# BÁO CÁO THỰC HÀNH

**Môn học: An toàn mạng máy tính nâng cao**

**Lab 3: Database Security**

*GVHD: Đỗ Thị Phương Uyên*

## 1. THÔNG TIN CHUNG:

*(Liệt kê tất cả các thành viên trong nhóm)*
Lớp: NT522.O21.ATCL.1- Nhóm 3

| STT | Họ và tên | MSSV | Email |
|---|---|---|---|
| 1 | Nguyễn Ngọc Trà My | 21520353 | 21520353@gm.uit.edu.vn |
| 2 | Bùi Hoàng Trúc Anh | 21521817 | 21521817@gm.uit.edu.vn |
| 3 | Lê Hoàng Oanh | 21521253 | 21521253@gm.uit.edu.vn |
| 4 | Huỳnh Minh Tân Tiến | 21521520 | 21521520@gm.uit.edu.vn |

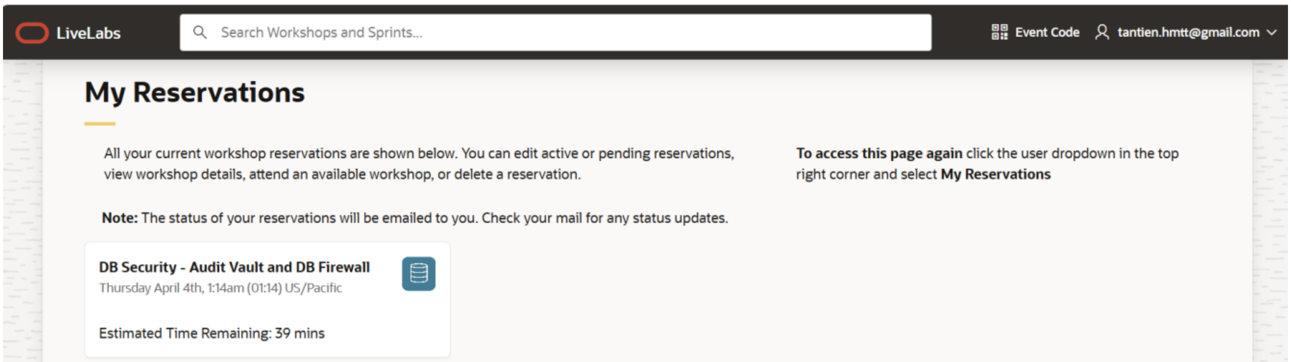
## 2. NỘI DUNG THỰC HIỆN:

| STT | Công việc | Kết quả tự đánh giá |
|---|---|---|
| 1 | **Yêu cầu 1** | 100% |
| 2 | **Yêu cầu 2** | 100% |

**Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.**

# BÁO CÁO CHI TIẾT

**Yêu cầu 1:** Tạo tài khoản Oracle và đăng ký DB Security - Audit Vault and DB Firewall LiveLabs cho workshop này theo hướng dẫn sau:



## 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 page again** click the user dropdown in the top right corner and select **My Reservations**

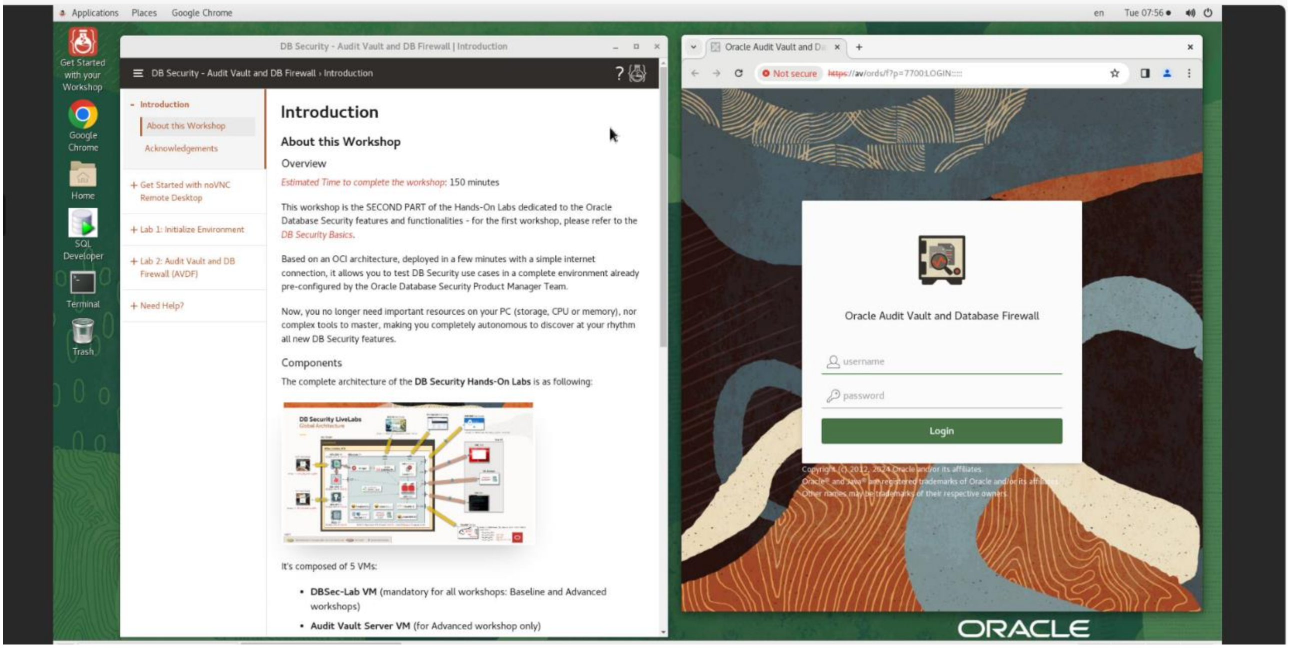
**Note:** The status of your reservations will be emailed to you. Check your mail for any status updates.

**DB Security - Audit Vault and DB Firewall**
Thursday April 4th, 1:14am (01:14) US/Pacific

Estimated Time Remaining: 39 mins

**Yêu cầu 2:** Thực hiện các yêu cầu của Workshop:
https://apexapps.oracle.com/pls/apex/r/dbpm/livelabs/view-workshop?wid=711

Lab1: Task 1: Access the Graphical Remote Desktop


Applications
Places
Google Chrome
en
Tue 07:56
Get Started with your Workshop
Google Chrome
Home
SQL Developer
Terminal
Trash
DB Security - Audit Vault and DB Firewall | Introduction
DB Security - Audit Vault and DB Firewall › Introduction
- Introduction
About this Workshop
Acknowledgements
+ Get Started with noVNC Remote Desktop
+ Lab 1: Initialize Environment
+ Lab 2: Audit Vault and DB Firewall (AVDF)
+ Need Help?
DB Security LiveLabs
Global Architecture
Oracle Audit Vault and D
Not secure
https://av/ords/f?p=7700:LOGIN:::::
username
password
Login
ORACLE

Introduction

About this Workshop

Overview

*Estimated Time to complete the workshop*: 150 minutes

This workshop is the SECOND PART of the Hands-On Labs dedicated to the Oracle Database Security features and functionalities - for the first workshop, please refer to the *DB Security Basics*.

Based on an OCI architecture, deployed in a few minutes with a simple internet connection, it allows you to test DB Security use cases in a complete environment already pre-configured by the Oracle Database Security Product Manager Team.

Now, you no longer need important resources on your PC (storage, CPU or memory), nor complex tools to master, making you completely autonomous to discover at your rhythm all new DB Security features.

Components

The complete architecture of the **DB Security Hands-On Labs** is as following:

It's composed of 5 VMs:

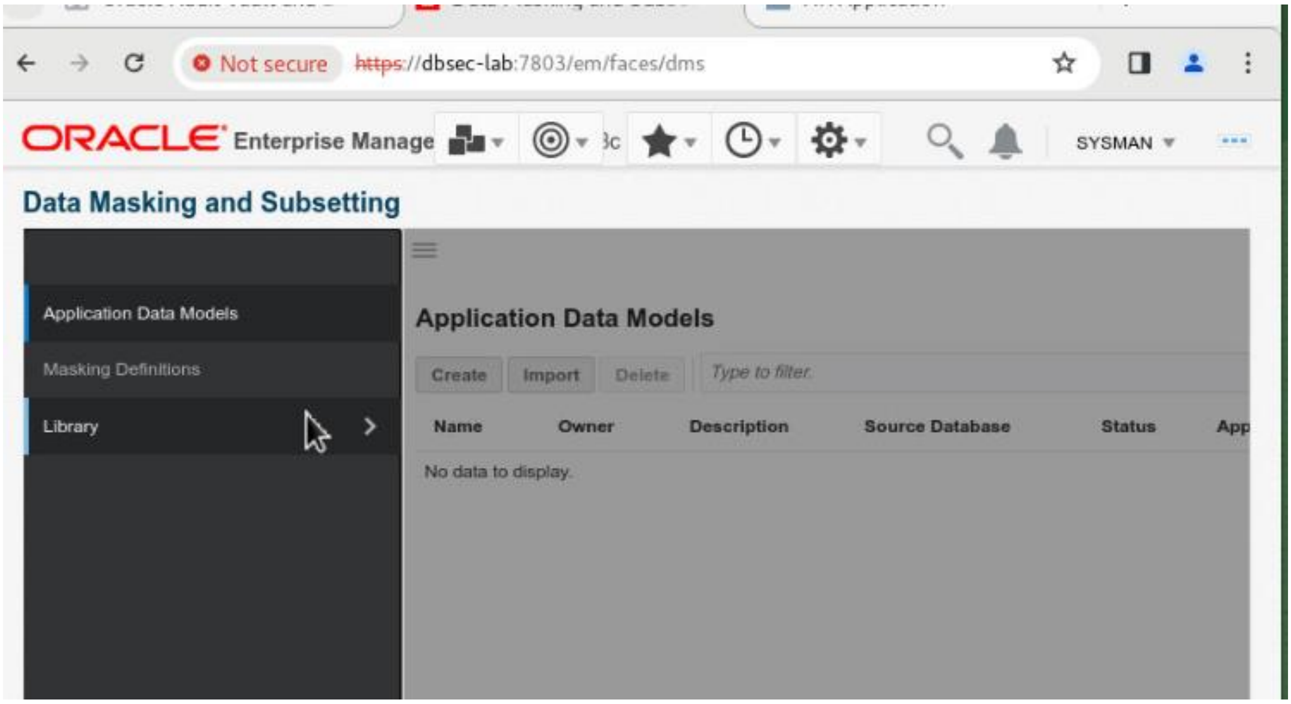
- **DBSec-Lab VM** (mandatory for all workshops: Baseline and Advanced workshops)
- **Audit Vault Server VM** (for Advanced workshop only)

Oracle Audit Vault and Database Firewall

Copyright (c) 2012, 2024 Oracle and/or its affiliates.
Oracle® and Java® are registered trademarks of Oracle and/or its affiliates.
Other names may be trademarks of their respective owners.

## Lab2: Initialize Environment

Task1:

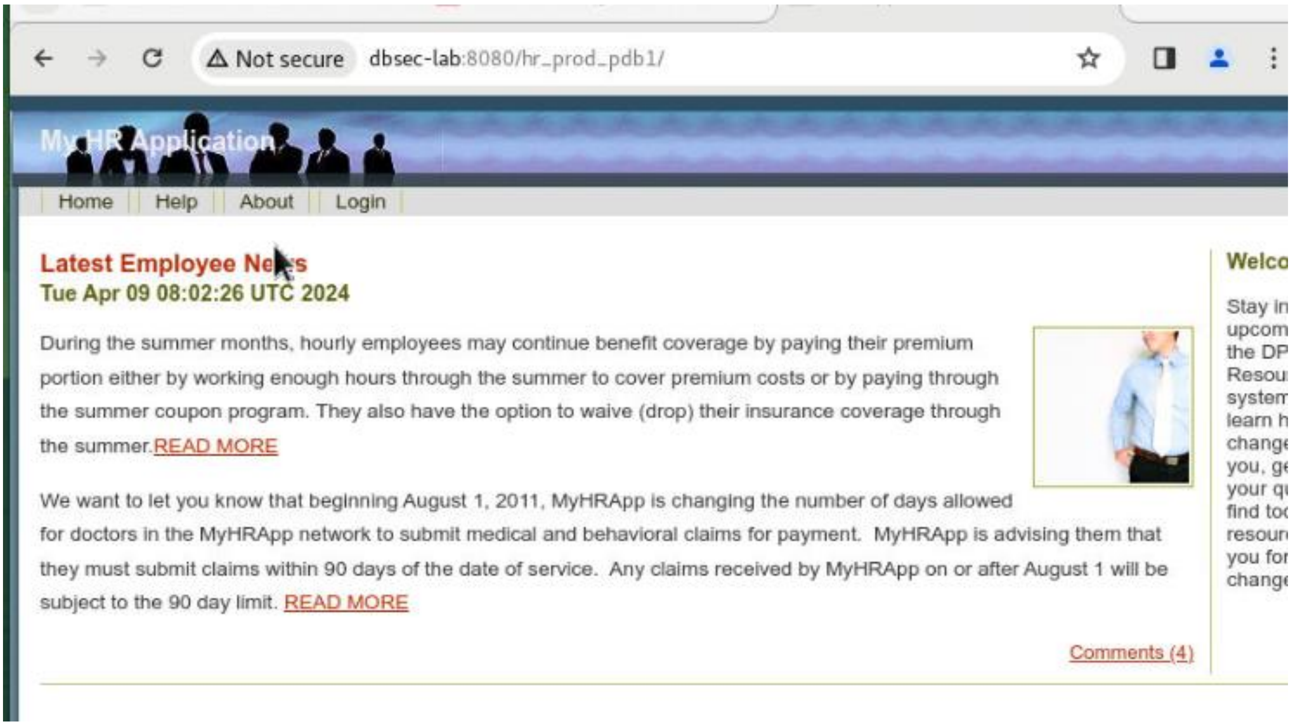


Data Masking and Subsetting

Application Data Models

| Name | Owner | Description | Source Database | Status | App |
|---|---|---|---|---|---|

No data to display.



Latest Employee News
Tue Apr 09 08:02:26 UTC 2024

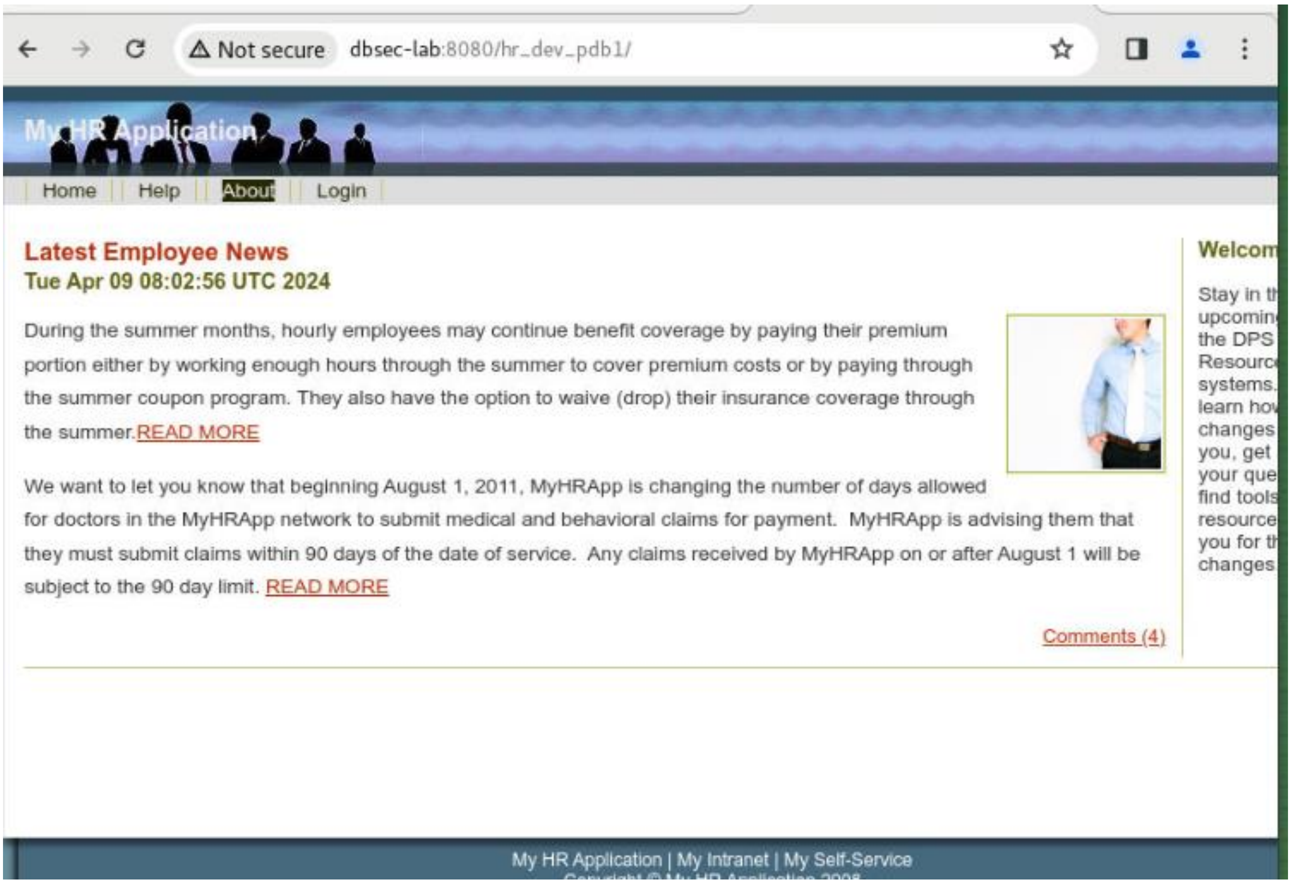
During the summer months, hourly employees may continue benefit coverage by paying their premium portion either by working enough hours through the summer to cover premium costs or by paying through the summer coupon program. They also have the option to waive (drop) their insurance coverage through the summer.READ MORE

We want to let you know that beginning August 1, 2011, MyHRApp is changing the number of days allowed for doctors in the MyHRApp network to submit medical and behavioral claims for payment. MyHRApp is advising them that they must submit claims within 90 days of the date of service. Any claims received by MyHRApp on or after August 1 will be subject to the 90 day limit. READ MORE

Comments (4)

Welco

Stay in upcom the DP Resou system learn h change you, ge your qu find too resour you for change



Latest Employee News
Tue Apr 09 08:02:56 UTC 2024

During the summer months, hourly employees may continue benefit coverage by paying their premium portion either by working enough hours through the summer to cover premium costs or by paying through the summer coupon program. They also have the option to waive (drop) their insurance coverage through the summer.READ MORE

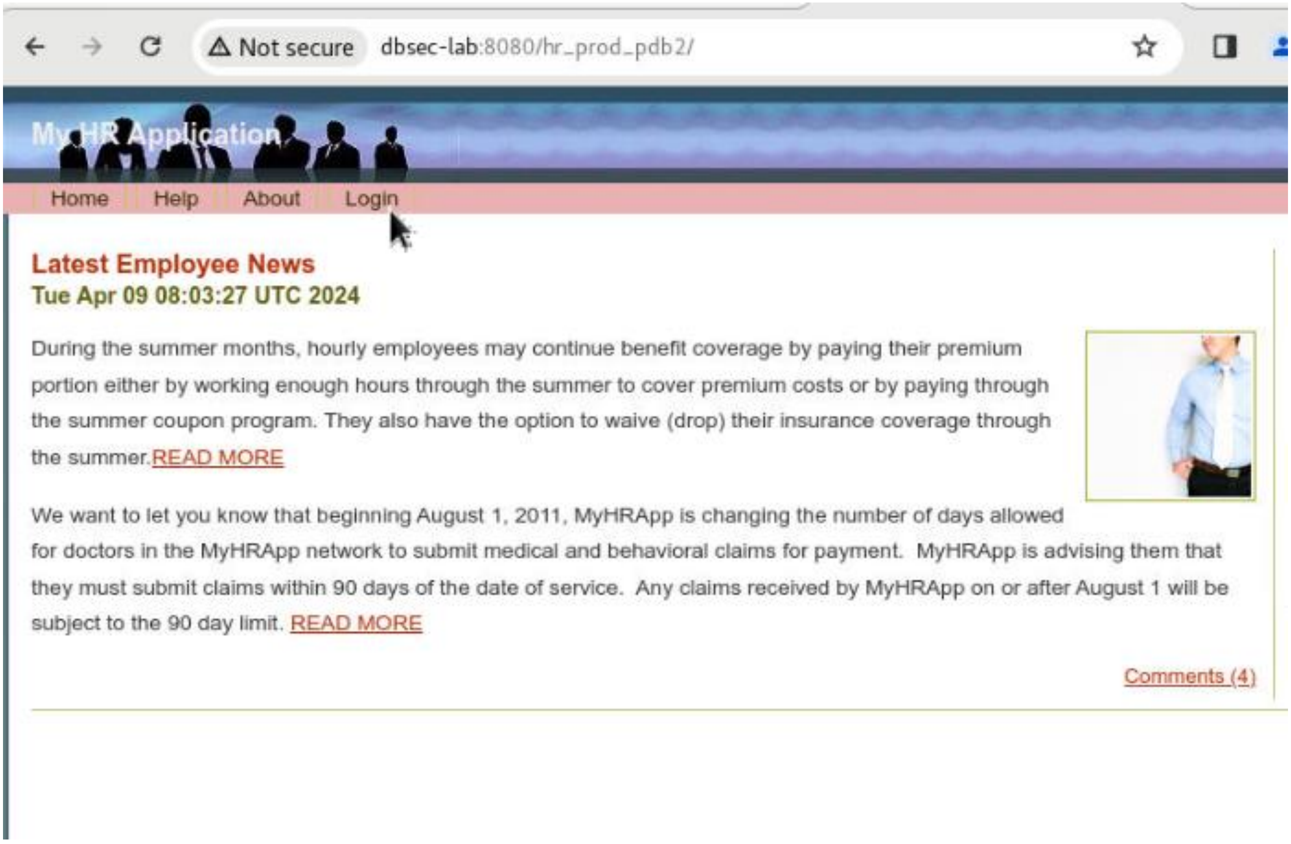
We want to let you know that beginning August 1, 2011, MyHRApp is changing the number of days allowed for doctors in the MyHRApp network to submit medical and behavioral claims for payment. MyHRApp is advising them that they must submit claims within 90 days of the date of service. Any claims received by MyHRApp on or after August 1 will be subject to the 90 day limit. READ MORE

Comments (4)

Welcom

Stay in th upcomin the DPS Resourc systems. learn how changes you, get your que find tools resource you for th changes

My HR Application | My Intranet | My Self-Service

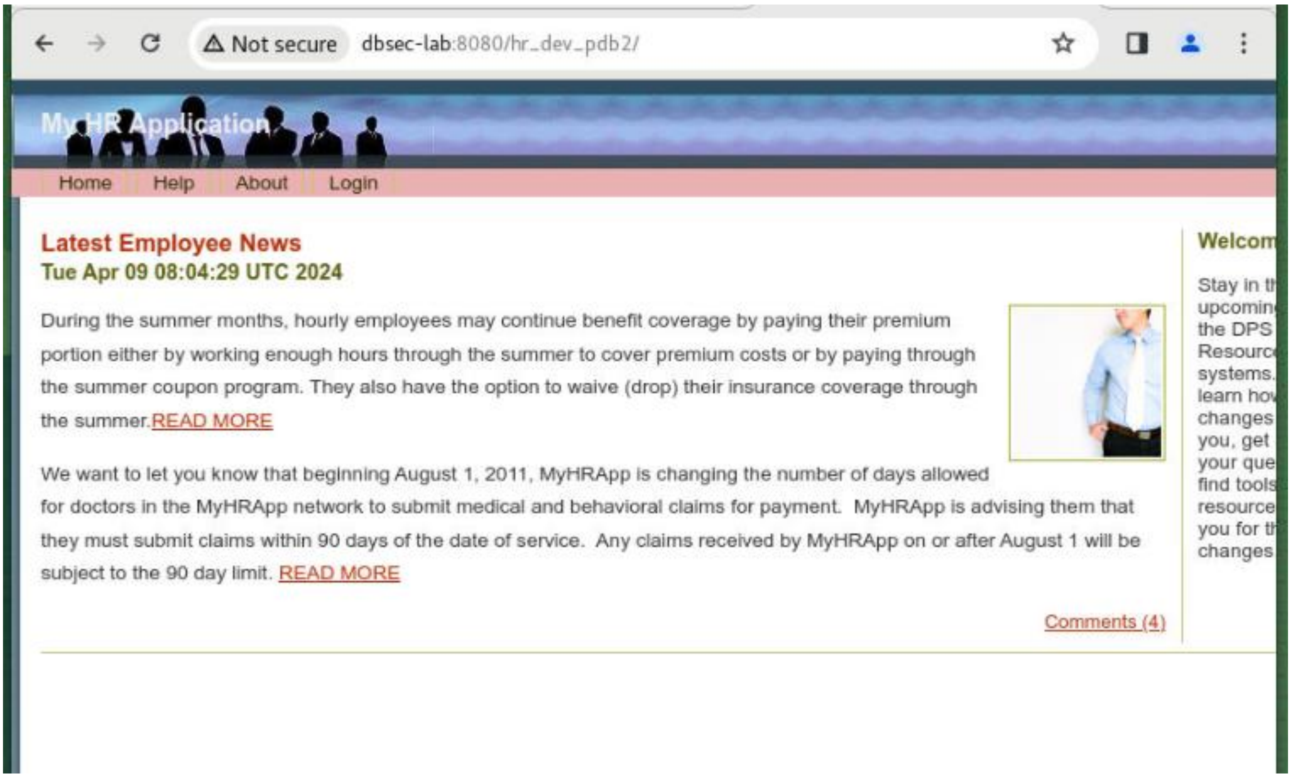


Latest Employee News
Tue Apr 09 08:03:27 UTC 2024

During the summer months, hourly employees may continue benefit coverage by paying their premium portion either by working enough hours through the summer to cover premium costs or by paying through the summer coupon program. They also have the option to waive (drop) their insurance coverage through the summer.READ MORE

We want to let you know that beginning August 1, 2011, MyHRApp is changing the number of days allowed for doctors in the MyHRApp network to submit medical and behavioral claims for payment. MyHRApp is advising them that they must submit claims within 90 days of the date of service. Any claims received by MyHRApp on or after August 1 will be subject to the 90 day limit. READ MORE

Comments (4)



**Latest Employee News**
**Tue Apr 09 08:04:29 UTC 2024**

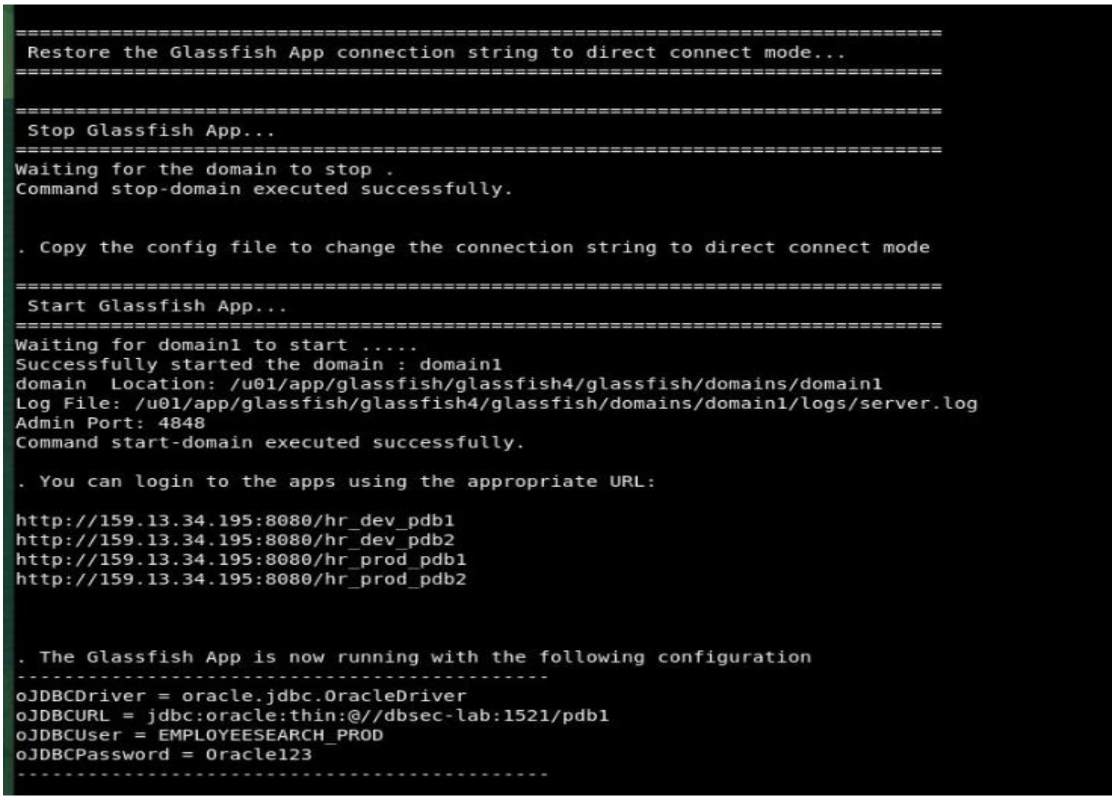
During the summer months, hourly employees may continue benefit coverage by paying their premium portion either by working enough hours through the summer to cover premium costs or by paying through the summer coupon program. They also have the option to waive (drop) their insurance coverage through the summer.READ MORE

We want to let you know that beginning August 1, 2011, MyHRApp is changing the number of days allowed for doctors in the MyHRApp network to submit medical and behavioral claims for payment. MyHRApp is advising them that they must submit claims within 90 days of the date of service. Any claims received by MyHRApp on or after August 1 will be subject to the 90 day limit. READ MORE

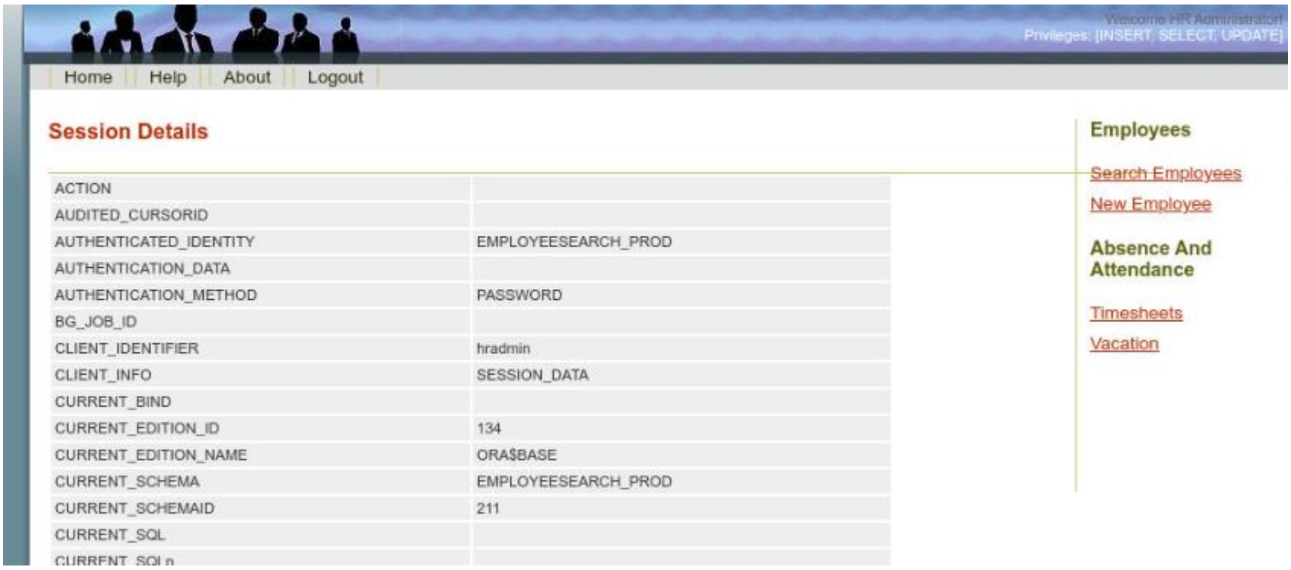
Comments (4)

**Welcom**

Stay in th
upcomin
the DPS
Resourc
systems.
learn ho
changes
you, get
your que
find tools
resource
you for th
changes



```
==============================================================================
 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://159.13.34.195:8080/hr_dev_pdb1
http://159.13.34.195:8080/hr_dev_pdb2
http://159.13.34.195:8080/hr_prod_pdb1
http://159.13.34.195:8080/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
oJDBCPassword = Oracle123
---------------------------------------------
```



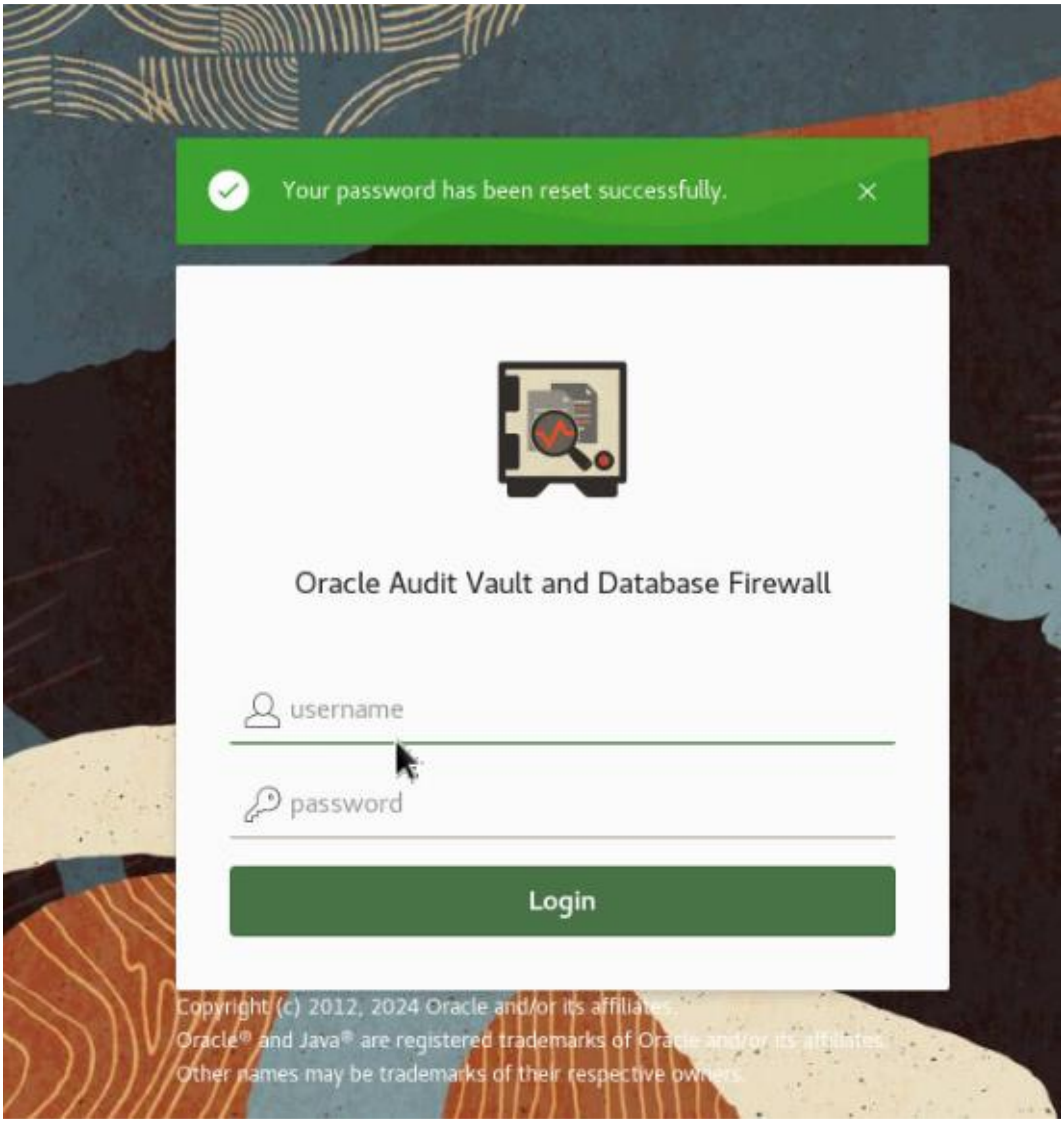
Welcome HR Administrator!
Privileges: [INSERT, SELECT, UPDATE]

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 | |

**Lab3: Oracle Audit Vault and DB Filewall**

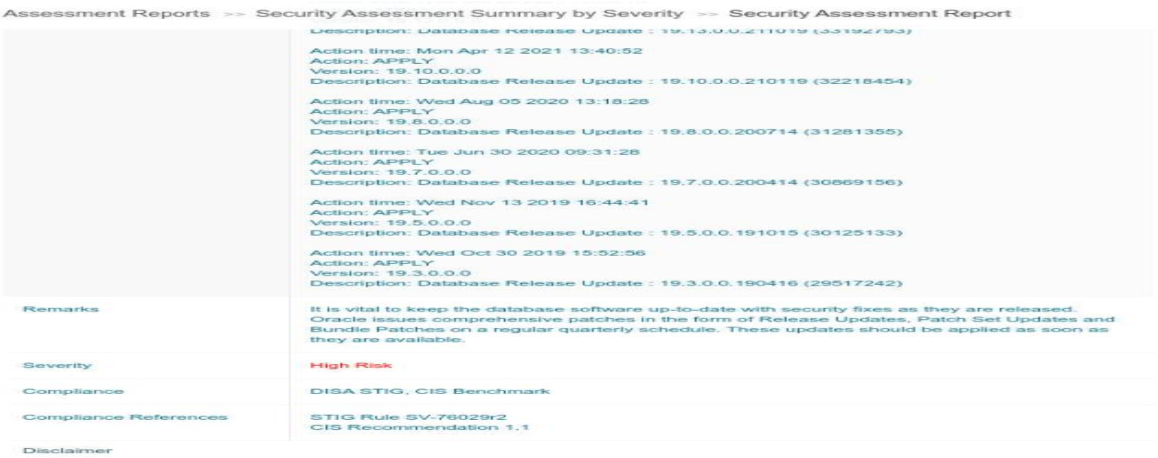
Task 1: Reset the randomly generated password



Your password has been reset successfully.

×
Oracle Audit Vault and Database Firewall
username
password
Login
Copyright (c) 2012, 2024 Oracle and/or its affiliates.
Oracle® and Java® are registered trademarks of Oracle and/or its affiliates.
Other names may be trademarks of their respective owners.

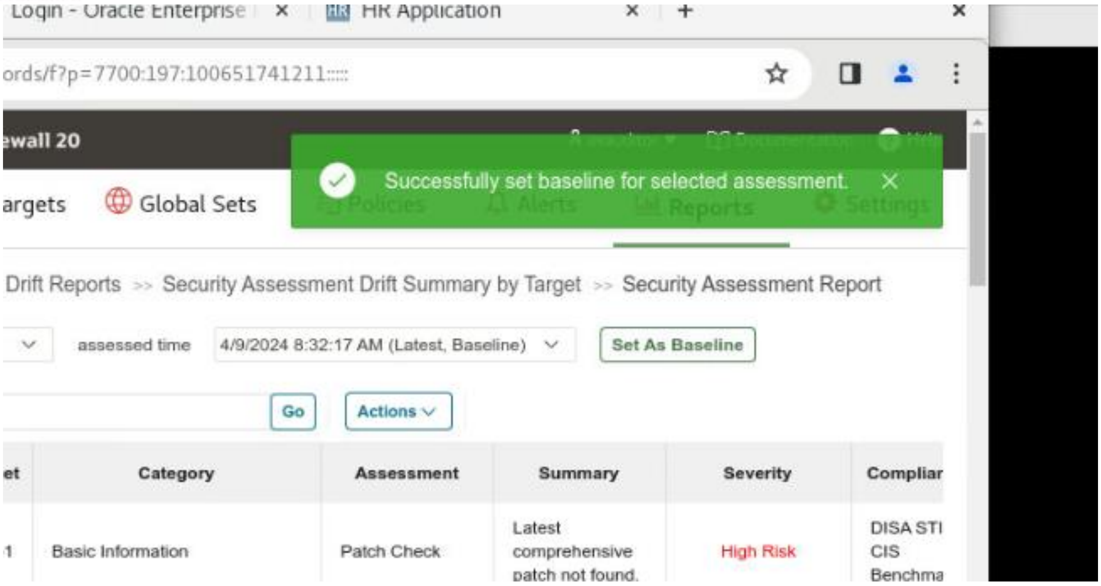
Task 2: Assess and Discover



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

```
Description: Database Release Update : 19.13.0.0.211019 (33192793)

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)

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)

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 (30869156)

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)

Action time: Wed Oct 30 2019 15:52:56
Action: APPLY
Version: 19.3.0.0.0
Description: Database Release Update : 19.3.0.0.190416 (29517242)
```

| | |
|---|---|
| Remarks | It is vital to keep the database software up-to-date with security fixes as they are released. Oracle issues comprehensive patches in the form of Release Updates, Patch Set Updates and Bundle Patches on a regular quarterly schedule. These updates should be applied as soon as they are available. |
| Severity | High Risk |
| Compliance | DISA STIG, CIS Benchmark |
| Compliance References | STIG Rule SV-76029r2<br>CIS Recommendation 1.1 |
| Disclaimer | |



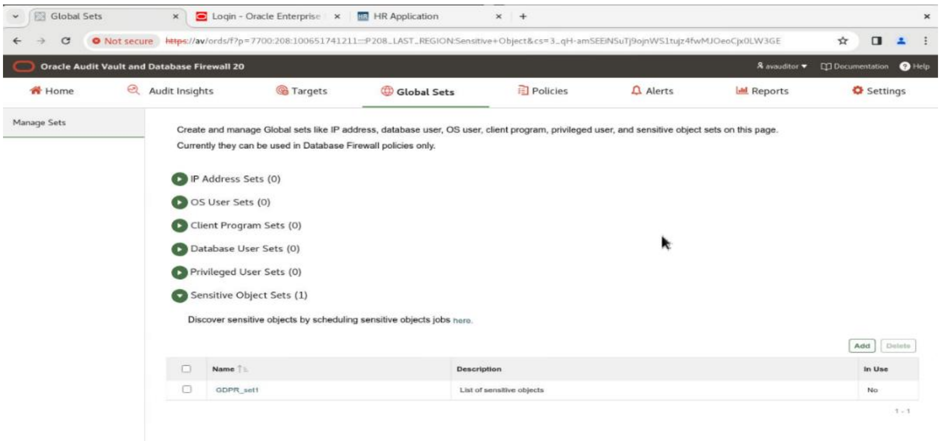
Successfully set baseline for selected assessment.

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

assessed time: 4/9/2024 8:32:17 AM (Latest, Baseline)  Set As Baseline

Go  Actions

| et | Category | Assessment | Summary | Severity | Compliar |
|---|---|---|---|---|---|
| 1 | Basic Information | Patch Check | Latest comprehensive patch not found. | High Risk | DISA STI<br>CIS<br>Benchma |



Global Sets
Login - Oracle Enterprise
HR Application
Not secure
https://av/ords/f?p=7700:208:100651741211:::P208_LAST_REGION:Sensitive+Object&cs=3_qH-amSEEiNSuTj9ojnWS1tujz4fwMJOeoCjx0LW3GE
Oracle Audit Vault and Database Firewall 20
avauditor
Documentation
Help
Home
Audit Insights
Targets
Global Sets
Policies
Alerts
Reports
Settings
Manage Sets

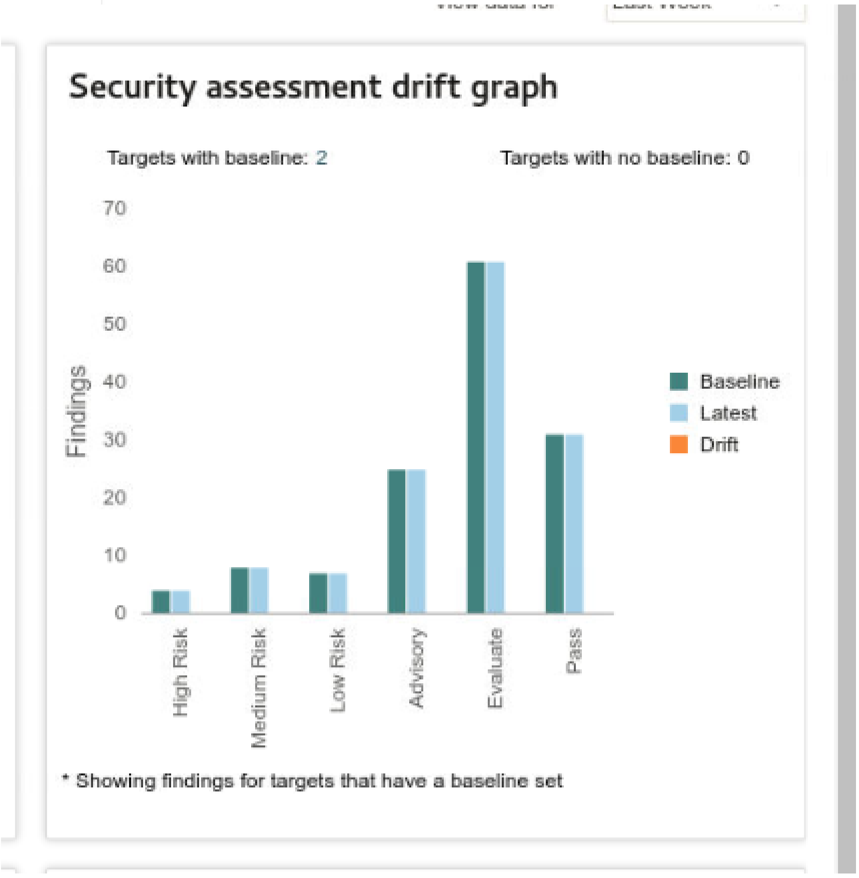
Create and manage Global sets like IP address, database user, OS user, client program, privileged user, and sensitive object sets on this page.
Currently they can be used in Database Firewall policies only.

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

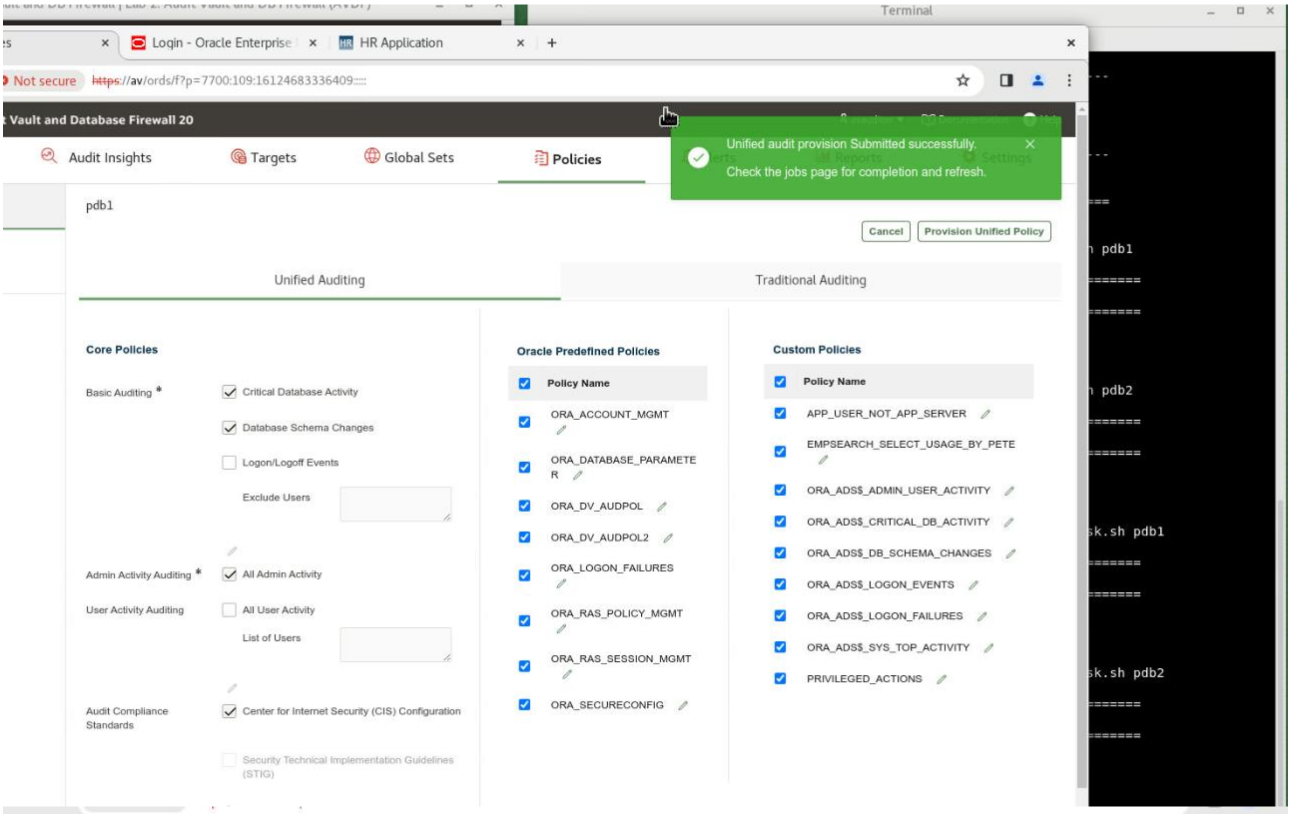
Discover sensitive objects by scheduling sensitive objects jobs here.

| □ | Name | Description | In Use |
|---|---|---|---|
| □ | GDPR_set1 | List of sensitive objects | No |

1 - 1



Task3: Audit and Monitor



Terminal
Login - Oracle Enterprise
HR Application
Not secure
https://av/ords/f?p=7700:109:16124683336409::::
Vault and Database Firewall 20
Audit Insights
Targets
Global Sets
Policies

Unified audit provision Submitted successfully.
Check the jobs page for completion and refresh.

pdb1

**Core Policies**

Basic Auditing *
- ☑ Critical Database Activity
- ☑ Database Schema Changes
- □ Logon/Logoff Events
- Exclude Users

Admin Activity Auditing *
- ☑ All Admin Activity

User Activity Auditing
- □ All User Activity
- List of Users

Audit Compliance Standards
- ☑ Center for Internet Security (CIS) Configuration
- □ Security Technical Implementation Guidelines (STIG)

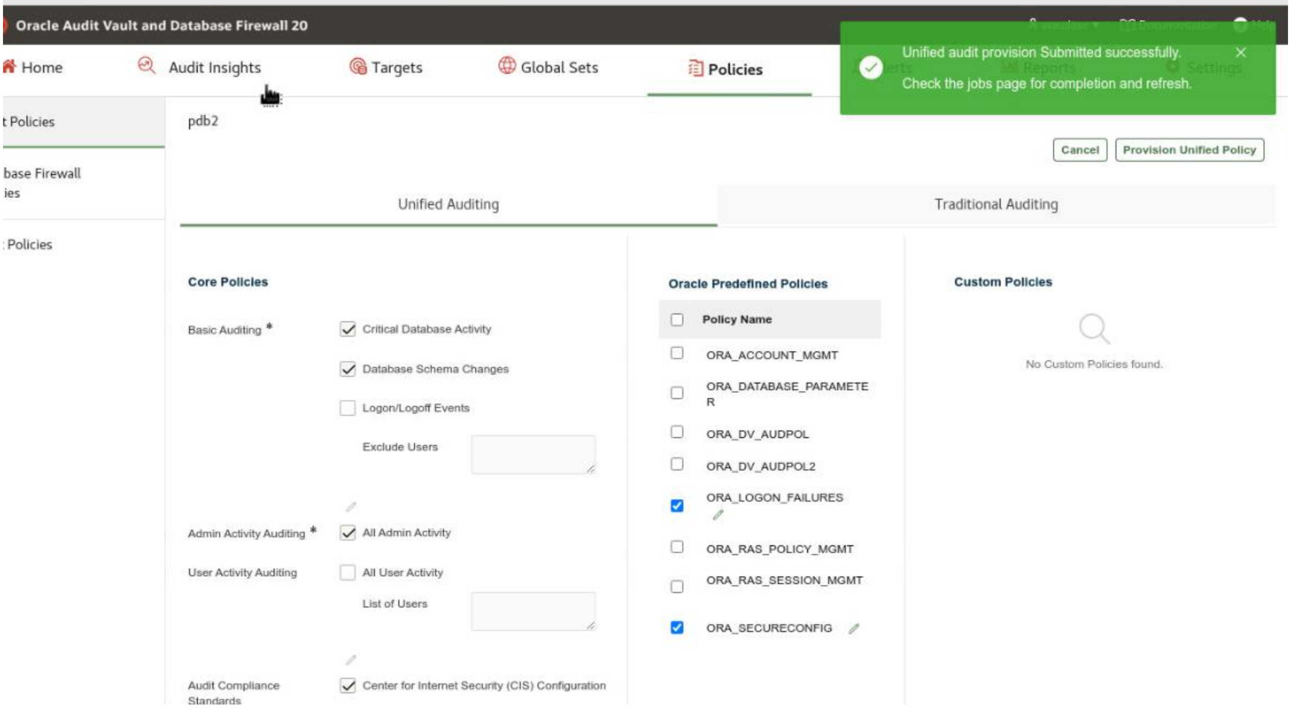
**Oracle Predefined Policies**

| ☑ | Policy Name |
|---|---|
| ☑ | ORA_ACCOUNT_MGMT |
| ☑ | ORA_DATABASE_PARAMETER |
| ☑ | ORA_DV_AUDPOL |
| ☑ | ORA_DV_AUDPOL2 |
| ☑ | ORA_LOGON_FAILURES |
| ☑ | ORA_RAS_POLICY_MGMT |
| ☑ | ORA_RAS_SESSION_MGMT |
| ☑ | ORA_SECURECONFIG |

**Custom Policies**

| ☑ | Policy Name |
|---|---|
| ☑ | APP_USER_NOT_APP_SERVER |
| ☑ | EMPSEARCH_SELECT_USAGE_BY_PETE |
| ☑ | 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 |
| ☑ | PRIVILEGED_ACTIONS |

```
---
---
===
h pdb1
=======
=======
h pdb2
=======
=======
sk.sh pdb1
=======
=======
sk.sh pdb2
=======
=======
```



Unified audit provision Submitted successfully.
Check the jobs page for completion and refresh.

pdb2

**Core Policies**

Basic Auditing *
- ☑ Critical Database Activity
- ☑ Database Schema Changes
- □ Logon/Logoff Events
- Exclude Users

Admin Activity Auditing *
- ☑ All Admin Activity

User Activity Auditing
- □ All User Activity
- List of Users

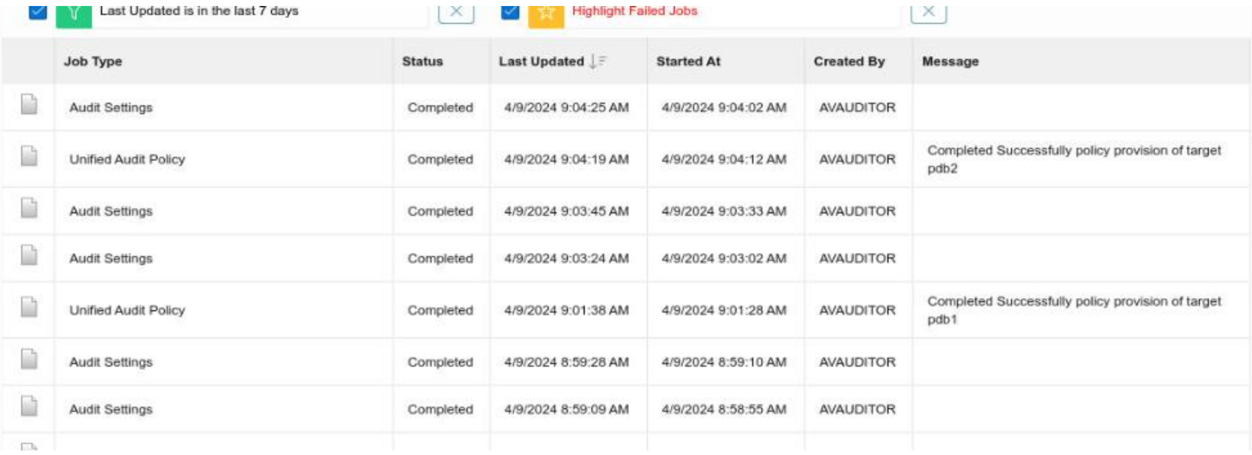
Audit Compliance Standards
- ☑ Center for Internet Security (CIS) Configuration

**Oracle Predefined Policies**

| □ | Policy Name |
|---|---|
| □ | ORA_ACCOUNT_MGMT |
| □ | ORA_DATABASE_PARAMETER |
| □ | ORA_DV_AUDPOL |
| □ | ORA_DV_AUDPOL2 |
| ☑ | ORA_LOGON_FAILURES |
| □ | ORA_RAS_POLICY_MGMT |
| □ | ORA_RAS_SESSION_MGMT |
| ☑ | ORA_SECURECONFIG |

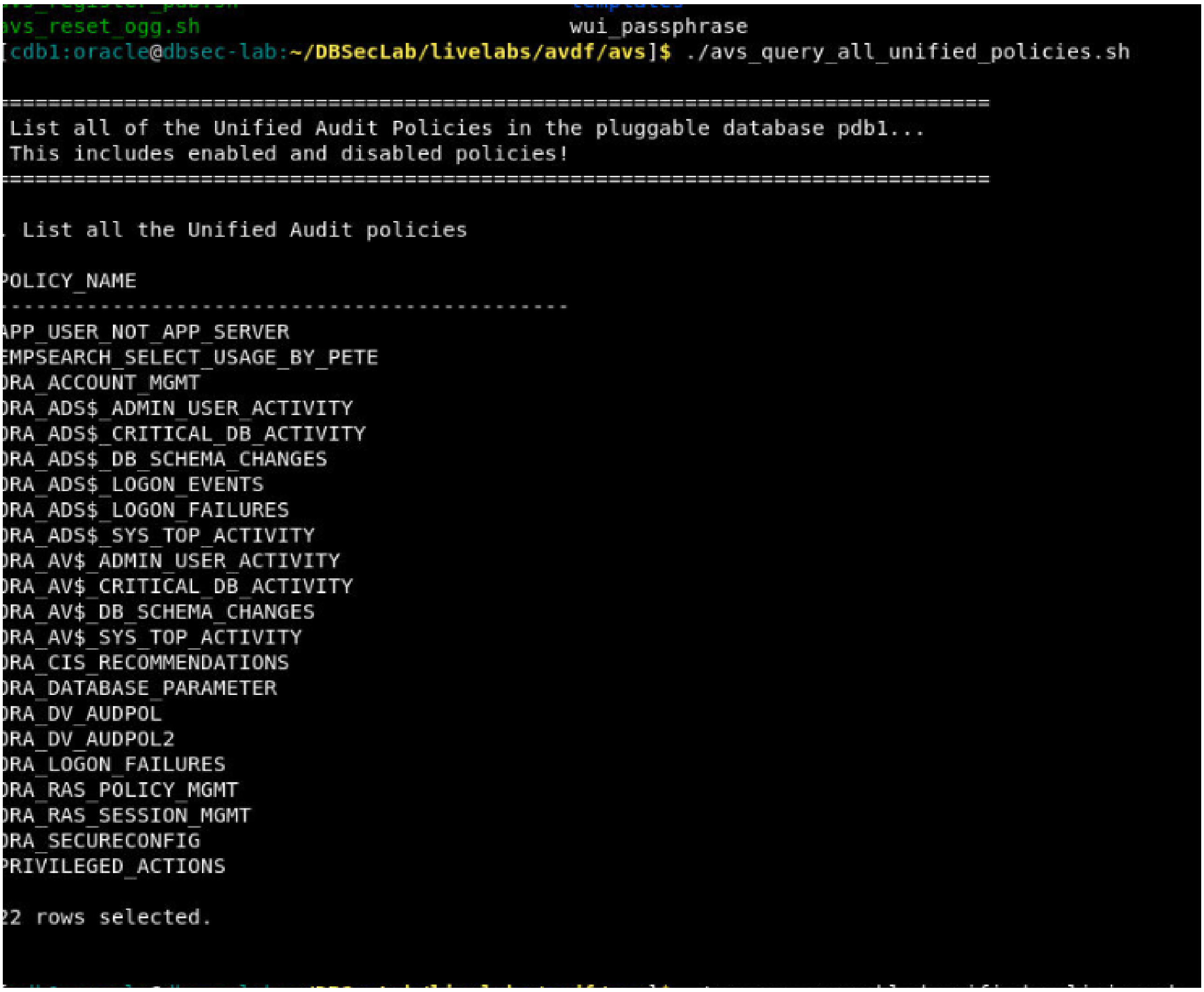
**Custom Policies**

No Custom Policies found.

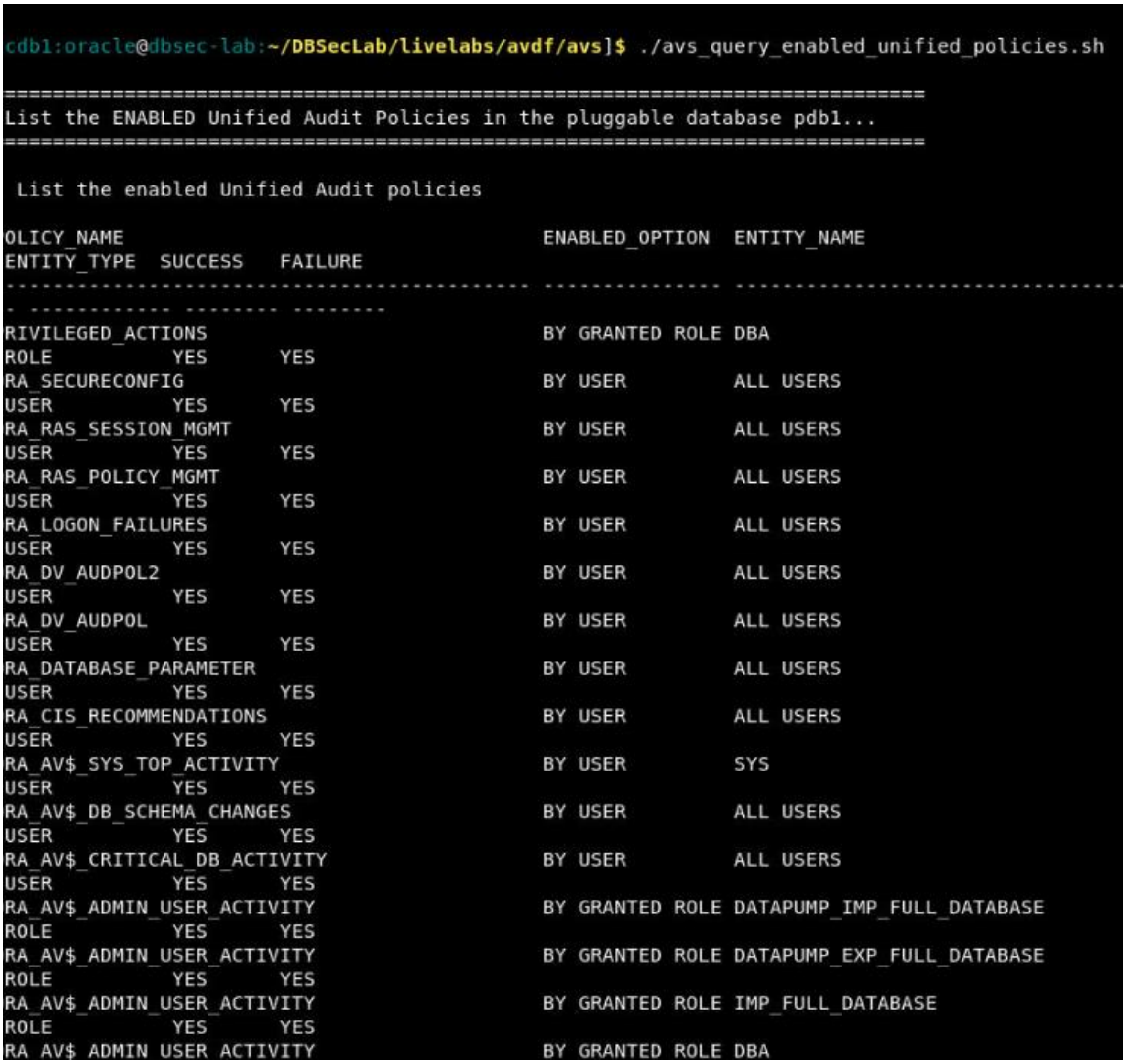


☑ Last Updated is in the last 7 days ✕ ☑ Highlight Failed Jobs ✕

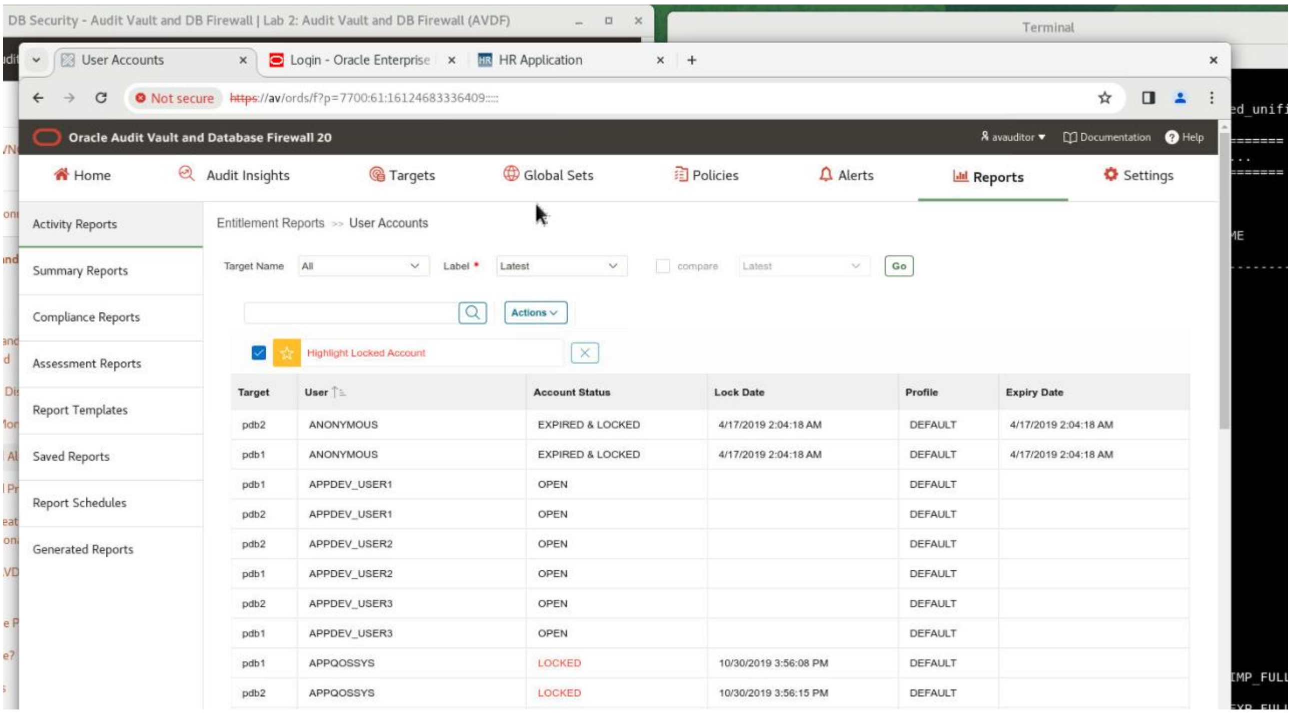
| | Job Type | Status | Last Updated | Started At | Created By | Message |
|---|---|---|---|---|---|---|
| | Audit Settings | Completed | 4/9/2024 9:04:25 AM | 4/9/2024 9:04:02 AM | AVAUDITOR | |
| | Unified Audit Policy | Completed | 4/9/2024 9:04:19 AM | 4/9/2024 9:04:12 AM | AVAUDITOR | Completed Successfully policy provision of target pdb2 |
| | Audit Settings | Completed | 4/9/2024 9:03:45 AM | 4/9/2024 9:03:33 AM | AVAUDITOR | |
| | Audit Settings | Completed | 4/9/2024 9:03:24 AM | 4/9/2024 9:03:02 AM | AVAUDITOR | |
| | Unified Audit Policy | Completed | 4/9/2024 9:01:38 AM | 4/9/2024 9:01:28 AM | AVAUDITOR | Completed Successfully policy provision of target pdb1 |
| | Audit Settings | Completed | 4/9/2024 8:59:28 AM | 4/9/2024 8:59:10 AM | AVAUDITOR | |
| | Audit Settings | Completed | 4/9/2024 8:59:09 AM | 4/9/2024 8:58:55 AM | AVAUDITOR | |



```
avs_reset_ogg.sh                                wui_passphrase
[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_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
PRIVILEGED_ACTIONS

22 rows selected.
```



```
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

OLICY_NAME                                   ENABLED_OPTION  ENTITY_NAME
ENTITY_TYPE  SUCCESS   FAILURE
-------------------------------------------- --------------- ---------------------------------
- ------------ -------- --------
RIVILEGED_ACTIONS                            BY GRANTED ROLE DBA
ROLE          YES       YES
RA_SECURECONFIG                              BY USER         ALL USERS
USER          YES       YES
RA_RAS_SESSION_MGMT                          BY USER         ALL USERS
USER          YES       YES
RA_RAS_POLICY_MGMT                           BY USER         ALL USERS
USER          YES       YES
RA_LOGON_FAILURES                            BY USER         ALL USERS
USER          YES       YES
RA_DV_AUDPOL2                                BY USER         ALL USERS
USER          YES       YES
RA_DV_AUDPOL                                 BY USER         ALL USERS
USER          YES       YES
RA_DATABASE_PARAMETER                        BY USER         ALL USERS
USER          YES       YES
RA_CIS_RECOMMENDATIONS                       BY USER         ALL USERS
USER          YES       YES
RA_AV$_SYS_TOP_ACTIVITY                      BY USER         SYS
USER          YES       YES
RA_AV$_DB_SCHEMA_CHANGES                     BY USER         ALL USERS
USER          YES       YES
RA_AV$_CRITICAL_DB_ACTIVITY                  BY USER         ALL USERS
USER          YES       YES
RA_AV$_ADMIN_USER_ACTIVITY                   BY GRANTED ROLE DATAPUMP_IMP_FULL_DATABASE
ROLE          YES       YES
RA_AV$_ADMIN_USER_ACTIVITY                   BY GRANTED ROLE DATAPUMP_EXP_FULL_DATABASE
ROLE          YES       YES
RA_AV$_ADMIN_USER_ACTIVITY                   BY GRANTED ROLE IMP_FULL_DATABASE
ROLE          YES       YES
RA_AV$_ADMIN_USER_ACTIVITY                   BY GRANTED ROLE DBA
```

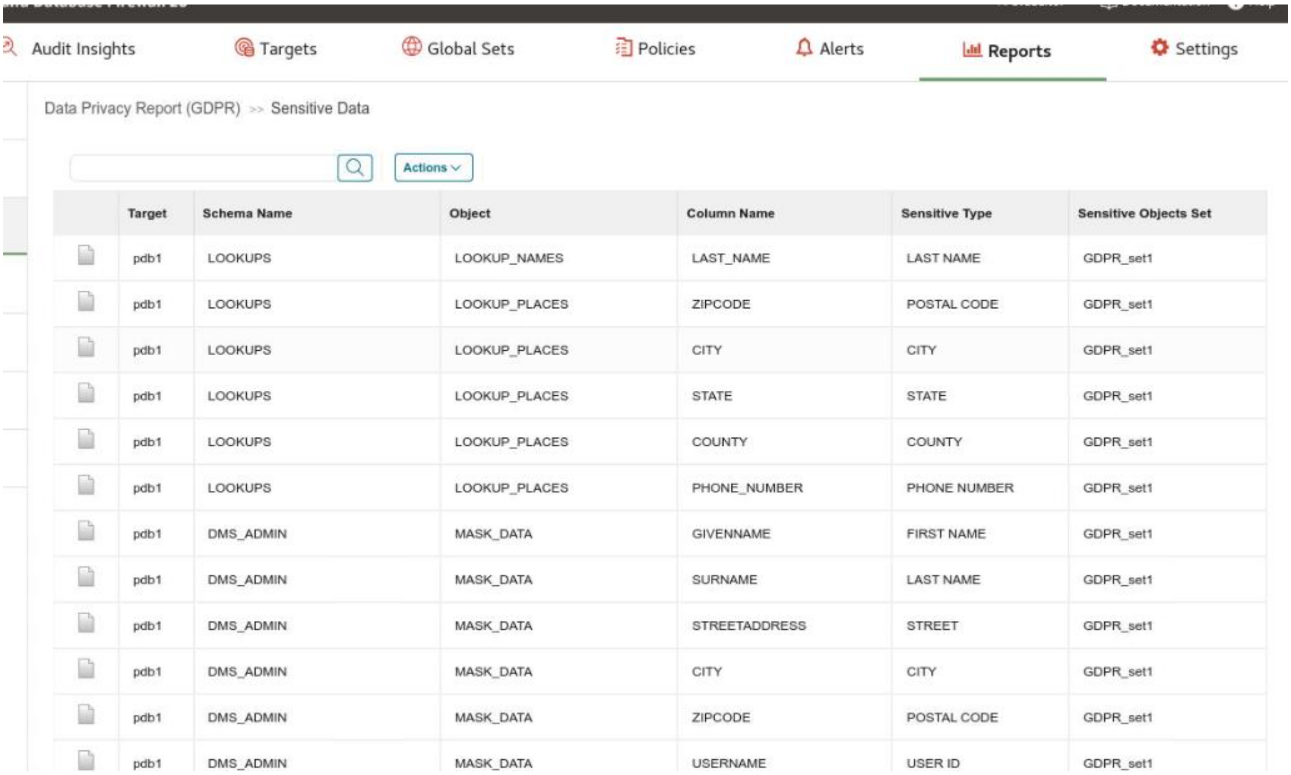


Target Name: All
Label *: Latest
□ compare: Latest

☑ Highlight Locked Account

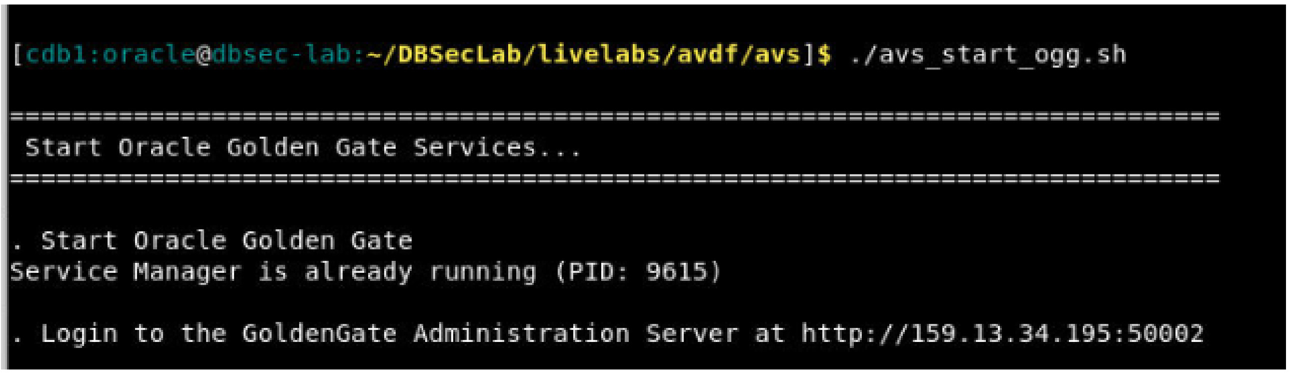
| Target | User | Account Status | Lock Date | Profile | Expiry Date |
|---|---|---|---|---|---|
| pdb2 | ANONYMOUS | EXPIRED & LOCKED | 4/17/2019 2:04:18 AM | DEFAULT | 4/17/2019 2:04:18 AM |
| pdb1 | ANONYMOUS | EXPIRED & LOCKED | 4/17/2019 2:04:18 AM | DEFAULT | 4/17/2019 2:04:18 AM |
| pdb1 | APPDEV_USER1 | OPEN |  | DEFAULT |  |
| pdb2 | APPDEV_USER1 | OPEN |  | DEFAULT |  |
| pdb2 | APPDEV_USER2 | OPEN |  | DEFAULT |  |
| pdb1 | APPDEV_USER2 | OPEN |  | DEFAULT |  |
| pdb2 | APPDEV_USER3 | OPEN |  | DEFAULT |  |
| pdb1 | APPDEV_USER3 | OPEN |  | DEFAULT |  |
| pdb1 | APPQOSSYS | LOCKED | 10/30/2019 3:56:08 PM | DEFAULT |  |
| pdb2 | APPQOSSYS | LOCKED | 10/30/2019 3:56:15 PM | DEFAULT |  |

## Task 4: Report and Alert

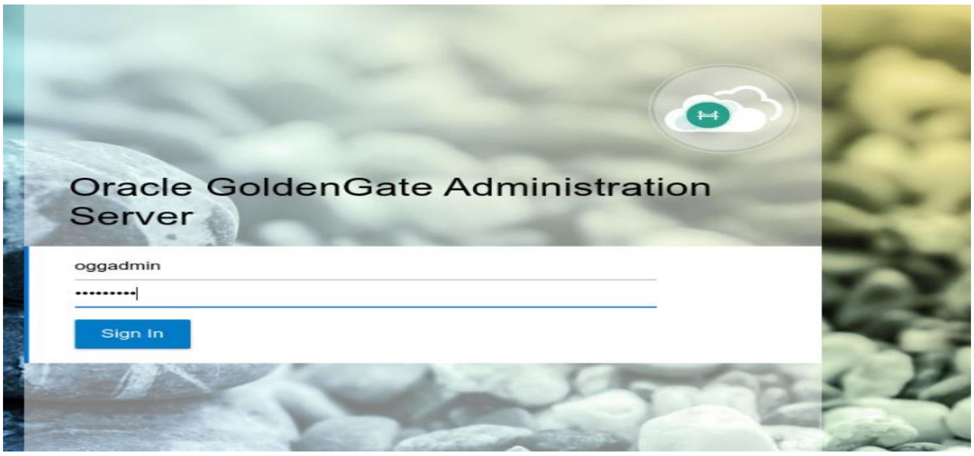


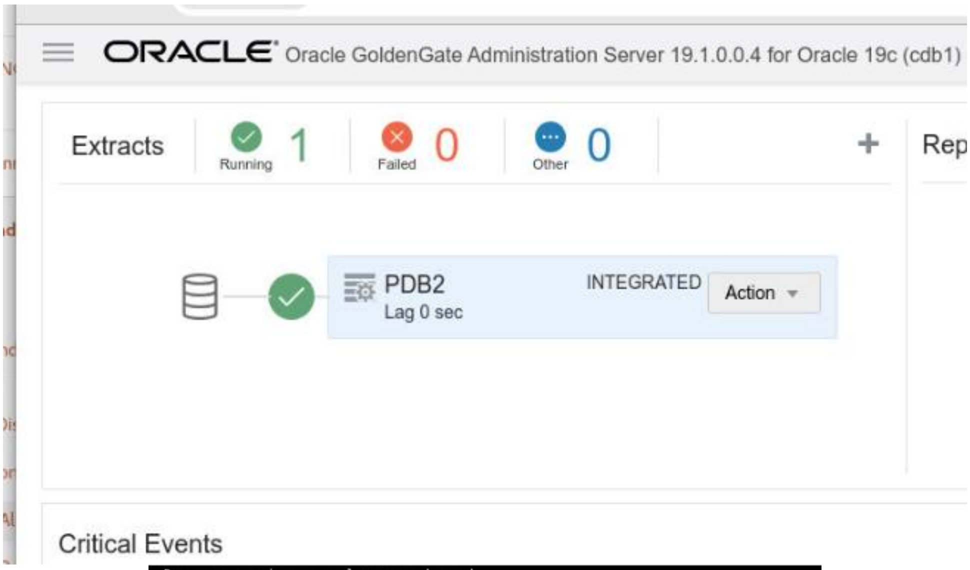
Data Privacy Report (GDPR) >> Sensitive Data

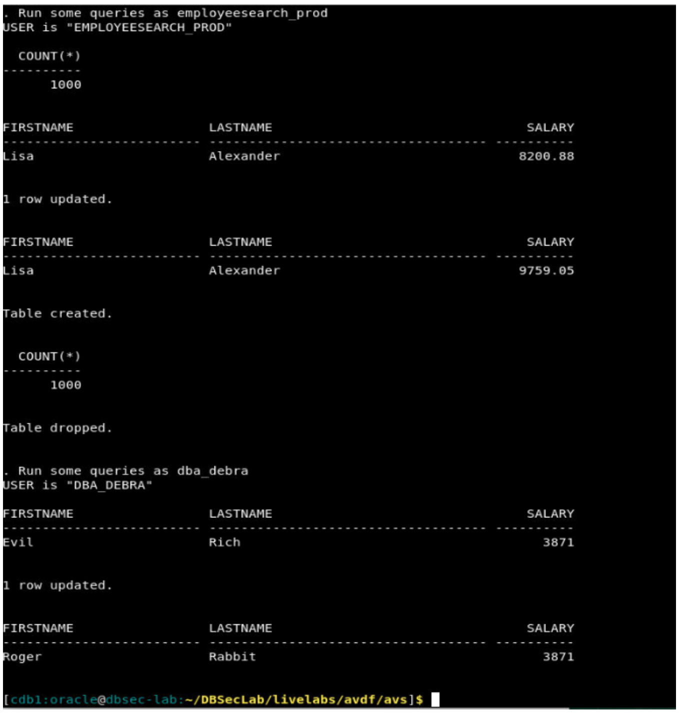
| | Target | Schema Name | Object | Column Name | Sensitive Type | Sensitive Objects Set |
|---|---|---|---|---|---|---|
| | pdb1 | LOOKUPS | LOOKUP_NAMES | LAST_NAME | LAST NAME | GDPR_set1 |
| | pdb1 | LOOKUPS | LOOKUP_PLACES | ZIPCODE | POSTAL CODE | GDPR_set1 |
| | pdb1 | LOOKUPS | LOOKUP_PLACES | CITY | CITY | GDPR_set1 |
| | pdb1 | LOOKUPS | LOOKUP_PLACES | STATE | STATE | GDPR_set1 |
| | pdb1 | LOOKUPS | LOOKUP_PLACES | COUNTY | COUNTY | GDPR_set1 |
| | pdb1 | LOOKUPS | LOOKUP_PLACES | PHONE_NUMBER | PHONE NUMBER | GDPR_set1 |
| | 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 |



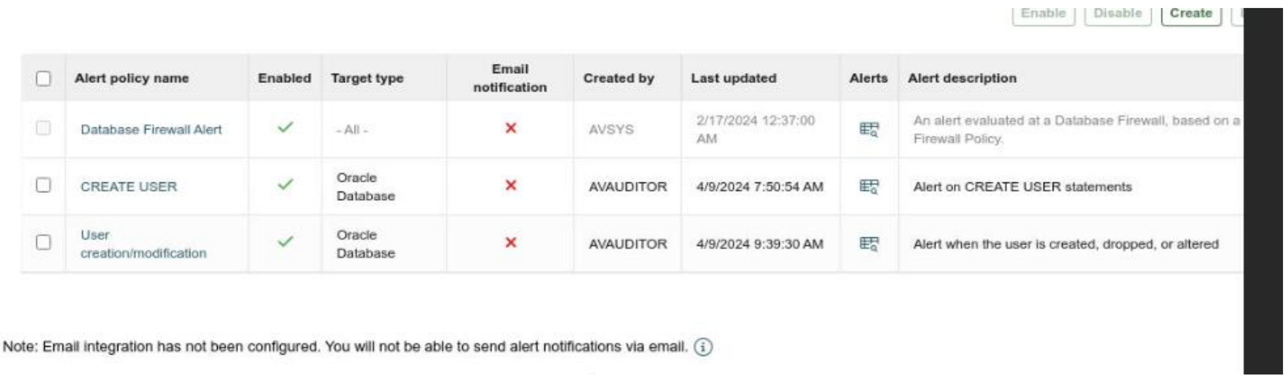
```
[cdb1:oracle@dbsec-lab:~/DBSecLab/livelabs/avdf/avs]$ ./avs_start_ogg.sh

==============================================================================
 Start Oracle Golden Gate Services...
==============================================================================

. Start Oracle Golden Gate
Service Manager is already running (PID: 9615)

. Login to the GoldenGate Administration Server at http://159.13.34.195:50002
```





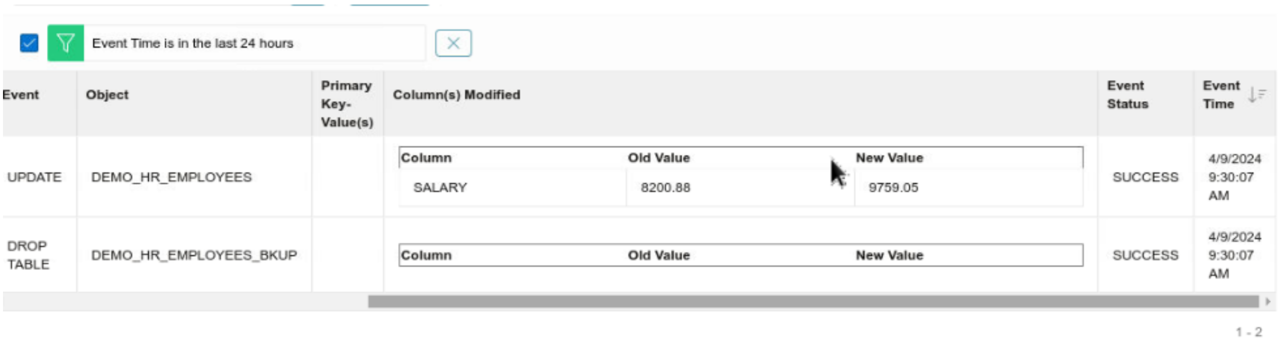


```
. Run some queries as employeesearch_prod
USER is "EMPLOYEESEARCH_PROD"

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

FIRSTNAME                 LASTNAME                                 SALARY
------------------------- ------------------------------------ ----------
Lisa                      Alexander                               8200.88

1 row updated.

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

Table created.

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

Table dropped.

. Run some queries as dba_debra
USER is "DBA_DEBRA"

FIRSTNAME                 LASTNAME                                 SALARY
------------------------- ------------------------------------ ----------
Evil                      Rich                                       3871

1 row updated.

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

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



| ☐ | Alert policy name | Enabled | Target type | Email notification | Created by | Last updated | Alerts | Alert description |
|---|---|---|---|---|---|---|---|---|
| ☐ | Database Firewall Alert | ✓ | - All - | ✗ | AVSYS | 2/17/2024 12:37:00 AM | ▤ | An alert evaluated at a Database Firewall, based on a Firewall Policy. |
| ☐ | CREATE USER | ✓ | Oracle Database | ✗ | AVAUDITOR | 4/9/2024 7:50:54 AM | ▤ | Alert on CREATE USER statements |
| ☐ | User creation/modification | ✓ | Oracle Database | ✗ | AVAUDITOR | 4/9/2024 9:39:30 AM | ▤ | Alert when the user is created, dropped, or altered |

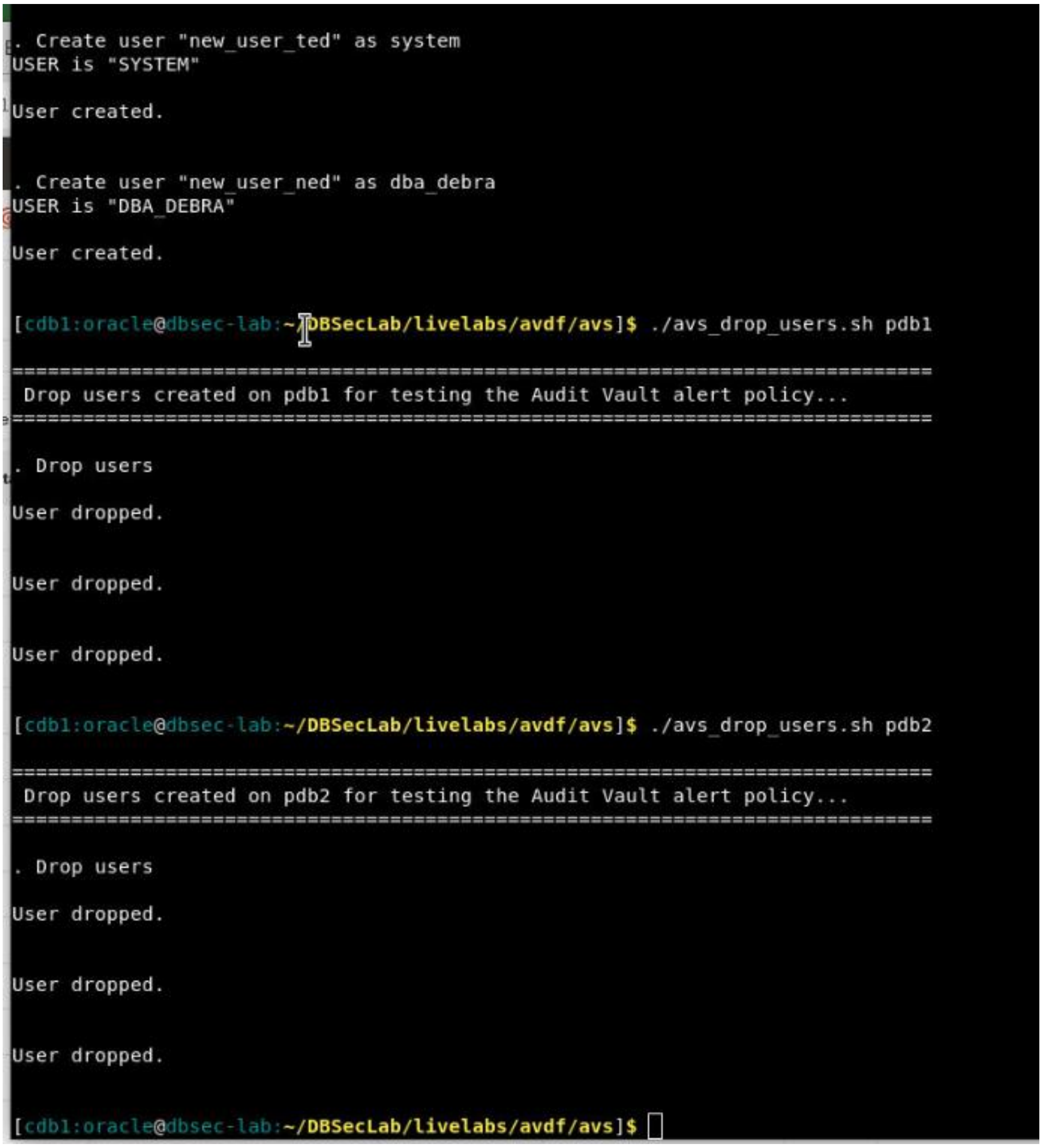
Note: Email integration has not been configured. You will not be able to send alert notifications via email. ⓘ



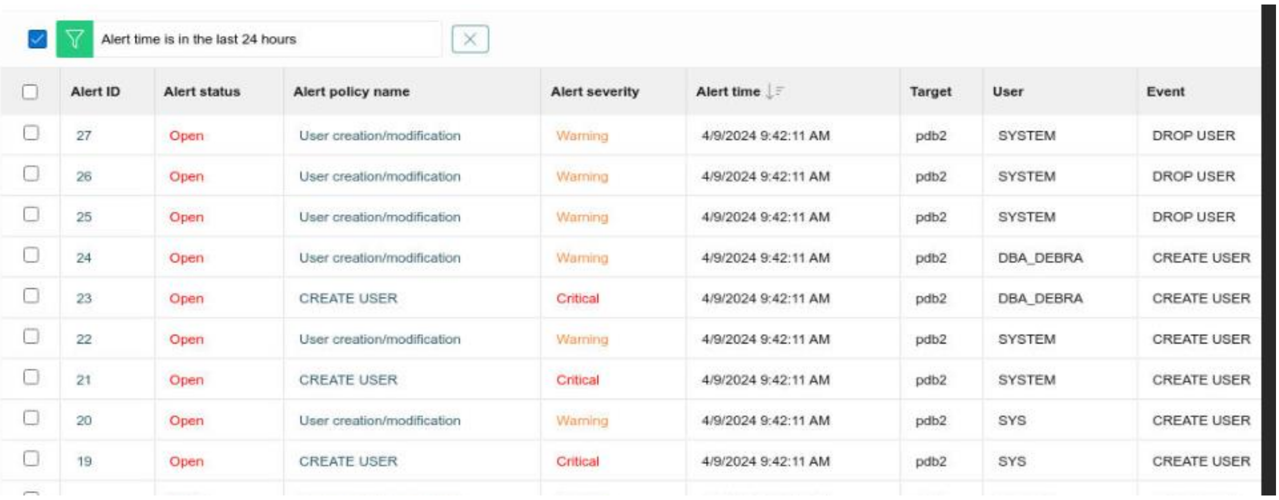
☑ Event Time is in the last 24 hours ✕

| Event | Object | Primary Key-Value(s) | Column(s) Modified | Event Status | Event Time |
|---|---|---|---|---|---|
| UPDATE | DEMO_HR_EMPLOYEES | | Column / Old Value / New Value<br>SALARY / 8200.88 / 9759.05 | SUCCESS | 4/9/2024 9:30:07 AM |
| DROP TABLE | DEMO_HR_EMPLOYEES_BKUP | | Column / Old Value / New Value | SUCCESS | 4/9/2024 9:30:07 AM |

1 - 2

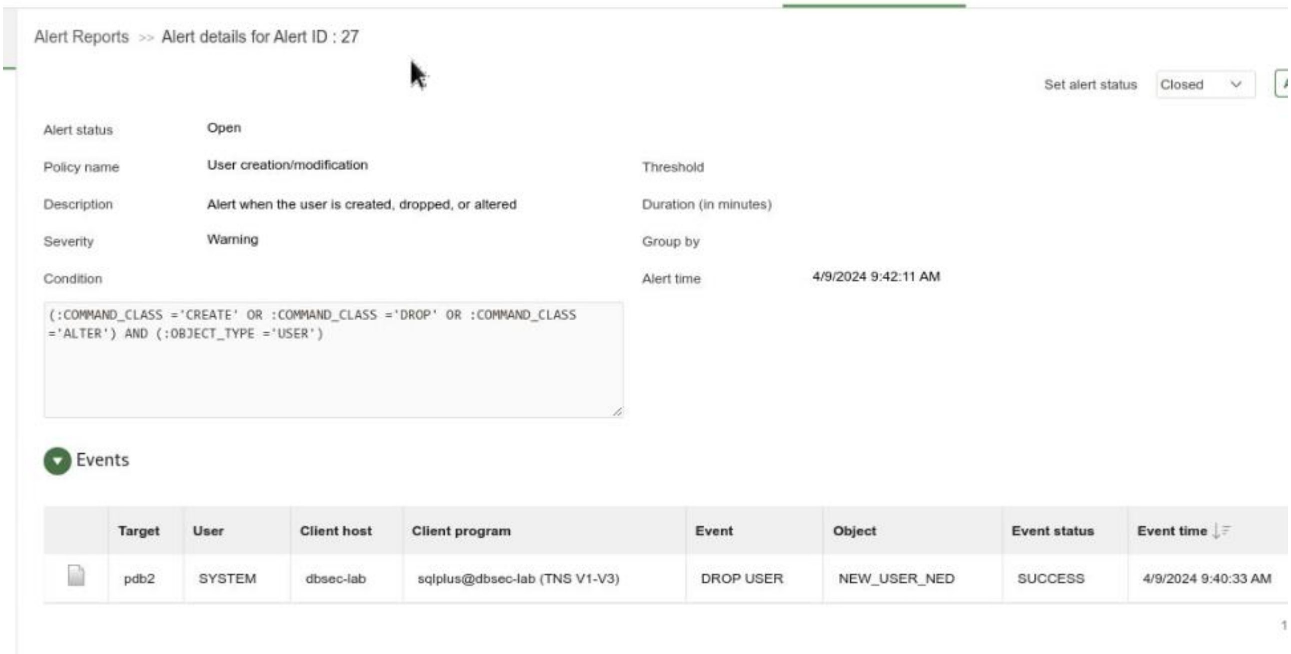


```
. Create user "new_user_ted" as system
USER is "SYSTEM"

User created.


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

User created.


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



☑ Alert time is in the last 24 hours

| □ | Alert ID | Alert status | Alert policy name | Alert severity | Alert time | Target | User | Event |
|---|---|---|---|---|---|---|---|---|
| □ | 27 | Open | User creation/modification | Warning | 4/9/2024 9:42:11 AM | pdb2 | SYSTEM | DROP USER |
| □ | 26 | Open | User creation/modification | Warning | 4/9/2024 9:42:11 AM | pdb2 | SYSTEM | DROP USER |
| □ | 25 | Open | User creation/modification | Warning | 4/9/2024 9:42:11 AM | pdb2 | SYSTEM | DROP USER |
| □ | 24 | Open | User creation/modification | Warning | 4/9/2024 9:42:11 AM | pdb2 | DBA_DEBRA | CREATE USER |
| □ | 23 | Open | CREATE USER | Critical | 4/9/2024 9:42:11 AM | pdb2 | DBA_DEBRA | CREATE USER |
| □ | 22 | Open | User creation/modification | Warning | 4/9/2024 9:42:11 AM | pdb2 | SYSTEM | CREATE USER |
| □ | 21 | Open | CREATE USER | Critical | 4/9/2024 9:42:11 AM | pdb2 | SYSTEM | CREATE USER |
| □ | 20 | Open | User creation/modification | Warning | 4/9/2024 9:42:11 AM | pdb2 | SYS | CREATE USER |
| □ | 19 | Open | CREATE USER | Critical | 4/9/2024 9:42:11 AM | pdb2 | SYS | CREATE USER |



Alert Reports >> Alert details for Alert ID : 27

Set alert status: Closed

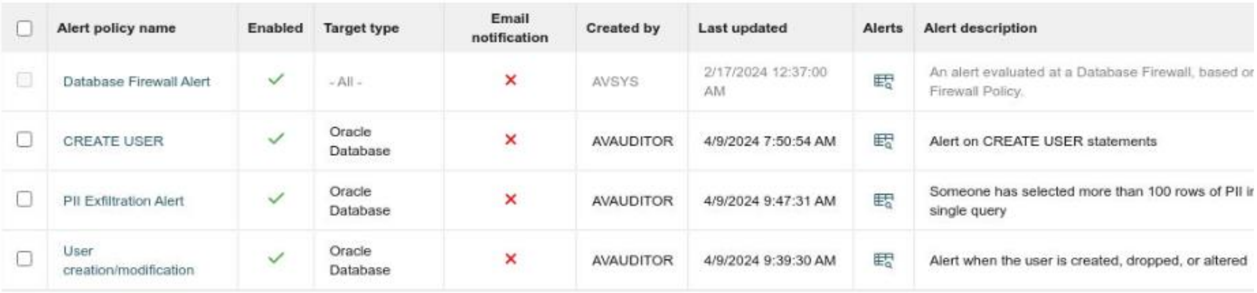
| | | | |
|---|---|---|---|
| Alert status | Open | | |
| Policy name | User creation/modification | Threshold | |
| Description | Alert when the user is created, dropped, or altered | Duration (in minutes) | |
| Severity | Warning | Group by | |
| Condition | | Alert time | 4/9/2024 9:42:11 AM |

```
(:COMMAND_CLASS ='CREATE' OR :COMMAND_CLASS ='DROP' OR :COMMAND_CLASS
='ALTER') AND (:OBJECT_TYPE ='USER')
```

Events

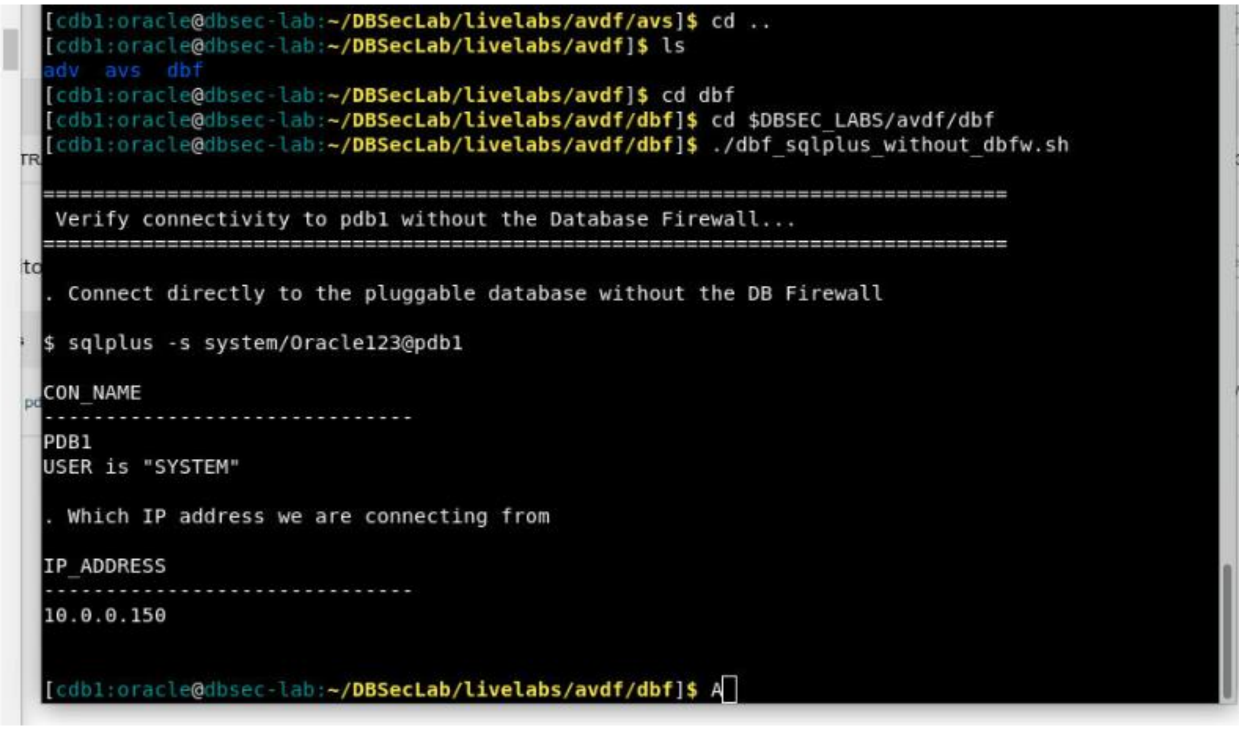
| | Target | User | Client host | Client program | Event | Object | Event status | Event time |
|---|---|---|---|---|---|---|---|---|
| | pdb2 | SYSTEM | dbsec-lab | sqlplus@dbsec-lab (TNS V1-V3) | DROP USER | NEW_USER_NED | SUCCESS | 4/9/2024 9:40:33 AM |

1

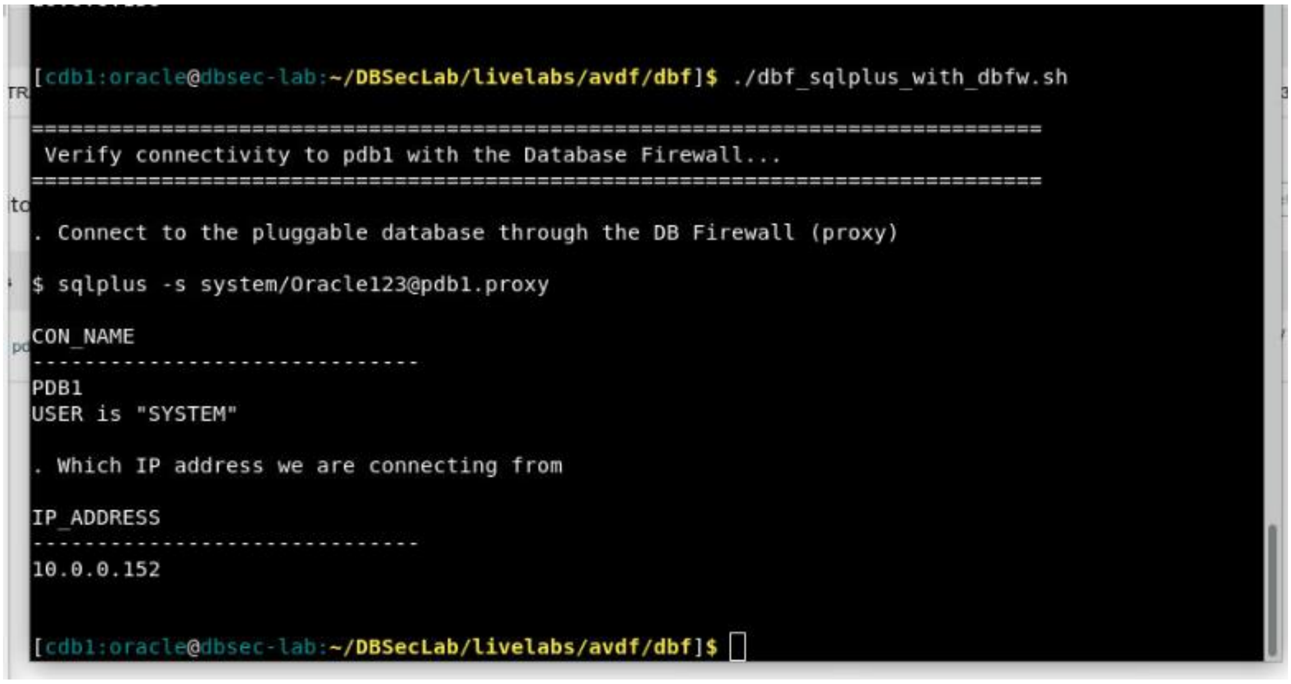


| □ | Alert policy name | Enabled | Target type | Email notification | Created by | Last updated | Alerts | Alert description |
|---|---|---|---|---|---|---|---|---|
| □ | Database Firewall Alert | ✓ | - All - | ✗ | AVSYS | 2/17/2024 12:37:00 AM | | An alert evaluated at a Database Firewall, based or Firewall Policy. |
| □ | CREATE USER | ✓ | Oracle Database | ✗ | AVAUDITOR | 4/9/2024 7:50:54 AM | | Alert on CREATE USER statements |
| □ | PII Exfiltration Alert | ✓ | Oracle Database | ✗ | AVAUDITOR | 4/9/2024 9:47:31 AM | | Someone has selected more than 100 rows of PII ir single query |
| □ | User creation/modification | ✓ | Oracle Database | ✗ | AVAUDITOR | 4/9/2024 9:39:30 AM | | Alert when the user is created, dropped, or altered |

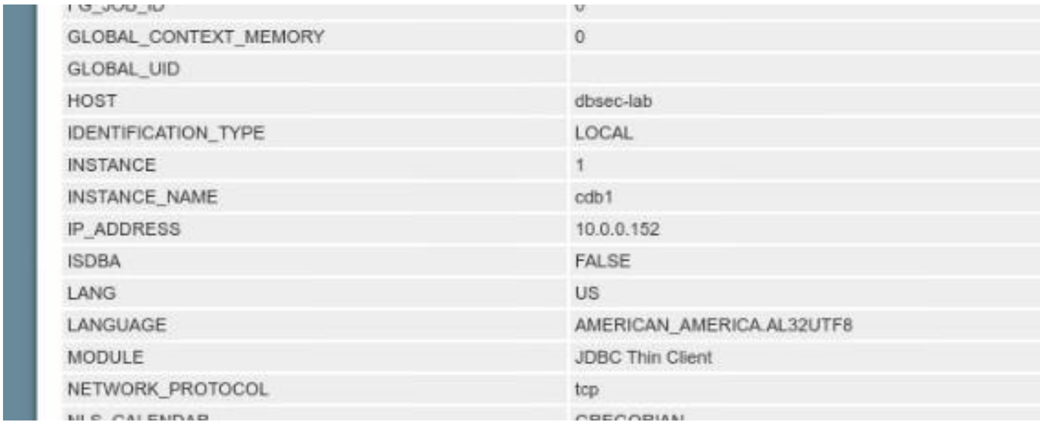
Task 5: Protect and Prevent



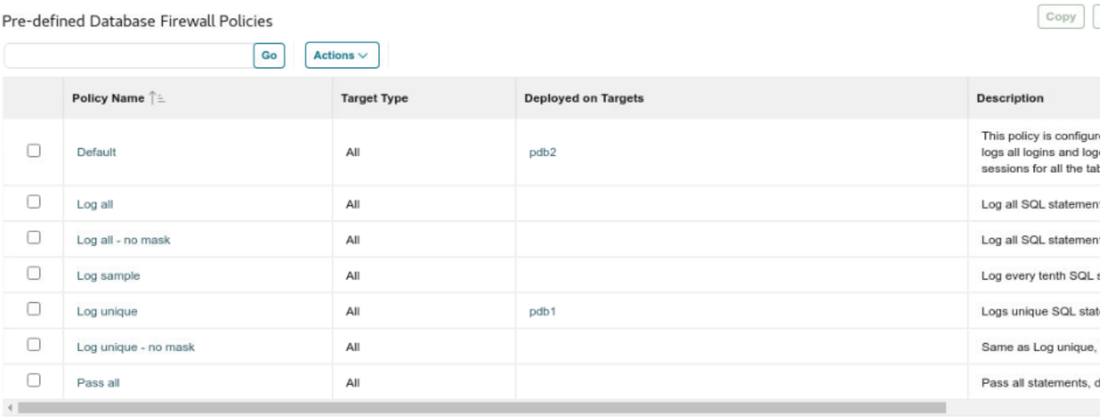
```
[cdb1:oracle@dbsec-lab:~/DBSecLab/livelabs/avdf/avs]$ cd ..
[cdb1:oracle@dbsec-lab:~/DBSecLab/livelabs/avdf]$ ls
adv  avs  dbf
[cdb1:oracle@dbsec-lab:~/DBSecLab/livelabs/avdf]$ cd dbf
[cdb1:oracle@dbsec-lab:~/DBSecLab/livelabs/avdf/dbf]$ cd $DBSEC_LABS/avdf/dbf
[cdb1:oracle@dbsec-lab:~/DBSecLab/livelabs/avdf/dbf]$ ./dbf_sqlplus_without_dbfw.sh

==============================================================================
 Verify connectivity to pdb1 without the Database Firewall...
==============================================================================

. Connect directly to the pluggable database without the DB Firewall

$ sqlplus -s system/Oracle123@pdb1

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

. Which IP address we are connecting from

IP_ADDRESS
------------------------------
10.0.0.150


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



```
[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


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

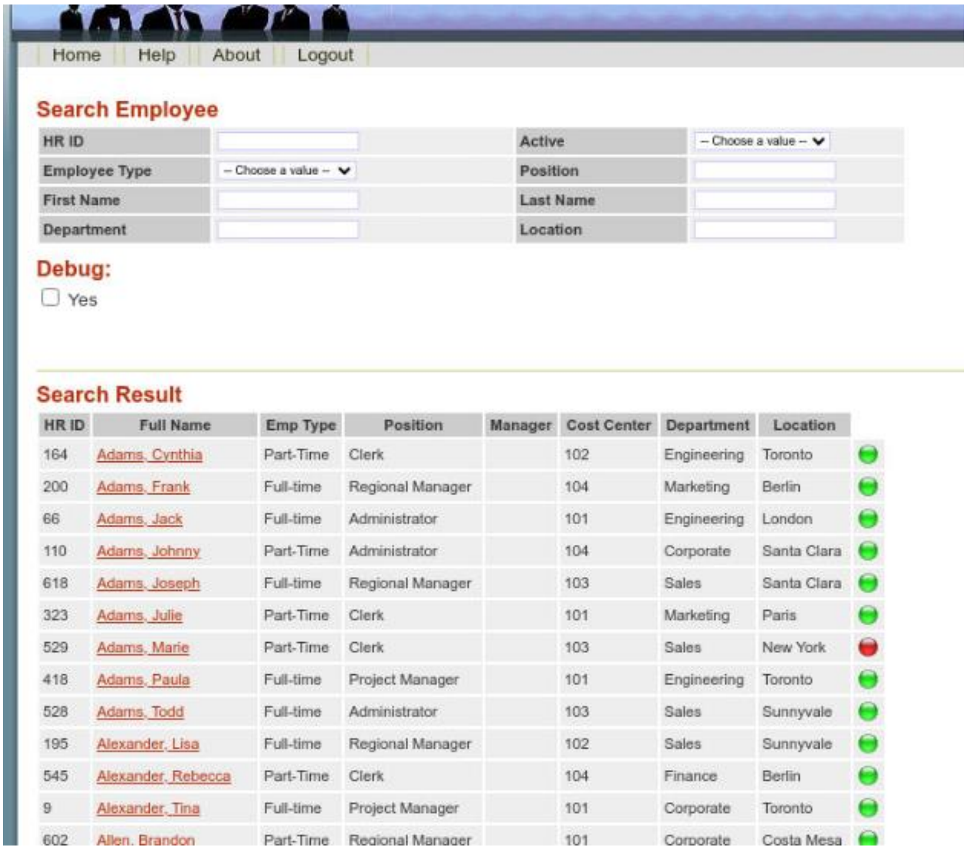


| | |
|---|---|
| FG_JOB_ID | 0 |
| GLOBAL_CONTEXT_MEMORY | 0 |
| GLOBAL_UID | |
| HOST | dbsec-lab |
| IDENTIFICATION_TYPE | LOCAL |
| INSTANCE | 1 |
| INSTANCE_NAME | cdb1 |
| IP_ADDRESS | 10.0.0.152 |
| ISDBA | FALSE |
| LANG | US |
| LANGUAGE | AMERICAN_AMERICA.AL32UTF8 |
| MODULE | JDBC Thin Client |
| NETWORK_PROTOCOL | tcp |
| NLS_CALENDAR | GREGORIAN |



Pre-defined Database Firewall Policies

| | Policy Name | Target Type | Deployed on Targets | Description |
|---|---|---|---|---|
| □ | Default | All | pdb2 | This policy is configur<br>logs all logins and log<br>sessions for all the tab |
| □ | Log all | All | | Log all SQL statemen |
| □ | Log all - no mask | All | | Log all SQL statemen |
| □ | Log sample | All | | Log every tenth SQL s |
| □ | Log unique | All | pdb1 | Logs unique SQL stat |
| □ | Log unique - no mask | All | | Same as Log unique, |
| □ | Pass all | All | | Pass all statements, d |



Search Employee

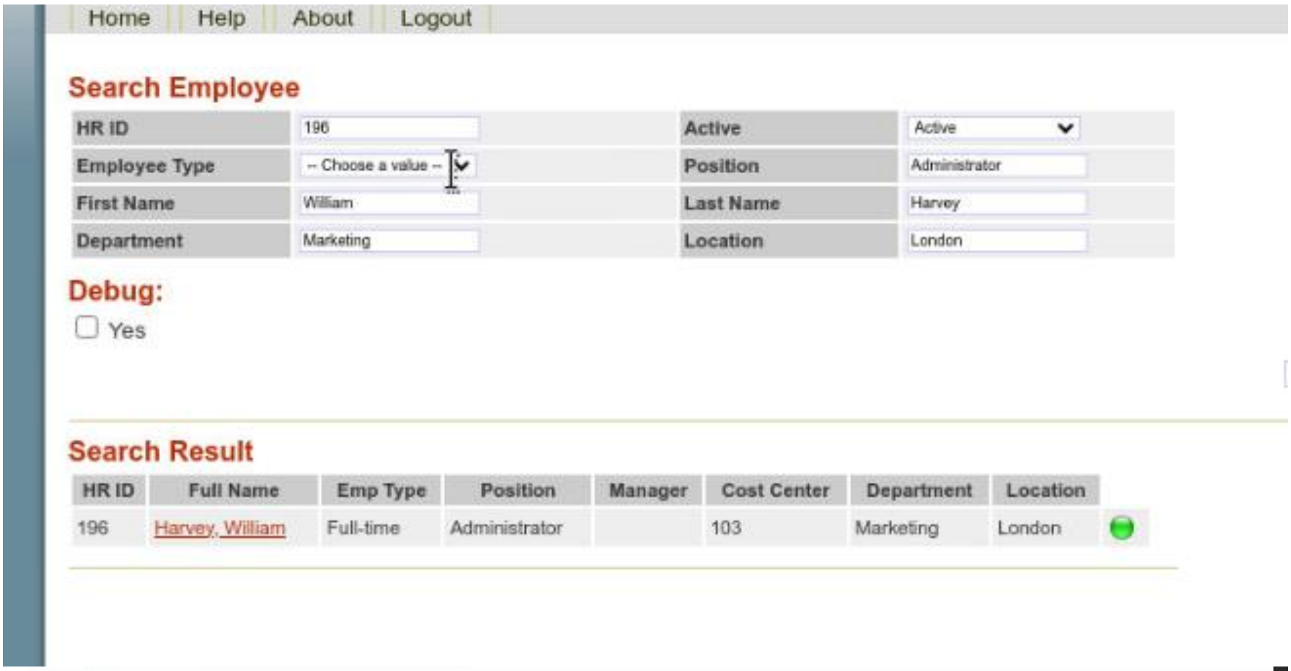
| | | | |
|---|---|---|---|
| HR ID | | Active | -- Choose a value -- |
| Employee Type | -- Choose a value -- | Position | |
| First Name | | Last Name | |
| Department | | Location | |

Debug:

□ Yes

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 | 🟢 |



Search Employee

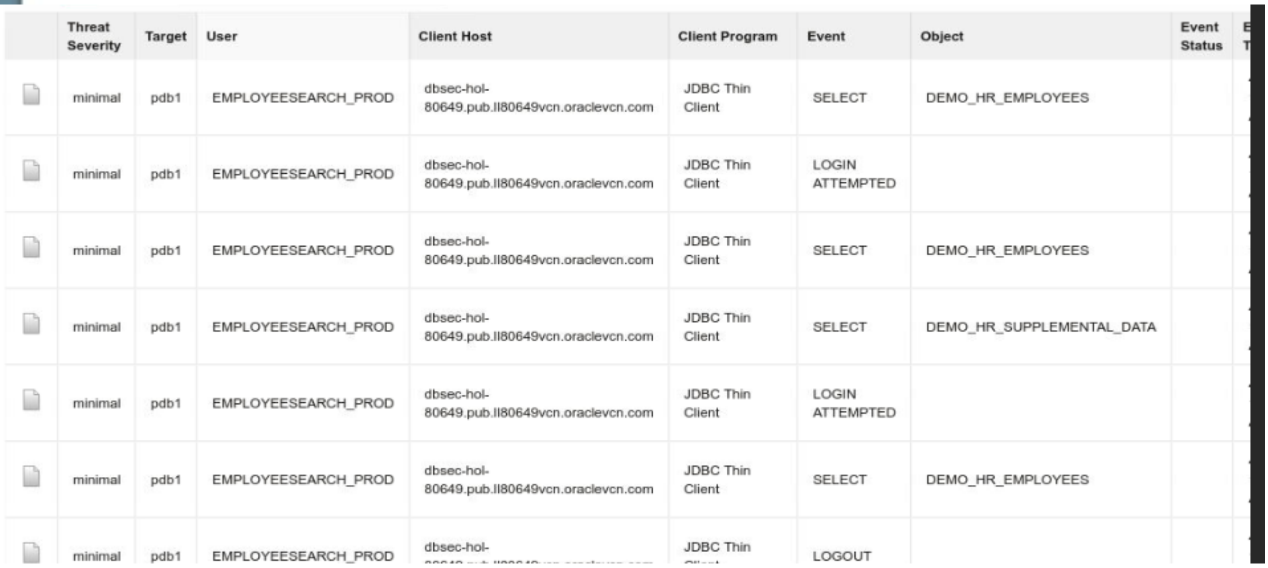
| | | | |
|---|---|---|---|
| HR ID | 196 | Active | Active |
| Employee Type | -- Choose a value -- | Position | Administrator |
| First Name | William | Last Name | Harvey |
| Department | Marketing | Location | London |

Debug:

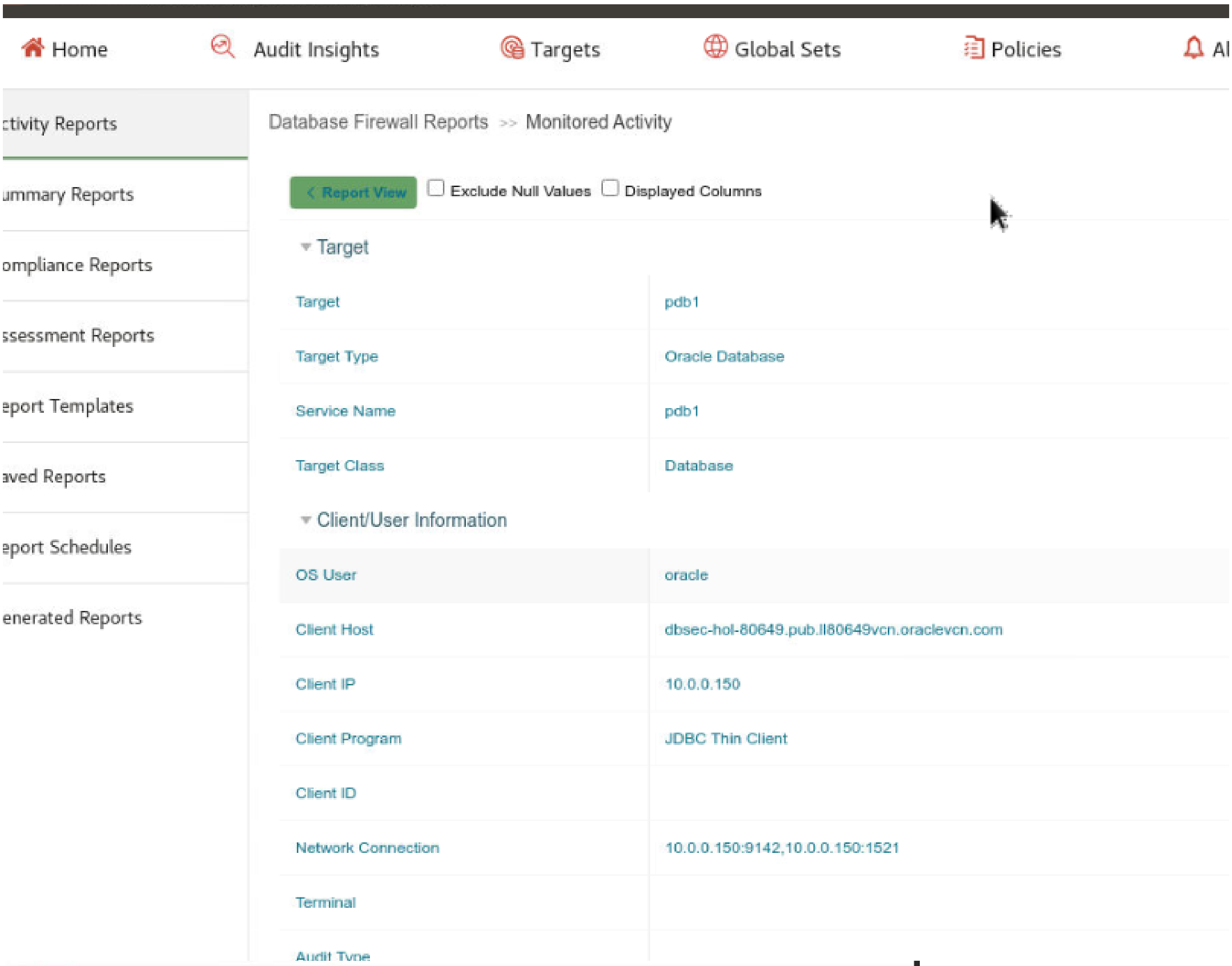
□ Yes

Search Result

| HR ID | Full Name | Emp Type | Position | Manager | Cost Center | Department | Location | |
|---|---|---|---|---|---|---|---|---|
| 196 | Harvey, William | Full-time | Administrator | | 103 | Marketing | London | ● |



| | Threat Severity | Target | User | Client Host | Client Program | Event | Object | Event Status | E T |
|---|---|---|---|---|---|---|---|---|---|
| | minimal | pdb1 | EMPLOYEESEARCH_PROD | dbsec-hol-80649.pub.ll80649vcn.oraclevcn.com | JDBC Thin Client | SELECT | DEMO_HR_EMPLOYEES | | |
| | minimal | pdb1 | EMPLOYEESEARCH_PROD | dbsec-hol-80649.pub.ll80649vcn.oraclevcn.com | JDBC Thin Client | LOGIN ATTEMPTED | | | |
| | minimal | pdb1 | EMPLOYEESEARCH_PROD | dbsec-hol-80649.pub.ll80649vcn.oraclevcn.com | JDBC Thin Client | SELECT | DEMO_HR_EMPLOYEES | | |
| | minimal | pdb1 | EMPLOYEESEARCH_PROD | dbsec-hol-80649.pub.ll80649vcn.oraclevcn.com | JDBC Thin Client | SELECT | DEMO_HR_SUPPLEMENTAL_DATA | | |
| | minimal | pdb1 | EMPLOYEESEARCH_PROD | dbsec-hol-80649.pub.ll80649vcn.oraclevcn.com | JDBC Thin Client | LOGIN ATTEMPTED | | | |
| | minimal | pdb1 | EMPLOYEESEARCH_PROD | dbsec-hol-80649.pub.ll80649vcn.oraclevcn.com | JDBC Thin Client | SELECT | DEMO_HR_EMPLOYEES | | |
| | minimal | pdb1 | EMPLOYEESEARCH_PROD | dbsec-hol- | JDBC Thin | LOGOUT | | | |



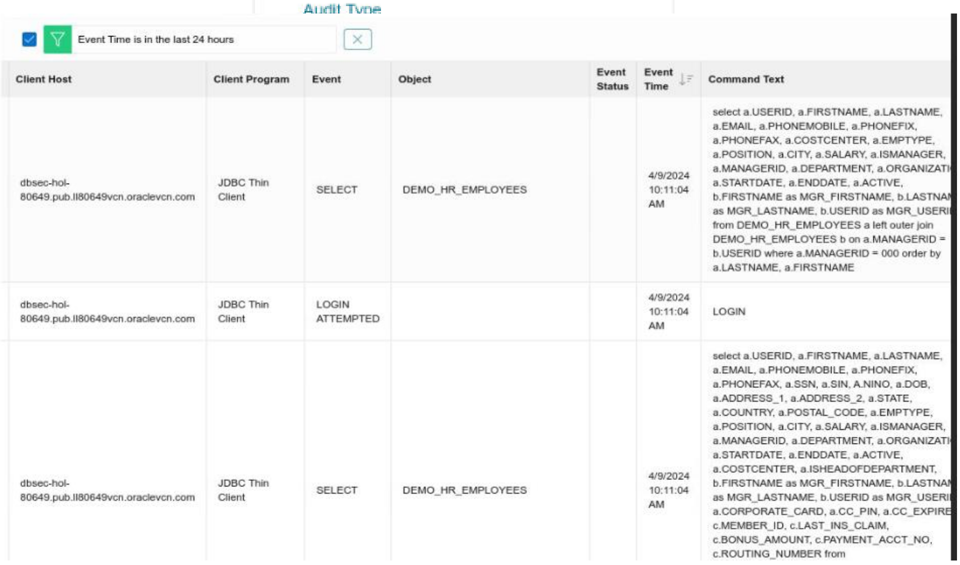
Database Firewall Reports >> Monitored Activity

Target

| | |
|---|---|
| Target | pdb1 |
| Target Type | Oracle Database |
| Service Name | pdb1 |
| Target Class | Database |

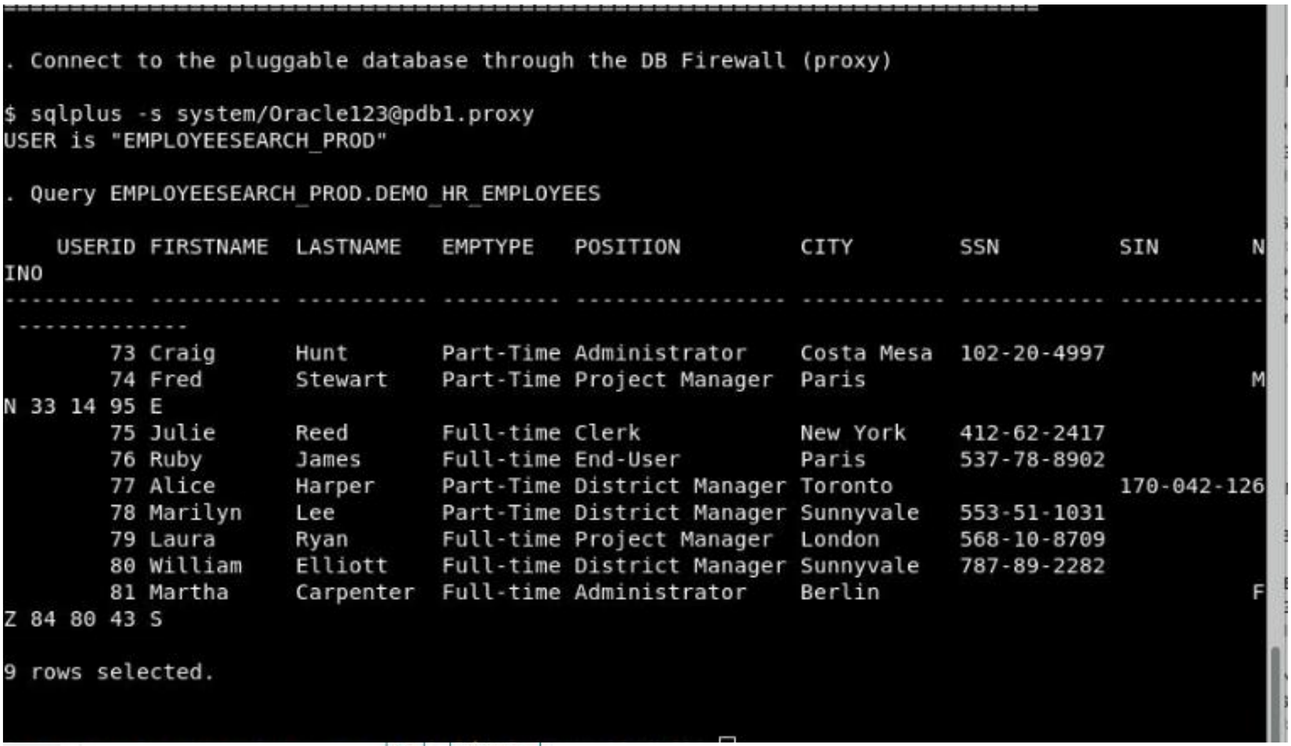
Client/User Information

| | |
|---|---|
| OS User | oracle |
| Client Host | dbsec-hol-80649.pub.ll80649vcn.oraclevcn.com |
| Client IP | 10.0.0.150 |
| Client Program | JDBC Thin Client |
| Client ID | |
| Network Connection | 10.0.0.150:9142,10.0.0.150:1521 |
| Terminal | |
| Audit Type | |

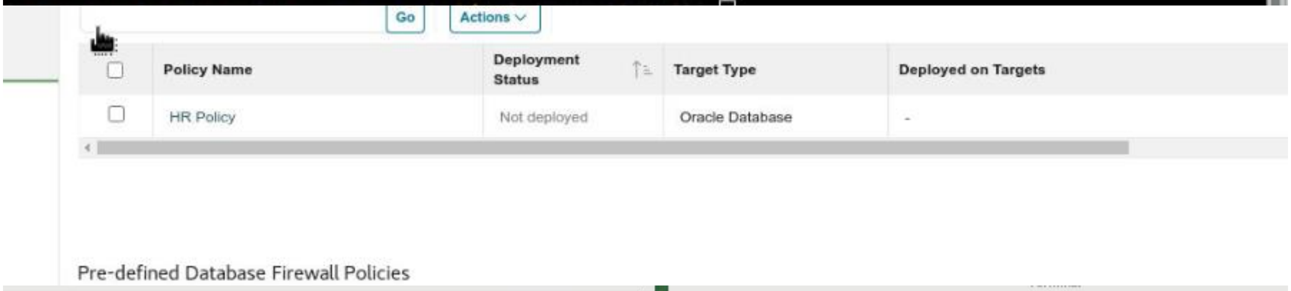


☑ Event Time is in the last 24 hours

| Client Host | Client Program | Event | Object | Event Status | Event Time | Command Text |
|---|---|---|---|---|---|---|
| dbsec-hol-80649.pub.ll80649vcn.oraclevcn.com | JDBC Thin Client | SELECT | DEMO_HR_EMPLOYEES | | 4/9/2024 10:11:04 AM | select a.USERID, a.FIRSTNAME, a.LASTNAME, a.EMAIL, a.PHONEMOBILE, a.PHONEFIX, a.PHONEFAX, a.COSTCENTER, a.EMPTYPE, a.POSITION, a.CITY, a.SALARY, a.ISMANAGER, a.MANAGERID, a.DEPARTMENT, a.ORGANIZATI a.STARTDATE, a.ENDDATE, a.ACTIVE, b.FIRSTNAME as MGR_FIRSTNAME, b.LASTNAI as MGR_LASTNAME, b.USERID as MGR_USERI from DEMO_HR_EMPLOYEES a left outer join DEMO_HR_EMPLOYEES b on a.MANAGERID = b.USERID where a.MANAGERID = 000 order by a.LASTNAME, a.FIRSTNAME |
| dbsec-hol-80649.pub.ll80649vcn.oraclevcn.com | JDBC Thin Client | LOGIN ATTEMPTED | | | 4/9/2024 10:11:04 AM | LOGIN |
| dbsec-hol-80649.pub.ll80649vcn.oraclevcn.com | JDBC Thin Client | SELECT | DEMO_HR_EMPLOYEES | | 4/9/2024 10:11:04 AM | select a.USERID, a.FIRSTNAME, a.LASTNAME, a.EMAIL, a.PHONEMOBILE, a.PHONEFIX, a.PHONEFAX, a.SSN, a.SIN, A.NINO, a.DOB, a.ADDRESS_1, a.ADDRESS_2, a.STATE, a.COUNTRY, a.POSTAL_CODE, a.EMPTYPE, a.POSITION, a.CITY, a.SALARY, a.ISMANAGER, a.MANAGERID, a.DEPARTMENT, a.ORGANIZATI a.STARTDATE, a.ENDDATE, a.ACTIVE, a.COSTCENTER, a.ISHEADOFDEPARTMENT, b.FIRSTNAME as MGR_FIRSTNAME, b.LASTNAI as MGR_LASTNAME, b.USERID as MGR_USERI a.CORPORATE_CARD, a.CC_PIN, a.CC_EXPIRE c.MEMBER_ID, c.LAST_INS_CLAIM, c.BONUS_AMOUNT, c.PAYMENT_ACCT_NO, c.ROUTING_NUMBER from |

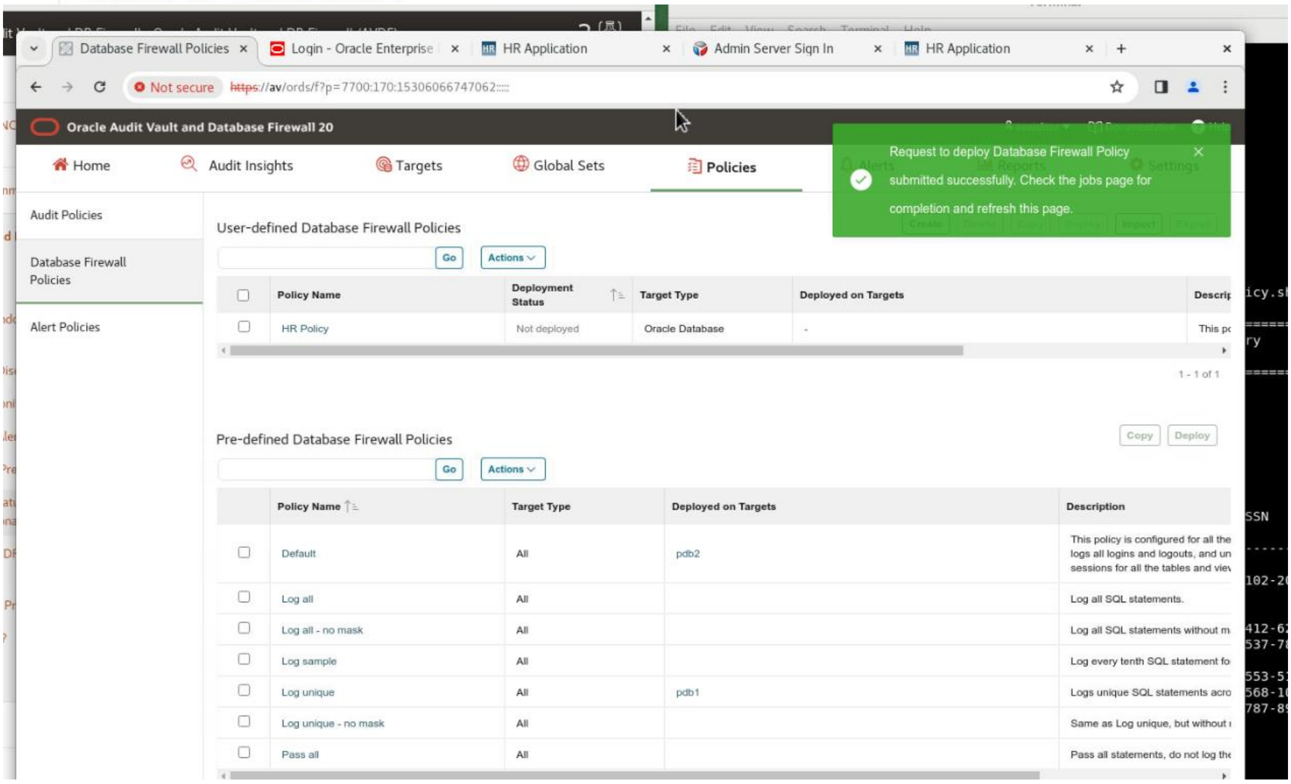


```
=================================================================================

. 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         N
INO
---------- ---------- ---------- ---------- ----------------- ----------- ----------- -----------
 -------------
        73 Craig      Hunt       Part-Time Administrator      Costa Mesa  102-20-4997
        74 Fred       Stewart    Part-Time Project Manager    Paris                               M
N 33 14 95 E
        75 Julie      Reed       Full-time Clerk              New York    412-62-2417
        76 Ruby       James      Full-time End-User           Paris       537-78-8902
        77 Alice      Harper     Part-Time District Manager   Toronto                 170-042-126
        78 Marilyn    Lee        Part-Time District Manager   Sunnyvale   553-51-1031
        79 Laura      Ryan       Full-time Project Manager    London      568-10-8709
        80 William    Elliott    Full-time District Manager   Sunnyvale   787-89-2282
        81 Martha     Carpenter  Full-time Administrator      Berlin                              F
Z 84 80 43 S

9 rows selected.
```



| □ | Policy Name | Deployment Status | Target Type | Deployed on Targets |
|---|---|---|---|---|
| □ | HR Policy | Not deployed | Oracle Database | - |

Pre-defined Database Firewall Policies



Database Firewall Policies
Login - Oracle Enterprise
HR Application
Admin Server Sign In
HR Application
Not secure
https://av/ords/f?p=7700:170:15306066747062:::::
Oracle Audit Vault and Database Firewall 20
Home
Audit Insights
Targets
Global Sets
Policies
Audit Policies
Database Firewall Policies
Alert Policies

Request to deploy Database Firewall Policy submitted successfully. Check the jobs page for completion and refresh this page.

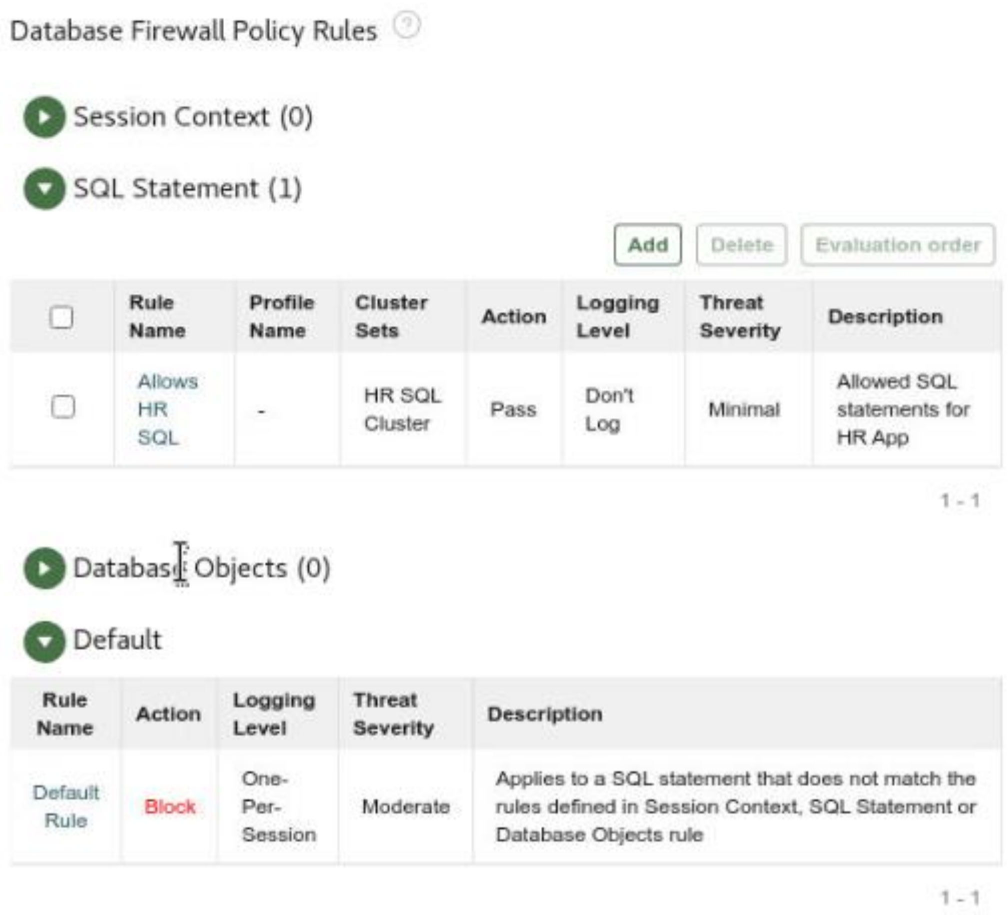
User-defined Database Firewall Policies

| □ | Policy Name | Deployment Status | Target Type | Deployed on Targets | Descrip |
|---|---|---|---|---|---|
| □ | HR Policy | Not deployed | Oracle Database | - | This pc |

1 - 1 of 1

Pre-defined Database Firewall Policies

| | Policy Name | Target Type | Deployed on Targets | Description |
|---|---|---|---|---|
| □ | Default | All | pdb2 | This policy is configured for all the logs all logins and logouts, and un sessions for all the tables and viev |
| □ | Log all | All | | Log all SQL statements. |
| □ | Log all - no mask | All | | Log all SQL statements without m |
| □ | Log sample | All | | Log every tenth SQL statement fo |
| □ | Log unique | All | pdb1 | Logs unique SQL statements acro |
| □ | Log unique - no mask | All | | Same as Log unique, but without ı |
| □ | Pass all | All | | Pass all statements, do not log the |



Database Firewall Policy Rules

Session Context (0)

SQL Statement (1)

| ☐ | Rule Name | Profile Name | Cluster Sets | Action | Logging Level | Threat Severity | Description |
|---|---|---|---|---|---|---|---|
| ☐ | Allows HR SQL | - | HR SQL Cluster | Pass | Don't Log | Minimal | Allowed SQL statements for HR App |

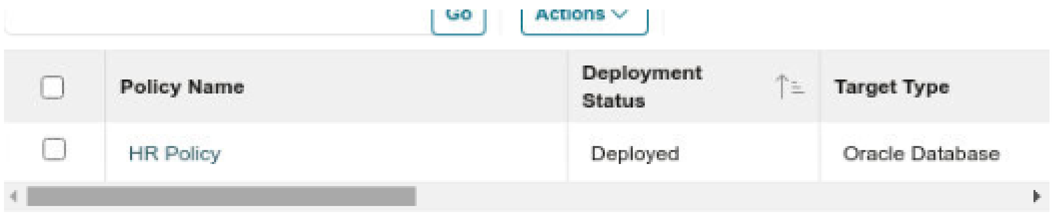
1 - 1

Database Objects (0)

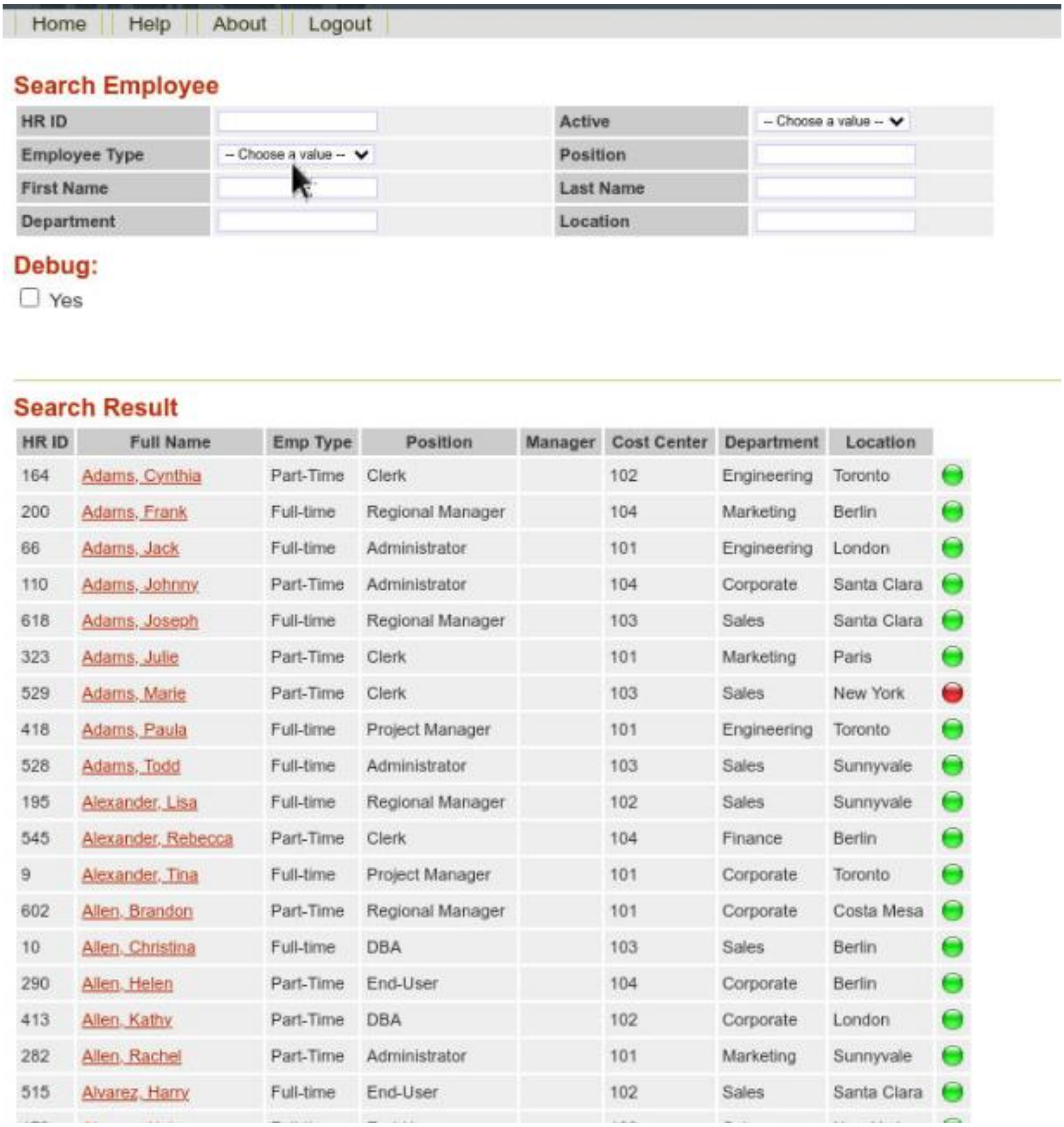
Default

| Rule Name | Action | Logging Level | Threat Severity | Description |
|---|---|---|---|---|
| Default Rule | Block | One-Per-Session | Moderate | Applies to a SQL statement that does not match the rules defined in Session Context, SQL Statement or Database Objects rule |

1 - 1



| ☐ | Policy Name | Deployment Status | Target Type |
|---|---|---|---|
| ☐ | HR Policy | Deployed | Oracle Database |



## Search Employee

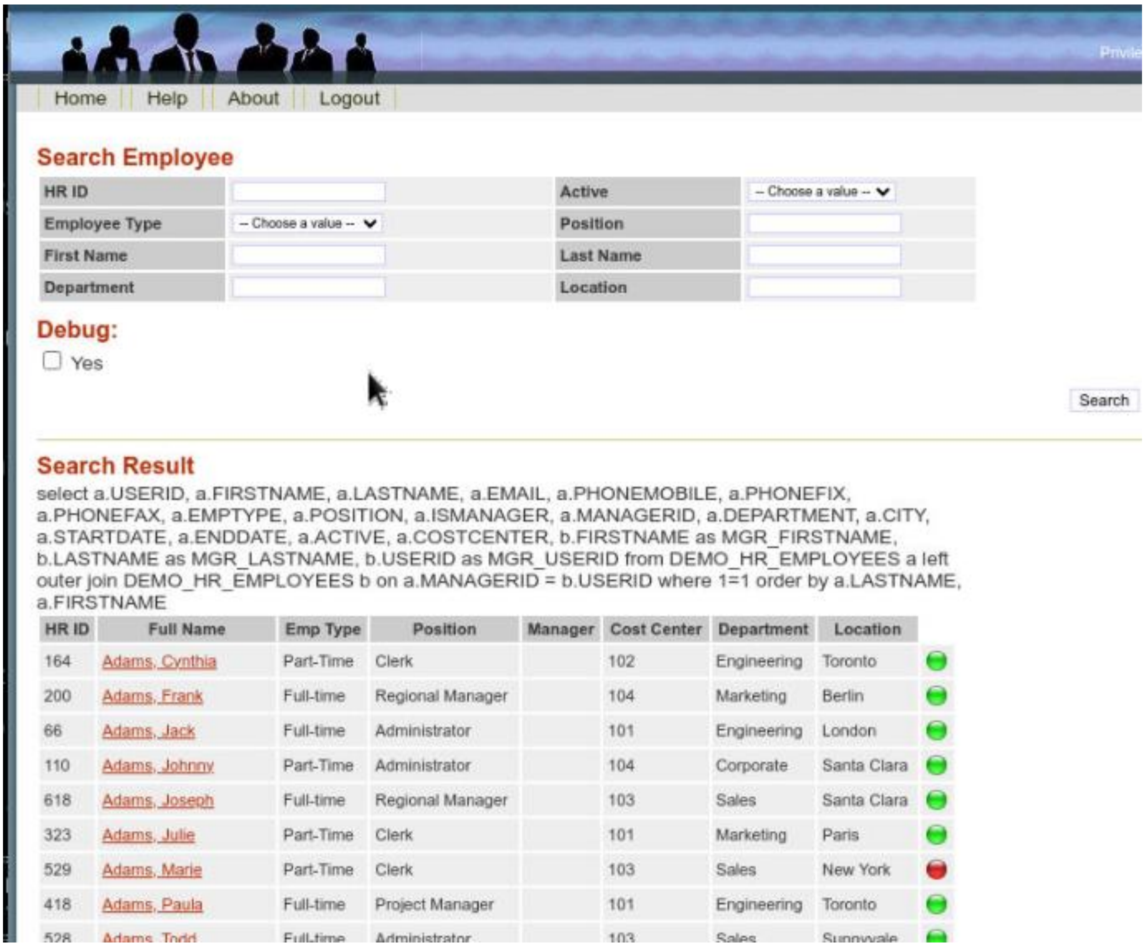
| | | | |
|---|---|---|---|
| HR ID | | Active | -- Choose a value -- |
| Employee Type | -- Choose a value -- | Position | |
| First Name | | Last Name | |
| Department | | Location | |

**Debug:**

□ Yes

## 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 | 🟢 |



## Search Employee

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

**Debug:**

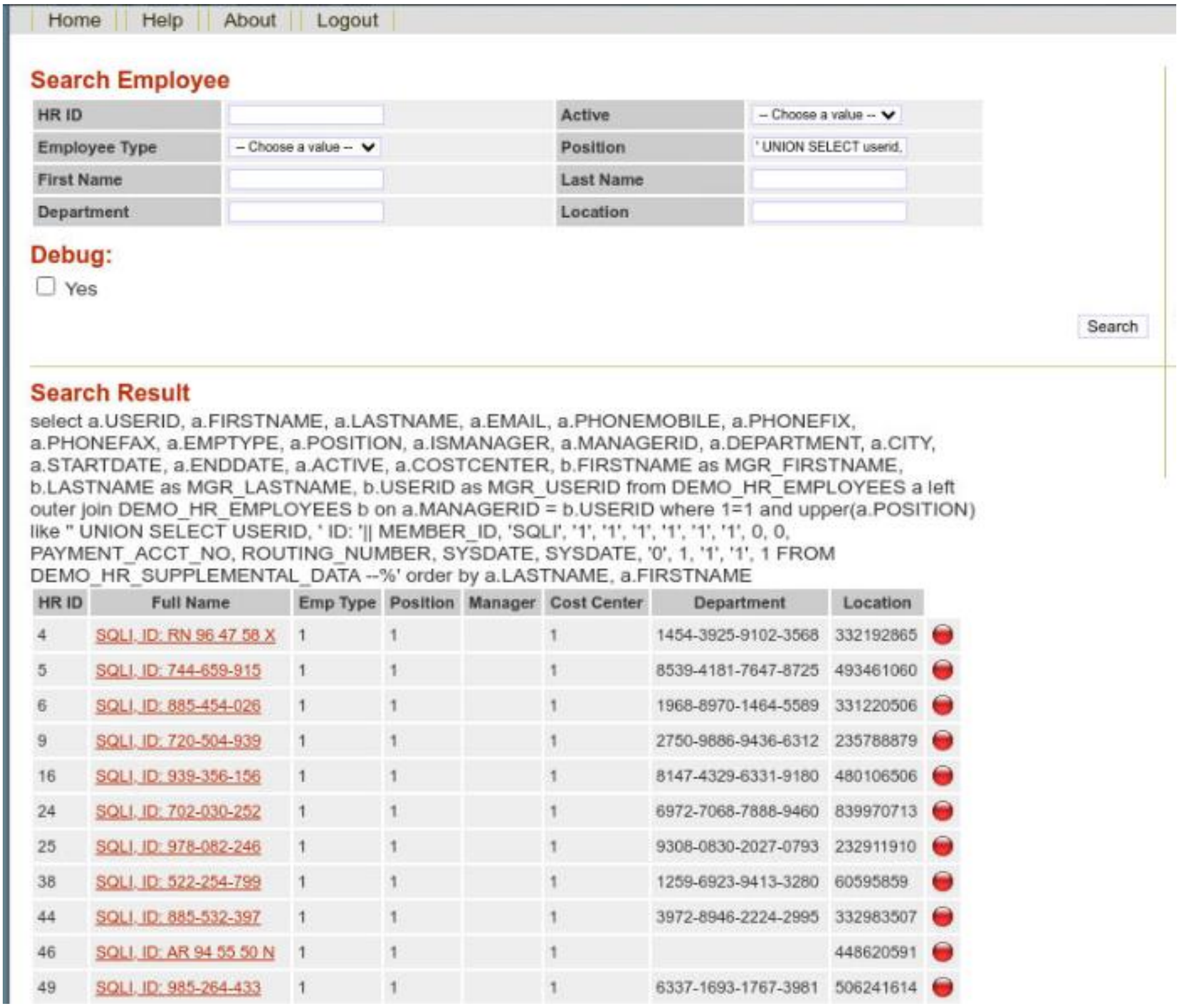
☐ Yes

Search

## Search Result

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

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



## Search Employee

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

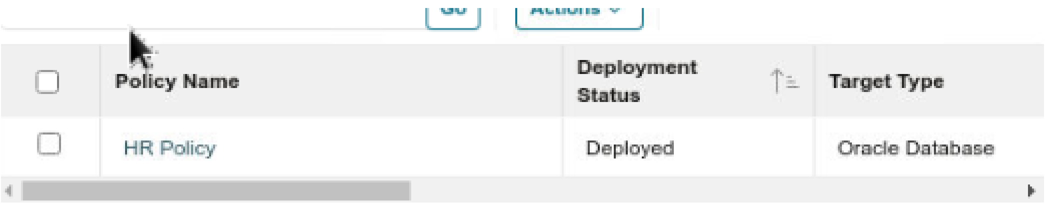
Debug:

□ Yes

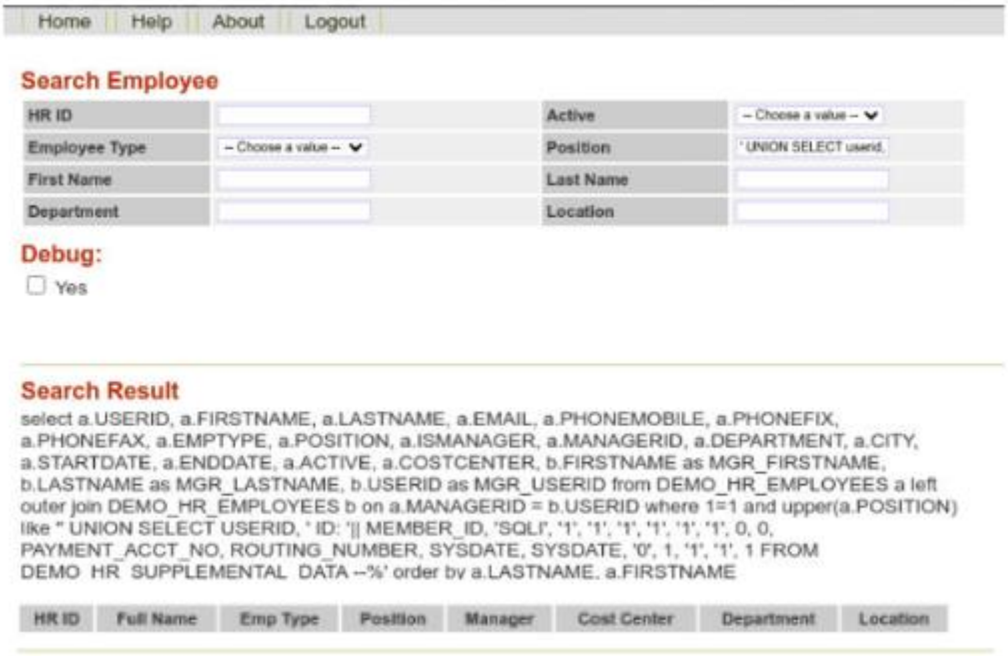
Search Result

```
select a.USERID, a.FIRSTNAME, a.LASTNAME, a.EMAIL, a.PHONEMOBILE, a.PHONEFIX,
a.PHONEFAX, a.EMPTYPE, a.POSITION, a.ISMANAGER, a.MANAGERID, a.DEPARTMENT, a.CITY,
a.STARTDATE, a.ENDDATE, a.ACTIVE, a.COSTCENTER, b.FIRSTNAME as MGR_FIRSTNAME,
b.LASTNAME as MGR_LASTNAME, b.USERID as MGR_USERID from DEMO_HR_EMPLOYEES a left
outer join DEMO_HR_EMPLOYEES b on a.MANAGERID = b.USERID where 1=1 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 | SQLI, ID: RN 96 47 58 X | 1 | 1 | | 1 | 1454-3925-9102-3568 | 332192865 | ● |
| 5 | SQLI, ID: 744-659-915 | 1 | 1 | | 1 | 8539-4181-7647-8725 | 493461060 | ● |
| 6 | SQLI, ID: 885-454-026 | 1 | 1 | | 1 | 1968-8970-1464-5589 | 331220506 | ● |
| 9 | SQLI, ID: 720-504-939 | 1 | 1 | | 1 | 2750-9886-9436-6312 | 235788879 | ● |
| 16 | SQLI, ID: 939-356-156 | 1 | 1 | | 1 | 8147-4329-6331-9180 | 480106506 | ● |
| 24 | SQLI, ID: 702-030-252 | 1 | 1 | | 1 | 6972-7068-7888-9460 | 839970713 | ● |
| 25 | SQLI, ID: 978-082-246 | 1 | 1 | | 1 | 9308-0830-2027-0793 | 232911910 | ● |
| 38 | SQLI, ID: 522-254-799 | 1 | 1 | | 1 | 1259-6923-9413-3280 | 60595859 | ● |
| 44 | SQLI, ID: 885-532-397 | 1 | 1 | | 1 | 3972-8946-2224-2995 | 332983507 | ● |
| 46 | SQLI, ID: AR 94 55 50 N | 1 | 1 | | 1 | | 448620591 | ● |
| 49 | SQLI, ID: 985-264-433 | 1 | 1 | | 1 | 6337-1693-1767-3981 | 506241614 | ● |



| □ | Policy Name | Deployment Status | Target Type |
|---|---|---|---|
| □ | HR Policy | Deployed | Oracle Database |



Search Employee

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

Debug:

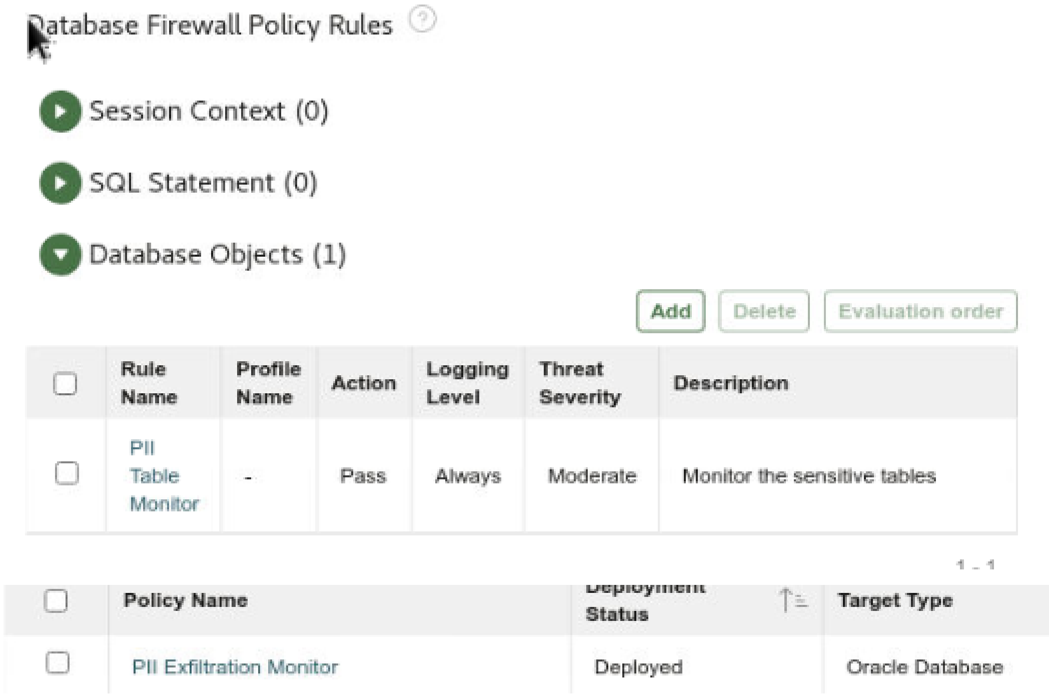
□ Yes

Search Result

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

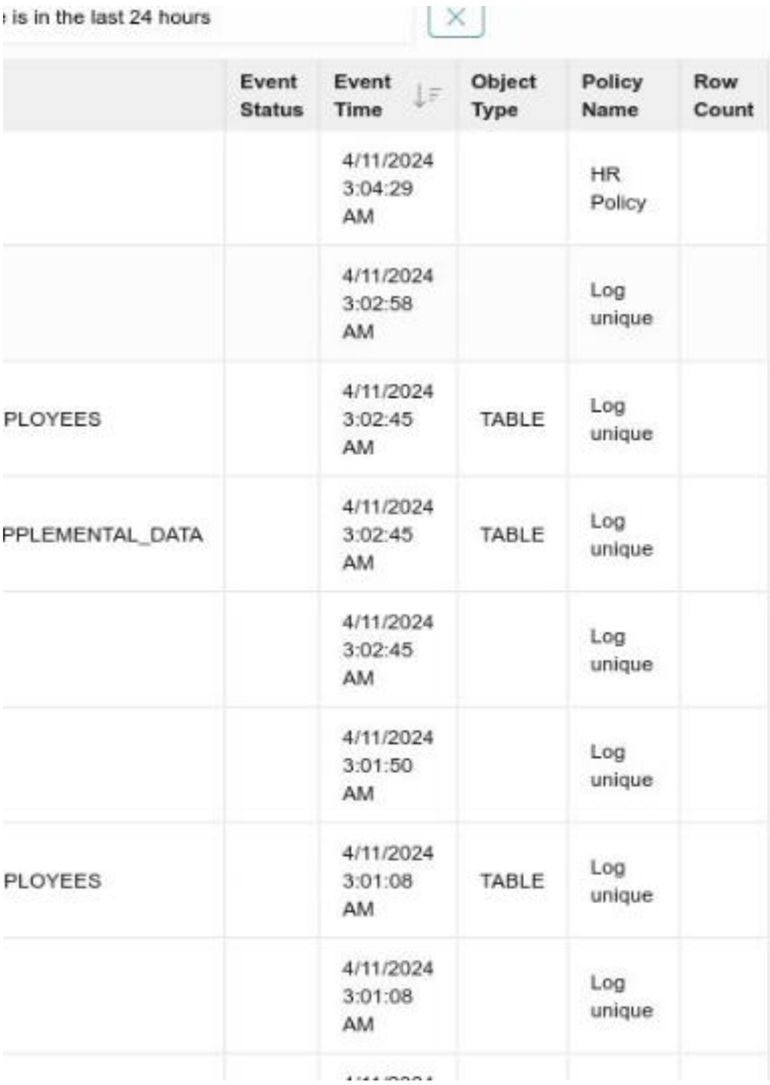
Step 6:


Database Firewall Policy Rules

| □ | Rule Name | Profile Name | Action | Logging Level | Threat Severity | Description |
|---|---|---|---|---|---|---|
| □ | PII Table Monitor | - | Pass | Always | Moderate | Monitor the sensitive tables |

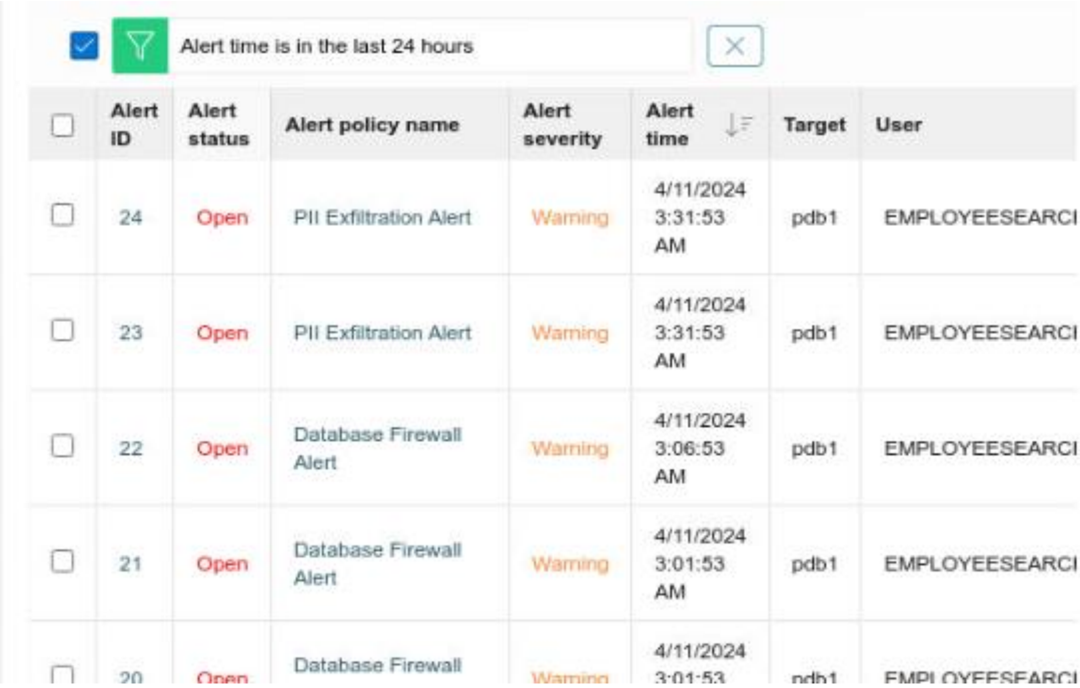
1 - 1

| □ | Policy Name | Deployment Status | Target Type |
|---|---|---|---|
| □ | PII Exfiltration Monitor | Deployed | Oracle Database |



is in the last 24 hours

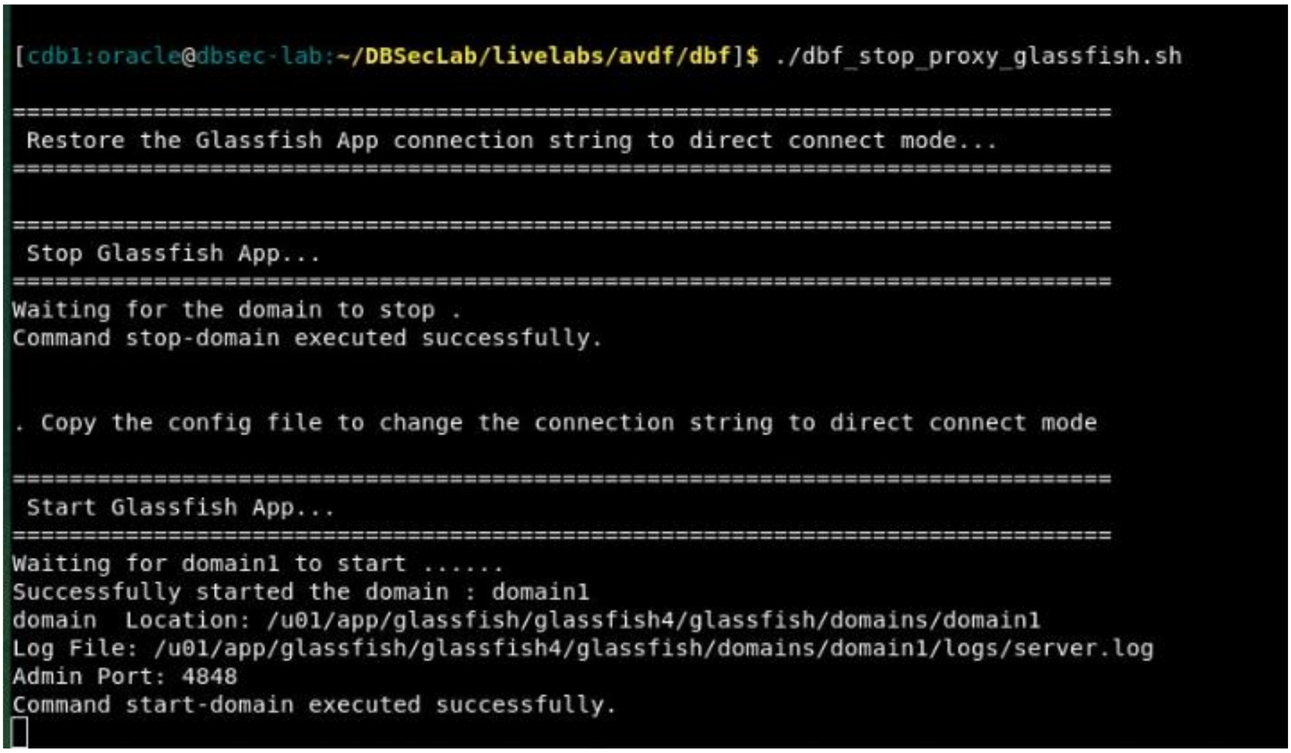
| | Event Status | Event Time | Object Type | Policy Name | Row Count |
|---|---|---|---|---|---|
| | | 4/11/2024 3:04:29 AM | | HR Policy | |
| | | 4/11/2024 3:02:58 AM | | Log unique | |
| PLOYEES | | 4/11/2024 3:02:45 AM | TABLE | Log unique | |
| PPLEMENTAL_DATA | | 4/11/2024 3:02:45 AM | TABLE | Log unique | |
| | | 4/11/2024 3:02:45 AM | | Log unique | |
| | | 4/11/2024 3:01:50 AM | | Log unique | |
| PLOYEES | | 4/11/2024 3:01:08 AM | TABLE | Log unique | |
| | | 4/11/2024 3:01:08 AM | | Log unique | |



☑ Alert time is in the last 24 hours

| □ | Alert ID | Alert status | Alert policy name | Alert severity | Alert time | Target | User |
|---|---|---|---|---|---|---|---|
| □ | 24 | Open | PII Exfiltration Alert | Warning | 4/11/2024 3:31:53 AM | pdb1 | EMPLOYEESEARCI |
| □ | 23 | Open | PII Exfiltration Alert | Warning | 4/11/2024 3:31:53 AM | pdb1 | EMPLOYEESEARCI |
| □ | 22 | Open | Database Firewall Alert | Warning | 4/11/2024 3:06:53 AM | pdb1 | EMPLOYEESEARCI |
| □ | 21 | Open | Database Firewall Alert | Warning | 4/11/2024 3:01:53 AM | pdb1 | EMPLOYEESEARCI |
| □ | 20 | Open | Database Firewall | Warning | 4/11/2024 3:01:53 | pdb1 | EMPLOYEESEARCI |

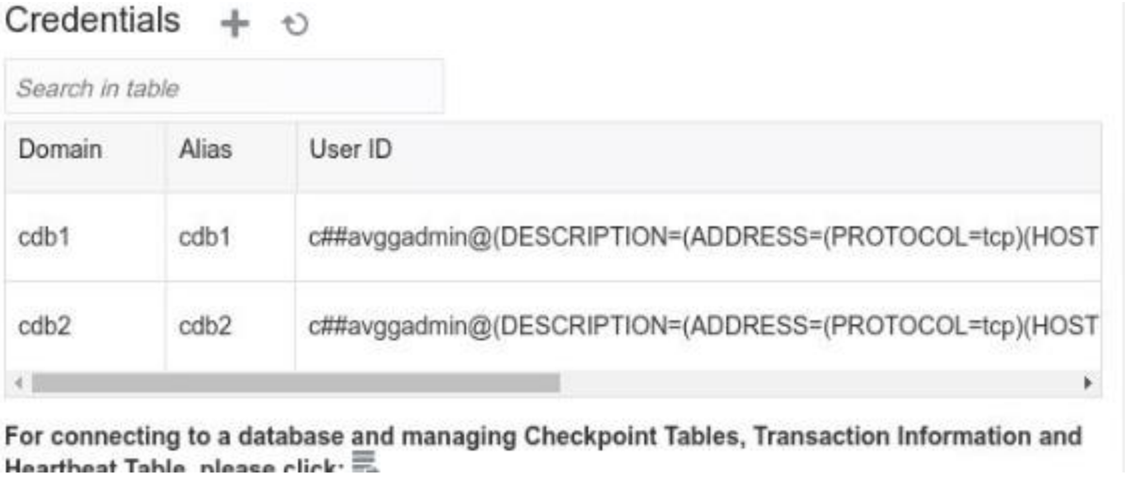
Step 7



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

Task 6: Advanced feature configuration

Step 1

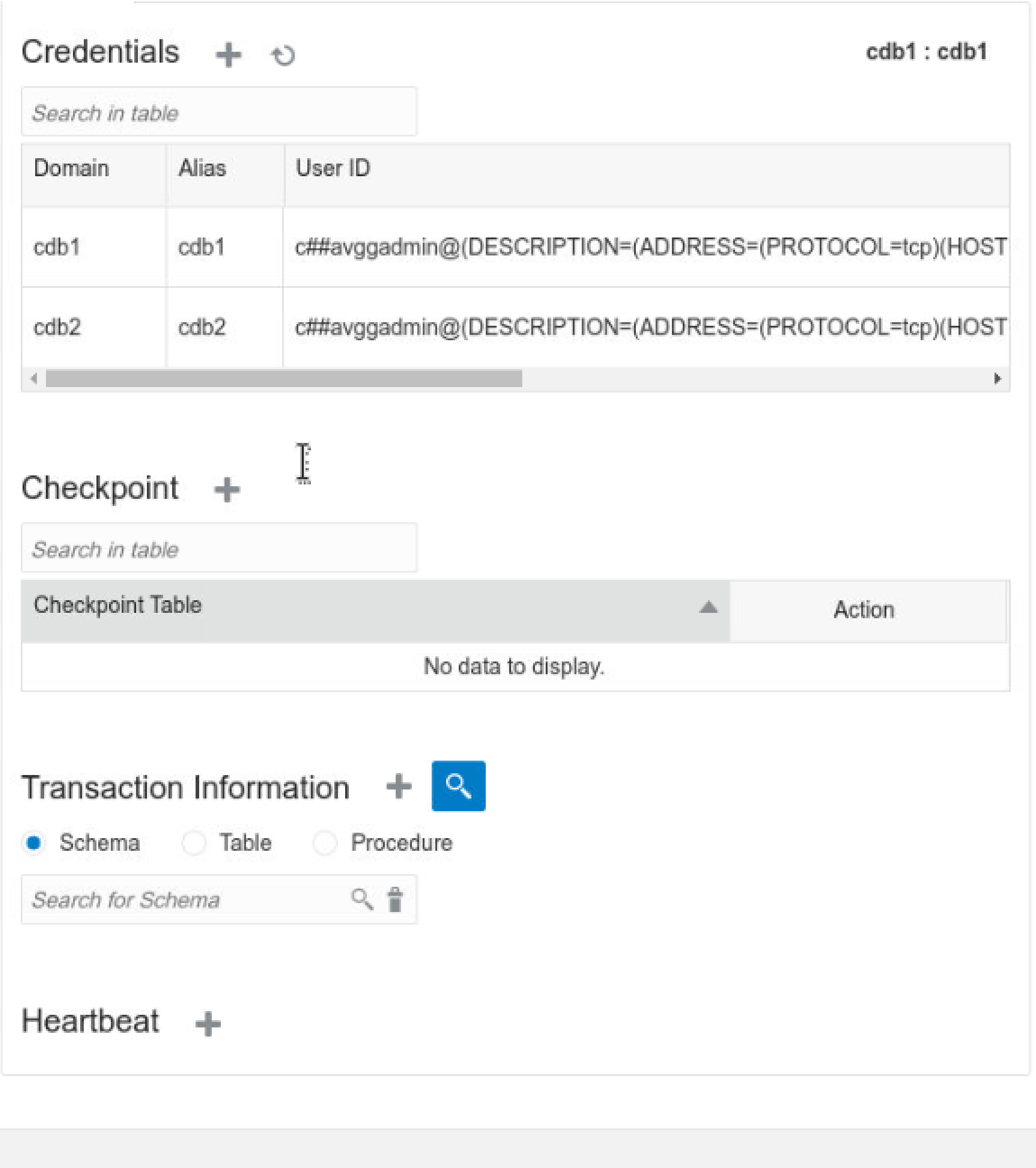


Credentials + ↻

Search in table

| Domain | Alias | User ID |
|---|---|---|
| cdb1 | cdb1 | c##avggadmin@(DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST |
| cdb2 | cdb2 | c##avggadmin@(DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST |

For connecting to a database and managing Checkpoint Tables, Transaction Information and Heartbeat Table, please click:



Credentials ＋ ↻ cdb1 : cdb1

Search in table

| Domain | Alias | User ID |
|---|---|---|
| cdb1 | cdb1 | c##avggadmin@(DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST |
| cdb2 | cdb2 | c##avggadmin@(DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST |

Checkpoint ＋

Search in table

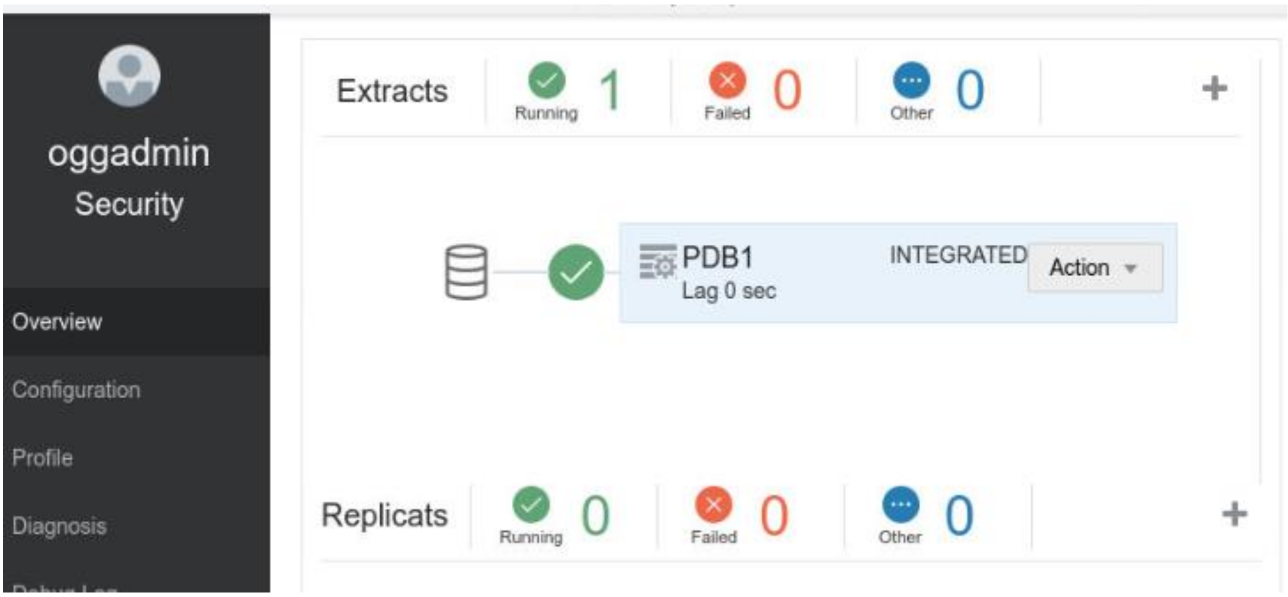
| Checkpoint Table | Action |
|---|---|
| No data to display. | |

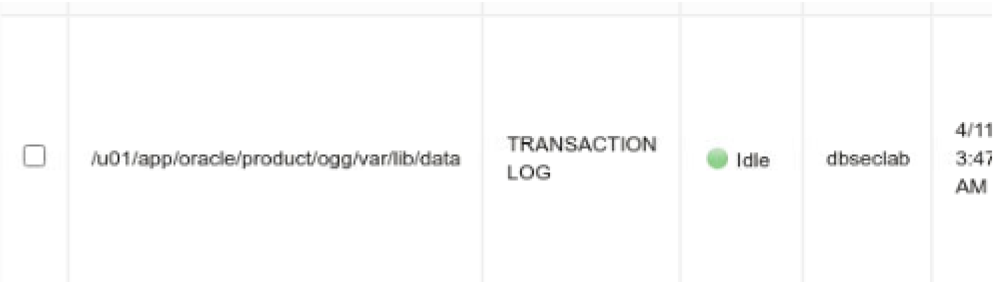
Transaction Information ＋

● Schema ○ Table ○ Procedure

Search for Schema

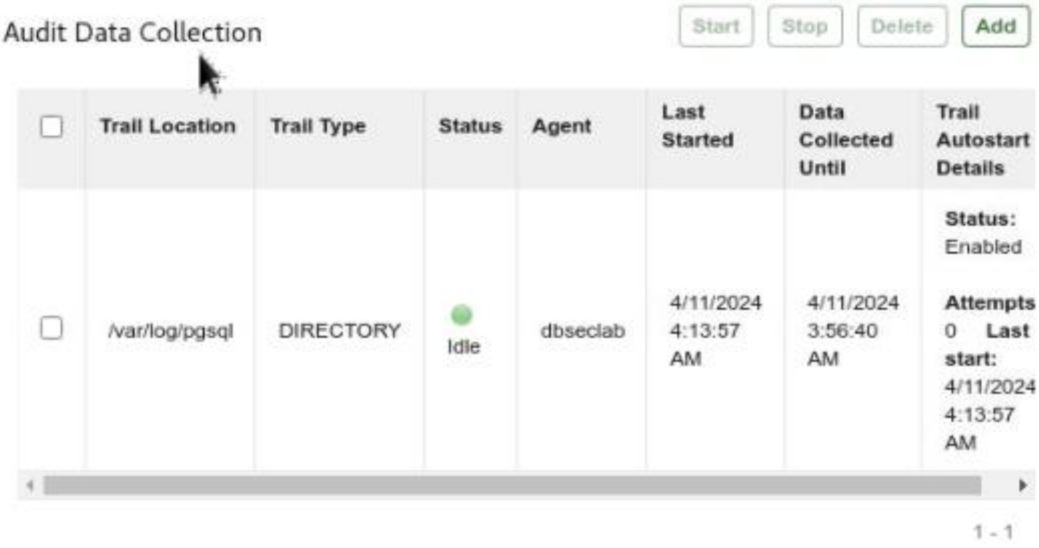
Heartbeat ＋





| | | | | | |
|---|---|---|---|---|---|
| ☐ | /u01/app/oracle/product/ogg/var/lib/data | TRANSACTION LOG | ● Idle | dbseclab | 4/11<br>3:47<br>AM |

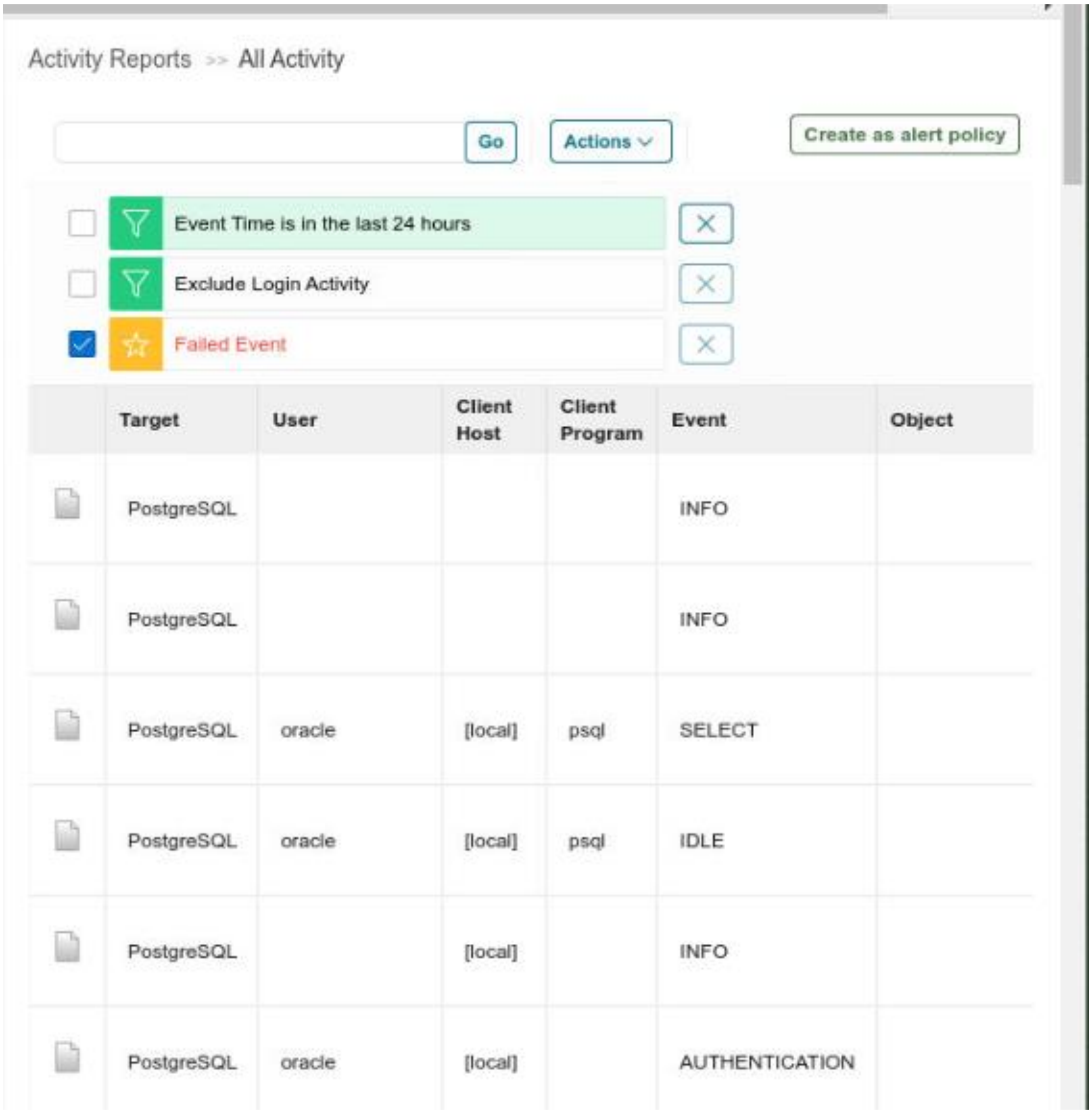
Step 2:



Audit Data Collection

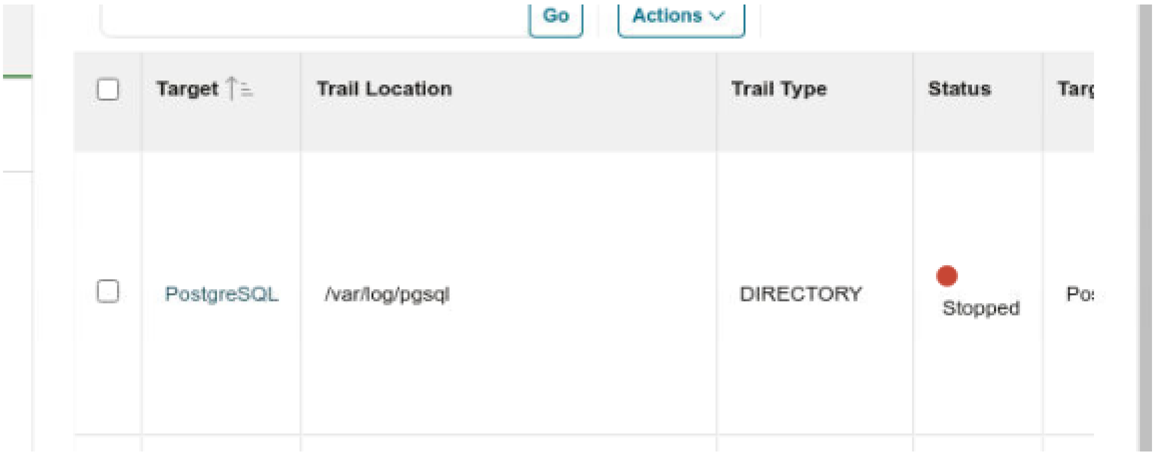
| ☐ | Trail Location | Trail Type | Status | Agent | Last Started | Data Collected Until | Trail Autostart Details |
|---|---|---|---|---|---|---|---|
| ☐ | /var/log/pgsql | DIRECTORY | ● Idle | dbseclab | 4/11/2024 4:13:57 AM | 4/11/2024 3:56:40 AM | **Status:** Enabled<br>**Attempts** 0 **Last start:** 4/11/2024 4:13:57 AM |

1 - 1

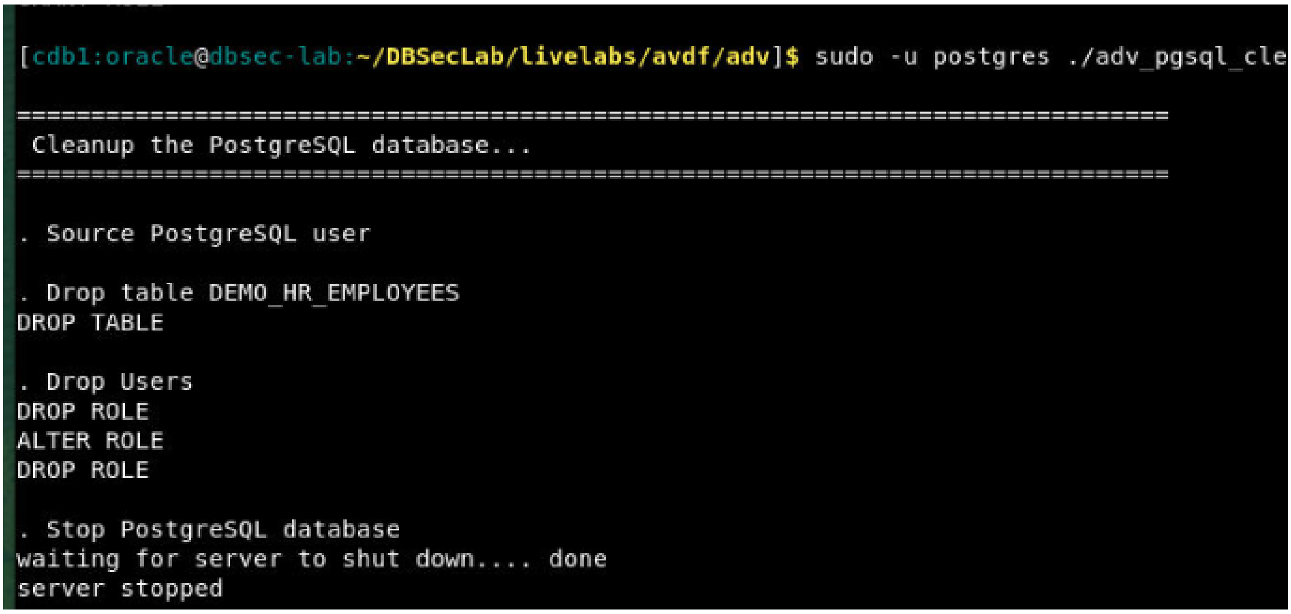


□ Event Time is in the last 24 hours
□ Exclude Login Activity
☑ Failed Event

| | Target | User | Client Host | Client Program | Event | Object |
|---|---|---|---|---|---|---|
| | PostgreSQL | | | | INFO | |
| | PostgreSQL | | | | INFO | |
| | PostgreSQL | oracle | [local] | psql | SELECT | |
| | PostgreSQL | oracle | [local] | psql | IDLE | |
| | PostgreSQL | | [local] | | INFO | |
| | PostgreSQL | oracle | [local] | | AUTHENTICATION | |

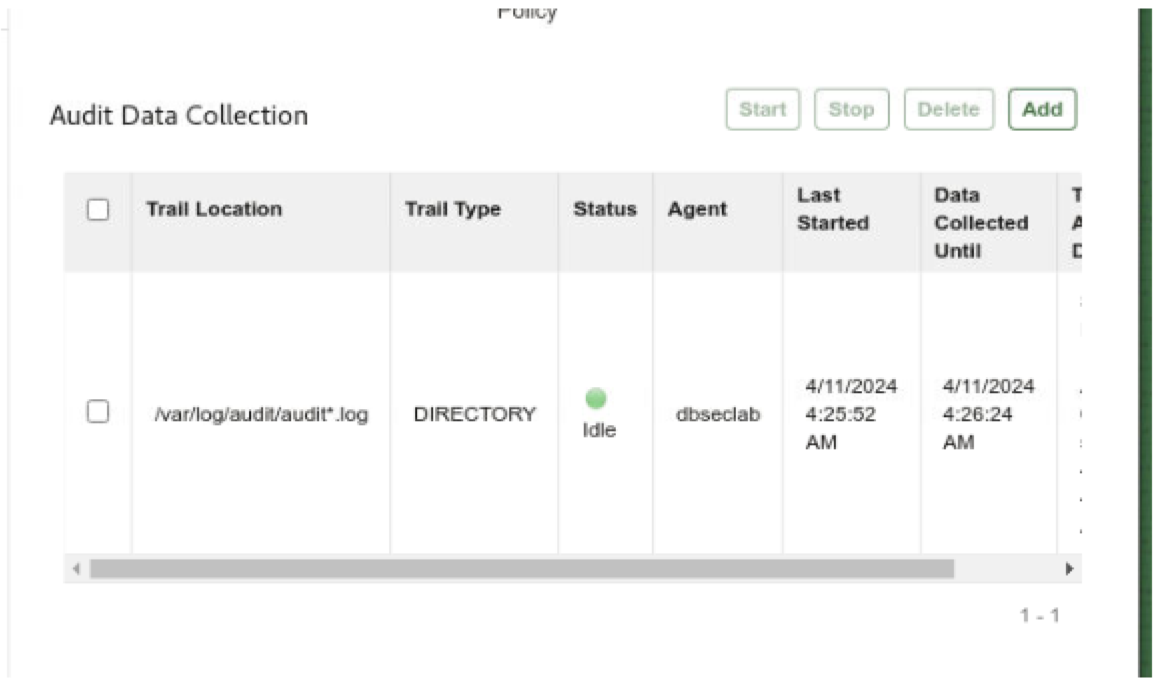


| □ | Target | Trail Location | Trail Type | Status | Targ |
|---|---|---|---|---|---|
| □ | PostgreSQL | /var/log/pgsql | DIRECTORY | ● Stopped | Po: |



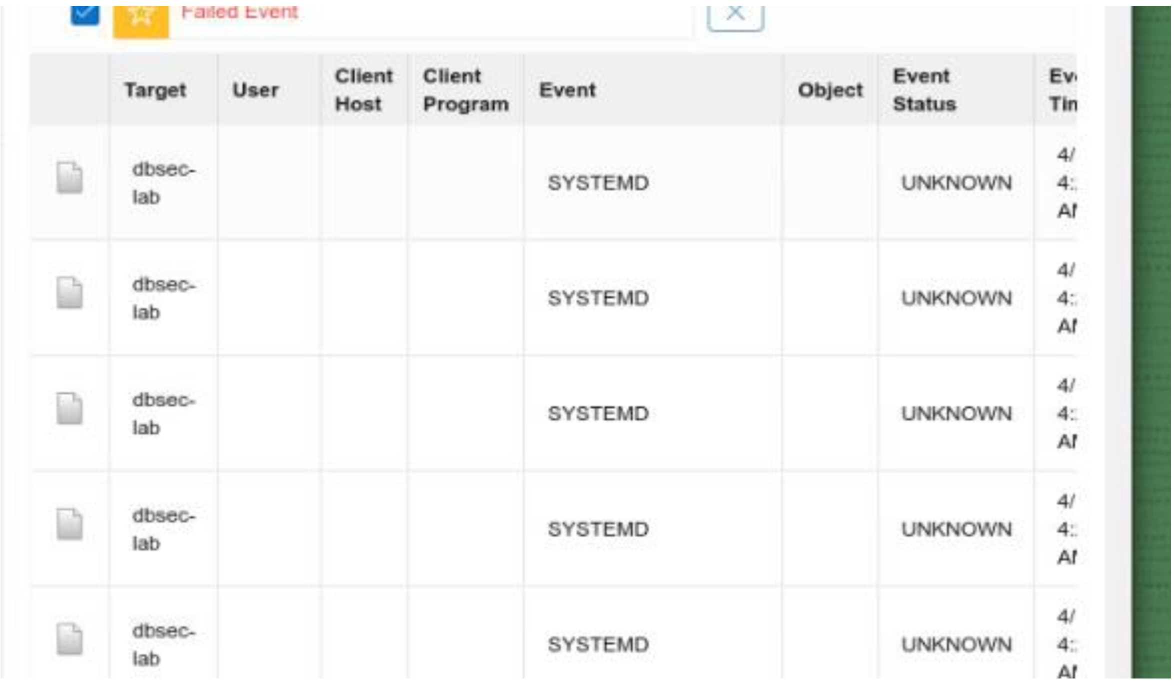
```
[cdb1:oracle@dbsec-lab:~/DBSecLab/livelabs/avdf/adv]$ sudo -u postgres ./adv_pgsql_cle

==============================================================================
 Cleanup the PostgreSQL database...
==============================================================================

. Source PostgreSQL user

. Drop table DEMO_HR_EMPLOYEES
DROP TABLE

. Drop Users
DROP ROLE
ALTER ROLE
DROP ROLE

. Stop PostgreSQL database
waiting for server to shut down.... done
server stopped
```

Step 3



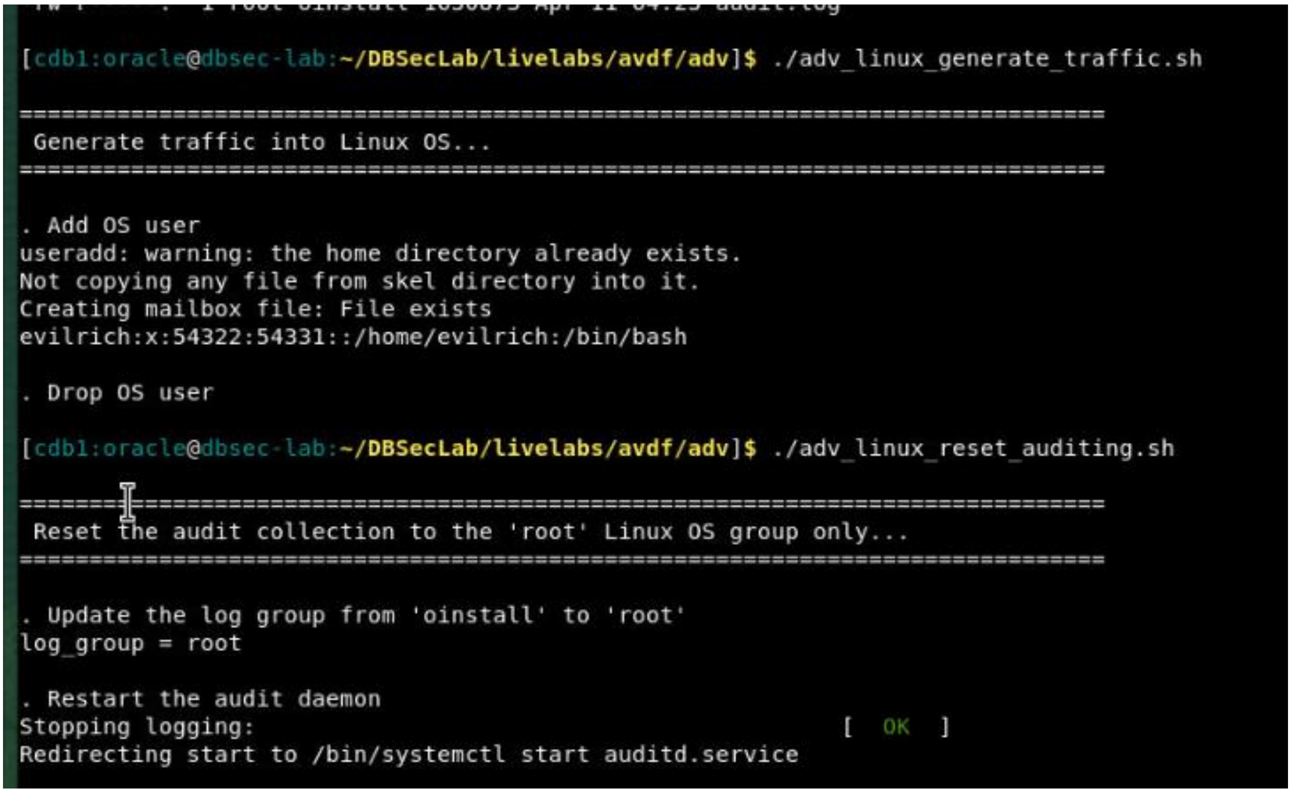
Audit Data Collection

| ☐ | Trail Location | Trail Type | Status | Agent | Last Started | Data Collected Until |
|---|---|---|---|---|---|---|
| ☐ | /var/log/audit/audit*.log | DIRECTORY | ● Idle | dbseclab | 4/11/2024 4:25:52 AM | 4/11/2024 4:26:24 AM |



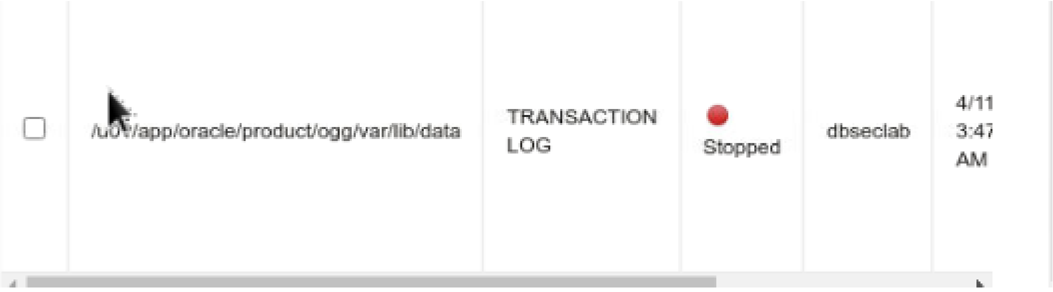
☑ Failed Event

| | Target | User | Client Host | Client Program | Event | Object | Event Status | Ev Tin |
|---|---|---|---|---|---|---|---|---|
| | dbsec-lab | | | | SYSTEMD | | UNKNOWN | 4/ 4: AI |
| | dbsec-lab | | | | SYSTEMD | | UNKNOWN | 4/ 4: AI |
| | dbsec-lab | | | | SYSTEMD | | UNKNOWN | 4/ 4: AI |
| | dbsec-lab | | | | SYSTEMD | | UNKNOWN | 4/ 4: AI |
| | dbsec-lab | | | | SYSTEMD | | UNKNOWN | 4/ 4: AI |

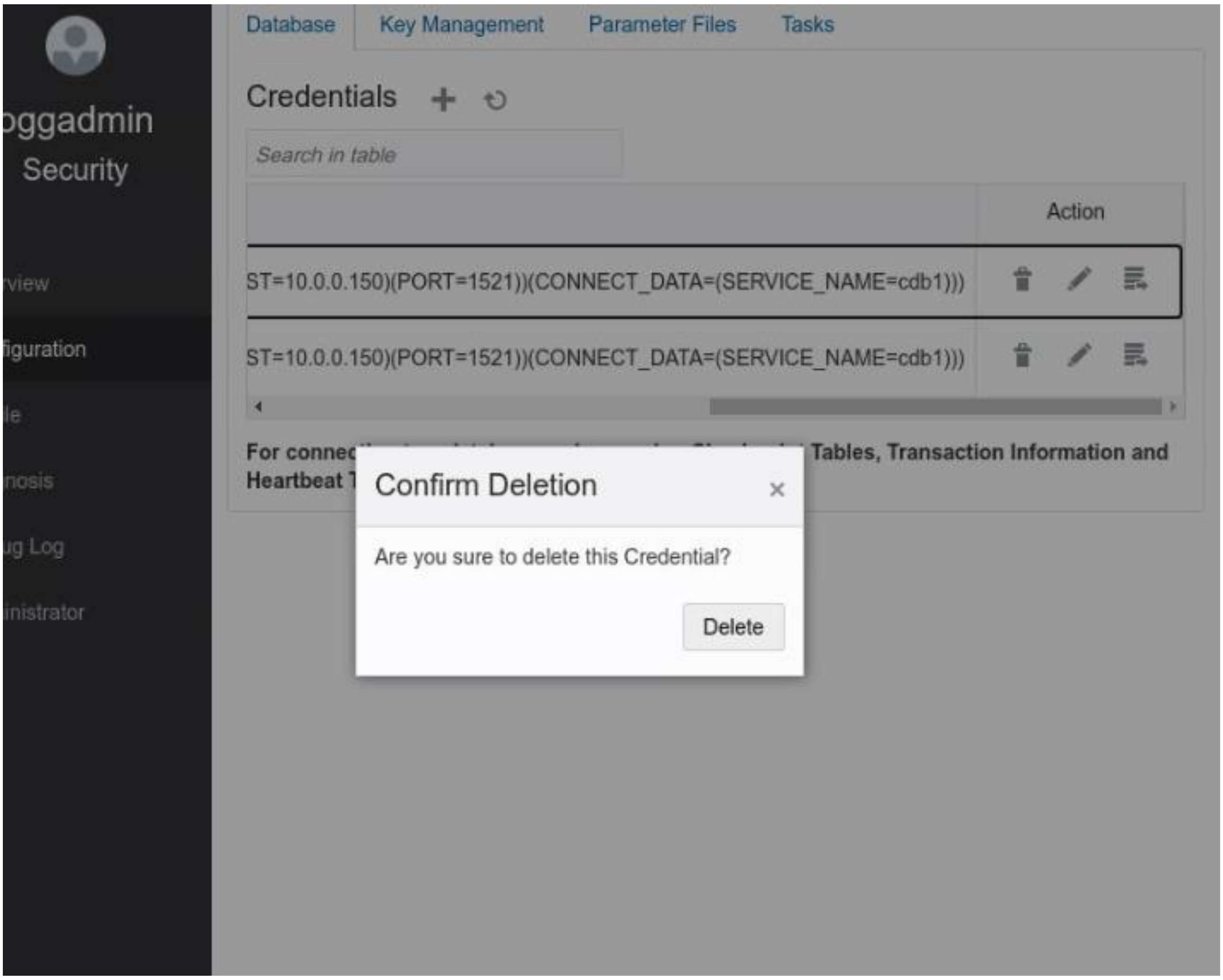


```
rw-r-----. 1 root oinstall 1030873 Apr 11 04:23 audit.log

[cdb1:oracle@dbsec-lab:~/DBSecLab/livelabs/avdf/adv]$ ./adv_linux_generate_traffic.sh

==============================================================================
 Generate traffic into Linux OS...
==============================================================================

. Add OS user
useradd: warning: the home directory already exists.
Not copying any file from skel directory into it.
Creating mailbox file: File exists
evilrich:x:54322:54331::/home/evilrich:/bin/bash

. Drop OS user

[cdb1:oracle@dbsec-lab:~/DBSecLab/livelabs/avdf/adv]$ ./adv_linux_reset_auditing.sh

==============================================================================
 Reset the audit collection to the 'root' Linux OS group only...
==============================================================================

. Update the log group from 'oinstall' to 'root'
log_group = root

. Restart the audit daemon
Stopping logging:                                          [  OK  ]
Redirecting start to /bin/systemctl start auditd.service
```

Task7: Reset the AVDF Lab configuration



| | | | | | |
|---|---|---|---|---|---|
| □ | /u01/app/oracle/product/ogg/var/lib/data | TRANSACTION LOG | ● Stopped | dbseclab | 4/11 3:47 AM |



Credentials

Search in table

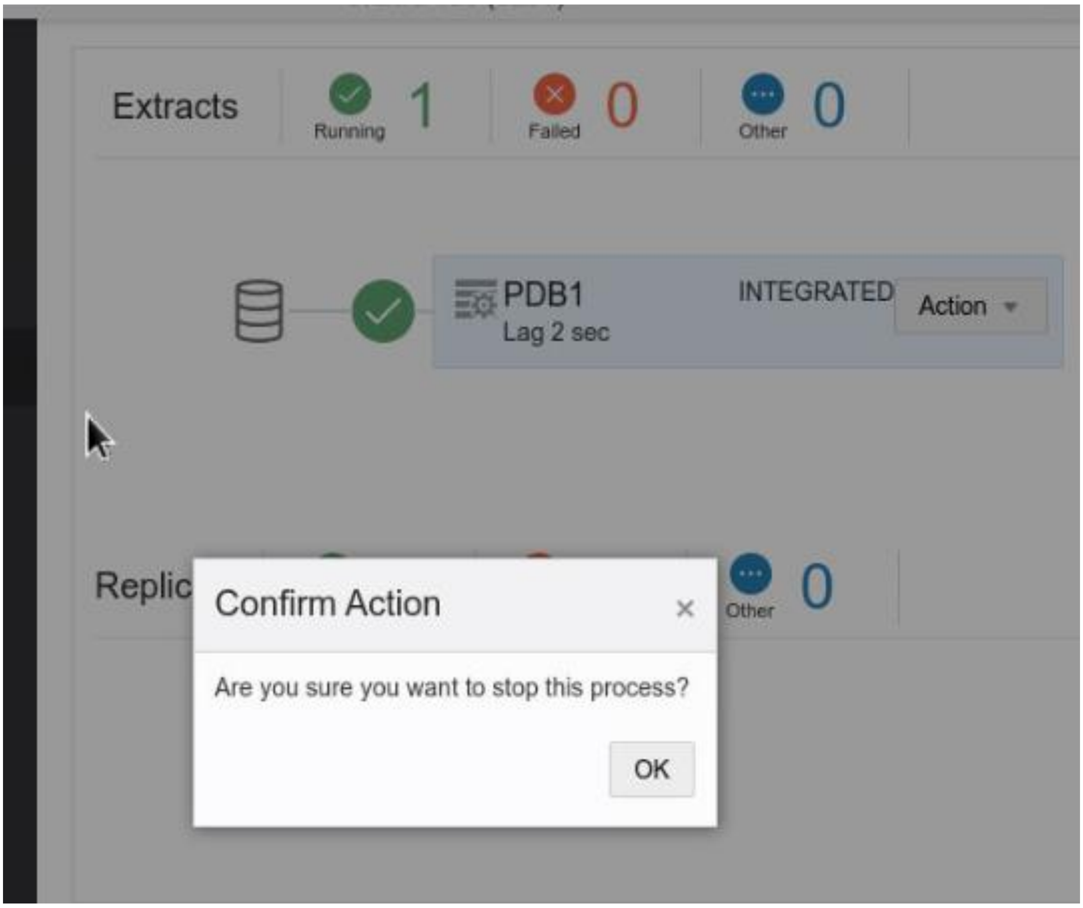
| | Action |
|---|---|
| ST=10.0.0.150)(PORT=1521))(CONNECT_DATA=(SERVICE_NAME=cdb1))) | |
| ST=10.0.0.150)(PORT=1521))(CONNECT_DATA=(SERVICE_NAME=cdb1))) | |

For connec… Tables, Transaction Information and Heartbeat T…

Confirm Deletion ×

Are you sure to delete this Credential?

Delete



Confirm Action

Are you sure you want to stop this process?