



BÁO CÁO LAB 3

Môn: An toàn mạng máy tính nâng cao

GVTH: Đỗ Thị Phương Uyên

Sinh viên thực hiện	Sinh viên 1 MSSV: 21521182 Họ tên: Nguyễn Đại Nghĩa Sinh viên 2 MSSV: 21521295 Họ tên: Phạm Hoàng Phúc Sinh viên 3 MSSV: 21521848 Họ tên: Hoàng Gia Bảo Sinh viên 4 MSSV: 21521386 Họ tên: Lê Xuân Sơn
Lớp	NT534.O21.ATCL.1
Tổng thời gian thực hiện Lab trung bình	
Phân chia công việc (nếu là nhóm)	[Sinh viên 1]: Lab 1, Lab 2, Task 1 Lab 3 [Sinh viên 2]: Task 4, 5 Lab 3 [Sinh viên 3]: Task 6, 7 Lab 3 [Sinh viên 4]: Task 2, 3 Lab 3
Link Video thực hiện (nếu có yêu cầu)	



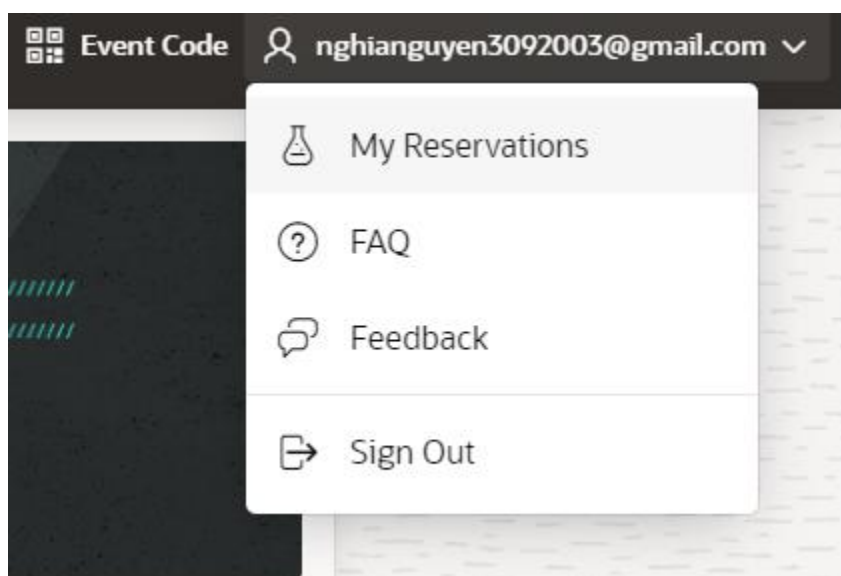
Ý kiến (nếu có) + Khó khăn gặp phải + Đề xuất, góp ý...	
Điểm tự đánh giá (bắt buộc)	9.5 /10

Lab 1: Environment Setup

Task 1: Access the Graphical Remote Desktop:

Để hoàn thành lab 1 này, em sẽ thực hiện theo hướng dẫn với các bước như sau:

Truy cập vào mục “My Reservations”:



Màn hình như sau xuất hiện:



My Reservations

All your current workshop reservations are shown below. You can edit active or pending reservations, view workshop details, attend an available workshop, or delete a reservation.

To access this right corner ar

Note: The status of your reservations will be emailed to you. Check your mail for any status updates.

DB Security - Audit Vault and DB Firewall

Sunday April 14th, 3:13am (03:13) US/Pacific



Launch Workshop

Details

Delete

Kế đến là ấn vào nút “Launch Workshop” và chọn vào “View Login Info”:

The screenshot shows the LiveLabs interface. At the top, there is a search bar with the text "Search Workshops and Sprints...". Below the search bar, the "View Login Info" button is circled in red. The main content area displays the "Introduction" section for the "DB Security - Audit Vault and DB Firewall" workshop. The left sidebar contains a list of links: "Introduction", "About this Workshop", "Acknowledgements", "Lab 1: Environment Setup", "Lab 2: Initialize Environment", "Lab 3: Audit Vault and DB Firewall (AVDF)", and "Need Help?". The main content area includes the "Introduction" heading, "About this Workshop" section, "Overview", "Estimated Time to complete the workshop: 150 minutes", and a description of the workshop. The bottom of the page shows a navigation bar with links to "OCI Data Safe Web Console" and "OEM".

Rồi chọn vào “Remote Desktop URL”:



Reservation Information



Compartment

LL81322-COMPARTMENT

Compartment OCID

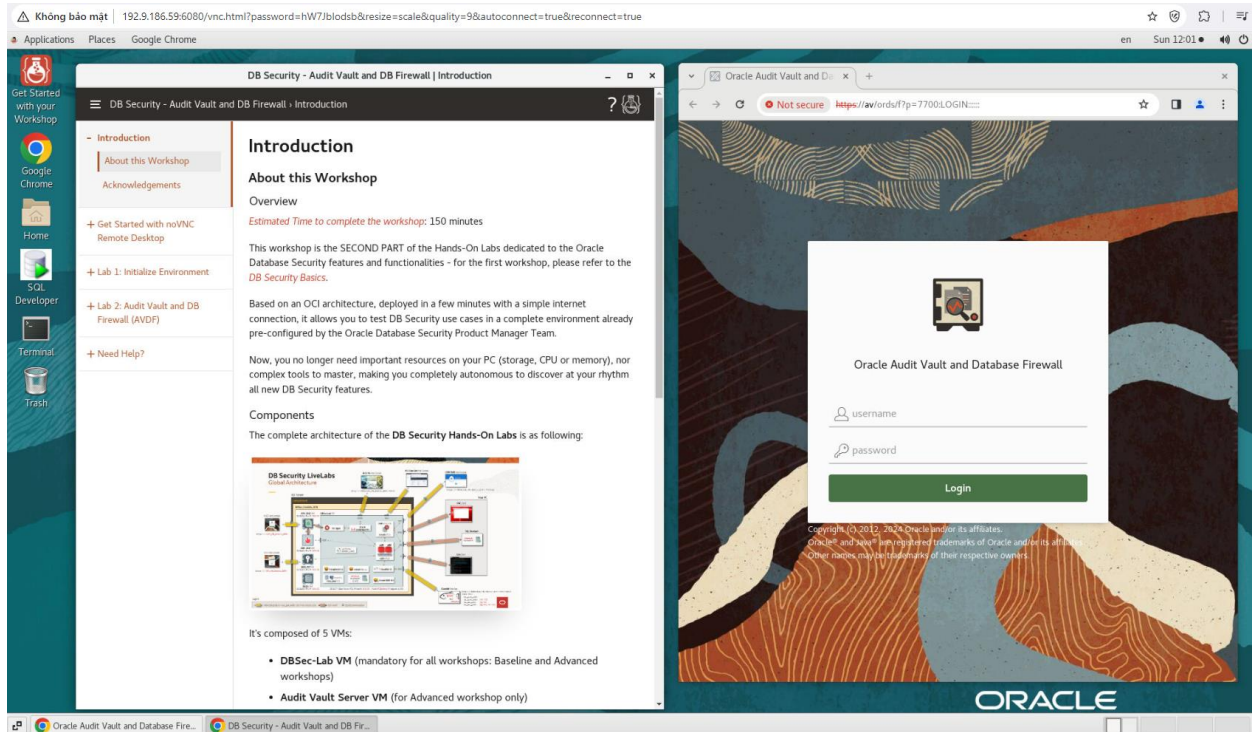
**ocid1.compartment.oc1..aaaaaaaai7kor65io
kpya2c5qhsqsp4e3reprdl6je7k5cya5viomv
kcona**

Copy Compartment OCID

Terraform Values

Host1	: dbsec-hol-81322 - 192.9.186.59	Copy value
Host2	: avs-hol-81322 - 152.67.115.108	Copy value
Host3	: dbfw-hol-81322 - 192.9.170.25	Copy value
Remote Desktop URL	: http://192.9.186.59:6080/vnc.html? password=hW7Jblodsb&resize=scale&quality=9&autoconnect=true&reconnect=true	
UI Passphrase	: 'uoNd7Y4pk:_2Own1'	Copy value

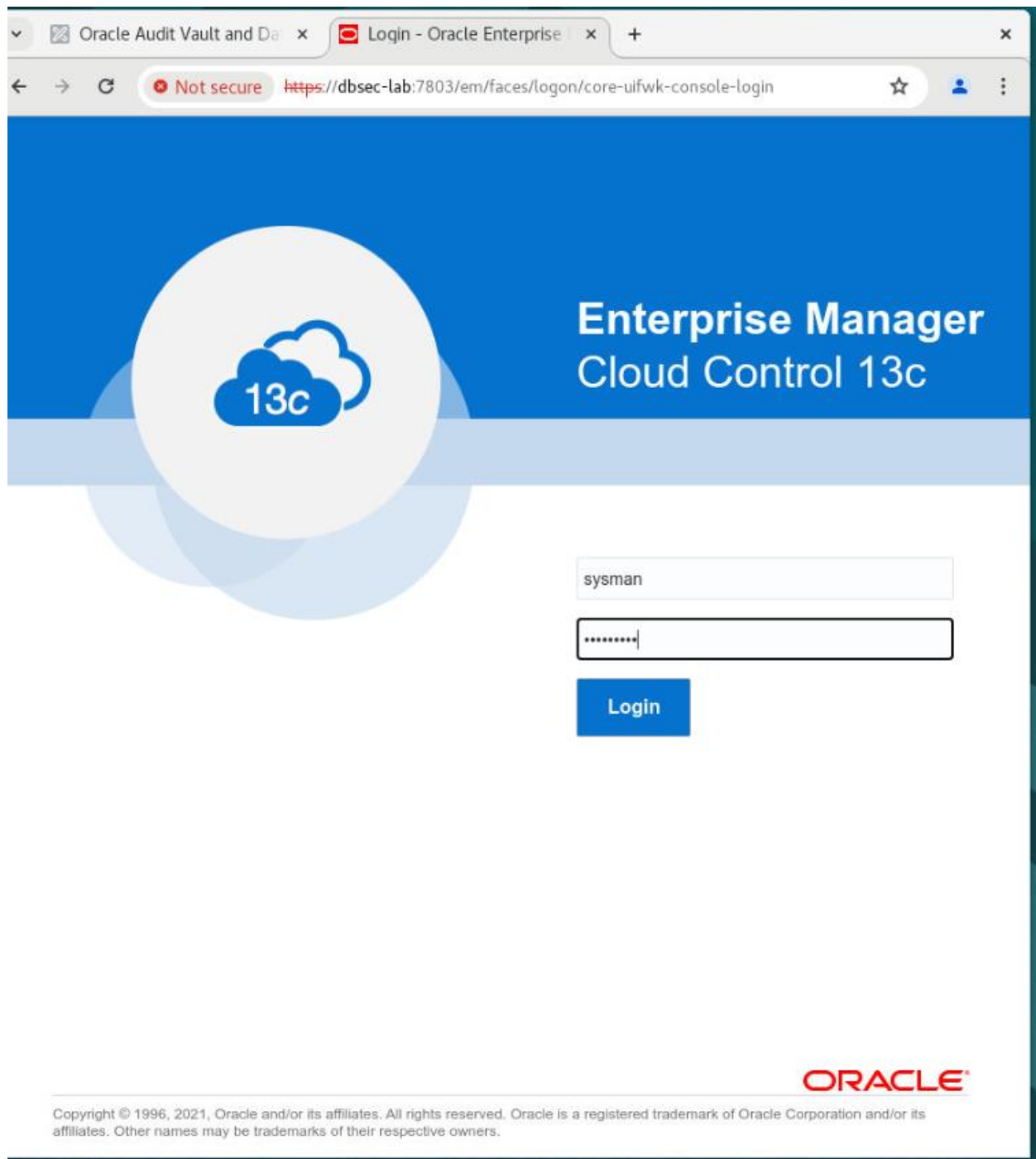
Kết quả nhận được:



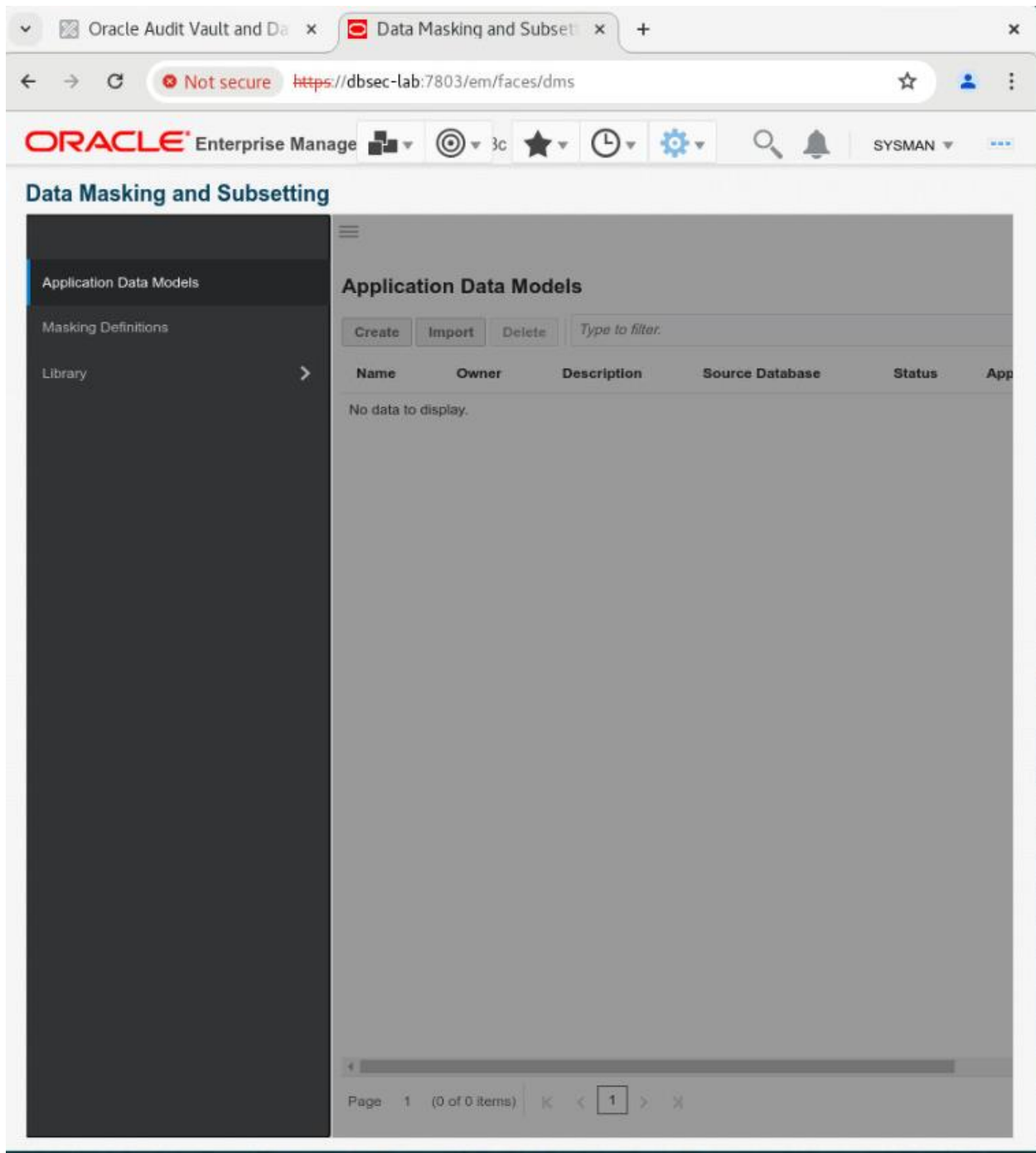
Lab 2: Initialize Environment

Task 1: Validate That Required Processes are Up and Running:

Em sẽ thực hiện đăng nhập vào Enterprise Manager với Username là sysman và Password là Oracle123:



Sau khi đăng nhập thành công, màn hình sau hiển thị:



Kế đến em thực hiện mở tab mới và chạy các đường dẫn sau để kiểm tra xem môi trường đã sẵn sàng chưa:



o PDB1

Prod: http://dbsec-lab:8080/hr_prod_pdb1

Copy

Dev: http://dbsec-lab:8080/hr_dev_pdb1

Copy

o PDB2

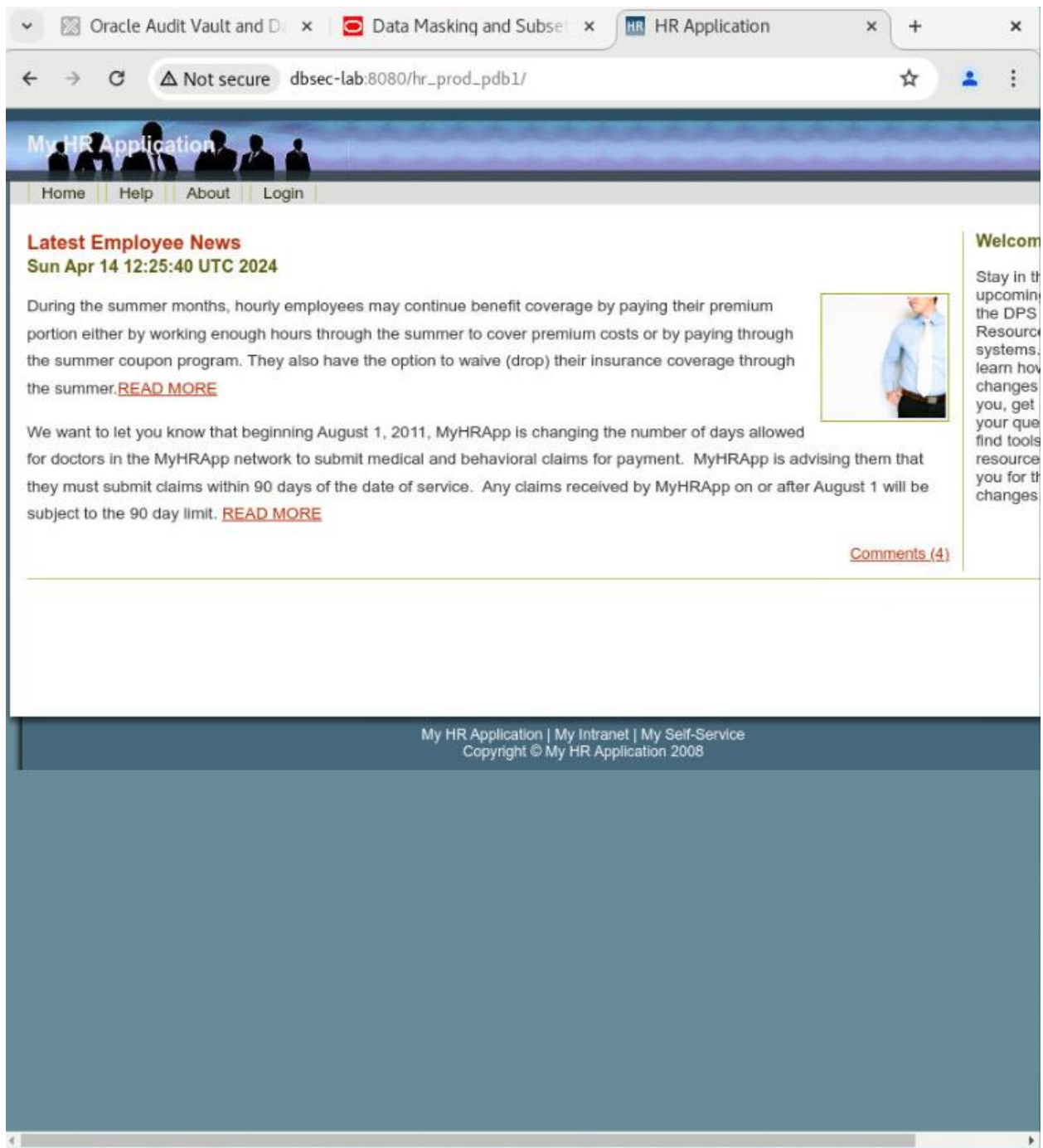
Prod: http://dbsec-lab:8080/hr_prod_pdb2

Copy

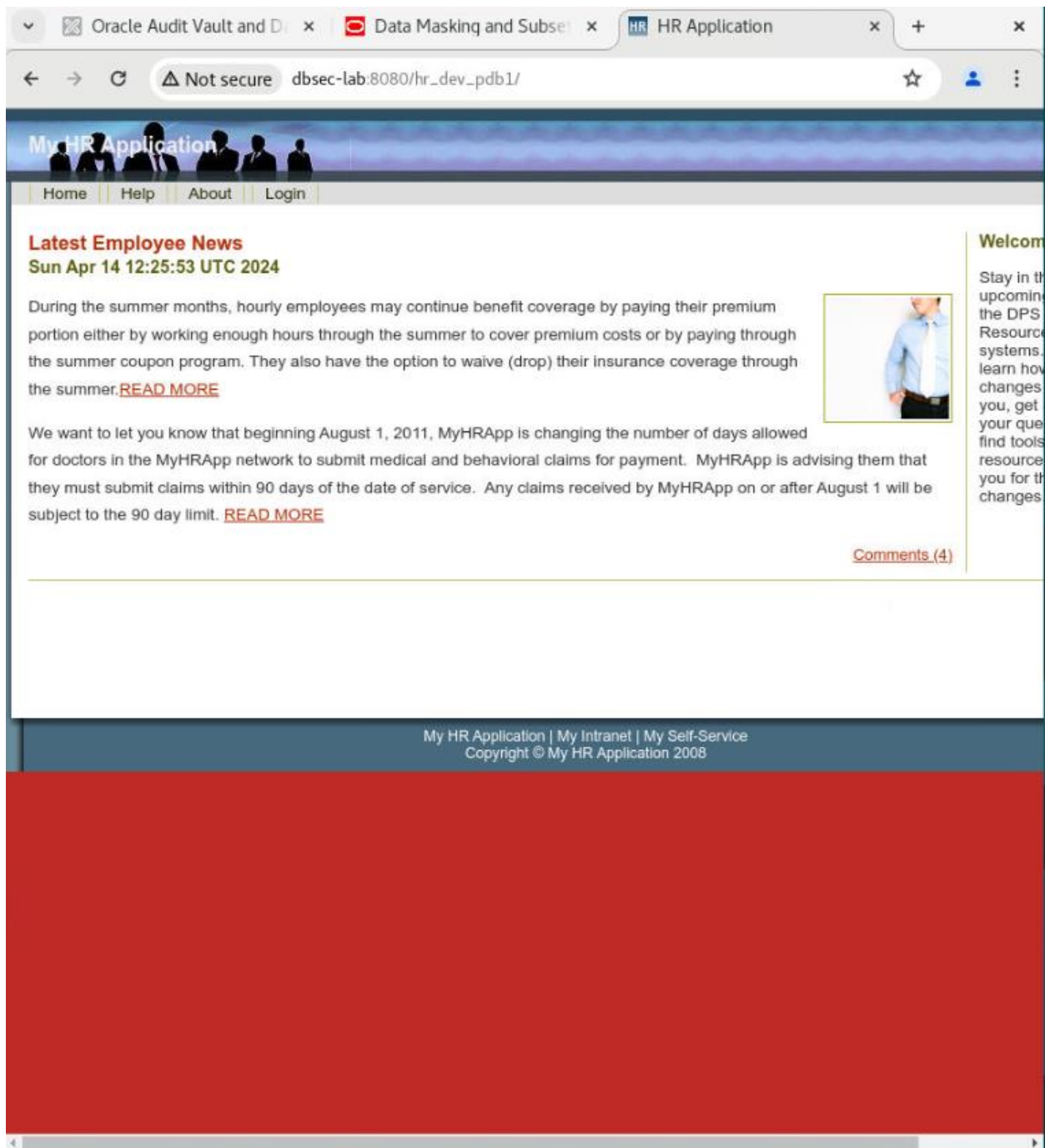
Dev: http://dbsec-lab:8080/hr_dev_pdb2

Copy

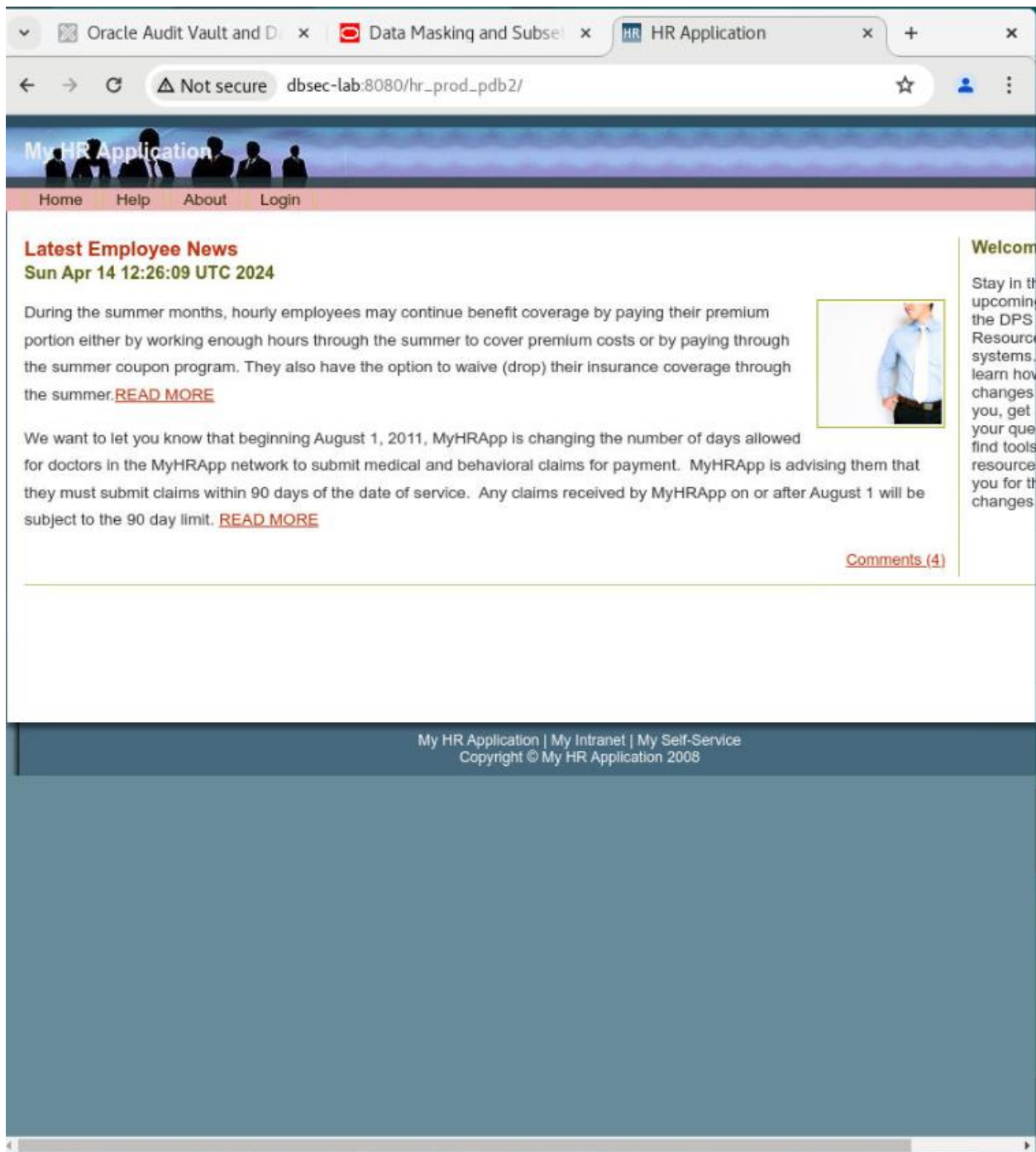
Với đường dẫn thứ nhất:



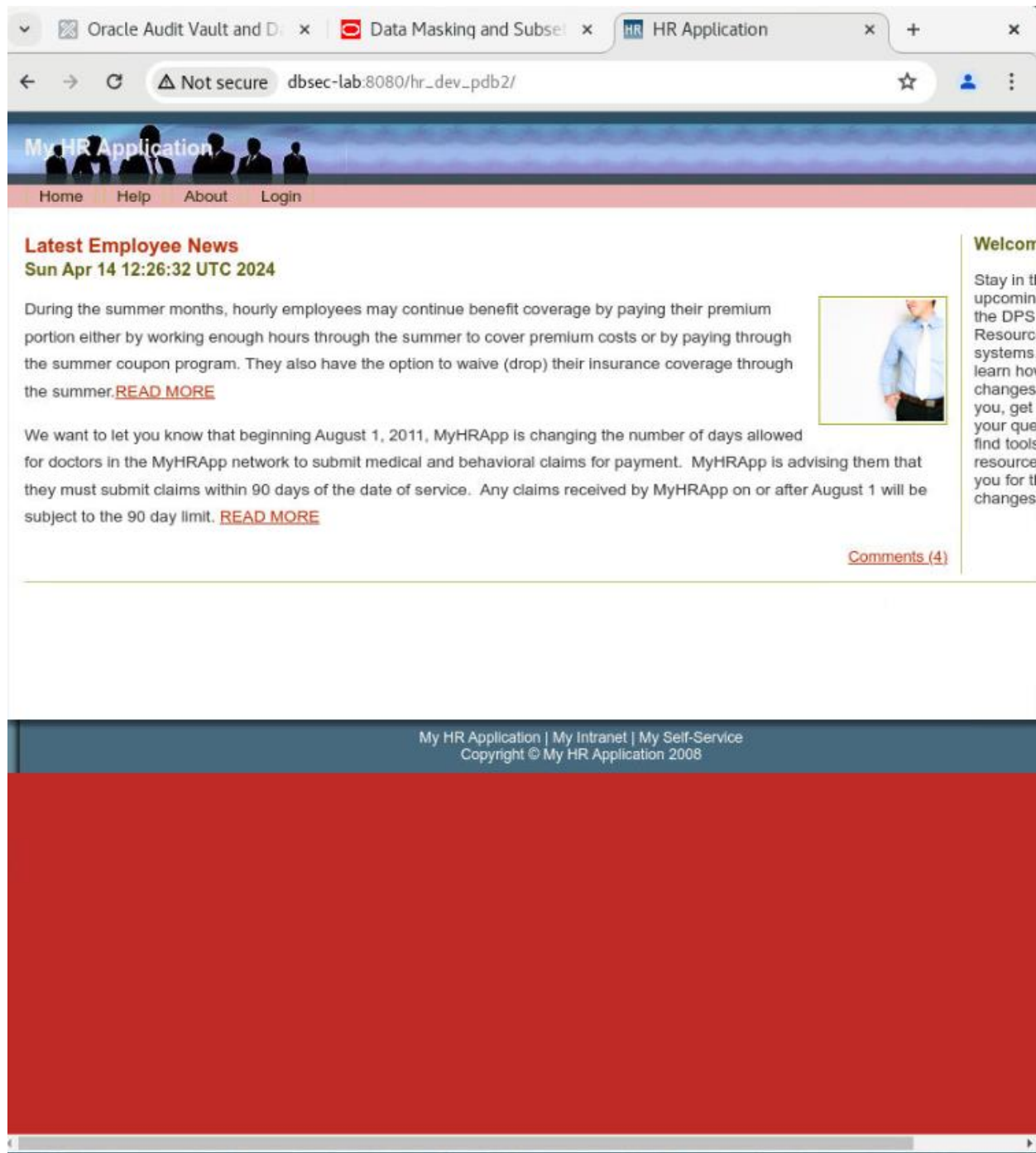
Đường dẫn thứ 2:



Đường dẫn thứ 3:



Đường dẫn thứ 4:



Qua các kết quả trên có thể thấy được rằng cả 4 đường dẫn đều chạy, có thể kết luận rằng môi trường đã sẵn sàng.



Task 2 - Set Glassfish to use pdb1 database in the dbsec lab VM:

Bước đầu tiên em sẽ mở terminal lên và chạy lệnh “sudo su – oracle”:

```
=====
DBSecLab VM
=====
ENV VARIABLES
=====
. PUBLIC_IP    = 192.9.186.59
. PRIVATE_IP   = 10.0.0.150
. HOSTNAME     = dbsec-lab
=====
. ORACLE_HOME  = /u01/app/oracle/product/19.0.0/dbhome_1
. DATA_DIR    = /u01/oradata/cdb1
. DBSEC_HOME   = /home/oracle/DBSecLab
. DBSEC_ADMIN  = /home/oracle/DBSecLab/admin
. DBSEC_LABS   = /home/oracle/DBSecLab/livelabs (Alias: labs)
=====
. ORACLE_SID   = cdb1
. PDB_NAME     = pdb1
. AVUSR_PWD    = uoNd7Y4pk:_20wn1
. OKVUSR_PWD   =
=====
USE THIS SCRIPT TO CHANGE ENV
source /home/oracle/DBSecLab/admin/setEnv-cdb.sh <CDB> <PDB>
=====

[cdb1:oracle@dbsec-lab:~/DBSecLab]$ sudo su - oracle
```

Sau đó đến đường dẫn “\$DBSEC_LABS/sqlfw”:



```
=====
DBSecLabs v1.0
=====
ENV VARIABLES
=====
. PUBLIC_IP    = 192.9.186.59
. PRIVATE_IP   = 10.0.0.150
. HOSTNAME     = dbsec-lab
=====
. ORACLE_HOME  = /u01/app/oracle/product/19.0.0/dbhome_1
. DATA_DIR    = /u01/oradata/cdb1
. DBSEC_HOME   = /home/oracle/DBSecLab
. DBSEC_ADMIN  = /home/oracle/DBSecLab/admin
. DBSEC_LABS   = /home/oracle/DBSecLab/livelabs (Alias: labs)
=====
. ORACLE_SID   = cdb1
. PDB_NAME     = pdb1
. AVUSR_PWD    = uoNd7Y4pk:_20wn1
. OKVUSR_PWD   =
=====
USE THIS SCRIPT TO CHANGE ENV
source /home/oracle/DBSecLab/admin/setEnv-cdb.sh <CDB> <PDB>
=====

[cdb1:oracle@dbsec-lab:~/DBSecLab]$ cd $DBSEC_LABS/sqlfw
[cdb1:oracle@dbsec-lab:~/DBSecLab/livelabs/sqlfw]$
```

Chạy “./sqlfw_glassfish_stop_db23c.sh”:



```
-----
                        USE THIS SCRIPT TO CHANGE ENV
                        source /home/oracle/DBSecLab/admin/setEnv-cdb.sh <CDB> <PDB>
=====

[cdb1:oracle@dbsec-lab:~/DBSecLab]$ cd $DBSEC LABS/sqlfw
[cdb1:oracle@dbsec-lab:~/DBSecLab/live labs/sqlfw]$ ./sqlfw_glassfish_stop_db23c.sh

=====
Restore the Glassfish App connection string to direct connect mode...
=====

=====
Stop Glassfish App...
=====
Waiting for the domain to stop .
Command stop-domain executed successfully.

. Copy the config file to change the connection string to direct connect mode

=====
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.

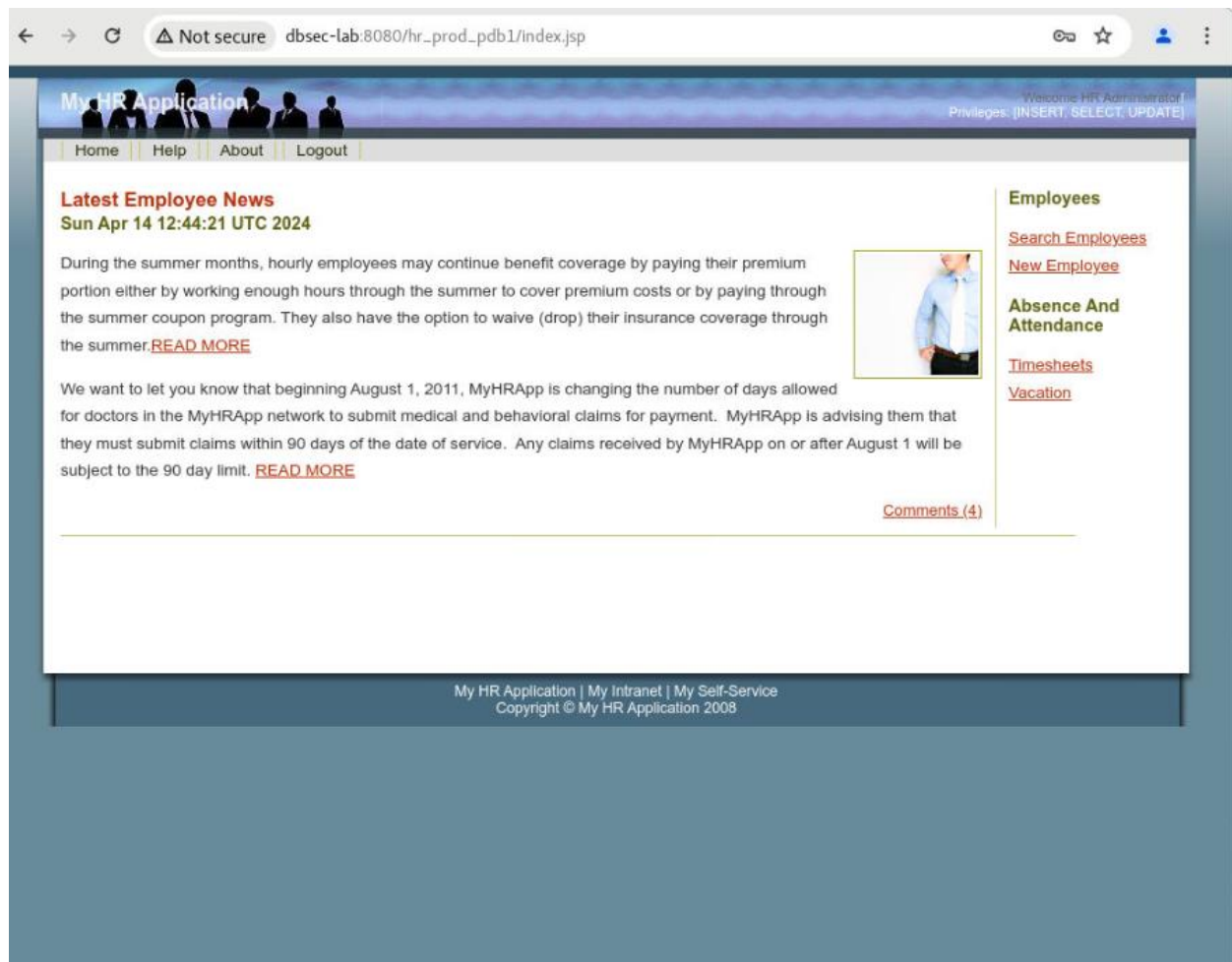
. You can login to the apps using the appropriate URL:

http://192.9.186.59:8080/hr_dev_pdb1
http://192.9.186.59:8080/hr_dev_pdb2
http://192.9.186.59:8080/hr_prod_pdb1
http://192.9.186.59:8080/hr_prod_pdb2

. The Glassfish App is now running with the following configuration
-----
oJDBCDriver = oracle.jdbc.OracleDriver
oJDBCURL = jdbc:oracle:thin:@//dbsec-lab:1521/pdb1
oJDBCUser = EMPLOYEESEARCH_PROD
oJBCPassword = Oracle123
-----

[cdb1:oracle@dbsec-lab:~/DBSecLab/live labs/sqlfw]$
```

Tiếp đến em sẽ kiểm tra xem nó đã hoạt động đúng mong đợi chưa bằng cách truy cập vào url http://dbsec-lab:8080/hr_prod_pdb1 để kết nối đến Glassfish App. Rồi đăng nhập vào với username là “hradmin” và password là “Oracle123”:



Sau khi đăng nhập xong thì màn hình như trên xuất hiện ra.

Lúc này khi bấm vào dòng chữ “Welcome HR Administrator” ở bên góc phải trên cùng màn hình thì cửa sổ Session Details xuất hiện:



← → ↺ ⚠ Not secure dbsec-lab:8080/hr_prod_pdb1/session_data.jsp ☆ 👤 ⋮

Welcome HR Administrator
Privileges: [INSERT, SELECT, UPDATE]

Home Help About Logout

Session Details

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	211
CURRENT_SQL	
CURRENT_SQLn	
CURRENT_SQL_LENGTH	
CURRENT_USER	EMPLOYEESEARCH_PROD
CURRENT_USERID	211
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

Employees

- [Search Employees](#)
- [New Employee](#)

Absence And Attendance

- [Timesheets](#)
- [Vacation](#)

Lab 3: Audit Vault and DB Firewall (AVDF)

Task 1: Reset the randomly generated password:

Bước đầu em sẽ truy cập đến đường dẫn "\$DBSEC_LABS/avdf/avs" thông qua terminal:



```
=====
DBSecLab V0.0
=====
ENV VARIABLES
=====
. PUBLIC_IP    = 192.9.186.59
. PRIVATE_IP   = 10.0.0.150
. HOSTNAME     = dbsec-lab
=====
. ORACLE_HOME  = /u01/app/oracle/product/19.0.0/dbhome_1
. DATA_DIR    = /u01/oradata/cdb1
. DBSEC_HOME   = /home/oracle/DBSecLab
. DBSEC_ADMIN  = /home/oracle/DBSecLab/admin
. DBSEC_LABS   = /home/oracle/DBSecLab/livelabs (Alias: labs)
=====
. ORACLE_SID   = cdb1
. PDB_NAME     = pdb1
. AVUSR_PWD    = uoNd7Y4pk:_20wn1
. OKVUSR_PWD   =
=====
USE THIS SCRIPT TO CHANGE ENV
source /home/oracle/DBSecLab/admin/setEnv-cdb.sh <CDB> <PDB>
=====

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

Sau đó sẽ mở “\$AVUSR_PWD” lên:



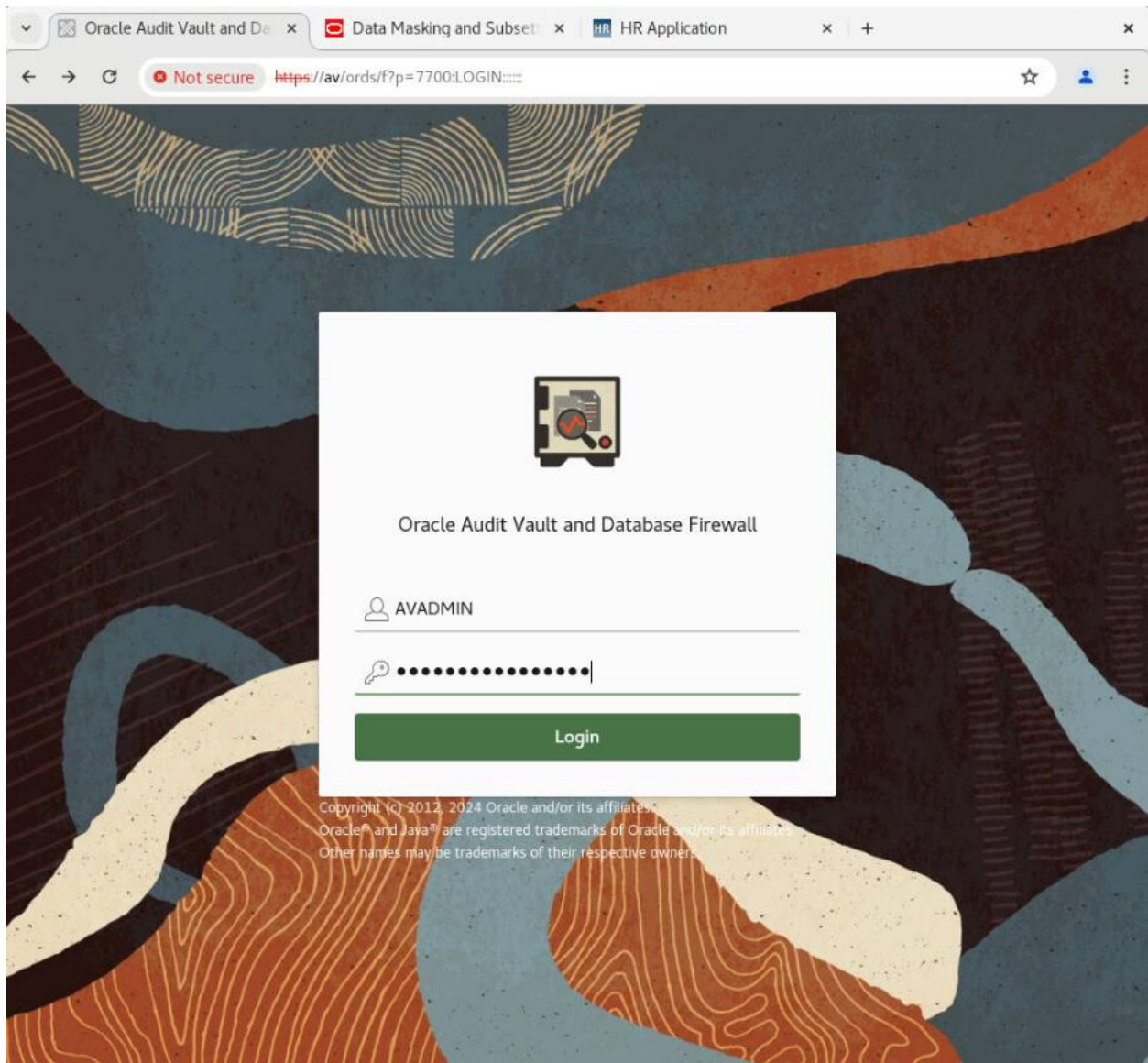
```
=====
DBSecLabs v6.0
=====

ENV VARIABLES
=====
. PUBLIC_IP    = 192.9.186.59
. PRIVATE_IP   = 10.0.0.150
. HOSTNAME     = dbsec-lab
=====
. ORACLE_HOME  = /u01/app/oracle/product/19.0.0/dbhome_1
. DATA_DIR    = /u01/oradata/cdb1
. DBSEC_HOME   = /home/oracle/DBSecLab
. DBSEC_ADMIN  = /home/oracle/DBSecLab/admin
. DBSEC_LABS   = /home/oracle/DBSecLab/livelabs (Alias: labs)
=====
. ORACLE_SID   = cdb1
. PDB_NAME     = pdb1
. AVUSR_PWD    = uoNd7Y4pk:_20wn1
. OKVUSR_PWD   =
=====

USE THIS SCRIPT TO CHANGE ENV
source /home/oracle/DBSecLab/admin/setEnv-cdb.sh <CDB> <PDB>
=====

[cdb1:oracle@dbsec-lab:~/DBSecLab]$ cd $DBSEC_LABS/avdf/avs
[cdb1:oracle@dbsec-lab:~/DBSecLab/livelabs/avdf/avs]$ echo $AVUSR_PWD
uoNd7Y4pk:_20wn1
[cdb1:oracle@dbsec-lab:~/DBSecLab/livelabs/avdf/avs]$ █
```

Kế tiếp em thực hiện truy cập đến <https://av> và đăng nhập với username là AVADMIN, password là password random vừa mở từ \$AVUSR_PWD:



Sau khi đăng nhập xong, màn hình reset password hiện ra:



Reset Password Data Masking and Subsetting HR Application

Not secure <https://av/ords/f?p=7700:8:::8::&cs=3hy3tEsJgiZYFOb06MTybniPh3j0nrJopUWRWYyudr3C4>

Reset Expired Password

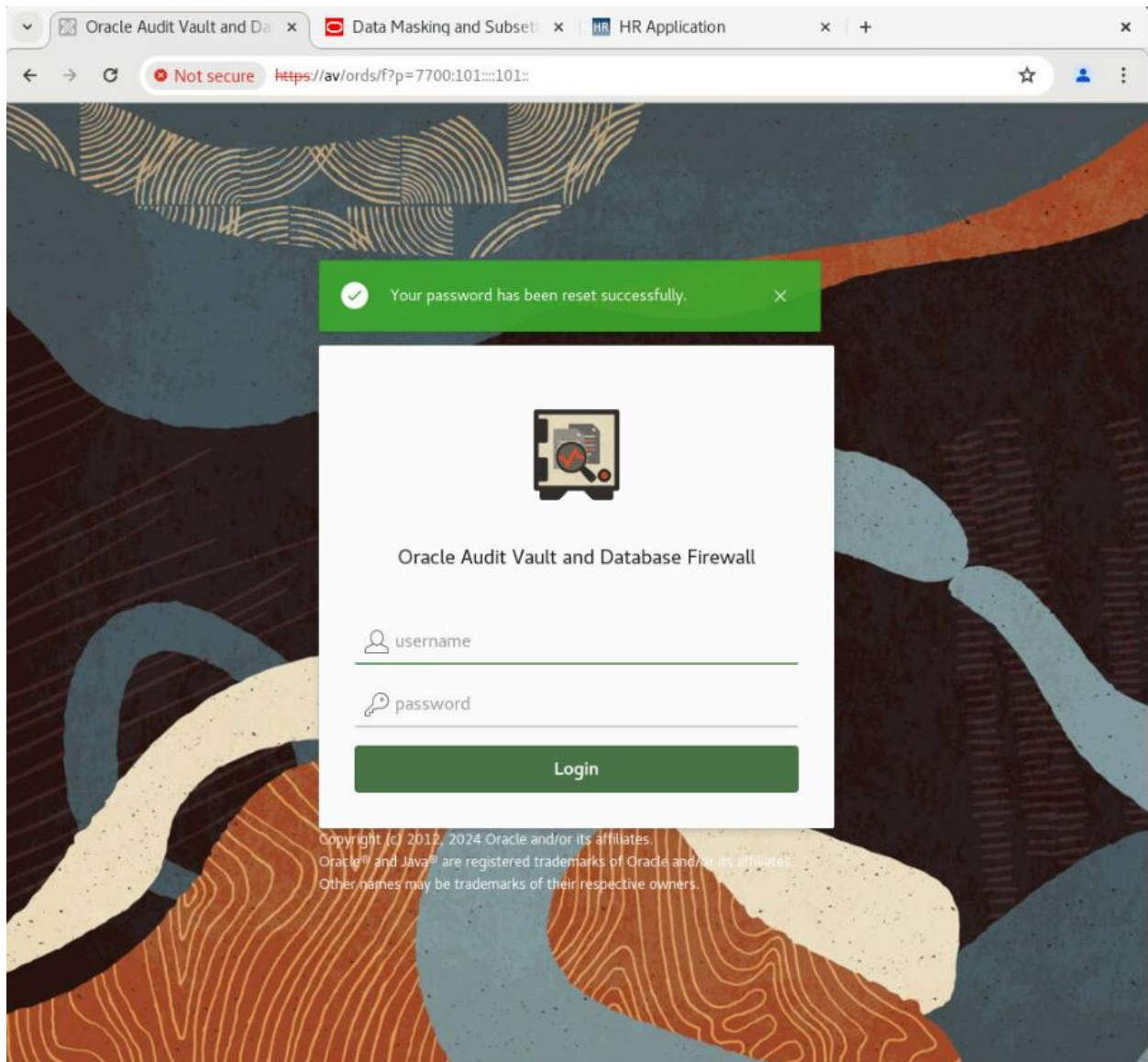
AVADMIN, your password has expired.

old password

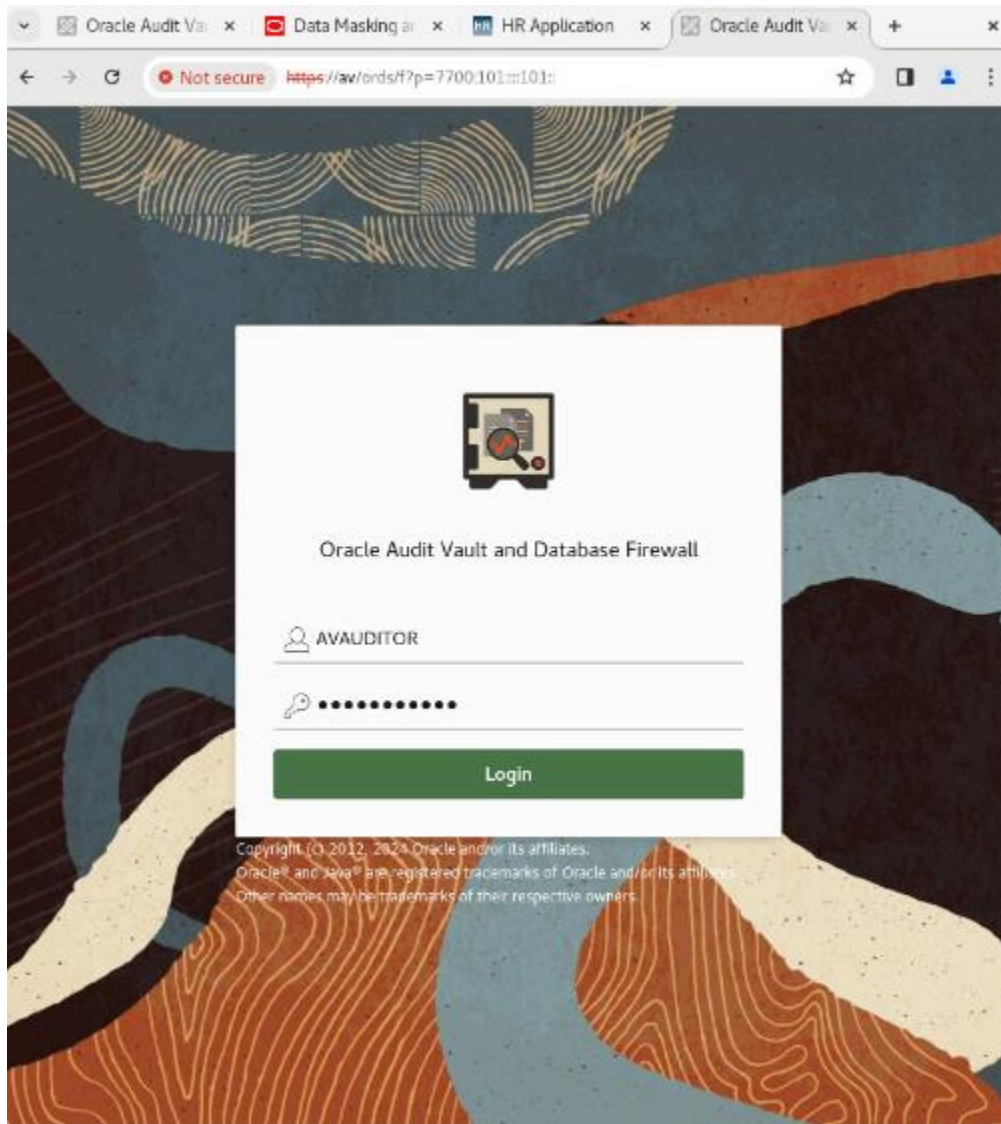
new password

confirm password

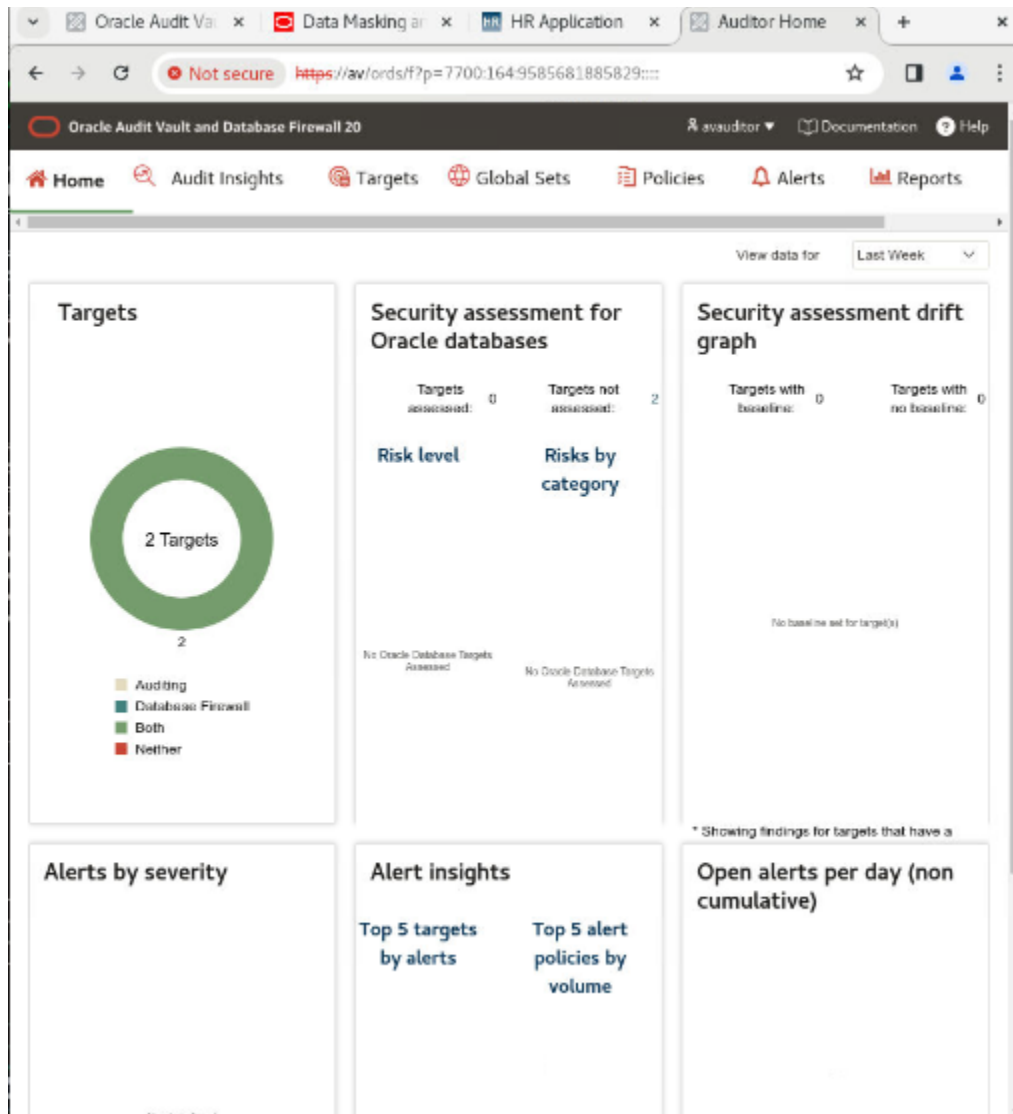
Em tiến hành đổi password và submit, kết quả nhận được là:



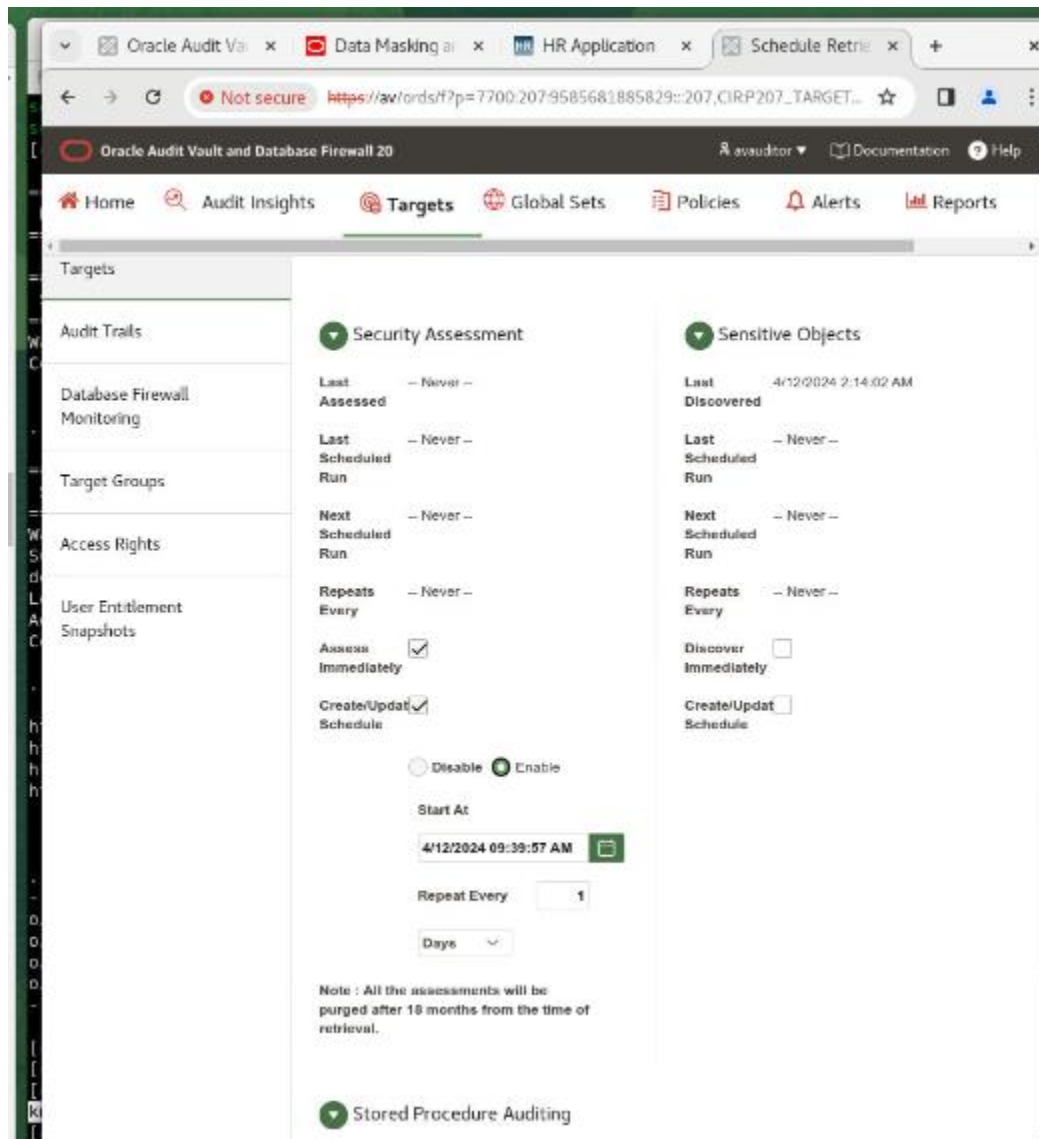
Task 2: Assess and Discover:



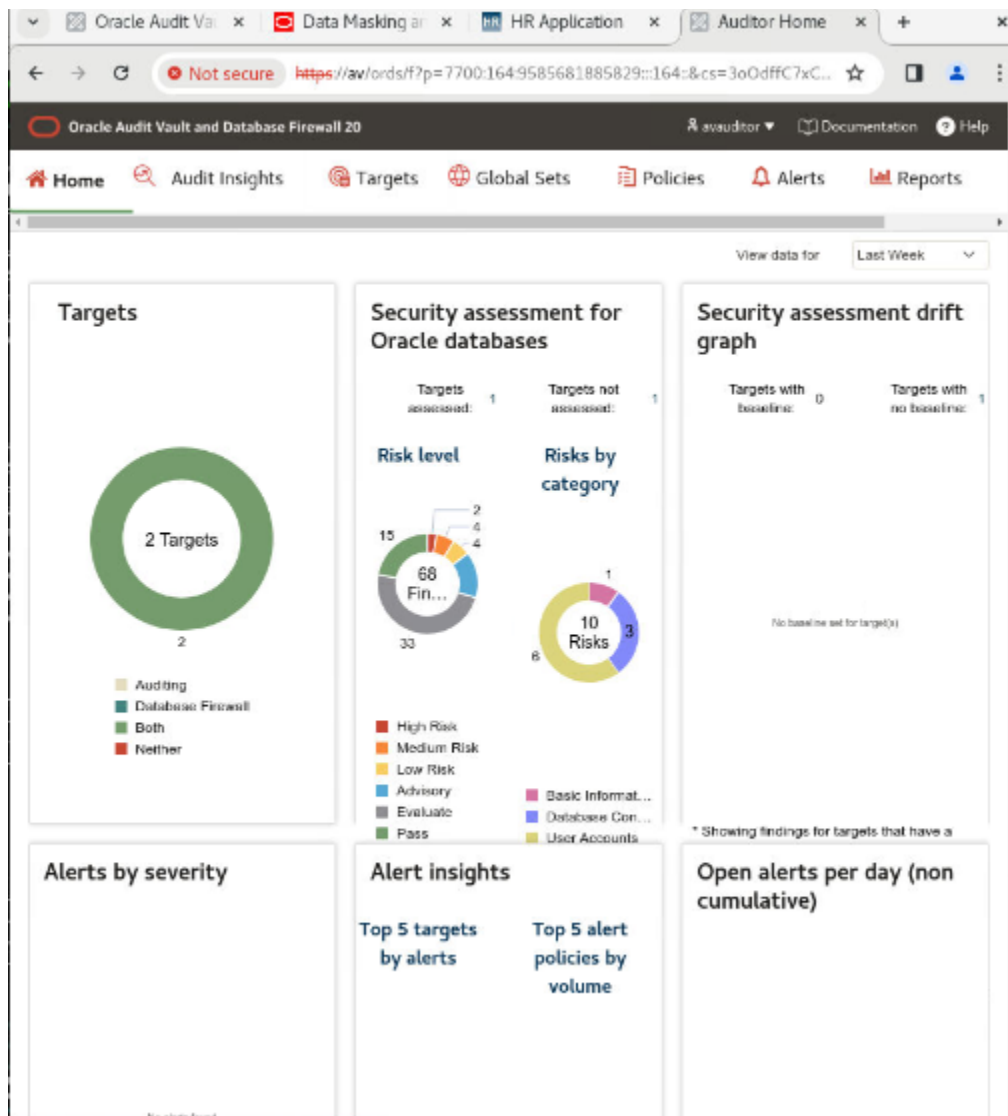
Login vào tài khoản AVAUDITOR bằng mật khẩu đã đổi ở task1



Màn hình home của tài khoản:



Trong tab Target, click vào **Schedule Retrieval Jobs** của pdb1. Tick vào 2 ô trong mục Security Assesment và enable. Nhấn Save:



Quay lại Home, ta thấy phần Security Assessment đã có thêm các mục mới



The screenshot shows the Oracle Audit Vault and Database Firewall 20 web interface. The left sidebar contains a navigation menu with the following items: Activity Reports, Summary Reports, Compliance Reports, Assessment Reports (highlighted), Report Templates, Saved Reports, Report Schedules, and Generated Reports. The main content area displays the 'Assessment Reports' section, specifically the 'Security Assessment Summary by Severity' report. Above the table, there are search and action buttons labeled 'Go' and 'Actions'. The table lists various risk levels and their corresponding counts across different categories.

Severity	Targets	Basic Information	User Accounts	Privileges And Roles	Authorization Control	Fine-Grained Access Control	Auditing	Enc
High Risk	1	1	0	0	0	0	0	
Medium Risk	1	0	3	0	0	0	0	
Low Risk	1	0	3	0	0	0	0	
Advisory	1	0	0	1	2	5	1	
Evaluate	1	0	1	17	0	0	11	
Pass	1	0	5	4	0	0	0	

Trong tab Report, click vào Security Assessment Summary by Serenity trong cột Assessment Report. Ta có thể thấy các risk với các mức độ báo động khác nhau.



Oracle Audit Vault and Database Firewall 20

Home Audit Insights Targets Global Sets Policies Alerts Reports Settings

Activity Reports
Summary Reports
Compliance Reports
Assessment Reports
Report Templates
Saved Reports
Report Schedules
Generated Reports

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

Category	Basic Information
Assessment	Patch Check
Summary	Latest comprehensive patch not found.
Details	<p>Latest comprehensive patch: Sep 30 2023 (194 days ago)</p> <p>SQL Patch History:</p> <p>Action time: Thu Dec 21 2023 12:40:19 Action: APPLY Version: 19.21.0.0.0 Description: Database Release Update : 19.21.0.0.231017 (35643107)</p> <p>Action time: Wed Jan 11 2023 12:13:53 Action: APPLY Version: 19.17.0.0.0 Description: Database Release Update : 19.17.0.0.221018 (34419443)</p> <p>Action time: Wed Oct 20 2021 13:33:15 Action: APPLY Version: 19.13.0.0.0 Description: Database Release Update : 19.13.0.0.211018 (32182793)</p> <p>Action time: Mon Apr 12 2021 13:40:52 Action: APPLY Version: 19.10.0.0.0 Description: Database Release Update : 19.10.0.0.210119 (32218454)</p> <p>Action time: Wed Aug 05 2020 13:18:28 Action: APPLY Version: 19.8.0.0.0 Description: Database Release Update : 19.8.0.0.200714 (31281355)</p> <p>Action time: Tue Jun 30 2020 09:31:28 Action: APPLY Version: 19.7.0.0.0 Description: Database Release Update : 19.7.0.0.200414 (30869155)</p> <p>Action time: Wed Nov 13 2019 16:44:41 Action: APPLY Version: 19.5.0.0.0 Description: Database Release Update : 19.5.0.0.191015 (30125133)</p> <p>Action time: Wed Oct 30 2019 15:52:56</p>

VD: High risk assessments



Oracle Audit Vault and Database Firewall 20

Home Audit Insights Targets Global Sets

Successfully set baseline for selected assessment. X

Assessment Drift Reports >> Security Assessment Drift Summary by Target >> Security Assessment Report

Target: pdb1 assessed time: 4/12/2024 9:40:10 AM (Latest, Baseline) Set As Baseline

Go Actions

Target	Category	Assessment	Summary	Severity	Compliance
pdb1	Basic Information	Patch Check	Latest comprehensive patch not found.	High Risk	DISA STIG, CIS Benchmark
pdb1	Database Configuration	Database Backup	No Backup Records found for the last 90 days.	High Risk	DISA STIG
pdb1	Database Configuration	Network Communication	Examined 4 initialization parameters. Found 1 issue.	Medium Risk	DISA STIG, CIS Benchmark
pdb1	User Accounts	Account Locking after Failed Login Attempts	Found 42 users with unlimited failed login attempts. Found 43 users without minimum lock time.	Medium Risk	DISA STIG, CIS Benchmark
pdb1	User Accounts	Password Verification Functions	Found 43 users not using password verification function.	Medium Risk	DISA STIG, CIS Benchmark
pdb1	User Accounts	Sample Schemas	Found 2 sample schemas.	Medium Risk	DISA STIG, CIS Benchmark
pdb1	Database Configuration	Triggers	No logon triggers found. Found 1 disabled trigger.	Low Risk	Oracle Best Practices
pdb1	User Accounts	Inactive Users	Found 41 user accounts that would remain open even if inactive. Found 39 unlocked users inactive for more than 30 days.	Low Risk	DISA STIG
pdb1	User Accounts	Users with	Found 40 users with	Low Risk	DISA STIG

Trong mục Target with no baseline ở Home, ta chọn pdb1 để set baseline.

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

Tạo drift cho pdb1



Home

Audit Insights

Targets

Global Sets

Policies

Alerts

Reports

Settings

Targets

Audit Trails

Database Firewall Monitoring

Target Groups

Access Rights

User Entitlement Snapshots

Note : All the user entitlement snapshots will be purged after 18 months from the time of retrieval.

Security Assessment

Last Assessed

4/12/2024 8:40:10 AM

Last Scheduled Run

4/12/2024 9:39:57 AM

Next Scheduled Run

4/13/2024 9:39:57 AM

Repeats Every

1 Day

Assess Immediately

☒

Create/Update Schedule

☐

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

Stored Procedure Auditing

Last Scheduled Run

-- Never --

Next Scheduled Run

-- Never --

Repeats Every

-- Never --

Create/Update Schedule

☐

Sensitive Objects

Last Discovered

4/12/2024 2:14:02 AM

Last Scheduled Run

-- Never --

Next Scheduled Run

-- Never --

Repeats Every

-- Never --

Discover Immediately

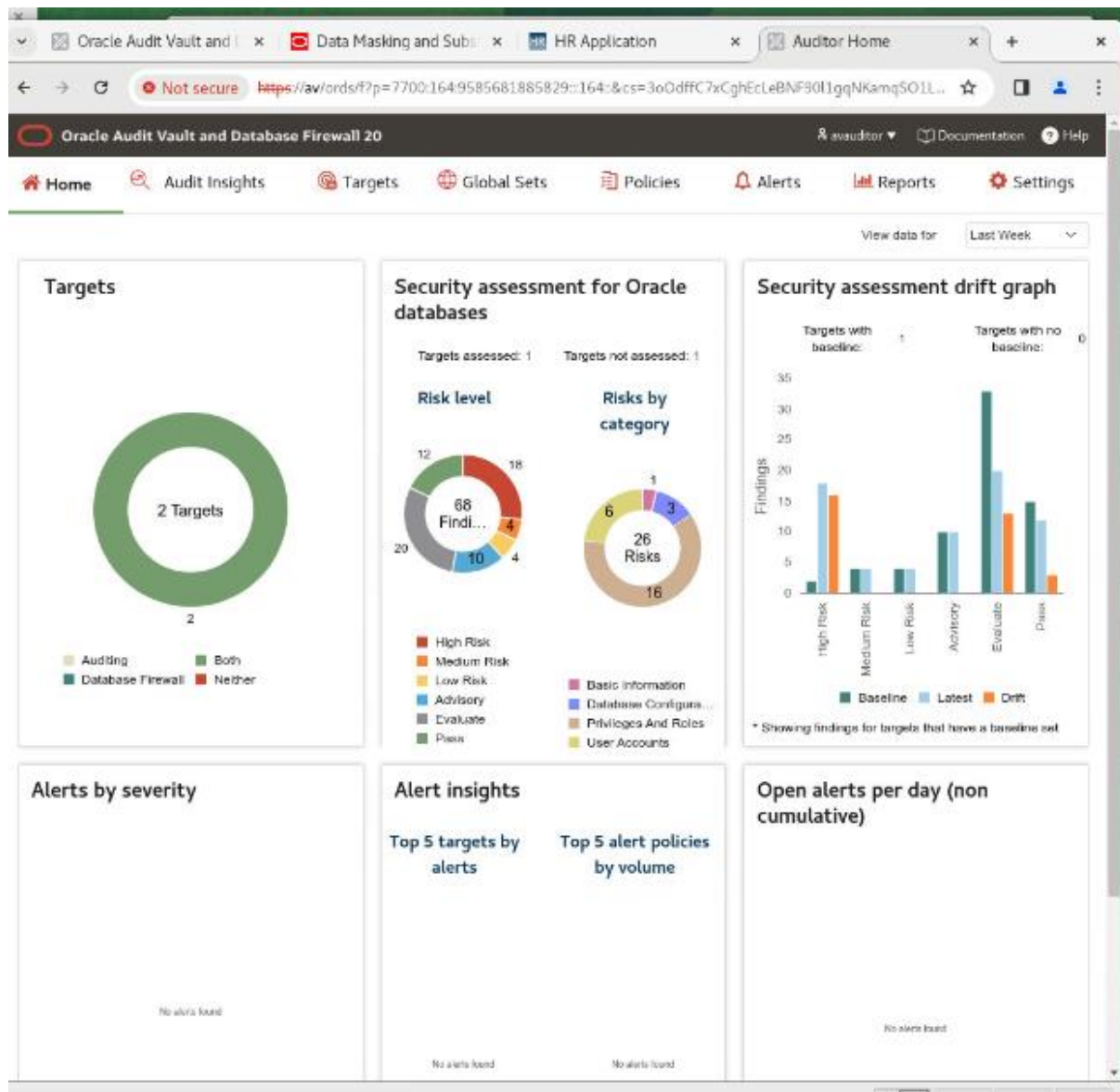
☐

Create/Update Schedule

☐

Trong tab Target, click vào **Schedule Retrieval Jobs** của pdb1. Tick vào ô Assess Immediately trong mục Security Assesment và enable. Nhấn Save

Trang 30 / 42



Ta thấy rằng mục Target with baseline đã chuyển thành 1 với dữ liệu thống kê cho pdb1

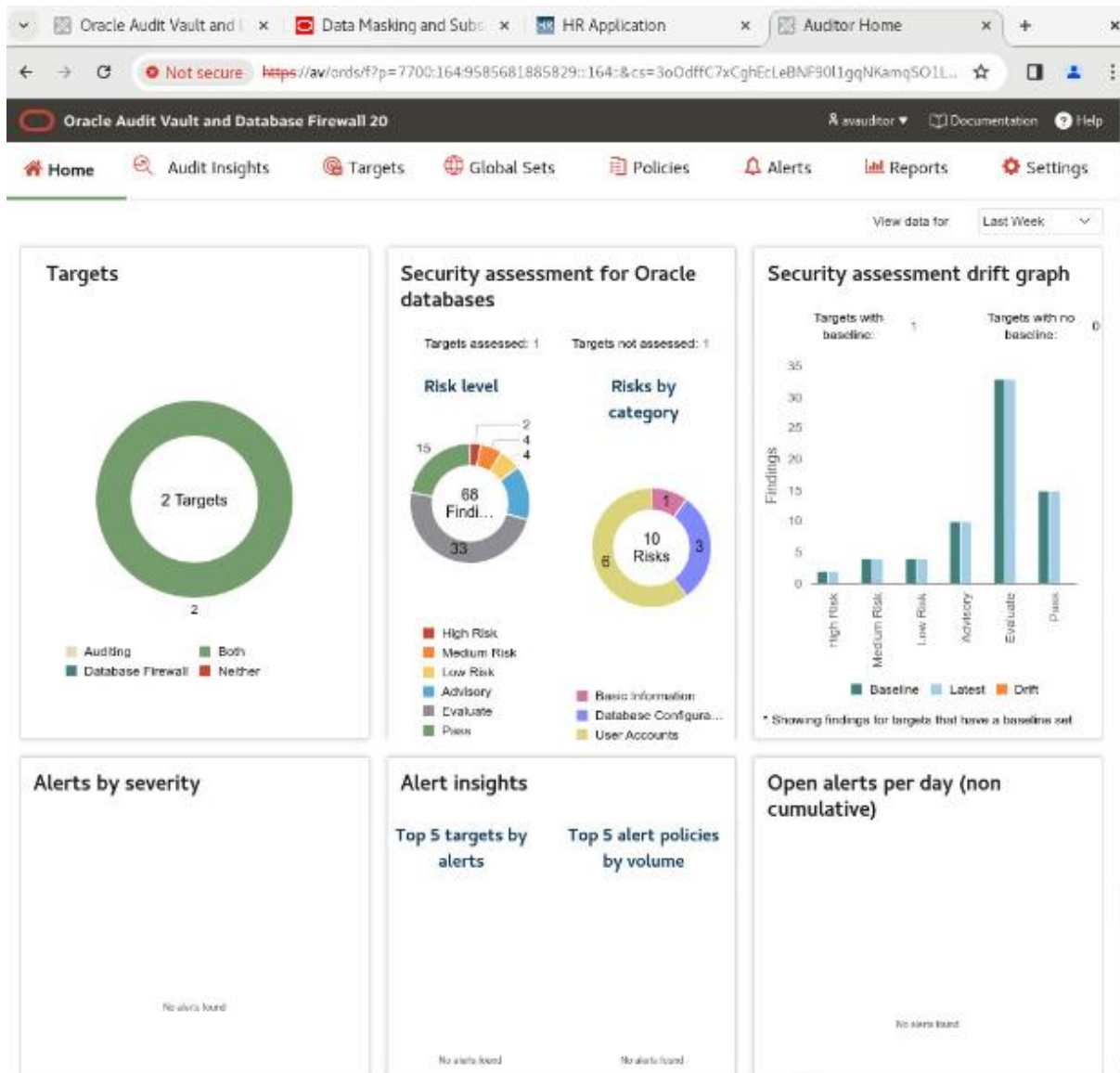
```
[cdb1:oracle@dbsec-lab:~/DBSecLab/liveLabs/avdf/avs]$ ./avs_mitigate-risk.sh pdb1

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

Revoke succeeded.

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

Giảm độ risk của drift trên pdb1



Kết quả sau khi giảm độ risk của drift trên pdb1



Oracle Audit Vault and Database Firewall 20

Home Audit Insights Targets Global Sets Policies Alerts Reports Settings

Targets

Note : All the user entitlement snapshots will be purged after 18 months from the time of retrieval.

Security Assessment

Last Assessed 4/12/2024 9:53:30 AM

Last Scheduled Run 4/12/2024 9:39:57 AM

Next Scheduled Run 4/13/2024 9:39:57 AM

Repeats Every 1 Day

Assess Immediately ☐

Create/Update Schedule ☐

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

Sensitive Objects

Last Discovered 4/12/2024 2:14:02 AM

Last Scheduled Run -- Never --

Next Scheduled Run -- Never --

Repeats Every -- Never --

Discover Immediately ☒

Create/Update Schedule ☒

Disable ☐ Enable ☒

Start At 4/12/2024 09:59:03 AM

Repeat Every 1 Days

Stored Procedure Auditing

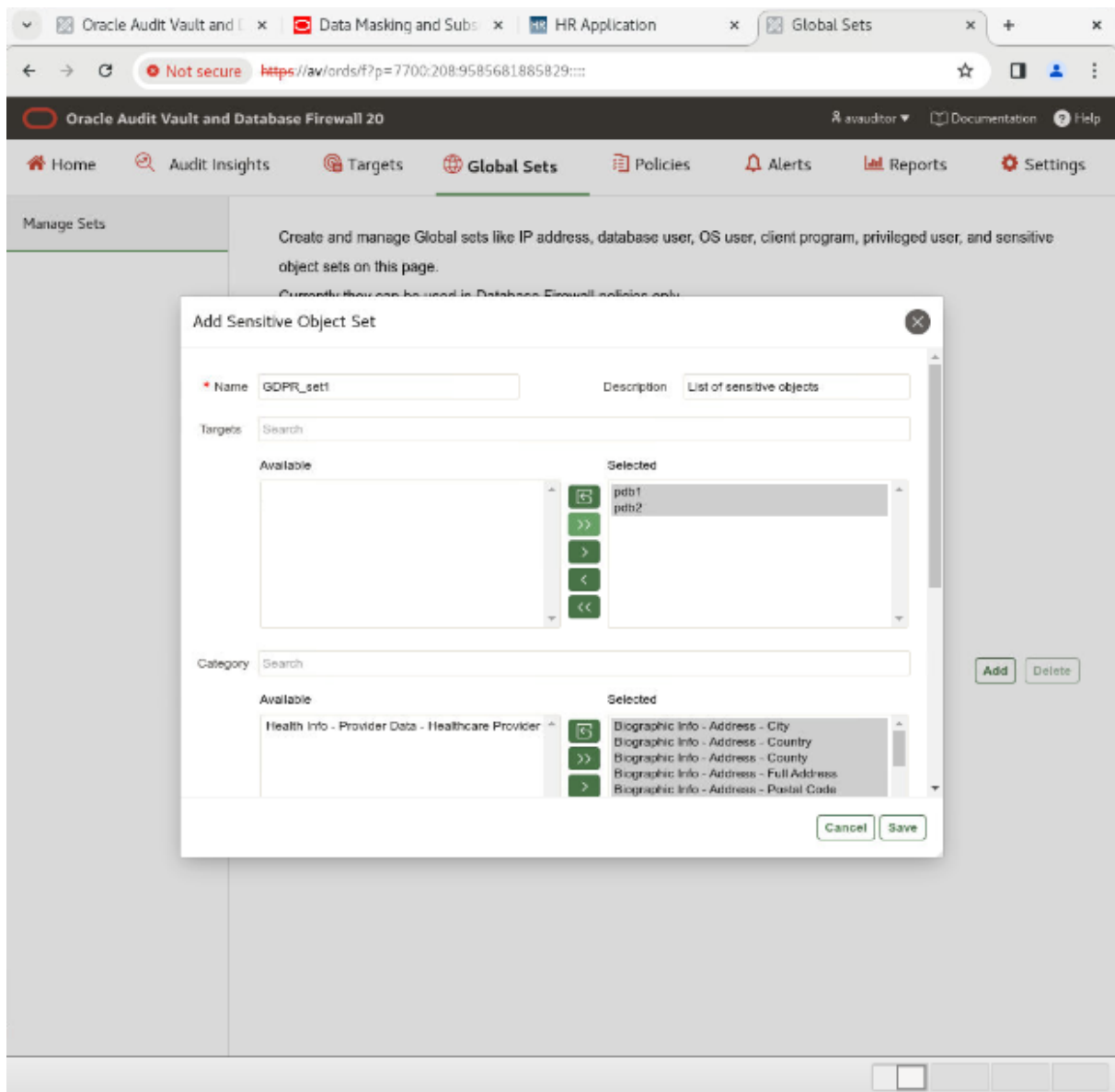
Last Scheduled Run -- Never --

Next Scheduled Run -- Never --

Repeats Every -- Never --

Create/Update ☐

Trong tab Target, click vào **Schedule Retrieval Jobs** của pdb1. Tick vào 2 ô trong mục **Sensitive Objects** và enable. Nhấn Save



Trong tab Global Sets, click vào hành **Sensitive object sets** để mở rộng. Chọn add. Đặt tên, mô tả và chọn cả 2 pdb1 và pdb2. Nhấn Save



Currently they can be used in Database Firewall policies only.

- ▶ IP Address Sets (0)
- ▶ OS User Sets (0)
- ▶ Client Program Sets (0)
- ▶ Database User Sets (0)
- ▶ Privileged User Sets (0)
- ▶ Sensitive Object Sets (1)

Discover sensitive objects by scheduling sensitive objects jobs `name`.

[Add](#) [Delete](#)

<input type="checkbox"/>	Name ↑	Description	In Use
<input type="checkbox"/>	GDPR_List1	List of sensitive objects	No

1 - 1

Kết quả sau khi tạo sets

Task3: Audit and Monitor:



Trong tab Target, click vào **Schedule Retrieval Jobs** của pdb1. Tick vào 2 ô trong mục **Audit Policy** và enable. Nhấn Save



Trong Tab Policies, mục Audit Policies, click các mục:

- *Critical Database Activity*
- *Database Schema Changes*
- *All Admin Activity*
- *Center for Internet Security (CIS) Configuration*

Nhấn **Provision Unified Policy**



Oracle Audit Vault and Database Firewall 20

Home Audit Insights Targets Global Sets Policies Alerts Reports Settings

Manage Auditors
Distribution Lists
Email Templates
Alert Syslog Templates
Jobs

Last Updated is in the last 7 days
Highlight Failed Jobs

Job Type	Status	Last Updated	Started At	Created By	Message
Unified Audit Policy	Completed	4/12/2024 10:30:11 AM	4/12/2024 10:30:01 AM	AVAUDITOR	Completed Successfully policy provision of target p1b1
Audit Settings	Completed	4/12/2024 10:04:36 AM	4/12/2024 10:04:40 AM	AVAUDITOR	
Audit Settings	Completed	4/12/2024 10:00:40 AM	4/12/2024 10:00:19 AM	AVAUDITOR	
DBSAT Data Discovery	Completed	4/12/2024 9:59:06 AM	4/12/2024 9:59:03 AM	AVAUDITOR	DBSAT Data Discovered Successfully
DBSAT Data Discovery	Completed	4/12/2024 9:54:46 AM	4/12/2024 9:54:42 AM	AVAUDITOR	DBSAT Data Discovered Successfully
Security Assessment	Completed	4/12/2024 9:53:33 AM	4/12/2024 9:53:13 AM	AVAUDITOR	
Security Assessment	Completed	4/12/2024 9:52:18 AM	4/12/2024 9:51:57 AM	AVAUDITOR	
Security Assessment	Completed	4/12/2024 9:50:19 AM	4/12/2024 9:50:09 AM	AVAUDITOR	
Security Assessment	Completed	4/12/2024 9:40:19 AM	4/12/2024 9:39:57 AM	AVAUDITOR	
Security Assessment	Completed	4/12/2024 9:36:47 AM	4/12/2024 9:36:28 AM	AVAUDITOR	
Audit Vault Server health check job	Completed	4/12/2024 7:36:42 AM	4/12/2024 7:36:41 AM	avsys	Audit Vault Server health check job completed
User Entitlement	Failed	4/12/2024 2:14:28 AM	4/12/2024 2:14:03 AM	AVADMIN	Failed to connect to DB

Kiểm tra trong mục Setting, trong mục Jobs ta có thể thấy một job tên **Unified Audit Policy** đã hoàn thành ở trên đầu



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

=====
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
-----
APP_USER_NOT_APP_SERVER
EMPSEARCH_SELECT_USAGE_BY_PETE
ORA_ACCOUNT_MGMT
ORA_ADS$ ADMIN_USER_ACTIVITY
ORA_ADS$ CRITICAL DB ACTIVITY
ORA_ADS$ DB_SCHEMA_CHANGES
ORA_ADS$ LOGON_EVENTS
ORA_ADS$ LOGON_FAILURES
ORA_ADS$ SYS_TOP_ACTIVITY
ORA_AVS ADMIN_USER_ACTIVITY
ORA_AVS CRITICAL DB ACTIVITY
ORA_AVS DB_SCHEMA_CHANGES
ORA_AVS 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
PRIVILEGED_ACTIONS

22 rows selected.

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

Kiểm tra các Unified Audit Policies sử dụng **SQL*Plus**



```
File Edit View Search Terminal Help

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

=====
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
-----
PRIVILEGED ACTIONS    BY GRANTED ROLE DBA                                ROLE       YES     YES
ORA_SECURECONFIG      BY USER        ALL USERS        USER        YES     YES
ORA_RAS_SESSION_MGMT  BY USER        ALL USERS        USER        YES     YES
ORA_RAS_POLICY_MGMT   BY USER        ALL USERS        USER        YES     YES
ORA_LOGON_FAILURES    BY USER        ALL USERS        USER        YES     YES
ORA_DV_AUDPOL2        BY USER        ALL USERS        USER        YES     YES
ORA_DV_AUDPOL         BY USER        ALL USERS        USER        YES     YES
ORA_DATABASE_PARAMETER BY USER        ALL USERS        USER        YES     YES
ORA_CIS_RECOMMENDATIONS BY USER        ALL USERS        USER        YES     YES
ORA_AVS_SYS_TOP_ACTIVITY BY USER        SYS              USER        YES     YES
ORA_AVS_DB_SCHEMA_CHANGES BY USER        ALL USERS        USER        YES     YES
ORA_AVS_CRITICAL_DB_ACTIVITY BY USER        ALL USERS        USER        YES     YES
ORA_AVS_ADMIN_USER_ACTIVITY BY GRANTED ROLE DATAPUMP_IMP_FULL_DATABASE ROLE       YES     YES
ORA_AVS_ADMIN_USER_ACTIVITY BY GRANTED ROLE DATAPUMP_EXP_FULL_DATABASE ROLE       YES     YES
ORA_AVS_ADMIN_USER_ACTIVITY BY GRANTED ROLE IMP_FULL_DATABASE ROLE       YES     YES
ORA_AVS_ADMIN_USER_ACTIVITY BY GRANTED ROLE DBA                                ROLE       YES     YES
ORA_AVS_ADMIN_USER_ACTIVITY BY USER        SYSRAC           USER        YES     YES
ORA_AVS_ADMIN_USER_ACTIVITY BY USER        SYSKM           USER        YES     YES
ORA_AVS_ADMIN_USER_ACTIVITY BY USER        SYSDBG           USER        YES     YES
ORA_AVS_ADMIN_USER_ACTIVITY BY USER        SYSBACKUP        USER        YES     YES
ORA_AVS_ADMIN_USER_ACTIVITY BY USER        PUBLIC           USER        YES     YES
ORA_AVS_ADMIN_USER_ACTIVITY BY GRANTED ROLE EXP_FULL_DATABASE ROLE       YES     YES
ORA_AVS$ SYS_TOP_ACTIVITY BY USER        SYS              USER        YES     YES
ORA_AVS$ LOGON_FAILURES BY USER        ALL USERS        USER        NO      YES
ORA_AVS$ LOGON_EVENTS BY USER        ALL USERS        USER        YES     YES
ORA_AVS$ DB_SCHEMA_CHANGES BY USER        ALL USERS        USER        YES     YES
ORA_AVS$ CRITICAL_DB_ACTIVITY BY USER        ALL USERS        USER        YES     YES
ORA_AVS$ ADMIN_USER_ACTIVITY BY USER        SYSBACKUP        USER        YES     YES
ORA_AVS$ ADMIN_USER_ACTIVITY BY GRANTED ROLE DBA                                ROLE       YES     YES
ORA_AVS$ ADMIN_USER_ACTIVITY BY USER        PUBLIC           USER        YES     YES
ORA_AVS$ ADMIN_USER_ACTIVITY BY USER        SYSDBG           USER        YES     YES
ORA_AVS$ ADMIN_USER_ACTIVITY BY GRANTED ROLE DATAPUMP_IMP_FULL_DATABASE ROLE       YES     YES
ORA_AVS$ ADMIN_USER_ACTIVITY BY GRANTED ROLE DATAPUMP_EXP_FULL_DATABASE ROLE       YES     YES
ORA_AVS$ ADMIN_USER_ACTIVITY BY USER        SYSKM           USER        YES     YES
ORA_AVS$ ADMIN_USER_ACTIVITY BY USER        SYSRAC           USER        YES     YES
ORA_AVS$ ADMIN_USER_ACTIVITY BY GRANTED ROLE EXP_FULL_DATABASE ROLE       YES     YES
ORA_AVS$ ADMIN_USER_ACTIVITY BY GRANTED ROLE IMP_FULL_DATABASE ROLE       YES     YES
ORA_ACCOUNT_MGMT      BY USER        ALL USERS        USER        YES     YES
EMPSEARCH_SELECT_USAGE BY USER        ALL USERS        USER        YES     YES
APP_USER_NOT_APP_SERVER BY USER        ALL USERS        USER        YES     YES
```

Kiểm tra các Unified Audit Policies đã được bật.



Trong tab Target, click vào **Schedule Retrieval Jobs** của pdb1. Tick vào 2 ô trong mục **User Entitlements** và enable. Nhấn Save



Oracle Audit Vault and Database Firewall 20

Home Audit Insights Targets Global Sets Policies Alerts Reports Settings

Activity Reports Entitlement Reports >> User Accounts

Summary Reports

Compliance Reports

Assessment Reports

Report Templates

Saved Reports

Report Schedules

Generated Reports

Highlight Locked Account

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
pdb1	APPDEV_USER1	OPEN		DEFAULT	
pdb1	APPDEV_USER2	OPEN		DEFAULT	
pdb1	APPDEV_USER3	OPEN		DEFAULT	
pdb1	APPOSSYS	LOCKED	10/30/2019 3:56:06 PM	DEFAULT	
pdb1	AUDSYS	LOCKED	10/30/2019 3:56:06 PM	DEFAULT	
pdb1	AVALIDUSER	OPEN		DEFAULT	
pdb1	BACKUP_ADMIN	OPEN		DEFAULT	
pdb1	BA_BETTY	OPEN		DEFAULT	
pdb1	C##AVGGADMIN	OPEN		DEFAULT	
pdb1	C##DBA_DAVE	OPEN		DEFAULT	
pdb1	C##DVACCTMCR	OPEN		DEFAULT	
pdb1	C##DVACCTMCR_BACKUP	OPEN		DEFAULT	
pdb1	C##DVOWNER	OPEN		DEFAULT	
pdb1	C##DVOWNER_BACKUP	OPEN		DEFAULT	
pdb1	C##KEYMASTER	OPEN		DEFAULT	
pdb1	C##SEC_DBA_SAL	OPEN		DEFAULT	
pdb1	C##ZEUS	OPEN		DEFAULT	
pdb1	CTXSYS	EXPIRED & LOCKED	10/30/2019 3:56:06 PM	DEFAULT	10/30/2019 3:56:06 PM
pdb1	DBA_DEBRA	OPEN		DEFAULT	

Trong tab Reports, ở phần **Entitlement Reports**, nhấn vào **User Accounts**. Ở phần label chọn Latest và chọn tất cả Target Name, sau khi nhấn Go ta sẽ có được danh sách user entitlement.