



## 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 ( <i>nếu có</i> ) + Khó khăn + Đề xuất, kiến nghị	

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

## Bài thực hành số 03: Database Security

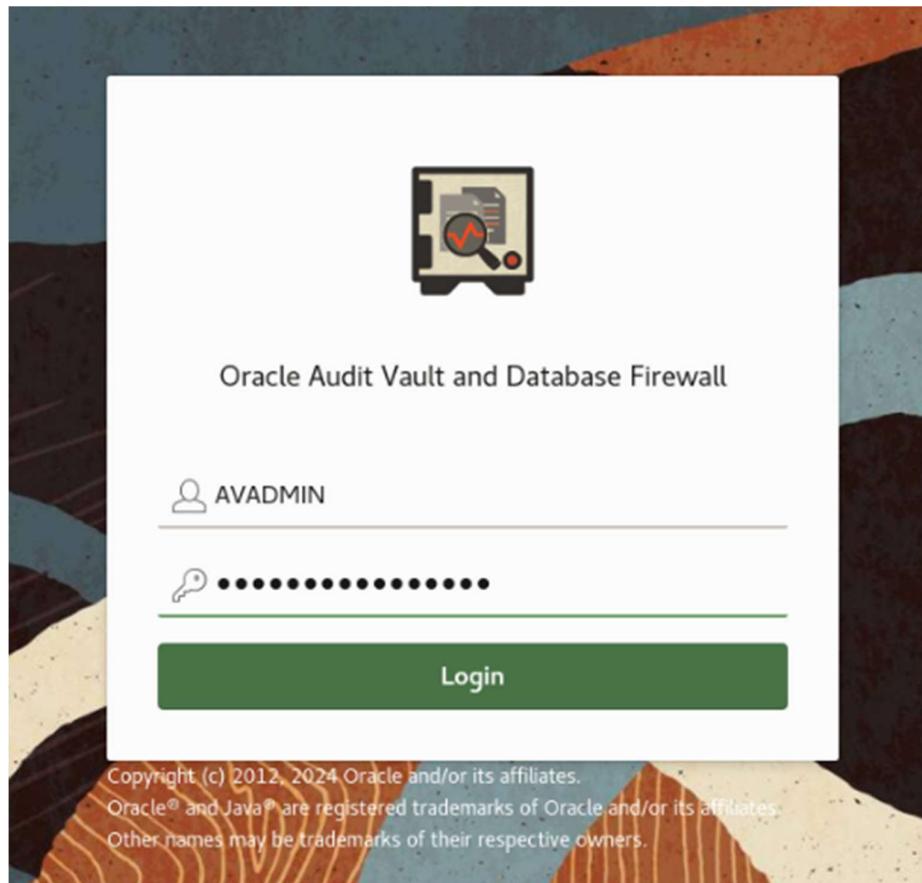
### A. BÁO CÁO CHI TIẾT

#### 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

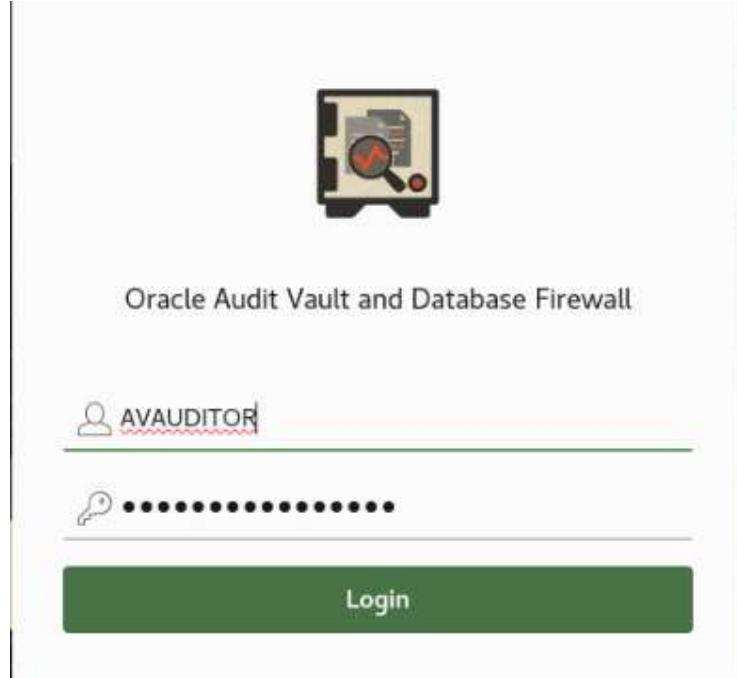
## Bài thực hành số 03: Database Security

## Reset Expired Password

AVADMIN, your password has expired.

 .....
 .....
 .....

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



- Cài lại mật khẩu

## Bài thực hành số 03: Database Security

### Reset Expired Password

AVAUDITOR, your password has expired.

The screenshot shows a password reset form. It consists of three input fields, each with a key icon and a red asterisk indicating it is required. The third field is highlighted with a green border. Below the fields is a 'Submit' button.

## 2. Task 2: Assess and Discover

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

The screenshot shows the 'Targets' page of the Oracle Audit Vault and Database Firewall 20 interface. It lists two targets: 'Audit Trails' (pdb1) and 'Database Firewall Monitoring' (pdb2). The table includes columns for Name, Type, Connect String, Schedule Retrieval Jobs, Retention Policy, and Description.

Name	Type	Connect String	Schedule Retrieval Jobs	Retention Policy	Description
Audit Trails	Oracle Database	10.0.0.150.1521 pdb1		3 months online, 6 months in archive	
Database Firewall Monitoring	Oracle Database	10.0.0.150.1521 pdb2		3 months online, 6 months in archive	

The screenshot shows the 'Security Assessment' configuration page. It displays various settings and a scheduled run configuration.

Setting	Value
Last Assessed	4/4/2025 2:54:01 PM
Last Scheduled Run	-- Never --
Next Scheduled Run	-- Never --
Repeats Every	-- Never --
Assess Immediately	<input checked="" type="checkbox"/>
Create/Update Schedule	<input checked="" type="checkbox"/>
Disable	<input type="radio"/>
Enable	<input checked="" type="radio"/>
Start At	4/4/2025 03:15:04 PM
Repeat Every	1 Days

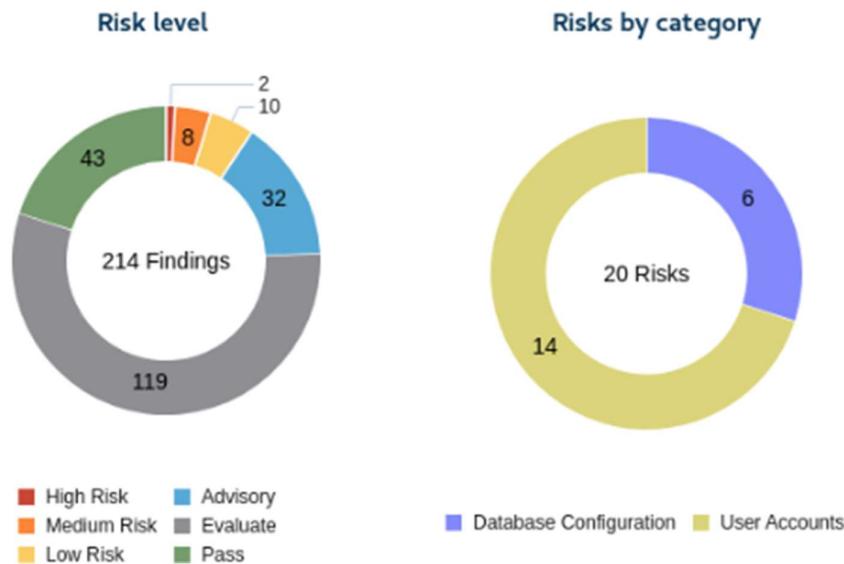
- Nay có thể xem rủi ro cho tất cả các mục tiêu trực tiếp trên dashboard và có thể truy cập vào rủi ro bằng cách nhấp vào rủi ro màu trong vòng tròn ta chọn.

## Bài thực hành số 03: Database Security

### Security assessment for Oracle databases

Targets assessed: 2

Targets not assessed: 0



- 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 hoàn đánh giá.

Security Assessment Reports >> Summary by Severity >> Detailed Report

Target: All | assessed time: Latest | Set as baseline | Add exception

Severity = Medium Risk

Target	Category	Assessment	Summary	Action	Severity	Compliance	Assessment exception
pdb1	Database Configuration	Control Files	Found 2 control files.	Ensure control files have redundancy	Medium Risk	DISA STIG	
pdb1	Database Configuration	PDB OS User	Oracle OS user will be used to interact with the operating system.	Ensure the highly privileged Oracle OS user is not being used to run external OS jobs from the database	Medium Risk	CIS Benchmark	
pdb1	User Accounts	Account Locking after Failed Login Attempts	Found 42 users with unlimited failed login attempts. User accounts are configured to stay locked for a minimum duration after being locked due to failed login attempts.	Lock the account after limited number of failed login attempts	Medium Risk	DISA STIG, CIS Benchmark	
pdb1	User Accounts	Users with no Password Complexity Requirements	Found 42 users not governed by a password verification function.	Ensure password verify function is set in user profiles	Medium Risk	DISA STIG, CIS Benchmark	
pdb2	Database Configuration	Control Files	Found 2 control files.	Ensure control files have redundancy	Medium Risk	DISA STIG	
pdb2	Database Configuration	PDB OS User	Oracle OS user will be used to interact with the operating system.	Ensure the highly privileged Oracle OS user is not being used to run external OS jobs from the database	Medium Risk	CIS Benchmark	
pdb2	User Accounts	Account Locking after Failed Login Attempts	Found 42 users with unlimited failed login attempts. User accounts are configured to stay locked for a minimum duration after being locked due to failed login attempts.	Lock the account after limited number of failed login attempts	Medium Risk	DISA STIG, CIS Benchmark	
pdb2	User Accounts	Users with no Password Complexity Requirements	Found 42 users not governed by a password verification function.	Ensure password verify function is set in user profiles	Medium Risk	DISA STIG, CIS Benchmark	

- 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.

## Bài thực hành số 03: Database Security

Assessment Check	<input type="checkbox"/>
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.ctf, /u01/oradata/cdb1/control02.ctf 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

The figure consists of two side-by-side screenshots of a web-based security assessment tool. Both screenshots show the 'Drift Summary by Target > Detailed Report' page. The top screenshot is for target 'pdb1', and the bottom one is for target 'pdb2'. Each screenshot includes a dropdown menu for 'Target' (set to 'pdb1' or 'pdb2'), a date and time selector ('assessed time' set to '4/4/2025 3:15:21 PM (Latest)'), a 'Set as baseline' button (highlighted in green), and 'Go' and 'Actions' buttons.

- 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]$ ]
```

## Bài thực hành số 03: Database Security

▼ Security Assessment

Last Assessed	4/4/2025 3:15:21 PM
Last Scheduled Run	4/4/2025 3:15:04 PM
Next Scheduled Run	4/5/2025 3:15:04 PM
Repeats Every	1 Day
Assess Immediately	<input checked="" type="checkbox"/>
Create/Update Schedule	<input type="checkbox"/>

Note : All the assessments will be purged after 18 months from the time of retrieval.

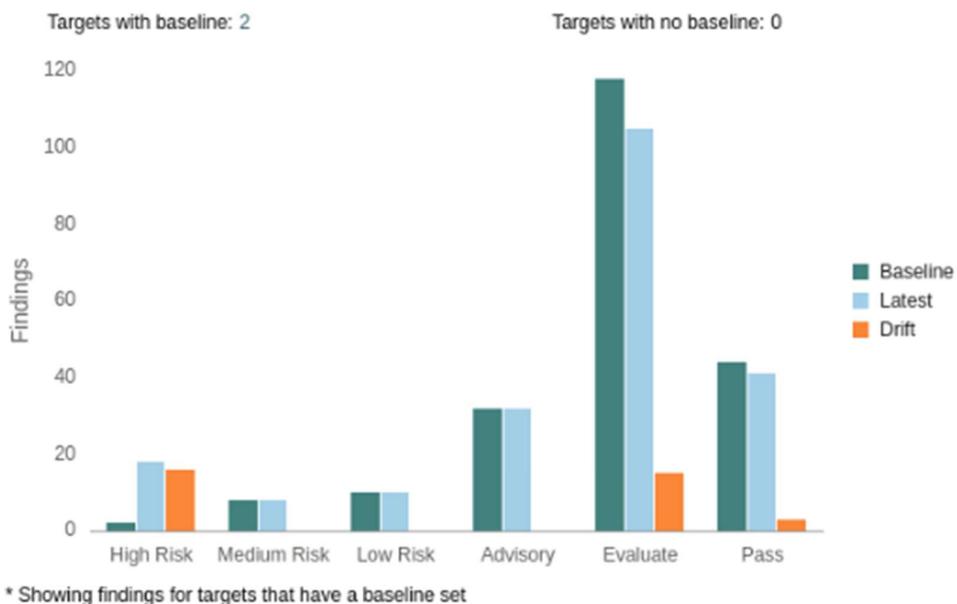
▼ Security Assessment

Last Assessed	4/4/2025 2:59:41 PM
Last Scheduled Run	4/4/2025 2:59:29 PM
Next Scheduled Run	4/7/2025 2:59:29 PM
Repeats Every	3 Days
Assess Immediately	<input checked="" type="checkbox"/>
Create/Update Schedule	<input type="checkbox"/>

Note : All the assessments will be purged after 18 months from the time of retrieval.

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

### Security assessment drift graph



## Bài thực hành số 03: Database Security

- 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

**▼ Security Assessment**

Last Assessed	4/4/2025 3:45:01 PM
Last Scheduled Run	4/4/2025 3:15:04 PM
Next Scheduled Run	4/5/2025 3:15:04 PM
Repeats Every	1 Day
Assess Immediately	<input checked="" type="checkbox"/>
Create/Update Schedule	<input type="checkbox"/>

Note : All the assessments will be purged after 18 months from the time of retrieval.

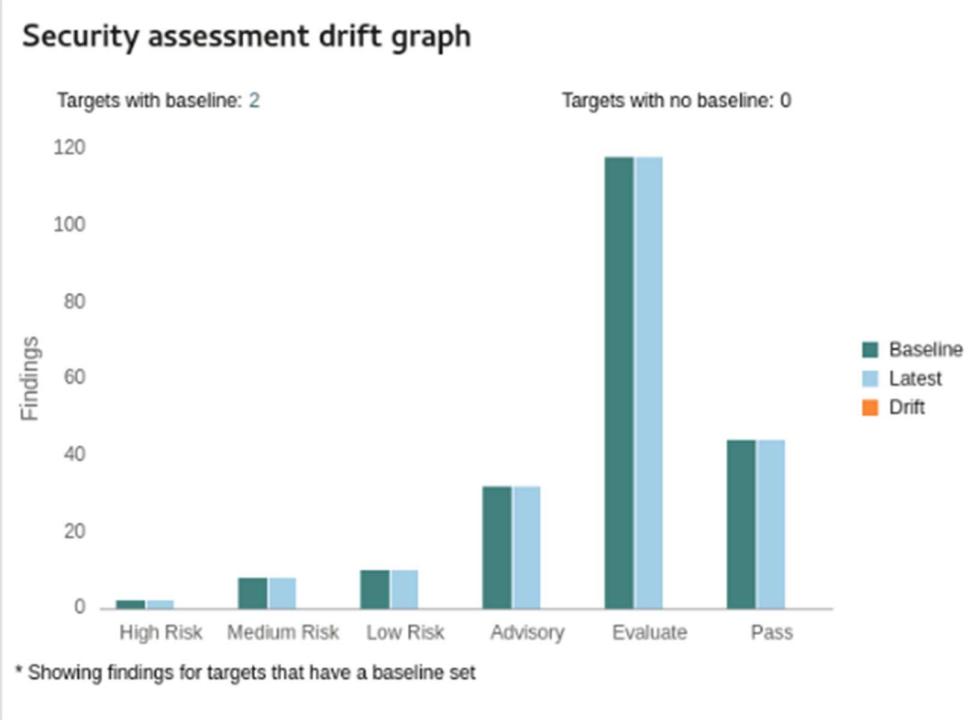
**▼ Security Assessment**

Last Assessed	4/4/2025 2:59:41 PM
Last Scheduled Run	4/4/2025 2:59:29 PM
Next Scheduled Run	4/7/2025 2:59:29 PM
Repeats Every	3 Days
Assess Immediately	<input checked="" type="checkbox"/>
Create/Update Schedule	<input type="checkbox"/>

Note : All the assessments will be purged after 18 months from the time of retrieval.

- 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.

## Bài thực hành số 03: Database Security



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

Sensitive Objects

Last Discovered	4/4/2025 2:53:46 PM
Last Scheduled Run	-- Never --
Next Scheduled Run	-- Never --
Repeats Every	-- Never --
Discover Immediately	<input checked="" type="checkbox"/>
Create/Update Schedule	<input checked="" type="checkbox"/>
<input type="radio"/> Disable <input checked="" type="radio"/> Enable	
Start At	4/4/2025 03:54:02 PM <input type="button" value=""/>
Repeat Every	<input type="text" value="1"/> Days <input type="button" value=""/>

## Bài thực hành số 03: Database Security

Create and manage Global sets like IP address, database user, OS user, client program, privileged user, and sensitive object sets on this page.  
They can be used in Database Firewall policies and reports.

- IP Address Sets (0)
- OS User Sets (0)
- Client Program Sets (0)
- Database User Sets (0)
- Privileged User Sets (0)
- Sensitive Object Sets (0)

Discover sensitive objects by scheduling sensitive object sets.

### 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
  - o pdb1 sử dụng phương pháp agent-based audit collection
  - o pdb2 sử dụng agentless audit collection
- Truy cập giao diện Audit Vault Web Console bằng tài khoản AVAUDITOR
- Cấu hình audit cho pdb1:
  - o Vào tab Targets → chọn Schedule Retrieval Jobs cho pdb1
  - o 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

## Bài thực hành số 03: Database Security

Audit Policy

Last Retrieved	4/4/2025 2:54:09 PM
Last Scheduled Run	-- Never --
Next Scheduled Run	-- Never --
Repeats Every	-- Never --
Retrieve Immediately	<input checked="" type="checkbox"/>
Create/Update Schedule	<input checked="" type="checkbox"/>
<input type="radio"/> Disable <input checked="" type="radio"/> Enable	
Start At	4/4/2025 03:58:35 PM
Repeat Every	1 Days

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

The screenshot shows the Oracle Database Policy Management interface. The 'Unified Auditing' tab is selected. In the 'Core Policies' section under 'Basic Auditing', several checkboxes are checked: 'Critical Database Activity', 'Database Schema Changes', 'All Admin Activity', and 'Center for Internet Security (CIS) Configuration'. A red box highlights this section. In the 'Oracle Predefined Policies' section, several policies are listed, with some checked: ORA\_ACCOUNT\_MGMT, ORA\_DATABASE\_PARAMETER, ORA\_DV\_AUDPOL, ORA\_DV\_AUDPOL2, ORA\_LOGON\_FAILURES, ORA\_RAS\_POLICY\_MGMT, ORA\_RAS\_SESSION\_MGMT, and ORA\_SECURECONFIG. A red box highlights the 'Provision Unified Policy' button at the top right.

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

## Bài thực hành số 03: Database Security

The screenshot shows the Oracle Audit Insights interface. On the left, there's a sidebar with options like 'Manage Auditors', 'Distribution Lists', 'Email Templates', 'Alert Syslog Templates', and 'Jobs'. The main area has tabs for 'Audit Insights', 'Targets', 'Global Sets', 'Policies', 'Alerts', 'Reports', and 'Settings'. Under 'Audit Insights', there are filters for 'Last Updated is in the last 7 days' and 'Highlight Failed Jobs'. A table lists audit jobs: 'Unified Audit Policy' (Completed, 4/4/2025 3:55:42 PM), 'Audit Settings' (Completed, 4/4/2025 3:54:30 PM), 'DBSAT Data Discovery' (Completed, 4/4/2025 3:54:05 PM), and 'Checklist AVDF System account traffic status' (Completed, 4/4/2025 3:54:42 PM). A red box highlights the first row.

- Tương tự cho cấp phát chính sách audit cho pdb2

This screenshot shows the Oracle Audit Insights interface for pdb2. It has tabs for 'Unified Auditing' and 'Traditional Auditing'. Under 'Core Policies', there are sections for 'Basic Auditing', 'Admin Activity Auditing', 'User Activity Auditing', and 'Audit Compliance Standards'. Under 'Oracle Predefined Policies', there is a list of policies with checkboxes: 'ORA\_ACCOUNT\_MGMT', 'ORA\_DATABASE\_PARAMETER', 'ORA\_DV\_AUDPOL', 'ORA\_DV\_AUDPOL2', 'ORA\_LOGON\_FAILURES' (which is checked), 'ORA\_RAS\_POLICY\_MGMT', 'ORA\_RAS\_SESSION\_MGMT', and 'ORA\_SECURECONFIG' (which is checked). Under 'Custom Policies', there is a search bar and a message stating 'No Custom Policies found.' A red box highlights the 'Provision Unified Policy' button in the top right corner.

- Kiểm tra trạng thái Jobs pdb2:

The screenshot shows the Oracle Audit Insights interface for pdb2. It has a sidebar with 'Email Templates', 'Alert Syslog Templates', and 'Jobs'. The main area shows audit jobs: 'Unified Audit Policy' (Completed, 4/4/2025 3:57:25 PM), 'Unified Audit Policy' (Completed, 4/4/2025 3:55:42 PM), and 'Audit Settings' (Completed, 4/4/2025 3:54:30 PM). A red box highlights the first row.

- Kiểm tra chính sách audit bằng SQL\*Plus

- o Liệt kê tất cả Unified Audit Policies trên pdb1

```
[cdb1:oracle@dbsec-lab:~/DBSecLab/livelabs/avdf/avs]$ ./avs_query_all_unified_policies.sh pdb1
=====
List all of the Unified Audit Policies in the pluggable database pdb1...
This includes enabled and disabled policies!
=====

. List all the Unified Audit policies

POLICY_NAME
-----
ORA_ACCOUNT_MGMT
ORA_AV$_ADMIN_USER_ACTIVITY
ORA_AV$_CRITICAL_DB_ACTIVITY
ORA_AV$_DB_SCHEMA_CHANGES
ORA_AV$_SYS_TOP_ACTIVITY
ORA_CIS_RECOMMENDATIONS
ORA_DATABASE_PARAMETER
ORA_DV_AUDPOL
ORA_DV_AUDPOL2
ORA_LOGON_FAILURES
ORA_RAS_POLICY_MGMT
ORA_RAS_SESSION_MGMT
ORA_SECURECONFIG

13 rows selected.

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

- o Liệt kê các Unified Audit Policies đang được kích hoạt

## Bài thực hành số 03: Database Security

```
15 rows selected.
[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

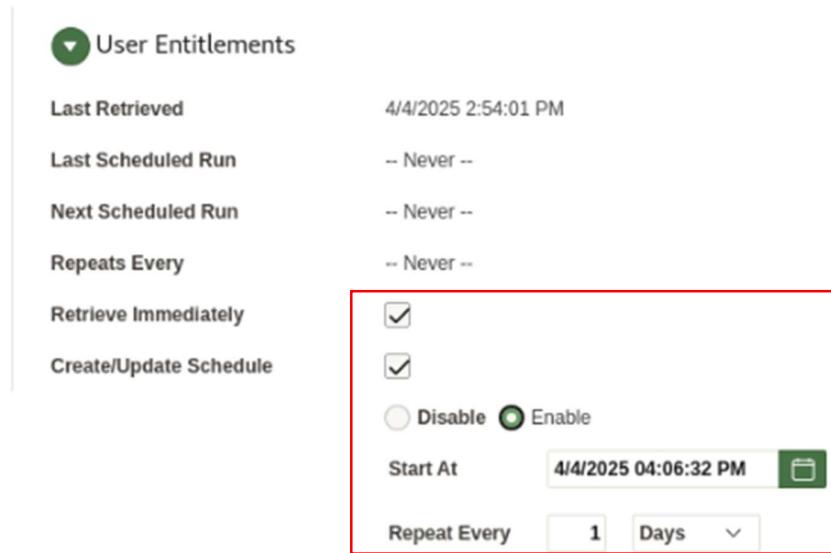
POLICY_NAME          ENABLED_OPTION ENTITY_NAME      ENTITY_TYPE  SUCCESS  FAILURE
-----              -----
ORA_SECURECONFIG      BY USER      ALL USERS        USER         YES      YES
ORA_LOGON_FAILURES   BY USER      ALL USERS        USER         NO       YES
ORA_CIS_RECOMMENDATIONS BY USER    ALL 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 AVDFULL10R
```

### 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

## Bài thực hành số 03: Database Security

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	APPDEV_USER5	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.

## Bài thực hành số 03: Database Security

Modify Target Group

Group Name Data Privacy (GDPR)

Description Data Privacy related targets

Members

Search Targets to add in the group

Available

Selected

pdb1 (Oracle Database)  
pdb2 (Oracle Database)

Cancel Save

The screenshot shows a 'Modify Target Group' dialog box. At the top, it displays the group name 'Data Privacy (GDPR)' and a description 'Data Privacy related targets'. Below this is a section titled 'Members' with a search bar labeled 'Search Targets to add in the group'. There are two columns: 'Available' and 'Selected'. The 'Available' column is currently empty. The 'Selected' column contains two items: 'pdb1 (Oracle Database)' and 'pdb2 (Oracle Database)'. To the right of the 'Selected' column are five green navigation buttons: a circular arrow, double right, right, left, and double left. At the bottom right of the dialog are 'Cancel' and 'Save' buttons.

- Chọn báo cáo Sensitive Data để xem chi tiết:

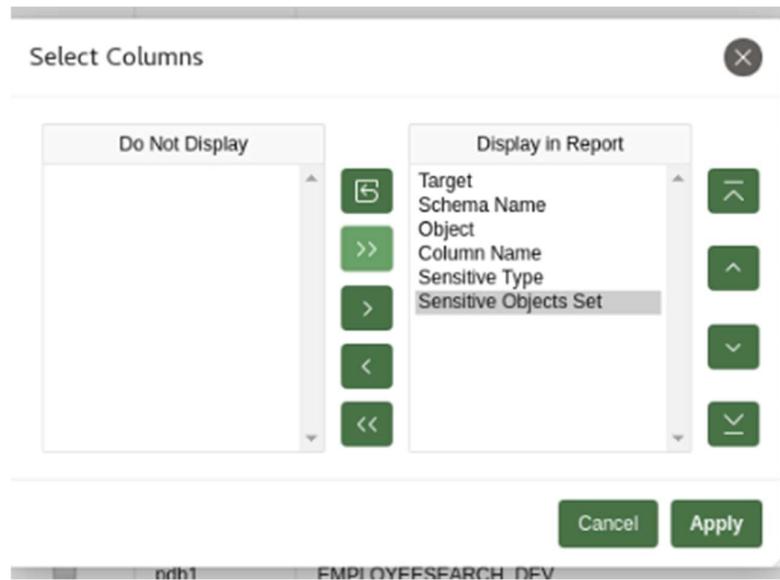
Data Privacy Report (GDPR) >> Sensitive Data

Actions

	Target	Schema Name	Object	Column Name	Sensitive Type
1	pdb1	DMS_ADMIN	MASK_DATA	GIVENNAME	FIRST NAME
2	pdb1	DMS_ADMIN	MASK_DATA	SURNNAME	LAST NAME
3	pdb1	DMS_ADMIN	MASK_DATA	STREETADDRESS	STREET
4	pdb1	DMS_ADMIN	MASK_DATA	CITY	CITY
5	pdb1	DMS_ADMIN	MASK_DATA	ZIPCODE	POSTAL CODE
6	pdb1	DMS_ADMIN	MASK_DATA	USERNAME	USER ID
7	pdb1	DMS_ADMIN	MASK_DATA	TELEPHONENUMBER	PHONE NUMBER
8	pdb1	EMPLOYEESEARCH_DEV	DEMO_HR_EMPLOYEES	USERID	USER ID
9	pdb1	EMPLOYEESEARCH_DEV	DEMO_HR_EMPLOYEES	FIRSTNAME	FIRST NAME
10	pdb1	EMPLOYEESEARCH_DEV	DEMO_HR_EMPLOYEES	LASTNAME	LAST NAME
11	pdb1	EMPLOYEESEARCH_DEV	DEMO_HR_EMPLOYEES	EMAIL	EMAIL ADDRESS
12	pdb1	EMPLOYEESEARCH_DEV	DEMO_HR_EMPLOYEES	CITY	CITY
13	pdb1	EMPLOYEESEARCH_DEV	DEMO_HR_EMPLOYEES	DOB	DATE OF BIRTH
14	pdb1	EMPLOYEESEARCH_DEV	DEMO_HR_EMPLOYEES	SSN	US SOCIAL SECURITY NUMBER (SSN)
15	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

## Bài thực hành số 03: Database Security



- 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.

pdb2 (Oracle Database)

Connect String: jdbc:oracle:thin:@10.0.0.150:1521:pdb2

Retention Policy: 3 months online, 6 months in archive

Audit Data Collection		Database Firewall Monitoring	
Trail Location	Trail Type	Status	Agent
UNIFIED_AUDIT_TRAIL	TABLE	Idle	Agentless Collection
A01/apporacle/product/loggvar/lib/data	TRANSACTION LOG	Idle	dtseclab

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

Home    Audit Insights    Targets    Global Sets    Policies    Alerts    Reports    Settings

Targets	Target	Trail Location	Trail Type	Status	Target Type	Agent	Last Started	Data Collected Until
Audit Trails	pdb1	UNIFIED_AUDIT_TRAIL	TABLE	Idle	Oracle Database	dtseclab	4/4/2025 2:57:29 PM	4/4/2025 4:16:44 PM
Database Firewall Monitoring	pdb2	A01/apporacle/product/loggvar/lib/data	TRANSACTION LOG	Idle	Oracle Database	Agentless Collection	4/4/2025 2:57:29 PM	4/4/2025 4:16:47 PM

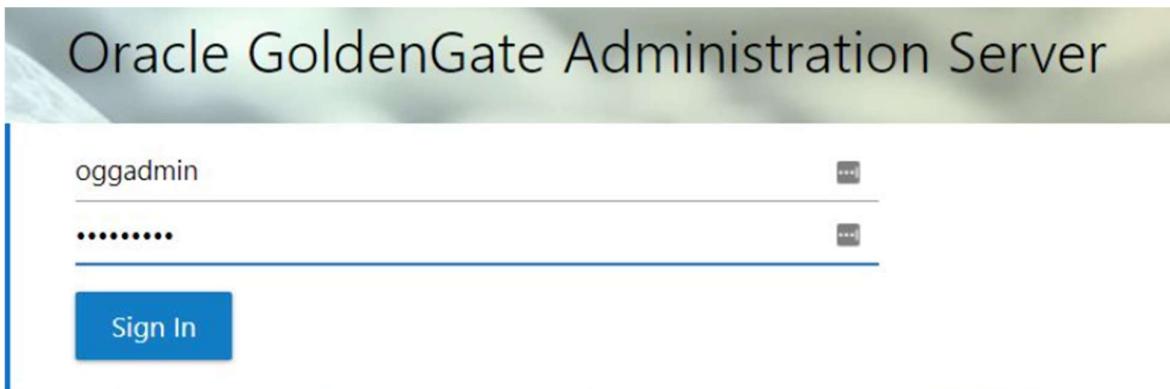
- Đảm bảo dịch vụ Oracle GoldenGate đang hoạt động

## Bài thực hành số 03: Database Security

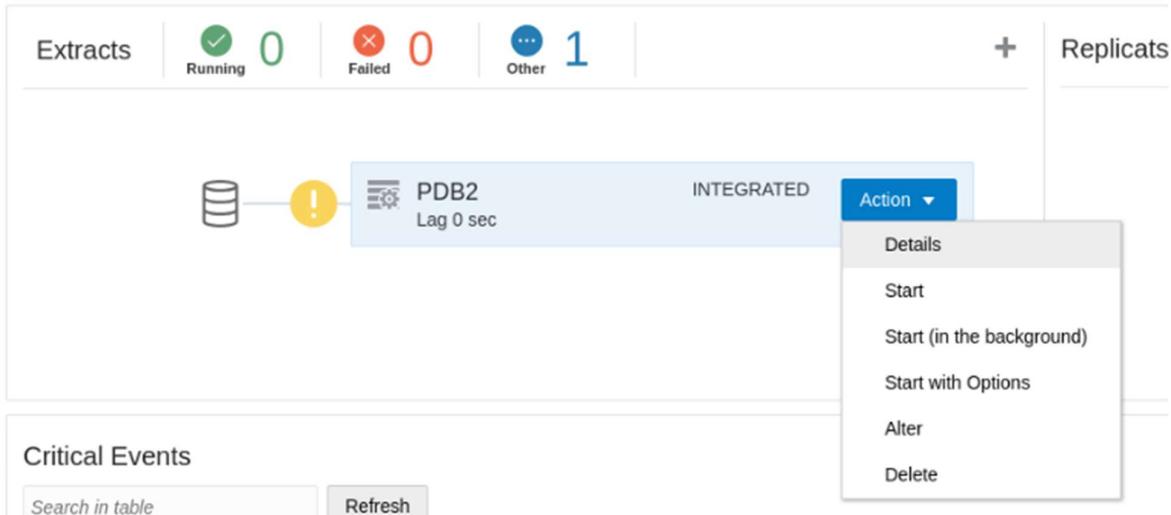
```
wir [cdb1:oracle@dbsec-lab:~/DBSecLab/livelabs/avdf/avs]$ ./avs_start_ogg.sh
sin=====
We Start Oracle Golden Gate Services...
=====
. Start Oracle Golden Gate
Service Manager is already running (PID: 15449)
.
. Login to the GoldenGate Administration Server at http://192.9.177.42:50002

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

- Đăng nhập GoldenGate Web Console



- Khởi động Extract cho pdb2



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

## Bài thực hành số 03: Database Security

```
. 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

[cdh1:oracle@dbsec-lab: ~/DBSecLab/livelabs/avdf/avsl]
```

- Xem báo cáo chứa dữ liệu thay đổi

Target	User	Client Host	Client Program	Event	Object	Primary Key Value(s)	Column(s) Modified	Event Status	Event Time
pd2	EMPLOYEESEARCH_PROD	dbsec-lab	sqlplus@dbsec-lab (TNS V1-V2)	UPDATE	DEMO_HR_EMPLOYEES		Column SALARY Old Value 9759.05 New Value 11613.27	SUCCESS	4/4/2025 4:43:47 PM

### e. Thiết lập chính sách cảnh báo

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

## Bài thực hành số 03: Database Security

### o Điền các thông tin

Alert policy name \* User creation/modification

Alert description Alert when the user is created, dropped, or altered

Target type \* Oracle Database

Severity \* Warning

Condition \*  
(:COMMAND\_CLASS = 'CREATE' OR :COMMAND\_CLASS = 'DROP' OR :COMMAND\_CLASS = 'ALTER')  
AND (:OBJECT\_TYPE = 'USER')

**Copy condition from examples** **Copy condition from alert policies**

**Create condition using report** **Create condition using global sets**

Add optional threshold condition ⓘ

Threshold (number) 1 ⓘ Duration (in minutes) 1 ⓘ Group by - Select - ⓘ

**Configure email notification**

Enable email notification  No

- Cảnh báo đã được bắt đầu

<input type="checkbox"/>	Alert policy name	Enabled	Target type	Email notification	Created by	Last updated	Alerts	Alert description
<input type="checkbox"/>	Database Firewall Alert	<input checked="" type="checkbox"/>	All	<input checked="" type="checkbox"/>	AVSYS	2/28/2025 5:17:18 PM		An alert evaluated at a Database Firewall, based on a Firewall Policy.
<input type="checkbox"/>	CREATE USER	<input checked="" type="checkbox"/>	Oracle Database	<input checked="" type="checkbox"/>	AVAUDITOR	4/4/2025 2:57:29 PM		Alert on CREATE USER statements
<input type="checkbox"/>	User creation/modification	<input checked="" type="checkbox"/>	Oracle Database	<input checked="" type="checkbox"/>	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

## Bài thực hành số 03: Database Security

```
[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"
1
User created.

2

. Create user "new_user_ned" as dba_debra
USER is "DBA_DEBRA"
3
User created.

4

[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"
1
User created.

2

. Create user "new_user_ted" as system
USER is "SYSTEM"
3
User created.

4

. Create user "new_user_ned" as dba_debra
USER is "DBA_DEBRA"
5
User created.

6

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

## Bài thực hành số 03: Database Security

```
[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]$ ./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

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

- Nội dung chi tiết cảnh báo

## Bài thực hành số 03: Database Security

Alert Reports >> Alert details for Alert ID : 118

Alert status: Open  
Policy name: User creation/modification  
Description: Alert when the user is created, dropped, or altered  
Severity: Warning  
Condition: (:COMMAND\_CLASS = 'CREATE' OR :COMMAND\_CLASS = 'DROP' OR :COMMAND\_CLASS = 'ALTER') AND (:OBJECT\_TYPE = 'USER')

Threshold: Duration (in minutes)  
Group by: Alert time: 4/4/2025 4:53:20 PM

Set alert status: Closed

### Events

Target	User	Client host	Client program	Event	Object	Event status	Event time
ptb1	SYSTEM	dbsec-lab	sqlplus@dbsec-lab (TNS V1-V3)	DROP USER	NEW_USER_NED	SUCCESS	4/4/2025 4:52:52 PM

1 - 1

### Notification

No notifications found

### Notes

Note	Created time	Created by

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

Alert policy name \*: PII Exfiltration Alert

Alert description: Someone has selected more than 100 rows of PII in a single query

Target type \*: Oracle Database

Severity \*: Warning

Condition \*: :ROW\_COUNT > 100 and :TARGET\_OBJECT like "%DEMO\_HR%"

Add optional threshold condition

Threshold (number):  Duration (in minutes):  Group by:

### Configure email notification

Enable email notification

- Cảnh báo đã được tạo và chạy

CREATE USER	CREATE DATABASE	GRANT	REVOKE	ALTER	ALTER SYSTEM	ALTER PLUGGABLE DATABASE
<input type="checkbox"/> PII Exfiltration Alert	<input checked="" type="checkbox"/> Oracle Database	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> AVAUDITOR	4/4/2025 4:57:51 PM	<input checked="" type="checkbox"/>	Someone has selected more than 100 rows of PII in a single query
<input type="checkbox"/> User creation/modification	<input checked="" type="checkbox"/> Oracle Database	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> AVAUDITOR	4/4/2025 4:50:39 PM	<input checked="" type="checkbox"/>	Alert when the user is created, dropped, or altered

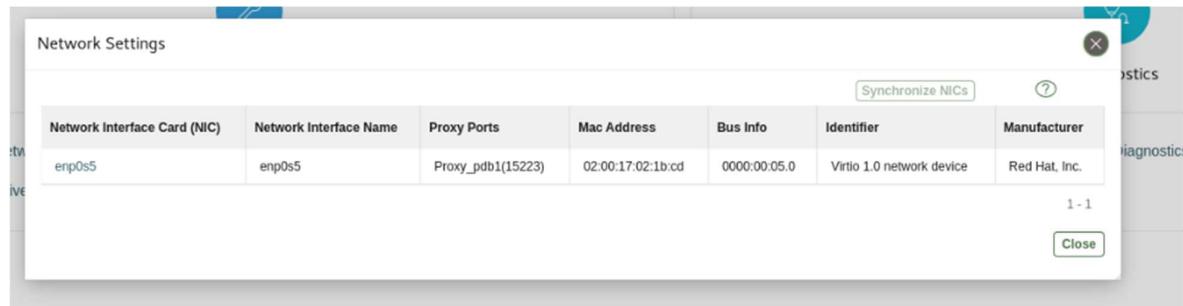
## Bài thực hành số 03: Database Security

### 5. Task 5: Protect and Prevent

#### f. Bật DB Firewall Monitoring

Database Firewall Monitoring							Start	Stop	Delete	Add	
	Connection Details	Primary Status	Standby Status	Database Firewall	Network Interface Card	Proxy Port	Mode				
	10.0.0.150 : 1521 : pdb1	Up	n/a	dbfw	enp0s5 (enp0s5)	Proxy_pdb1 (15223)	Monitoring / Blocking (Proxy)				

- 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

```
[cdb1:oracle@dbsec-lab:~/DBSecLab/livelabs/avdf/avs]$ cd $DBSEC_LABS/avdf/dbf
[cdb1:oracle@dbsec-lab:~/DBSecLab/livelabs/avdf/dbf]$ ./dbf_sqlplus_without_dbfw.sh
=====
Verify connectivity to pdb1 without the Database Firewall...
=====
ie. Connect directly to the pluggable database without the DB Firewall
ox$ sqlplus -s system/Oracle123@pdb1
CON_NAME
PDB1
USER is "SYSTEM"
. Which IP address we are connecting from
IP_ADDRESS
10.0.0.150
IT

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

- 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 kết nối là từ IP 10.0.0.150, vốn là địa chỉ IP của DBSec-Lab VM

## Bài thực hành số 03: Database Security

```
[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.

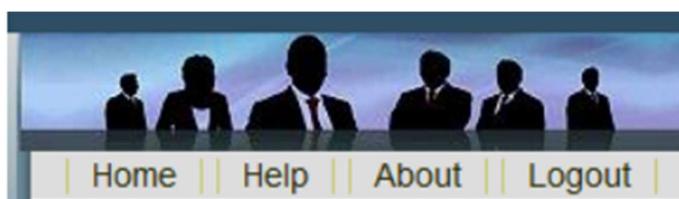
The screenshot shows the 'MyHR Application' web interface. At the top, there is a header bar with the title 'MyHR Application' and a user welcome message: 'Welcome HR Administrator! Privileges: [INSERT, SELECT, UPDATE]'. Below the header, there is a navigation menu with links for 'Home', 'Help', 'About', and 'Logout'. The main content area features a section titled 'Latest Employee News' with a timestamp 'Fri Apr 04 17:24:38 GMT 2025'. It contains two paragraphs of text about employee benefit coverage and medical claims. To the right of the text is a small thumbnail image of a person in a blue shirt and black pants. At the bottom right of the main content area, there is a link 'Comments (4)'. On the far right, there is a sidebar with links for 'Employees', 'Search Employees', 'New Employee', 'Absence And Attendance', 'Timesheets', and 'Vacation'.

- Tiến hành mở Web Browser tại URL: [http://dbsec-lab:8080/hr\\_prod\\_pdb1](http://dbsec-lab:8080/hr_prod_pdb1) và đăng nhập với tài khoản và mật khẩu lần lượt là **hadmin** và **Oracle123**

## Bài thực hành số 03: Database Security

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**



## Bài thực hành số 03: Database Security

- Bây giờ ta sẽ tiến hành đăng xuất

```
[cdb1:oracle@dbsec-lab:~/DBSecLab/livelabs/avdf/dbf]$ ./dbf_start_proxy_glassfish.sh
=====
Migrate the Glassfish App connection string to proxy through the DB Firewall...
=====

=====
Stop Glassfish App...
=====

Waiting for the domain to stop .
Command stop-domain executed successfully.

. Copy the config file to change the connection string to proxy through the DB Firewall
=====
Start Glassfish App...
=====

Waiting for domain1 to start .....
Successfully started the domain : domain1
domain Location: /u01/app/glassfish/glassfish4/glassfish/domains/domain1
Log File: /u01/app/glassfish/glassfish4/glassfish/domains/domain1/logs/server.log
Admin Port: 4848
Command start-domain executed successfully.

. You can login to the apps using the appropriate URL:
http://192.9.177.42:8080/hr_dev_pdb1
http://192.9.177.42:8080/hr_dev_pdb2
http://192.9.177.42:8080/hr_prod_pdb1
http://192.9.177.42:8080/hr_prod_pdb2

is. The Glassfish App is now running with the following configuration
-----
oJDBCDriver = oracle.jdbc.OracleDriver
o JDBCURL = jdbc:oracle:thin:@//dbf:15223/pdb1
o JDBCUser = EMPLOYEESEARCH_PROD
o JDBCPassword = Oracle123
-----
cc
[cdb1:oracle@dbsec-lab:~/DBSecLab/livelabs/avdf/dbf]$ ]
```

- 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.

## Bài thực hành số 03: Database Security

BG_JOB_ID	
CLIENT_IDENTIFIER	hadmin
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**

## Bài thực hành số 03: Database Security

System Services

DNS      SSH/SNMP      Date and Time

System Time: 4/4/2025 17:33:07

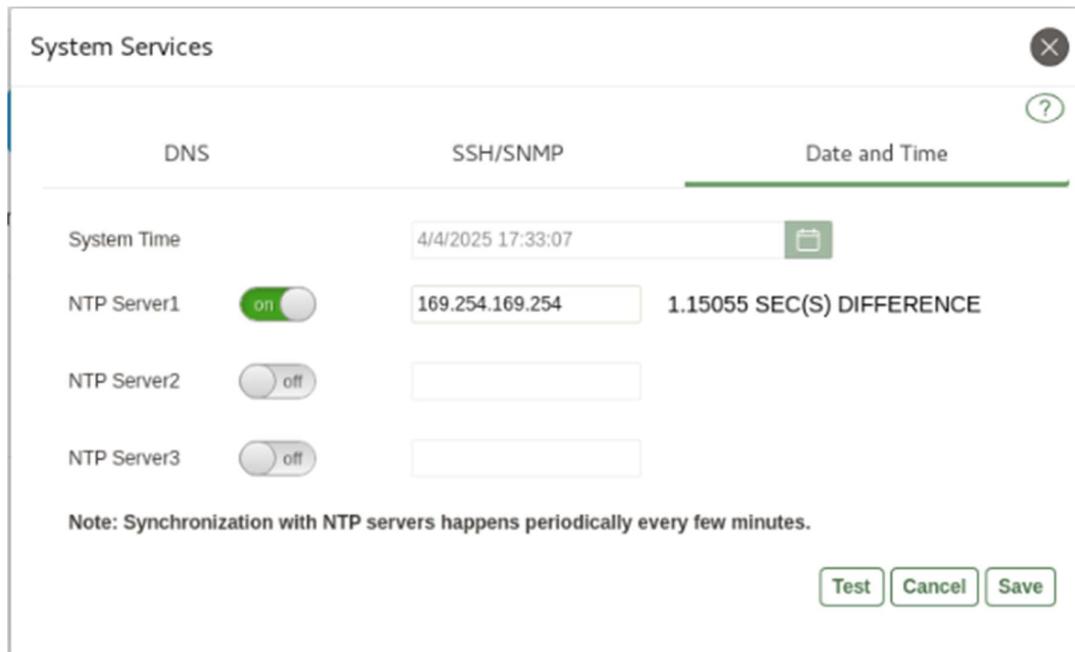
NTP Server1: On (169.254.169.254) - 1.15055 SEC(S) DIFFERENCE

NTP Server2: Off

NTP Server3: Off

Note: Synchronization with NTP servers happens periodically every few minutes.

Test    Cancel    Save



- 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

Defined Database Firewall Policies			
Policy Name	Target Type	Deployed on Targets	Description
<input type="checkbox"/> Default	All	pdb1	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.
<input type="checkbox"/> Log all	All		Log all SQL statements.
<input type="checkbox"/> Log all - no mask	All		Log all SQL statements without masking data.
<input type="checkbox"/> Log sample	All		Log every tenth SQL statement for a cluster.
<input checked="" type="checkbox"/> Log unique	All		Logs unique SQL statements across sessions for all the tables and views.
<input type="checkbox"/> Log unique - no mask	All		Same as Log unique, but without masking any data.
<input type="checkbox"/> Pass all	All		Pass all statements, do not log them.

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

## Bài thực hành số 03: Database Security

Deploy Policy

Policy Name: Log unique ?

Target Type: Oracle Database ▼

Select Targets to deploy

Go Actions ▾

	Target Name
<input type="checkbox"/>	pdb1

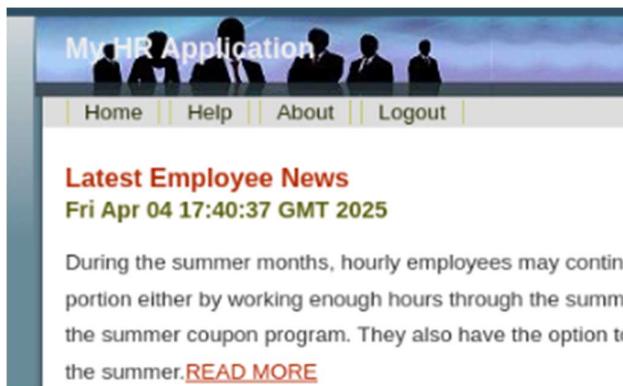
1 - 1 of 1

Cancel Deploy

- Chọn Target Name là pdb1 và chọn Deploy

Policy Name	Target Type	Deployed on Targets	Description
<input type="checkbox"/> 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.
<input type="checkbox"/> Log all	All		Log all SQL statements.
<input type="checkbox"/> Log all - no mask	All		Log all SQL statements without masking data.
<input type="checkbox"/> Log sample	All		Logs every tenth SQL statement for a cluster.
<input type="checkbox"/> Log unique	All	pdb1	Logs unique SQL statements across sessions for all the tables and views.
<input type="checkbox"/> Log unique - no mask	All		Same as Log unique, but without masking any data.
<input type="checkbox"/> 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

## Bài thực hành số 03: Database Security

### 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
400	Anderson, Jason	Full-time	Regional Manager		102	Engineering	Paris

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

## Bài thực hành số 03: Database Security

Search Employee

HR ID	196	Active	Active
Employee Type	-- Choose a value --	Position	Administrator
First Name	William	Last Name	Harvey
Department	Marketing	Location	London

Debug:

Yes

---

Search Result

HR ID	Full Name	Emp Type	Position	Manager	Cost Center	Department	Location
196	<a href="#">Harvey, William</a>	Full-time	Administrator		103	Marketing	London

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

## Bài thực hành số 03: Database Security

### Employee Profile

Identity	Supplemental Data	Organization	Communication
HR ID	196		
Full Name	Harvey, William		
SSN / SIN / NINO	342-53-6218		
Date of Birth	1967-12-08 00:00:00.0		
Address	23 Sommers Street PA, 19131		
Corporate Card / Expiration	340720701206429 / 2016-02-01 00:00:00.0		
Employee Type	Full-time		
Position	Administrator		
Location	London		
Salary	519.14		
Active	 Yes, Active		

[Modify Employee](#)

### Direct Reports

[HR ID](#) [Full Name](#) [Emp Type](#) [Position](#) [Location](#) [Manager](#) [Cost Center](#) [Department](#) [Organization](#)

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

Event Time is in the last 24 hours								
Threat Severity	Target	User	Client Host	Client Program	Event	Object	Event Status	Event Time ↓
minimal	pdb1	EMPLOYEESEARCH_PROD	dbsec-hol-141366.pub.l141366vcn.oraclevcn.com	JDBC Thin Client	LOGOUT			4/4/2025 5:41:04 PM
minimal	pdb1	EMPLOYEESEARCH_PROD	dbsec-hol-141366.pub.l141366vcn.oraclevcn.com	JDBC Thin Client	LOGIN ATTEMPTED			4/4/2025 5:41:04 PM
minimal	pdb1	EMPLOYEESEARCH_PROD	dbsec-hol-141366.pub.l141366vcn.oraclevcn.com	JDBC Thin Client	LOGOUT			4/4/2025 5:41:04 PM
minimal	pdb1	EMPLOYEESEARCH_PROD	dbsec-hol-141366.pub.l141366vcn.oraclevcn.com	JDBC Thin Client	SELECT	DEMO_HR_ROLES		4/4/2025 5:41:04 PM
minimal	pdb1	EMPLOYEESEARCH_PROD	dbsec-hol-141366.pub.l141366vcn.oraclevcn.com	JDBC Thin Client	BEGIN			4/4/2025 5:41:04 PM
minimal	pdb1	EMPLOYEESEARCH_PROD	dbsec-hol-141366.pub.l141366vcn.oraclevcn.com	JDBC Thin Client	SELECT	DEMO_HR_USERS		4/4/2025 5:41:04 PM
minimal	pdb1	EMPLOYEESEARCH_PROD	dbsec-hol-141366.pub.l141366vcn.oraclevcn.com	JDBC Thin Client	LOGIN ATTEMPTED			4/4/2025 5:41:04 PM
minimal	pdb1	EMPLOYEESEARCH_PROD	dbsec-hol-141366.pub.l141366vcn.oraclevcn.com	JDBC Thin Client	LOGOUT			4/4/2025 5:32:05 PM
minimal	pdb1	EMPLOYEESEARCH_PROD	dbsec-hol-141366.pub.l141366vcn.oraclevcn.com	JDBC Thin Client	LOGIN ATTEMPTED			4/4/2025 5:32:05 PM
minimal	pdb1	EMPLOYEESEARCH_PROD	dbsec-hol-141366.pub.l141366vcn.oraclevcn.com	JDBC Thin Client	LOGIN ATTEMPTED			4/4/2025 5:32:00 PM
minimal	pdb1	SYSTEM	dbsec-hol-141366.pub.l141366vcn.oraclevcn.com	sqlplus@dbsec-lab (TNS V1-V3)	LOGOUT			4/4/2025 5:18:42 PM
minimal	pdb1	SYSTEM	dbsec-hol-141366.pub.l141366vcn.oraclevcn.com	sqlplus@dbsec-lab (TNS V1-V3)	LOGIN ATTEMPTED			4/4/2025 5:18:42 PM

1 - 12 of 12

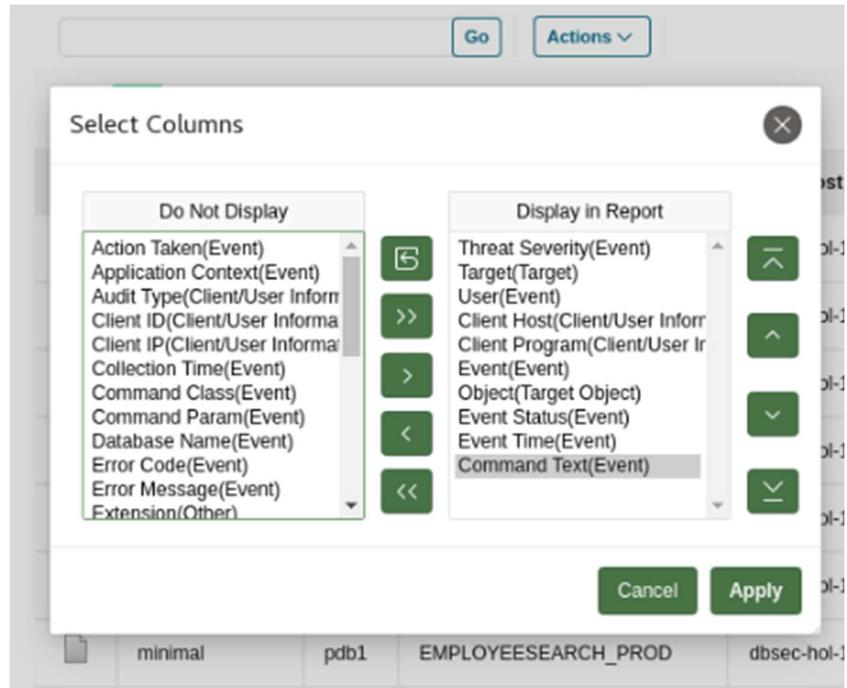
- Tiến hành kiểm tra Database Firewall Activity bằng cách chọn **Reports**, kéo xuống mục **Database Firewall Reports**, chọn mục **Monitored Activity** và có thể thấy các hoạt động truy vấn với User EMPLOYEESEARCH\_PROD với Client Program là “JDBC Thin Client”

## Bài thực hành số 03: Database Security

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:
  - o Policy Name: Log unique
  - o Threat Severity: minimal
  - o Location: Network
  - o Action Taken: Pass

## Bài thực hành số 03: Database Security



- 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.II141366vcn.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.PHONENEX, a.PHONEFAX, a.COSTCENTER, a.DEPARTMENT, a.EMPLOYEE_ID, a.GENDER, a.HIREDATE, a.MANAGERID, a.DEPARTMENT, a.ORGANIZATION, a.STARTDATE, a.ENDDATE, a.ACTIVE, a.FIRSTNAME as MGR_FIRSTNAME, a.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.FIRSTNAME
minimal	pdb1	EMPLOYEESEARCH_PROD	dbsec-hol-141366.pub.II141366vcn.oraclevcn.com	JDBC Thin Client	LOGIN_ATTEMPTED			4/4/2025 5:46:37 PM	LOGIN
minimal	pdb1	EMPLOYEESEARCH_PROD	dbsec-hol-141366.pub.II141366vcn.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.PHONENEX, 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.HIREDATE, a.DEPARTMENT, a.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.PREV_BONUS, c.NEXT_BONUS, c.NEXT_BONUS_DATE 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.II141366vcn.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**

## Bài thực hành số 03: Database Security

```
[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"

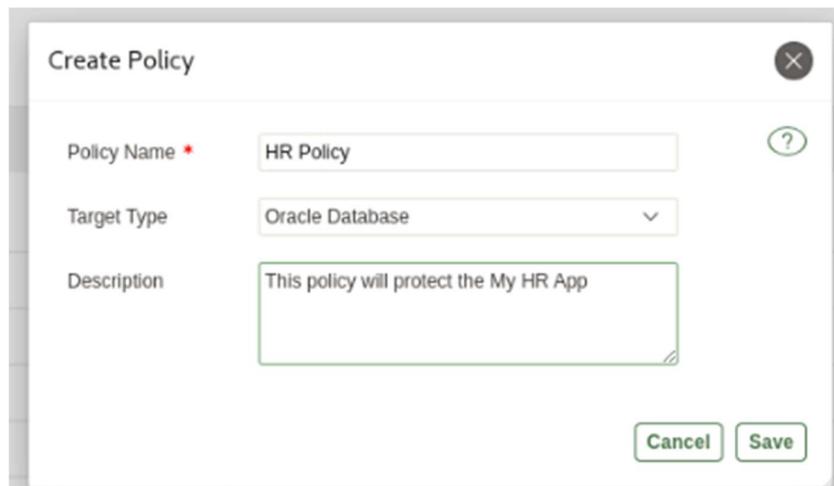
. Query EMPLOYEESEARCH_PROD.DEMO_HR_EMPLOYEES

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.

[cldb1: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**:
  - o Policy Name: HR Policy
  - o Target Type: Oracle Database
  - o Description: This policy will protect the My HR App

## Bài thực hành số 03: Database Security

Add SQL Cluster Set

Name *	HR SQL Cluster	Description	Known SQL statements for HR App
Target	pdb1	Show cluster for	Last 24 Hours
<input type="button" value="Actions"/> <input type="button" value="Go"/>			
<input type="button" value="Search"/> <input type="button" value="Actions"/>			
No SQL Cluster data found.			
<input type="button" value="Cancel"/> <input type="button" value="Save"/>			

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

Add SQL Cluster Set

Name *	HR SQL Cluster	Description	Known SQL statements for HR App																								
Target	pdb1	Show cluster for	Last 24 Hours																								
<input type="button" value="Actions"/> <input type="button" value="Go"/>																											
<input type="button" value="Search"/> <input type="button" value="Actions"/>																											
<table border="1"><thead><tr><th>SQL Statement</th><th>SQL Count</th><th>First Seen</th><th>Last Seen</th></tr></thead><tbody><tr><td>Sample SQL from Cluster</td><td></td><td></td><td></td></tr><tr><td>select USERID,FIRSTNAME,LASTNAME from DEMO_HR_USERS where (USERSTATUS is NULL or upper( USERSTATUS ) = 'A' ) and upper(USERID) = '1234567890' and password = '1234567890';</td><td>1</td><td>4/4/2025 5:41:04 PM</td><td>4/4/2025 5:41:04 PM</td></tr><tr><td>SELECT DECODE(USER, 'A', 'A', 'B', 'B', 'C', 'C', 'D', 'D', 'E', 'E', 'F', 'F', 'G', 'G', 'H', 'H', 'I', 'I', 'J', 'J', 'K', 'K', 'L', 'L', 'M', 'M', 'N', 'N', 'O', 'O', 'P', 'P', 'Q', 'Q', 'R', 'R', 'S', 'S', 'T', 'T', 'U', 'U', 'V', 'V', 'W', 'W', 'X', 'X', 'Y', 'Y', 'Z', 'Z');</td><td>1</td><td>4/4/2025 5:55:53 PM</td><td>4/4/2025 5:55:53 PM</td></tr><tr><td>BEGIN DBMS_APPLICATION_INFO.SET_MODULE(:0,NULL); END;</td><td>1</td><td>4/4/2025 5:55:53 PM</td><td>4/4/2025 5:55:53 PM</td></tr><tr><td>extracted_from_protocol transaction commit</td><td>1</td><td>4/4/2025 5:55:53 PM</td><td>4/4/2025 5:55:53 PM</td></tr></tbody></table>				SQL Statement	SQL Count	First Seen	Last Seen	Sample SQL from Cluster				select USERID,FIRSTNAME,LASTNAME from DEMO_HR_USERS where (USERSTATUS is NULL or upper( USERSTATUS ) = 'A' ) and upper(USERID) = '1234567890' and password = '1234567890';	1	4/4/2025 5:41:04 PM	4/4/2025 5:41:04 PM	SELECT DECODE(USER, 'A', 'A', 'B', 'B', 'C', 'C', 'D', 'D', 'E', 'E', 'F', 'F', 'G', 'G', 'H', 'H', 'I', 'I', 'J', 'J', 'K', 'K', 'L', 'L', 'M', 'M', 'N', 'N', 'O', 'O', 'P', 'P', 'Q', 'Q', 'R', 'R', 'S', 'S', 'T', 'T', 'U', 'U', 'V', 'V', 'W', 'W', 'X', 'X', 'Y', 'Y', 'Z', 'Z');	1	4/4/2025 5:55:53 PM	4/4/2025 5:55:53 PM	BEGIN DBMS_APPLICATION_INFO.SET_MODULE(:0,NULL); END;	1	4/4/2025 5:55:53 PM	4/4/2025 5:55:53 PM	extracted_from_protocol transaction commit	1	4/4/2025 5:55:53 PM	4/4/2025 5:55:53 PM
SQL Statement	SQL Count	First Seen	Last Seen																								
Sample SQL from Cluster																											
select USERID,FIRSTNAME,LASTNAME from DEMO_HR_USERS where (USERSTATUS is NULL or upper( USERSTATUS ) = 'A' ) and upper(USERID) = '1234567890' and password = '1234567890';	1	4/4/2025 5:41:04 PM	4/4/2025 5:41:04 PM																								
SELECT DECODE(USER, 'A', 'A', 'B', 'B', 'C', 'C', 'D', 'D', 'E', 'E', 'F', 'F', 'G', 'G', 'H', 'H', 'I', 'I', 'J', 'J', 'K', 'K', 'L', 'L', 'M', 'M', 'N', 'N', 'O', 'O', 'P', 'P', 'Q', 'Q', 'R', 'R', 'S', 'S', 'T', 'T', 'U', 'U', 'V', 'V', 'W', 'W', 'X', 'X', 'Y', 'Y', 'Z', 'Z');	1	4/4/2025 5:55:53 PM	4/4/2025 5:55:53 PM																								
BEGIN DBMS_APPLICATION_INFO.SET_MODULE(:0,NULL); END;	1	4/4/2025 5:55:53 PM	4/4/2025 5:55:53 PM																								
extracted_from_protocol transaction commit	1	4/4/2025 5:55:53 PM	4/4/2025 5:55:53 PM																								
1 - 14 of 14																											
<input type="button" value="Cancel"/> <input type="button" value="Save"/>																											

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

## Bài thực hành số 03: Database Security

Add SQL Cluster Set

Name *	Target	Description	Show cluster for	Actions												
HR SQL Cluster	pdb1	Known SQL statements for HR App	Last 24 Hours	<input type="button" value="Go"/>												
<table border="1"><thead><tr><th colspan="2">Actions</th></tr></thead><tbody><tr><td><input checked="" type="checkbox"/> extracted_from_protocol transaction commit</td><td>1 4/4/2025 5:55:53 PM</td></tr><tr><td><input checked="" type="checkbox"/> BEGIN DBMS_OUTPUT.ENABLE(NULL); END;</td><td>1 4/4/2025 5:55:53 PM</td></tr><tr><td><input type="checkbox"/> select userid, firstname, lastname, emptye, position, city, ssn, sin, nino from employeesearch_prod.demo_hr_employees where rownum &lt; 00</td><td>1 4/4/2025 5:55:53 PM</td></tr><tr><td><input checked="" type="checkbox"/> BEGIN dbms_session.set_identifier(0); END;</td><td>1 4/4/2025 5:41:04 PM</td></tr><tr><td colspan="2">-----</td></tr></tbody></table>					Actions		<input checked="" type="checkbox"/> extracted_from_protocol transaction commit	1 4/4/2025 5:55:53 PM	<input checked="" type="checkbox"/> BEGIN DBMS_OUTPUT.ENABLE(NULL); END;	1 4/4/2025 5:55:53 PM	<input type="checkbox"/> select userid, firstname, lastname, emptye, position, city, ssn, sin, nino from employeesearch_prod.demo_hr_employees where rownum < 00	1 4/4/2025 5:55:53 PM	<input checked="" type="checkbox"/> BEGIN dbms_session.set_identifier(0); END;	1 4/4/2025 5:41:04 PM	-----	
Actions																
<input checked="" type="checkbox"/> extracted_from_protocol transaction commit	1 4/4/2025 5:55:53 PM															
<input checked="" type="checkbox"/> BEGIN DBMS_OUTPUT.ENABLE(NULL); END;	1 4/4/2025 5:55:53 PM															
<input type="checkbox"/> select userid, firstname, lastname, emptye, position, city, ssn, sin, nino from employeesearch_prod.demo_hr_employees where rownum < 00	1 4/4/2025 5:55:53 PM															
<input checked="" type="checkbox"/> BEGIN dbms_session.set_identifier(0); END;	1 4/4/2025 5:41:04 PM															
-----																
1 - 14 of 14																
<input type="button" value="Cancel"/> <input type="button" value="Save"/>																

- 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)

SQL Statement

Rule Name *	Profile	Description	Cluster Set(s) *												
Allows HR SQL	-	Allowed SQL statements for HR App	Search clusters												
<table border="1"><thead><tr><th>Available</th><th>Selected</th></tr></thead><tbody><tr><td><input type="checkbox"/> HR SQL Cluster</td><td><input checked="" type="checkbox"/> HR SQL Cluster</td></tr><tr><td><input type="checkbox"/> &gt;&gt;</td><td><input type="checkbox"/> &gt;&gt;</td></tr><tr><td><input type="checkbox"/> &gt;</td><td><input type="checkbox"/> &gt;</td></tr><tr><td><input type="checkbox"/> &lt;</td><td><input type="checkbox"/> &lt;</td></tr><tr><td><input type="checkbox"/> &lt;&lt;</td><td><input type="checkbox"/> &lt;&lt;</td></tr></tbody></table>				Available	Selected	<input type="checkbox"/> HR SQL Cluster	<input checked="" type="checkbox"/> HR SQL Cluster	<input type="checkbox"/> >>	<input type="checkbox"/> >>	<input type="checkbox"/> >	<input type="checkbox"/> >	<input type="checkbox"/> <	<input type="checkbox"/> <	<input type="checkbox"/> <<	<input type="checkbox"/> <<
Available	Selected														
<input type="checkbox"/> HR SQL Cluster	<input checked="" type="checkbox"/> HR SQL Cluster														
<input type="checkbox"/> >>	<input type="checkbox"/> >>														
<input type="checkbox"/> >	<input type="checkbox"/> >														
<input type="checkbox"/> <	<input type="checkbox"/> <														
<input type="checkbox"/> <<	<input type="checkbox"/> <<														
<table border="1"><thead><tr><th>Action</th><th>Logging Level</th><th>Threat Severity</th></tr></thead><tbody><tr><td>Action: Pass</td><td>Logging Level: Don't Log</td><td>Threat Severity: Minimal</td></tr><tr><td colspan="3"><input type="checkbox"/> Set threshold for escalating action</td></tr></tbody></table>				Action	Logging Level	Threat Severity	Action: Pass	Logging Level: Don't Log	Threat Severity: Minimal	<input type="checkbox"/> Set threshold for escalating action					
Action	Logging Level	Threat Severity													
Action: Pass	Logging Level: Don't Log	Threat Severity: Minimal													
<input type="checkbox"/> Set threshold for escalating action															
<input type="button" value="Cancel"/> <input type="button" value="Save"/>															

## 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:
  - o Rule Name: Allows HR SQL
  - o Description: Allowed SQL statements for HR App
  - o Cluster Set(s): HR SQL Cluster
  - o Action: Pass
  - o Logging Level: Don't Log
  - o Threat Severity: Minimal

The screenshot shows the 'Default' rule configuration screen. It includes fields for Action (set to Block), Logging Level (One-Per-Session), Threat Severity (Moderate), and a Substitution SQL field containing the query 'SELECT 100 FROM dual WHERE 1=2'. At the bottom right are 'Cancel' and 'Save' buttons.

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

The screenshot shows the 'HR Policy' configuration screen. It includes fields for Policy Name (HR Policy), Description (This policy will protect the My HR App), and Target Type (Oracle Database). Below this, the 'Database Firewall Policy Rules' section shows a table for the 'Default' rule. The table has columns: Rule Name, Profile Name, Cluster Sets, Action, Logging Level, Threat Severity, and Description. The 'Default' rule entry is: Rule Name: Allows HR SQL, Profile Name: -, Cluster Sets: HR SQL Cluster, Action: Pass, Logging Level: One-Per-Session, Threat Severity: Minimal, Description: Allowed SQL statements for HR App. At the bottom left, there are sections for Database Objects (0) and Default. The 'Default' section shows a table with one row: Rule Name: Default Rule, Action: Block, Logging Level: One-Per-Session, Threat Severity: Moderate, and Description: Applies to a SQL statement that does not match the rules defined in Session Context, SQL Statement or Database Objects rule.

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

The screenshot shows the 'User-defined Database Firewall Policies' list screen. It includes a table with columns: Policy Name, Deployment Status, Target Type, Deployed on Targets, and Description. The table shows one row: Policy Name: HR Policy, Deployment Status: Not deployed, Target Type: Oracle Database, Deployed on Targets: -, Description: This policy will protect the My HR App. At the top right are buttons for Create, Delete, Copy, Deploy, Import, and Export.

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

## Bài thực hành số 03: Database Security

Deploy Policy

Policy Name: HR Policy

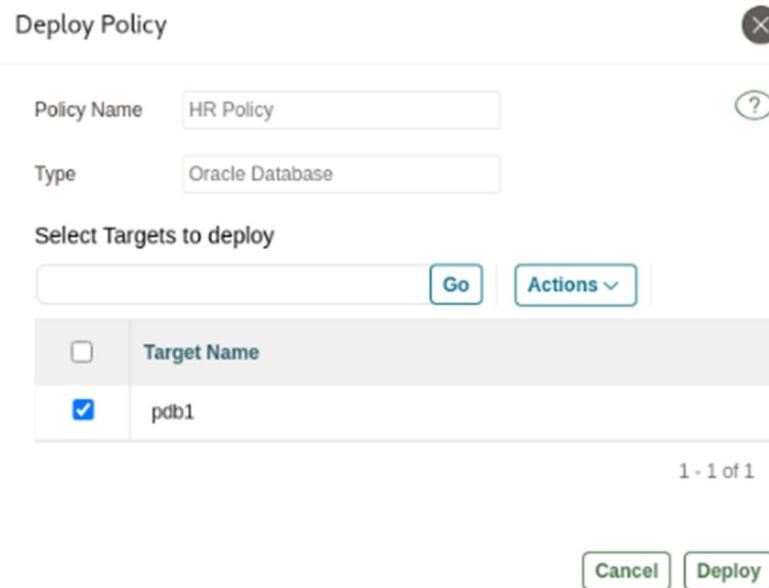
Type: Oracle Database

Select Targets to deploy

	Target Name
<input type="checkbox"/>	pdb1

1 - 1 of 1

**Cancel** **Deploy**



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

User-defined Database Firewall Policies				
		Go	Actions	
<input type="checkbox"/>	Policy Name	Deployment Status	Target Type	Deployed on Targets
<input type="checkbox"/>	HR Policy	Deployed	Oracle Database	pdb1

Create Delete Copy Deploy Import Export

This policy will protect the My HR App

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

## Bài thực hành số 03: Database Security

Home || Help || About || Logout

### Search Employee

HR ID	<input type="text"/>	Active	<input type="button" value="-- Choose a value --"/>
Employee Type	<input type="button" value="-- Choose a value --"/>	Position	<input type="text"/>
First Name	<input type="text"/>	Last Name	<input type="text"/>
Department	<input type="text"/>	Location	<input type="text"/>

**Debug:**

Yes

---

### Search Result

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

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

Home || Help || About || Logout

### Search Employee

HR ID	<input type="text" value="196"/>	Active	<input type="button" value="-- Choose a value --"/>
Employee Type	<input type="button" value="-- Choose a value --"/>	Position	<input type="text"/>
First Name	<input type="text"/>	Last Name	<input type="text"/>
Department	<input type="text"/>	Location	<input type="text"/>

**Debug:**

Yes

---

### Search Result

HR ID	Full Name	Emp Type	Position	Manager	Cost Center	Department	Location	
196	<a href="#">Harvey, William</a>	Full-time	Administrator		103	Marketing	London	

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

## Bài thực hành số 03: Database Security

```
[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)

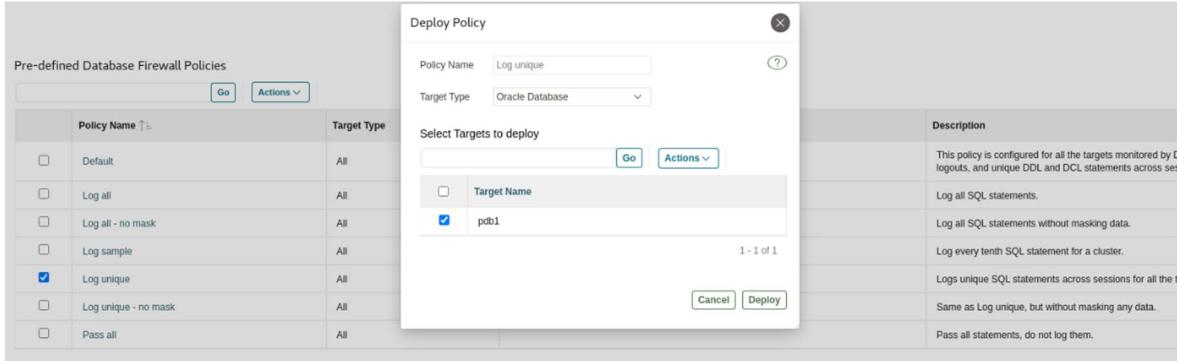
$ sqlplus -s system/Oracle123@pdb1.proxy
USER is "EMPLOYEESEARCH_PROD"

. 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

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.
<b>Log unique</b>	All	<b>pdb1</b>	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.

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

## Bài thực hành số 03: Database Security

**Search Employee**

HR ID	<input type="text"/>	Active	<input type="button" value="... Choose a value .."/>
Employee Type	<input type="button" value="-- Choose a value --"/>	Position	<input type="text"/>
First Name	<input type="text"/>	Last Name	<input type="text"/>
Department	<input type="text"/>	Location	<input type="text"/>

**Debug:**

Yes

---

**Search Result**

```
select a.USERID, a.FIRSTNAME, a.LASTNAME, a.EMAIL, a.PHONEMOBILE, a.PHONEFIX,
a.PHONEFAX, a.EMPTYTYPE, 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	<a href="#">Adams, Cynthia</a>	Part-Time	Clerk		102	Engineering	Toronto	
200	<a href="#">Adams, Frank</a>	Full-time	Regional Manager		104	Marketing	Berlin	
66	<a href="#">Adams, Jack</a>	Full-time	Administrator		101	Engineering	London	
110	<a href="#">Adams, Johnny</a>	Part-Time	Administrator		104	Corporate	Santa Clara	
618	<a href="#">Adams, Joseph</a>	Full-time	Regional Manager		103	Sales	Santa Clara	
323	<a href="#">Adams, Julie</a>	Part-Time	Clerk		101	Marketing	Paris	
529	<a href="#">Adams, Marie</a>	Part-Time	Clerk		103	Sales	New York	
418	<a href="#">Adams, Paula</a>	Full-time	Project Manager		101	Engineering	Toronto	
528	<a href="#">Adams, Todd</a>	Full-time	Administrator		103	Sales	Sunnyvale	
195	<a href="#">Alexander, Lisa</a>	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	<input type="text"/>	Active	<input type="button" value="... Choose a value .."/>
Employee Type	<input type="button" value="-- Choose a value --"/>	Position	<input type="text" value="UNION SELECT userid, 'ID: "/> "/>
First Name	<input type="text"/>	Last Name	<input type="text"/>
Department	<input type="text"/>	Location	<input type="text"/>

**Debug:**

Yes

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

## Bài thực hành số 03: Database Security

**Search Employee**

HR ID	<input type="text"/>	Active	-- Choose a value --
Employee Type	-- Choose a value --	Position	'UNION SELECT userid, 'ID:
First Name	<input type="text"/>	Last Name	<input type="text"/>
Department	<input type="text"/>	Location	<input type="text"/>

**Debug:**

Yes

**Search Result**

```
select a.USERID, a.FIRSTNAME, a.LASTNAME, a.EMAIL, a.PHONEMOBILE, a.PHONEFIX,
a.PHONEFAX, a.EMPTYTYPE, 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 and upper(a.POSITION)
like " UNION SELECT USERID, 'ID: '|| MEMBER_ID, 'SQLI', '1', '1', '1', '1', '1', '1', '0', '0',
PAYMENT_ACCT_NO, ROUTING_NUMBER, SYSDATE, SYSDATE, '0', '1', '1', '1', '1' FROM
DEMO_HR_SUPPLEMENTAL_DATA --%" order by a.LASTNAME, a.FIRSTNAME
```

HR ID	Full Name	Emp Type	Position	Manager	Cost Center	Department	Location
4	<a href="#">SQLI_ID: RN 96 47 58 X</a>	1	1		1	1454-3925-9102-3568	332192865
5	<a href="#">SQLI_ID: 744-659-915</a>	1	1		1	8539-4181-7647-8725	493461060
6	<a href="#">SQLI_ID: 885-454-026</a>	1	1		1	1968-8970-1464-5589	331220506
9	<a href="#">SQLI_ID: 720-504-939</a>	1	1		1	2750-9886-9436-6312	235788879
16	<a href="#">SQLI_ID: 939-356-156</a>	1	1		1	8147-4329-6331-9180	480106506
24	<a href="#">SQLI_ID: 702-030-252</a>	1	1		1	6972-7068-7888-9460	839970713
25	<a href="#">SQLI_ID: 978-082-246</a>	1	1		1	9308-0830-2027-0793	232911910
38	<a href="#">SQLI_ID: 522-254-799</a>	1	1		1	1259-6923-9413-3280	60595859
44	<a href="#">SQLI_ID: 885-532-397</a>	1	1		1	3972-8946-2224-2995	332983507
46	<a href="#">SQLI_ID: AR 94 55 50 N</a>	1	1		1		448620591
49	<a href="#">SQLI_ID: 985-264-433</a>	1	1		1	6337-1693-1767-3981	506241614
54	<a href="#">SQLI_ID: 140 10 200</a>	*	*	*	*	6337-1693-1767-3981	506241614

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

User-defined Database Firewall Policies					<a href="#">Create</a> <a href="#">Delete</a> <a href="#">Copy</a> <a href="#">Deploy</a> <a href="#">Import</a> <a href="#">Export</a>
<a href="#">Go</a> Actions					
<input type="checkbox"/>	Policy Name	Deployment Status	Target Type	Deployed on Targets	Description
<input checked="" type="checkbox"/>	HR Policy	Not deployed	Oracle Database	-	This policy will protect the My HR App

1 - 1 of 1

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

User-defined Database Firewall Policies					<a href="#">Create</a> <a href="#">Delete</a> <a href="#">Copy</a> <a href="#">Deploy</a> <a href="#">Import</a> <a href="#">Export</a>
<a href="#">Go</a> Actions					
<input type="checkbox"/>	Policy Name	Deployment Status	Target Type	Deployed on Targets	Description
<input checked="" type="checkbox"/>	HR Policy	Not deployed	Oracle Database	-	This policy will protect the My HR App

Pre-defined Database Firewall Policies

<a href="#">Go</a> Actions	Policy Name	Target Type	Deployed on Targets	Description
<input type="checkbox"/>	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.
<input type="checkbox"/>	Log all	All	-	Log all SQL statements.
<input type="checkbox"/>	Log all - no mask	All	-	Log all SQL statements without masking data.
<input type="checkbox"/>	Log sample	All	-	Log every tenth SQL statement for a cluster.
<input type="checkbox"/>	Log unique	All	-	Logs unique SQL statements across sessions for all the tables and views.
<input type="checkbox"/>	Log unique - no mask	All	-	Same as Log unique, but without masking any data.

Deploy Policy

Policy Name: HR Policy

Type: Oracle Database

Select Targets to deploy

Target Name: pdb1

[Cancel](#) [Deploy](#)

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

## Bài thực hành số 03: Database Security

User-defined Database Firewall Policies					<a href="#">Create</a> <a href="#">Delete</a> <a href="#">Copy</a> <a href="#">Deploy</a> <a href="#">Import</a> <a href="#">Export</a>
<input type="checkbox"/>	Policy Name	Deployment Status	Target Type	Deployed on Targets	Description
<input type="checkbox"/>	HR Policy	Deployed	Oracle Database	pdb1	This policy will protect the My HR App

1 - 1 0

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

**Search Employee**

HR ID	<input type="text"/>	Active	<input type="button" value="... Choose a value ..."/>
Employee Type	<input type="button" value="... Choose a value ..."/>	Position	' UNION SELECT userid, ' ID
First Name	<input type="text"/>	Last Name	<input type="text"/>
Department	<input type="text"/>	Location	<input type="text"/>

**Debug:**

Yes

---

**Search Result**

```
select a.USERID, a.FIRSTNAME, a.LASTNAME, a.EMAIL, a.PHONEMOBILE, a.PHONEFIX,  
a.PHONEFAX, a.EMPTYTYPE, 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 and upper(a.POSITION)  
like " UNION SELECT USERID, ' ID: '|| MEMBER_ID, 'SQLI', '1', '1', '1', '1', '1', '0, 0,  
PAYMENT_ACT_NO, ROUTING_NUMBER, SYSDATE, SYSDATE, '0', '1', '1', '1', 1 FROM  
DEMO_HR_SUPPLEMENTAL_DATA --%" order by a.LASTNAME, a.FIRSTNAME
```

HR ID	Full Name	Emp Type	Position	Manager	Cost Center	Department	Location
-------	-----------	----------	----------	---------	-------------	------------	----------

My HR Application | My Intranet | My Self-Service  
Copyright © My HR Application 2008

- 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

**Create Policy**

Policy Name *	<input type="text" value="PII Exfiltration Monitor"/>	<a href="#">?</a>
Target Type	<input type="button" value="Oracle Database"/>	
Description	This policy will monitor the PII exfiltration attempts	
<input type="button" value="Cancel"/> <input type="button" value="Save"/>		

- Tiến hành tạo Policy với các thông tin sau và lưu lại:

- o Policy Name: PII Exfiltration Monitor
- o Target Type: Oracle Database
- o Description: This policy will monitor the PII exfiltration attempts

## Bài thực hành số 03: Database Security

The screenshot shows the 'Database Objects' configuration page for a new rule named 'PII Table Monitor'. The 'Commands' section lists various DDL and DML statements. The 'Selected' column includes 'SELECT', 'INSERT', 'DELETE', and 'UPDATE'. A toggle switch indicates 'Capture number of rows returned for SELECT queries' is set to 'Yes'. The 'Action to be taken' section shows 'Action: Pass', 'Logging Level: Always', and 'Threat Severity: Moderate'. Buttons for 'Cancel' and 'Save' are at the bottom right.

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

The screenshot shows the 'Deploy Policy' dialog box for the 'PII Exfiltration Monitor' policy. It lists the target 'Target Name: pdb1'. The main interface shows a table of pre-defined policies like 'Default', 'Log all', etc., and their descriptions. A note at the bottom right says '1 - 2 of 2'.

- Tiến hành triển khai PII Exfiltration Monitor lên pdb1

## Bài thực hành số 03: Database Security

User-defined Database Firewall Policies				
<input type="checkbox"/>	Policy Name	Deployment Status	Target Type	Deployed on Targets
<input type="checkbox"/>	PII Exfiltration Monitor	Deployed	Oracle Database	pdb1
<input type="checkbox"/>	HR Policy	Not deployed	Oracle Database	-

1 - 2 of 2

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

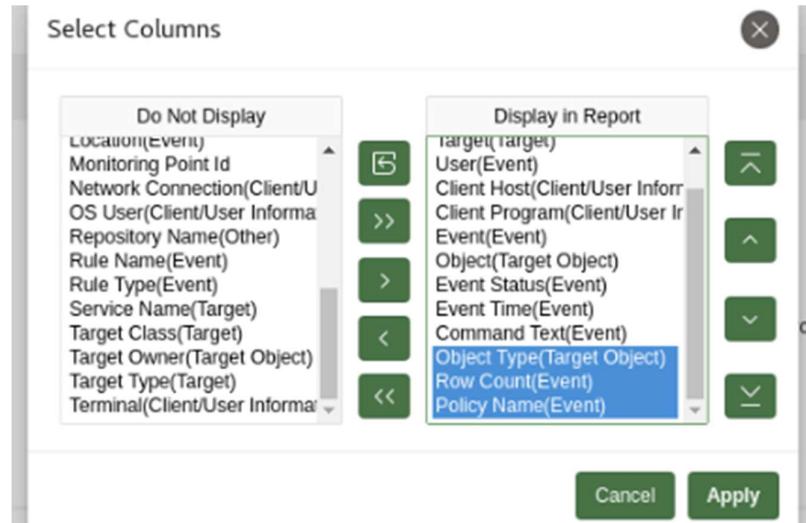
```
[cdb1:oracle@dbsec-lab:~/DBSecLab/livelabs/avdf/dbf]$ ./dbf_exfiltrate_with_dbfw.sh
```

USERID	FIRSTNAME	LASTNAME
964	George	Young
964	George	Young
612	Harold	Young
612	Harold	Young

```
122 rows selected.
```

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

- Tiến hành mở Terminal, chạy script dbf\_exfiltrate\_with\_dbfw.sh để trích xuất thông tin thử



- Trong Database Firewall Reports, tiến hành the

## Bài thực hành số 03: Database Security

Threat Severity	Target	User	Client Host	Client Program	Event	Object	Event Status	Event Time	Object Type	Row Count	Policy Name
moderate	pd1	EMPLOYEESEARCH_PROD	dbsec-hol-141366 pub.ii141366vcn.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	pd1	EMPLOYEESEARCH_PROD	dbsec-hol-141366 pub.ii141366vcn.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	pd1	EMPLOYEESEARCH_PROD	dbsec-hol-141366 pub.ii141366vcn.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	pd1	EMPLOYEESEARCH_PROD	dbsec-hol-141366 pub.ii141366vcn.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	pd1	EMPLOYEESEARCH_PROD	dbsec-hol-141366 pub.ii141366vcn.oraclevcn.com	sqlplus@dbsec-lab (TNS V1-V3)	SELECT	DUAL		4/4/2025 6:47:35 PM	TABLE	-1	PII Exfiltration Monitor
moderate	pd1	EMPLOYEESEARCH_PROD	dbsec-hol-141366 pub.ii141366vcn.oraclevcn.com	sqlplus@dbsec-lab (TNS V1-V3)	SELECT	DUAL	SUCCESS	4/4/2025 6:47:35 PM	TABLE	1	PII Exfiltration Monitor
moderate	pd1	EMPLOYEESEARCH_PROD	dbsec-hol-141366 pub.ii141366vcn.oraclevcn.com	JDBC Thin Client	SELECT	DEMO_HR_EMPLOYEES		4/4/2025 6:30:39 PM	TABLE		HR Policy
moderate	nvth1	FMDI_OYFFSEARCH_PROD	dbsec-hol-	INRC 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

OD	USERID	FIRSTNAME	LASTNAME
OD			EMAIL
OD	894	Martin	Welch
OD	Martin.Welch@oracledemo.com		1-(412)760-5458
OD	488	Joseph	West
OD	Joseph.West@oracledemo.com		
OD	826	Beverly	Young
OD	Beverly.Young@oracledemo.com		1-(901)461-5522
OD	USERID	FIRSTNAME	LASTNAME
OD			EMAIL
OD	964	George	Young
OD	George.Young@oracledemo.com		1-(916)254-0088
OD	612	Harold	Young
OD	Harold.Young@oracledemo.com		1-(678)643-2538
OD	122 rows selected.		

<input checked="" type="checkbox"/>	Alert ID	Alert status	Alert policy name	Alert severity	Alert time	Target	User	Event
<input type="checkbox"/>	205	Open	PII Exfiltration Alert	Warning	4/4/2025 6:50:59 PM	pd1	EMPLOYEESEARCH_PROD	SELECT
<input type="checkbox"/>	204	Open	PII Exfiltration Alert	Warning	4/4/2025 6:50:59 PM	pd1	EMPLOYEESEARCH_PROD	SELECT
<input type="checkbox"/>	203	Open	Database Firewall Alert	Warning	4/4/2025 6:33:59 PM	pd1	EMPLOYEESEARCH_PROD	SELECT
<input type="checkbox"/>								

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

## Bài thực hành số 03: Database Security

Alert Reports >> Alert details for Alert ID : 205

Set alert status

Alert status	Open	Threshold
Policy name	PII Exfiltration Alert	Duration (in minutes)
Description	Someone has selected more than 100 rows of PII in a single query	Group by
Severity	Warning	USER_NAME
Condition	:ROW_COUNT > 100 and :OBJECT like '%DEMO_HR%'	Alert time
4/4/2025 6:50:59 PM		

Events

	Target	User	Client host	Client program	Event	Object	Event status	Event time
	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

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

Target	pdb1
Target type	Database
Location	Network
User	EMPLOYEESEARCH_PROD
OS user	oracle
Client host	dbsec-hol-141366.pub.ll141366vcn.oraclevcn.com
Client ip	10.0.0.150
Client program	sqlplus@dbsec-lab (TNS V1-V3)
Client id	
Event	SELECT
Action	SELECT
Command text	select a.USERID, a.FIRSTNAME, a.LASTNAME, a.EMAIL, a.PHONEMOBILE from DEMO_HR_EMPLOYEES a left outer join DEMO_HR_EMPLOYEES b on a.MANAGERID = b.USERID where 0=0 and upper(a.CITY) like '#####' order by a.LASTNAME, a.FIRSTNAME
Command param	
Application context	
Event status	SUCCESS
Event time	4/4/2025 6:47:35 PM
Object	DEMO_HR_EMPLOYEES
Object type	TABLE

HẾT