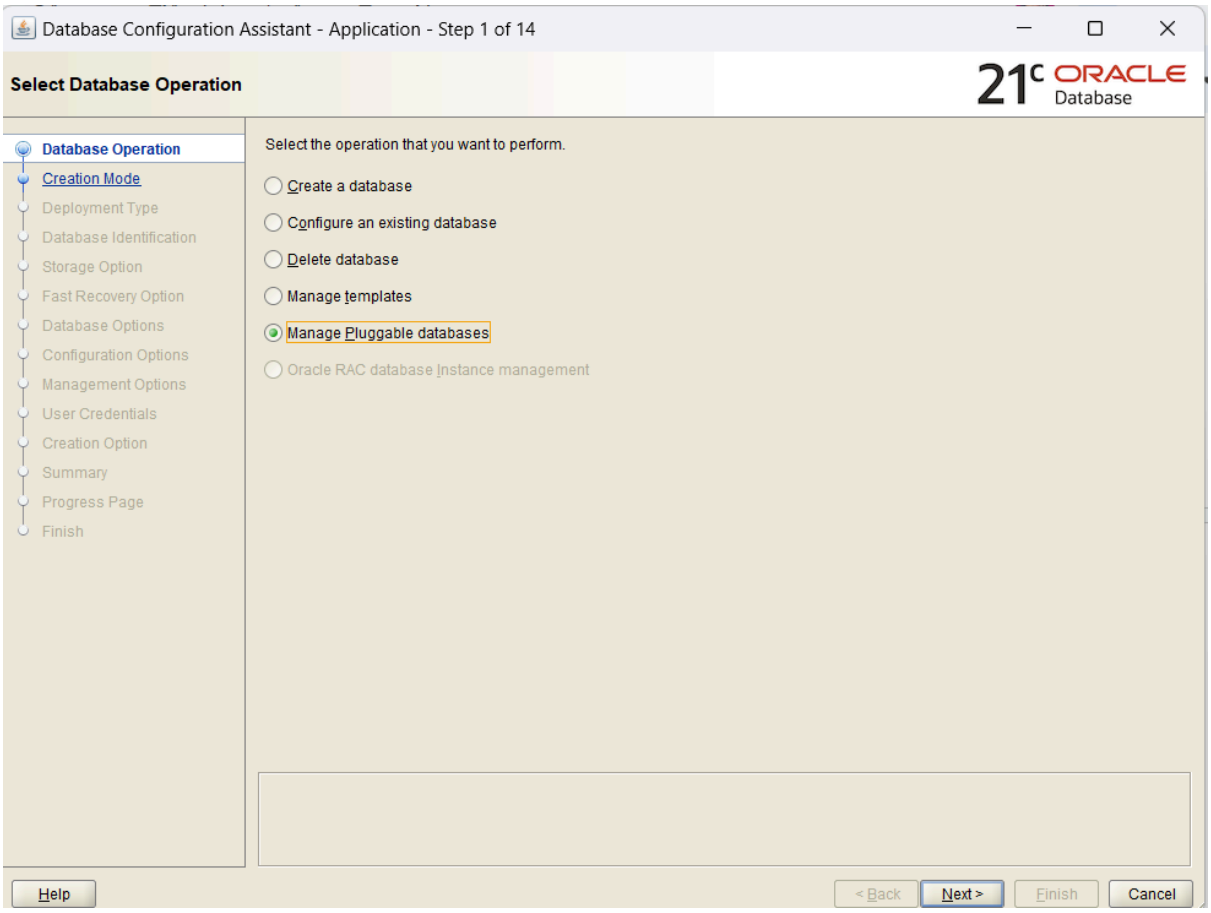
# II. Hướng dẫn build và run chương trình - Phân hệ 2:

CHÚ Ý: Để chạy được ứng dụng thì trước đó phải vào Oracle sql developer và thực hiện đoạn lệnh ở file **sys.sql** với quyền sys để thực hiện chạy PDB database server.

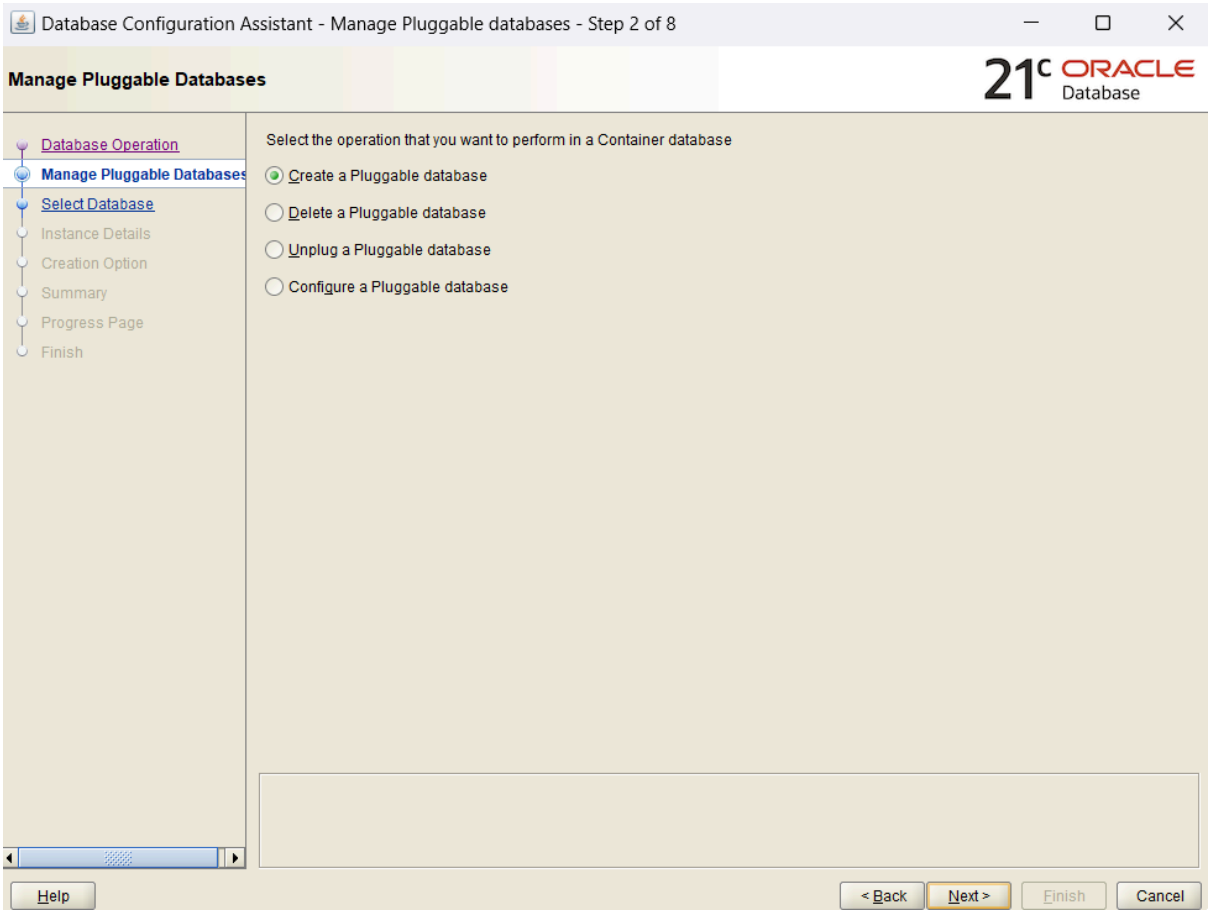
```
alter session set current_schema = sys;
ALTER SESSION SET "_ORACLE_SCRIPT" = TRUE;
alter session set container = PDB_ATBMHTTT;
alter pluggable database PDB_ATBMHTTT open READ WRITE;
```

1. Yêu cầu 1, Yêu cầu 3:

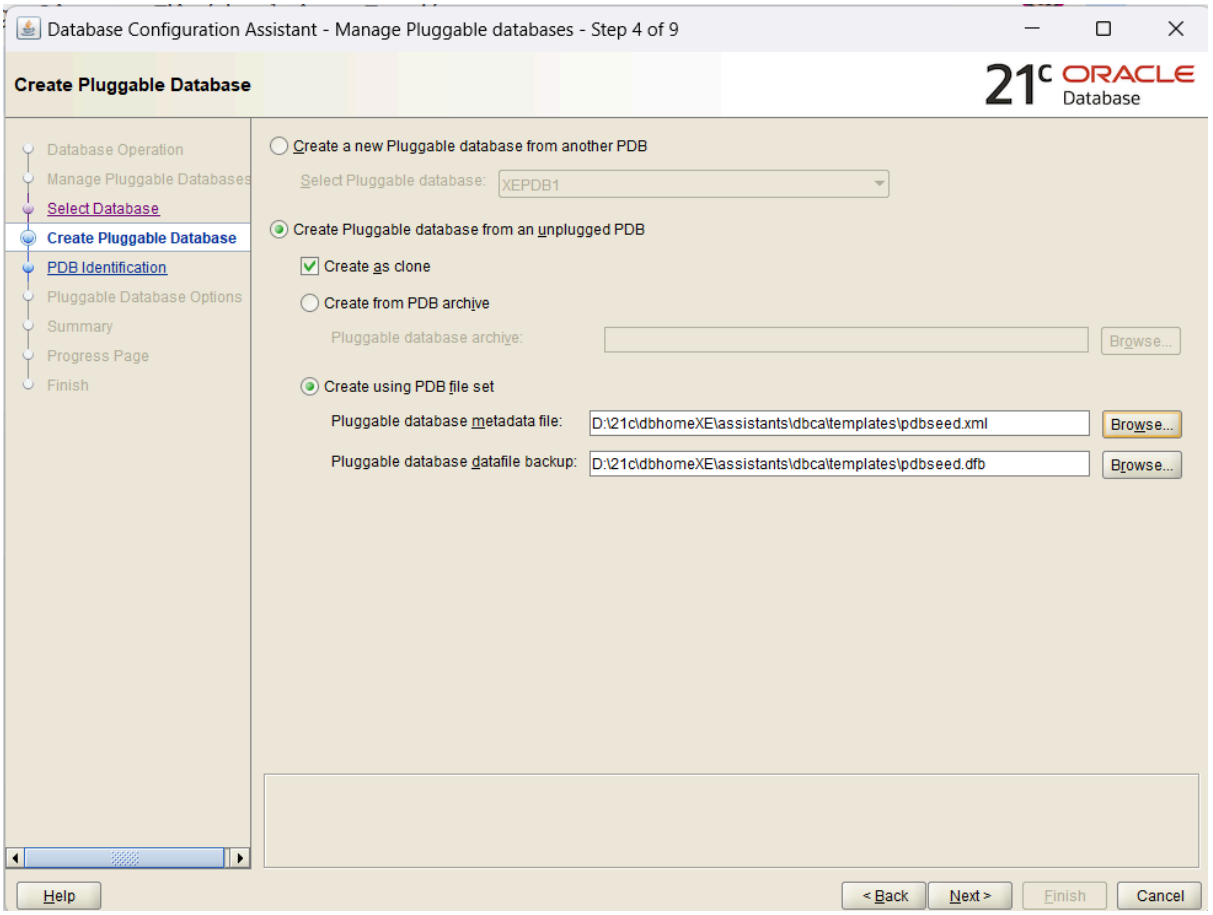
- Chạy DBCA trong cmd hoặc start menu



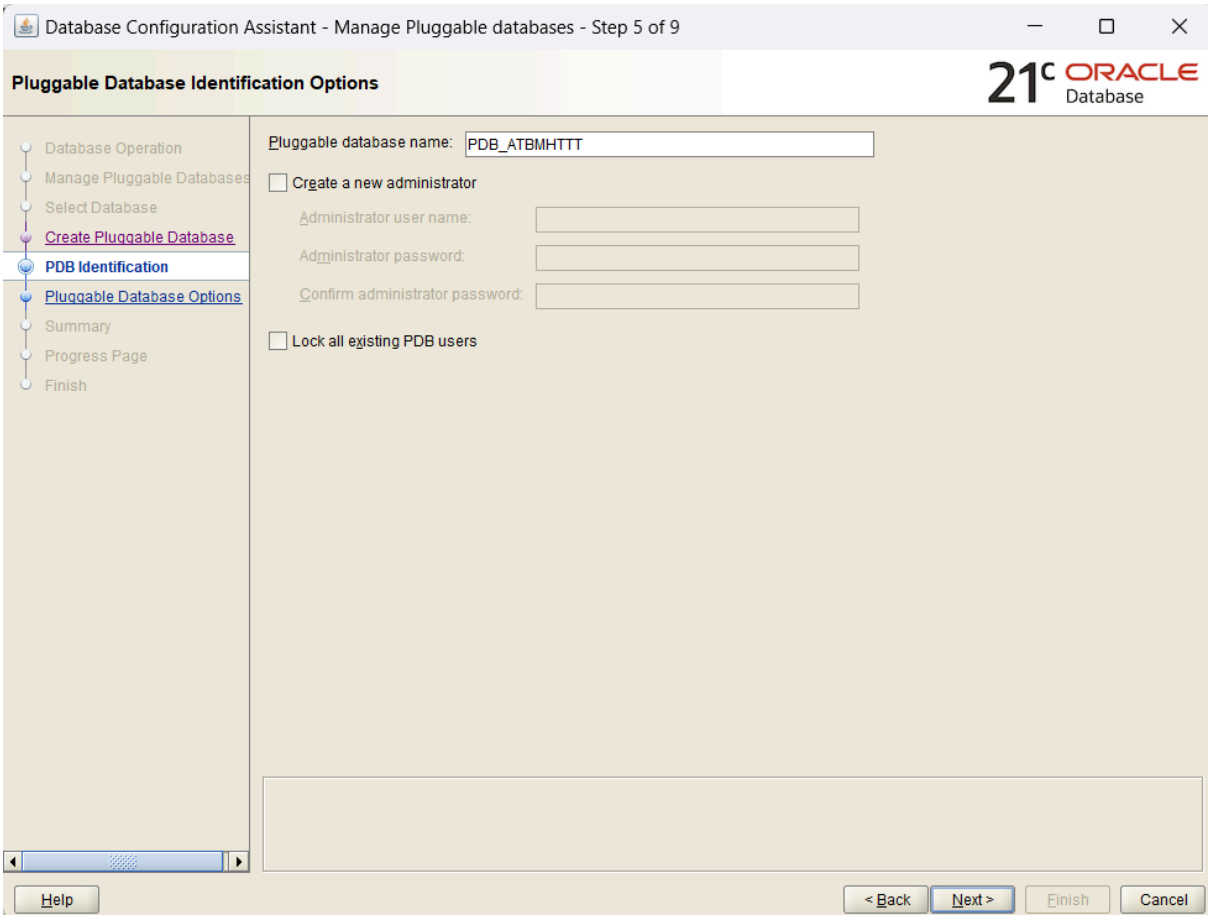

- Chọn tạo PDB



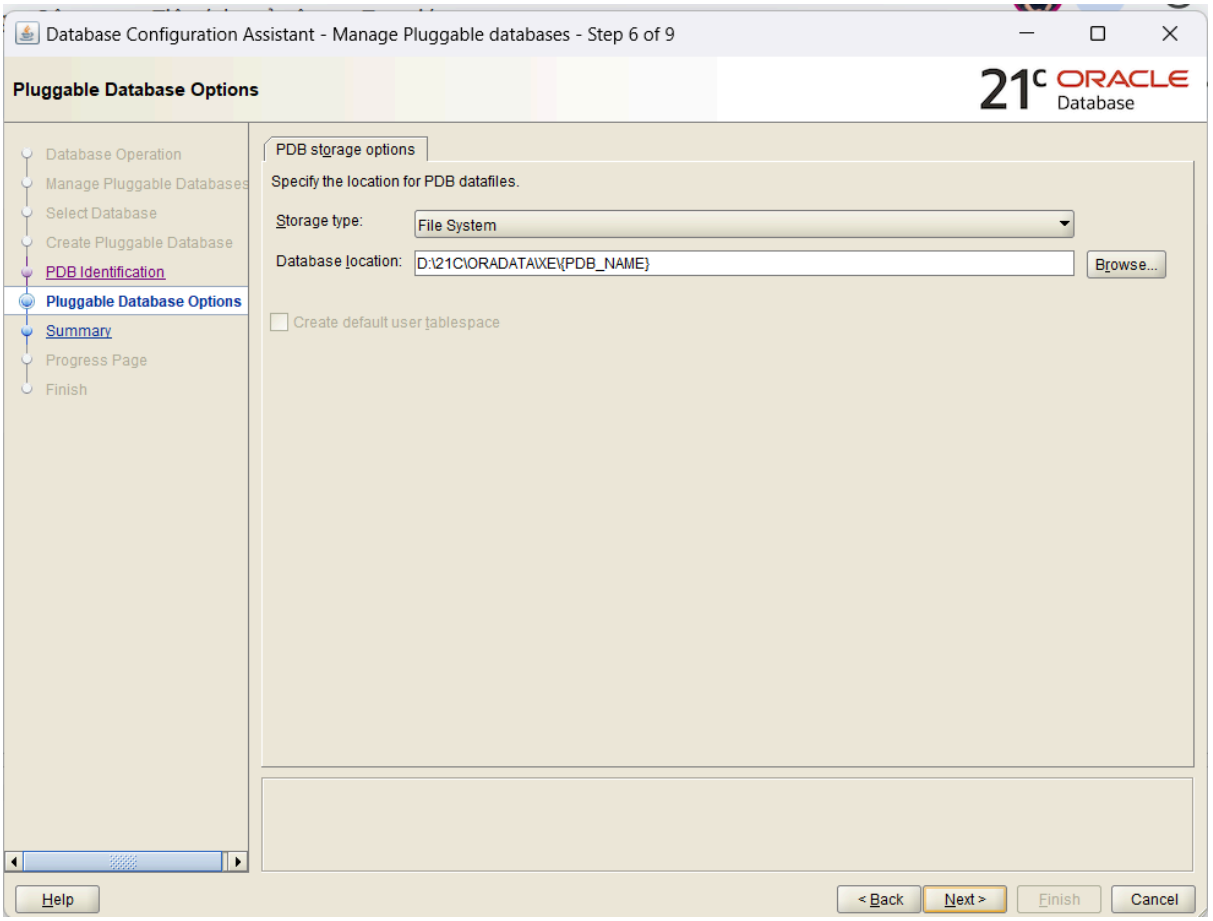

- Chọn CDB@ROOT muốn tạo PDB bên trong và cấu hình PDB



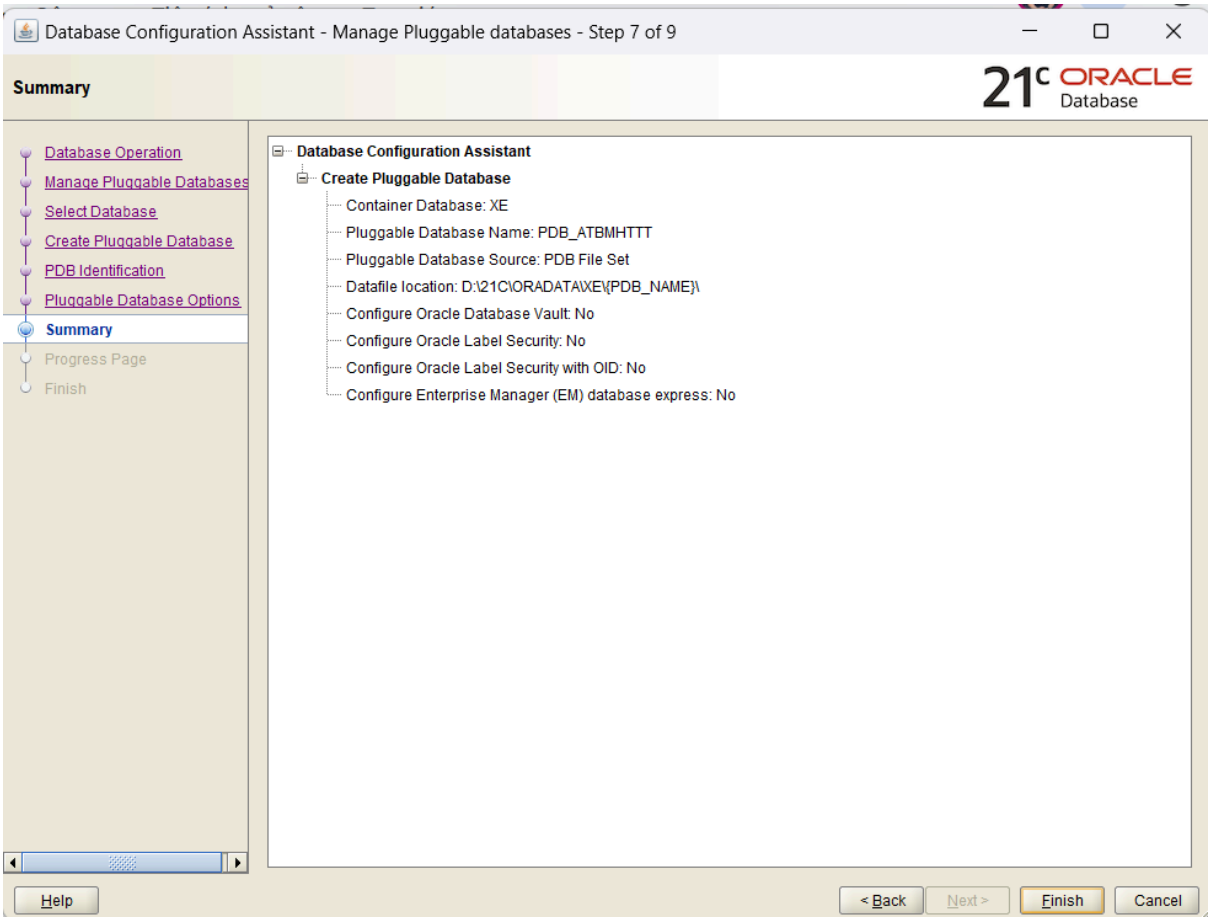

- Đặt tên cho PDB



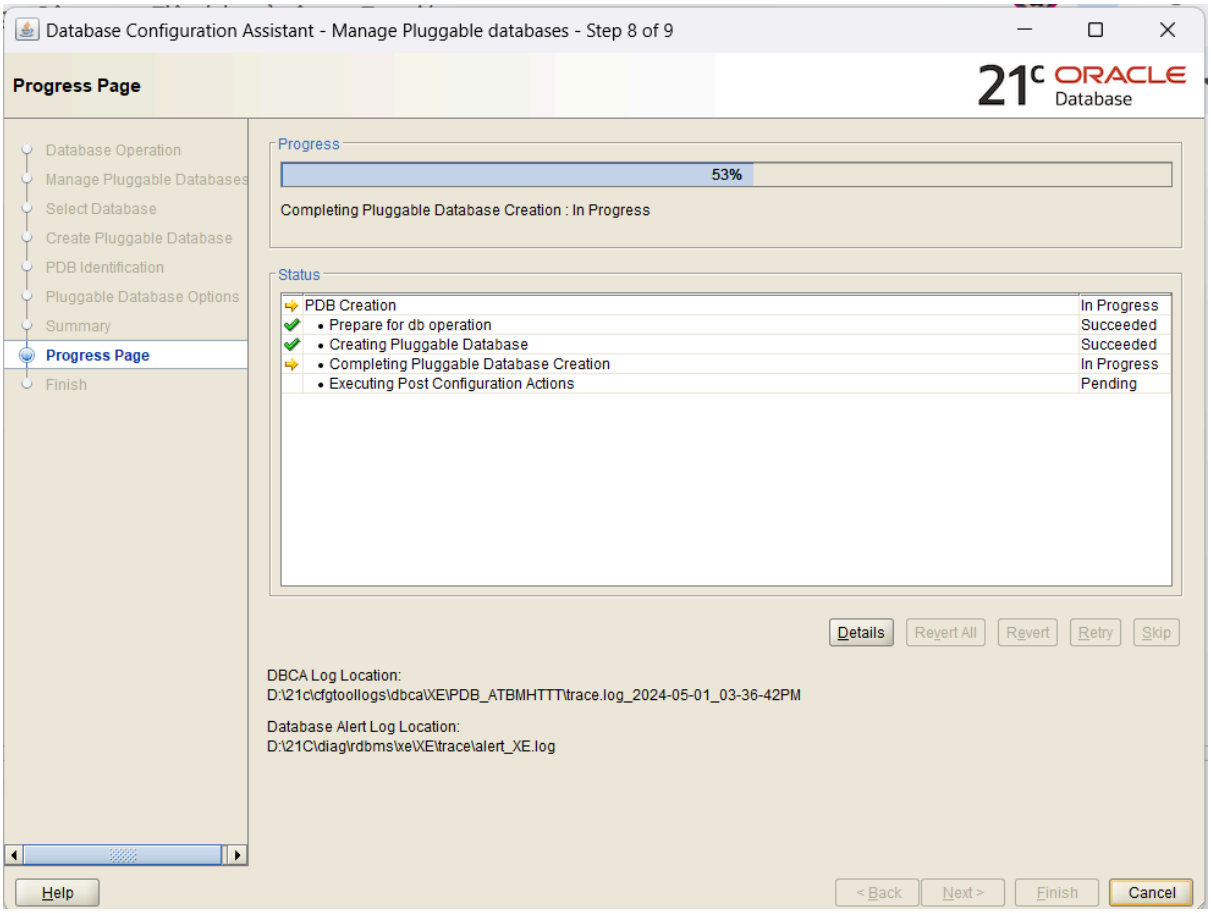

- Chọn nơi muốn lưu PDB

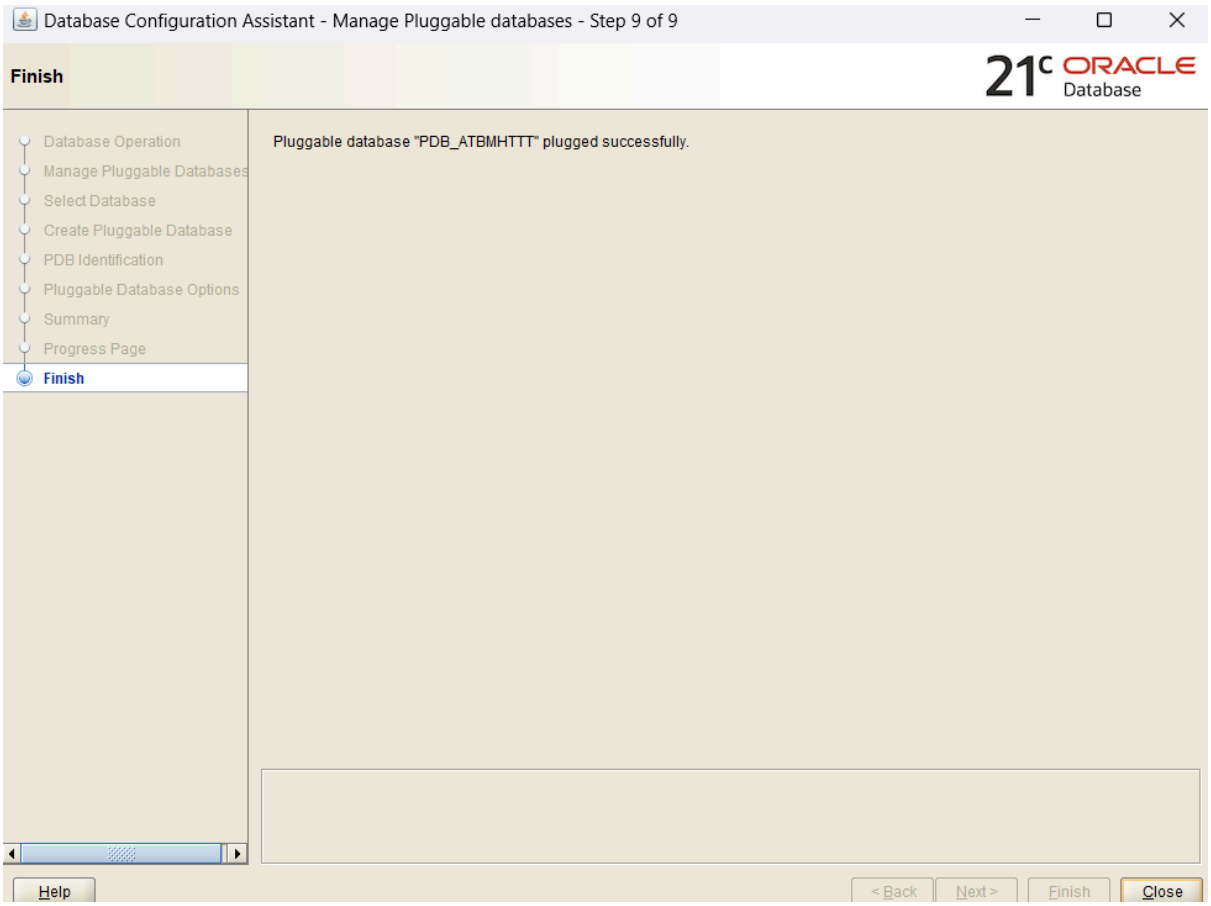



- Chọn Next để xem lại các cài đặt PDB trước khi tạo

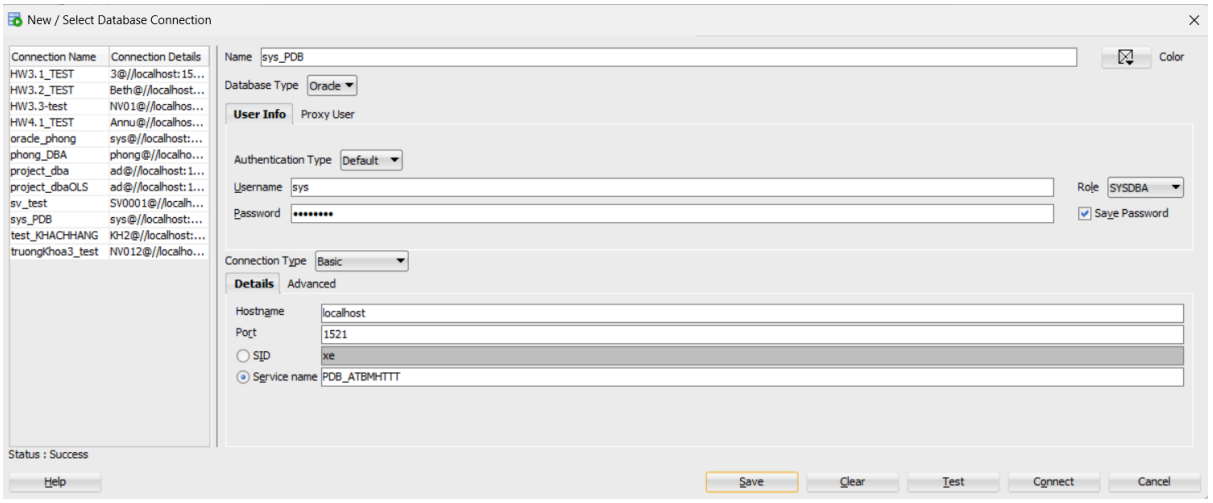

Database Configuration Assistant - Manage Pluggable databases - Step 7 of 9
Summary
21c ORACLE Database
Database Operation
Manage Pluggable Databases
Select Database
Create Pluggable Database
PDB Identification
Pluggable Database Options
Summary
Progress Page
Finish
Database Configuration Assistant
Create Pluggable Database
Container Database: XE
Pluggable Database Name: PDB_ATBMHTTT
Pluggable Database Source: PDB File Set
Datafile location: D:\21C\ORADATA\XE\{PDB_NAME}\
Configure Oracle Database Vault: No
Configure Oracle Label Security: No
Configure Oracle Label Security with OID: No
Configure Enterprise Manager (EM) database express: No
Help
< Back
Next >
Finish
Cancel

- Tạo PDB


Database Configuration Assistant - Manage Pluggable databases - Step 8 of 9
Progress Page
21c ORACLE Database
Database Operation
Manage Pluggable Databases
Select Database
Create Pluggable Database
PDB Identification
Pluggable Database Options
Summary
Progress Page
Finish
Progress
53%
Completing Pluggable Database Creation : In Progress
Status
PDB Creation In Progress
• Prepare for db operation Succeeded
• Creating Pluggable Database Succeeded
• Completing Pluggable Database Creation In Progress
• Executing Post Configuration Actions Pending
Details
Revert All
Revert
Retry
Skip
DBCA Log Location:
D:\21c\cfgtoollogs\dbca\XE\PDB_ATBMHTTT\trace.log_2024-05-01_03-36-42PM
Database Alert Log Location:
D:\21C\diag\rdbms\xe\XE\trace\alert_XE.log
Help
< Back
Next >
Finish
Cancel


Database Configuration Assistant - Manage Pluggable databases - Step 9 of 9
Finish
21c ORACLE Database
Database Operation
Manage Pluggable Databases
Select Database
Create Pluggable Database
PDB Identification
Pluggable Database Options
Summary
Progress Page
Finish
Pluggable database "PDB_ATBMHTTT" plugged successfully.
Help
< Back
Next >
Finish
Close

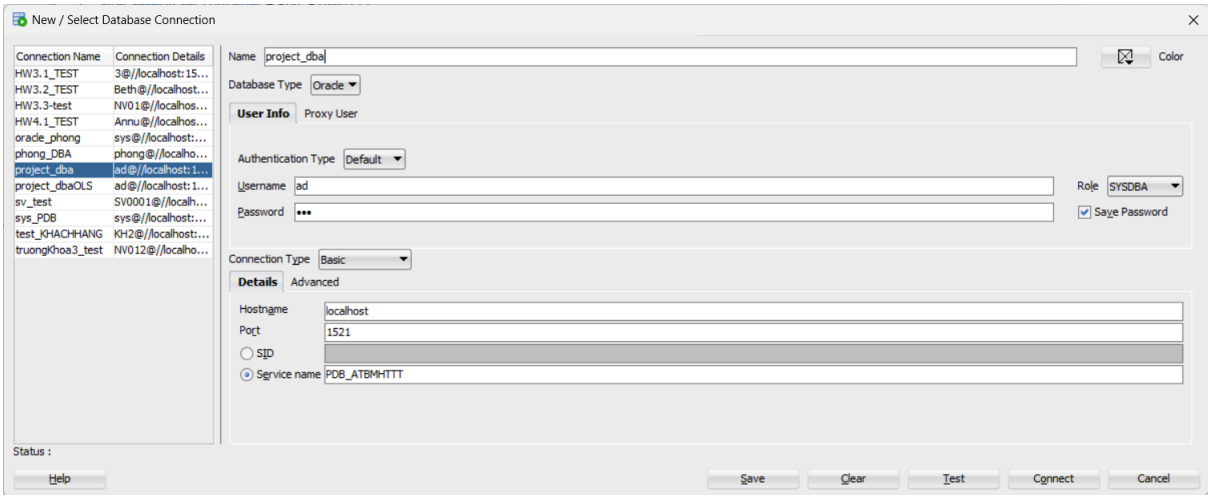
- Tạo connection sys và kết nối vào DB là PDB




- Chạy Script của file sys.sql từ đầu tới phần trước OLS để tạo user ad vào cấp quyền cho user ad

```
1  alter session set current_schema = sys;
2  ALTER SESSION SET "_ORACLE_SCRIPT" = TRUE;
3  alter session set container = PDB_ATBMHTTT;
4  alter pluggable database PDB_ATBMHTTT open READ WRITE;
5
6  --DROP USER ad cascade;
7
8  CREATE user ad IDENTIFIED by 123;
9  GRANT CREATE SESSION TO ad container = current;
10 --CONNECT ad/123;
11 show con_name;
12
13 Grant SYSDBA TO AD;
14 GRANT EXECUTE ANY PROCEDURE TO ad;
15 GRANT ALL PRIVILEGES TO ad;
16 grant execute on sys.DBMS_RLS to ad; -- to add policy
17 GRANT INHERIT PRIVILEGES ON USER sys TO ad; -- to create function
18 ----------------------------------------------------------------------------------
```

- Tạo connection cho AD




- Sử dụng Connection AD chạy các thao tác sau:
    - Chạy script tạo cấu trúc cơ sở dữ liệu bằng file **tabel_creation.sql**
    - Chạy script tạo dữ liệu bằng file **DataGen.sql**
    - Chạy script yêu cầu 1 của phân hệ 2 bằng file **Policy.sql** để tạo các chính sách, user và role (Thực hiện access control bằng RBAC và VPD)
    - Chạy script yêu cầu 2 của phân hệ 2 bằng file **Audit.sql** để thực hiện ghi audit của yêu cầu Fine-grained Audit và ghi audit khi người dùng select trên các bảng có trong cơ sở dữ liệu.

## 2. Hướng dẫn build và run chương trình: yêu cầu 2 - OLS

- Connect vào PDB bằng sys - và chạy file **sys.sql**
  ---> Kiểm tra OLS đã được bật chưa (Connect bằng Sys user)

```
SELECT VALUE FROM v$option WHERE parameter = 'Oracle Label Security';
SELECT status FROM dba ols status WHERE name = 'OLS CONFIGURE STATUS';
```

  Nếu chưa thực hiện

```
EXEC LBACSYS.CONFIGURE_OLS;
EXEC LBACSYS.OLS_ENFORCEMENT.ENABLE_OLS;
--SELECT name, open_mode FROM v$pdbs;
SHUTDOWN IMMEDIATE;
STARTUP;
```

- Kiểm tra PDB có chưa (Vì không thể tạo OLS trên CDB)

```
select * from v$services;
```

- Unlock LBACSYS (OLS Admin)

```
ALTER USER lbacsys IDENTIFIED BY lbacsys ACCOUNT UNLOCK container = all;
```

- Nếu có rồi thì mở PDB

```
ALTER SESSION SET CONTAINER= PDB_ATBMHTTT;
```

- Tạo Admin OLS & cấp quyền cho Ad

```
--CREATE USER ad IDENTIFIED BY 123 CONTAINER = CURRENT;
GRANT CONNECT,RESOURCE, SELECT_CATALOG_ROLE TO ad; --CẤP QUYỀN CON
GRANT UNLIMITED TABLESPACE TO ad; --CẤP QUOTA CHO ADMIN_OLS
GRANT SELECT ANY DICTIONARY TO ad; --CẤP QUYỀN ĐỌC DICTIONARY


---> CẤP QUYỀN EXECUTE CHO ADMIN_OLS
GRANT EXECUTE ON LBACSYS.SA_COMPONENTS TO ad WITH GRANT OPTION;
GRANT EXECUTE ON LBACSYS.SA_SYSDBA TO ad WITH GRANT OPTION;
GRANT EXECUTE ON LBACSYS.sa_user_admin TO ad WITH GRANT OPTION;
GRANT EXECUTE ON LBACSYS.sa_label_admin TO ad WITH GRANT OPTION;
GRANT EXECUTE ON sa_policy_admin TO ad WITH GRANT OPTION;
GRANT EXECUTE ON char_to_label TO ad WITH GRANT OPTION; ---> ADD A
GRANT LBAC_DBA TO ad;
GRANT EXECUTE ON sa_sysdba TO ad;
GRANT EXECUTE ON TO_LBAC_DATA_LABEL TO ad; -- CẤP QUYỀN THỰC THI
GRANT notification_policy_DBA to ad;

GRANT inherit privileges ON USER sys TO lbacsys;
GRANT lbac_dba to SYS;
```

- Tạo chính sách OLS (KHỞI ĐỘNG LẠI SQLDEV ĐỂ CẬP NHẬT OLS ENABLE) connect bằng ad với user: ad - mật khẩu: 123 và chạy bằng file **OLS.sql**

```
BEGIN
    SA_SYSDBA.CREATE_POLICY(
    policy_name => 'notification_policy',
    column_name => 'notification_label'
    );
END;
```

- Tạo Level Compartment Group

```
EXECUTE SA_COMPONENTS.CREATE_LEVEL('notification_policy',300,'TK', 'TRUONG KHOA');
EXECUTE SA_COMPONENTS.CREATE_LEVEL('notification_policy',250,'TDV','TRUONG DON VI');
EXECUTE SA_COMPONENTS.CREATE_LEVEL('notification_policy',200,'GVN','GIAO VIEN');
EXECUTE SA_COMPONENTS.CREATE_LEVEL('notification_policy',150,'GV','GIAO VU');
EXECUTE SA_COMPONENTS.CREATE_LEVEL('notification_policy',100,'NV','NHAN VIEN');
EXECUTE SA_COMPONENTS.CREATE_LEVEL('notification_policy',50,'SV','SINH VIEN');

-- create compartment
EXECUTE SA_COMPONENTS.CREATE_COMPARTMENT('notification_policy',5,'HTTT','HE THONG THONG TIN');
EXECUTE SA_COMPONENTS.CREATE_COMPARTMENT('notification_policy',10,'CNPM','CONG NGHE PHAN MEM');
EXECUTE SA_COMPONENTS.CREATE_COMPARTMENT('notification_policy',15,'KHMT','KHOA HOC MAY TINH');
EXECUTE SA_COMPONENTS.CREATE_COMPARTMENT('notification_policy',20,'CNTT','CONG NGHE THONG TIN');
EXECUTE SA_COMPONENTS.CREATE_COMPARTMENT('notification_policy',25,'TGMT','THI GIAC MAY TINH');
EXECUTE SA_COMPONENTS.CREATE_COMPARTMENT('notification_policy',30,'MMT','MANG MAY TINH');

-- create group
EXECUTE SA_COMPONENTS.CREATE_GROUP('notification_policy',10,'CS1','CO SO 1');
EXECUTE SA_COMPONENTS.CREATE_GROUP('notification_policy',15,'CS2','CO SO 2');
```

- Chạy hàm tạo label

```
CREATE OR REPLACE FUNCTION gen_notification_label(VAITRO VARCHAR2, MADV VARCHAR2, COSO VARCHAR2)
RETURN lbacsys.lbac_label AS
label VARCHAR2(30);
BEGIN
    label := VAITRO || ':' || MADV || ':' || COSO;
    RETURN to_lbac_data_label('notification_policy', label);
END;
/
```

- Áp dụng policy vào bảng THONGBAO

```
BEGIN
    SA_POLICY_ADMIN.REMOVE_TABLE_POLICY('notification_policy', 'AD', 'THONGBAO');
    SA_POLICY_ADMIN.APPLY_TABLE_POLICY (
        policy_name    => 'notification_policy',
        schema_name    => 'AD',
        table_name     => 'THONGBAO',
        table_options  => 'READ_CONTROL',
        label_function => 'AD.gen_notification_label(:new.VAITRO,:new.MADV,:new.COSO)',
        predicate => NULL
    );
END;
```

- Connect vào bằng quyền của sys
- Cấp quyền cho tài khoản

```
GRANT SELECT ON AD.THONGBAO TO NV002, NV006, NV016, NV017, NV018, NV028, NV014, SV0002, SV0015;
```

- Gán label cho user

```
BEGIN
 SA_USER_ADMIN.SET_USER_LABELS('notification_policy','NV002','TK:HTTT,CNPM,KHMT,CNTT,TGMT,MMT:CS1,CS2');
 SA_USER_ADMIN.SET_USER_LABELS(
      policy_name    => 'notification_policy',
      user_name      => 'NV016',
      max_read_label => 'TDV:HTTT,CNPM,KHMT,CNTT,TGMT,MMT:CS1,CS2');
 SA_USER_ADMIN.SET_USER_LABELS('notification_policy','NV006','GV:HTTT,CNPM,KHMT,CNTT,TGMT,MMT:CS1,CS2');
 SA_USER_ADMIN.SET_USER_LABELS('notification_policy','NV017','TDV:HTTT,CNPM,KHMT,CNTT,TGMT,MMT:CS1,CS2');
 SA_USER_ADMIN.SET_USER_LABELS('notification_policy','SV0002','SV:HTTT:CS1');
 SA_USER_ADMIN.SET_USER_LABELS('notification_policy','NV018','TDV:KHMT:CS1');
 SA_USER_ADMIN.SET_USER_LABELS('notification_policy','NV018','TDV:KHMT:CS1,CS2');
 SA_USER_ADMIN.SET_USER_LABELS('notification_policy','NV028','GVN:HTTT:CS1,CS2');
 SA_USER_ADMIN.SET_USER_LABELS('notification_policy','SV0015','SV:HTTT,CNPM,KHMT,CNTT,TGMT,MMT:CS1,CS2');
 SA_USER_ADMIN.SET_USER_LABELS('notification_policy','NV014','GVN:HTTT,CNPM,KHMT,CNTT,TGMT,MMT:CS1,CS2');
END;
```

3. Hướng dẫn build và run chương trình: yêu cầu 4 - Backup và Recovery

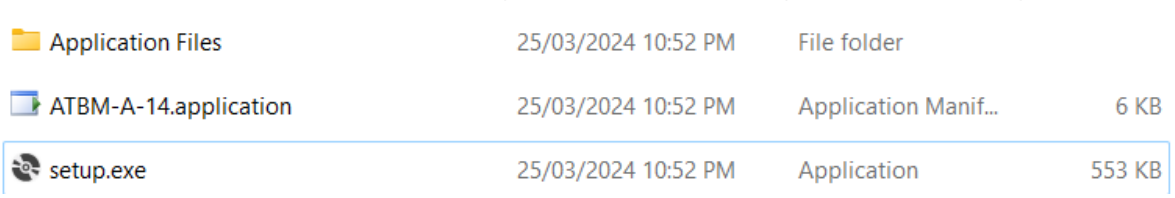
- Thực hiện cấu hình FRA gồm dung lượng và địa chỉ:
  alter system set db_recovery_file_dest_size = 10g scope = both;
  alter system set db_recovery_file_dest = '' scope = both;
- Recovery(trường hợp xảy ra sự cố mất file dữ liệu) - command line
- Kết nối vào sql bằng quyền sysdba
  sqlplus / as sysdba;
- Tắt cơ sở dữ liệu và khởi động ở chế độ nomount;
  shut abort;
  startup nomount;
- kết nối vào rman bằng lệnh
  rman target /
- Chọn control file từ thư mục auto backup trong FRA và thực hiện restore control file từ đường dẫn file backup trên:
  restore controlfile from '.BKP';
- Thay đổi database thành chế độ mount.
  alter database mount
- Thực hiện restore database, recover database.
  restore database;
  recover database;
- Mở database ở chế độ resetlogs.
  alter database open resetlogs;
- Kết thúc
  exit;

# III. Thông tin kèm theo

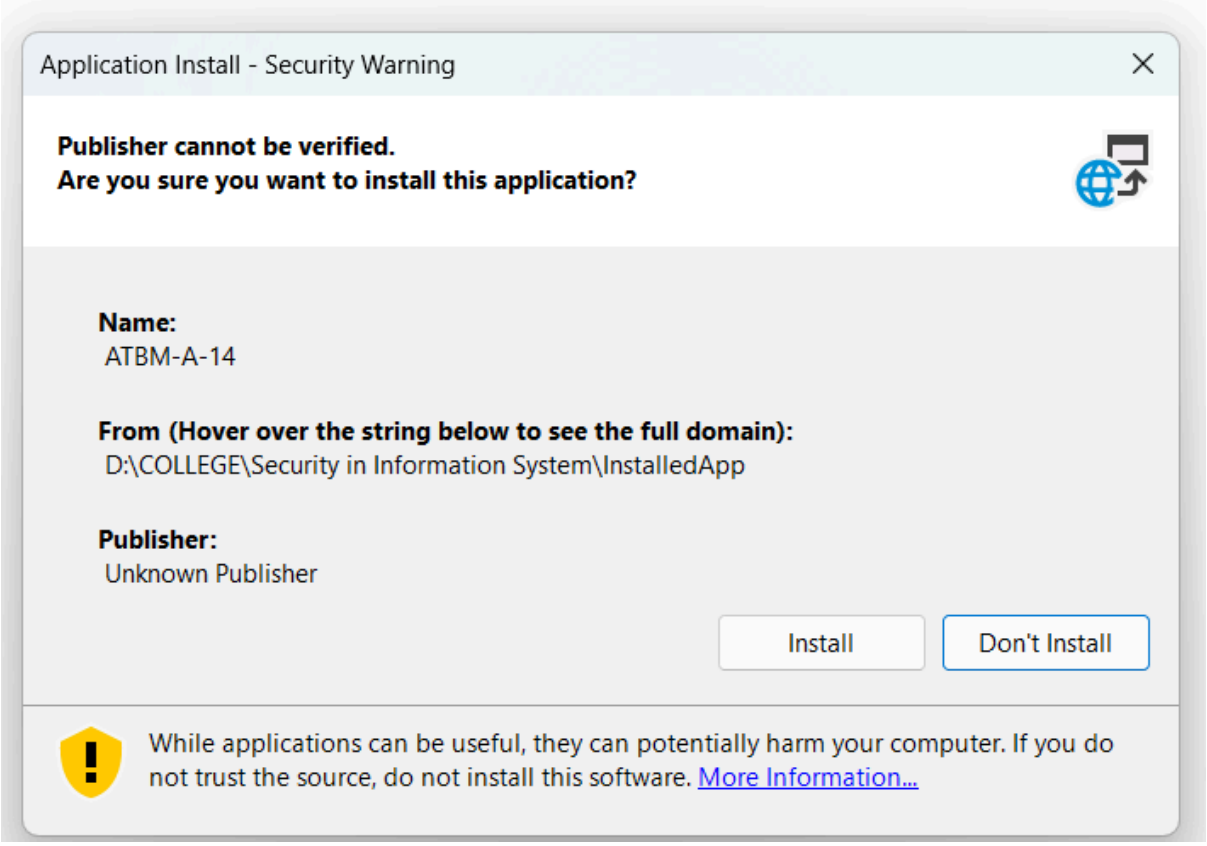
- Tên tài khoản của người dùng có toàn quyền hệ thống của Oracle DB Server: sys
- Tên tài khoản của người dùng có quyền quản trị trên Oracle DB Server: ad - Mật khẩu: 123

# IV. Hướng dẫn cài đặt App:

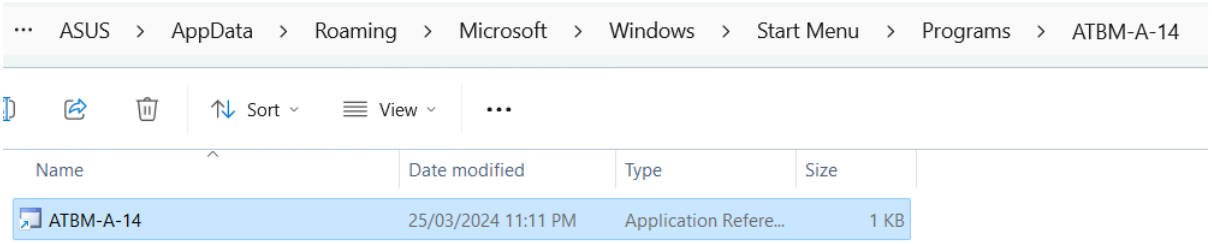
- Trong thư mục **Installations** chứa file thực thi cài đặt app




- Click file setup.exe để cài đặt app




- Click Install và App sẽ được cài đặt




- Sau khi cài đặt App sẽ có shortcut ở StartMenu