BÁO CÁO THỰC HÀNH

Bài thực hành số 03: Database Security

Môn học: An toàn mạng nâng cao

Lớp: NT534.P21.ANTT

- **THÀNH VIÊN THỰC HIỆN (Nhóm xx):**

STT	Họ và tên	MSSV
1	Phạm Phúc Hậu	21520836
2	Phan Nguyễn Nhật Trâm	22521501
3	Diệp Tấn Phát	22521066
4	Nguyễn Hải Phong	22521088

Điểm tự đánh giá
10

- **ĐÁNH GIÁ KHÁC:**

Tổng thời gian thực hiện	7 ngày
Phân chia công việc	
Ý kiến *(nếu có)* + Khó khăn + Đề xuất, kiến nghị	

Phần bên dưới của báo cáo này là báo cáo chi tiết của nhóm thực hiện

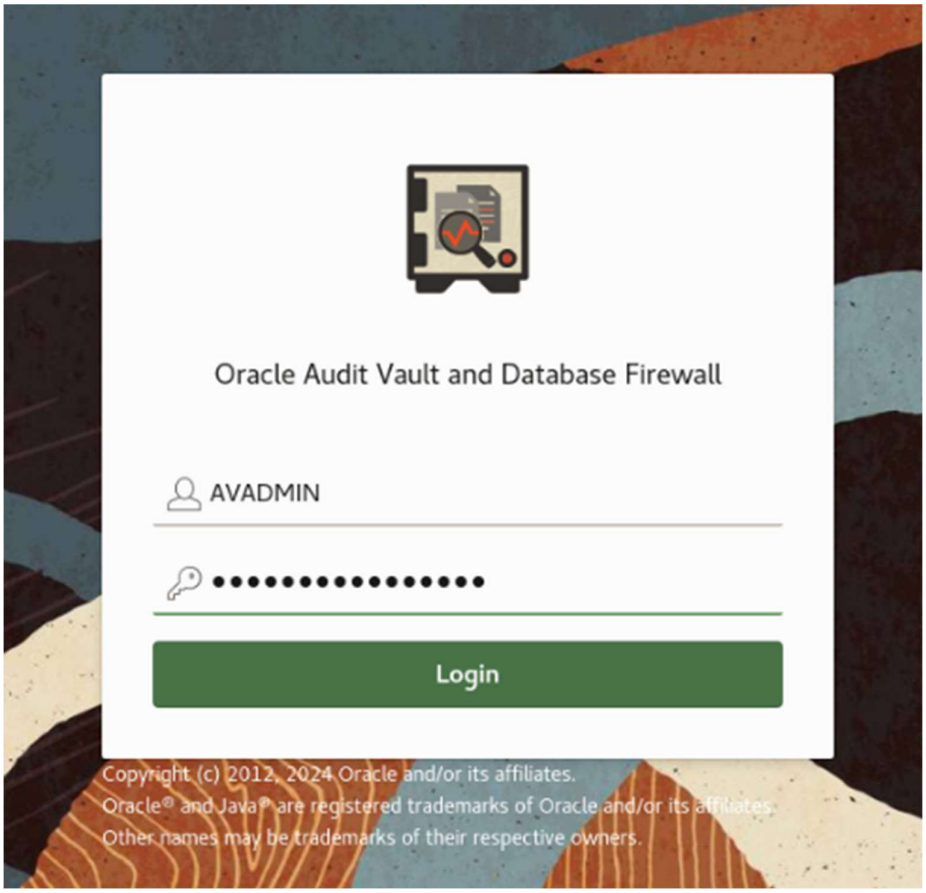
A. BÁO CÁO CHI TIẾT

1. Task 1: Reset the randomly generated password

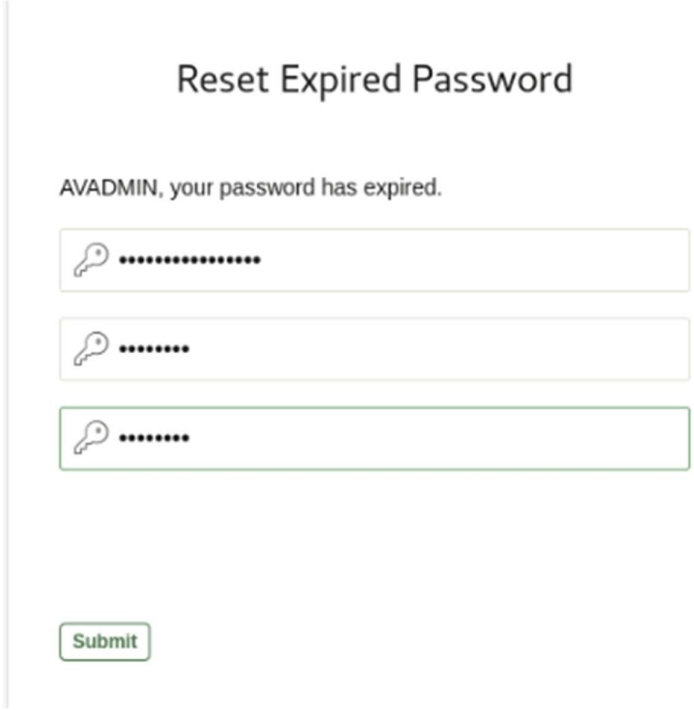
- Tìm nơi mật khẩu được tạo ngẫu nhiên

```
[cdb1:oracle@dbsec-lab:~/DBSecLab]$ cd $DBSEC_LABS/avdf/avs
[cdb1:oracle@dbsec-lab:~/DBSecLab/livelabs/avdf/avs]$ echo $AVUSR_PWD
w2LC95NVb2g0J+_n
[cdb1:oracle@dbsec-lab:~/DBSecLab/livelabs/avdf/avs]$
```

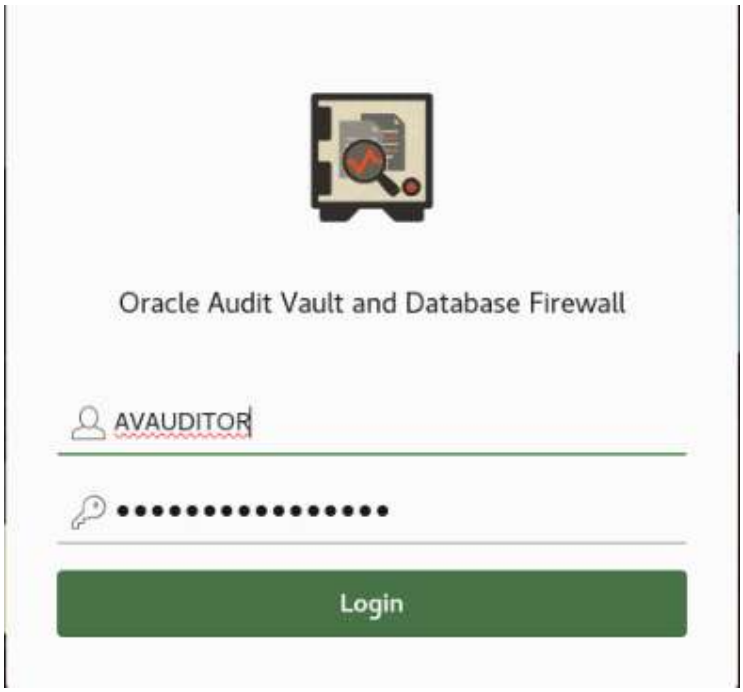
- Đăng nhập với AVADMIN và mật khẩu vừa tìm được



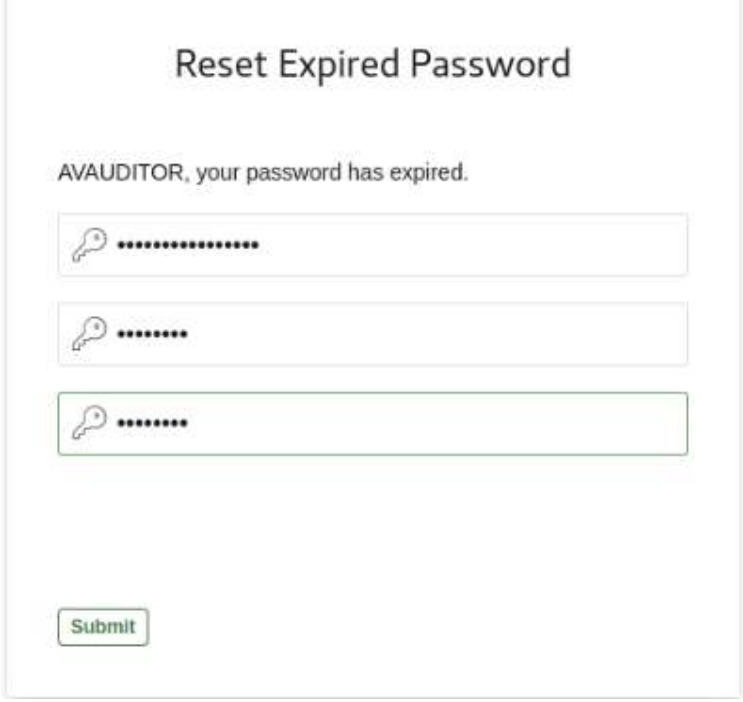
- Cài lại mật khẩu



- Đăng nhập với AVAUDITOR và mật khẩu đã tìm được ở trên

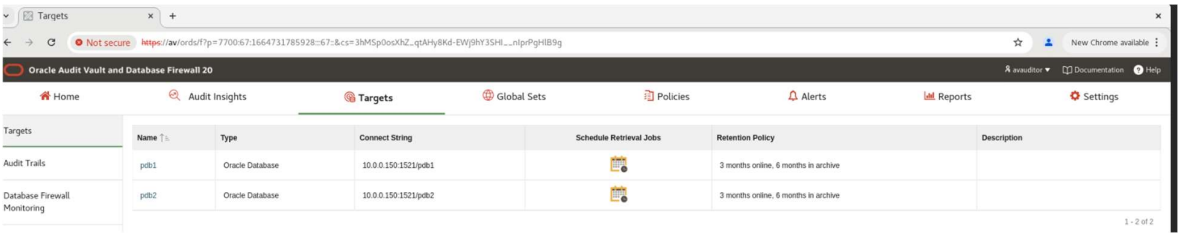


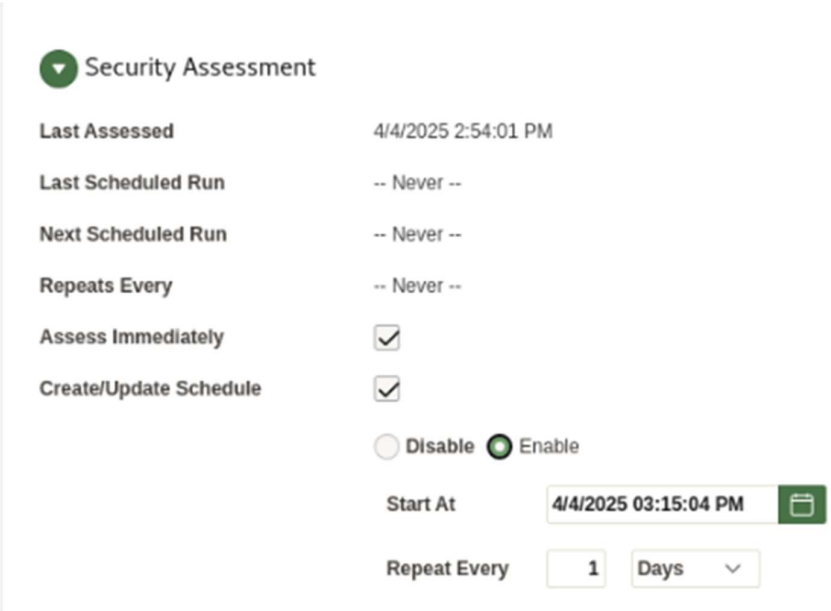
- Cài lại mật khẩu



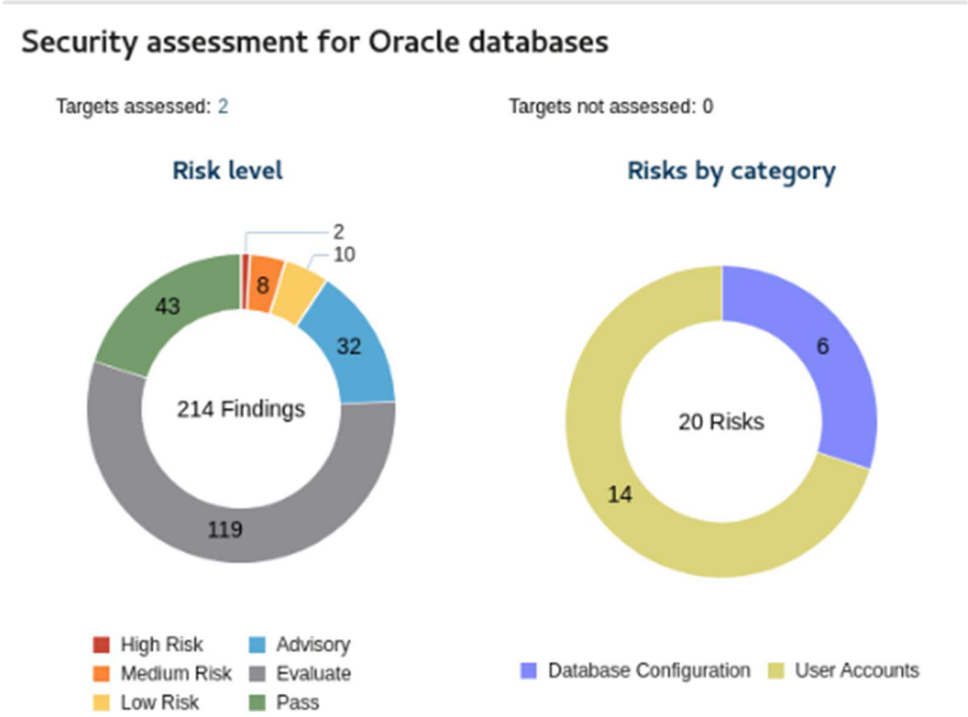
2. Task 2: Assess and Discover

- Đánh giá tình hình bảo mật của cơ sở dữ liệu Oracle





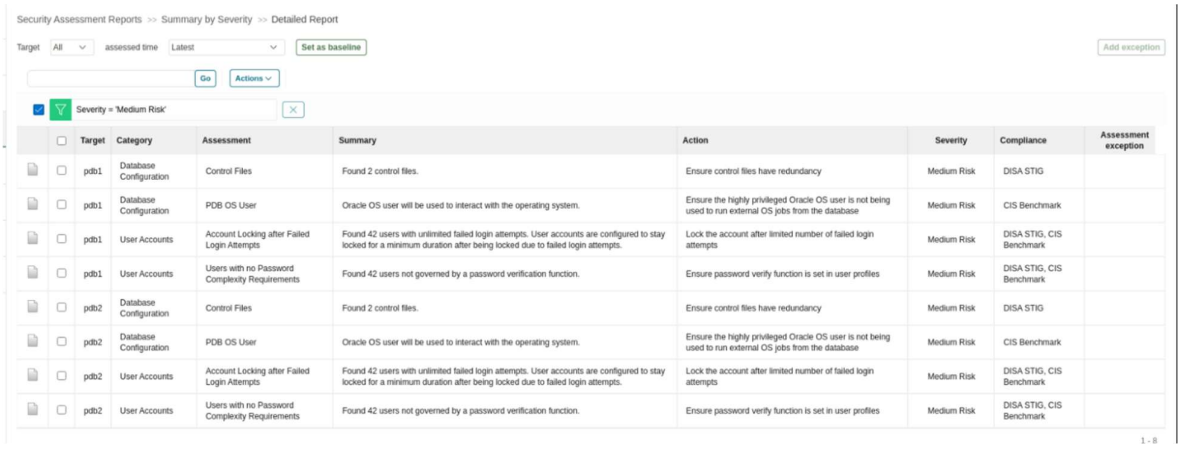
- Bây giờ có thể xem rủi ro cho tất cả các mục tiêu trực tiếp trên dashboard và có thể truy cập vào rủi ro bằng cách nhấp vào rủi ro màu trong vòng tròn ta chọn.



- Đối với tất cả các mục tiêu của ta, giờ đây có thể xem đánh giá đầy đủ về các rủi ro được phân loại theo mức độ nghiêm trọng cho từng danh mục

Severity	Targets	Basic Information	User Accounts	Privileges And Roles	Authorization Control	Fine-Grained Access Control	Auditing	Encryption	Database Configuration
High Risk	2	0	0	0	0	0	0	0	2
Medium Risk	2	0	4	0	0	0	0	0	4
Low Risk	2	0	10	0	0	0	0	0	0
Advisory	2	0	0	2	4	10	16	0	0
Evaluate	2	0	18	50	6	0	20	8	16
Pass	2	2	14	8	0	0	2	0	18

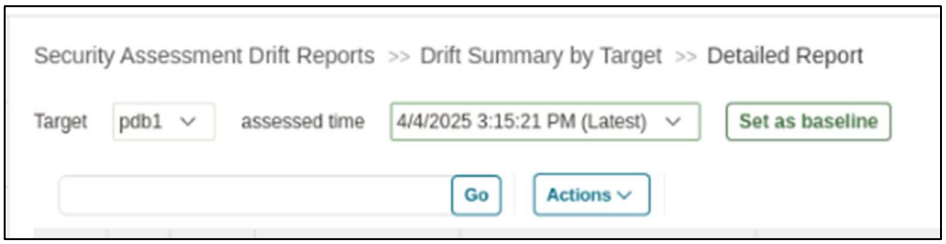
- Nhấp vào Medium Risk để xem các rủi ro được phát hiện cho tất cả các mục tiêu của ta
- Nhấp vào một trong số chúng để xem chi tiết. Ngoài ra, ta cũng có thể nhấp vào một trong các đánh giá và thêm ngoại lệ bằng cách thay đổi mức độ nghiêm trọng hoặc hoãn đánh giá.

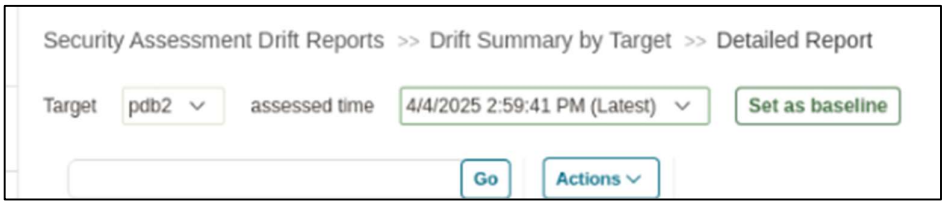


- Ta có thể xem tất cả các chi tiết về rủi ro này, lý do tại sao bạn có nguy cơ và không tuân thủ cũng như cách khắc phục.

Assessment Check	☐
Target	pdb1
Category	Database Configuration
Assessment	Control Files
Summary	Found 2 control files.
Action	Ensure control files have redundancy
Details	Control file(s) location: /u01/oradata/cdb1/control01.ctl, /u01/oradata/cdb1/control02.ctl All control files are in same directory.
Remarks	A control file tracks the physical components of the database. It is the root file that the database uses to find all the other files used by the database. Loss of access to the control files can affect database availability, integrity, and recovery. Due to the importance of the control file and to reduce the risk of losing it due to corruption, or accidental or intentional removal, Oracle recommends that the control file be multiplexed or have multiple identical copies. Organizations using RAID policies for multiplexing must review them to ensure control files are on separate, archived directories within one or more RAID devices.
Severity	Medium Risk
Oracle defined severity	Medium Risk
Assessment exception	
Compliance	DISA STIG
Compliance references	STIG V-219827
Disclaimer	

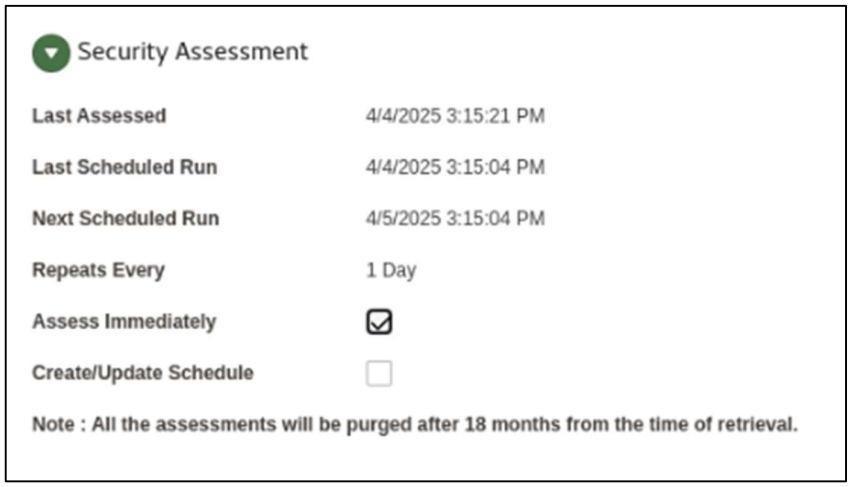
- Đặt đường cơ sở (baseline) và theo dõi độ trôi so với đường cơ sở

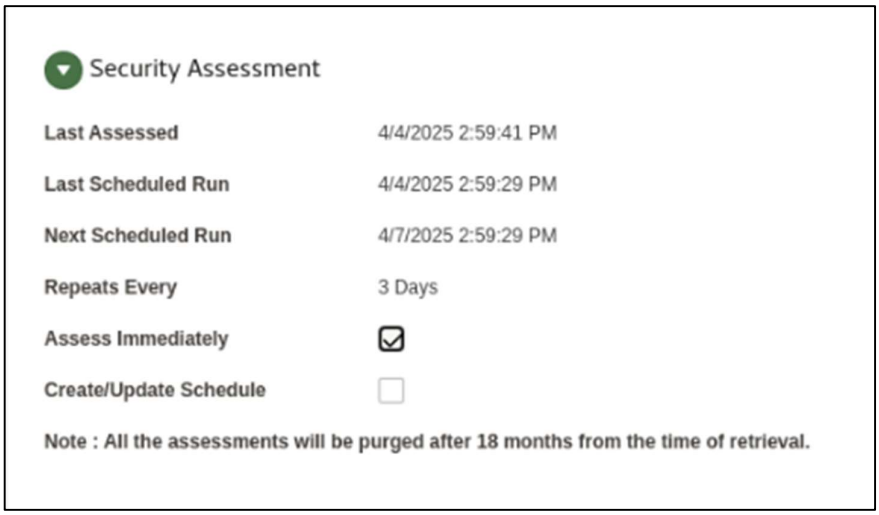




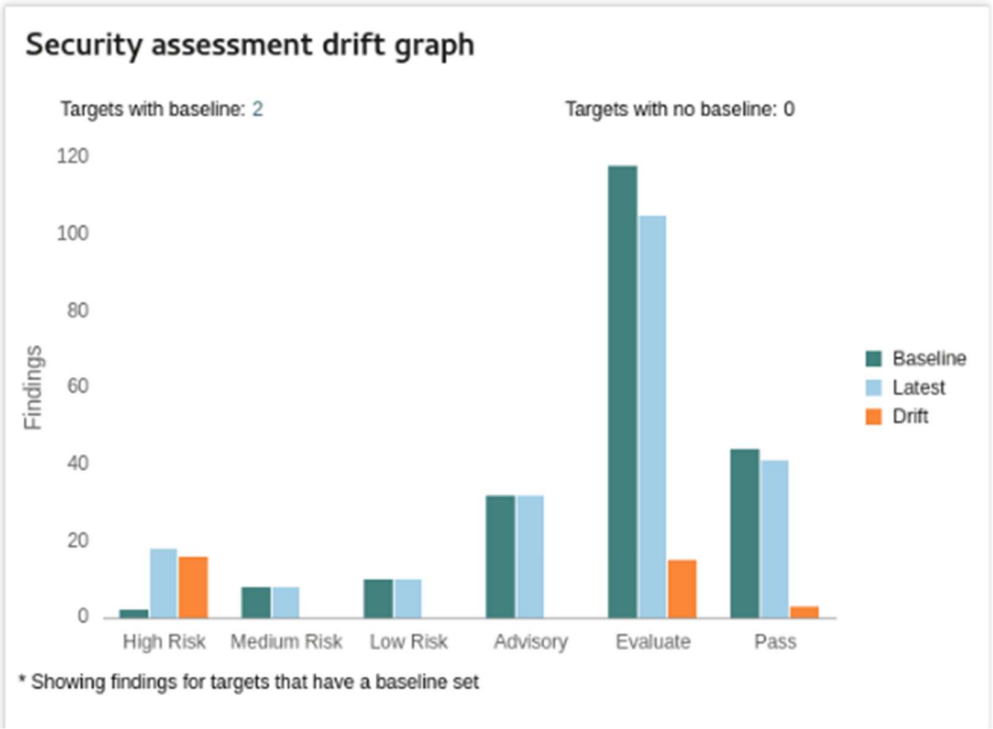
- Tạo ra drift từ lần quét trước

```
[cdb1:oracle@dbsec-lab:~/DBSecLab]$ cd $DBSEC_LABS/avdf/avs
[cdb1:oracle@dbsec-lab:~/DBSecLab/livelabs/avdf/avs]$ ./avs_drift-gen.sh pdb1

================================================================================
 Generate drift on pdb1...
================================================================================

Grant succeeded.


[cdb1:oracle@dbsec-lab:~/DBSecLab/livelabs/avdf/avs]$ ./avs_drift-gen.sh pdb2

================================================================================
 Generate drift on pdb2...
================================================================================

Grant succeeded.


[cdb1:oracle@dbsec-lab:~/DBSecLab/livelabs/avdf/avs]$
```





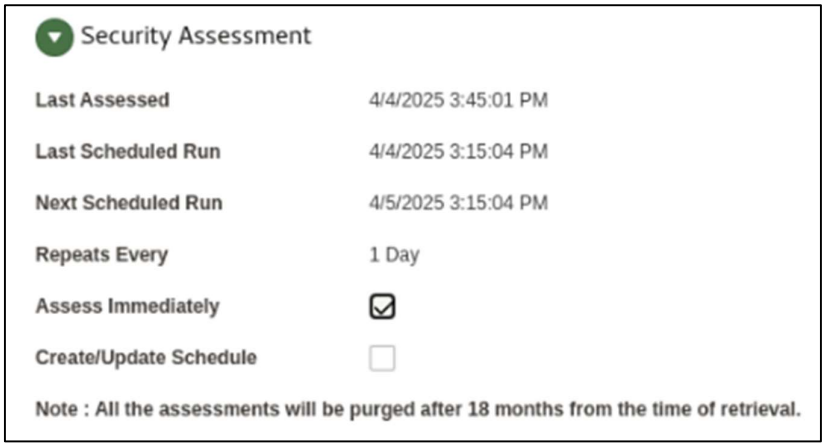
- Nhấp vào bất kỳ đánh giá nào sẽ đưa ta đến báo cáo trôi dạt chi tiết

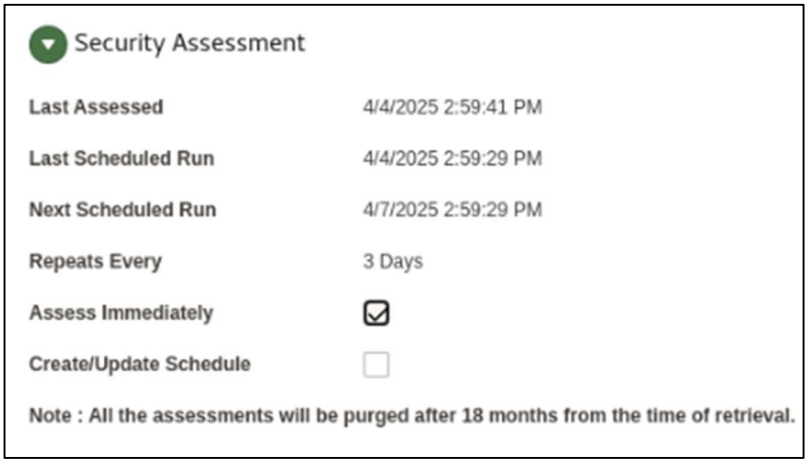


- Quay lại phiên cuối cùng để giảm thiểu rủi ro

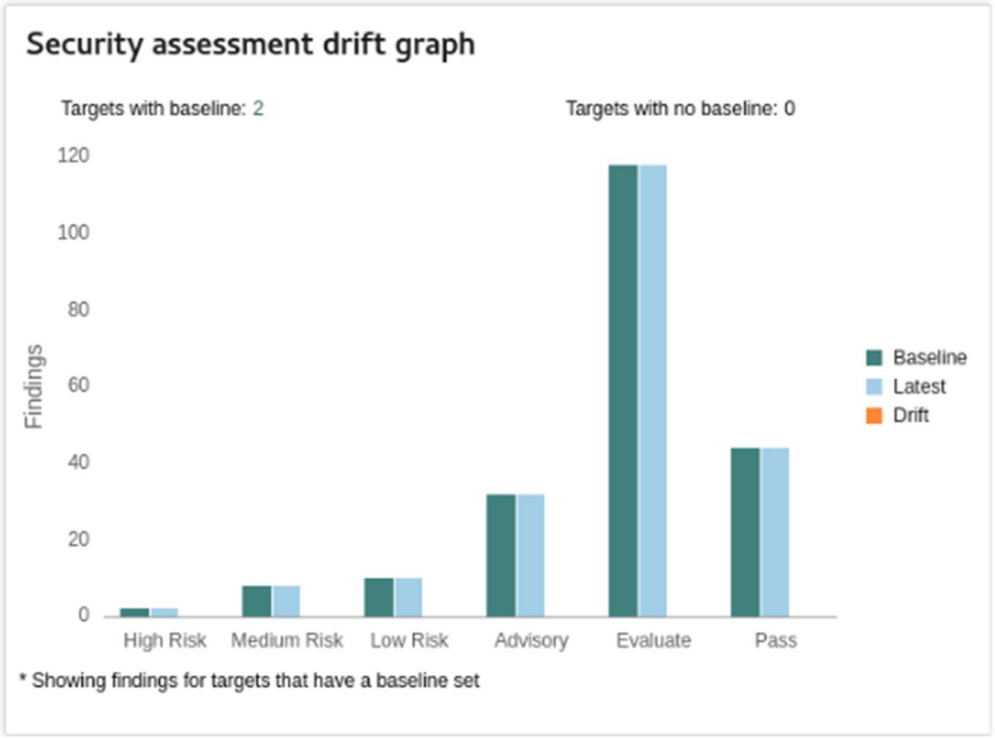
```
[cdb1:oracle@dbsec-lab:~/DBSecLab/livelabs/avdf/avs]$ ./avs_mitigate-risk.sh pdb1

================================================================================
 Mitigate the drift risk on pdb1...
================================================================================

Revoke succeeded.

[cdb1:oracle@dbsec-lab:~/DBSecLab/livelabs/avdf/avs]$ ./avs_mitigate-risk.sh pdb2

================================================================================
 Mitigate the drift risk on pdb2...
================================================================================

Revoke succeeded.

[cdb1:oracle@dbsec-lab:~/DBSecLab/livelabs/avdf/avs]$
```

- Quay lại Audit Vault Web Console với tư cách là AVAUDITOR để tạo đánh giá

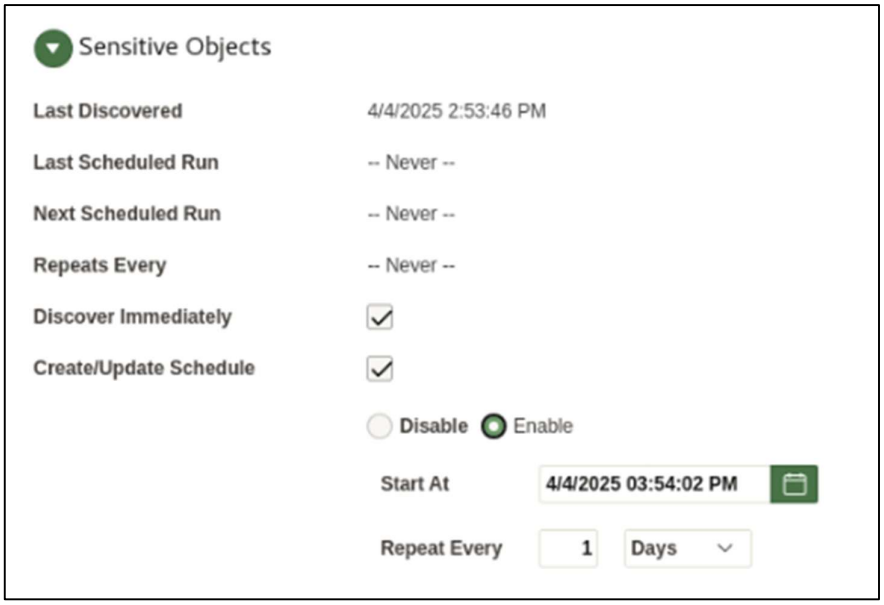


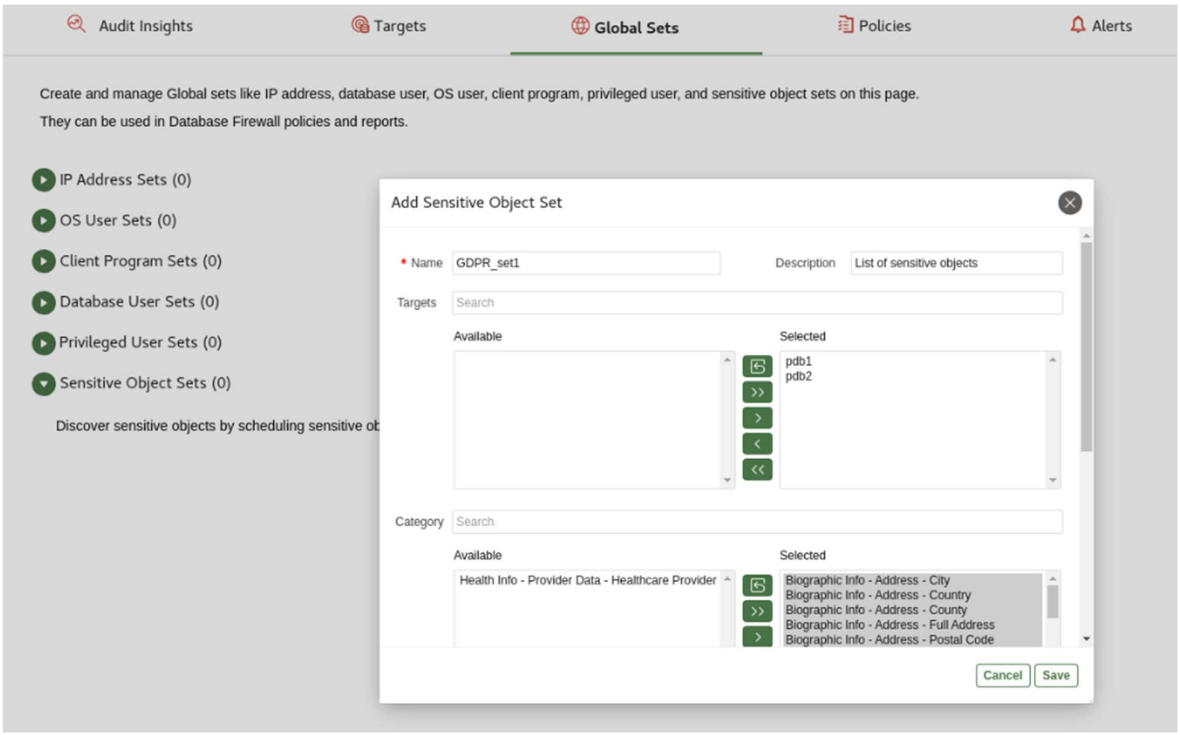


- Ta nhận thấy rằng sau khi thu hồi các quyền được cấp ở bước 4, số lượng rủi ro sẽ trở về trạng thái trước đó là rủi ro cao bằng không.



- Khám phá dữ liệu nhạy cảm trong cơ sở dữ liệu của ta và tạo một tập hợp toàn cầu

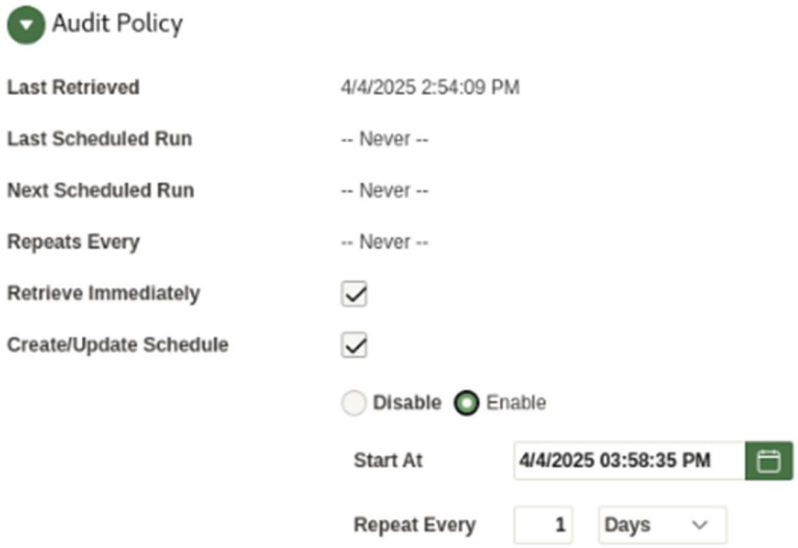




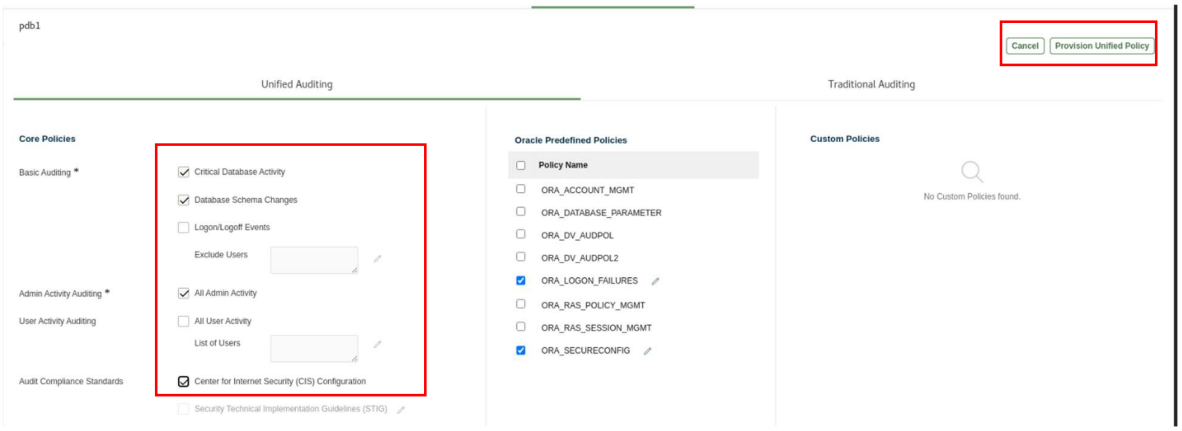
3. Task 3: AUDIT AND MONITOR

a. Quản lý và cấp phát chính sách audit từ AVDF cho cơ sở dữ liệu Oracle

- Audit trail đã được cấu hình sẵn cho hai cơ sở dữ liệu pdb1 và pdb2
    - pdb1 sử dụng phương pháp agent-based audit collection
    - pdb2 sử dụng agentless audit collection
- Truy cập giao diện Audit Vault Web Console bằng tài khoản AVAUDITOR
- Cấu hình audit cho pdb1:
    - Vào tab Targets → chọn Schedule Retrieval Jobs cho pdb1
    - Trong phần Audit Policy:
        - Tích chọn Retrieve Immediately
        - Tích chọn Create/Update Schedule
        - Bật chế độ Enable cho Schedule
        - Cài đặt lặp lại: Repeat Every 1 Days - Hệ thống sẽ tự động lấy các bản ghi audit từ cơ sở dữ liệu hằng ngày
        - Lưu cấu hình

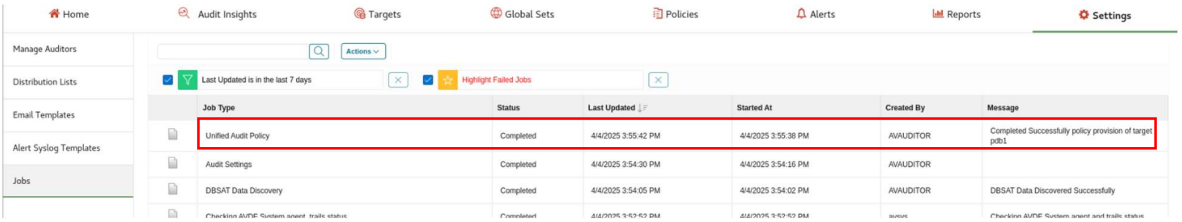


- Cấp phát chính sách audit cho pdb1:
  - Vào tab Policies → chọn pdb1
  - Chuyển sang tab Unified Auditing
  - Trong phần Core Policies, tích chọn:
    - Critical Database Activity
    - Database Schema Changes
    - All Admin Activity
    - Center for Internet Security (CIS) Configuration
  - Chọn Provision Unified Policy để cấp phát chính sách

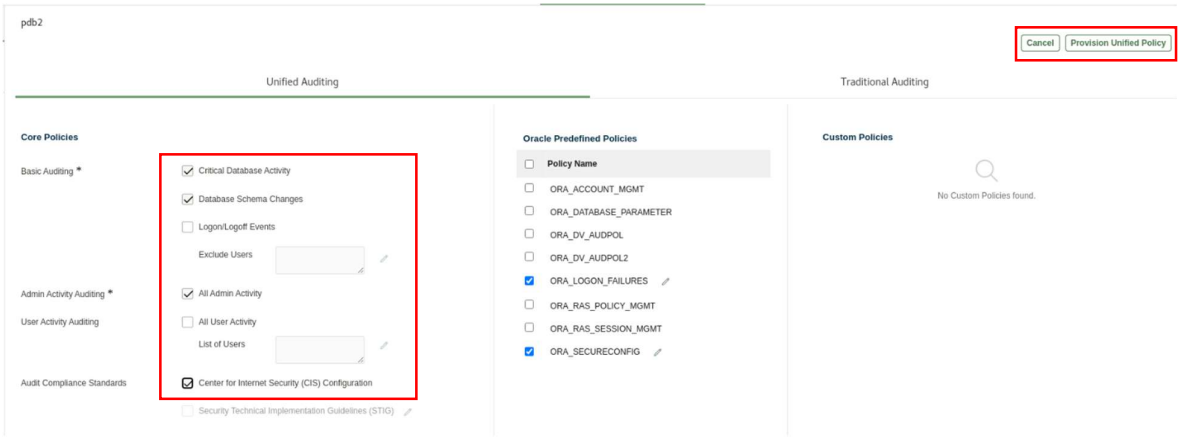


- Kiểm tra trạng thái Jobs:
  - Vào tab Settings → chọn Jobs.
  - Kiểm tra Job Type

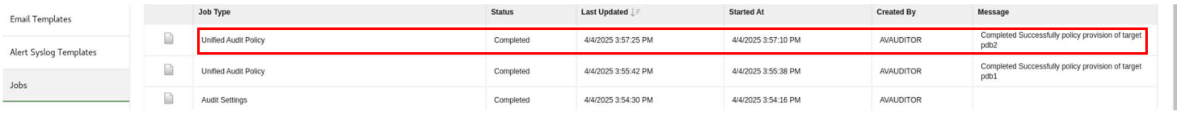
Bài thực hành số 03: Database Security



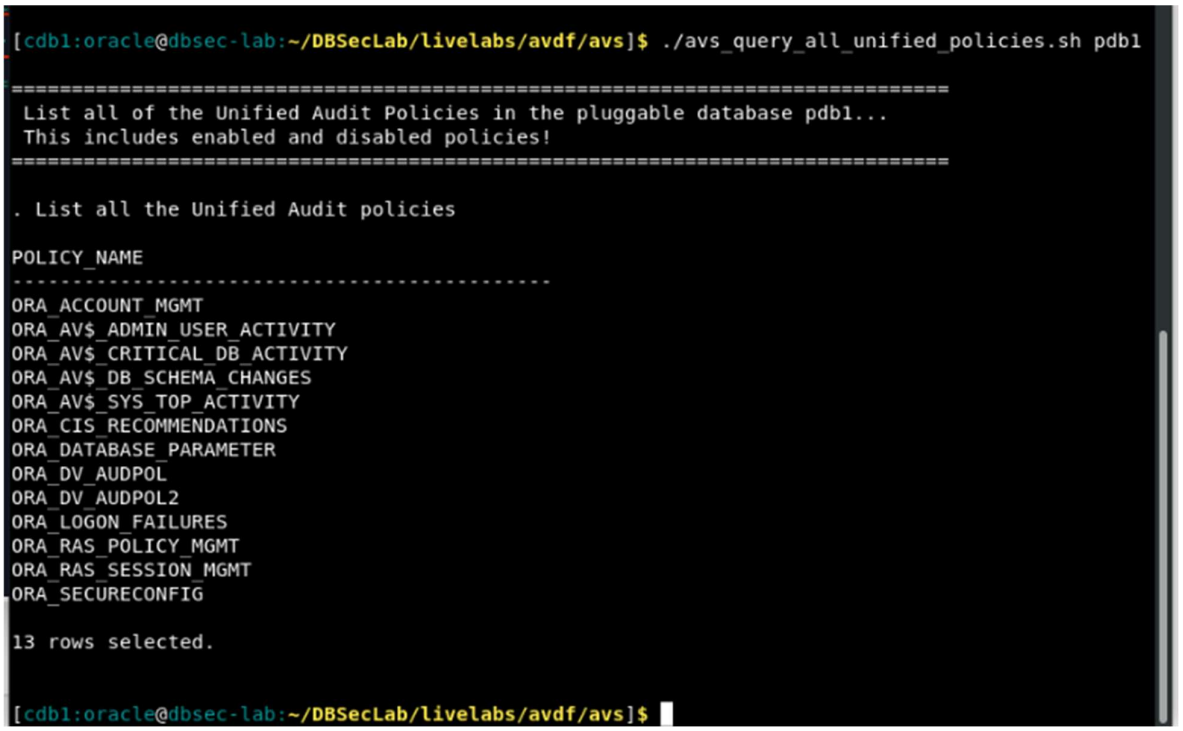
- Tương tự cho cấp phát chính sách audit cho pdb2



- Kiểm tra trạng thái Jobs pdb2:



- Kiểm tra chính sách audit bằng SQL*Plus
  - Liệt kê tất cả Unified Audit Policies trên pdb1



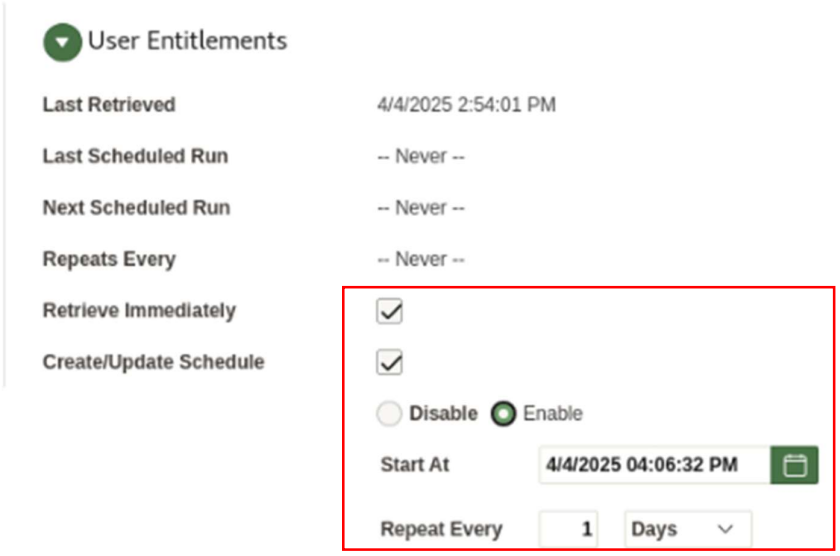
  - Liệt kê các Unified Audit Policies đang được kích hoạt

```
[cdb1:oracle@dbsec-lab:~/DBSecLab/livelabs/avdf/avs]$ ./avs_query_enabled_unified_policies.sh pdb1

==========================================================================
 List the ENABLED Unified Audit Policies in the pluggable database pdb1...
==========================================================================

. List the enabled Unified Audit policies

POLICY_NAME                                ENABLED_OPTION  ENTITY_NAME                      ENTITY_TYPE  SUCCESS     FAILURE
------------------------------------------ --------------- -------------------------------- ------------ ----------- -------
ORA_SECURECONFIG                           BY USER         ALL USERS                        USER         YES         YES
ORA_LOGON_FAILURES                         BY USER         ALL USERS                        USER         NO          YES
ORA_CIS_RECOMMENDATIONS                    BY USER         ALL USERS                        USER         YES         YES
ORA_AV$_SYS_TOP_ACTIVITY                   BY USER         SYS                              USER         YES         YES
ORA_AV$_DB_SCHEMA_CHANGES                  BY USER         ALL USERS                        USER         YES         YES
ORA_AV$_CRITICAL_DB_ACTIVITY               BY USER         ALL USERS                        USER         YES         YES
ORA_AV$_ADMIN_USER_ACTIVITY                BY USER         SYSKM                            USER         YES         YES
ORA_AV$_ADMIN_USER_ACTIVITY                BY USER         SYSRAC                           USER         YES         YES
ORA_AV$_ADMIN_USER_ACTIVITY                BY USER         SYSDG                            USER         YES         YES
ORA_AV$_ADMIN_USER_ACTIVITY                BY USER         SYSBACKUP                        USER         YES         YES
ORA_AV$_ADMIN_USER_ACTIVITY                BY GRANTED ROLE DBA                              ROLE         YES         YES
ORA_AV$_ADMIN_USER_ACTIVITY                BY GRANTED ROLE DATAPUMP_EXP_FULL_DATABASE       ROLE         YES         YES
ORA_AV$_ADMIN_USER_ACTIVITY                BY GRANTED ROLE DATAPUMP_IMP_FULL_DATABASE       ROLE         YES         YES
ORA_AV$_ADMIN_USER_ACTIVITY                BY USER         PUBLIC                           USER         YES         YES
ORA_AV$_ADMIN_USER_ACTIVITY                BY GRANTED ROLE IMP_FULL_DATABASE                ROLE         YES         YES
ORA_AV$_ADMIN_USER_ACTIVITY                BY GRANTED ROLE EXP_FULL_DATABASE                ROLE         YES         YES

16 rows selected.

[cdb1:oracle@dbsec-lab:~/DBSecLab/livelabs/avdf/avs]$
```

out in stay logged as AVAUDITOR)

b. Thu thập và giám sát phân quyền người dùng

- Truy cập lại tab Targets → chọn Schedule Retrieval Jobs cho pdb1.
- Trong phần User Entitlements:
  - Tích chọn Retrieve Immediately.
  - Tích chọn Create/Update Schedule.
  - Bật chế độ Enable cho Schedule.
  - Lặp lại mỗi 1 ngày.
- Lưu lại cấu hình.



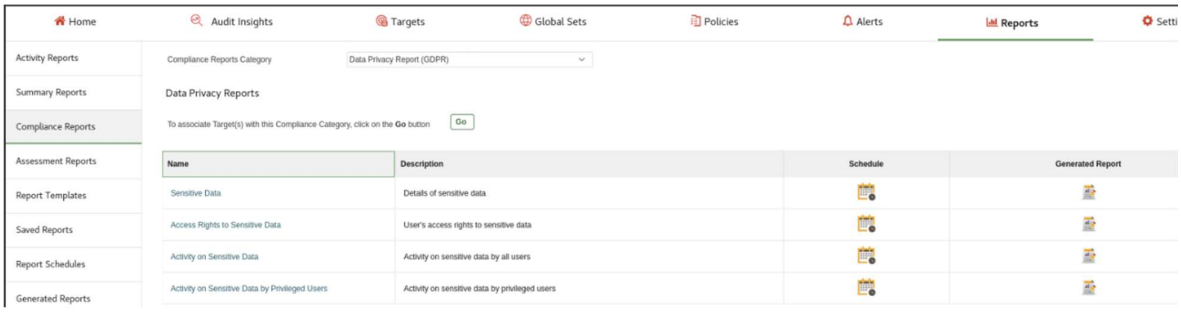
- Chuyển sang tab Reports.
- Cuộn xuống phần Entitlement Reports → chọn User Accounts.
  - Trong mục Target Name: chọn All
  - Trong Label: chọn Latest
  - Chọn Go để xem báo cáo phân quyền người dùng mới nhất

Target	User	Account Status	Lock Date	Profile	Expiry Date
pdb1	ANONYMOUS	EXPIRED & LOCKED	4/17/2019 2:04:18 AM	DEFAULT	4/17/2019 2:04:18 AM
pdb2	ANONYMOUS	EXPIRED & LOCKED	4/17/2019 2:04:18 AM	DEFAULT	4/17/2019 2:04:18 AM
pdb2	APPDEV_USER1	OPEN		DEFAULT	
pdb1	APPDEV_USER1	OPEN		DEFAULT	
pdb2	APPDEV_USER2	OPEN		DEFAULT	
pdb1	APPDEV_USER2	OPEN		DEFAULT	
pdb2	APPDEV_USER3	OPEN		DEFAULT	
pdb1	APPDEV_USER3	OPEN		DEFAULT	
pdb1	APPQOSSYS	LOCKED	10/20/2024 2:51:27 PM	DEFAULT	
pdb2	APPQOSSYS	LOCKED	10/20/2024 4:14:45 PM	DEFAULT	
pdb1	AUDSYS	LOCKED	10/20/2024 2:51:27 PM	DEFAULT	
pdb2	AUDSYS	LOCKED	10/20/2024 4:14:45 PM	DEFAULT	
pdb2	AVAUDITUSER	OPEN		DEFAULT	
pdb1	AVAUDITUSER	OPEN		DEFAULT	
pdb1	BACKUP_ADMIN	OPEN		DEFAULT	
pdb2	BACKUP_ADMIN	OPEN		DEFAULT	
pdb2	BA_BETTY	OPEN		DEFAULT	

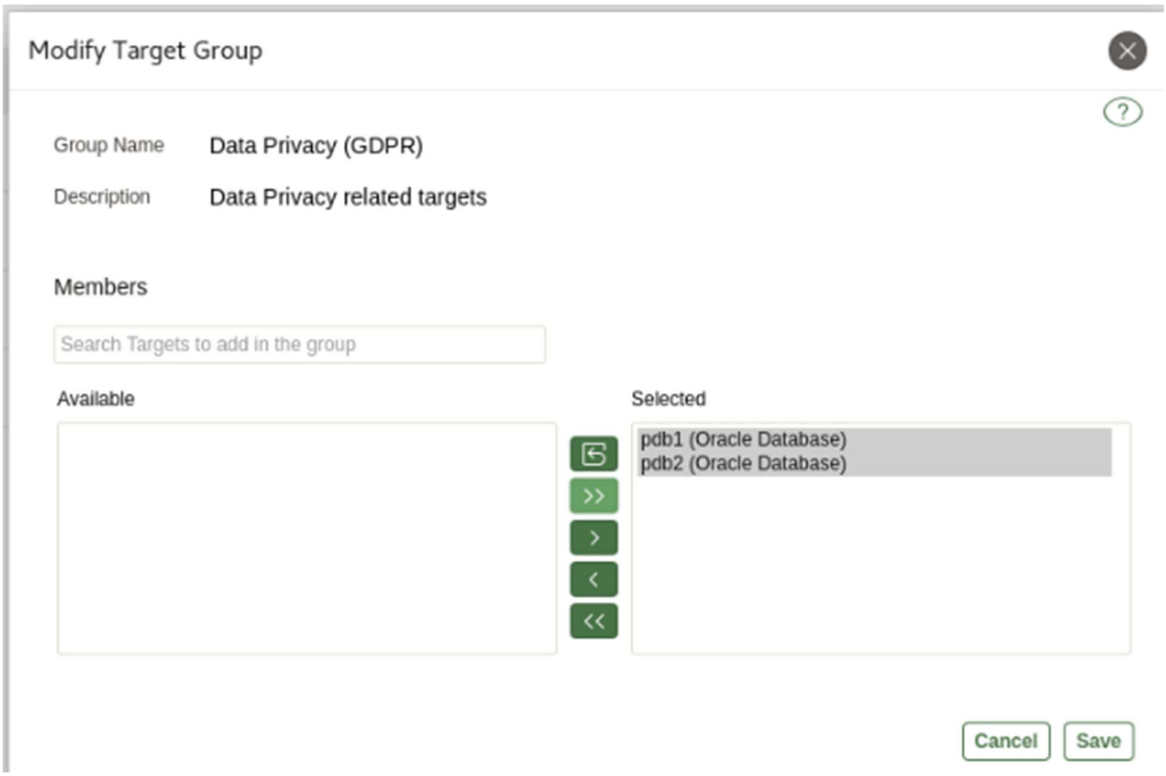
4. Task 4: Report and Alert

c. Phân tích quyền truy cập người dùng và hoạt động trên dữ liệu nhạy cảm

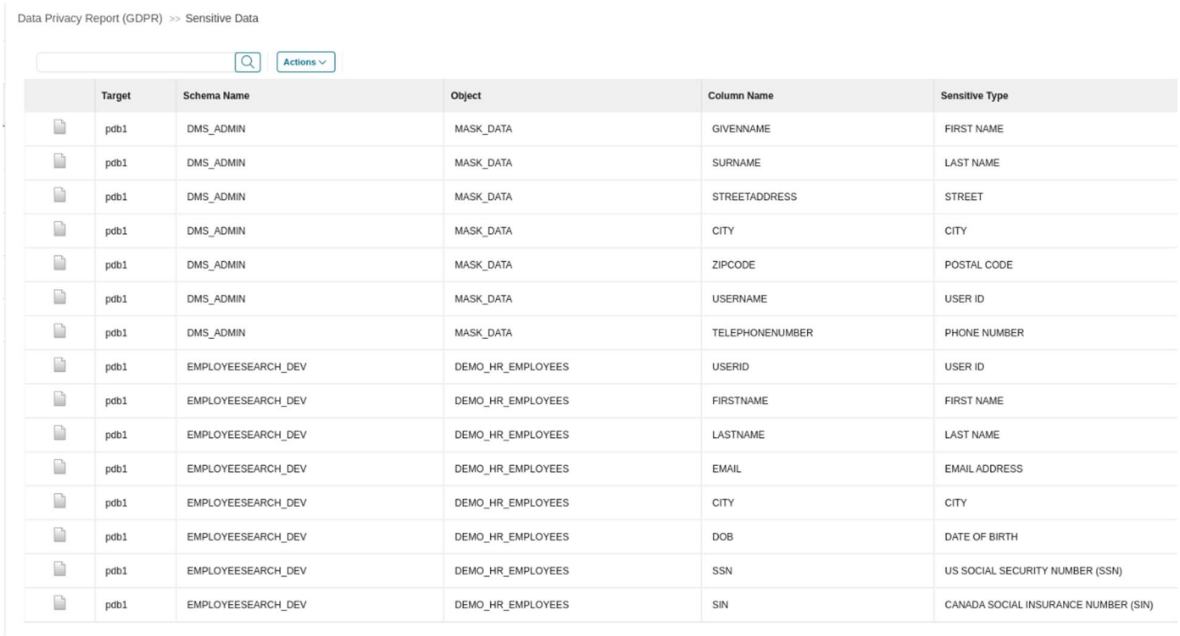
- Đăng nhập vào Audit Vault Web Console với tài khoản AVAUDITOR
- Vào tab Reports → chọn Compliance Reports từ menu bên trái
- Chọn "Data Private Report (GDPR)" trong mục Compliance Reports Category → chọn Go



- Chọn liên kết với hai CSDL: pdb1 và pdb2, sau đó chọn Save để lưu.

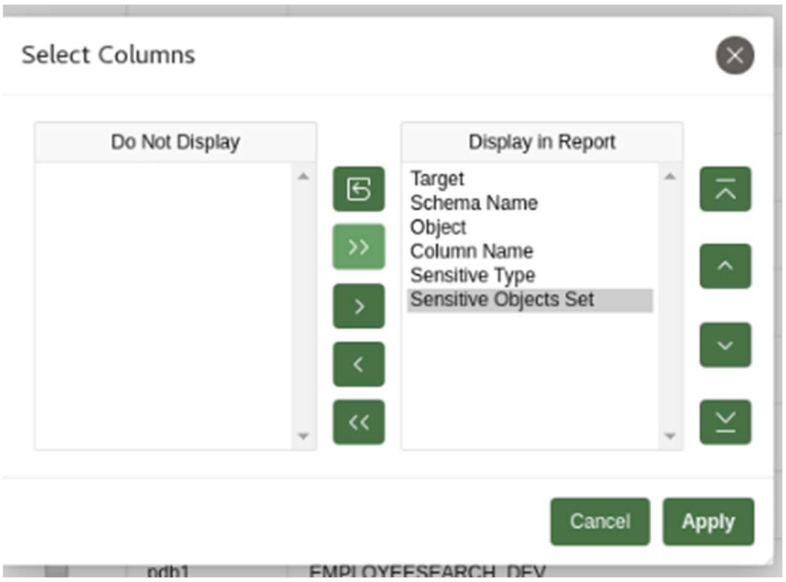


- Chọn báo cáo Sensitive Data để xem chi tiết:



	Target	Schema Name	Object	Column Name	Sensitive Type
	pdb1	DMS_ADMIN	MASK_DATA	GIVENNAME	FIRST NAME
	pdb1	DMS_ADMIN	MASK_DATA	SURNAME	LAST NAME
	pdb1	DMS_ADMIN	MASK_DATA	STREETADDRESS	STREET
	pdb1	DMS_ADMIN	MASK_DATA	CITY	CITY
	pdb1	DMS_ADMIN	MASK_DATA	ZIPCODE	POSTAL CODE
	pdb1	DMS_ADMIN	MASK_DATA	USERNAME	USER ID
	pdb1	DMS_ADMIN	MASK_DATA	TELEPHONENUMBER	PHONE NUMBER
	pdb1	EMPLOYEESEARCH_DEV	DEMO_HR_EMPLOYEES	USERID	USER ID
	pdb1	EMPLOYEESEARCH_DEV	DEMO_HR_EMPLOYEES	FIRSTNAME	FIRST NAME
	pdb1	EMPLOYEESEARCH_DEV	DEMO_HR_EMPLOYEES	LASTNAME	LAST NAME
	pdb1	EMPLOYEESEARCH_DEV	DEMO_HR_EMPLOYEES	EMAIL	EMAIL ADDRESS
	pdb1	EMPLOYEESEARCH_DEV	DEMO_HR_EMPLOYEES	CITY	CITY
	pdb1	EMPLOYEESEARCH_DEV	DEMO_HR_EMPLOYEES	DOB	DATE OF BIRTH
	pdb1	EMPLOYEESEARCH_DEV	DEMO_HR_EMPLOYEES	SSN	US SOCIAL SECURITY NUMBER (SSN)
	pdb1	EMPLOYEESEARCH_DEV	DEMO_HR_EMPLOYEES	SIN	CANADA SOCIAL INSURANCE NUMBER (SIN)

- Tuỳ chỉnh thêm bằng cách chọn Actions → Select Columns → tích chọn Sensitive Objects Sets → chọn Apply

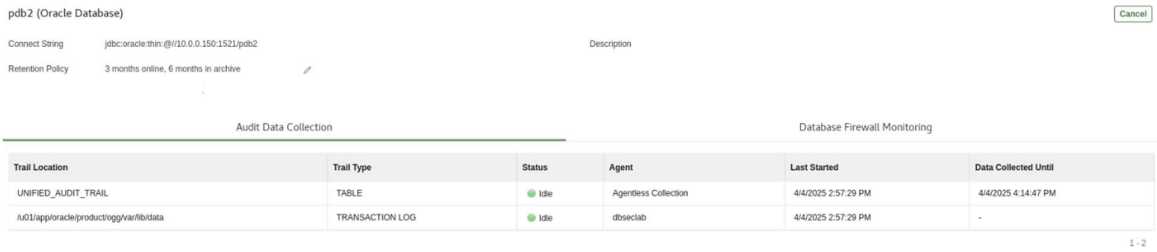


- Global set liên quan

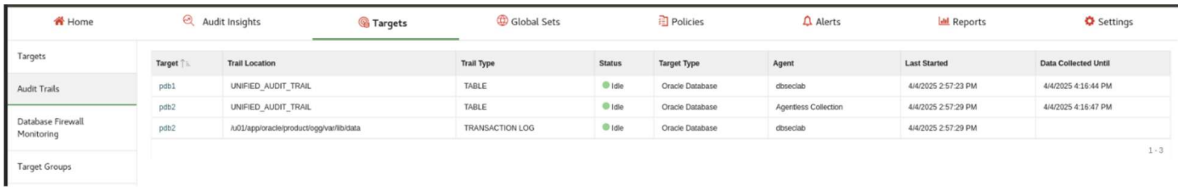
	Target	Schema Name	Object	Column Name	Sensitive Type	Sensitive Objects Set
	pdb1	DMS_ADMIN	MASK_DATA	GIVENNAME	FIRST NAME	GDPR_set1
	pdb1	DMS_ADMIN	MASK_DATA	SURNAME	LAST NAME	GDPR_set1
	pdb1	DMS_ADMIN	MASK_DATA	STREETADDRESS	STREET	GDPR_set1
	pdb1	DMS_ADMIN	MASK_DATA	CITY	CITY	GDPR_set1
	pdb1	DMS_ADMIN	MASK_DATA	ZIPCODE	POSTAL CODE	GDPR_set1
	pdb1	DMS_ADMIN	MASK_DATA	USERNAME	USER ID	GDPR_set1
	pdb1	DMS_ADMIN	MASK_DATA	TELEPHONENUMBER	PHONE NUMBER	GDPR_set1
	pdb1	EMPLOYEESEARCH_DEV	DEMO_HR_EMPLOYEES	USERID	USER ID	GDPR_set1
	pdb1	EMPLOYEESEARCH_DEV	DEMO_HR_EMPLOYEES	FIRSTNAME	FIRST NAME	GDPR_set1
	pdb1	EMPLOYEESEARCH_DEV	DEMO_HR_EMPLOYEES	LASTNAME	LAST NAME	GDPR_set1

d.Theo dõi thay đổi dữ liệu ("Before-After" Values Auditing) trên pdb2

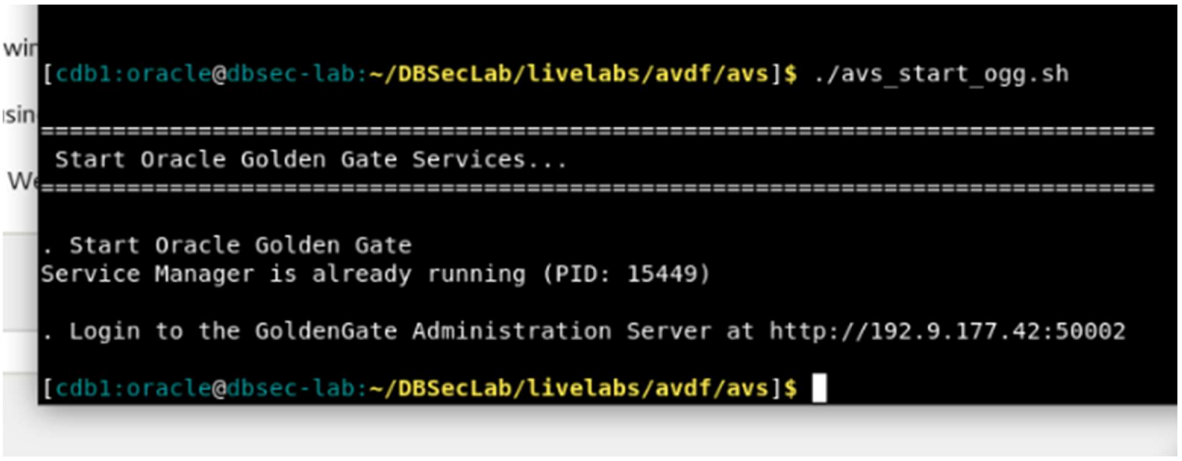
- Kiểm tra Log trail có hoạt động không:
  - Vào tab Targets → chọn pdb2
  - Kiểm tra trong phần Audit Trail, xác nhận trạng thái là COLLECTING hoặc IDLE.



- Kiểm tra trạng thái thu thập log, đảm bảo hệ thống đang thu thập dữ liệu

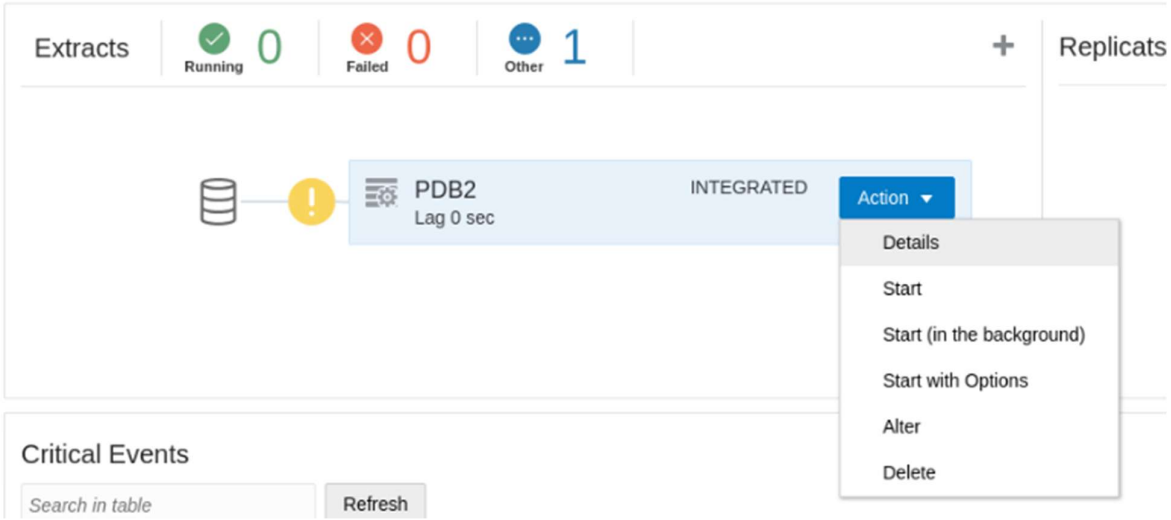


- Đảm bảo dịch vụ Oracle GoldenGate đang hoạt động



- Đăng nhập GoldenGate Web Console

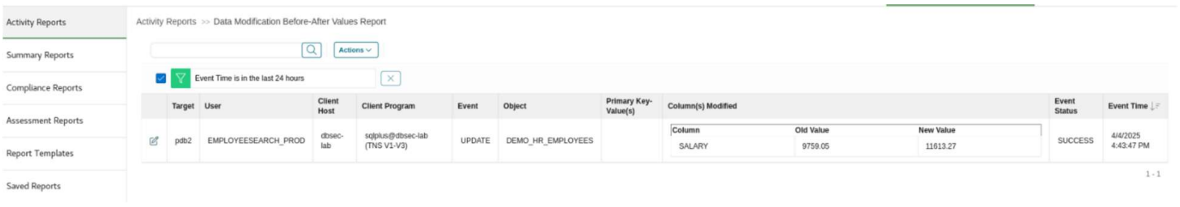
- Khởi động Extract cho pdb2



- Tạo một số thao tác cập nhật dữ liệu trong database

```
. Run some queries as employeesearch_prod
USER is "EMPLOYEESEARCH_PROD"

  COUNT(*)
----------
      1000


FIRSTNAME                 LASTNAME                                 SALARY
------------------------- ---------------------------------- ----------
Lisa                      Alexander                              9759.05


1 row updated.


FIRSTNAME                 LASTNAME                                 SALARY
------------------------- ---------------------------------- ----------
Lisa                      Alexander                             11613.27


Table created.


  COUNT(*)
----------
      1000


Table dropped.


. Run some queries as dba_debra
USER is "DBA_DEBRA"
FIRSTNAME                 LASTNAME                                 SALARY
------------------------- ---------------------------------- ----------
Evil                      Rich                                     3871


1 row updated.


FIRSTNAME                 LASTNAME                                 SALARY
------------------------- ---------------------------------- ----------
Roger                     Rabbit                                   3871


[cdb1:oracle@dbsec-lab:~/DBSecLab/livelabs/avdf/avs]$
```

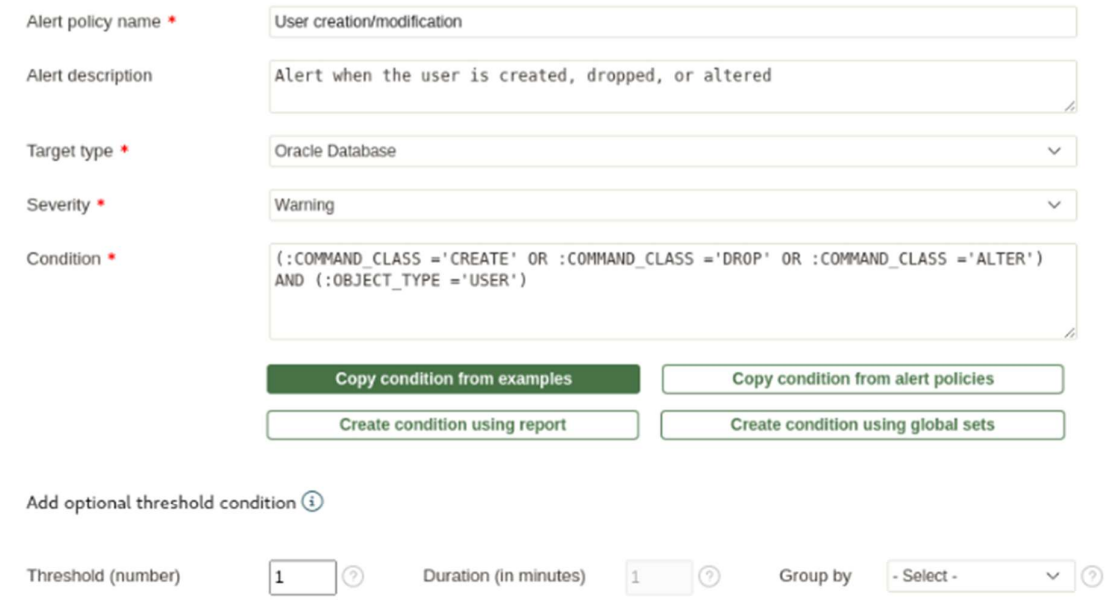
- Xem báo cáo chứa dữ liệu thay đổi



e. Thiết lập chính sách cảnh báo

- Cảnh báo khi có thao tác tạo/sửa/xóa người dùng
  - Vào tab Policies → Alert Policies → [Create].

- Điền các thông tin



- Cảnh báo đã được bắt đầu

Alert policy name	Enabled	Target type	Email notification	Created by	Last updated	Alerts	Alert description
Database Firewall Alert	✓	- All -	✗	AVSYS	2/28/2025 5:17:18 PM		An alert evaluated at a Database Firewall, based on a Firewall Policy.
CREATE USER	✓	Oracle Database	✗	AVAUDITOR	4/4/2025 2:57:29 PM		Alert on CREATE USER statements
User creation/modification	✓	Oracle Database	✗	AVAUDITOR	4/4/2025 4:50:39 PM		Alert when the user is created, dropped, or altered

1 - 3

- Chạy script tạo và xóa người dùng

```
[cdb1:oracle@dbsec-lab:~/DBSecLab/livelabs/avdf/avs]$ ./avs_create_users.sh pdb1

================================================================================
 Created users on pdb1 for testing the Audit Vault alert policy...
================================================================================

. Create user "new_user_fred" as sys
USER is "SYS"

User created.


. Create user "new_user_ted" as system
USER is "SYSTEM"

User created.


. Create user "new_user_ned" as dba_debra
USER is "DBA_DEBRA"

User created.


[cdb1:oracle@dbsec-lab:~/DBSecLab/livelabs/avdf/avs]$
```

```
[cdb1:oracle@dbsec-lab:~/DBSecLab/livelabs/avdf/avs]$ ./avs_create_users.sh pdb2

================================================================================
 Created users on pdb2 for testing the Audit Vault alert policy...
================================================================================

. Create user "new_user_fred" as sys
USER is "SYS"

User created.


. Create user "new_user_ted" as system
USER is "SYSTEM"

User created.


. Create user "new_user_ned" as dba_debra
USER is "DBA_DEBRA"

User created.


[cdb1:oracle@dbsec-lab:~/DBSecLab/livelabs/avdf/avs]$
```

```
[cdb1:oracle@dbsec-lab:~/DBSecLab/livelabs/avdf/avs]$ ./avs_drop_users.sh pdb1

==========================================================================
 Drop users created on pdb1 for testing the Audit Vault alert policy...
==========================================================================

. Drop users

User dropped.


User dropped.


User dropped.

[cdb1:oracle@dbsec-lab:~/DBSecLab/livelabs/avdf/avs]$
```

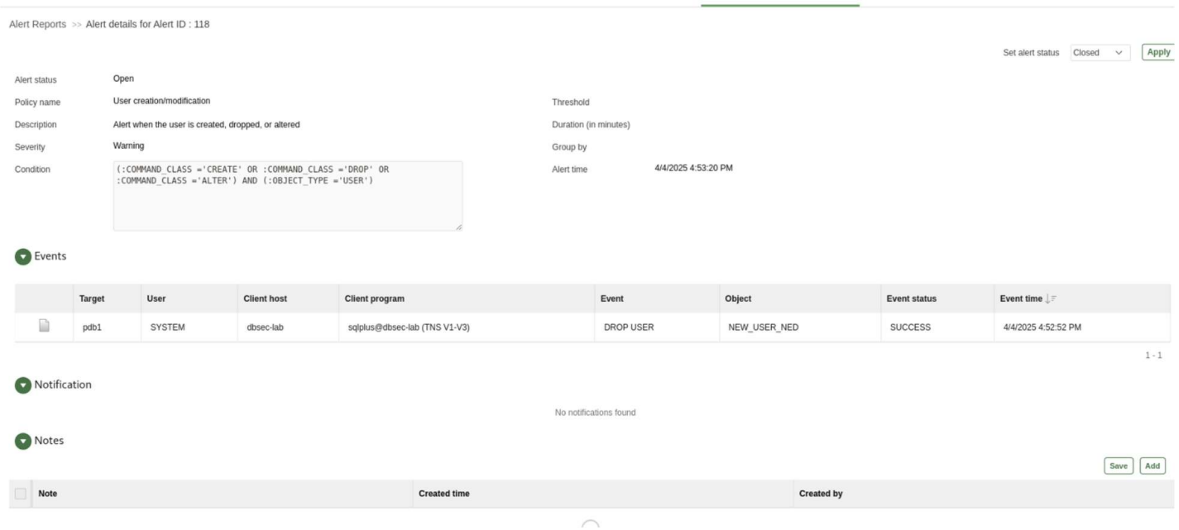
```
[cdb1:oracle@dbsec-lab:~/DBSecLab/livelabs/avdf/avs]$ ./avs_drop_users.sh pdb2

==========================================================================
 Drop users created on pdb2 for testing the Audit Vault alert policy...
==========================================================================

. Drop users

User dropped.


User dropped.


User dropped.

[cdb1:oracle@dbsec-lab:~/DBSecLab/livelabs/avdf/avs]$
```

- Vào tab Alerts để xem các cảnh báo đã xảy ra

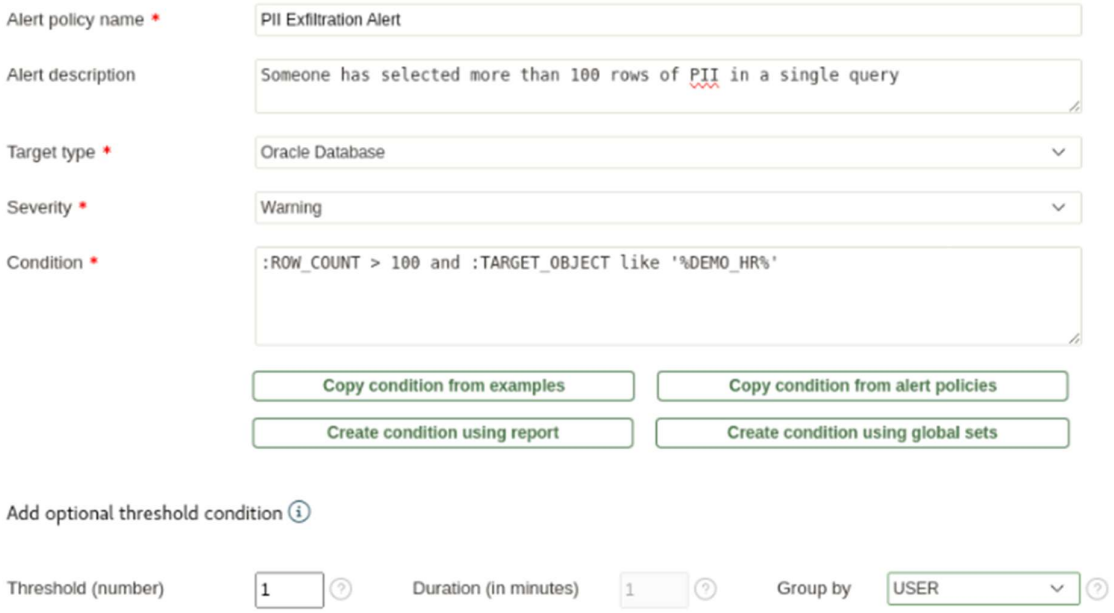
Alert time is in the last 24 hours

Alert ID	Alert status	Alert policy name	Alert severity	Alert time	Target	User	Event
118	Open	User creation/modification	Warning	4/4/2025 4:53:20 PM	pdb1	SYSTEM	DROP USER
117	Open	User creation/modification	Warning	4/4/2025 4:53:20 PM	pdb1	SYSTEM	DROP USER
116	Open	User creation/modification	Warning	4/4/2025 4:53:20 PM	pdb1	SYSTEM	DROP USER
115	Open	User creation/modification	Warning	4/4/2025 4:53:20 PM	pdb2	SYSTEM	DROP USER
114	Open	User creation/modification	Warning	4/4/2025 4:53:20 PM	pdb2	SYSTEM	DROP USER
113	Open	User creation/modification	Warning	4/4/2025 4:53:20 PM	pdb2	SYSTEM	DROP USER
112	Open	User creation/modification	Warning	4/4/2025 4:52:35 PM	pdb1	DBA_DEBRA	CREATE USER
111	Open	CREATE USER	Critical	4/4/2025 4:52:35 PM	pdb1	DBA_DEBRA	CREATE USER
110	Open	User creation/modification	Warning	4/4/2025 4:52:35 PM	pdb1	SYSTEM	CREATE USER
109	Open	CREATE USER	Critical	4/4/2025 4:52:35 PM	pdb1	SYSTEM	CREATE USER
108	Open	User creation/modification	Warning	4/4/2025 4:52:35 PM	pdb1	SYS	CREATE USER
107	Open	User creation/modification	Warning	4/4/2025 4:52:35 PM	pdb2	DBA_DEBRA	CREATE USER
106	Open	CREATE USER	Critical	4/4/2025 4:52:35 PM	pdb2	DBA_DEBRA	CREATE USER
105	Open	User creation/modification	Warning	4/4/2025 4:52:35 PM	pdb2	SYSTEM	CREATE USER
104	Open	CREATE USER	Critical	4/4/2025 4:52:35 PM	pdb2	SYSTEM	CREATE USER

- Nội dung chi tiết cảnh báo



- Cảnh báo khi có hành vi truy xuất dữ liệu nhạy cảm
  - Vào Policies → Alert Policies → Create
  - Cấu hình Policy

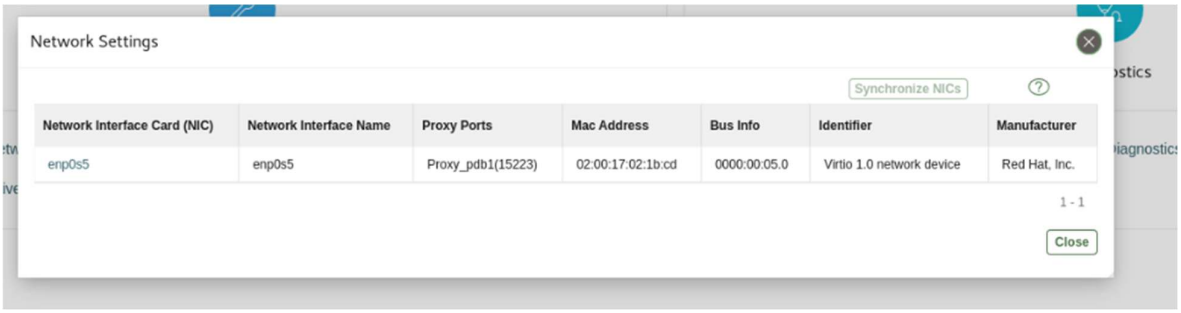


- Cảnh báo đã được tạo và chạy

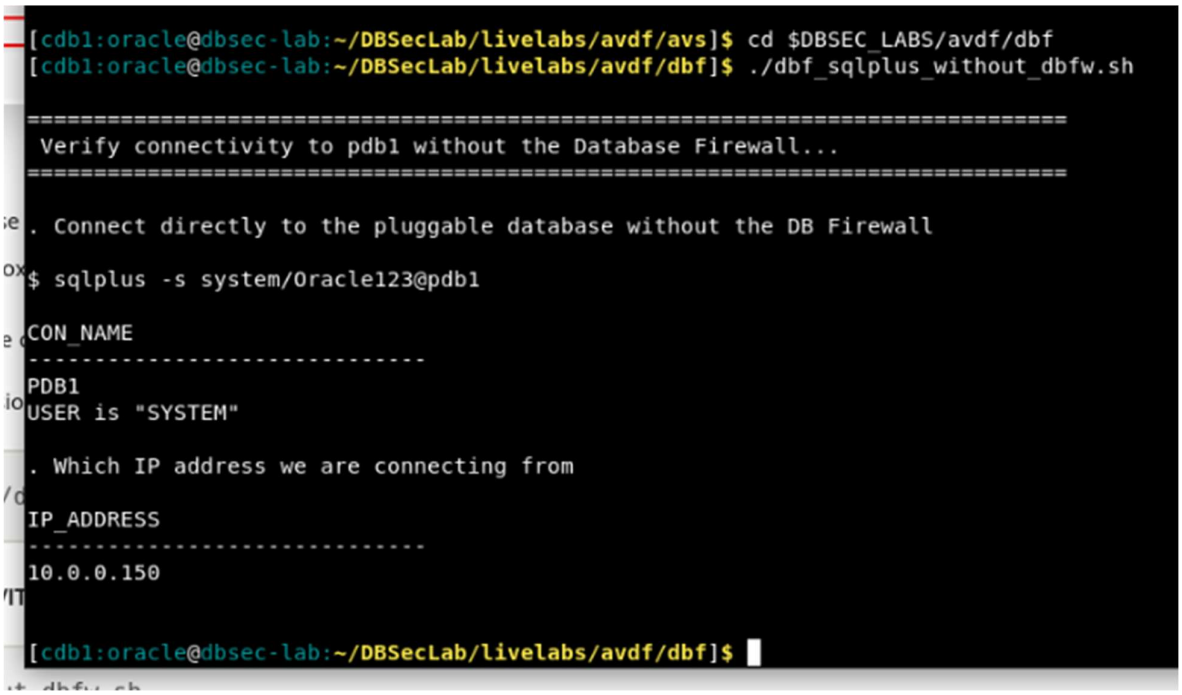
5. Task 5: Protect and Prevent

f. Bật DB Firewall Monitoring

- Đầu tiên, cần đảm bảo rằng Database Firewall phải trong trạng thái đã mở như hình ở trên



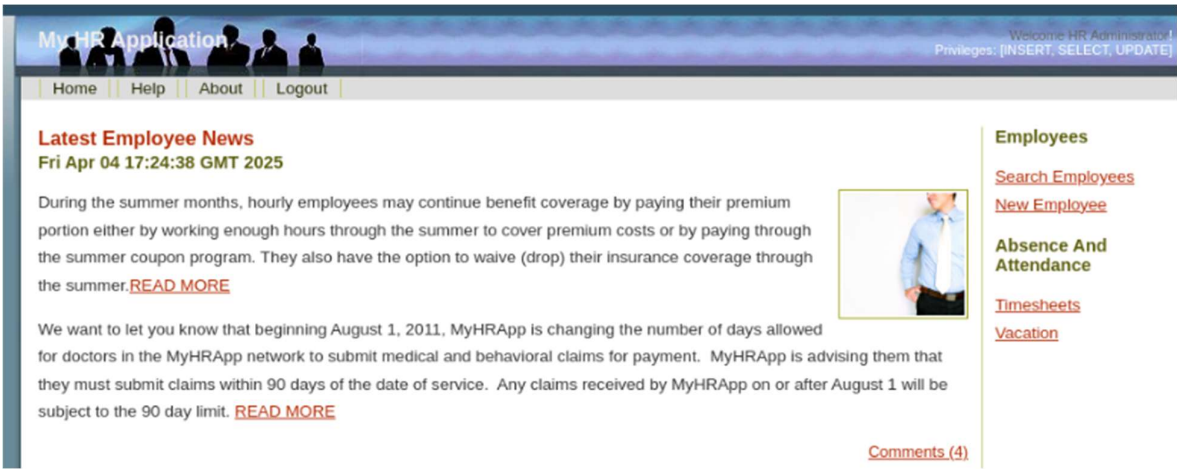
- Tiếp đến, ta sẽ tiến hành kiểm tra Network Settings của Firewall này để đảm bảo proxy ports trong phần Network Settings là 15223 cho pdb1, bởi vì chúng ta sẽ sử dụng những port này cho Database Firewall



- Tiến hành truy cập vào terminal và truy cập vào thư mục DBF, đồng thời tiến hành xác thực kết nối tới pdb1 mà không có Database Firewall. Có thể thấy rằng địa chỉ mà kết nối là từ IP 10.0.0.150, vốn là địa chỉ IP của DBSec-Lab VM

```
[cdb1:oracle@dbsec-lab:~/DBSecLab/livelabs/avdf/dbf]$ ./dbf_sqlplus_with_dbfw.sh

================================================================================
 Verify connectivity to pdb1 with the Database Firewall...
================================================================================

. Connect to the pluggable database through the DB Firewall (proxy)

$ sqlplus -s system/Oracle123@pdb1.proxy

CON_NAME
------------------------------
PDB1
USER is "SYSTEM"

. Which IP address we are connecting from

IP_ADDRESS
------------------------------
10.0.0.152
```

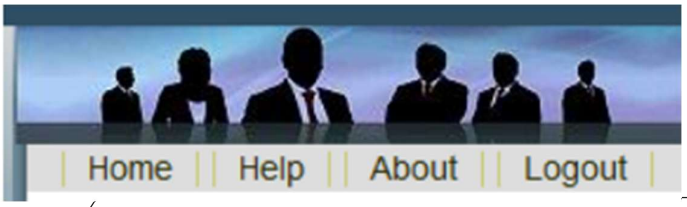
- **DB Firewall - Cấu hình và xác nhận App Glassfish đã sử dụng DB Firewall**
- Ta sẽ tiến hành xác thực lại kết nối khi mà đã có Database Firewall, có thể thấy địa chỉ IP kết nối là từ 10.0.0.152, là địa chỉ IP của DB Firewall VM.



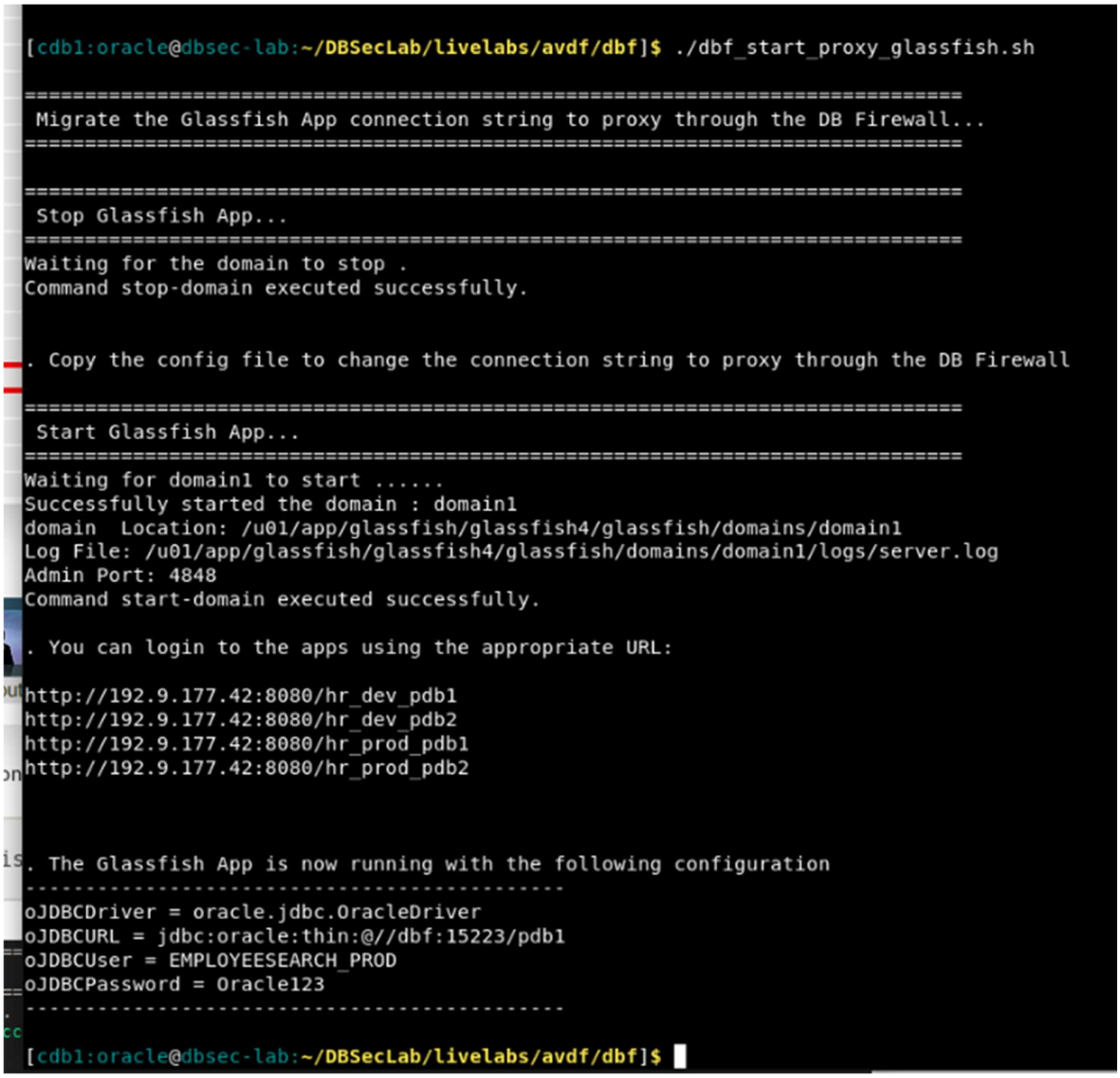
- Tiến hành mở Web Browser tại URL: http://dbsec-lab:8080/hr_prod_pdb1 và đăng nhập với tài khoản và mật khẩu lần lượt là **hradmin** và **Oracle123**

ACTION	
AUDITED_CURSORID	
AUTHENTICATED_IDENTITY	EMPLOYEESEARCH_PROD
AUTHENTICATION_DATA	
AUTHENTICATION_METHOD	PASSWORD
BG_JOB_ID	
CLIENT_IDENTIFIER	hradmin
CLIENT_INFO	SESSION_DATA
CURRENT_BIND	
CURRENT_EDITION_ID	134
CURRENT_EDITION_NAME	ORA$BASE
CURRENT_SCHEMA	EMPLOYEESEARCH_PROD
CURRENT_SCHEMAID	146
CURRENT_SQL	
CURRENT_SQLn	
CURRENT_SQL_LENGTH	
CURRENT_USER	EMPLOYEESEARCH_PROD
CURRENT_USERID	146
DATABASE_ROLE	PRIMARY
DB_DOMAIN	
DB_NAME	PDB1
DB_UNIQUE_NAME	cdb1
DBLINK_INFO	
ENTRYID	
ENTERPRISE_IDENTITY	
FG_JOB_ID	0
GLOBAL_CONTEXT_MEMORY	0
GLOBAL_UID	
HOST	dbsec-lab
IDENTIFICATION_TYPE	LOCAL
INSTANCE	1
INSTANCE_NAME	cdb1
IP_ADDRESS	10.0.0.150
ISDBA	FALSE
LANG	US
LANGUAGE	AMERICAN_AMERICA.AL32UTF8
MODULE	JDBC Thin Client
NETWORK_PROTOCOL	tcp
NLS_CALENDAR	GREGORIAN
NLS_CURRENCY	$
NLS_DATE_FORMAT	DD-MON-RR
NLS_DATE_LANGUAGE	AMERICAN
NLS_SORT	BINARY
NLS_TERRITORY	AMERICA
OS_USER	oracle
POLICY_INVOKER	
PROXY_ENTERPRISE_IDENTITY	

- Ta có thể thấy được trong ở mục địa chỉ IP Address là địa chỉ IP của DBSec-Lab VM đã thiết lập trước đó. Các thông tin trên được lấy từ **userenv** bằng cách thực thi hàm **SYS_CONTEXT**



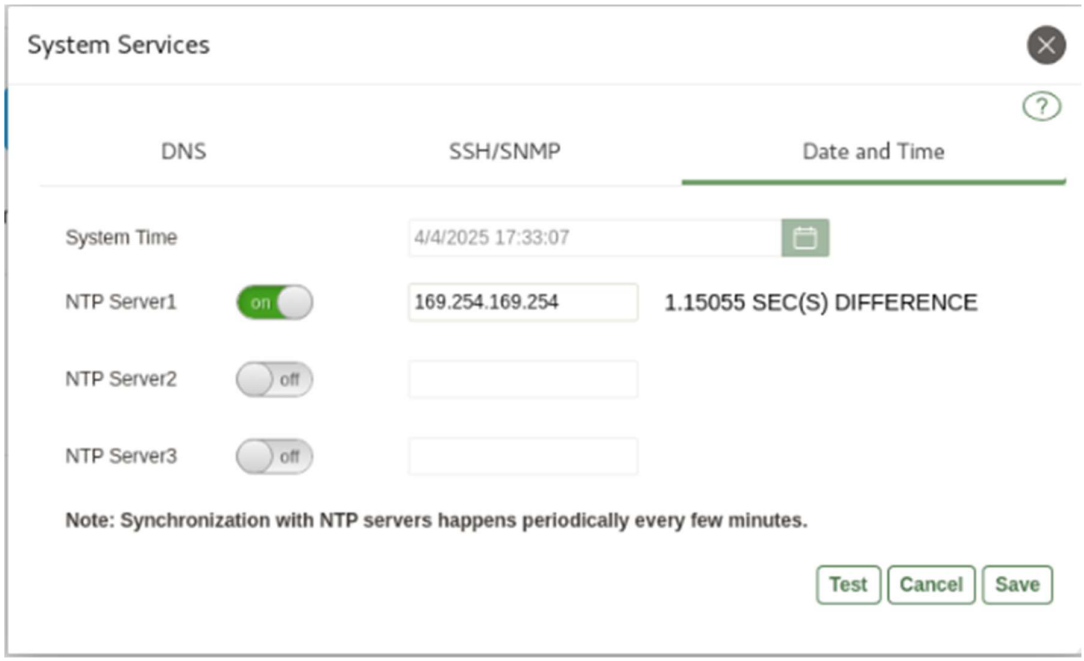
- Bây giờ ta sẽ tiến hành đăng xuất



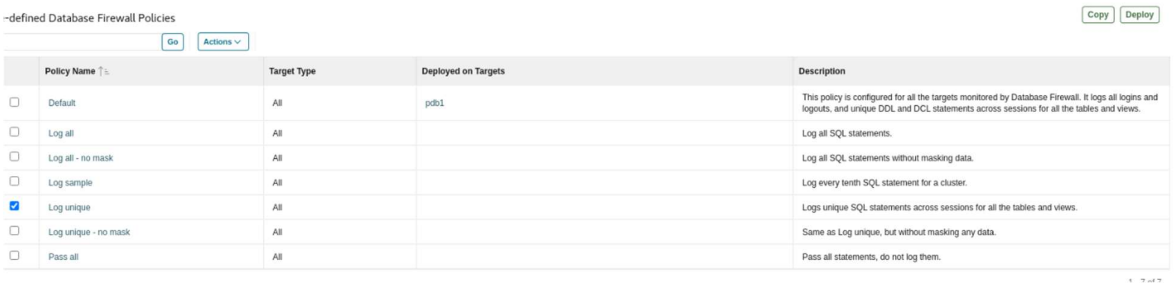
- Bây giờ, tiến hành quay trở lại terminal và chạy script dbf_start_proxy_glassfish.sh để tiến hành proxy kết nối của Glassfish Application thông qua Database Firewall.

BG_JOB_ID	
CLIENT_IDENTIFIER	hradmin
CLIENT_INFO	SESSION_DATA
CURRENT_BIND	
CURRENT_EDITION_ID	134
CURRENT_EDITION_NAME	ORA$BASE
CURRENT_SCHEMA	EMPLOYEESEARCH_PROD
CURRENT_SCHEMAID	146
CURRENT_SQL	
CURRENT_SQLn	
CURRENT_SQL_LENGTH	
CURRENT_USER	EMPLOYEESEARCH_PROD
CURRENT_USERID	146
DATABASE_ROLE	PRIMARY
DB_DOMAIN	
DB_NAME	PDB1
DB_UNIQUE_NAME	cdb1
DBLINK_INFO	
ENTRYID	
ENTERPRISE_IDENTITY	
FG_JOB_ID	0
GLOBAL_CONTEXT_MEMORY	0
GLOBAL_UID	
HOST	dbsec-lab
IDENTIFICATION_TYPE	LOCAL
INSTANCE	1
INSTANCE_NAME	cdb1
IP_ADDRESS	10.0.0.152
ISDBA	FALSE
LANG	US
LANGUAGE	AMERICAN_AMERICA.AL32UTF8
MODULE	JDBC Thin Client
NETWORK_PROTOCOL	tcp
NLS_CALENDAR	GREGORIAN

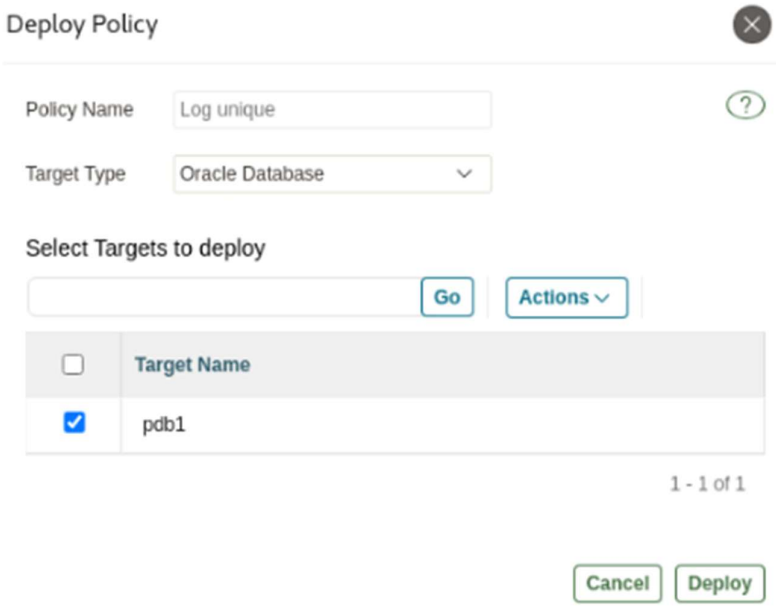
- Tiến hành đăng nhập lại thì trang Web ở trên thấy được ở trang Session Details, tại dòng IP Address đã thay đổi từ 10.0.0.150 sang 10.0.0.152, vốn là địa chỉ của Database Firewall VM.
- **DB Firewall - Huấn luyện DB Firewall đối với các SQL Traffic biết trước**



- Tiếp đến ta sẽ tiến hành cấu hình cần thiết cho việc huấn luyện DB Firewall chống được SQL Traffic
- Đầu tiên, ta sẽ tiến hành truy cập vào trong DB Firewall, dưới **Configuration** chọn **System Service**, chọn vào **Date and Time** và bật **NTP Server1** với IP là 169.254.169.254



- Ta sẽ tiến hành thiết lập Policies cho DB Firewall bằng cách chọn **Policies**, rồi chọn **Database Firewall Polices**, tích vào **Log Unique** và chọn **Deploy**

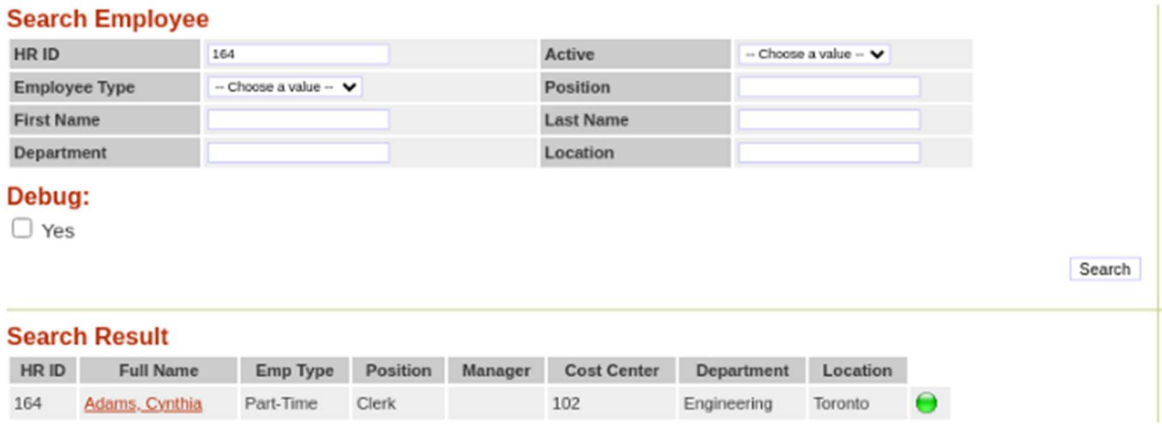


- Chọn **Target Name** là pdb1 và chọn **Deploy**

	Policy Name	Target Type	Deployed on Targets	Description
☐	Default	All		This policy is configured for all the targets monitored by Database Firewall. It logs all logins and logouts, and unique DDL and DCL statements across sessions for all the tables and views.
☐	Log all	All		Log all SQL statements.
☐	Log all - no mask	All		Log all SQL statements without masking data.
☐	Log sample	All		Log every tenth SQL statement for a cluster.
☐	Log unique	All	pdb1	Logs unique SQL statements across sessions for all the tables and views.
☐	Log unique - no mask	All		Same as Log unique, but without masking any data.
☐	Pass all	All		Pass all statements, do not log them.

- Tiến hành refresh lại trang và thấy được Log unique policy đã được cập nhật cho pdb1

- Tiến hành đăng xuất và đăng nhập lại với tài khoản và mật khẩu lần lượt là **hradmin** và **Oracle123**, chọn **Search Employees** và tiến hành truy xuất **HR ID** là 164 và chọn **Search**



Search Employee

HR ID	164	Active	-- Choose a value --
Employee Type	-- Choose a value --	Position	
First Name		Last Name	
Department		Location	

Debug:

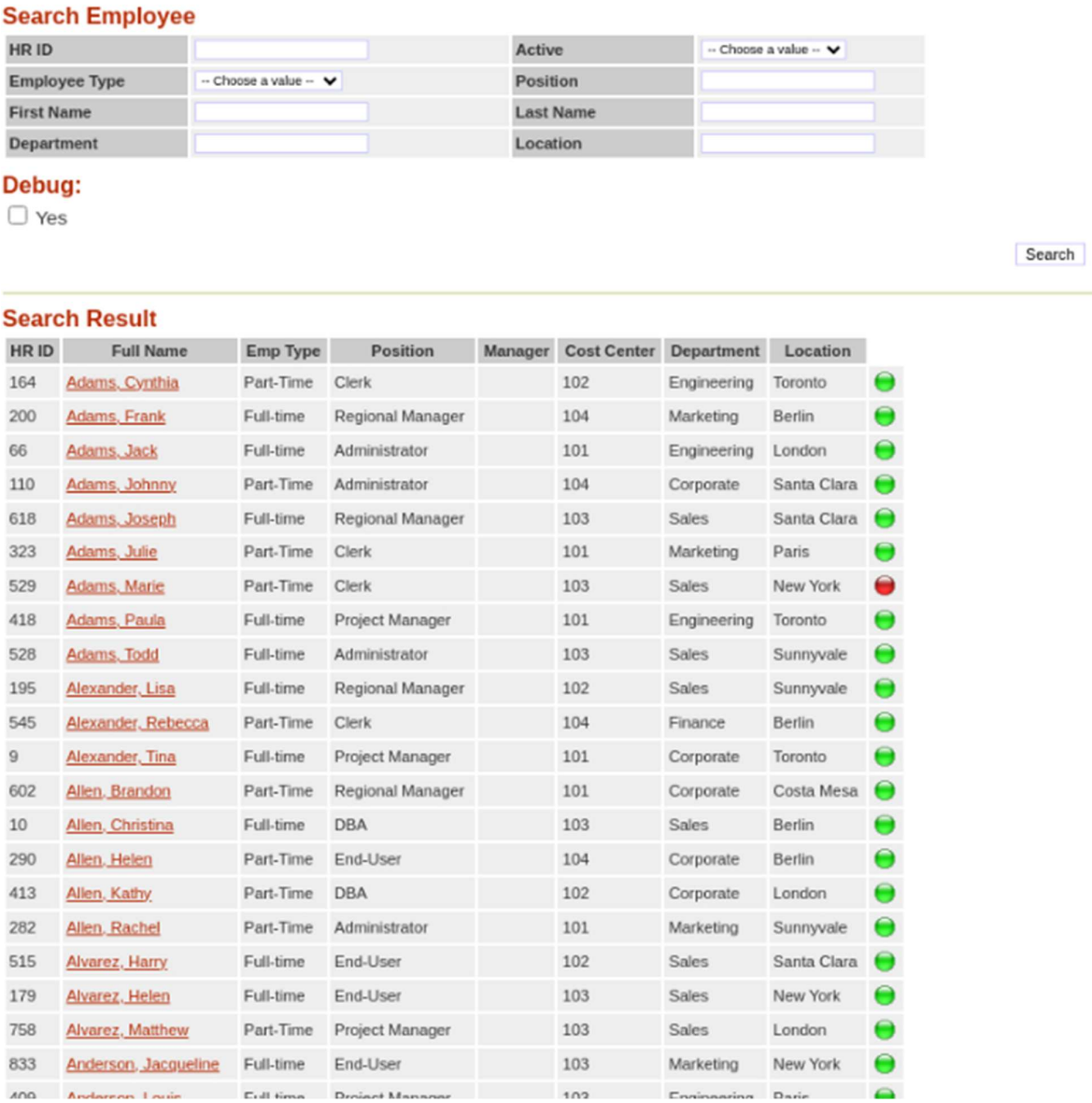
Yes

Search

Search Result

HR ID	Full Name	Emp Type	Position	Manager	Cost Center	Department	Location
164	Adams, Cynthia	Part-Time	Clerk		102	Engineering	Toronto

- Ta được kết quả như hình trên với truy vấn **HR ID** là **164**



Search Employee

HR ID		Active	-- Choose a value --
Employee Type	-- Choose a value --	Position	
First Name		Last Name	
Department		Location	

Debug:

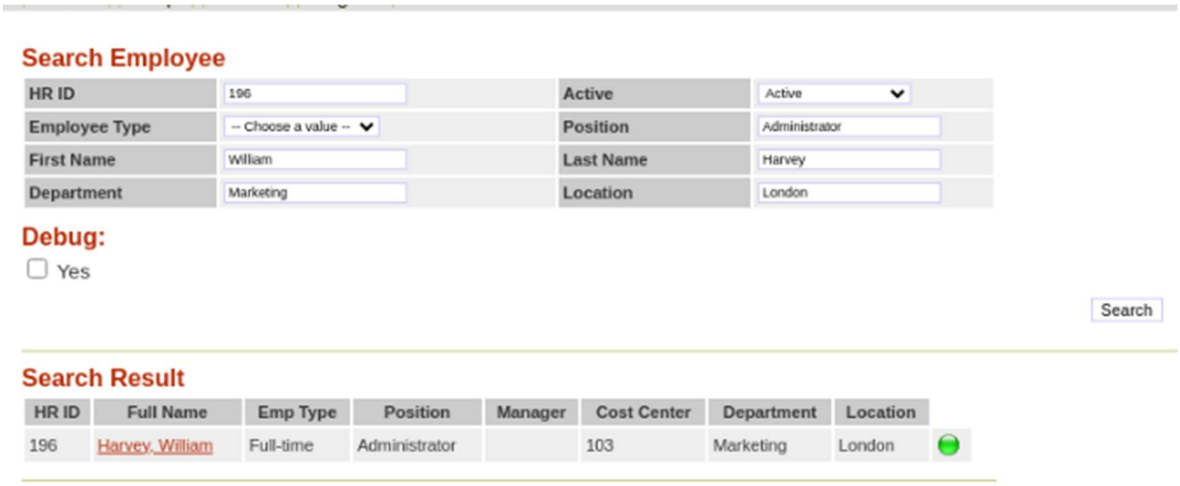
Yes

Search

Search Result

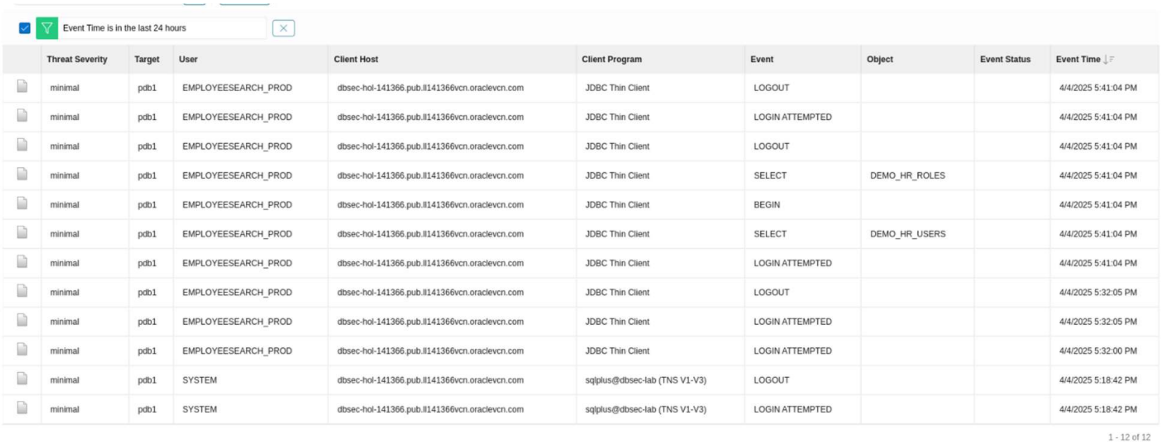
HR ID	Full Name	Emp Type	Position	Manager	Cost Center	Department	Location
164	Adams, Cynthia	Part-Time	Clerk		102	Engineering	Toronto
200	Adams, Frank	Full-time	Regional Manager		104	Marketing	Berlin
66	Adams, Jack	Full-time	Administrator		101	Engineering	London
110	Adams, Johnny	Part-Time	Administrator		104	Corporate	Santa Clara
618	Adams, Joseph	Full-time	Regional Manager		103	Sales	Santa Clara
323	Adams, Julie	Part-Time	Clerk		101	Marketing	Paris
529	Adams, Marie	Part-Time	Clerk		103	Sales	New York
418	Adams, Paula	Full-time	Project Manager		101	Engineering	Toronto
528	Adams, Todd	Full-time	Administrator		103	Sales	Sunnyvale
195	Alexander, Lisa	Full-time	Regional Manager		102	Sales	Sunnyvale
545	Alexander, Rebecca	Part-Time	Clerk		104	Finance	Berlin
9	Alexander, Tina	Full-time	Project Manager		101	Corporate	Toronto
602	Allen, Brandon	Part-Time	Regional Manager		101	Corporate	Costa Mesa
10	Allen, Christina	Full-time	DBA		103	Sales	Berlin
290	Allen, Helen	Part-Time	End-User		104	Corporate	Berlin
413	Allen, Kathy	Part-Time	DBA		102	Corporate	London
282	Allen, Rachel	Part-Time	Administrator		101	Marketing	Sunnyvale
515	Alvarez, Harry	Full-time	End-User		102	Sales	Santa Clara
179	Alvarez, Helen	Full-time	End-User		103	Sales	New York
758	Alvarez, Matthew	Part-Time	Project Manager		103	Sales	London
833	Anderson, Jacqueline	Full-time	End-User		103	Marketing	New York

- Tiến hành xóa giá trị trường **HR ID** và chọn **Search** lại sẽ được kết quả như hình trên.

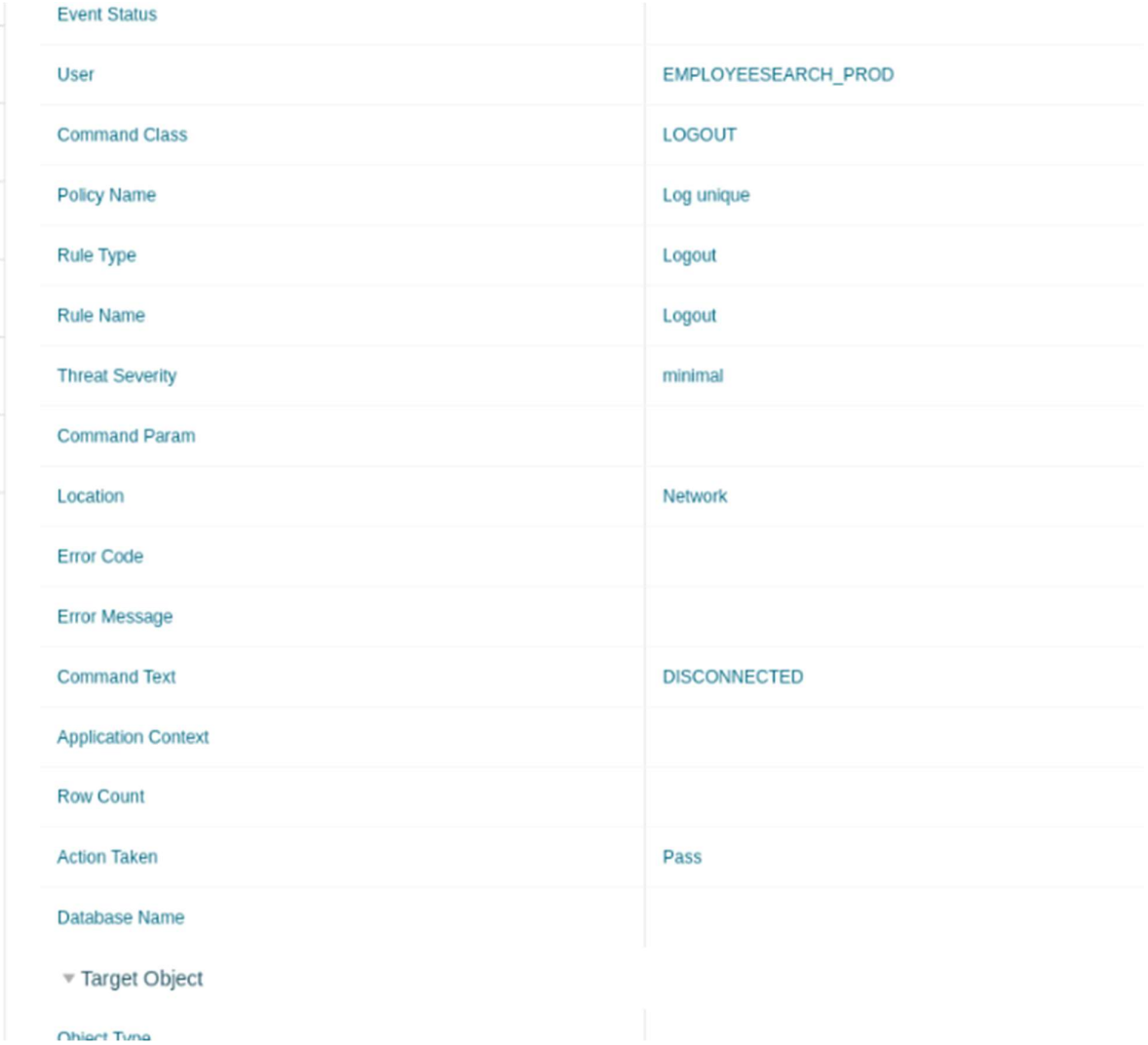


- Tiến hành truy xuất với các giá trị lần lượt như sau và bấm **Search**:
  - **HR ID: 196**
  - **Active: Active**
  - **Employee Type: Full-Time Employee**
  - **Position: Administrator**
  - **First Name: William**
  - **Last Name: Harvey**
  - **Department: Marketing**
  - **City: London**

- Tiến hành click vào **"Harvey, William"** để xem chi tiết thông tin của người nhân viên này.

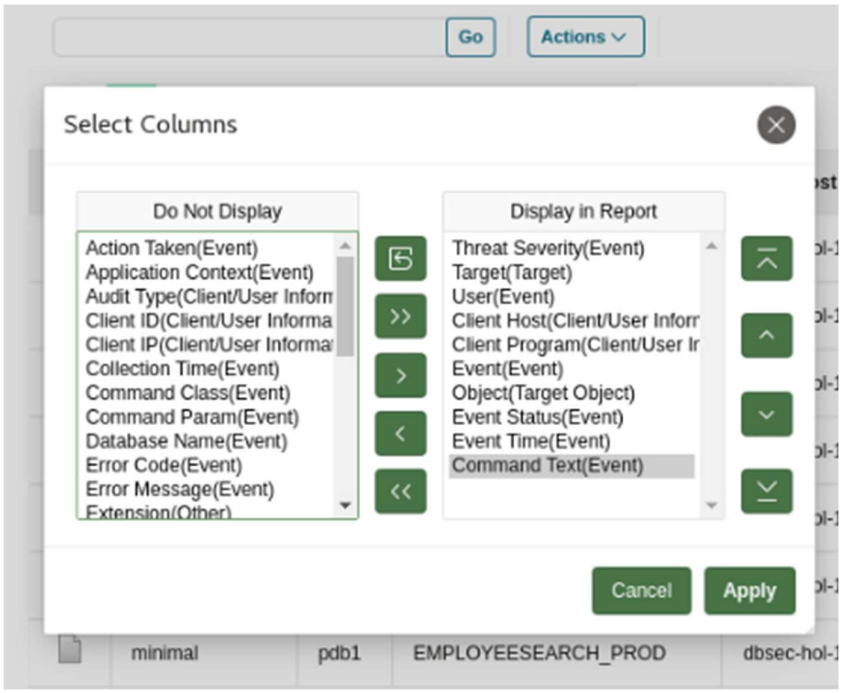


- Tiến hành kiểm tra Database Firewall Activity bằng cách chọn **Reports**, kéo xuống mục **Database Firewall Reports**, chọn mục **Monitored Activity** và có thể thấy các hoạt động truy vấn với User EMPLOYEESEARCH_PROD với Client Program là "JDBC Thin Client"



Event Status	
User	EMPLOYEESEARCH_PROD
Command Class	LOGOUT
Policy Name	Log unique
Rule Type	Logout
Rule Name	Logout
Threat Severity	minimal
Command Param	
Location	Network
Error Code	
Error Message	
Command Text	DISCONNECTED
Application Context	
Row Count	
Action Taken	Pass
Database Name	
▼ Target Object	
Object Type	

- Chọn vào chi tiết của các câu truy vấn và để ý các thông tin trong mục **Event**:
    - Policy Name: Log unique
    - Threat Severity: minimal
    - Location: Network
    - Action Taken: Pass



- Để có cái nhìn trực quan hơn về các report này, ta sẽ thêm cột **SQL Text** bằng cách chọn **Actions**, sau đó chọn **Select Columns**, sau đó thêm **Add Command Text(Event)** vào trong vùng **Display in Report**, then chọn **Apply**

	Threat Severity	Target	User	Client Host	Client Program	Event	Object	Event Status	Event Time	Command Text
	minimal	pdb1	EMPLOYEESEARCH_PROD	dbsec-hol-141366.pub.ll141366vcn.oraclevcn.com	JDBC Thin Client	SELECT	DEMO_HR_EMPLOYEES		4/4/2025 5:46:37 PM	select a.USERID, a.FIRSTNAME, a.LASTNAME, a.EMAIL, a.PHONEMOBILE, a.PHONEFIX, a.PHONEFAX, a.COSTCENTER, a.EMPTYPE, a.POSITION, a.CITY, a.SALARY, a.ISMANAGER, a.MANAGERID, a.DEPARTMENT, a.ORGANIZATION, a.STARTDATE, a.ENDDATE, a.ACTIVE, b.FIRSTNAME as MGR_FIRSTNAME, b.LASTNAME as MGR_LASTNAME, b.USERID as MGR_USERID from DEMO_HR_EMPLOYEES a left outer join DEMO_HR_EMPLOYEES b on a.MANAGERID = b.USERID where a.MANAGERID = 000 order by a.LASTNAME, a.FIRSTNAME
	minimal	pdb1	EMPLOYEESEARCH_PROD	dbsec-hol-141366.pub.ll141366vcn.oraclevcn.com	JDBC Thin Client	LOGIN ATTEMPTED			4/4/2025 5:46:37 PM	LOGIN
	minimal	pdb1	EMPLOYEESEARCH_PROD	dbsec-hol-141366.pub.ll141366vcn.oraclevcn.com	JDBC Thin Client	SELECT	DEMO_HR_EMPLOYEES		4/4/2025 5:46:37 PM	select a.USERID, a.FIRSTNAME, a.LASTNAME, a.EMAIL, a.PHONEMOBILE, a.PHONEFIX, a.PHONEFAX, a.SSN, a.SIN, A.NINO, a.DOB, a.ADDRESS_1, a.ADDRESS_2, a.STATE, a.COUNTRY, a.POSTAL_CODE, a.EMPTYPE, a.POSITION, a.CITY, a.SALARY, a.ISMANAGER, a.MANAGERID, a.DEPARTMENT, a.ORGANIZATION, a.STARTDATE, a.ENDDATE, a.ACTIVE, a.COSTCENTER, a.ISHEADOFDEPARTMENT, b.FIRSTNAME as MGR_FIRSTNAME, b.LASTNAME as MGR_LASTNAME, b.USERID as MGR_USERID, a.CORPORATE_CARD, a.CC_PIN, a.CC_EXPIRE, c.MEMBER_ID, c.LAST_INS_CLAIM, c.BONUS_AMOUNT, c.PAYMENT_ACCT_NO, c.ROUTING_NUMBER from DEMO_HR_EMPLOYEES a left outer join DEMO_HR_EMPLOYEES b on a.MANAGERID = b.USERID left outer join DEMO_HR_SUPPLEMENTAL_DATA c on a.USERID = c.USERID where a.USERID = 000

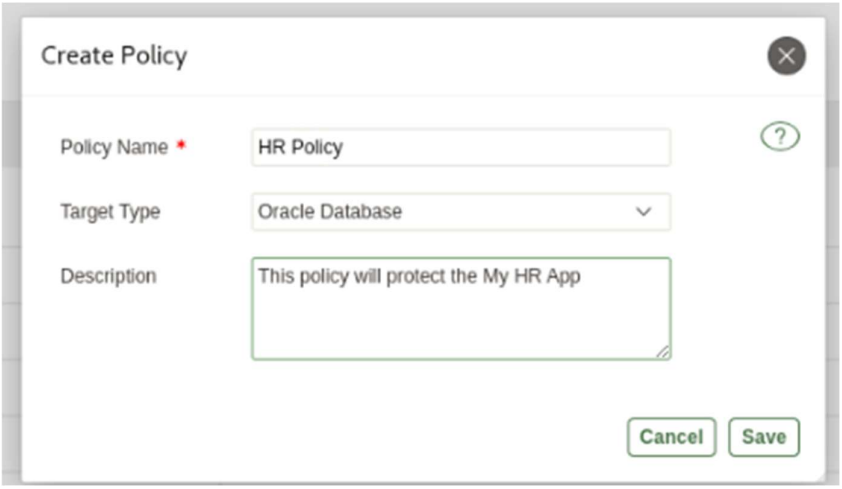
- Sau khi thiết lập thành công, sẽ hình thành cột chứa câu lệnh SQL truy vấn tương ứng

	minimal	pdb1	EMPLOYEESEARCH_PROD	dbsec-hol-141366.pub.ll141366vcn.oraclevcn.com	JDBC Thin Client	SELECT	DEMO_HR_USERS	4/4/2025 5:41:04 PM	select USERID,FIRSTNAME,LASTNAME from DEMO_HR_USERS where (USERSTATUS is NULL or upper(USERSTATUS) = '######') and upper(USERID) = '#######' and password = '#########'

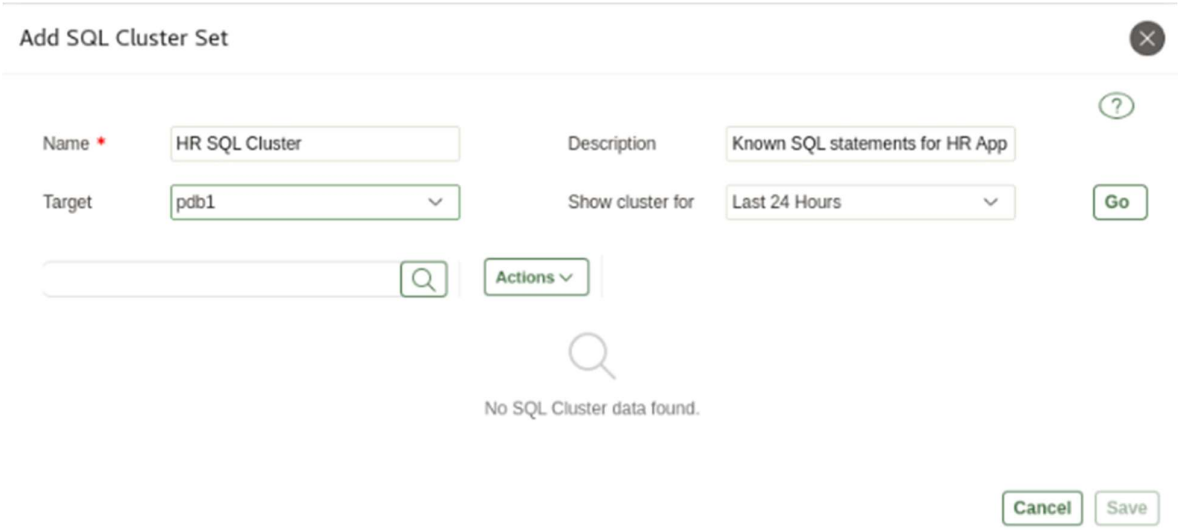
- Trên đây là một ví dụ của câu lệnh truy vấn trong **EMPLOYEESEARCH_PROD**: select USERID,FIRSTNAME,LASTNAME from DEMO_HR_USERS where (USERSTATUS is NULL or upper(USERSTATUS) = '######') and upper(USERID) = '#######' and password = '#########'
- **DB Firewall - Xây dựng và kiểm thử chính sách danh sách cho phép của DB Firewall**

```
[cdb1:oracle@dbsec-lab:~/DBSecLab/livelabs/avdf/dbf]$ ./dbf_query_fw_policy.sh

================================================================================
 Demonstrate connectivity through the DB Firewall and the ability to query
 the EMPLOYEESEARCH_PROD tables...
================================================================================

. Connect to the pluggable database through the DB Firewall (proxy)

$ sqlplus -s system/Oracle123@pdb1.proxy
USER is "EMPLOYEESEARCH_PROD"

. Query EMPLOYEESEARCH_PROD.DEMO_HR_EMPLOYEES

    USERID FIRSTNAME  LASTNAME   EMPTYPE   POSITION         CITY        SSN         SIN         NINO
---------- ---------- ---------- --------- ---------------- ----------- ----------- ----------- -------
        37 Heather    Wells      Part-Time End-User         Berlin      710-72-4053
        38 Jesse      Nguyen     Full-time DBA              Toronto                 522-254-799
        39 Albert     Gardner    Full-time District Manager Paris       665-21-8075
        40 Martha     Butler     Full-time Administrator    Berlin      751-47-6482
        41 Jose       Harrison   Part-Time Project Manager  Santa Clara 625-88-4997
        42 Lawrence   Daniels    Part-Time End-User         London      780-40-2910
        43 Eric       Thomas     Full-time Clerk            Berlin      936-90-1676
        44 Jeremy     Mitchell   Full-time Clerk            Toronto                 885-532-397
        45 Diane      Kim        Part-Time Regional Manager London      495-72-6178

9 rows selected.


[cdb1:oracle@dbsec-lab:~/DBSecLab/livelabs/avdf/dbf]$
[cdb1:oracle@dbsec-lab:~/DBSecLab/livelabs/avdf/dbf]$
```

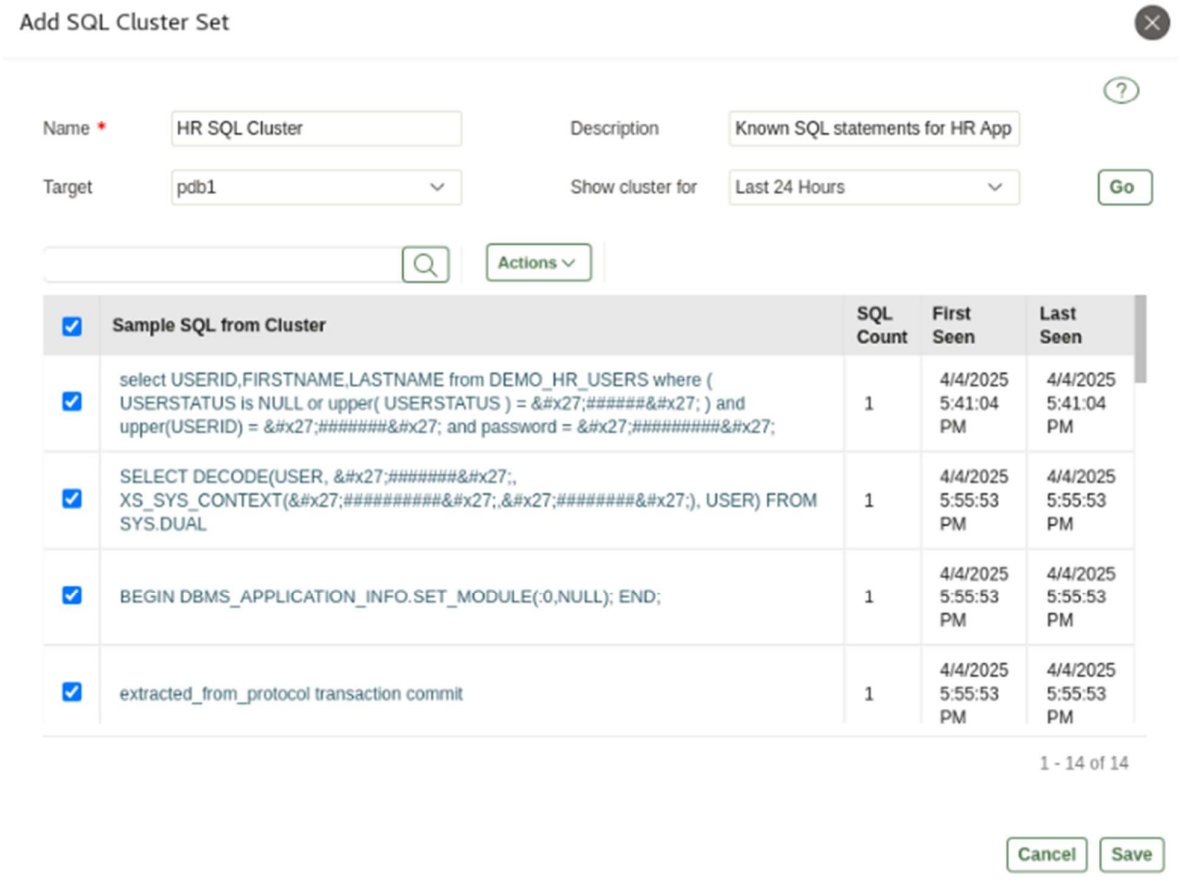
- Tiến hành thiết lập lại kết nối với Database Firewall và truy vấn bảng **EMPLOYEESEARCH_PROD** trước khi áp dụng các chính sách của DB Firewall



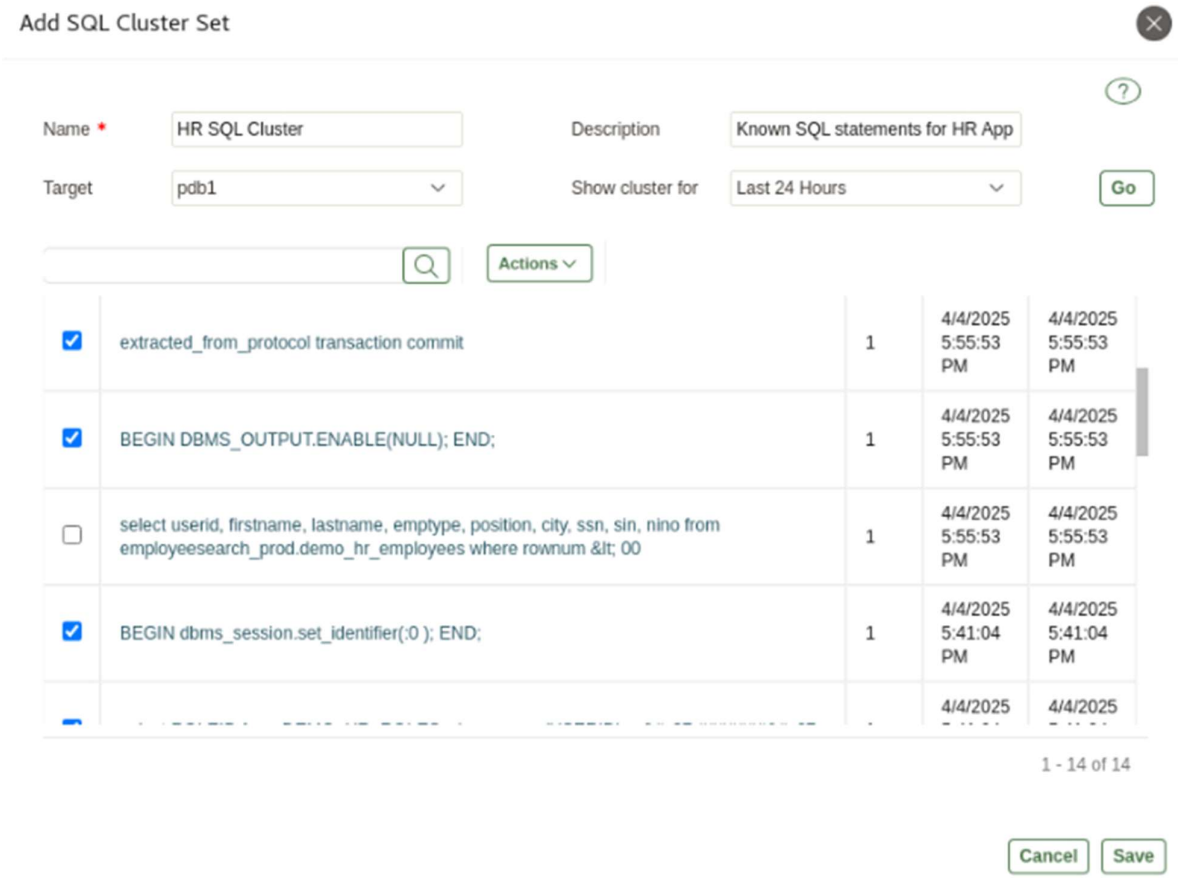
- Tiến hành tạo Policy mới mới với các thông tin nhập vào lần lượt và click **Save**:
  - Policy Name: HR Policy
  - Target Type: Oracle Database
  - Description: This policy will protect the My HR App



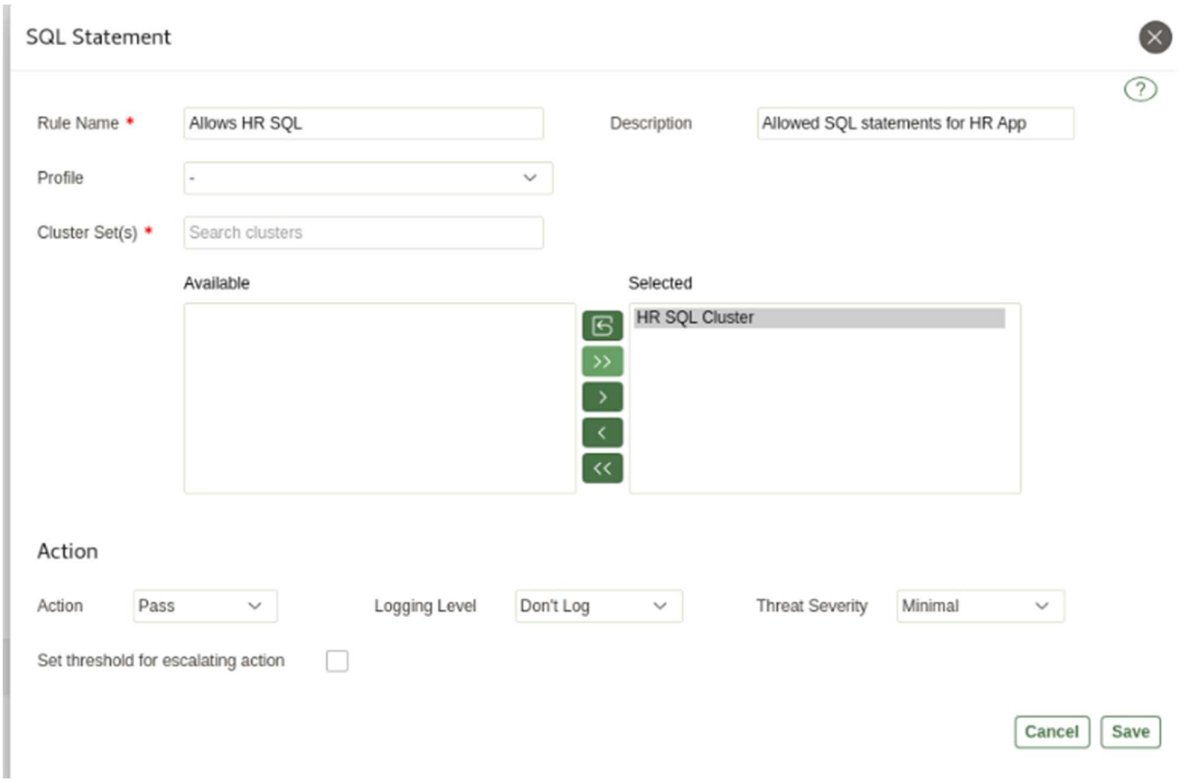
- Tiến hành tạo mới một SQL Cluster Set với các thông tin lần lượt và sau đó chọn **Go**:
  - Name: HR SQL Cluster
  - Description: Known SQL statements for HR App
  - Target: pdb1
  - Show cluster for: Last 24 Hours



- Hình trên kết quả trả về sau khi vừa thực hiện tạo mới một SQL Cluster Set

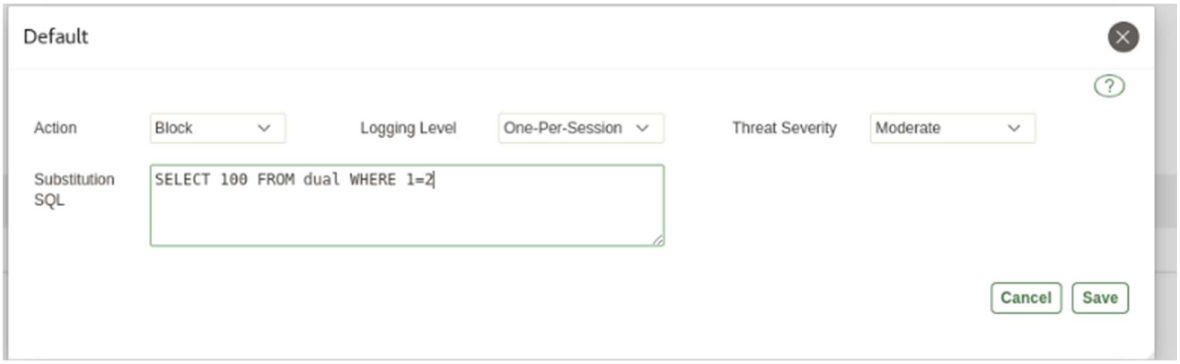


- Chọn box **Select all** nằm kế Header của "Cluster ID" để thêm tất các câu truy vấn đã được huấn luyện vào trong SQL Clusters (trừ dòng thứ 17)

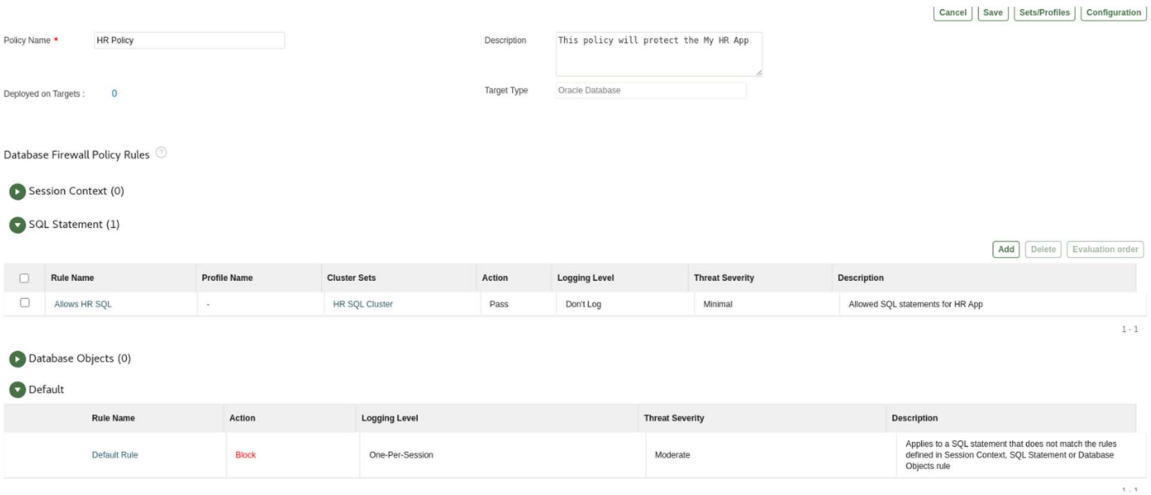


Bài thực hành số 03: Database Security

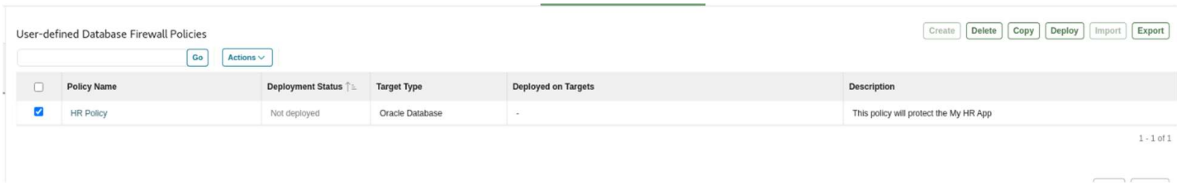
- Tiến hành tạo **SQL Statement** với các thông tin sau để cho phép **HR SQL Cluster** vừa tạo trước đó và lưu lại:
    - Rule Name: Allows HR SQL
    - Description: Allowed SQL statements for HR App
    - Cluster Set(s): HR SQL Cluster
    - Action: Pass
    - Logging Level: Don't Log
    - Threat Severity: Minimal



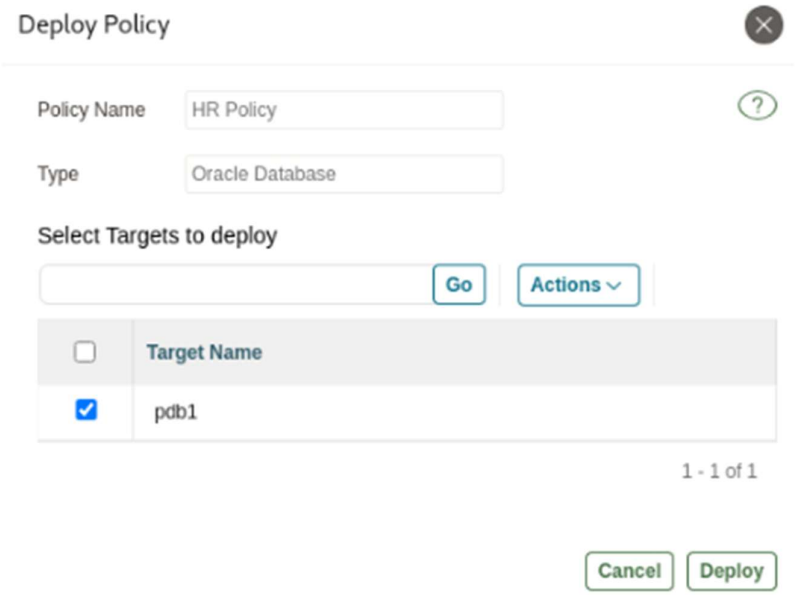
- Tiến hành chọn **Default Rule** và edit lại với các thông tin như sau và lưu lại:
    - Action: Block
    - Logging Level: One-Per-Session
    - Threat Severity: Moderate
    - Substitution SQL: SELECT 100 FROM dual WHERE 1=2



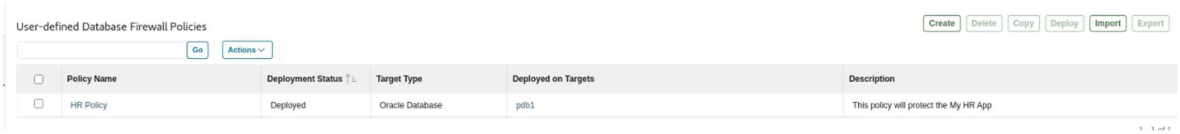
- Hình trên là giao diện của **HR Policy** sau khi cấu hình thành công:



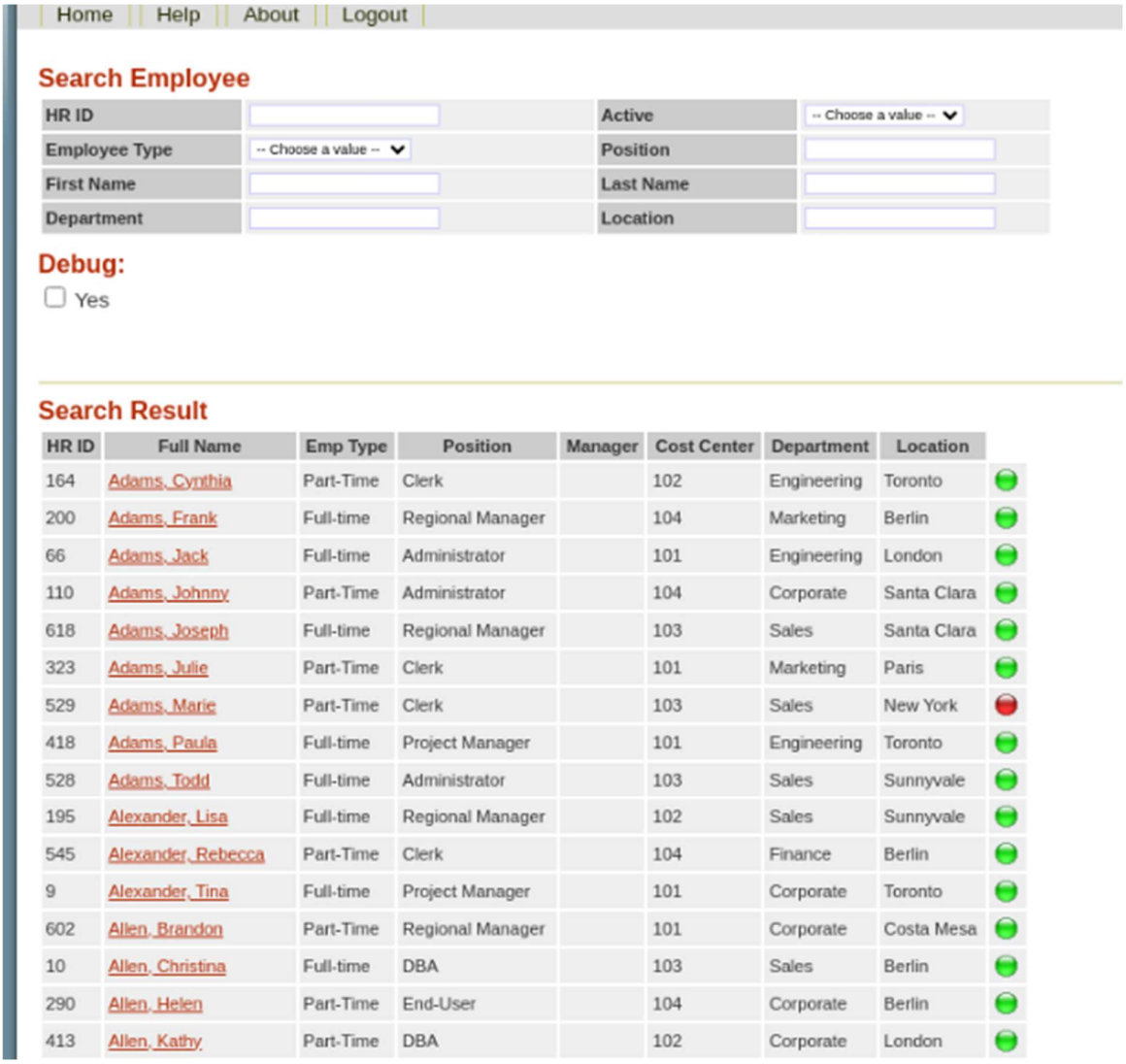
- Hiện giờ khi Policy này chưa được deploy, tiến hành deploy policy này.



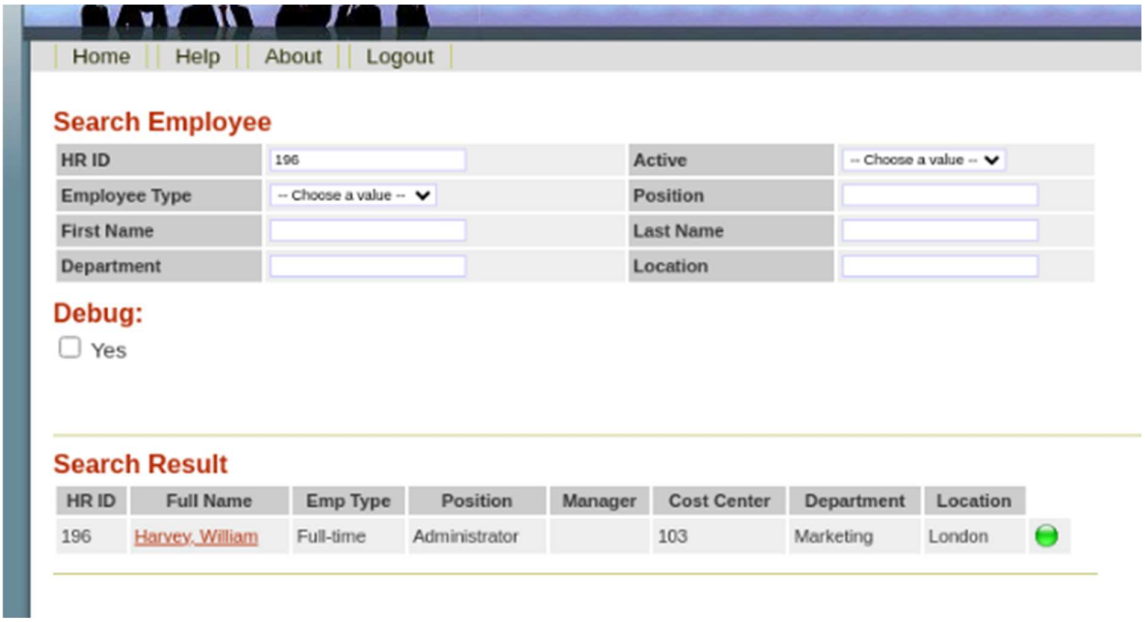
- Tiến hành deploy lên trên pdb1, sau đó tiến hành chọn **Deploy** để triển khai



- Giờ đây thì **HR Policy** đã được triển khai



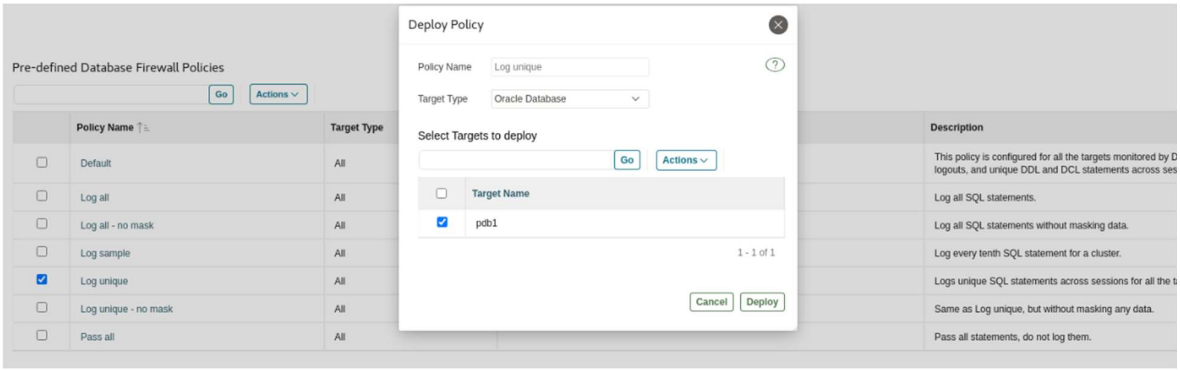
- Tiến hành đăng nhập lại app Glassfish và tiến hành truy xuất nhân viên



- Khi tiến hành truy xuất lại với **HR ID** là 196 thì vẫn truy xuất thành công

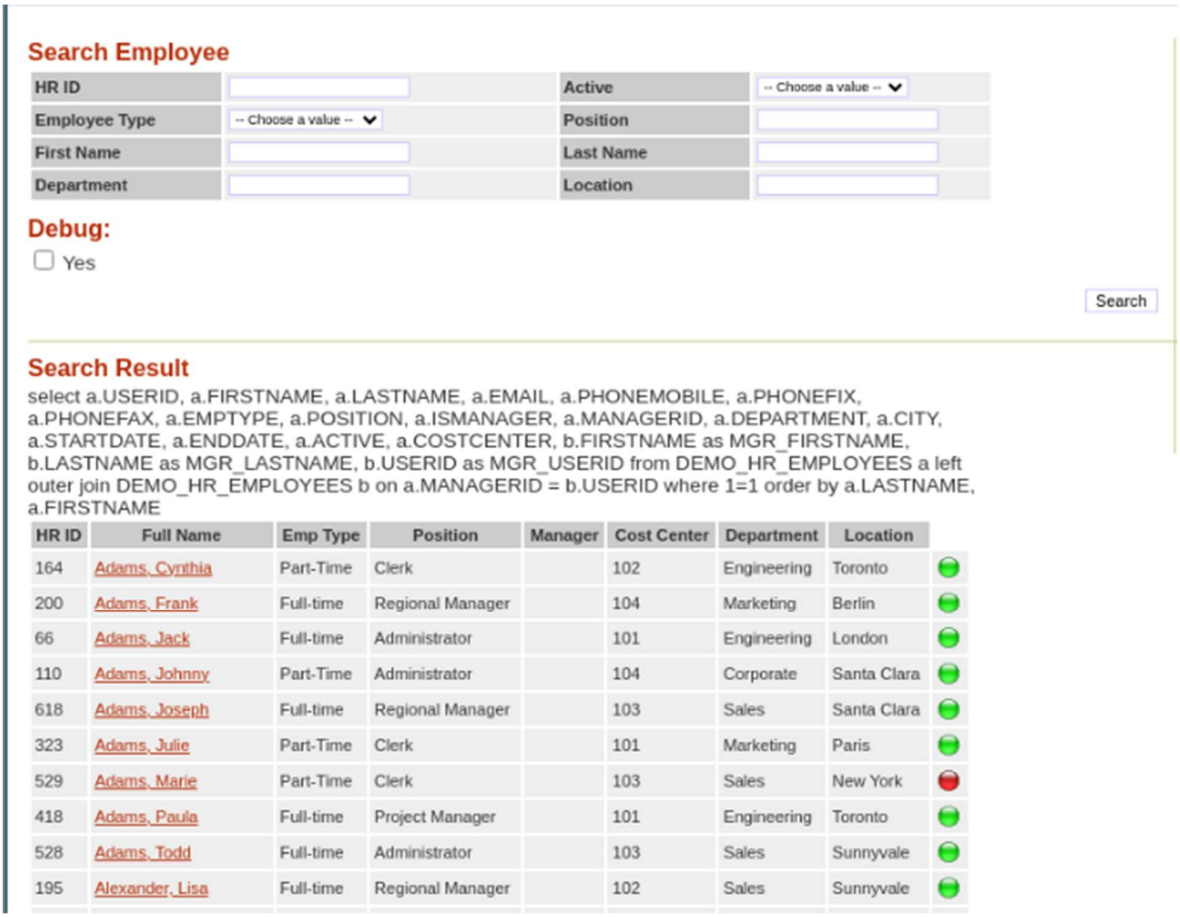
```
[cdb1:oracle@dbsec-lab:~/DBSecLab/livelabs/avdf/dbf]$ ./dbf_query_fw_policy.sh

================================================================================
 Demonstrate connectivity through the DB Firewall and the ability to query
 the EMPLOYEESEARCH_PROD tables...
================================================================================

. Connect to the pluggable database through the DB Firewall (proxy)

$ sqlplus -s system/Oracle123@pdb1.proxy
USER is "EMPLOYEESEARCH_PROD"

. Query EMPLOYEESEARCH_PROD.DEMO_HR_EMPLOYEES

no rows selected


[cdb1:oracle@dbsec-lab:~/DBSecLab/livelabs/avdf/dbf]$
```

- Quay lại terminal, chạy script dbf_query_fw_policy.sh để áp dụng chính sách của DB Firewall thì truy xuất không được
- **DB Firewall - Ngăn chặn SQL Injection Attack**



- Tiến hành triển khai policy **Log unique** trên **pdb1** và lưu lại

- Refresh lại trang thì thấy **Log unique** đã được deploy trên **pdb1**



Search Employee

HR ID		Active	-- Choose a value --
Employee Type	-- Choose a value --	Position	
First Name		Last Name	
Department		Location	

Debug:

Yes

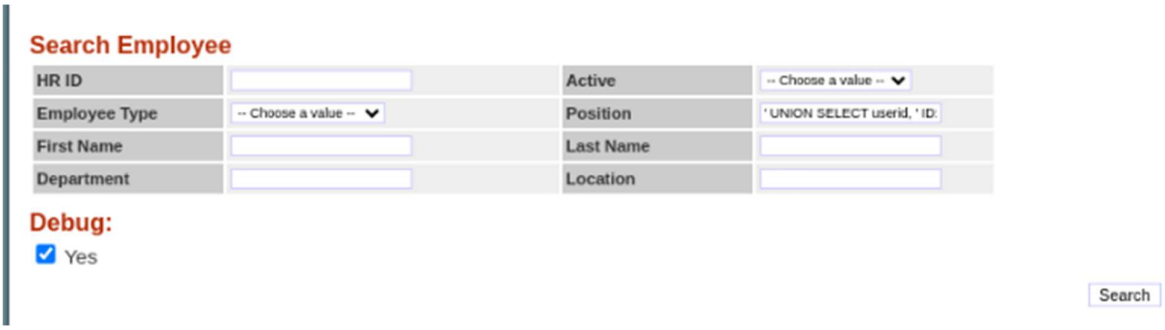
Search

Search Result

select a.USERID, a.FIRSTNAME, a.LASTNAME, a.EMAIL, a.PHONEMOBILE, a.PHONEFIX, a.PHONEFAX, a.EMPTYPE, a.POSITION, a.ISMANAGER, a.MANAGERID, a.DEPARTMENT, a.CITY, a.STARTDATE, a.ENDDATE, a.ACTIVE, a.COSTCENTER, b.FIRSTNAME as MGR_FIRSTNAME, b.LASTNAME as MGR_LASTNAME, b.USERID as MGR_USERID from DEMO_HR_EMPLOYEES a left outer join DEMO_HR_EMPLOYEES b on a.MANAGERID = b.USERID where 1=1 order by a.LASTNAME, a.FIRSTNAME

HR ID	Full Name	Emp Type	Position	Manager	Cost Center	Department	Location
164	Adams, Cynthia	Part-Time	Clerk		102	Engineering	Toronto
200	Adams, Frank	Full-time	Regional Manager		104	Marketing	Berlin
66	Adams, Jack	Full-time	Administrator		101	Engineering	London
110	Adams, Johnny	Part-Time	Administrator		104	Corporate	Santa Clara
618	Adams, Joseph	Full-time	Regional Manager		103	Sales	Santa Clara
323	Adams, Julie	Part-Time	Clerk		101	Marketing	Paris
529	Adams, Marie	Part-Time	Clerk		103	Sales	New York
418	Adams, Paula	Full-time	Project Manager		101	Engineering	Toronto
528	Adams, Todd	Full-time	Administrator		103	Sales	Sunnyvale
195	Alexander, Lisa	Full-time	Regional Manager		102	Sales	Sunnyvale

- Tiến hành đăng nhập lại app Glassfish và truy xuất thông tin nhân viên, vẫn truy xuất được vì vẫn còn cho phép truy xuất mọi thứ



Search Employee

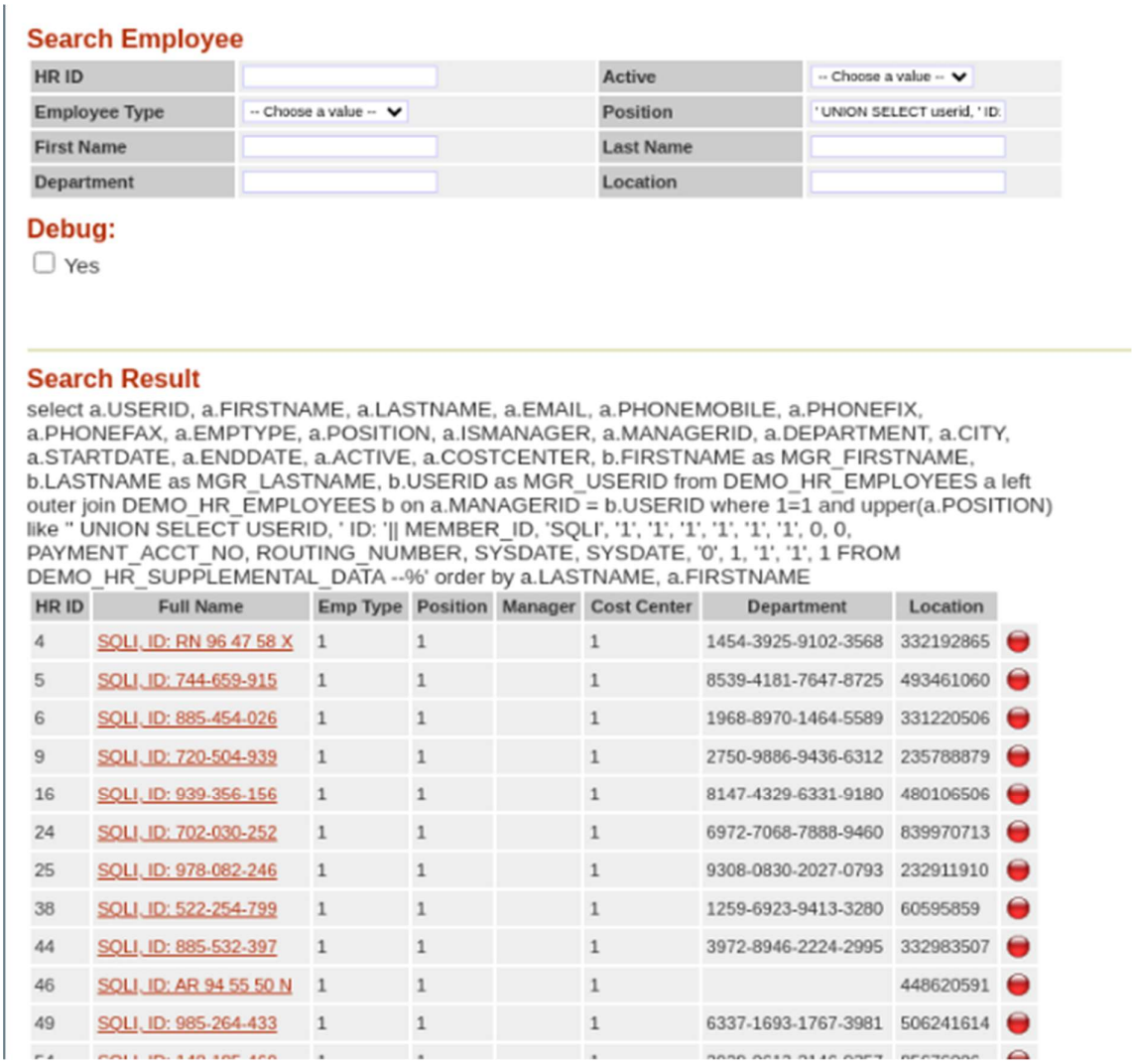
HR ID		Active	-- Choose a value --
Employee Type	-- Choose a value --	Position	' UNION SELECT userid, ' ID:
First Name		Last Name	
Department		Location	

Debug:

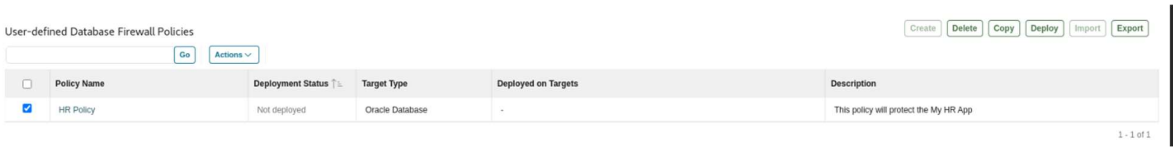
Yes

Search

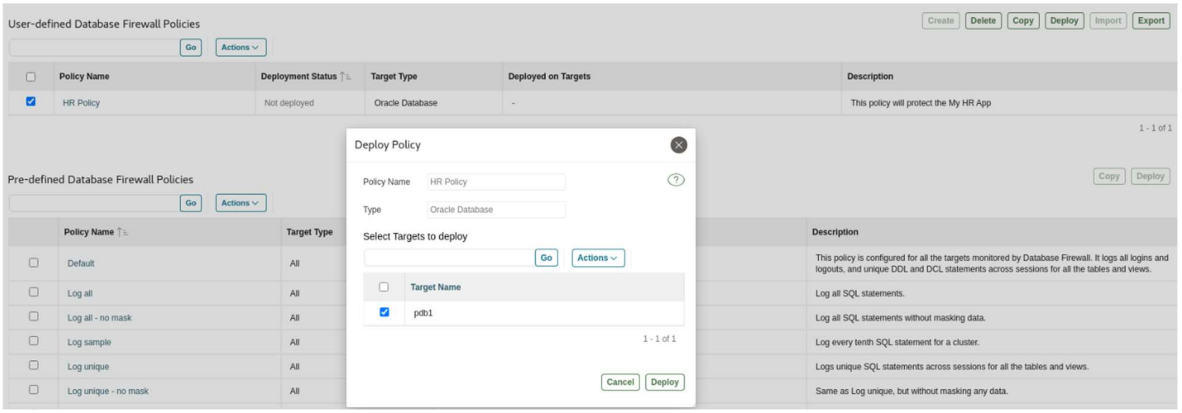
- Tiến hành bật debug để xem câu truy vấn sau của form này



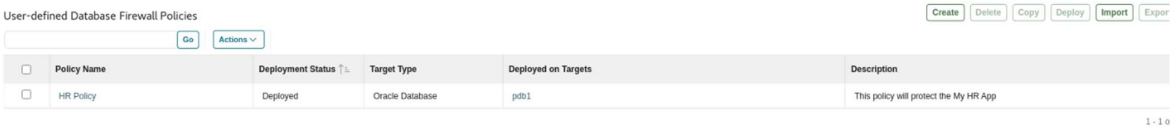
- Ta thấy kết quả trả về câu truy vấn của form này.



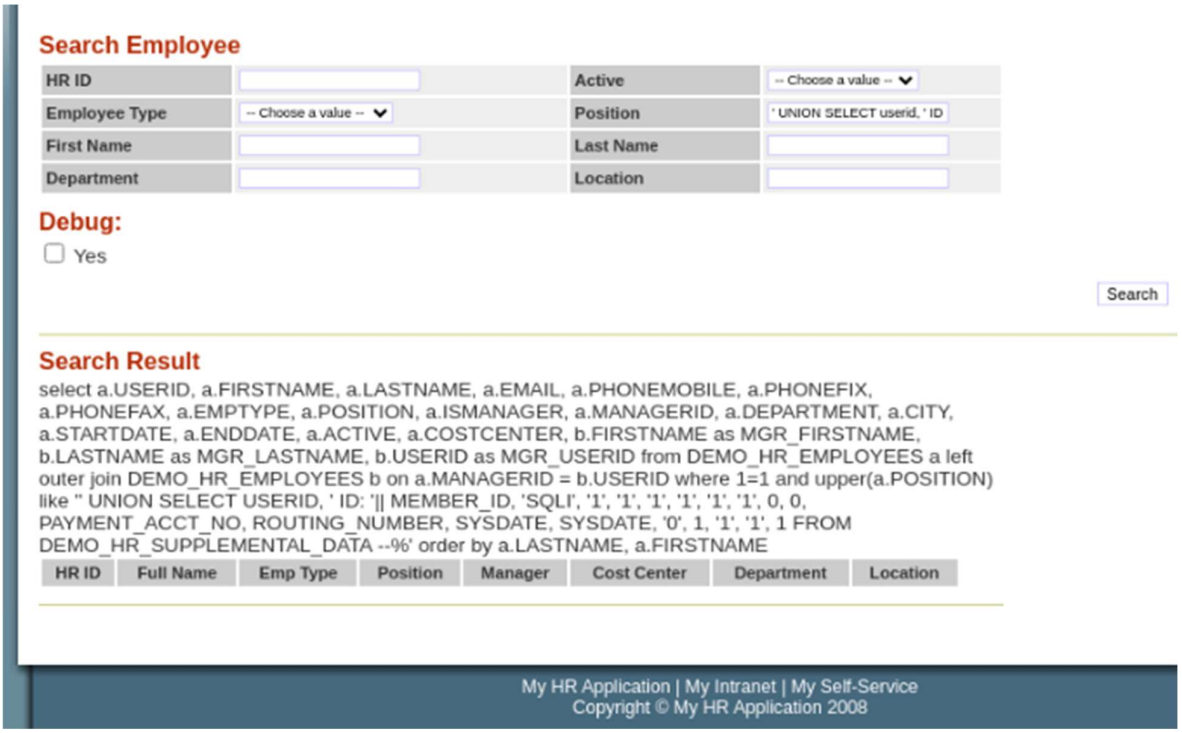
- Tiến hành triển khai **HR policy** trên pdb1



- Tiến hành chọn mục tiêu triển khai cho chính sách này là **pdb1**

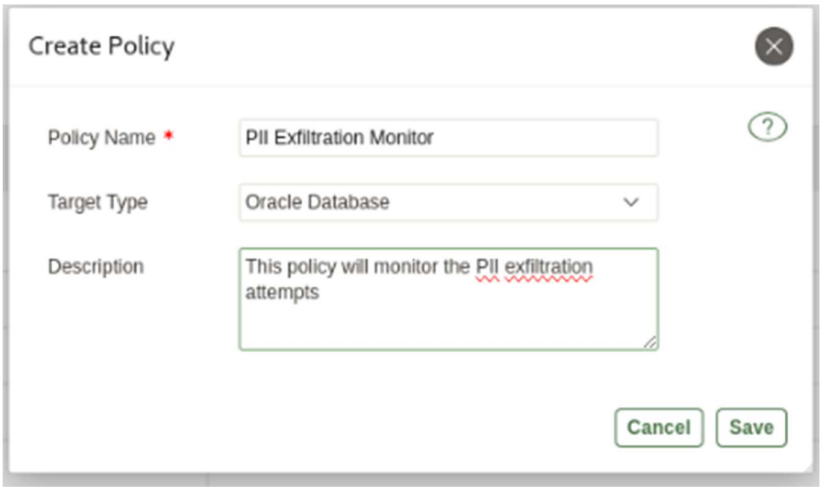


- Chính sách đã được triển khai trên **pdb1**



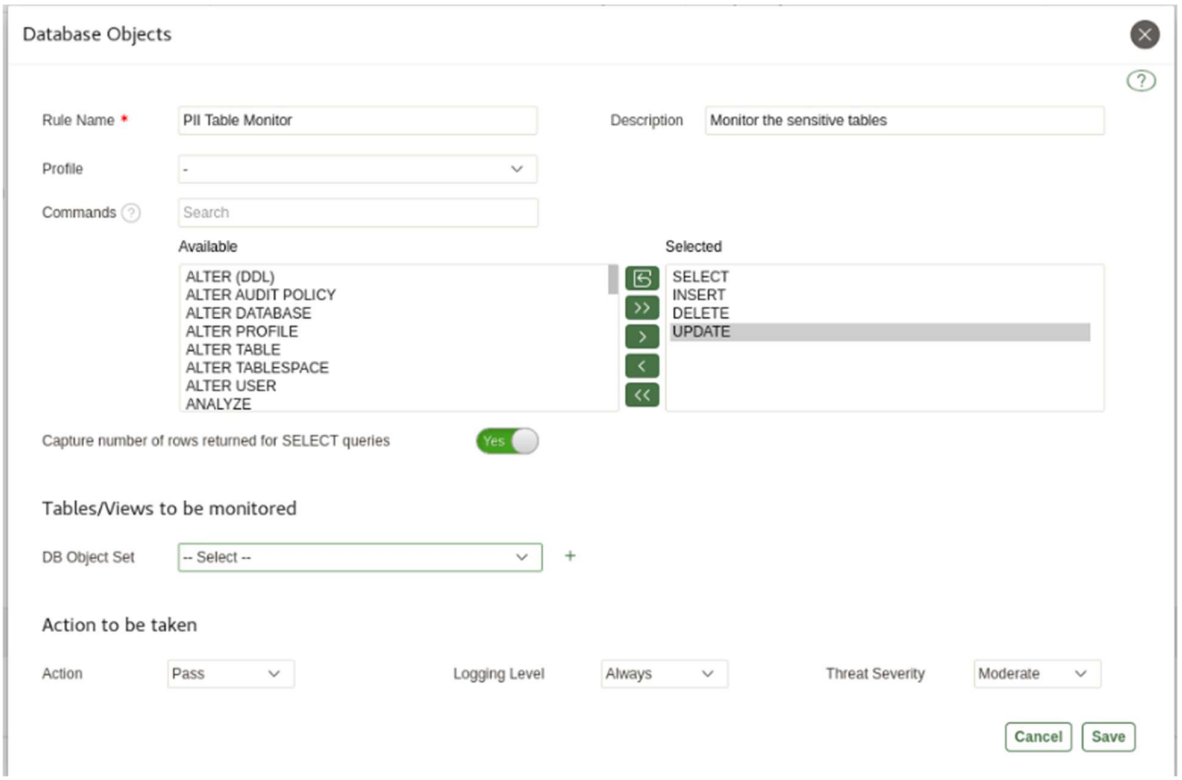
- Tiến hành tấn công Union-based SQL Injection lại thì kết quả trả về no rows.

g. DB Firewall - Phát hiện hành vi trích xuất thông tin trái phép

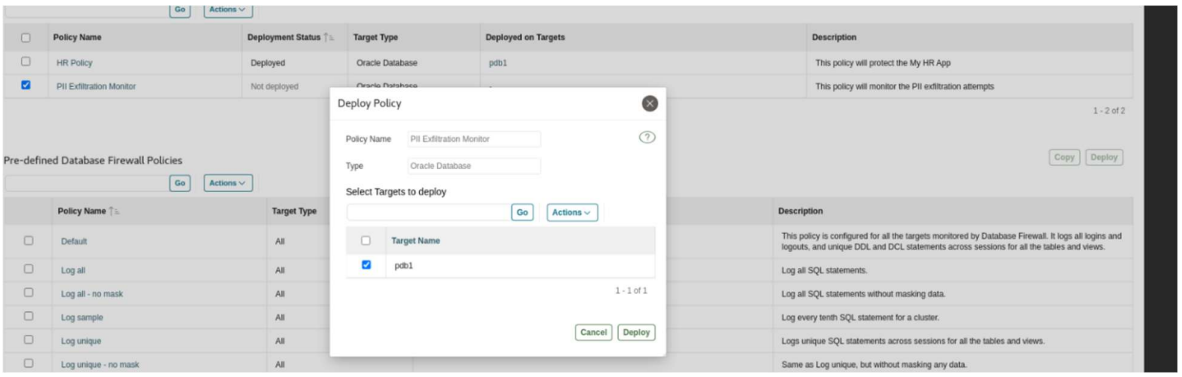


- Tiến hành tạo Policy với các thông tin sau và lưu lại:
  - Policy Name: PII Exfiltration Monitor
  - Target Type: Oracle Database
  - Description: This policy will monitor the PII exfiltration attempts

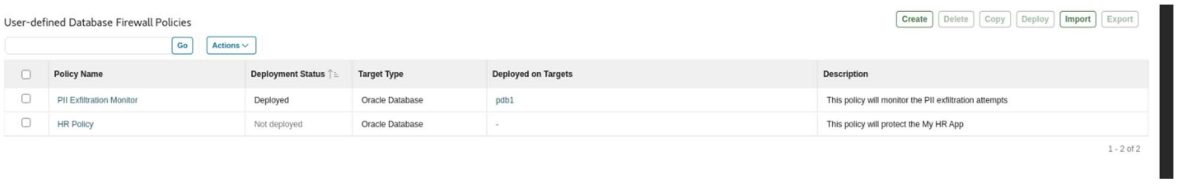
Bài thực hành số 03: Database Security



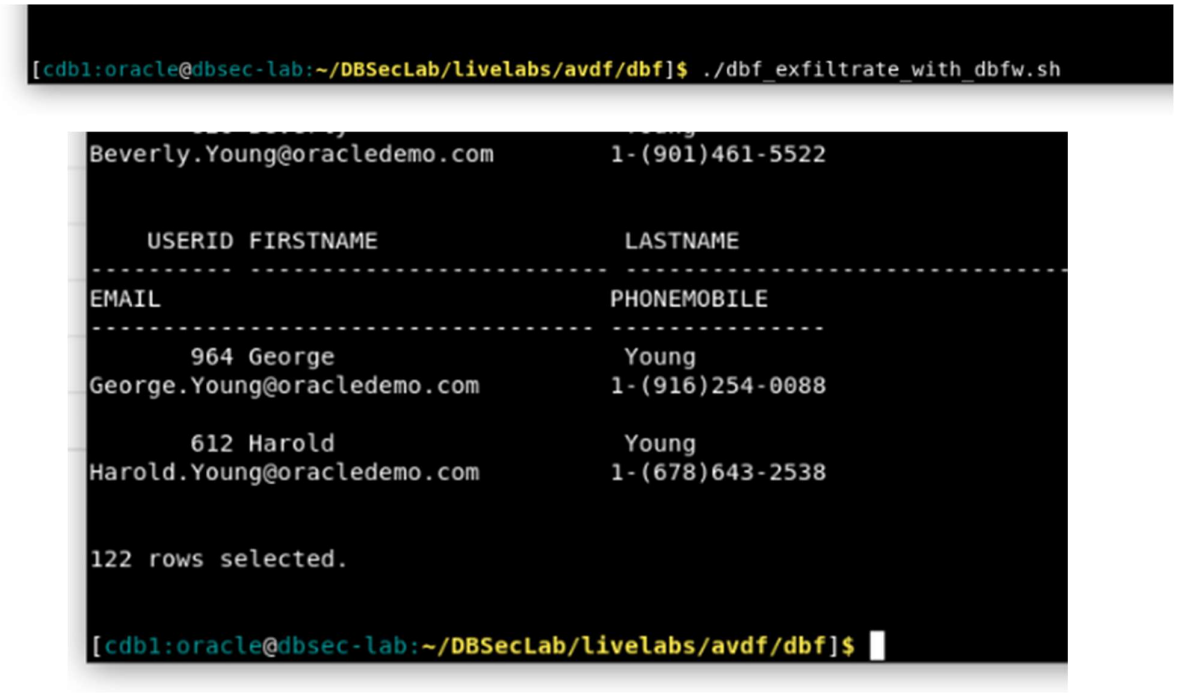
- Tiến hành tạo mới Database Object với các rule tương ứng:
    - Rule Name: PII Table Monitor
    - Description: Monitor the sensitive tables
    - Statement Classes: select DML instructions INSERT, UPDATE, DELETE and SELECT
    - Capture number of rows returned for SELECT queries: Yes
    - Action: Pass
    - Logging Level: Always
    - Threat Severity: Moderate



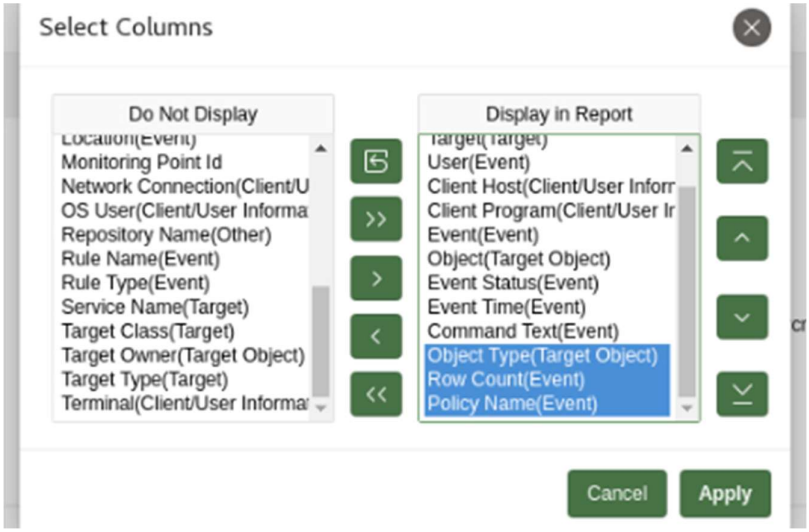
- Tiến hành triển khai **PII Exfiltration Monitor** lên **pdb1**



- Refresh lại trang thì thấy được **PII Exfiltration Monitor** đã được deploy lên **pdb1**



- Tiến hành mở Terminal, chạy script dbf_exfiltrate_with_dbfw.sh để trích xuất thông tin thử



- Trong **Database Firewall Reports,** tiến hành the

	Threat Severity	Target	User	Client Host	Client Program	Event	Object	Event Status	Event Time	Object Type	Row Count	Policy Name
	moderate	pdb1	EMPLOYEESEARCH_PROD	dbsec-hol-141366.pub.ll141366vcn.oraclevcn.com	sqlplus@dbsec-lab (TNS V1-V3)	SELECT	DEMO_HR_EMPLOYEES	SUCCESS	4/4/2025 6:47:35 PM	TABLE	122	PII Exfiltration Monitor
	moderate	pdb1	EMPLOYEESEARCH_PROD	dbsec-hol-141366.pub.ll141366vcn.oraclevcn.com	sqlplus@dbsec-lab (TNS V1-V3)	SELECT	DEMO_HR_SUPPLEMENTAL_DATA	SUCCESS	4/4/2025 6:47:35 PM	TABLE	415	PII Exfiltration Monitor
	moderate	pdb1	EMPLOYEESEARCH_PROD	dbsec-hol-141366.pub.ll141366vcn.oraclevcn.com	sqlplus@dbsec-lab (TNS V1-V3)	SELECT	DEMO_HR_EMPLOYEES	SUCCESS	4/4/2025 6:47:35 PM	TABLE	99	PII Exfiltration Monitor
	moderate	pdb1	EMPLOYEESEARCH_PROD	dbsec-hol-141366.pub.ll141366vcn.oraclevcn.com	sqlplus@dbsec-lab (TNS V1-V3)	SELECT	DEMO_HR_EMPLOYEES	SUCCESS	4/4/2025 6:47:35 PM	TABLE	1	PII Exfiltration Monitor
	moderate	pdb1	EMPLOYEESEARCH_PROD	dbsec-hol-141366.pub.ll141366vcn.oraclevcn.com	sqlplus@dbsec-lab (TNS V1-V3)	SELECT	DUAL		4/4/2025 6:47:35 PM	TABLE	-1	PII Exfiltration Monitor
	moderate	pdb1	EMPLOYEESEARCH_PROD	dbsec-hol-141366.pub.ll141366vcn.oraclevcn.com	sqlplus@dbsec-lab (TNS V1-V3)	SELECT	DUAL	SUCCESS	4/4/2025 6:47:35 PM	TABLE	1	PII Exfiltration Monitor
	moderate	pdb1	EMPLOYEESEARCH_PROD	dbsec-hol-141366.pub.ll141366vcn.oraclevcn.com	JDBC Thin Client	SELECT	DEMO_HR_EMPLOYEES		4/4/2025 6:30:39 PM	TABLE		HR Policy
	moderate	pdb1	EMPLOYEESEARCH_PROD	dbsec-hol-	JDBC Thin Client	SELECT	DEMO_HR_SUPPLEMENTAL_DATA		4/4/2025 6:30:39 PM	TABLE		HR Policy

- Đây là kết quả sau khi thêm các cột trên thành công

```
[cdb1:oracle@dbsec-lab:~/DBSecLab/livelabs/avdf/dbf]$ ./dbf_exfiltrate_with_dbfw.sh
```

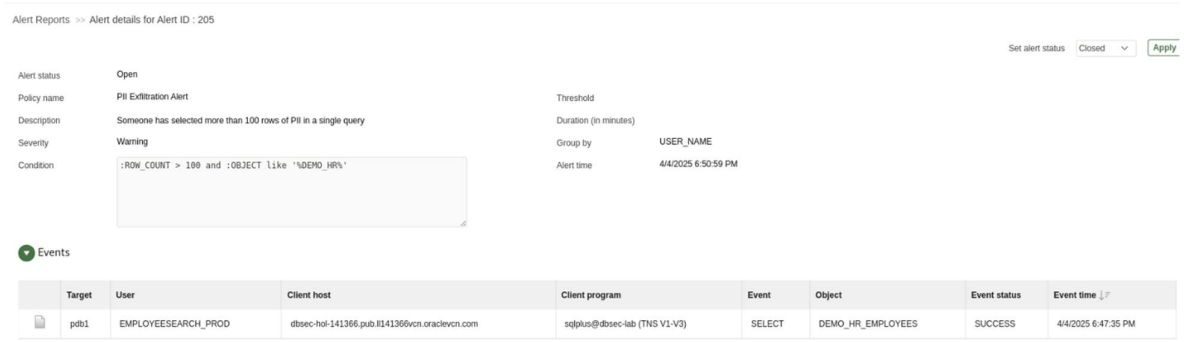
- Tiến hành chạy lại script dbf_exfiltrate_with_dbfw.sh để trích xuất thông tin để kiểm tra Policy đã hoạt động ổn chưa

```
    USERID FIRSTNAME                 LASTNAME
---------- ------------------------- --------------------
EMAIL                               PHONEMOBILE
----------------------------------- ---------------
       894 Martin                    Welch
Martin.Welch@oracledemo.com         1-(412)760-5458

       488 Joseph                    West
Joseph.West@oracledemo.com

       826 Beverly                   Young
Beverly.Young@oracledemo.com        1-(901)461-5522


    USERID FIRSTNAME                 LASTNAME
---------- ------------------------- --------------------
EMAIL                               PHONEMOBILE
----------------------------------- ---------------
       964 George                    Young
George.Young@oracledemo.com         1-(916)254-0088

       612 Harold                    Young
Harold.Young@oracledemo.com         1-(678)643-2538


122 rows selected.
```

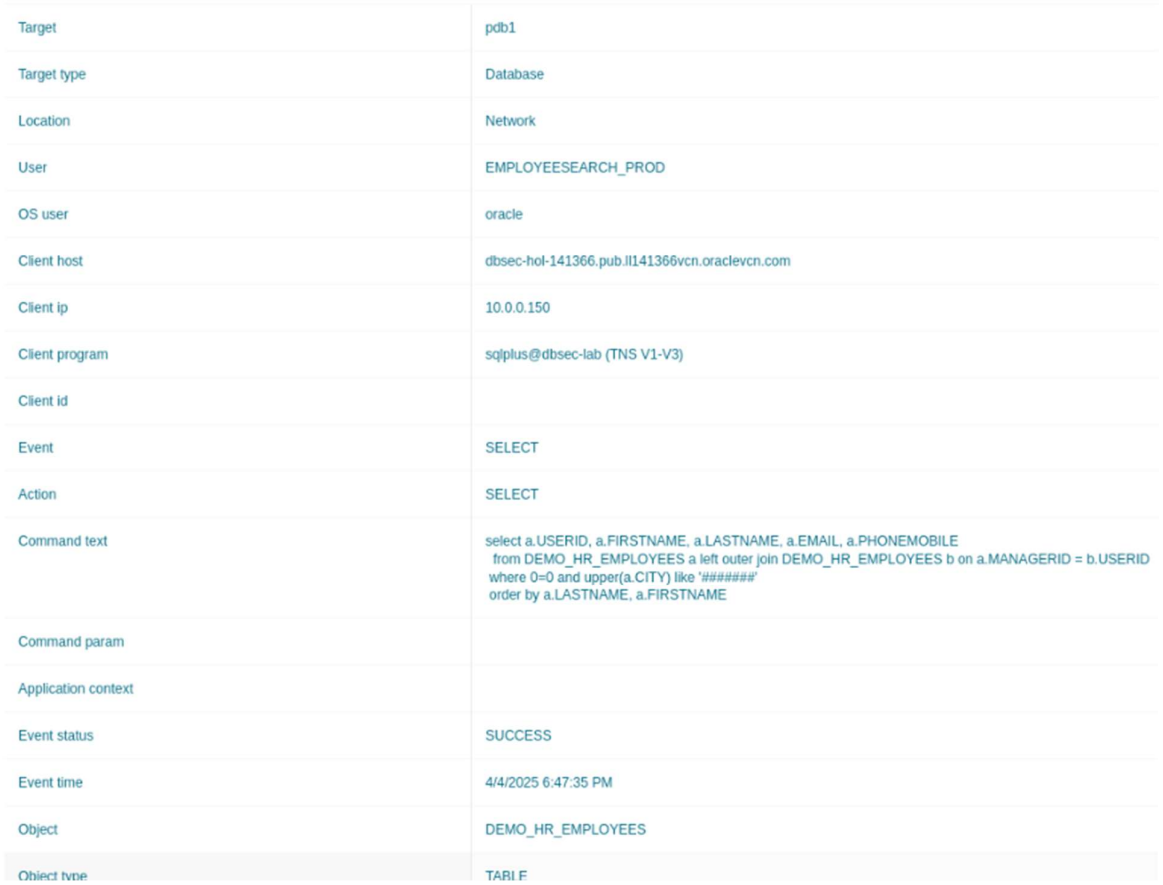
Alert time is in the last 24 hours

Alert ID	Alert status	Alert policy name	Alert severity	Alert time	Target	User	Event
205	Open	PII Exfiltration Alert	Warning	4/4/2025 6:50:59 PM	pdb1	EMPLOYEESEARCH_PROD	SELECT
204	Open	PII Exfiltration Alert	Warning	4/4/2025 6:50:59 PM	pdb1	EMPLOYEESEARCH_PROD	SELECT
203	Open	Database Firewall Alert	Warning	4/4/2025 6:33:59 PM	pdb1	EMPLOYEESEARCH_PROD	SELECT

- Ta có thể thấy được trong **Database Firewall Report** đã bắt được hành vi trích xuất thông tin trái phép



- Đây là hiển thị chi tiết về một trong các hành vi trích xuất thông tin trái phép



HẾT