Oracle Audit Vault and Database Firewall

POC Training

Melody Liu
Andrey Brozhko
Senior Principal Product Manager
Oracle Database Security
December 11, 2014

ORACLE

Program Agenda

1. Lesson 1 – 5 (45 min)
2. Lesson 6 – 13 (1 hour 15 min)
3. Lesson 14- 16 (30 min)
4. Lesson 17 – 22 (1 hour 15 min)

Program Agenda

1. Lesson 1 – 5
   - Register Hosts, Deploy Agent
   - Register a 12c DB Secured Target
   - Configure Proper Secured Target Audit Settings
   - Configure Audit Trail for 12cDB Secured Target
   - Register a Linux Secured Target and Add a Trail
   - Basic Audit Vault Server Set Up
2. Lesson 6 - 13
3. Lesson 14- 16
4. Lesson 17 - 22

Essential Pre-Course Set Up

Environment Requirements

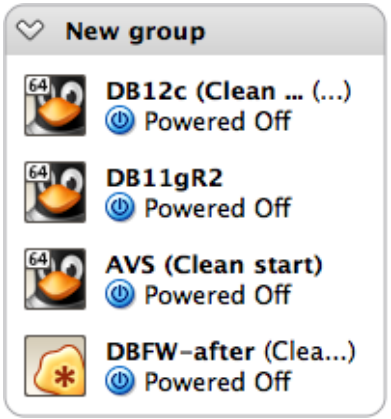
- Laptop
  - Win7 **64-bit** or Mac OSx or 64-bit Linux
  - RAM : 8GB minimum, 16 GB ideal
  - Enough disk space
- Vbox
  - Virtual Box (4.3.20) pre-installed
  - Virtual Box extensions pre-installed
- Reference : Networking in Vbox

- Download or copy 4 OVA files
  - Total File Size = 43GB
  - AVS (clean start)
  - DBFW
  - DB11gR2
  - DB12c (clean start)
- PuTTY (to access console)
- SCP to transfer files
- Flash

Lab Configuration

For these lab exercises, we will be using 4 VMs:

- DB12c
- DB11gR2
- AVS (clean start)
- DBFW-final



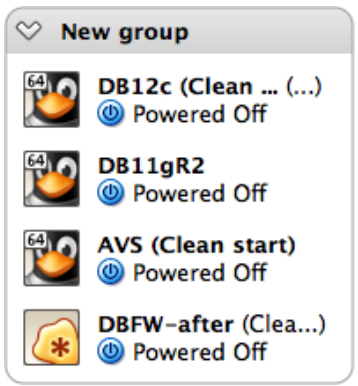
Hosts and IP addresses :

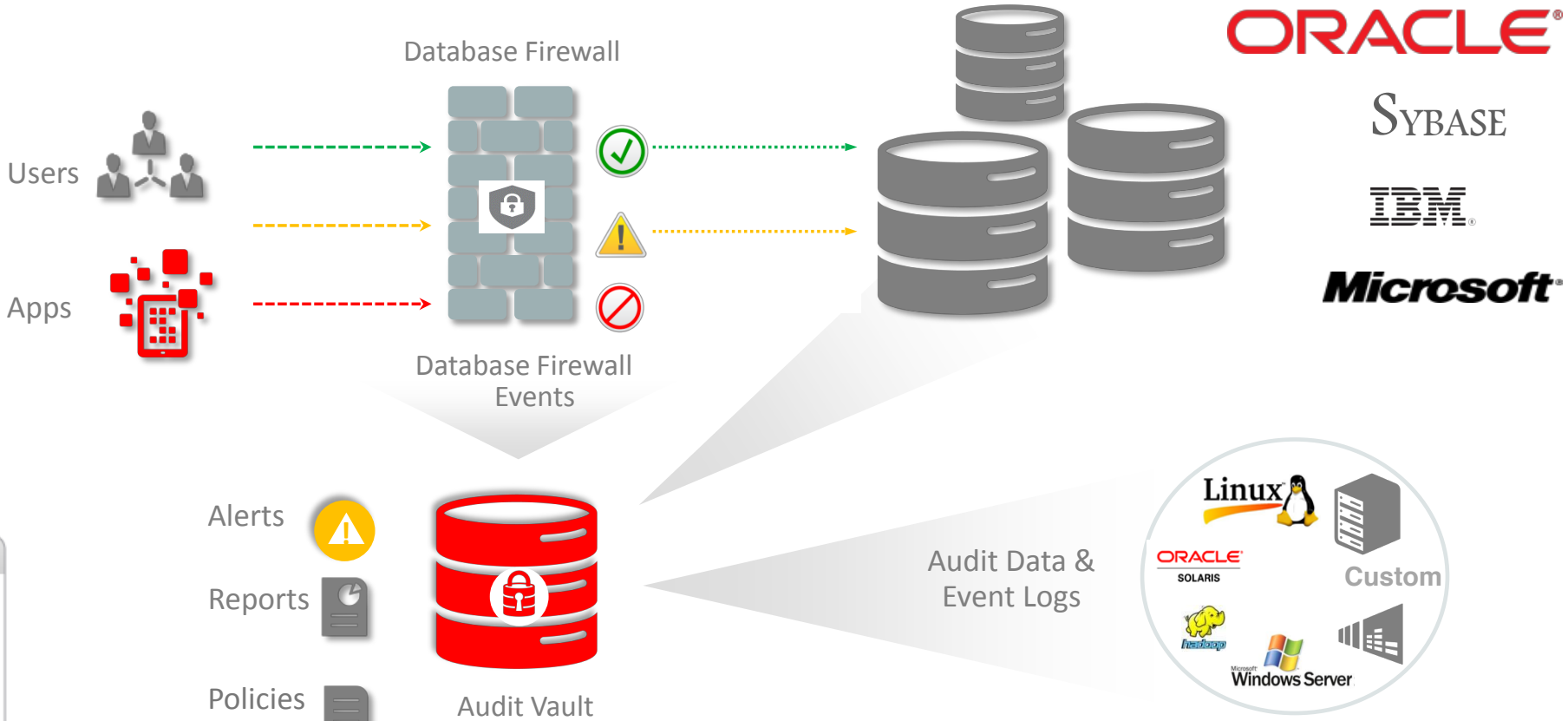
Host	IP Address
DB12c	192.168.56.101
DB11gR2	192.168.56.10
AVS	192.168.56.200
DBFW	192.168.56.12

Lab Login Accounts

AVS	AVAUDITOR, AVAUITOR_PCI	Root, support, oracle
DBFW	FWADMIN	Root, support, oracle
11gR2DB	DBA_DEBRA, DBA_NICOLE	Oracle
* HR Application	MALICIOUS_MALROY	
12cDB	DBA_DEBRA, DBA_NICOLE	oracle

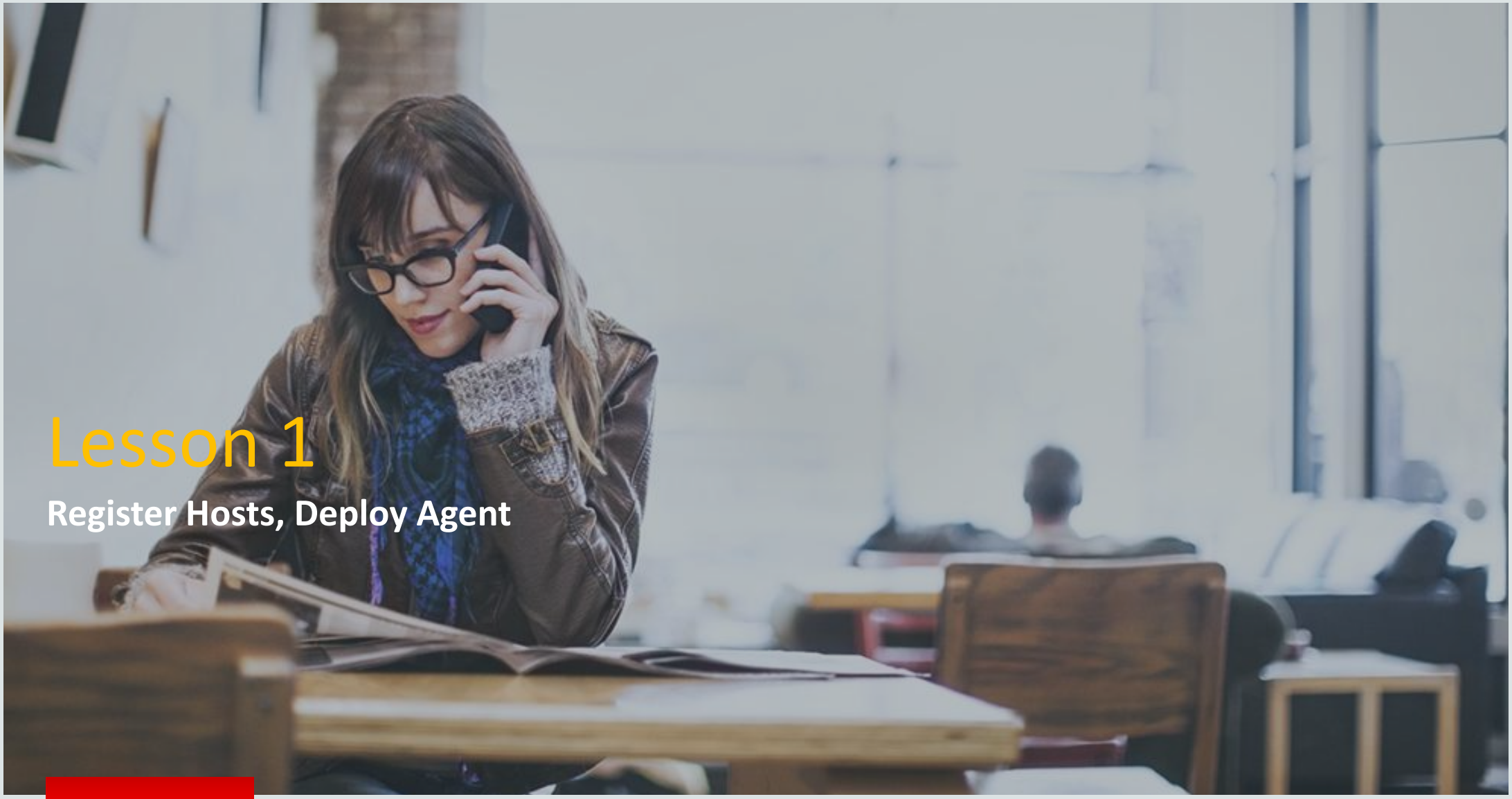
The password for all accounts is Manager_1





Audit Vault Server Use Cases

- ✓ Consolidate audit data from multiple platforms
- ✓ Meet compliance with out of box reports
- ✓ Continuously audit on sensitive or valuable data
- ✓ Alert suspicious and unauthorized activities in real time
- ✓ Identify excessive user rights, dormant users, and enable an entitlement review cycle
- ✓ Accelerate incident response and forensics investigations with filtering



Lesson 1

Register Hosts, Deploy Agent

Lesson Overview

- In this lesson, you will register a new host with a new 12cDB secured target and install/deploy an agent to the host

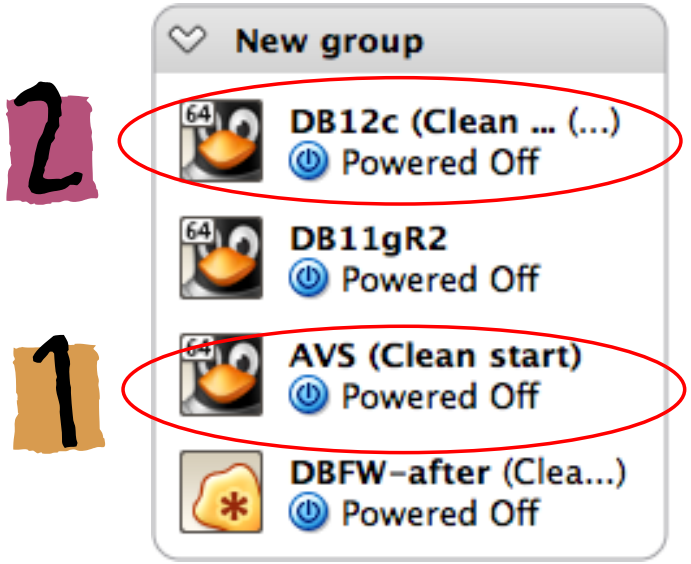
- There already exists 1 host (192.168.45.10) with 1 secured target (Oracle 11gR2) and 2 trails defined

Starting Up Your Environment

After OVA import, take a snapshot for a clean re-start

1) Start your AVS instance
2) Start your 12c instance

- Log into Linux as oracle/Manager_1
- Start a terminal session
  - $ **lsnrctl start**
  - $ sqlplus / as sysdba
  - SQL>**startup**

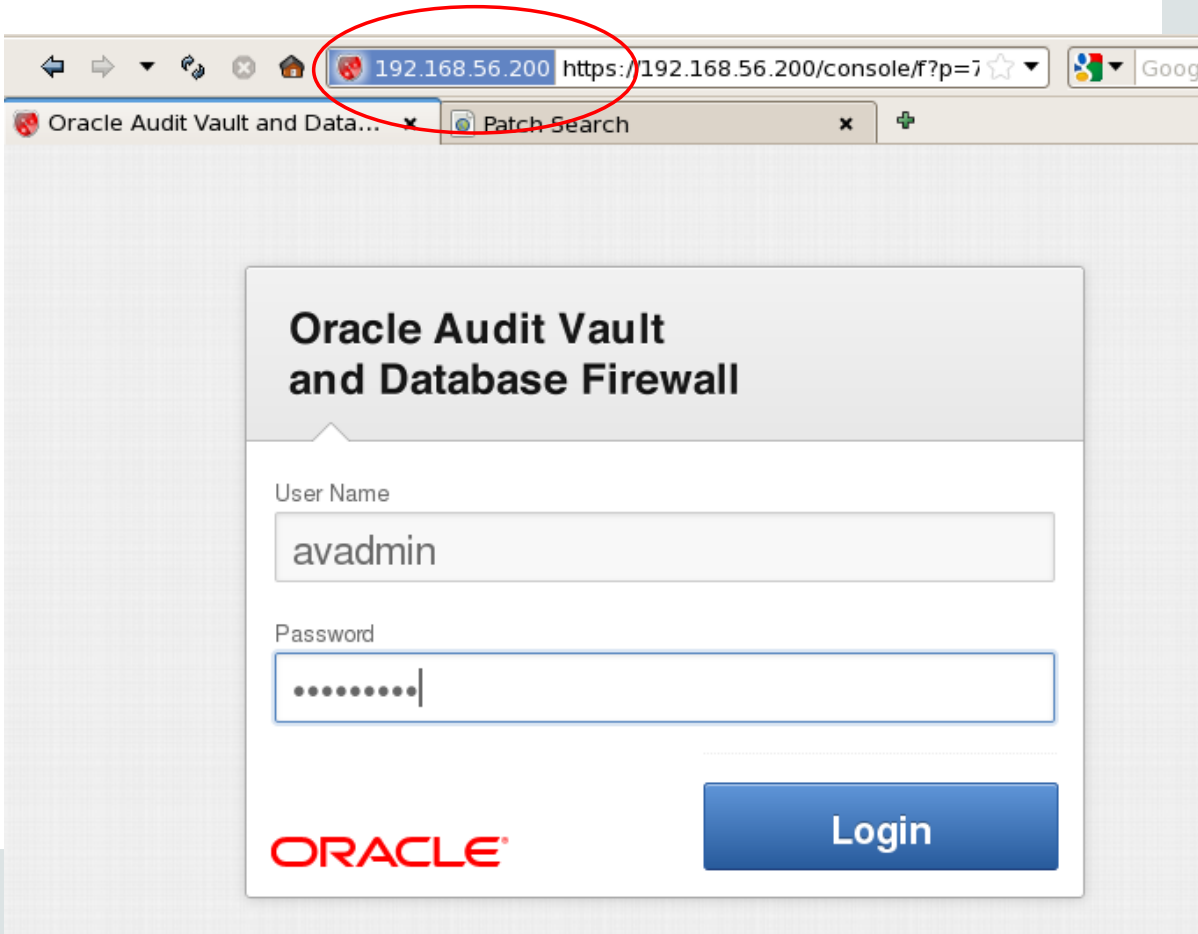


Log In to AVS Management Console

[after AVS VM is up]

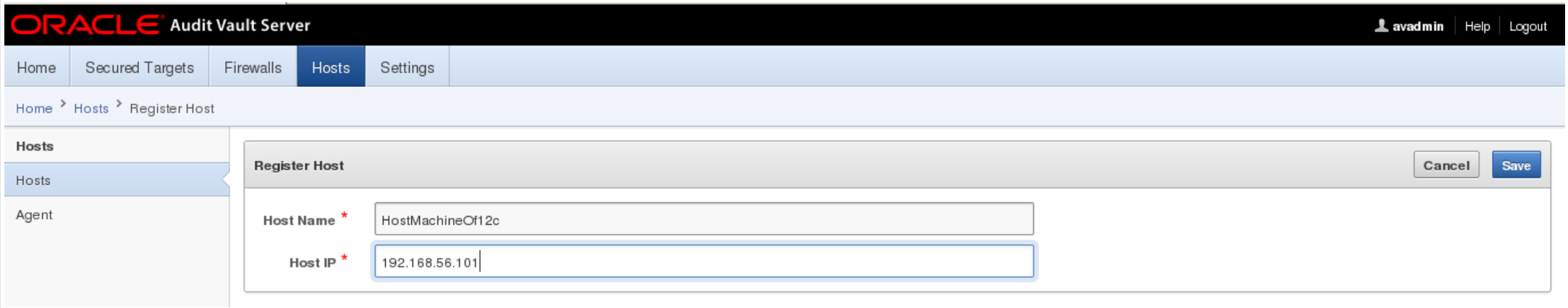
[Alt+F9 to view console]

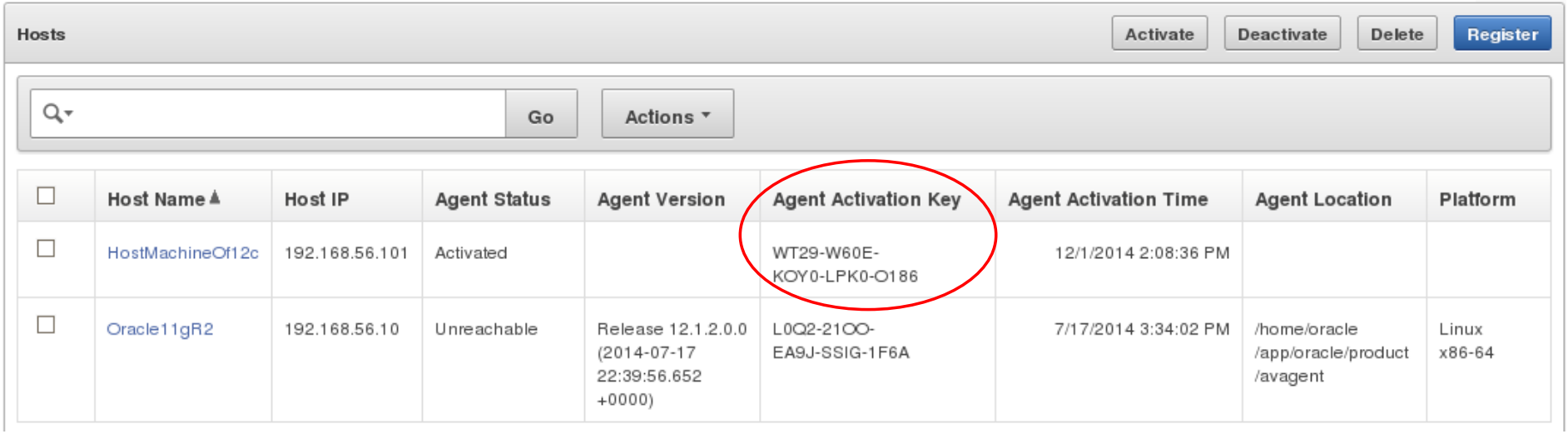
- Start a browser **from within 12c VM** and go to https://192.168.56.200
  - —or from your laptop browser
- When AVS console is up, log in with avadmin/Manager_1



Register Host of 12c

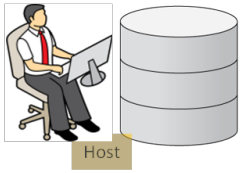
- Hosts > Register
  - Host Name = ***HostMachineOf12c*** (for demo, give it a meaningful name)
  - Host IP = 192.168.56.**101**
  - Save





Install Agent

- If you plan to collect audit records from the secured target, an agent must be installed onto the target
  - If you're deploying a Firewall, you will need to configure an Enforcement Point
- Installation of agent is a collaboration between AVS admin and Target Admin



- Register Hosts
  [key shows on console]
  [Email key]
- Download Agent

- ~~Approve Activation Request~~

- Copy agent.jar file from AVS to host
- Deploy agent : Java –jar agent.jar
- ~~Request activation : ./agentctl activate~~
- Start agent with key : ./agentctl start –k [xx]

Install Agent

1. Download agent (via GUI: Hosts > Agent > Download Agent) and save it to a file location of your choice
   - Since you're accessing AVADMIN GUI from Browser on 12c, the file is downloaded to your 12c host Desktop
   - In your POC, you may need to transport the agent.jar file to the secured target
2. Start a terminal session (whoami=oracle) on 12c
   and Create a directory avagent
   - ***cd /u01/app/oracle/product***
   - ***mkdir avagent*** (will be referred to as $AGENT_HOME)
   - ***ls –la*** to ensure they are drwxr-xr-x and **oracle oinstall**

Installing Agent – continued

3. cd /u01/app/oracle/product/avagent and move the agent.jar file there

4. Java –jar agent.jar

```
[oracle@lap-db12102 avagent]$ ls
agent.jar
[oracle@lap-db12102 avagent]$ pwd
/u01/app/oracle/product/avagent
[oracle@lap-db12102 avagent]$ java -jar agent.jar
Checking for updates...
Agent is updating. This operation may take a few minutes. Please wait...
Agent updated successfully.
Agent installed successfully.
If deploying hostmonitor please refer to product documentation for additional in
stallation steps.
[oracle@lap-db12102 avagent]$
```

When done, you will see new directories

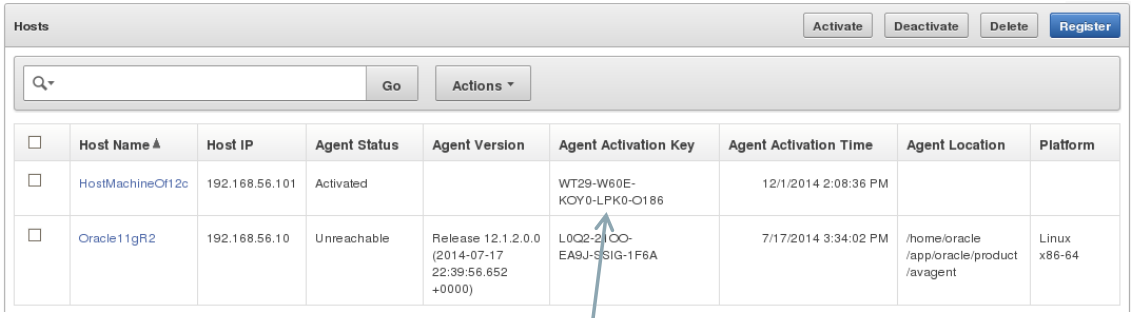
```
[oracle@lap-db12102 avagent]$ pwd
/u01/app/oracle/product/avagent
[oracle@lap-db12102 avagent]$ ls -al
total 39732
drwxr-xr-x 6 oracle oinstall     4096 Nov 11 20:08 .
drwxr-xr-x 4 oracle oinstall     4096 Nov 11 20:07 ..
-rw-r--r-- 1 oracle oinstall 40615809 Nov 11 20:06 agent.jar
drwxr-xr-x 8 oracle oinstall     4096 Nov 11 20:08 av
drwxr-xr-x 3 oracle oinstall     4096 Nov 11 20:08 bin
drwxr-xr-x 3 oracle oinstall     4096 Nov 11 20:08 network
drwxr-x--- 3 oracle oinstall     4096 Nov 11 20:08 stage
```

Installing Agent

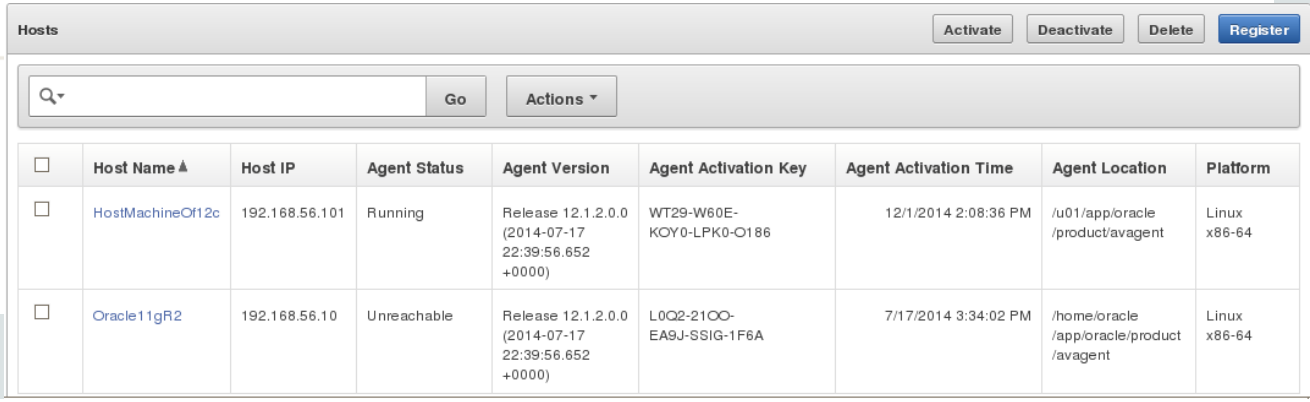
5. cd bin

./agentctl start –k

```
[oracle@lap-db12102 avagent]$ cd bin
[oracle@lap-db12102 bin]$ ls -al
total 36
drwxr-xr-x 3 oracle oinstall  4096 Nov 11 20:08 .
drwxr-xr-x 6 oracle oinstall  4096 Nov 11 20:08 ..
-rwxr-x--- 1 oracle oinstall 11697 Mar 28  2014 agentctl
-rw-r--r-- 1 oracle oinstall  9552 Mar 28  2014 agentctl.bat
drwxr-xr-x 2 oracle oinstall  4096 Nov 11 20:08 linux-x86-32
[oracle@lap-db12102 bin]$ ./agentctl start -k
Enter Activation Key:
Agent started successfully.
[oracle@lap-db12102 bin]$
```



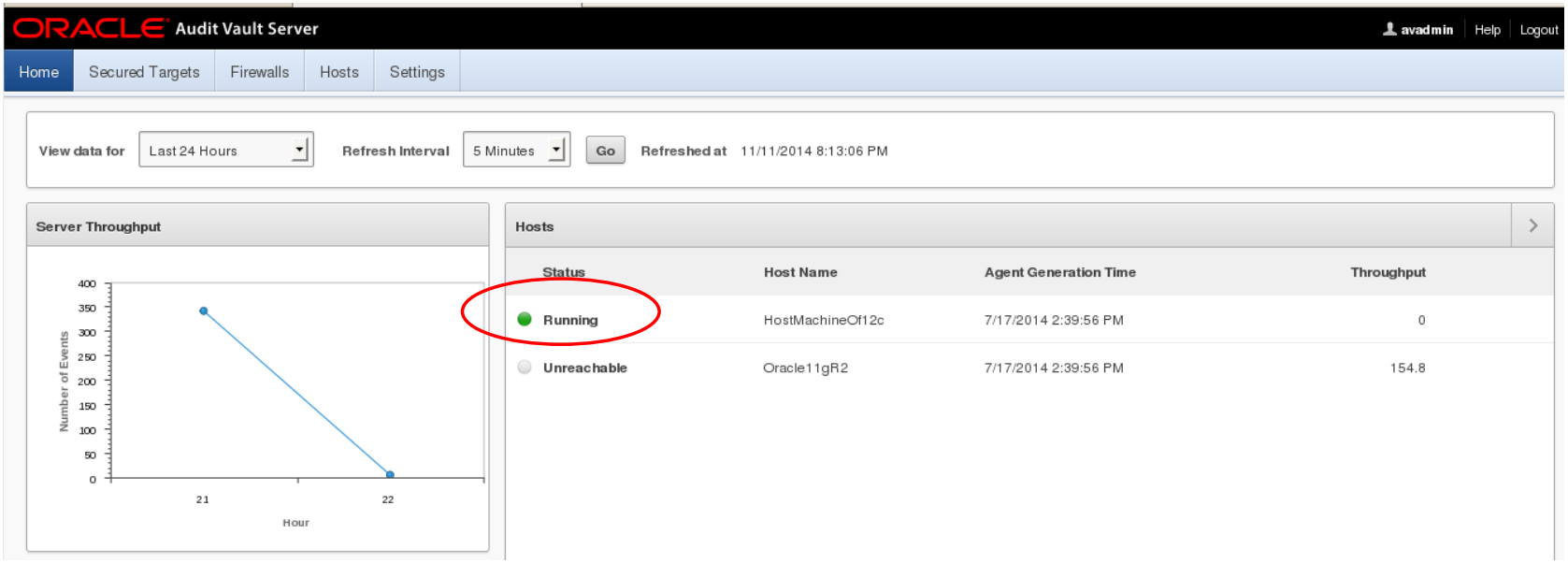
Obtain the key from Hosts page



ORACLE

Installing Agent

Go back to GUI home page and you will see the host in **Running** state



Lesson 2

Register a Secured Target

Setup Scripts – for 12c database

Setting up AVDF Account & Privileges

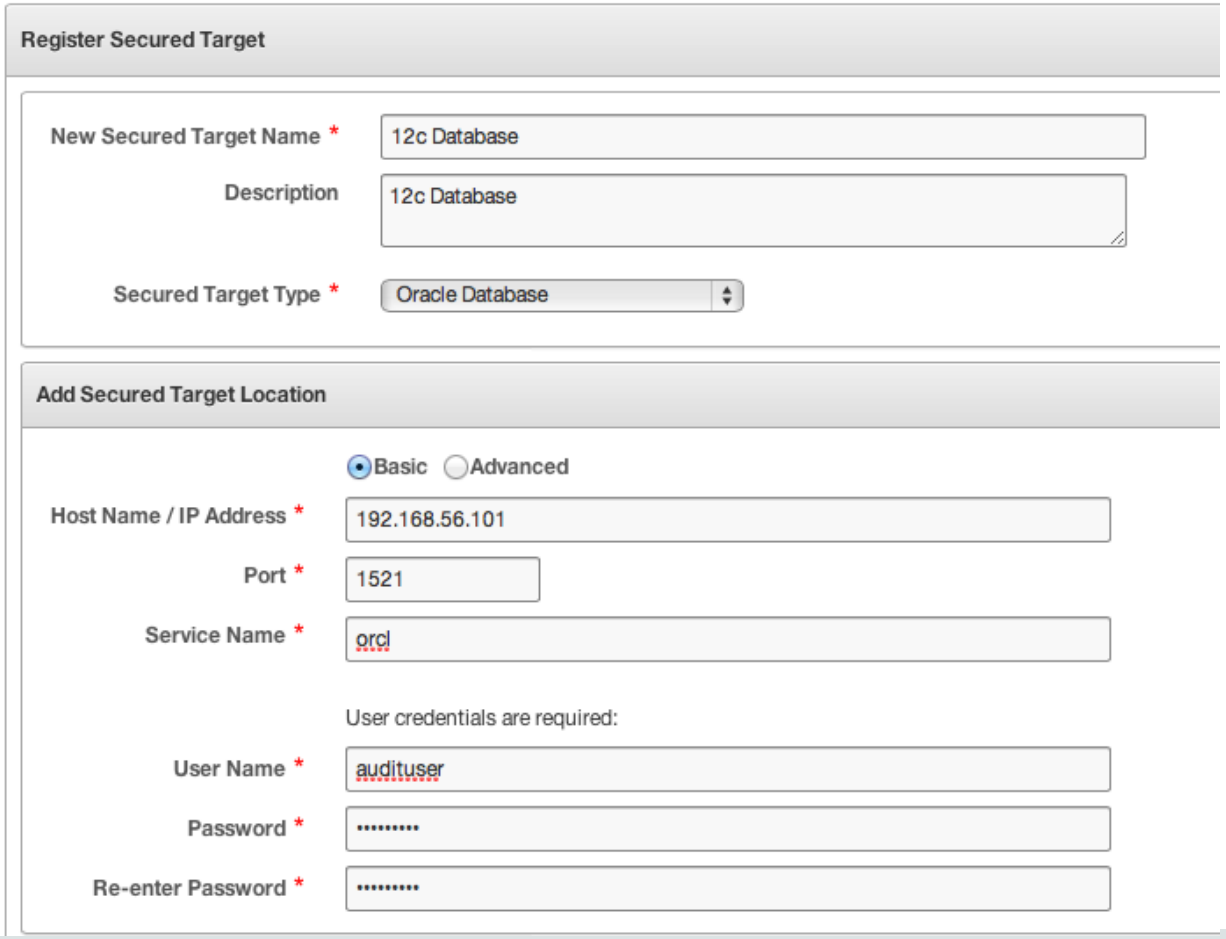
- SQL> CONNECT SYS / AS SYSDBA
- SQL> CREATE USER ***audituser*** IDENTIFIED BY ***Manager_1***
- SQL> GRANT DV_SECANALYST TO ***audituser***; (if DBV is enabled)
- SQL> GRANT DV_STREAMS_ADMIN TO ***audituser***;
- Locate scripts here :
  - $AGENT_HOME/av/plugins/com.oracle.av.plugin.{secured_target_type}/config/
- SQL>@oracle_user_setup username mode
  - Mode = ***setup, redo_coll, spa, entitlement***
  - SQL>@oracle_user_setup AUDITUSER SETUP

Run Setup Script

```
[oracle@lap-db12102 config]$ pwd
/u01/app/oracle/product/avagent/av/plugins/com.oracle.av.plugin.oracle/config
[oracle@lap-db12102 config]$ sqlplus / as sysdba

SQL*Plus: Release 12.1.0.2.0 Production on Tue Nov 18 18:49:07 2014

Copyright (c) 1982, 2014, Oracle.  All rights reserved.


Connected to:
Oracle Database 12c Enterprise Edition Release 12.1.0.2.0 - 64bit Production
With the Partitioning, OLAP, Advanced Analytics and Real Application Testing opt
ions

SQL> @oracle_user_setup audituser redo_coll;
Granting privileges to AUDITUSER ... Done.
Disconnected from Oracle Database 12c Enterprise Edition Release 12.1.0.2.0 - 64
bit Production
With the Partitioning, OLAP, Advanced Analytics and Real Application Testing opt
ions
[oracle@lap-db12102 config]$
```

Register 12c Database Secured Target

- Secured Target > Register
- Use Basic mode
- lsnrctl status to find port and service name
- **adituser** is the user you created in previous step



Register 12c Database Secured Target - continued

Optional Step

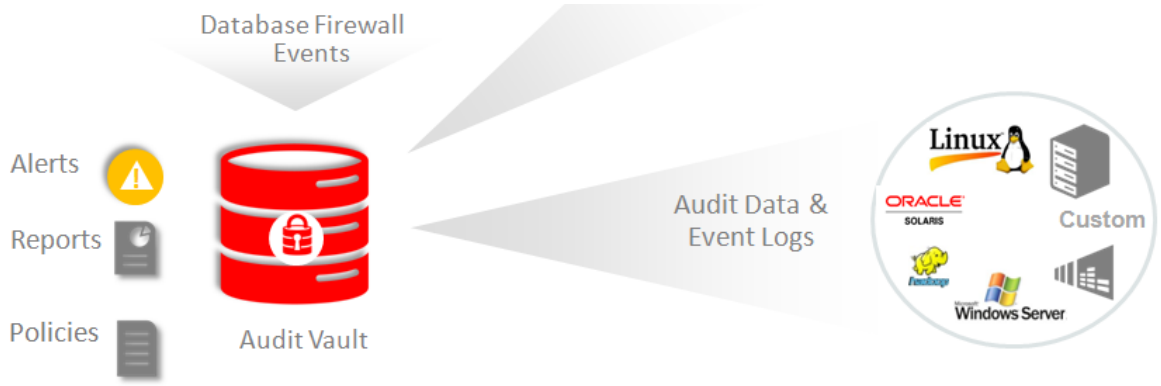
- Scroll Down to the Bottom and **Add** Collection Attributes :
- Attribute Name = **AV.COLLECTOR.CHKPNTWINDOW**
- Attribute Value = **8760 (hours in 1 year)**

Lesson 3

Configure Proper Secured Target Audit Settings

About Audit Vault Server

- It **consolidates** audit event records
  - Firewall feeds AVS
  - AV agent collects and feeds AVS
- It's a **Vault** (secured stores your audit data)
- **Successful AVDF Project starts with Proper Audit Policies**



Successful AVDF Project starts with Proper Audit Policies

1. *Start with Default Audit Settings*

secconf.sql :Oracle 12c Database Secured Configuration Script

See “Data Base Audit Settings” folder on your Desktop

```
IF USER_CHOICE = RDBMS11_CHOICE THEN
  -- 11g Secure Audit Configuration

  EXECUTE IMMEDIATE 'AUDIT ALTER ANY TABLE BY ACCESS';
  EXECUTE IMMEDIATE 'AUDIT CREATE ANY TABLE BY ACCESS';
  EXECUTE IMMEDIATE 'AUDIT DROP ANY TABLE BY ACCESS';
  EXECUTE IMMEDIATE 'AUDIT CREATE ANY PROCEDURE BY ACCESS';
  EXECUTE IMMEDIATE 'AUDIT DROP ANY PROCEDURE BY ACCESS';
  EXECUTE IMMEDIATE 'AUDIT ALTER ANY PROCEDURE BY ACCESS';
  EXECUTE IMMEDIATE 'AUDIT GRANT ANY PRIVILEGE BY ACCESS';
  EXECUTE IMMEDIATE 'AUDIT GRANT ANY OBJECT PRIVILEGE BY ACCESS';
  EXECUTE IMMEDIATE 'AUDIT GRANT ANY ROLE BY ACCESS';
  EXECUTE IMMEDIATE 'AUDIT AUDIT SYSTEM BY ACCESS';
  EXECUTE IMMEDIATE 'AUDIT CREATE EXTERNAL JOB BY ACCESS';
  EXECUTE IMMEDIATE 'AUDIT CREATE ANY JOB BY ACCESS';
  EXECUTE IMMEDIATE 'AUDIT CREATE ANY LIBRARY BY ACCESS';
  EXECUTE IMMEDIATE 'AUDIT CREATE PUBLIC DATABASE LINK BY ACCESS';
  EXECUTE IMMEDIATE 'AUDIT EXEMPT ACCESS POLICY BY ACCESS';
  EXECUTE IMMEDIATE 'AUDIT ALTER USER BY ACCESS';
  EXECUTE IMMEDIATE 'AUDIT CREATE USER BY ACCESS';
  EXECUTE IMMEDIATE 'AUDIT ROLE BY ACCESS';
  EXECUTE IMMEDIATE 'AUDIT CREATE SESSION BY ACCESS';
  EXECUTE IMMEDIATE 'AUDIT DROP USER BY ACCESS';
  EXECUTE IMMEDIATE 'AUDIT ALTER DATABASE BY ACCESS';
  EXECUTE IMMEDIATE 'AUDIT ALTER SYSTEM BY ACCESS';
  EXECUTE IMMEDIATE 'AUDIT ALTER PROFILE BY ACCESS';
  EXECUTE IMMEDIATE 'AUDIT DROP PROFILE BY ACCESS';
  EXECUTE IMMEDIATE 'AUDIT DATABASE LINK BY ACCESS';
  EXECUTE IMMEDIATE 'AUDIT SYSTEM AUDIT BY ACCESS';
  EXECUTE IMMEDIATE 'AUDIT PROFILE BY ACCESS';
  EXECUTE IMMEDIATE 'AUDIT PUBLIC SYNONYM BY ACCESS';
  EXECUTE IMMEDIATE 'AUDIT SYSTEM GRANT BY ACCESS';
  EXECUTE IMMEDIATE 'AUDIT CREATE SQL TRANSLATION PROFILE BY ACCESS';
  EXECUTE IMMEDIATE 'AUDIT CREATE ANY SQL TRANSLATION PROFILE BY ACCESS';
  EXECUTE IMMEDIATE 'AUDIT DROP ANY SQL TRANSLATION PROFILE BY ACCESS';
  EXECUTE IMMEDIATE 'AUDIT ALTER ANY SQL TRANSLATION PROFILE BY ACCESS';
  EXECUTE IMMEDIATE 'AUDIT TRANSLATE ANY SQL BY ACCESS';
  EXECUTE IMMEDIATE 'AUDIT PURGE DBA_RECYCLEBIN BY ACCESS';
  EXECUTE IMMEDIATE 'AUDIT LOGMINING BY ACCESS';
  EXECUTE IMMEDIATE 'AUDIT EXEMPT REDACTION POLICY BY ACCESS';
  EXECUTE IMMEDIATE 'AUDIT ADMINISTER KEY MANAGEMENT BY ACCESS';
  EXECUTE IMMEDIATE 'AUDIT DIRECTORY BY ACCESS';
  EXECUTE IMMEDIATE 'AUDIT PLUGGABLE DATABASE BY ACCESS';
  EXECUTE IMMEDIATE 'AUDIT EXECUTE ON DBMS_RLS BY ACCESS';
```

Successful AVDF Project starts with Proper Audit Policies

2. Only capture necessary audit data

- Not all data are equal
- Avoid noises
- Manage data growth

General Guideline :

- DDL (avoid DML when possible)
- Sensitive data (PII, PCI, PHI, IP, etc.)
- Direct database access
- Privileged account activities

Successful AVDF Project starts with Proper Audit Policies

What you should NOT audit

- noaudit select any dictionary;
- noaudit SELECT TABLE ;
- noaudit INSERT TABLE ;
- noaudit UPDATE TABLE ;
- noaudit DELETE TABLE ;

Instead Consider these

- audit SELECT TABLE whenever not successful
- audit UPDATE TABLE whenever not successful
- audit DELETE production_TABLE
- audit SELECT sensitive_table;

Use Case Sharing

Audit DDL/DML via SQLPLUS

Using the database login/logoff trigger approach is a useful and commonly deployed approach to ensure that auditing of all privileged users takes place whenever they login to a production database (which typically is thru SQL Plus, Toad, SQL Developer or other tools that bypass the application tier). This strategy is critical since auditing activities of privileged users is a common compliance requirement of IRS 1075 and other federal and state regulations.

So it is simply a matter of including the privileged user names in an IN list within the database login and logoff trigger code, and then also setting AUDIT_SYS_OPERATIONS to TRUE to audit all database connections as SYS. You guarantee that all of your privileged users are audited by access whenever they connect to the database.

Kurt Lysy | Principal Sales Consultant, Database Security

Successful AVDF Project starts with Proper Audit Policies

3. Choose AUDIT_TRAIL wisely to minimize performance

For best performance and most comprehensive reporting, we recommend **XML, X**

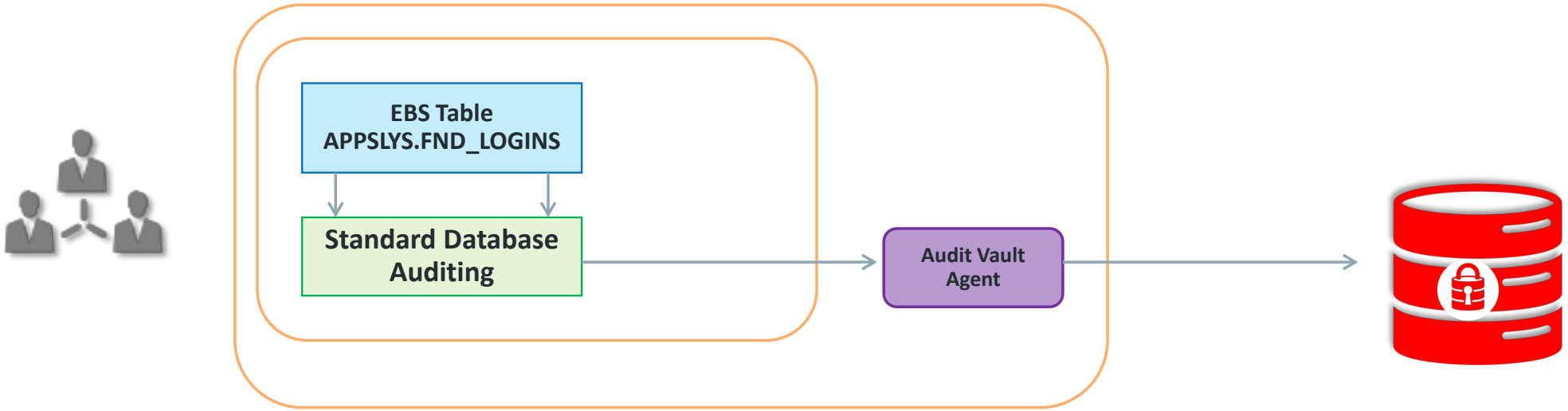
4. Audit privileged accounts

alter system set audit_trail=XML, EXTENDED audit_sys_operations=true scope=spfile;

[Will need to restart database]

Successful AVDF Project starts with Proper Audit Policies

5. Identify Sensitive Data Objects/Tables



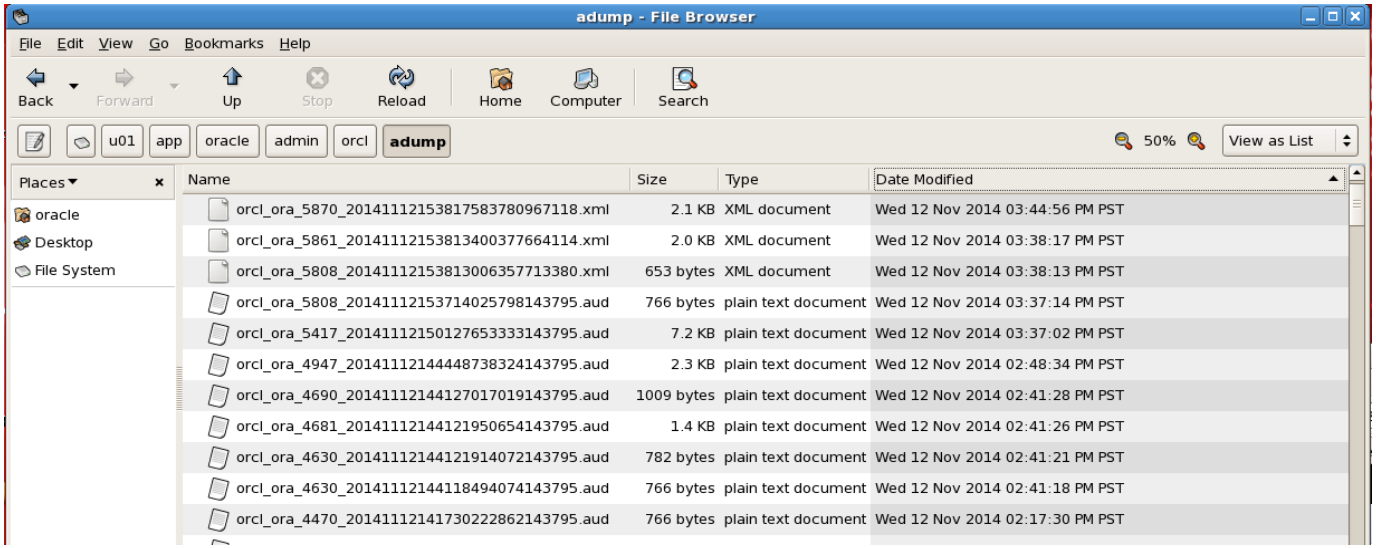
Audit Settings for Oracle Secured Target Type

- Sqlplus / as sysdba
- Show parameter audit
- *alter system set audit_trail=XML, EXTENDED audit_sys_operations=true scope=spfile;*
- Shutdown immediate;
- Startup;

```
SQL> show parameter audit;

NAME                                 TYPE        VALUE
------------------------------------ ----------- ------------------------------
audit_file_dest                      string      /u01/app/oracle/admin/orcl/adu
                                                 mp
audit_sys_operations                 boolean     TRUE
audit_syslog_level                   string
audit_trail                          string      XML, EXTENDED
unified_audit_sga_queue_size         integer     1048576
SQL>
```

Audit Settings for Oracle Secured Target Type

- XML files will show up in /u01/app/oracle/admin/orcl/adump directory



Now you are ready to add an audit trail on AVS

Audit Settings for This Lesson

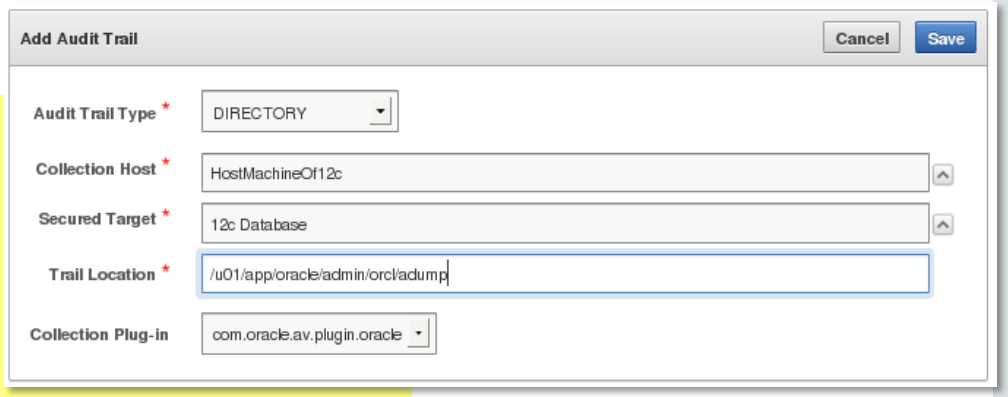
- Desktop > “Database Audit Settings”
- “Current audit settings”
- SQLPLUS audit statements [already done for you]

Lesson 4

Configure Audit Trail for 12c Secured Target

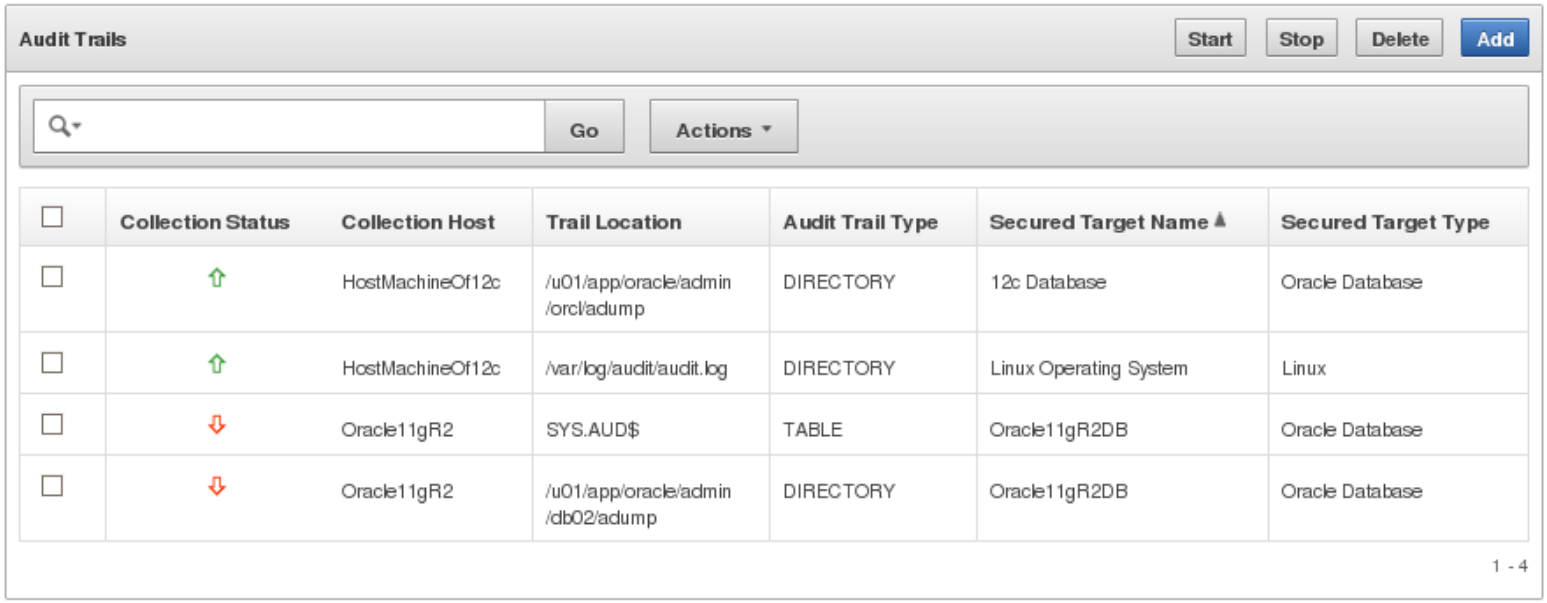
Add Audit Trails

- In order to start collecting audit data from 12c, you must configure an audit trail and the start the audit trail collection.
- You will define the audit trail that you just set in 12c : XML, EXTENDED
- Secured Targets > Audit Trails > **Add**
- Audit Trail type = DIRECTORY
- Collection Host = 192.168.56.101
- Secured Target Name = 12c Database
- Trail Location = /u01/app/oracle/admin/orcl/adump
- Save



Start Audit Trail

- Select newly created audit trails and **Start**
- You should see “Request Successful” message
- Refresh screen until you see audit trail up with green arrows



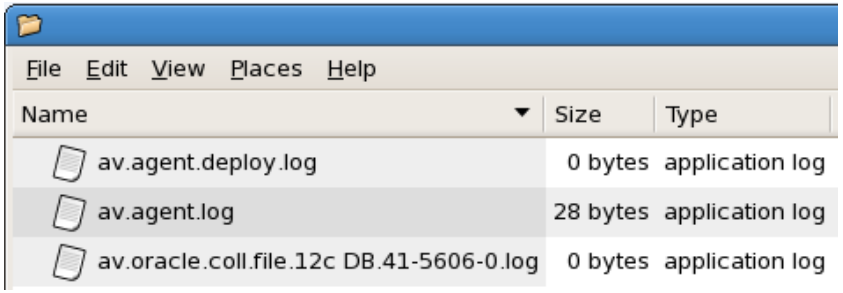
What You've Done So Far (POC Checklist)

1. Register Host from AVS GUI
2. Download Agent file, Install Agent on the Host, Start Agent
3. Create AVDF account on Target, Run setup script
4. Register a Secured Target from AVS GUI
5. Develop a Sensible Audit Policy and Configure Audit Settings on Target
6. Add an Audit Trail from AVS GUI

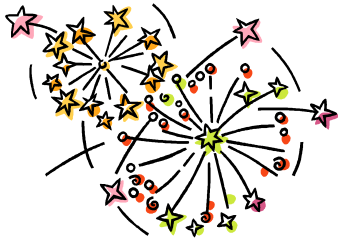
Register Secured Targets Troubleshooting

- Can you ping <AVS> -- <target db>
- lsrnctl status
- Is db started
- ./agentctl status/stop/start
- Is Host reachable from GUI (Running)
- Did you start audit trail
- Did you create audituser
- Did you run setup script
- Check syntax

- When all fail, get log files :
- $AGENT_HOME/av/log



You are done with 12c secured target.

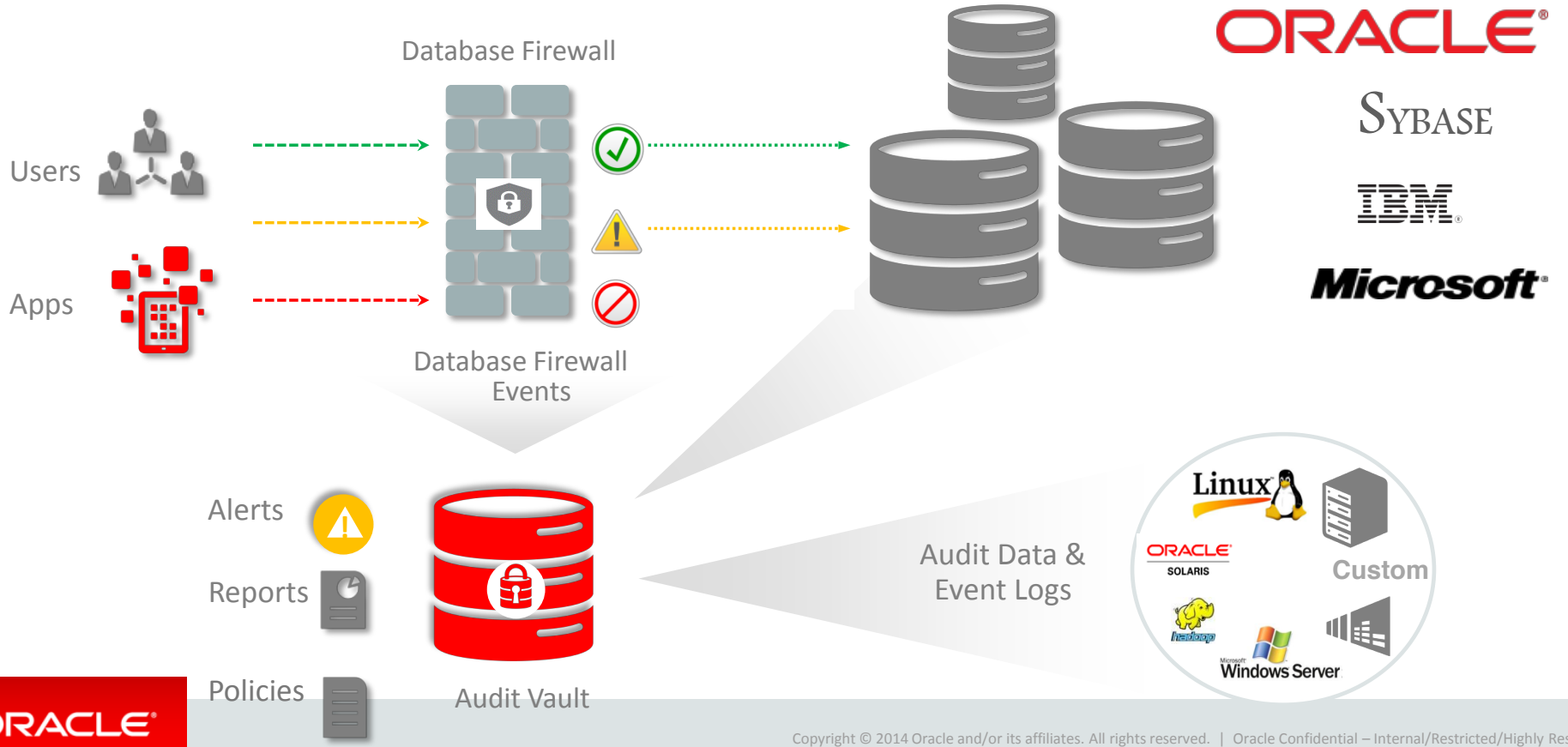


Now let's go register a Linux secured target.

Lesson 5

Register a Linux Secured Target & Add a Trail

Audit Data Consolidation

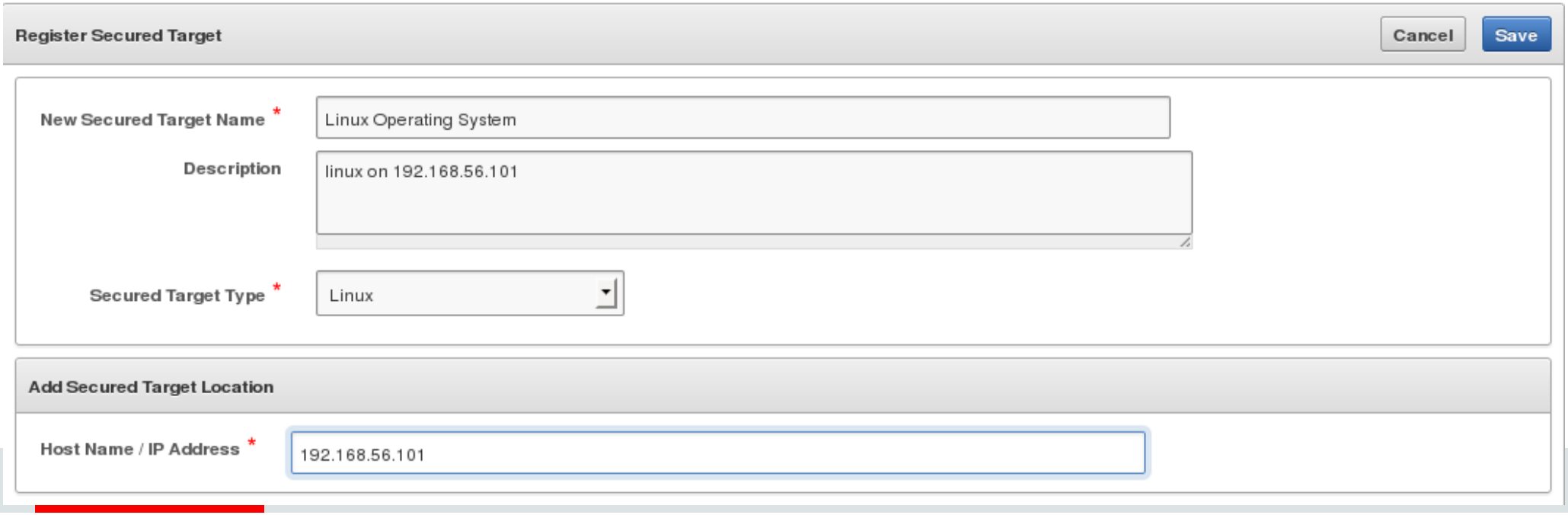


Critical Prep Work - Before Register **Linux** Secured Target

1. Ensure ***auditd*** requirement is met (***rpm -q audit***)
   - ***Yum update audit –y***
2. Audit files are owned by root so ***oinstall*** needs to be added to group in ***auditd.conf*** file if agent was started by user other than root (oracle)
   - id (as oracle) to see if group=oinstall
   - vi /etc/audit/auditd.conf (group = root→oinstall) as root
3. Data is stored in default location : /var/log/audit/audit*.log
   - ***chmod 555 /var/log/audit*** (r-x of the directory)
4. /etc/init.d/auditd start|stop

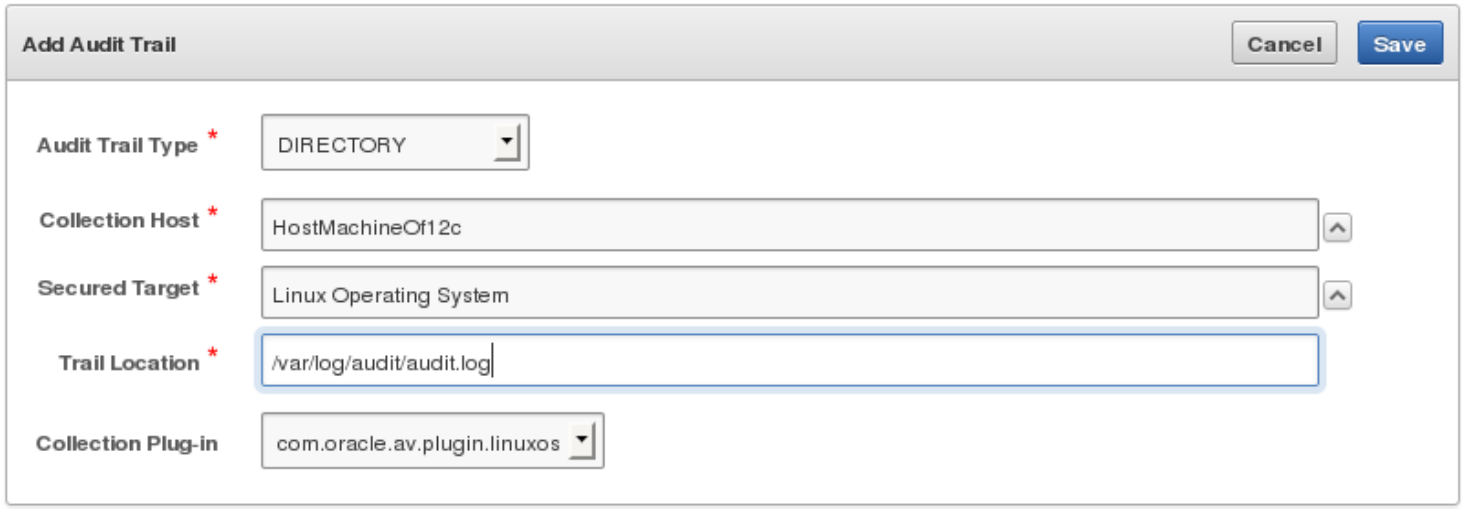
Register **Linux** Secured Target

- It's on the same host (192.168.56.101)
  - So no need to register hosts
- Register a new secured target

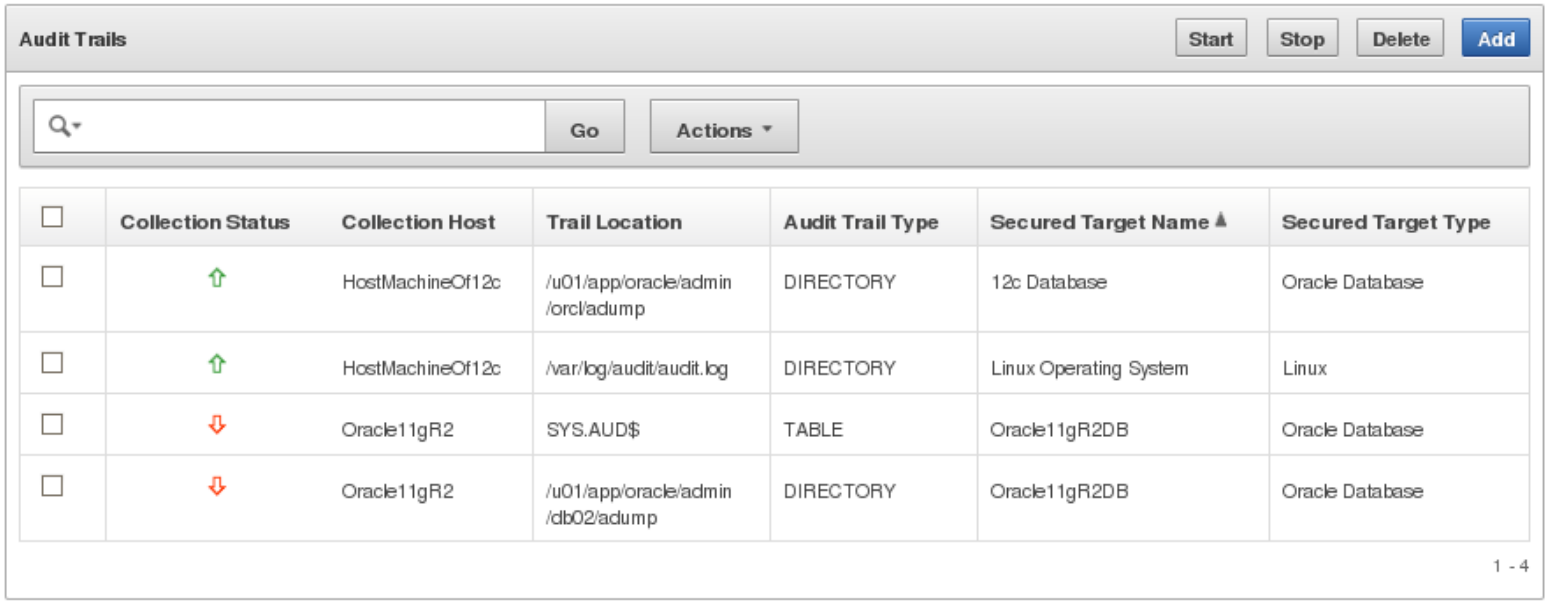


Add a Trail

- **TRAIL TYPE : DIRECTORY**
- {default path = /var/log/audit/audit*.log}



Start the Newly Added Linux Trail

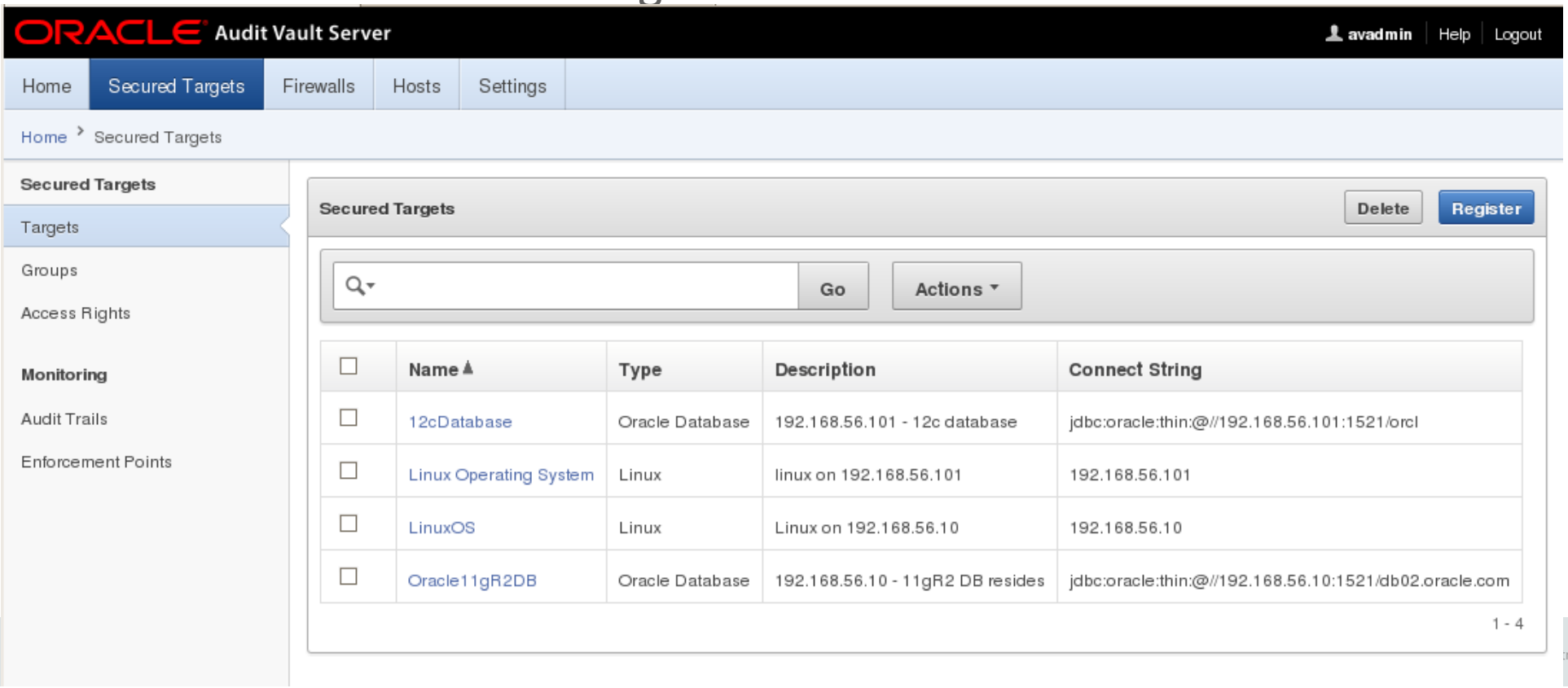


Linux Auditing 101

- Basic audit setting should suffice
- See Oracle Linux auditing best practices
- Oracle Linux Security Guide
- Ensure files are backed up weekly onto a different system
- Ensure old logs are closed out and new audit logs are started daily

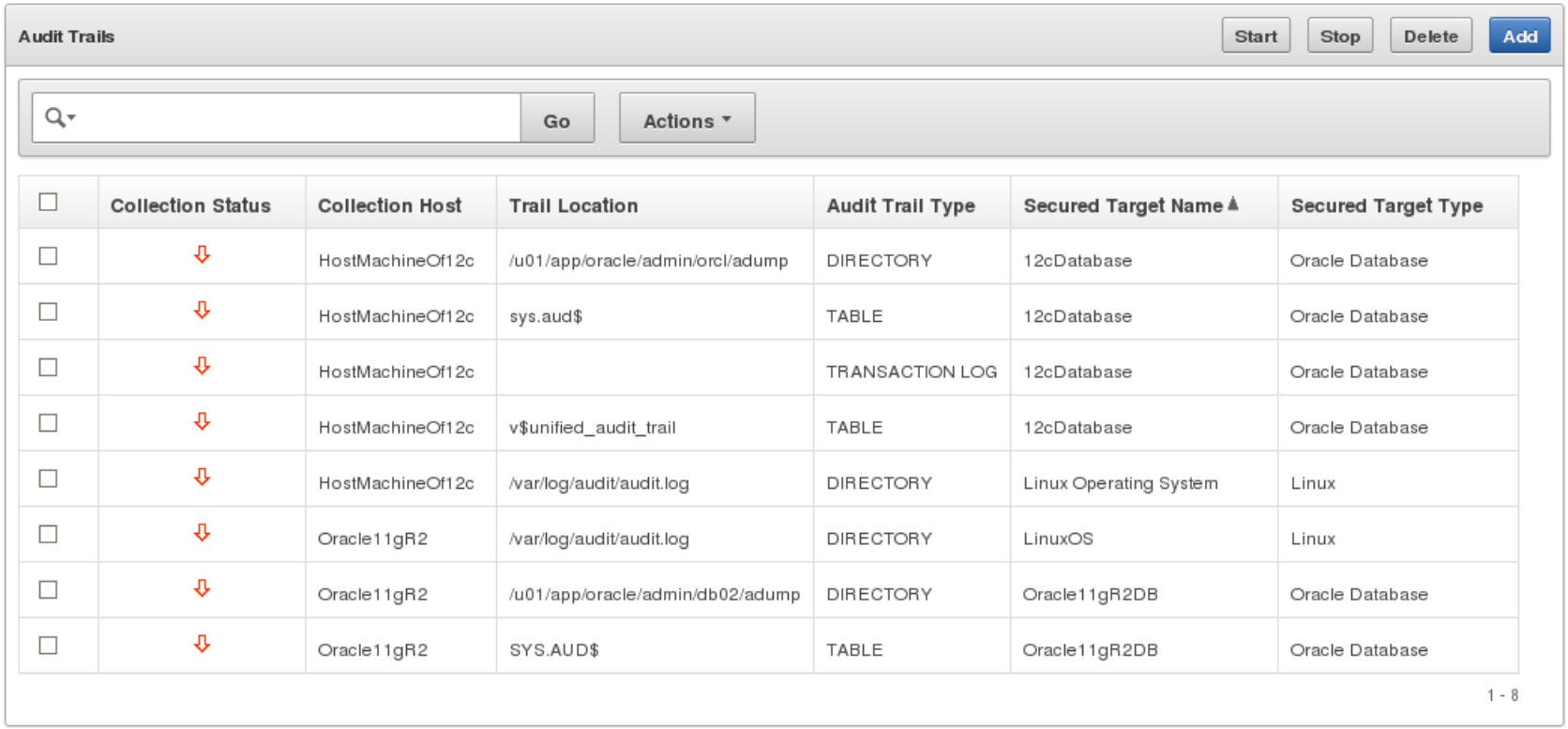
What You've Done So Far

- You now have 3 Secured Targets



Configurations on AVS-Final Instance

- You will have a few more Audit Trails by the end of the day
  - You will practice add TRANSACTION LOG trail later



Collection Status	Collection Host	Trail Location	Audit Trail Type	Secured Target Name	Secured Target Type
⇩	HostMachineOf12c	/u01/app/oracle/admin/orcl/adump	DIRECTORY	12cDatabase	Oracle Database
⇩	HostMachineOf12c	sys.aud$	TABLE	12cDatabase	Oracle Database
⇩	HostMachineOf12c		TRANSACTION LOG	12cDatabase	Oracle Database
⇩	HostMachineOf12c	v$unified_audit_trail	TABLE	12cDatabase	Oracle Database
⇩	HostMachineOf12c	/var/log/audit/audit.log	DIRECTORY	Linux Operating System	Linux
⇩	Oracle11gR2	/var/log/audit/audit.log	DIRECTORY	LinuxOS	Linux
⇩	Oracle11gR2	/u01/app/oracle/admin/db02/adump	DIRECTORY	Oracle11gR2DB	Oracle Database
⇩	Oracle11gR2	SYS.AUD$	TABLE	Oracle11gR2DB	Oracle Database

1 - 8

Lesson 0

Basic Audit Vault Server Set Up

Setting Up Audit Vault Server

- Log in to AV console as AVADMIN
- ★ Set Data, time, keyboard locale
  - Ideally, use NTP server
  - Timezone offset is always used in data centers to account for day light savings
  - Always check “Sync Time After Save” + “Enable NTP Sync”
- ★ Set network setting
  - Link Status : always “auto negotiated”
  - Change Host name to something friendly
- This will force AVServer to reboot

[this is already done for you]

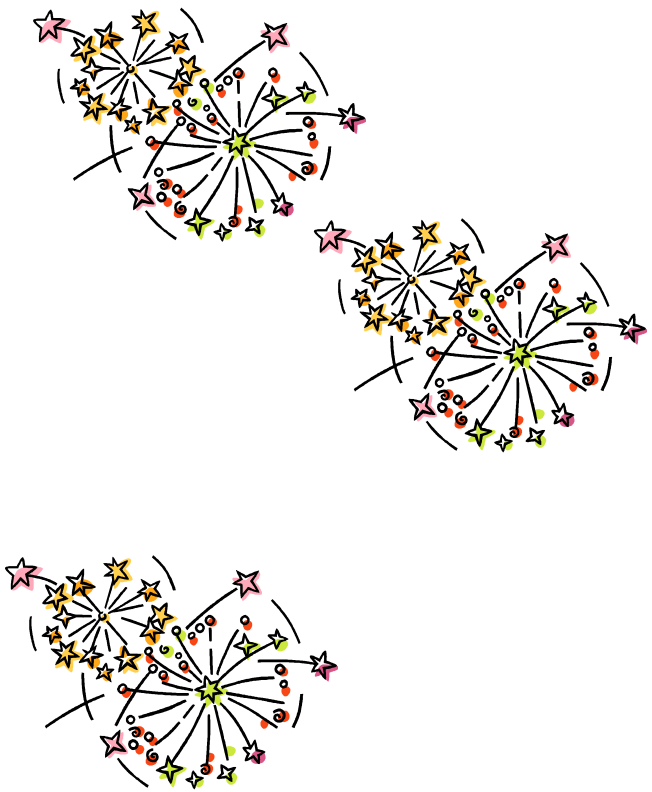
Setting Up Audit Vault Server

- Enable all services :
  - DNS (not using this during the class)
  - Web GUI
  - SSH console access
  - SNMP access

[this is already done for you]

- In POC, further lock down access by specifying IP addresses

- Your AVS configuration is done ! Congratulations !
- Now let’s switch gear to AVAUDITOR

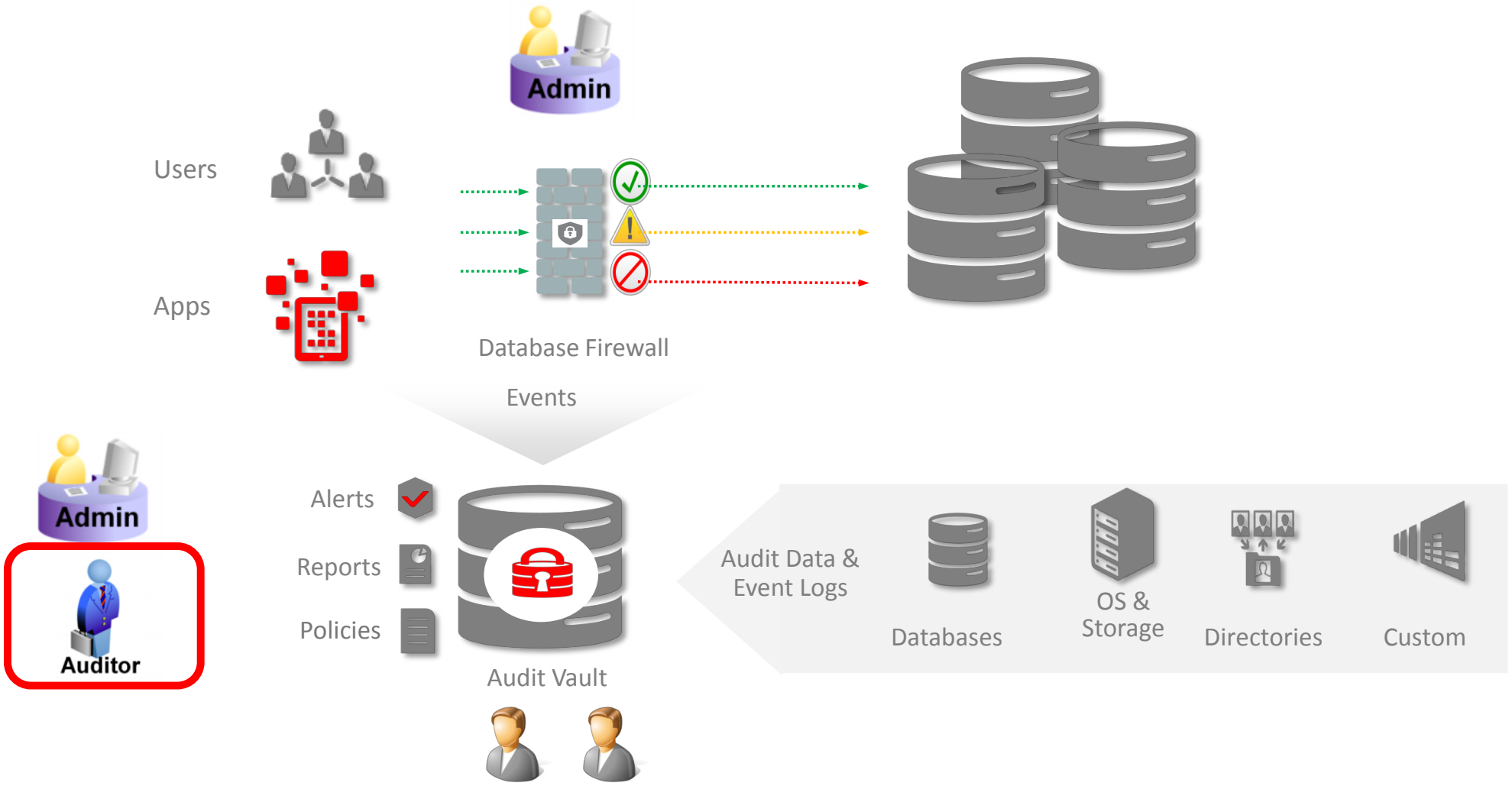


Program Agenda

1. Lesson 1 - 5
2. Lesson 6 – 13
   - Switching to Auditor
   - All About Reports
   - Audit Settings Management UI
   - Data Modification Before-After Value Report
   - Entitlement Report
   - Customize Reports
   - Investigate Suspicious Event
   - Alerts 101

Lesson 6

Switching to Auditor

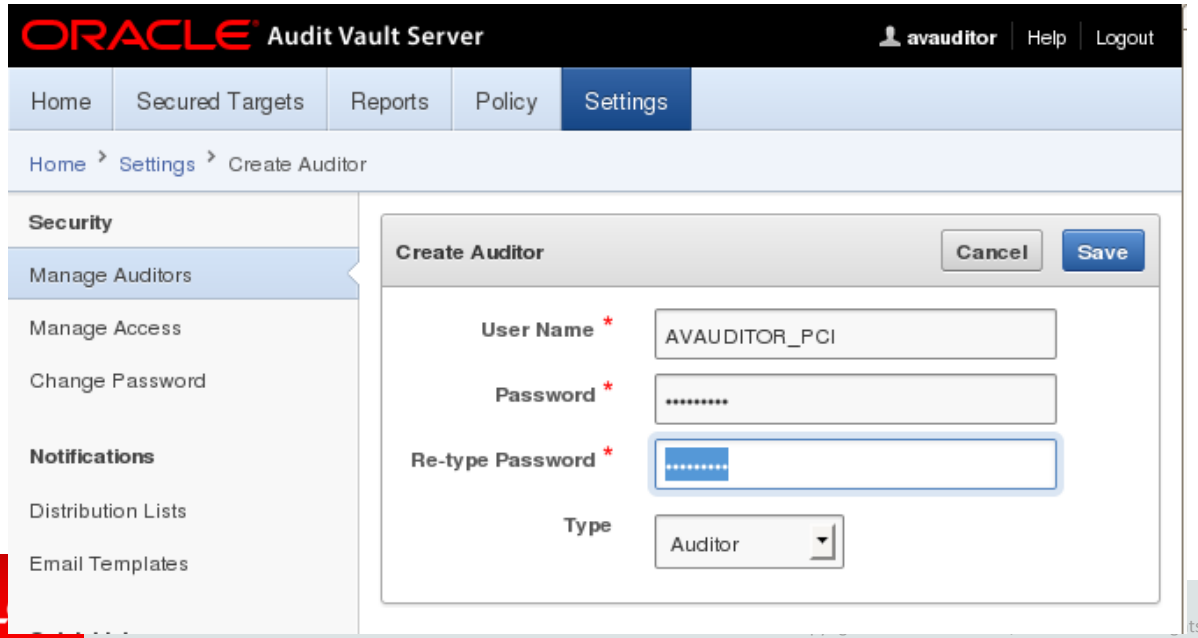


Auditor Tasks

- Manage Reports
  - View, download, add filter, save, schedule, annotate, attest, notify, customize
- Create Policies
  - Audit Alert Policies + Firewall Policies
- Manage Audit Settings (only 11g or traditional in 12)
- Manage Accounts

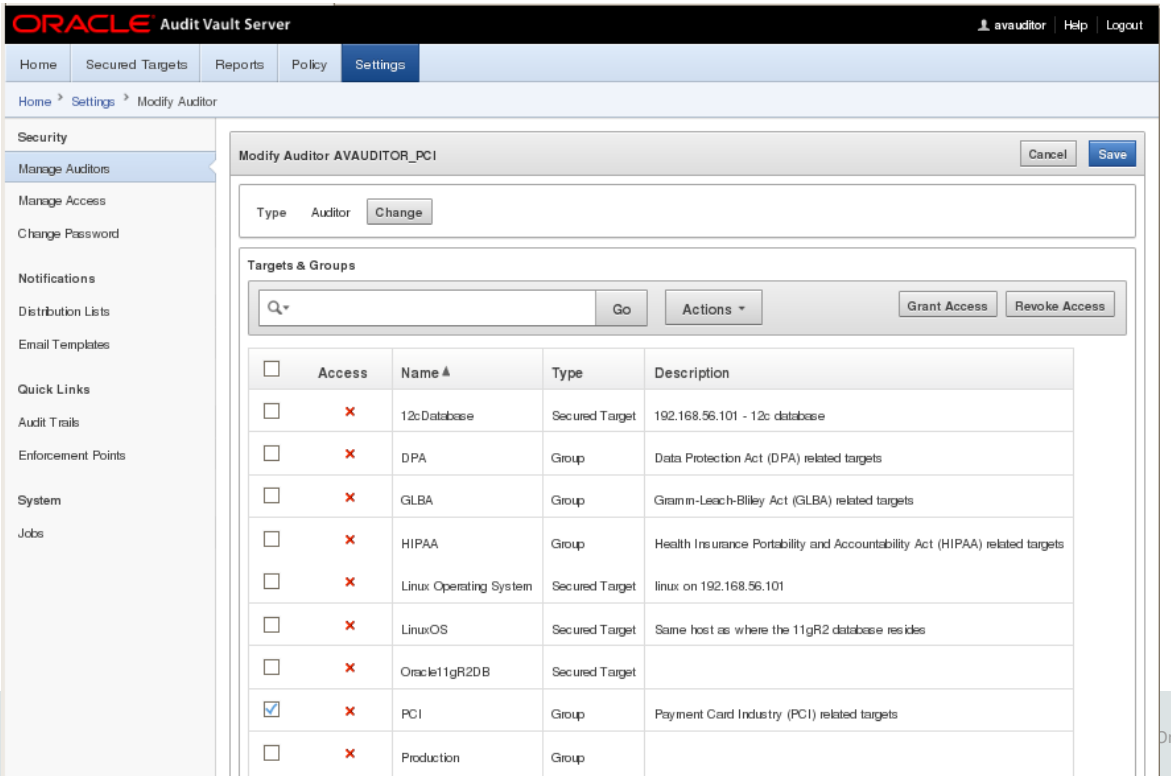
Create a New Auditor – AVAUDITOR_PCI

- Log in as super auditor : AVAUDITOR
- Settings > Manage Auditors > Create



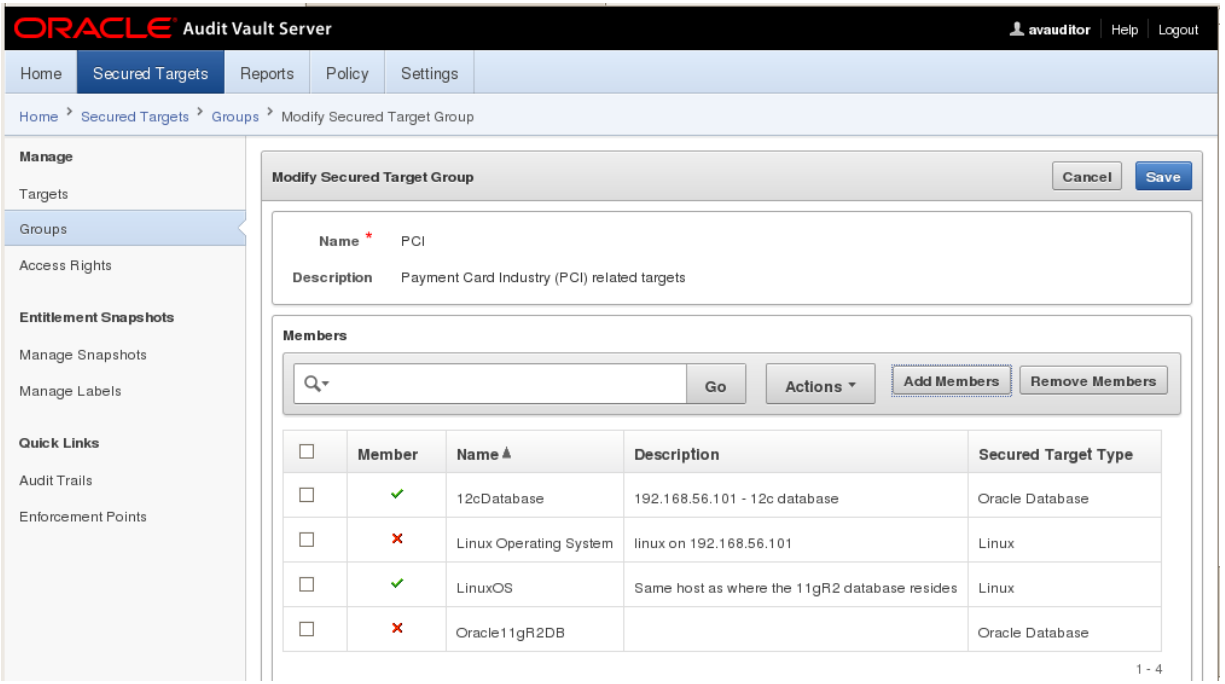
Create a New Auditor – AVAUDITOR_PCI

- After the auditor is created, go back to Manage Auditors page and click on the newly created auditor account
- Select PCI and then click **Grant Access** and then **Save**



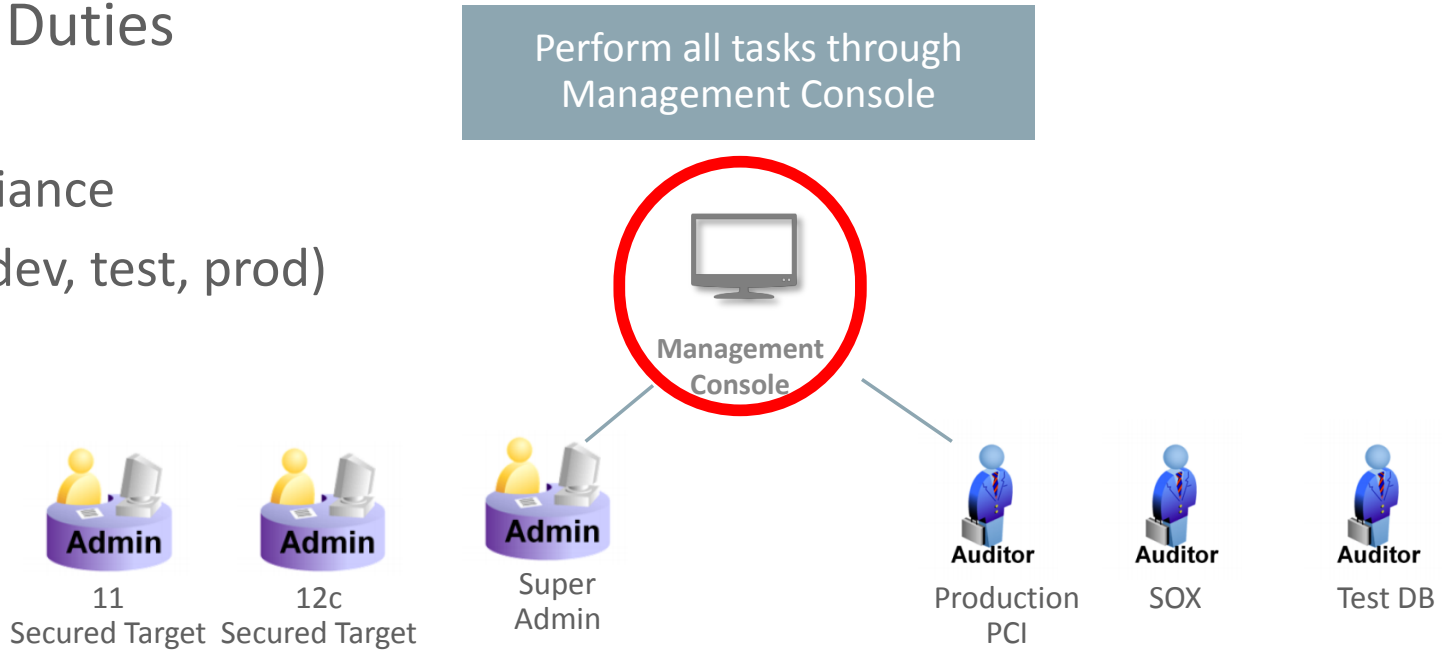
Assign Secured Target Member to PCI Group

- Secured Target > Group > PCI
- Select 12c database + Linux OS
- **Add Members + Save**
- Go back to PCI page and make sure 2 members are added

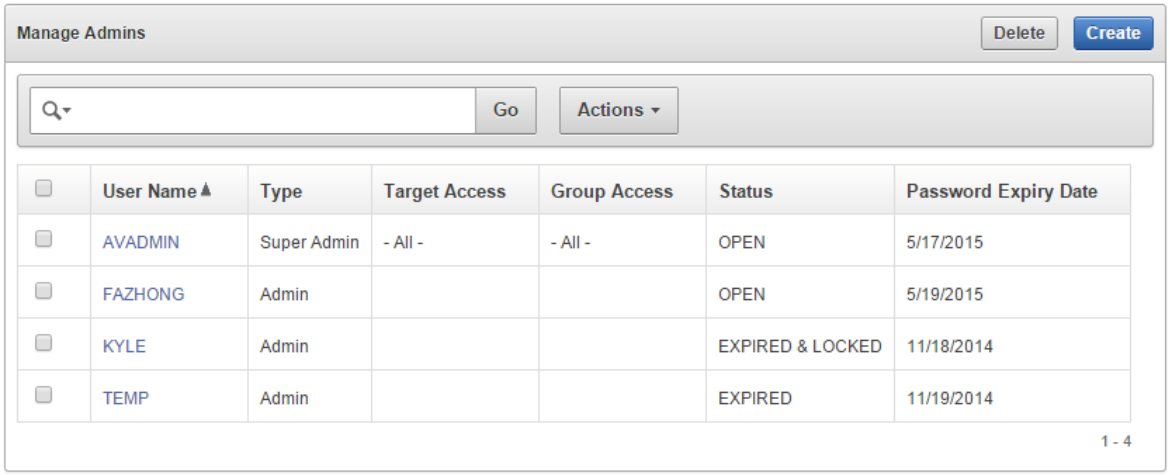


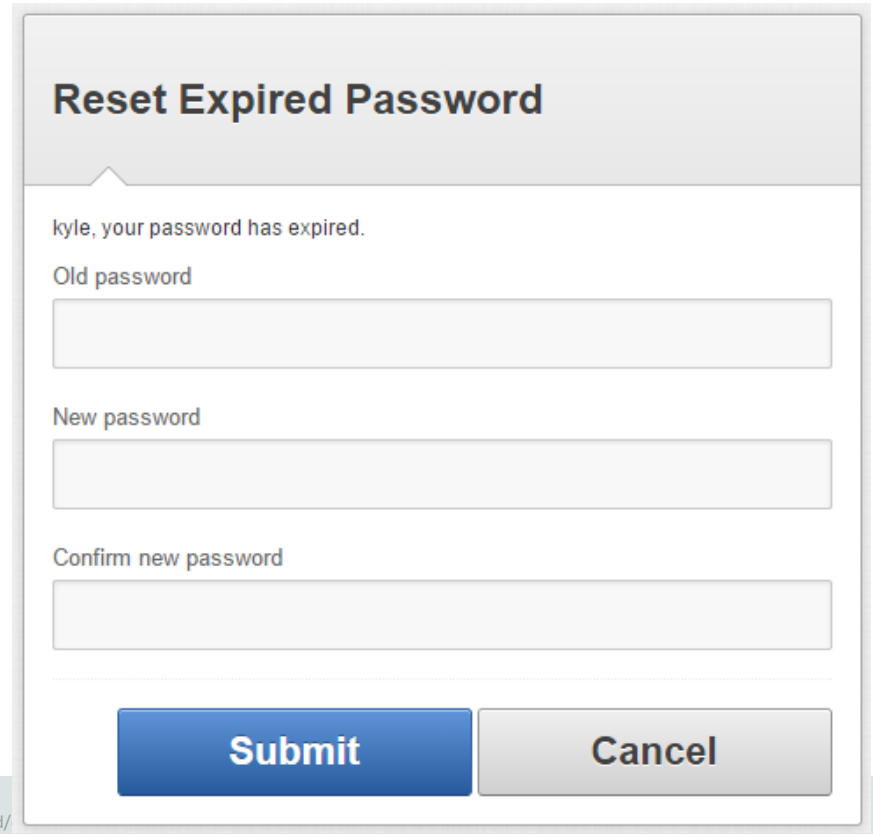
Best Practices for Accounts

- Always create new auditor accounts and use default account as backup
- Segregate Duties
  - By Target
  - By Compliance
  - By Type (dev, test, prod)



Some Accounts UI Improvements



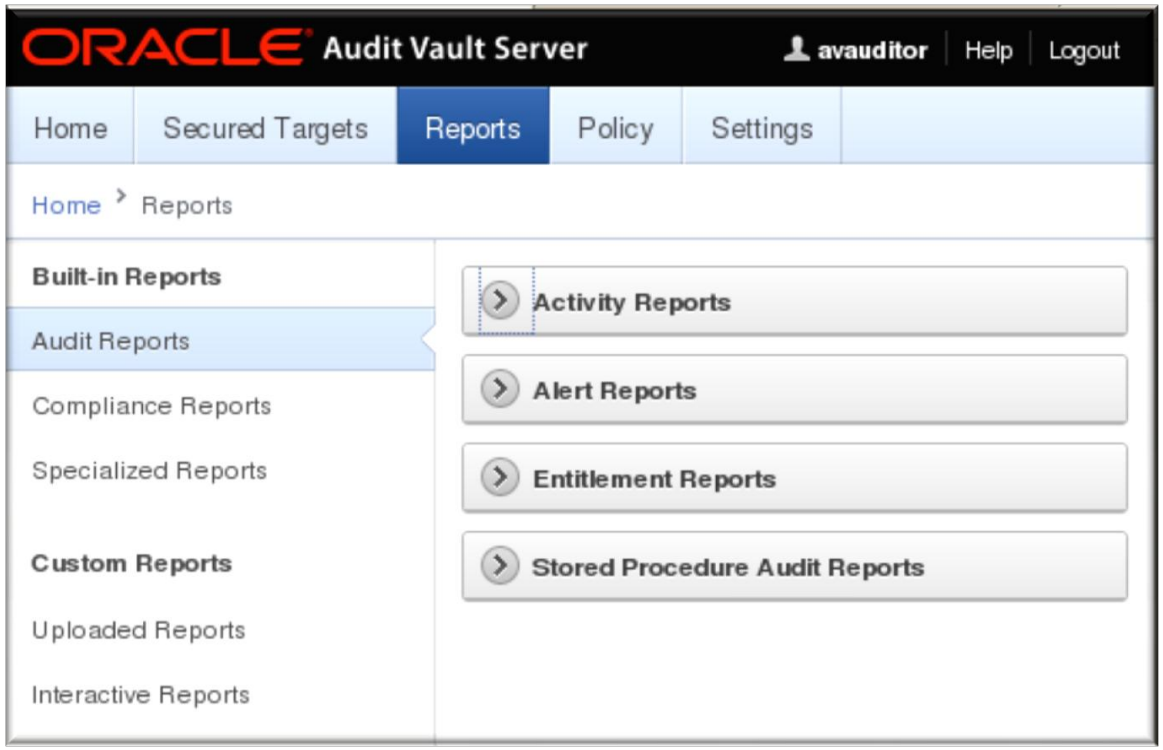


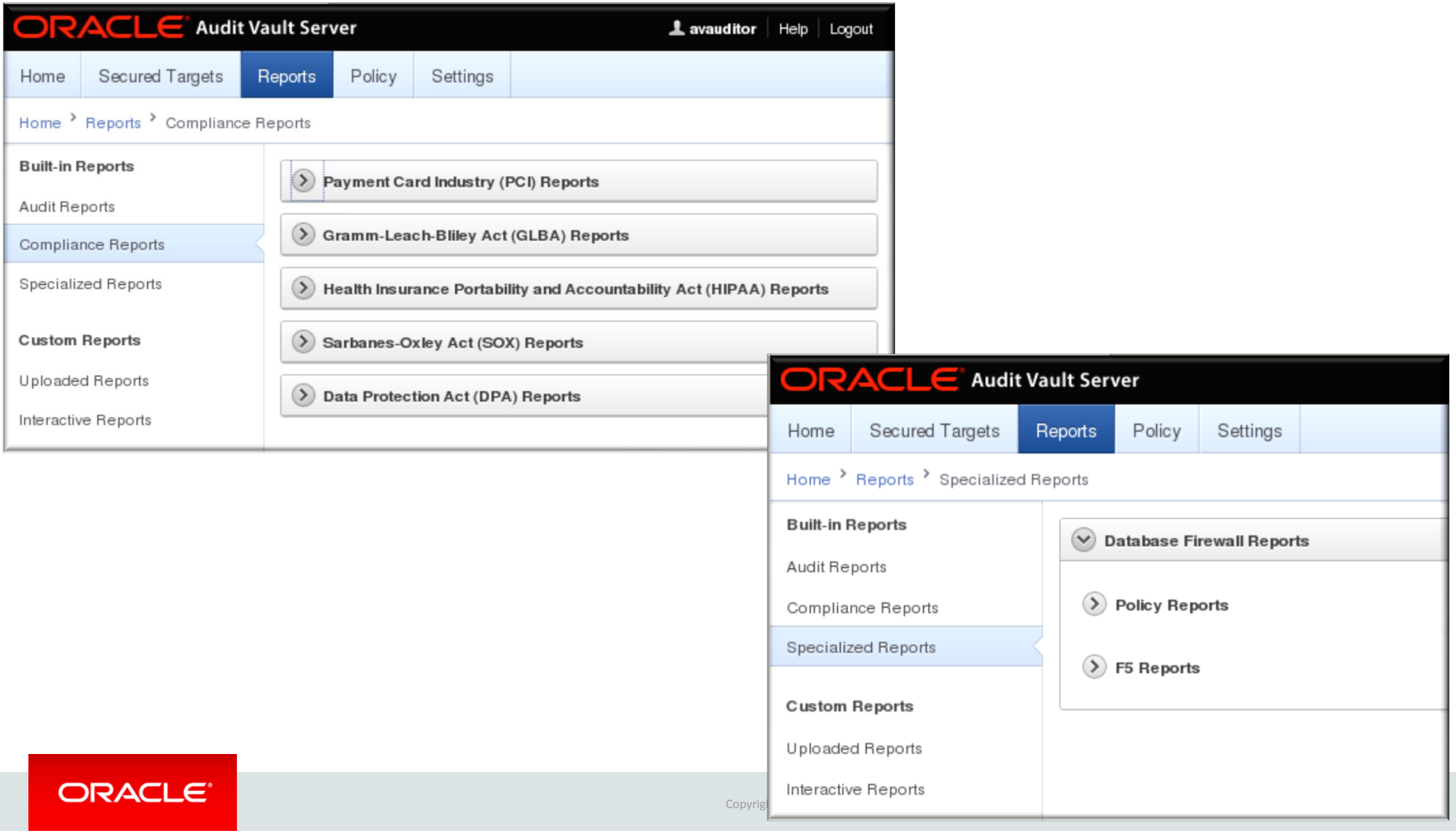
Lesson 7

All About Reports

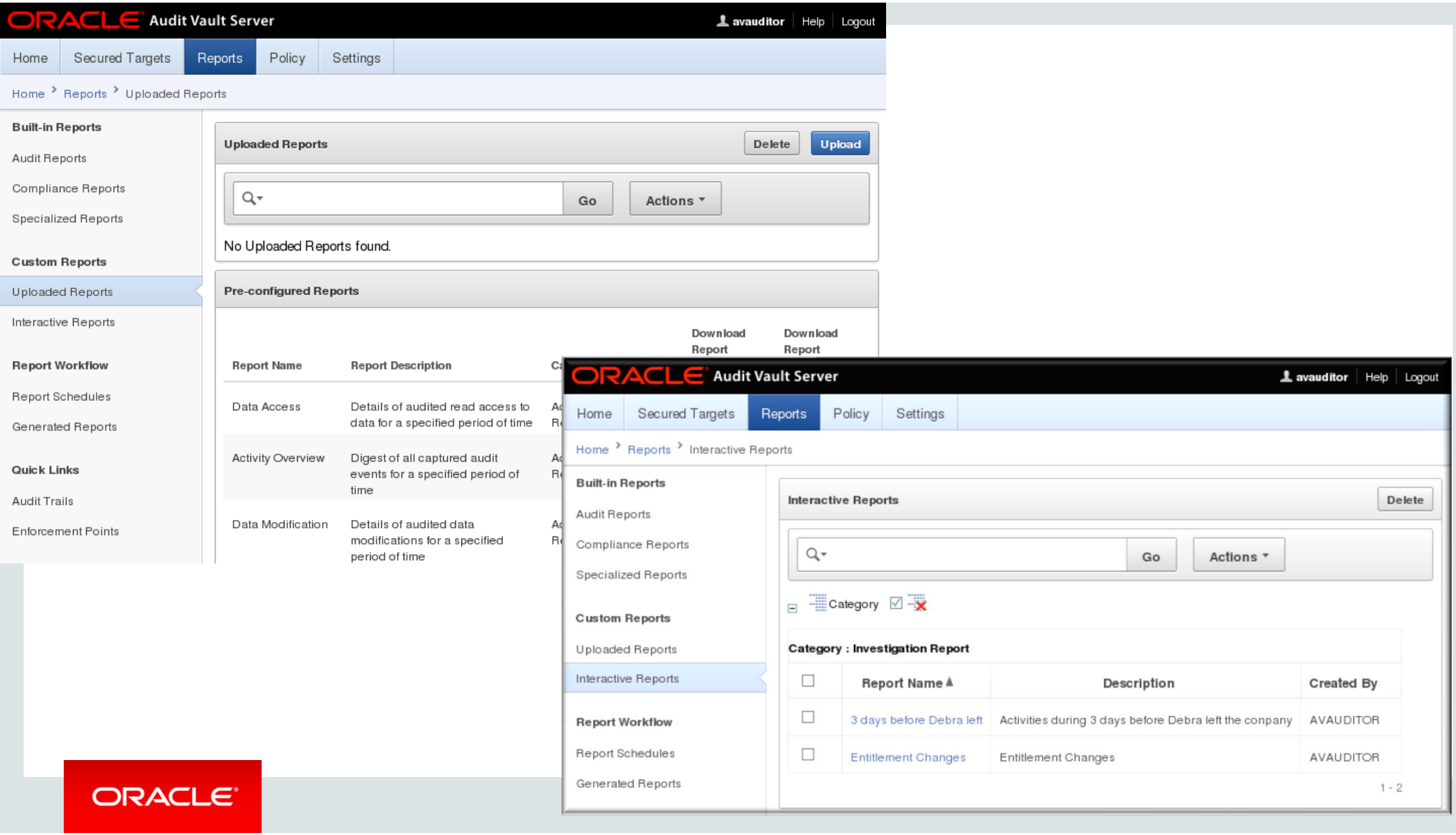
Browsing Reports

- **Built-in** (shipped out of box)
  - Audit reports
  - Compliance Reports
  - Specialized Reports
- **Custom** (User-defined)
  - Uploaded Reports
  - Interactive Reports

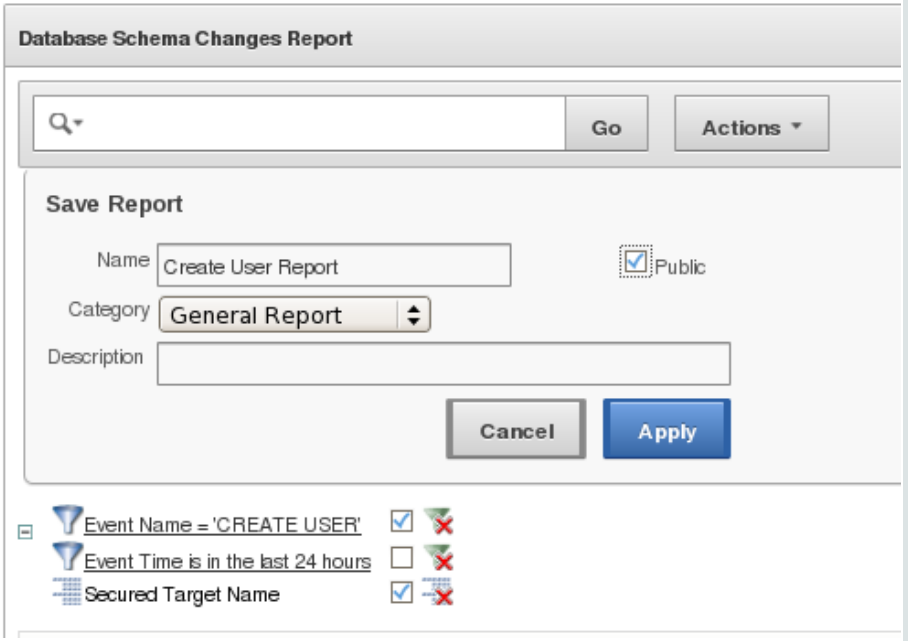




ORACLE


ORACLE Audit Vault Server
avauditor | Help | Logout
Home | Secured Targets | Reports | Policy | Settings
Home › Reports › Uploaded Reports
Built-in Reports
Audit Reports
Compliance Reports
Specialized Reports
Custom Reports
Uploaded Reports
Interactive Reports
Report Workflow
Report Schedules
Generated Reports
Quick Links
Audit Trails
Enforcement Points
Uploaded Reports
Delete
Upload
Go
Actions
No Uploaded Reports found.
Pre-configured Reports
Report Name
Report Description
Download Report
Download Report
Data Access
Details of audited read access to data for a specified period of time
Activity Overview
Digest of all captured audit events for a specified period of time
Data Modification
Details of audited data modifications for a specified period of time
ORACLE Audit Vault Server
avauditor | Help | Logout
Home | Secured Targets | Reports | Policy | Settings
Home › Reports › Interactive Reports
Built-in Reports
Audit Reports
Compliance Reports
Specialized Reports
Custom Reports
Uploaded Reports
Interactive Reports
Report Workflow
Report Schedules
Generated Reports
Interactive Reports
Delete
Go
Actions
Category
Category : Investigation Report
Report Name
Description
Created By
3 days before Debra left
Activities during 3 days before Debra left the conpany
AVAUDITOR
Entitlement Changes
Entitlement Changes
AVAUDITOR
1 - 2

View/Download/Save Reports

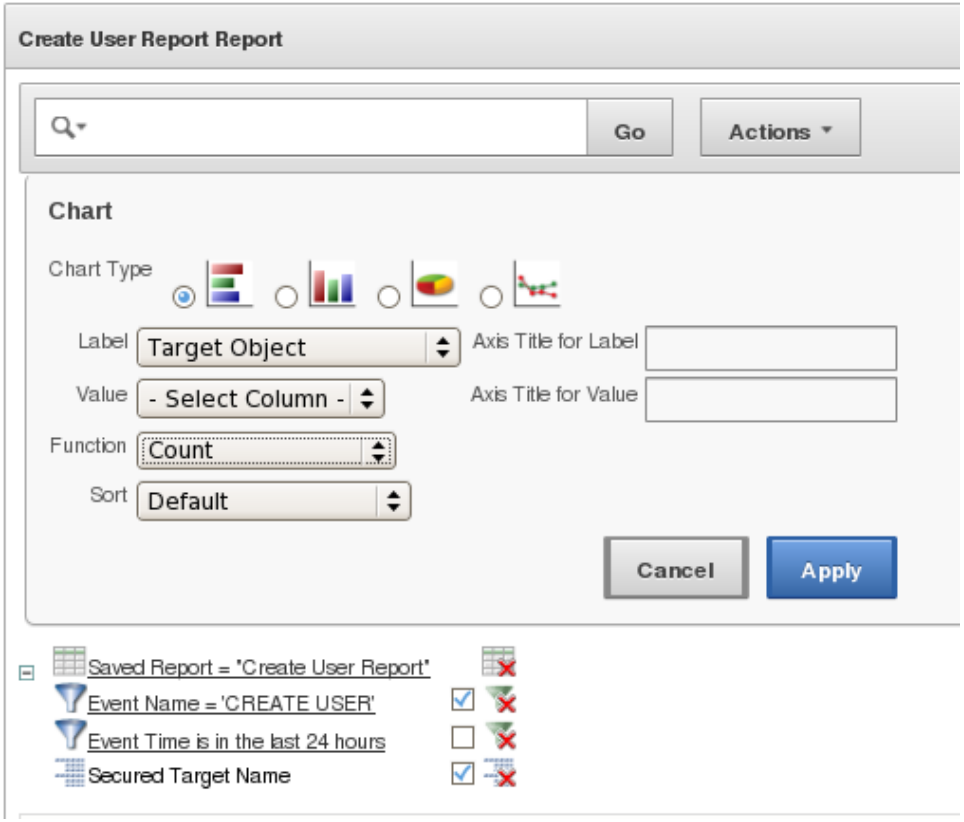


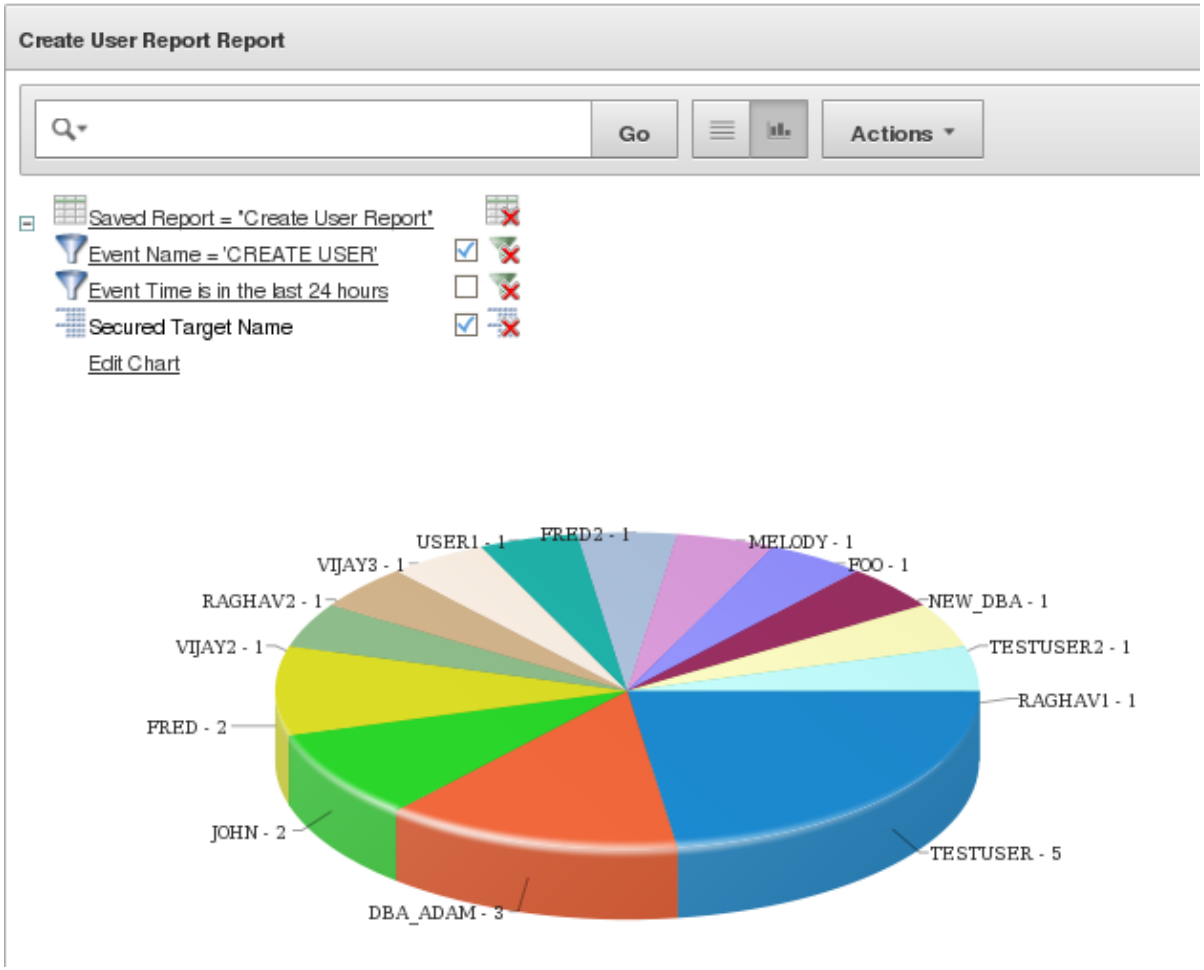
- Reports > Audit Reports
- Click  on *Database Schema Changes Report*
- Uncheck “Last 24 hours” filter
- Actions > **Select Columns** > Apply
  - Add Error Code
- Click on Event Name column and select “**Create User**”
- Actions > **Download** > HTML and save or open the file to view
- Actions > **Save Report** > {Give it a name} > Apply
- Go to Interactive Reports and you will see the newly created report

Note : can not schedule interactive reports

View Graphical Reports

- Select the newly created report
- Actions > Format > Chart
- Select Pie Chart Type
- Select "**Target Object**" in Label and
- "**Count**" in Function.
- Apply





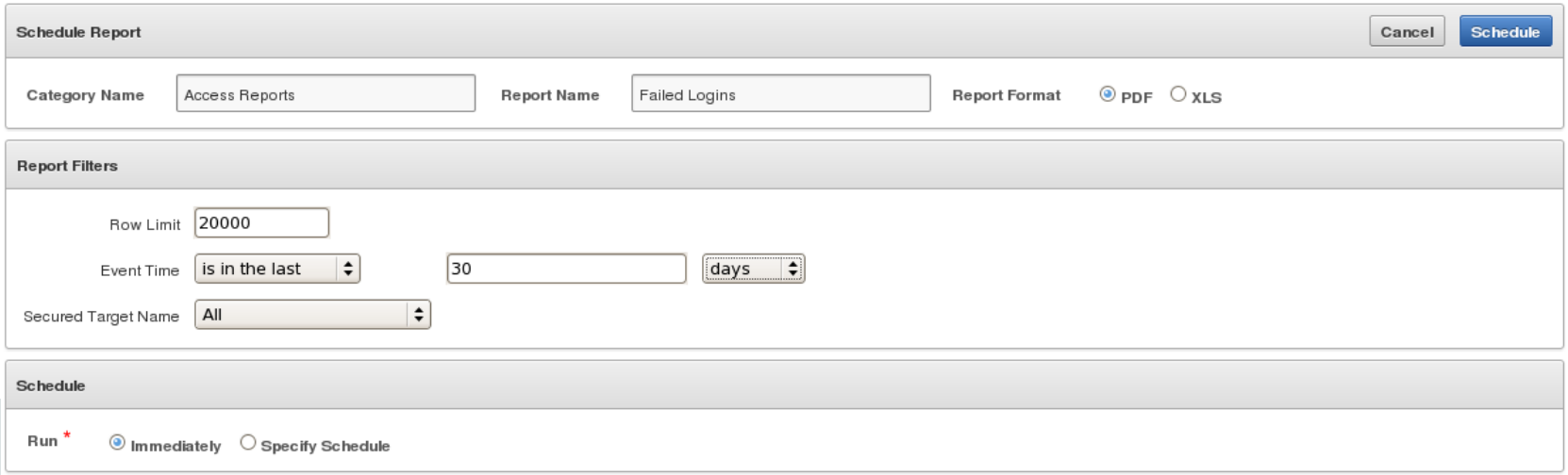
Create New Events to be Shown on your report

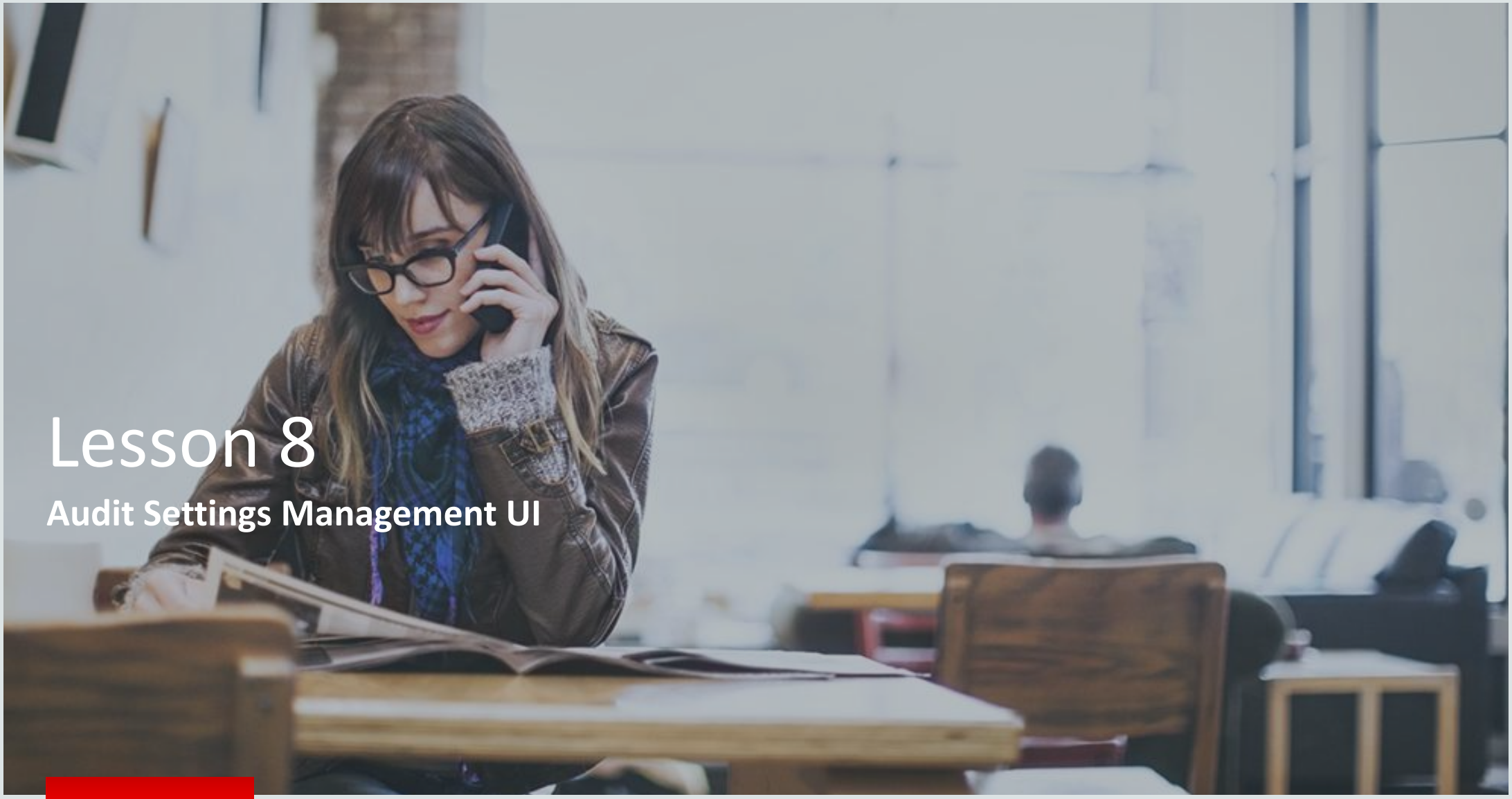
- Sqlplus DBA_DEBRA / Manager_1
- SQL> Select * from hr.jobs where job_id=1;
- You should see the event in Activity Overview Report

[*Did you set up audit setting to capture audit data ?]*

Schedule Report

- Select *Failed Login* Report
- Click the schedule icon
- Change Event Time to “last 30 days”
- Schedule
- You will be brought to Generated Reports
  - You won’t see the report immediately; instead, click “Show Pending Reports” button
  - The report will eventually show up in the queue





Lesson 8

Audit Settings Management UI

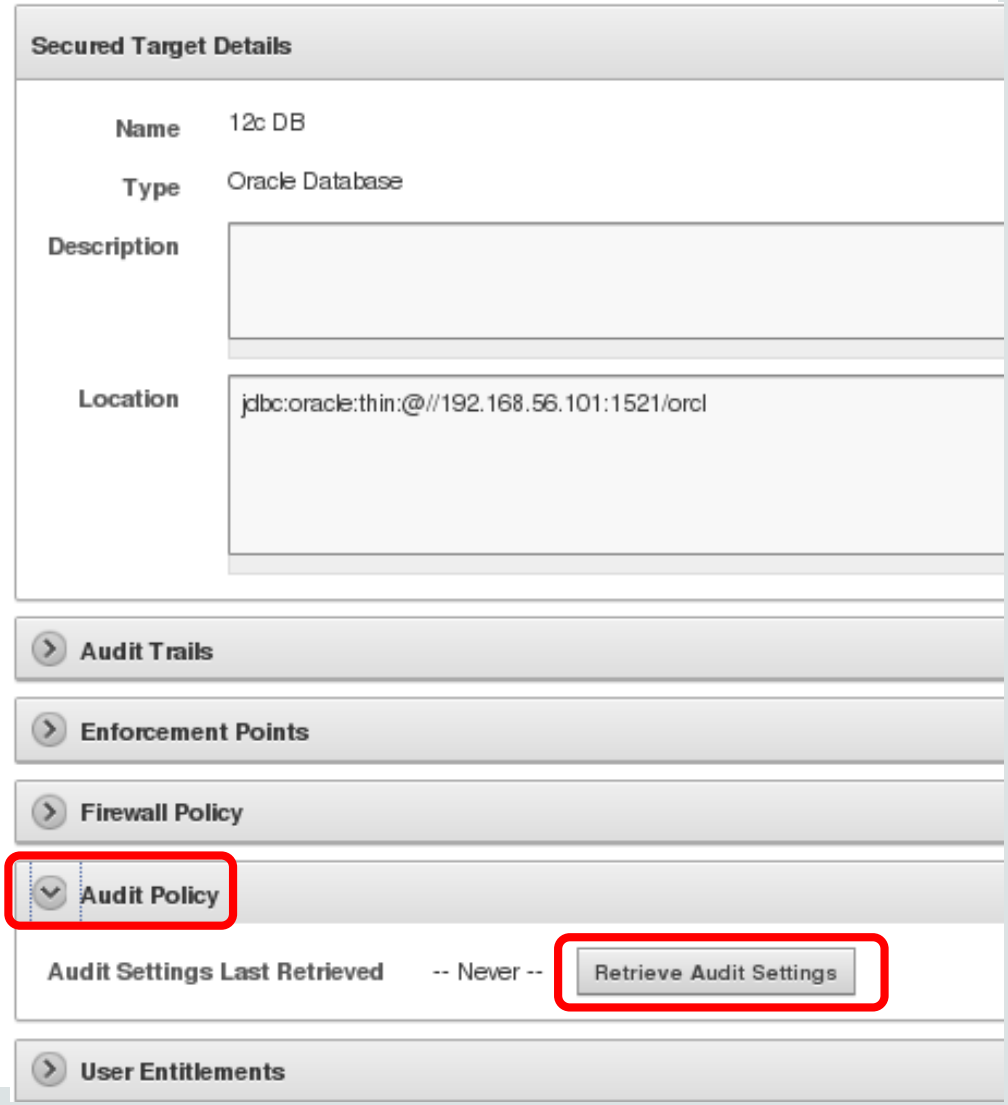
Audit Settings Management (UI for 11g, 12c traditional)

1. **Retrieve** and Review Current Audit Settings
2. **Create**/Update Audit Settings
3. **Provision** Desired New Auditing Settings
   - Or **Export** the settings to a text file and then execute on the target
4. If “Trouble” – sync up “In Use” and “Needed”

Step 1: Retrieve Audit Settings

Secured Targets > 12cDB > Audit Policy > Retrieve Audit Settings

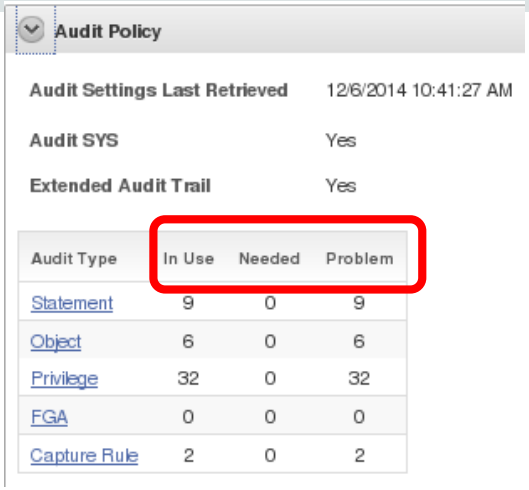
Check status :
Settings > Jobs

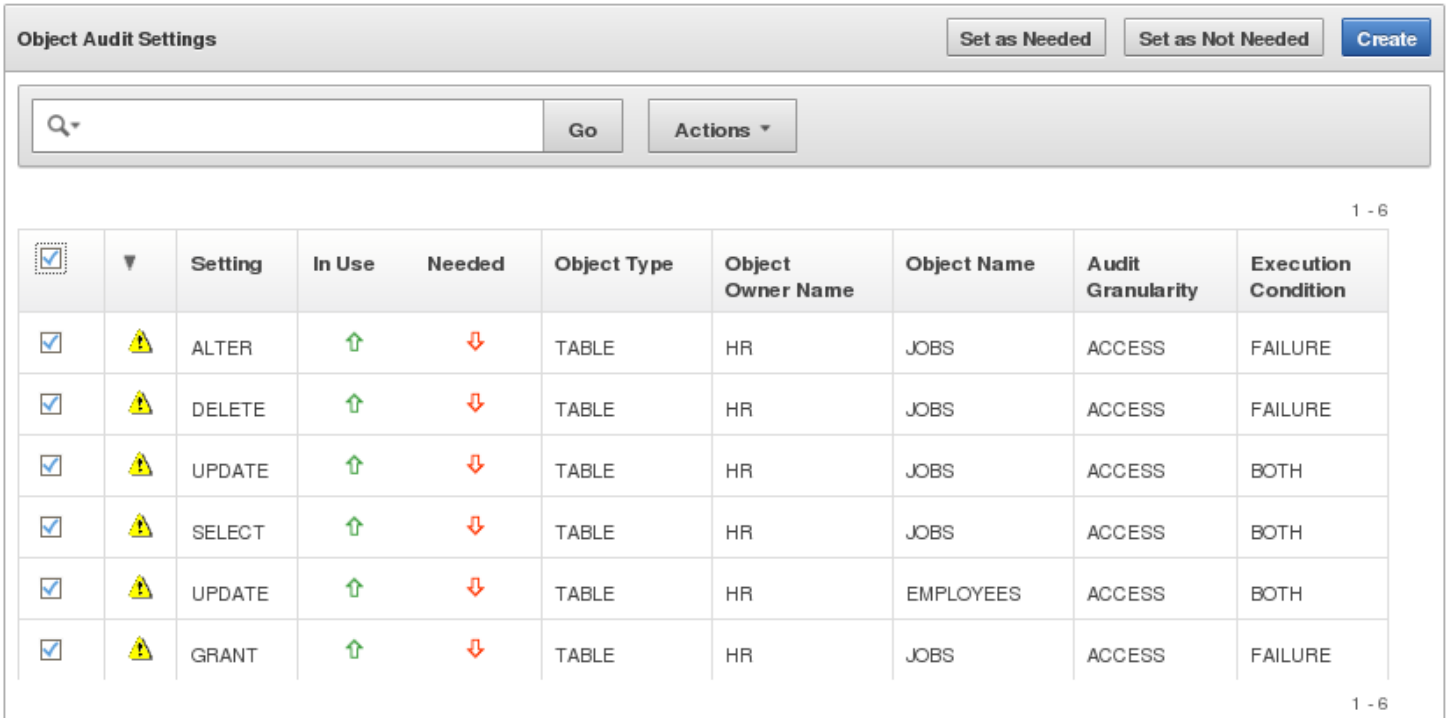


Step 1: Review

* When Job Completes, Policy > Audit Policy > 12c DB and you will see 0 Needed

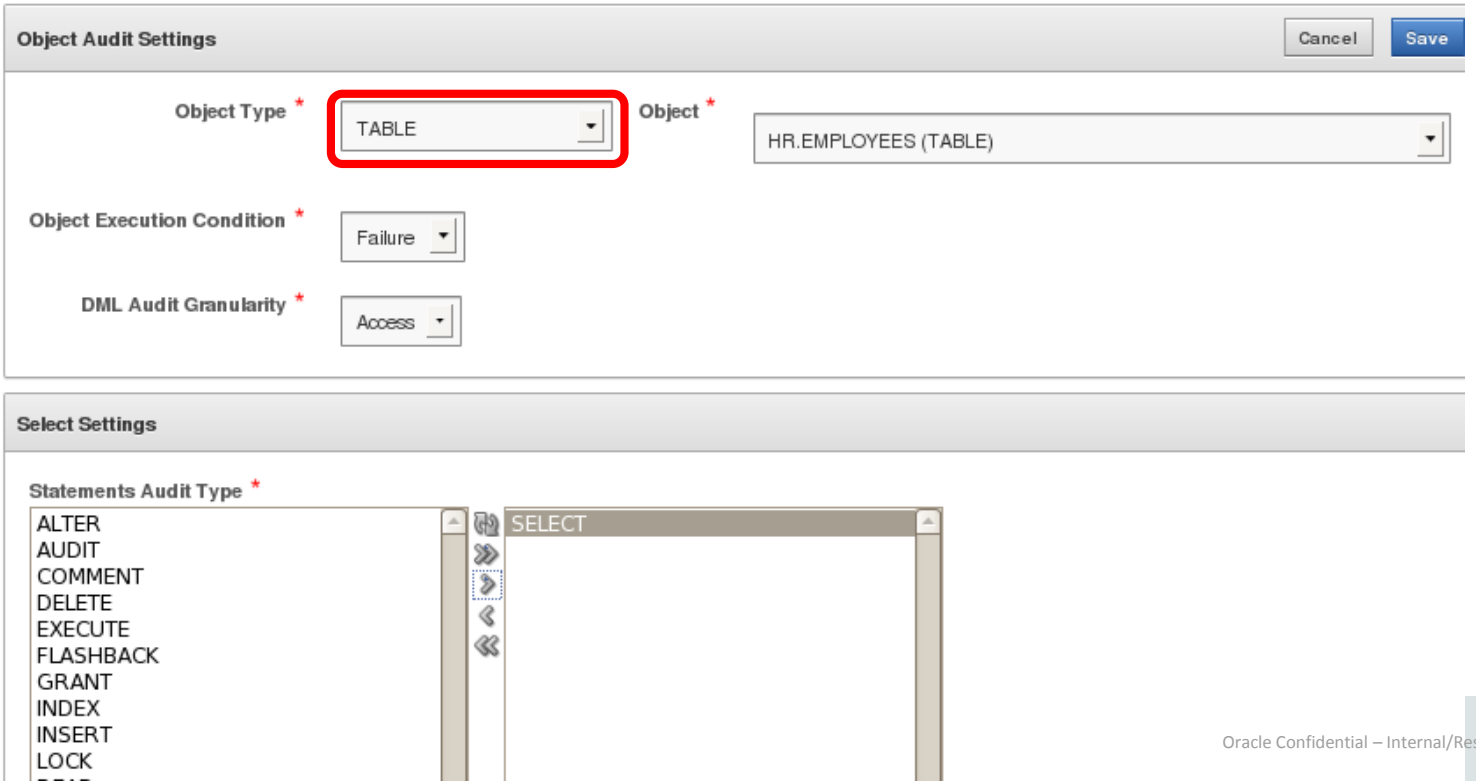
* Select **Object** and “Set as Needed”





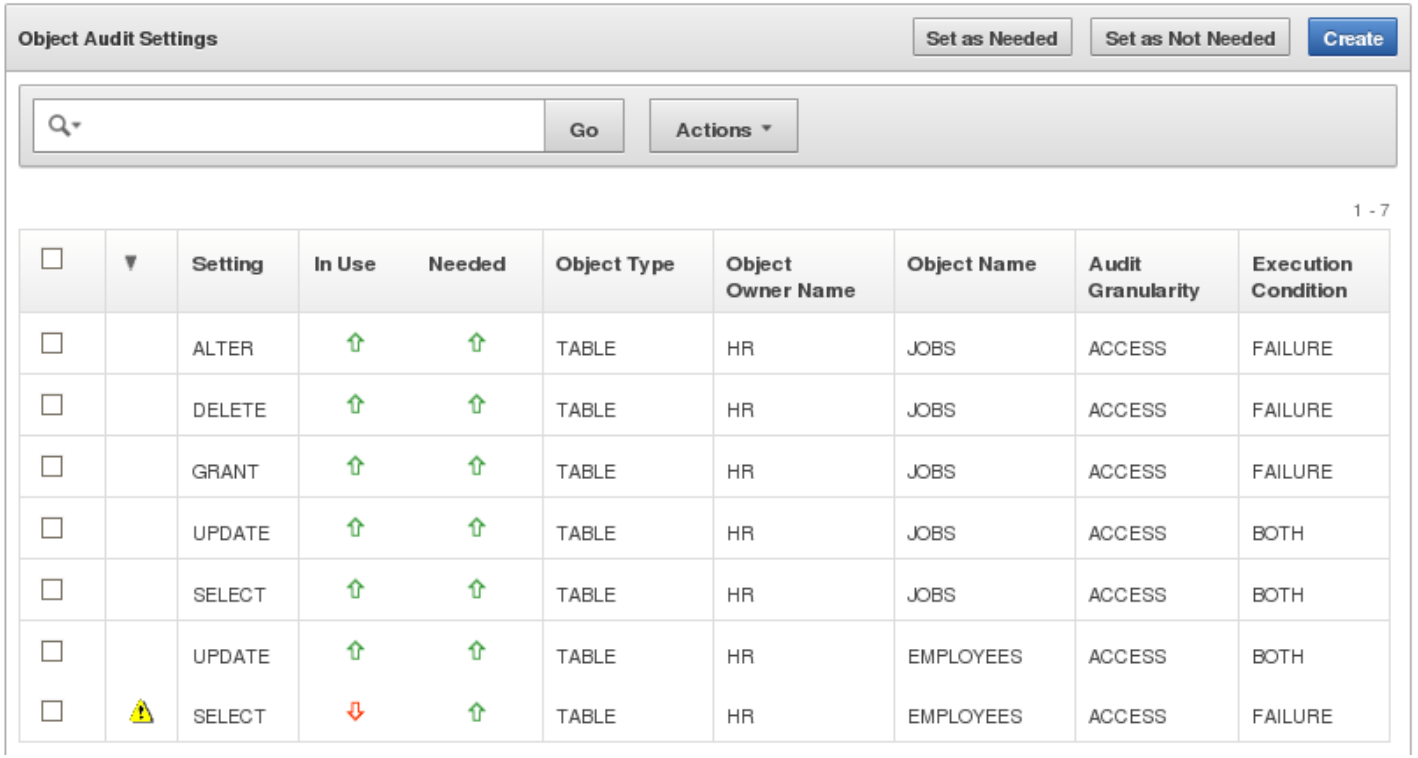
Step 2 : Create new settings

While in Object Audit Settings, select “Create”
[Add Select **HR.EMPLOYEES** when Failure]



Step 2 : Create New Settings

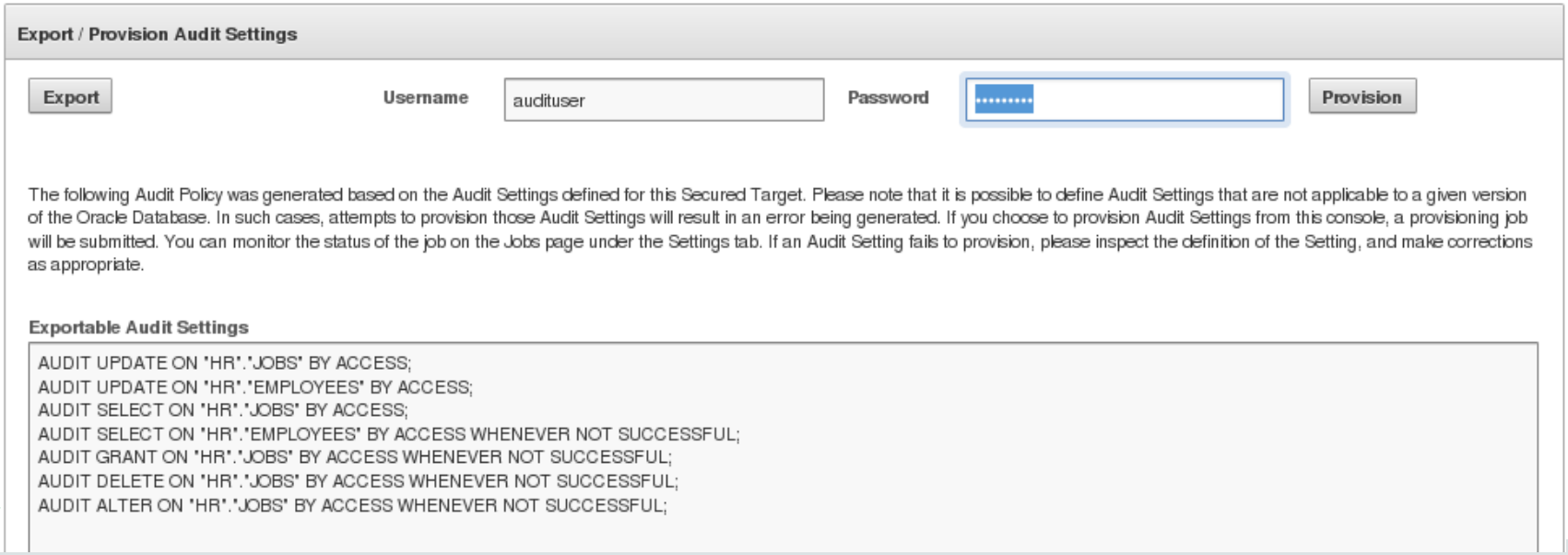
* You will see it's in Needed + Not In Use state

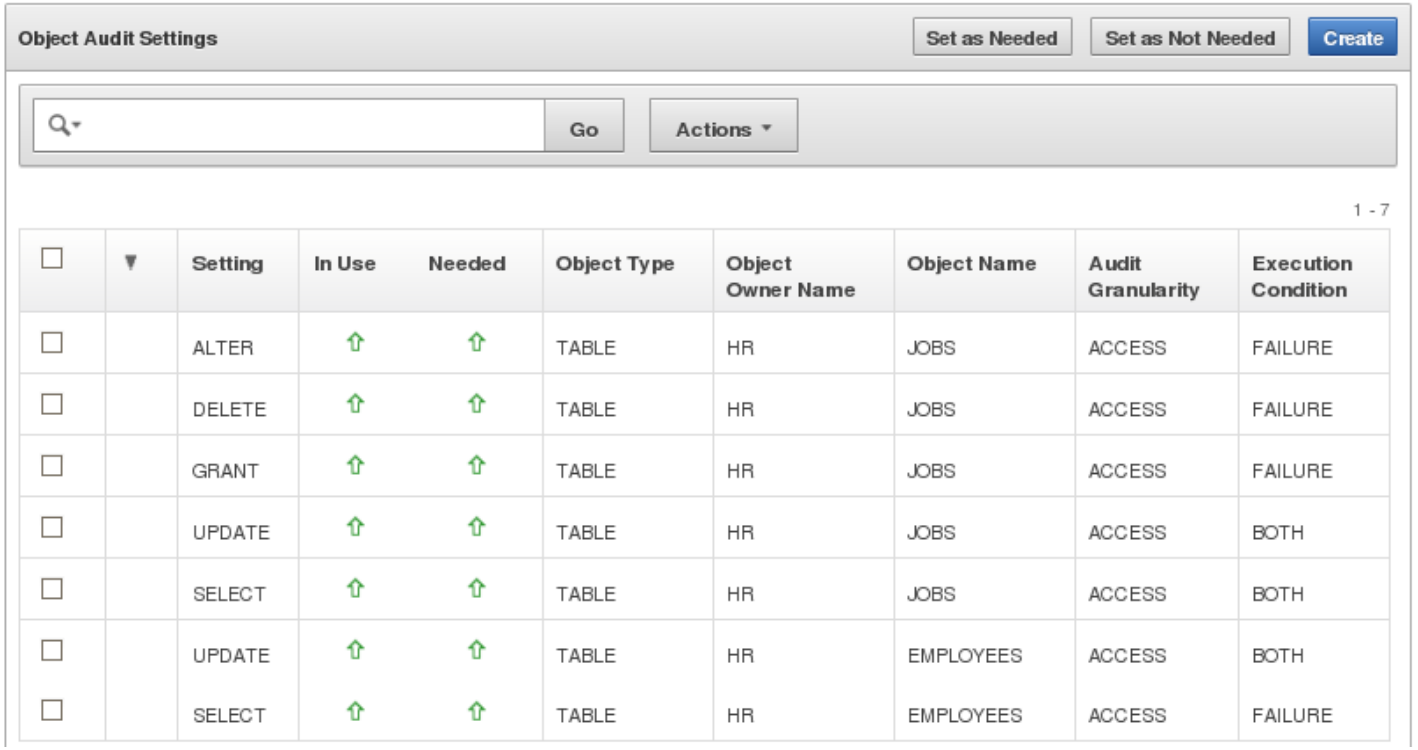


		Setting	In Use	Needed	Object Type	Object Owner Name	Object Name	Audit Granularity	Execution Condition
☐		ALTER	⇧	⇧	TABLE	HR	JOBS	ACCESS	FAILURE
☐		DELETE	⇧	⇧	TABLE	HR	JOBS	ACCESS	FAILURE
☐		GRANT	⇧	⇧	TABLE	HR	JOBS	ACCESS	FAILURE
☐		UPDATE	⇧	⇧	TABLE	HR	JOBS	ACCESS	BOTH
☐		SELECT	⇧	⇧	TABLE	HR	JOBS	ACCESS	BOTH
☐		UPDATE	⇧	⇧	TABLE	HR	EMPLOYEES	ACCESS	BOTH
☐	⚠	SELECT	⇩	⇧	TABLE	HR	EMPLOYEES	ACCESS	FAILURE

Step 3 : Export or Provision

* Go back to Audit Settings Overview, select Object and ‘Export/Provision’
* Choose Provision to execute or Export the SQL statements into a file
  [You can examine the SQL statements on screen]
* Settings > Jobs for status





When done, do the same for all other settings

Problems? No Problem ☺

In Use	Needed
	
	
	
	

Lesson 9

Data Modification Before-After Value Report

Data Modification Before-After Values Report

Audited Data showing Before and After Values

- REDO Collector captures before-after values using Oracle Streams which is available on Enterprise Edition databases only
- Audit data come from TRANSACTION LOG audit trail
- Let’s set up this audit trail

Critical Prep Work

Database Streams

- SQL> shutdown immediate
- SQL> startup mount
- SQL> **alter database archivelog;**
- SQL> alter system set global_names=true;
- SQL>alter database RENAME GLOBAL_NAME TO ORCL.us.oracle.com;
- SQL> alter database open;
- SQL> show parameter global;
- SQL> archive log list

```
SQL> archive log list
Database log mode              No Archive Mode
Automatic archival             Disabled
Archive destination            USE_DB_RECOVERY_FILE_DEST
Oldest online log sequence     21
Current log sequence           23
SQL> shutdown immediate
;
Database closed.
Database dismounted.
ORACLE instance shut down.
SQL> SP2-0223: No lines in SQL buffer.
SQL> startup mount
ORACLE instance started.

Total System Global Area  838860800 bytes
Fixed Size                  2929936 bytes
Variable Size             570428144 bytes
Database Buffers          260046848 bytes
Redo Buffers                5455872 bytes
alter database archivelogDatabase mounted.
SQL> ;

Database altered.

SQL> archive log list
Database log mode              Archive Mode
Automatic archival             Enabled
Archive destination            USE_DB_RECOVERY_FILE_DEST
Oldest online log sequence     21
Next log sequence to archive   23
Current log sequence           23
SQL> alter database open;

Database altered.
```

AVDF Setup

- Add Audit Trail

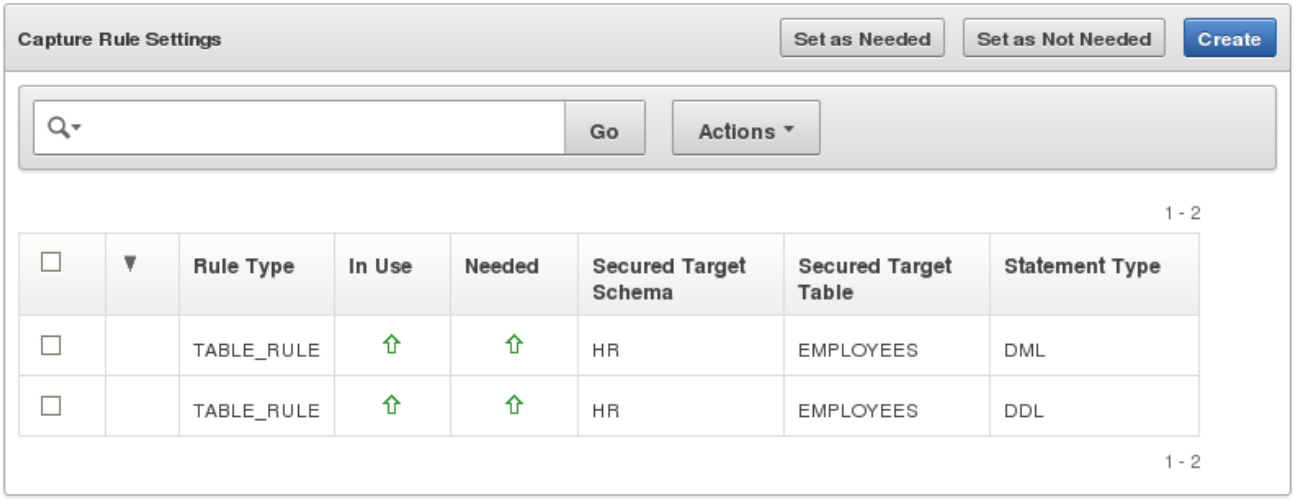
  As AVADMIN

- Create Capture Rule

  As AVAUDITOR

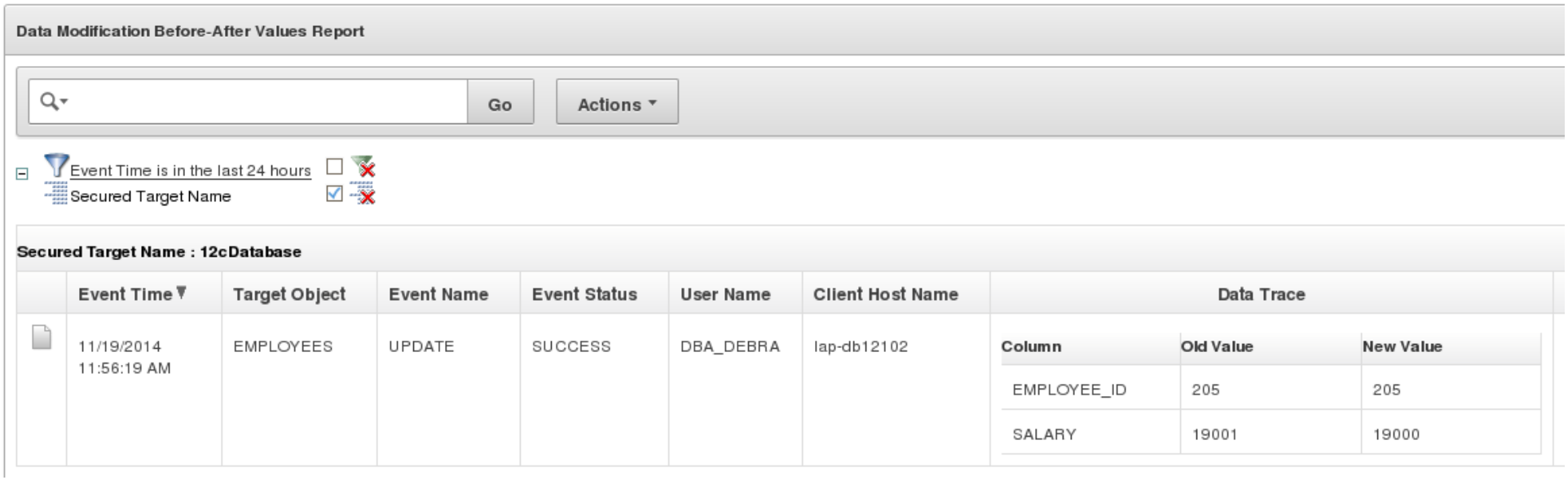
  - Audit Policy > Capture Rule

[this is done for you]



Generate Before-After Value Report

SQL>UPDATE HR.EMPLOYEES set salary=1900**0** where last_name='Higgins';



Data Modification Before-After Values Report

Go | Actions

Event Time is in the last 24 hours
Secured Target Name

Secured Target Name : 12cDatabase

Event Time	Target Object	Event Name	Event Status	User Name	Client Host Name	Data Trace
11/19/2014 11:56:19 AM	EMPLOYEES	UPDATE	SUCCESS	DBA_DEBRA	lap-db12102	

Column	Old Value	New Value
EMPLOYEE_ID	205	205
SALARY	19001	19000

Lesson 10

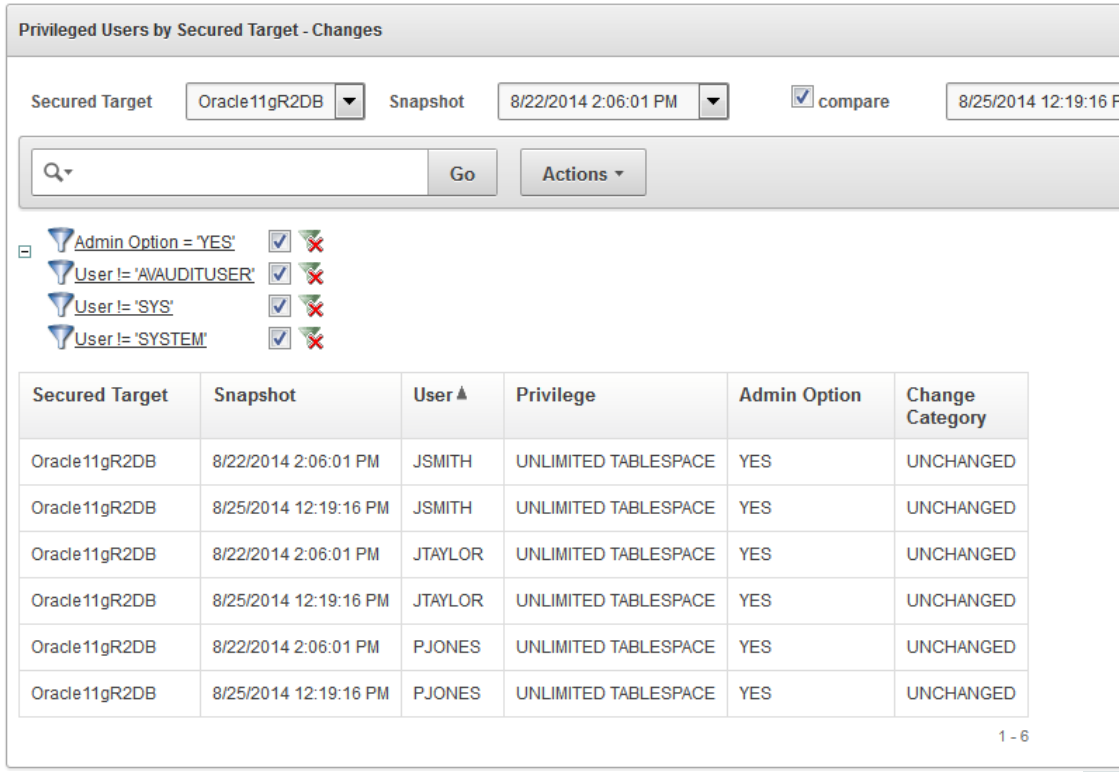
Entitlement Report

Create An Entitlement Report

- Home > Secured Target > select “12cDB“
  - Scroll down and expand “User Entitlement” > click Retrieve User Entitlement Data
  - [After job completes] you should see the Last Retrieved changed to current (You just took a snapshot at TimeA)
- Log in as DBA_NICOLE
- Create 2 DB users : 1 regular user named JOHN, 1 dba user named DBA_ADAM
- Grant dba role to both (note this is out of company policy to grant regular user dba role)
- Take another snap shot (TimeB) by repeating the first 2 steps above
- Browse “User Account By Secured Target” Entitle Report
  - Select TimeA and TimeB in drop-down menu and select Compare check box
  - Filter down change category as NEW
  - You will see the report is showing that what entitlements have changed

Create An Entitlement Report

- Select “Privileged Users by Secured Target (11gR2)”
- Create some filters to view DBA users other than sys, system, audituser
- Review account privileges



Lesson 11

Customize Reports

Pre-requisites

- *Word (to edit RFT file)*
- Text Editor (such as Notepad) to edit XML file
- Knowledge of AVSYS schema structure
- (optional) Knowledge of BI Publisher
  - BI Publisher Desktop – 600MB to download
  - Or BI Publisher add-in for Word – 237 MB to download
  - Oracle Database PL/SQL Package DBMS_XMLGEN

Customize Report

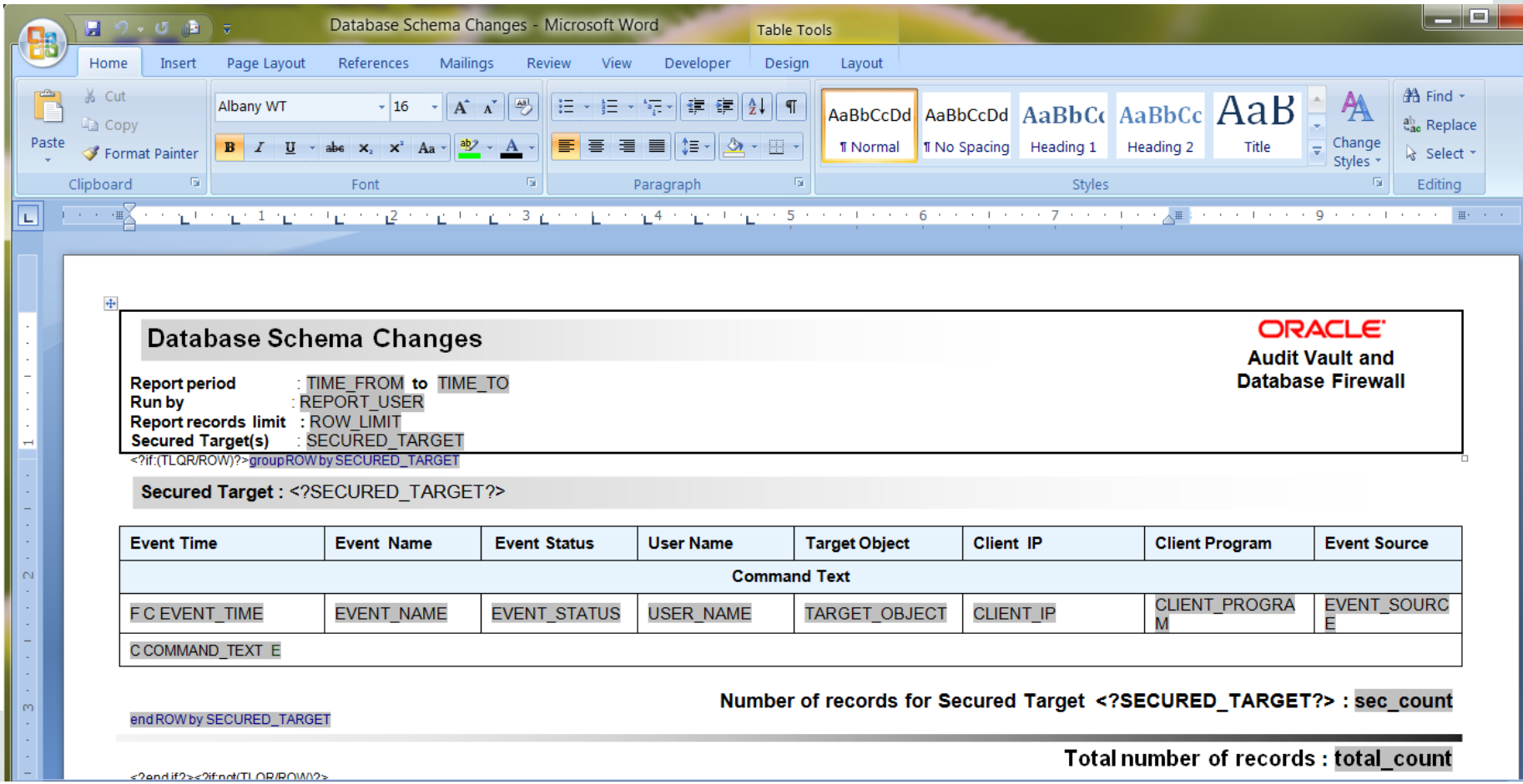
Step 1 : Download **both** RTF and XML files to your desktop

Pre-configured Reports

Report Name	Report Description	Category	Schedule	Download Report Template	Download Report Definition
Data Access	Details of audited read access to data for a specified period of time	Access Reports			
Activity Overview	Digest of all captured audit events for a specified period of time	Access Reports			
Data Modification	Details of audited data modifications for a specified period of time	Access Reports			
Data Modification Before-After Values	Details of audited data modifications for a specified period of time showing before and after values	Access Reports			
Database Schema Changes	Details of audited DDL activity for a specified period of time	Access Reports			
All Activity	Details of all captured audit events for a specified period of time	Access Reports			
Failed Logins	Details of audited failed user logins for a specified period of time	Access Reports			

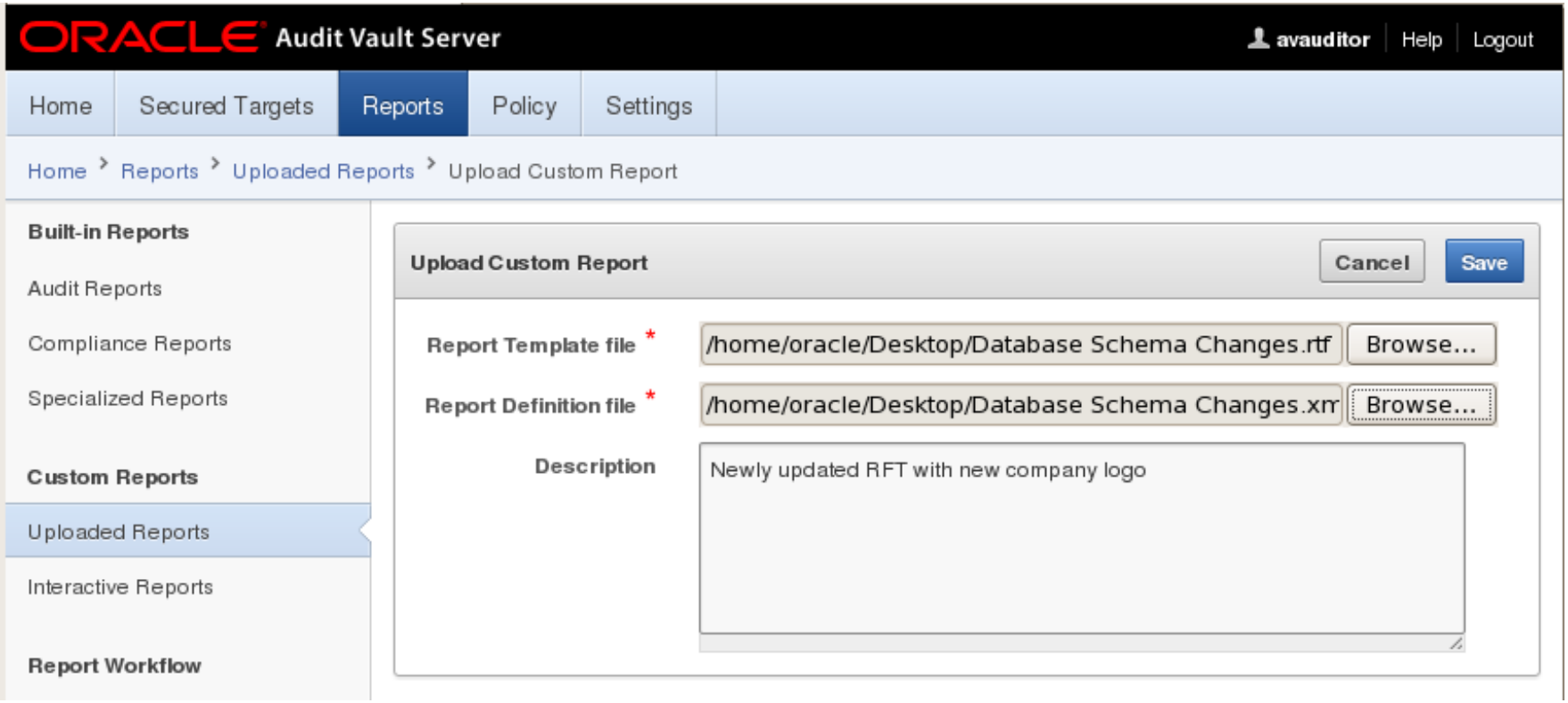
Customize Report

Step 2 : Modify RTF (report template)



Customize Report

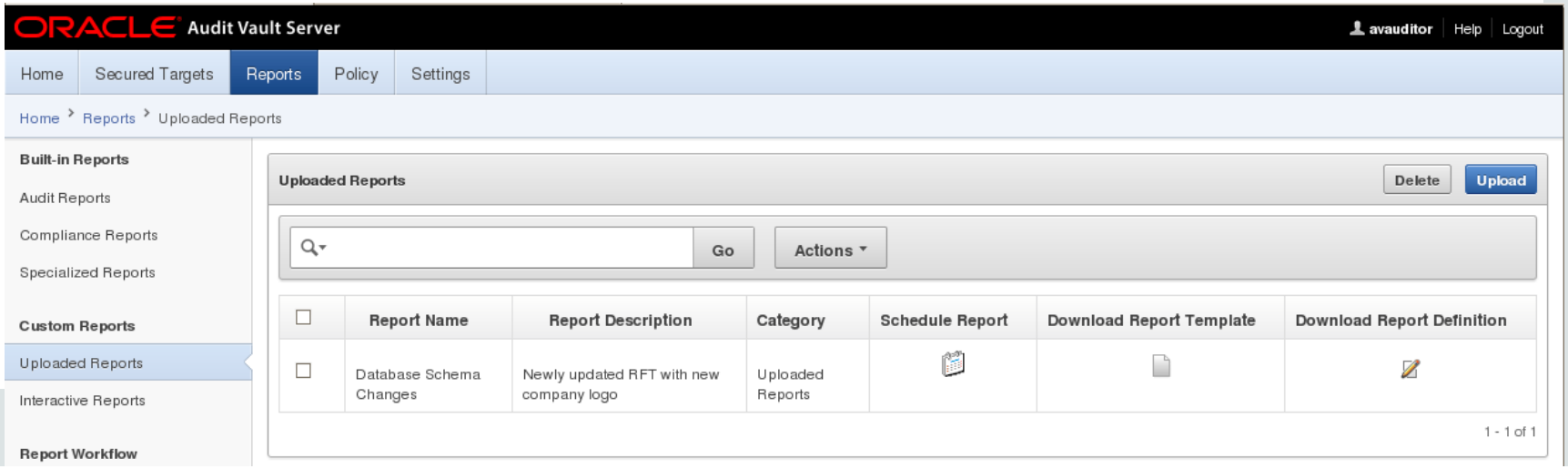
Step 3 : Upload BOTH RTF + XML

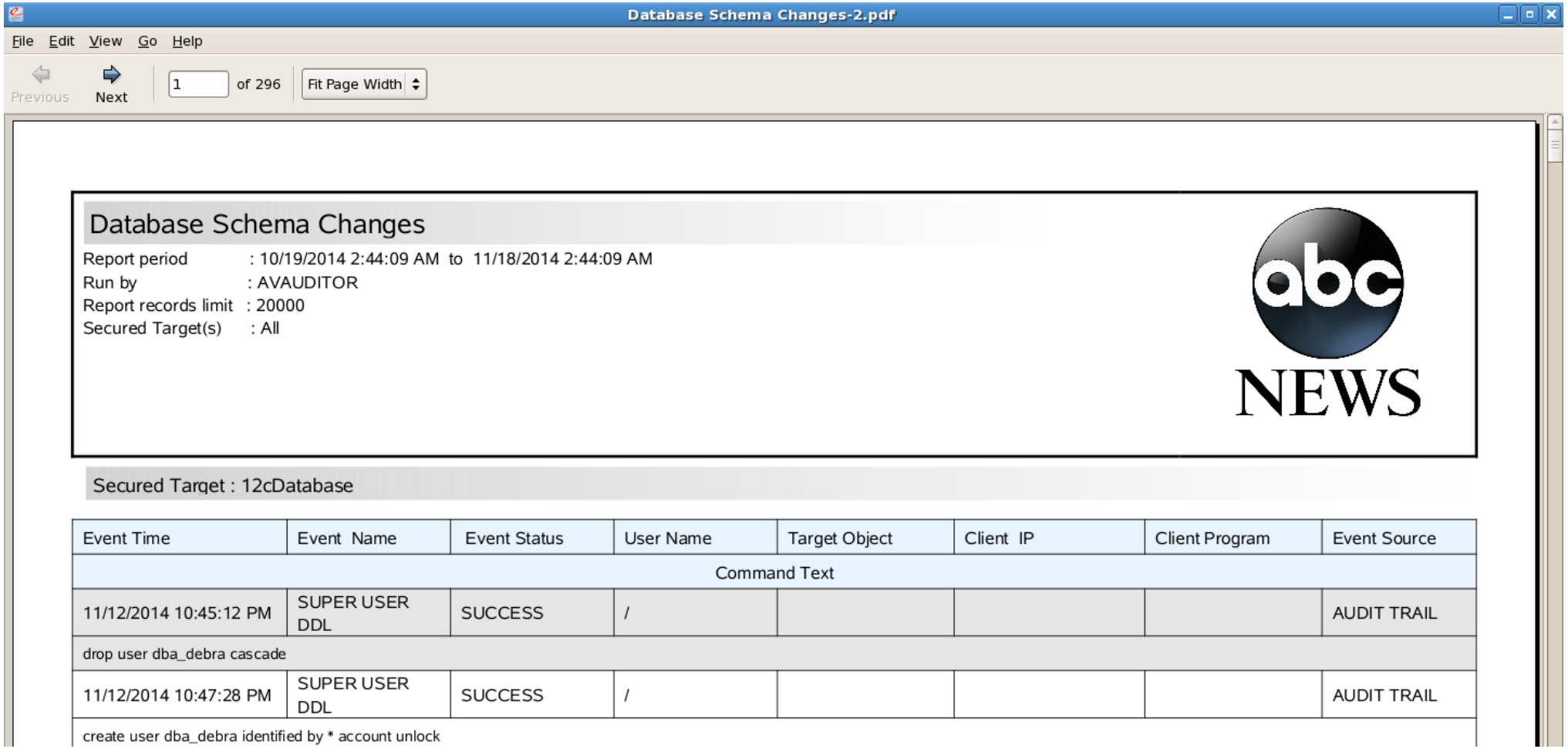


Customize Report

Step 4 : Testing results

- After the report is uploaded
- Schedule Report, immediate
- Reports > Generated Reports
- Click on Details
- “View Report”





Customize Report

Step 5 : Modify XML (report definition)

- .xml file contains SQL Query and structure of data set.
  - BI Publisher reporting engine runs the SQL query when generating the report and passes data to rendering engine.
  - Upload sample XML data file (containing sample test data) to test the report without connecting to AVS
- You can add columns directly into .xml file using BI Publisher tag.
  - For example, to add EVENT_STATUS column, use <?EVENT_STATUS?> tag
- http://docs.oracle.com/cd/E28280_01/bi.1111/e22254/create_rft_bldr.htm#BIPRD2621

Lesson 12

Investigate Suspicious Events

Scenario

Your company recently discovered that some of your customer's credit card information have been leaked and published publicly on the internet.
Security Officer has requested an immediate investigation.
There is strong reason to believe that some employee might have created a duplicate copy of the ORDERS table that contains customer credit card information.

This exercise is to investigate and prove that this indeed happened.
Can you find out who did it and how ?

- You can examine all available Build-in Reports such as All Activity Report and sort by Event_Time, by Event_Name, by TARGET_OBJECT and see if you can find relevant information. You may have to turn on/off certain filters to get the necessary data. You may also need to select more/less columns to display more/less data. **[Hint : DBA_DEBRA was let go on Aug 31, 2014]**

Answer :

- A custom report can be found as “10 Days Before Debra Left”. Around 12:18PM on Aug 22nd 2014, DBA_DEBRA created a new table My_ORDERS which contains table contents of DEMOAPPS.ORDERS. This was done via a PL/SQL Package.

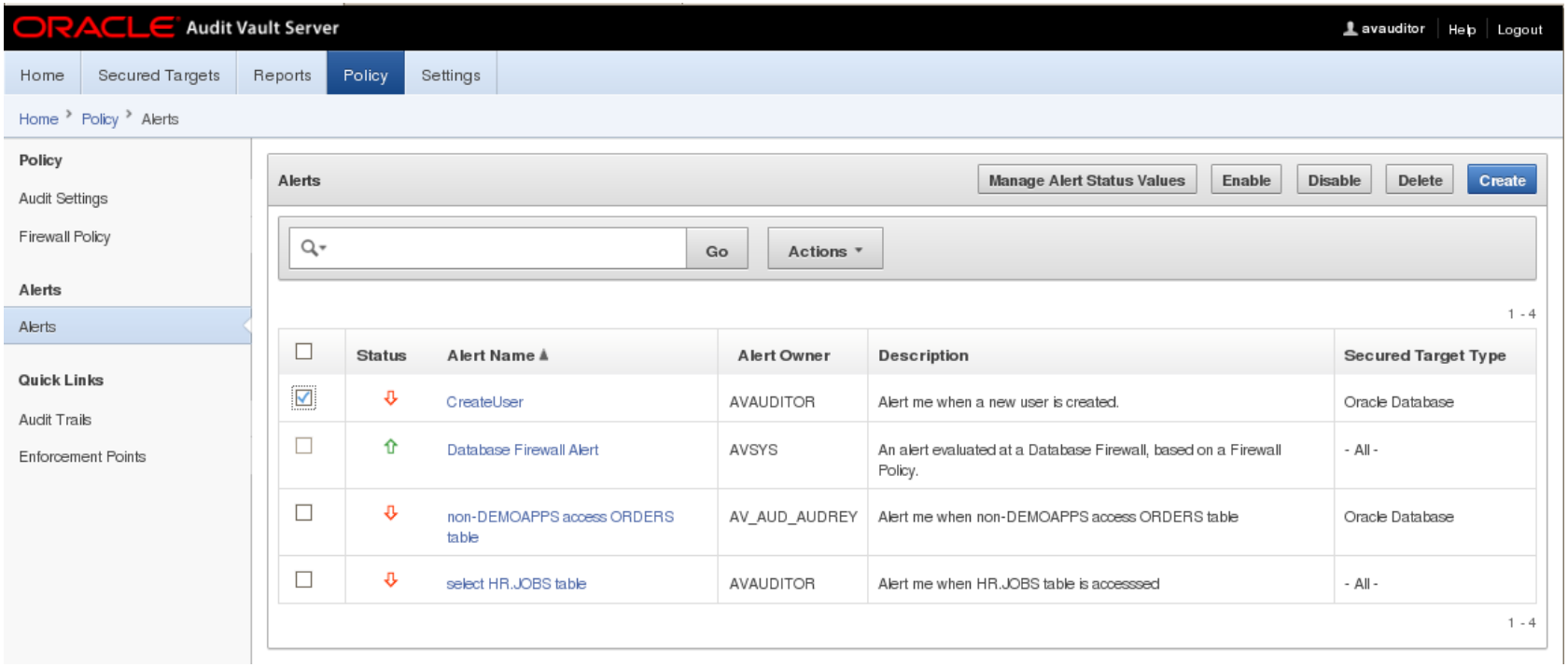
Lesson 13

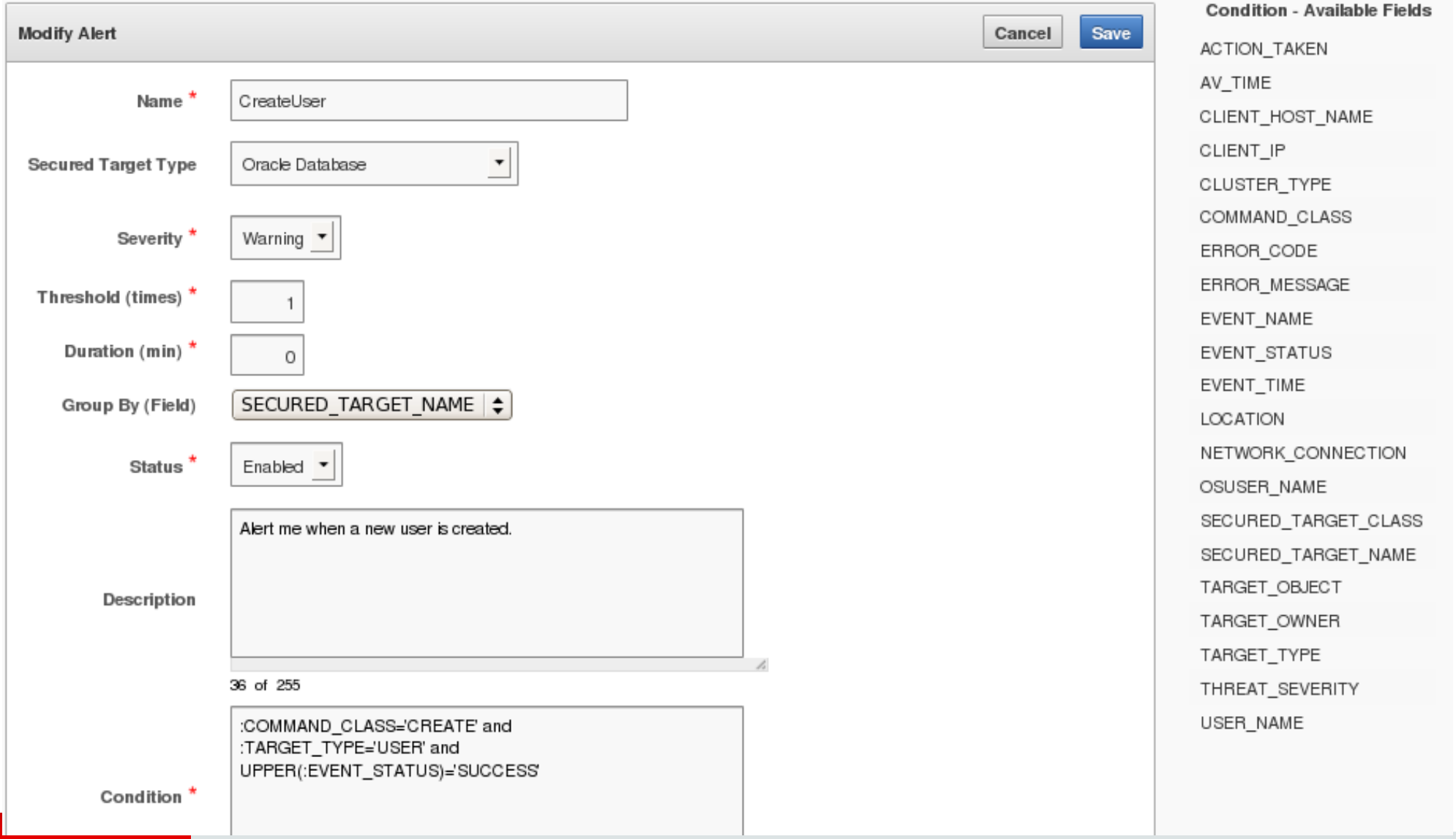
Alerts 101

Enable an Existing Alert

CreateUser, Select table, non-DEMOAPPS access table

Policy > Alerts > **Enable**



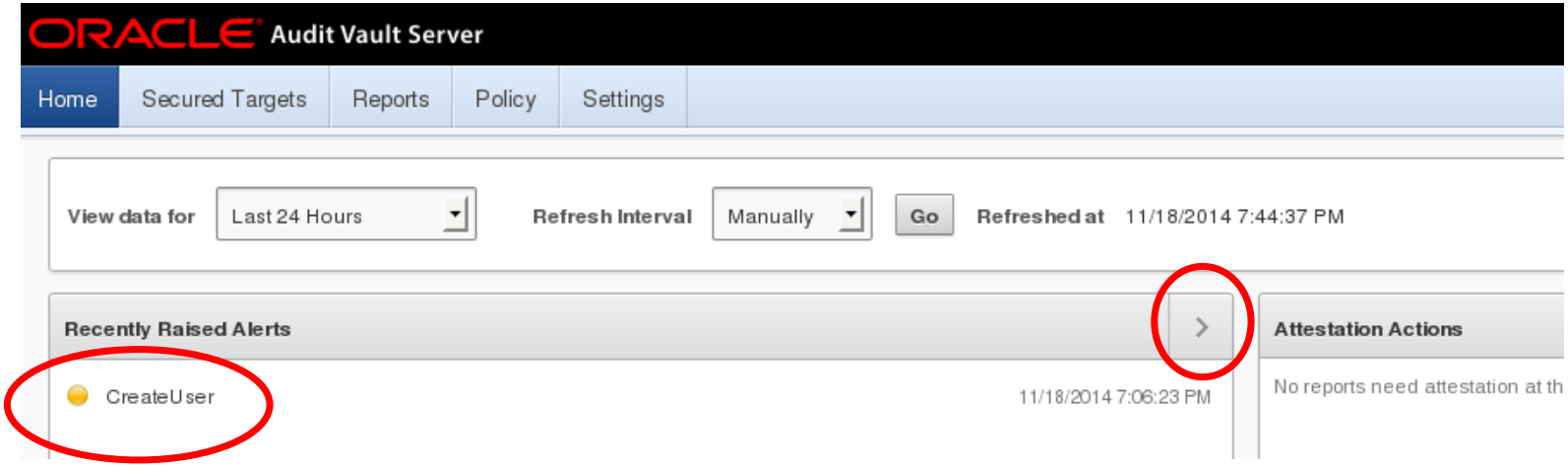


Firing the Alert

sqlplus DBA_DEBRA/Manager_1

SQL> Create user {melody} identified by Manager_1 account unlock;

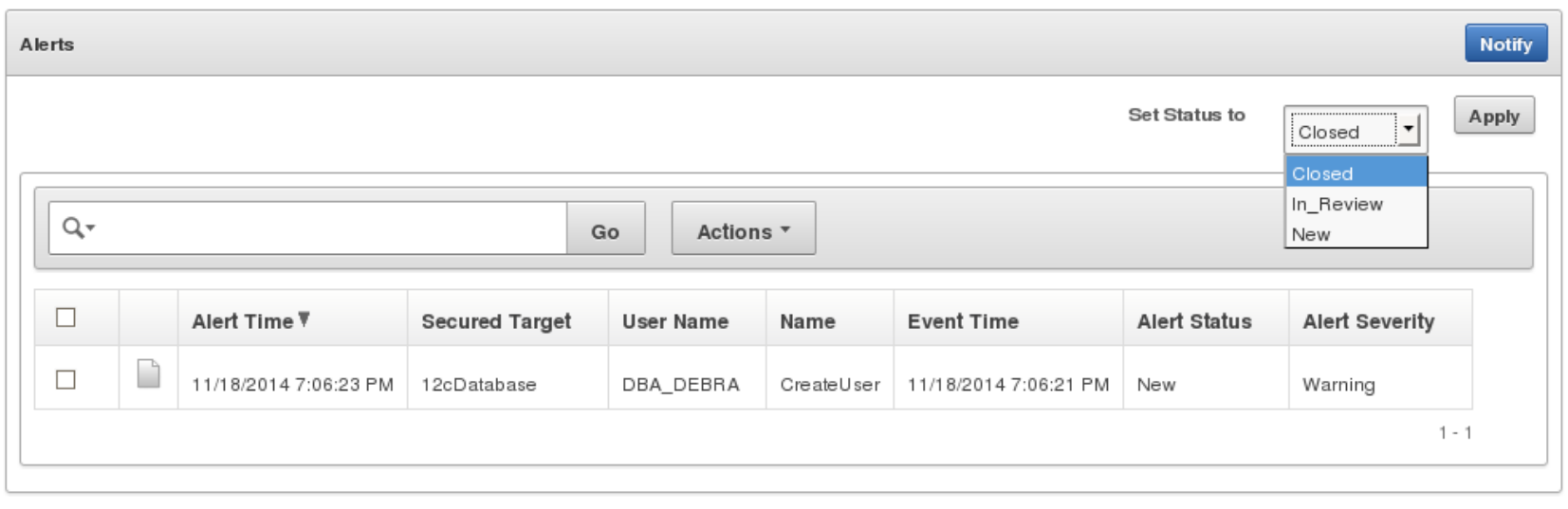
Refresh Interval "Manually" > Go



Manage Your Alerts

- Review details
- Attest, Notify
- Set Status : New, Closed, {custom}

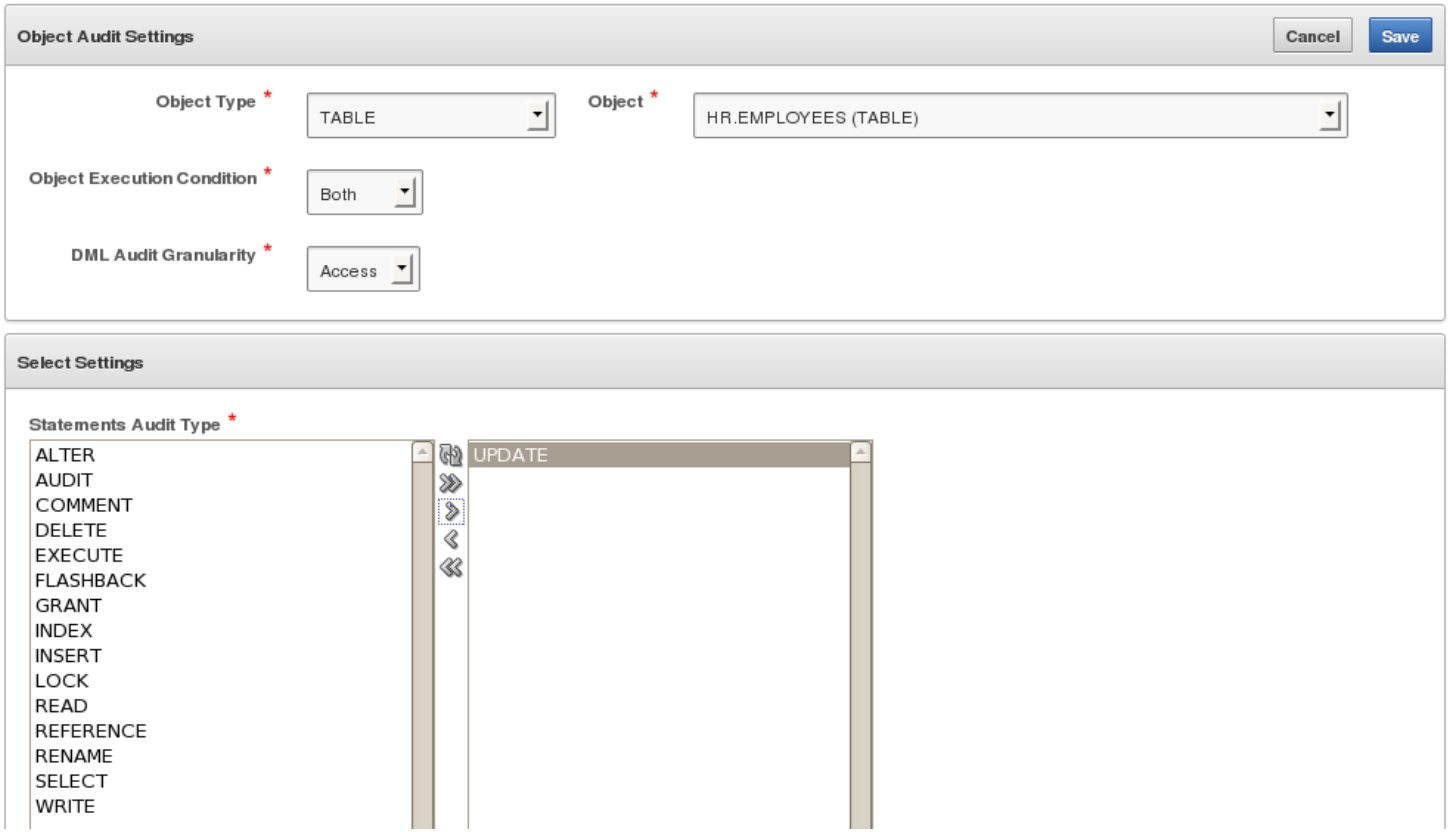
Other auditors must log in to see the attestation notice.
No email.



Create a New Alert

Alert Me When HR.EMPLOYEES table is Updated

1. Make sure audit setting on this object (table) is set



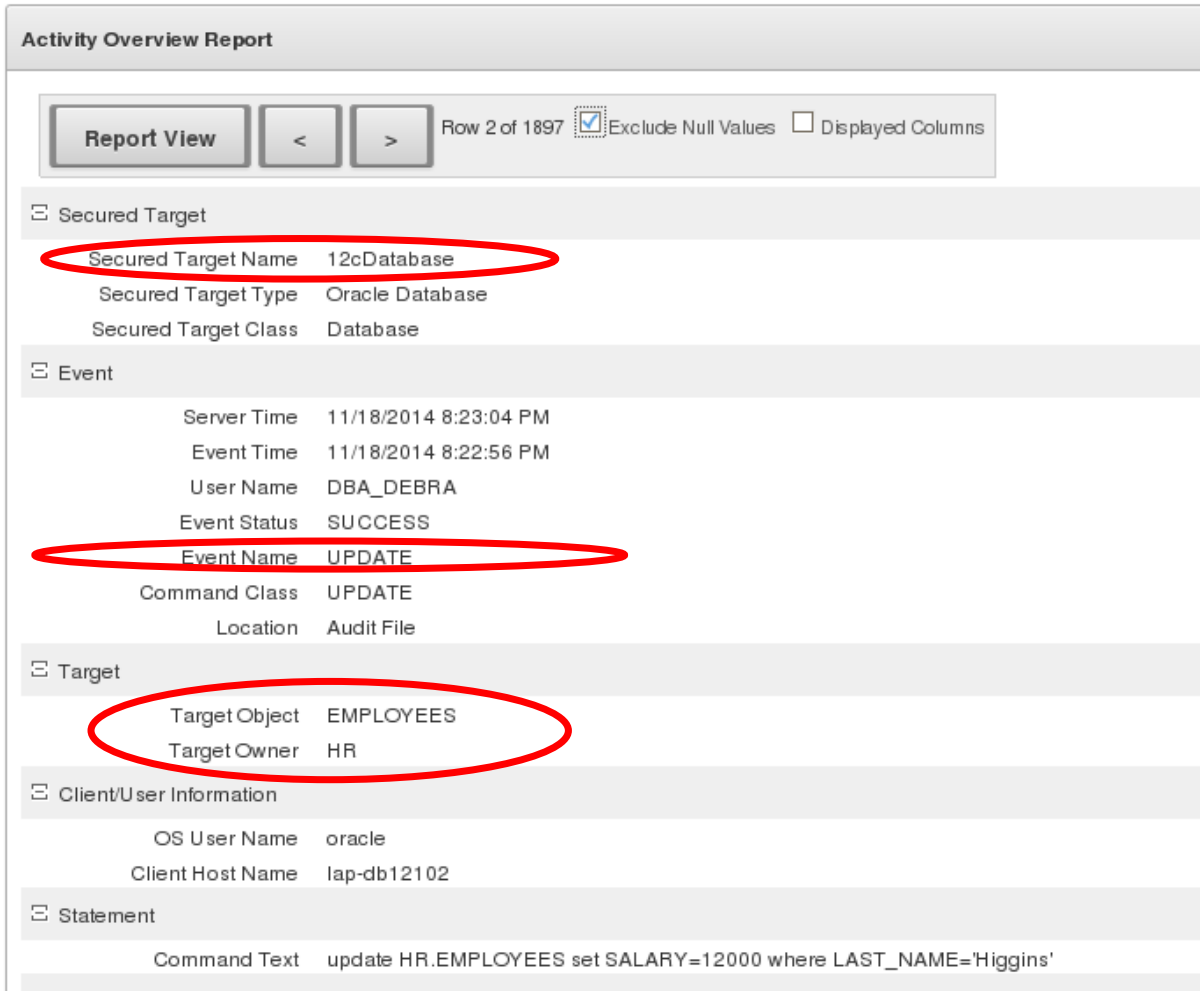
Create a New Alert

An Easier Way

2. **Create this audit event first** and examine the attributes in report

SQL> update HR.EMPLOYEES set SALARY=12000 where Last_name='Higgins';

- EVENT_NAME
- TARGET_OBJECT
- TARGET_OWNER



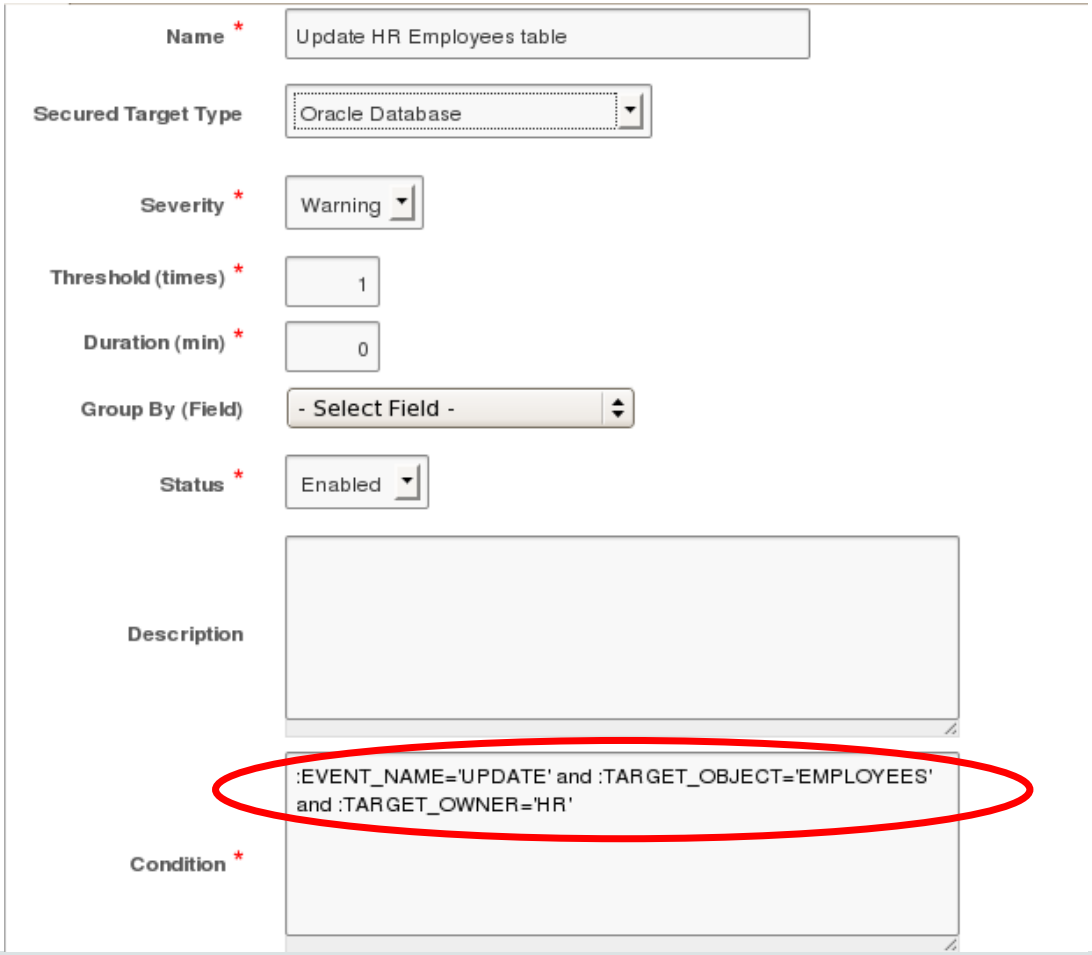
ORACLE

Create a New Alert

An Easier Way

3. Create the alert with corresponding syntax

Now fire the alert to ensure it's working



Troubleshooting Tips

No Alerts ….

- Is audit setting on secured target set ?
  - If you don’t see the event entry in All Activity Report, then there’s no audit data
- Check syntax. Use UPPER() function when needed.
- Are time settings sync’ed between AVS and target ?
- When all fails, see $AGENT_HOME/av/log

Audit Vault Server Use Cases

- ✓ Consolidate audit data from multiple platforms
- ✓ Meet compliance with out of box reports
- ✓ Continuously audit on sensitive and valuable data
- ✓ Alert suspicious and unauthorized activities in real time
- ✓ Identify excessive user rights, dormant users, and enable an entitlement review cycle
- ✓ Accelerate incident response and forensics investigations with filtering

Sharing Time

Building Alerts for Anomaly Detection

Server as a starting point and an example of the ease of rule creation and management

- Establish an Approved List
  - List of DBA (sys, system, dbsnmp, DBA_NICOLE)
  - List of OS users that the application server is running with
  - List of allowed OS users in client server architecture
  - Database users that own or access the application data (ex HR_apps)
  - Application-specific OS users that have administrative privileges in the database
  - List of sensitive objects that should be given extra protection (tables continaing sensitive data such as PII,CC or stored procedure used to encryption/decryptio of sensitive data

What To Alert

Server as a starting point and an example of the ease of rule creation and management

- User in DB_users but os user not in list of admin_os_users
- Object in sensitive object but statement does not contain “where”
- Object in sensitive_object but user not in db_users or osuser not in os_users

Program Agenda

1. Lesson 1 - 5
2. Lesson 6 - 13
3. Lesson 14 - 16
   - AVS Use Cases
   - AVS and FW Installs & Maintenance
   - Other topics
4. Lesson 17 - 22

Lesson 14

AVS Use Cases

Audit Vault Server Use Cases

- Audit consolidation from heterogeneous sources into one repository
- Out of box reports to achieve security compliance
- Proof of audit
- Detect and alert on suspicious activities :
  - Privileged users
  - Approved operations
  - Direct database access

Lesson 15

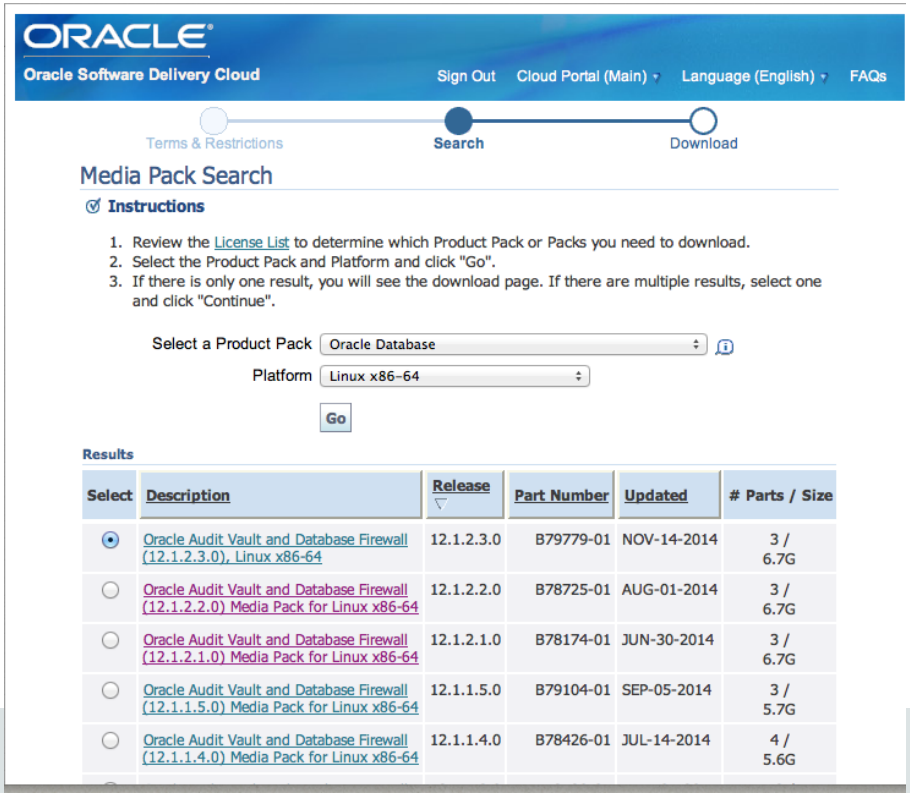
AVS and FW Installs & Upgrades

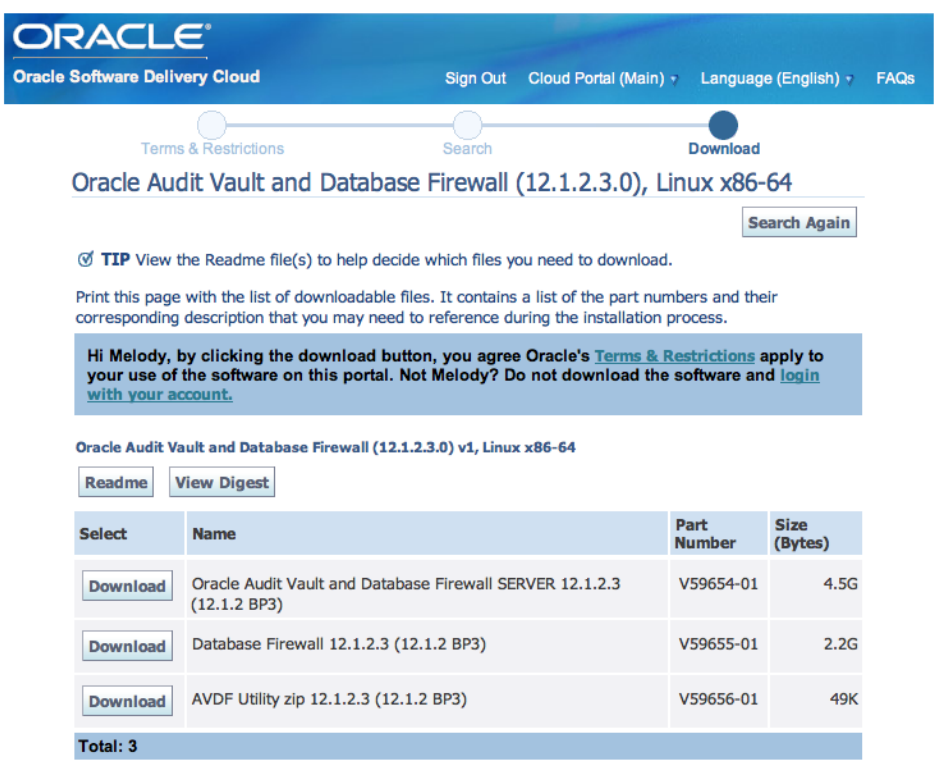
Check List

- Hardware
- Disk : minimum 150GB
- RAM : min 2GB, recommended 4GB
- Download ISO http://eDelivery.oracle.com

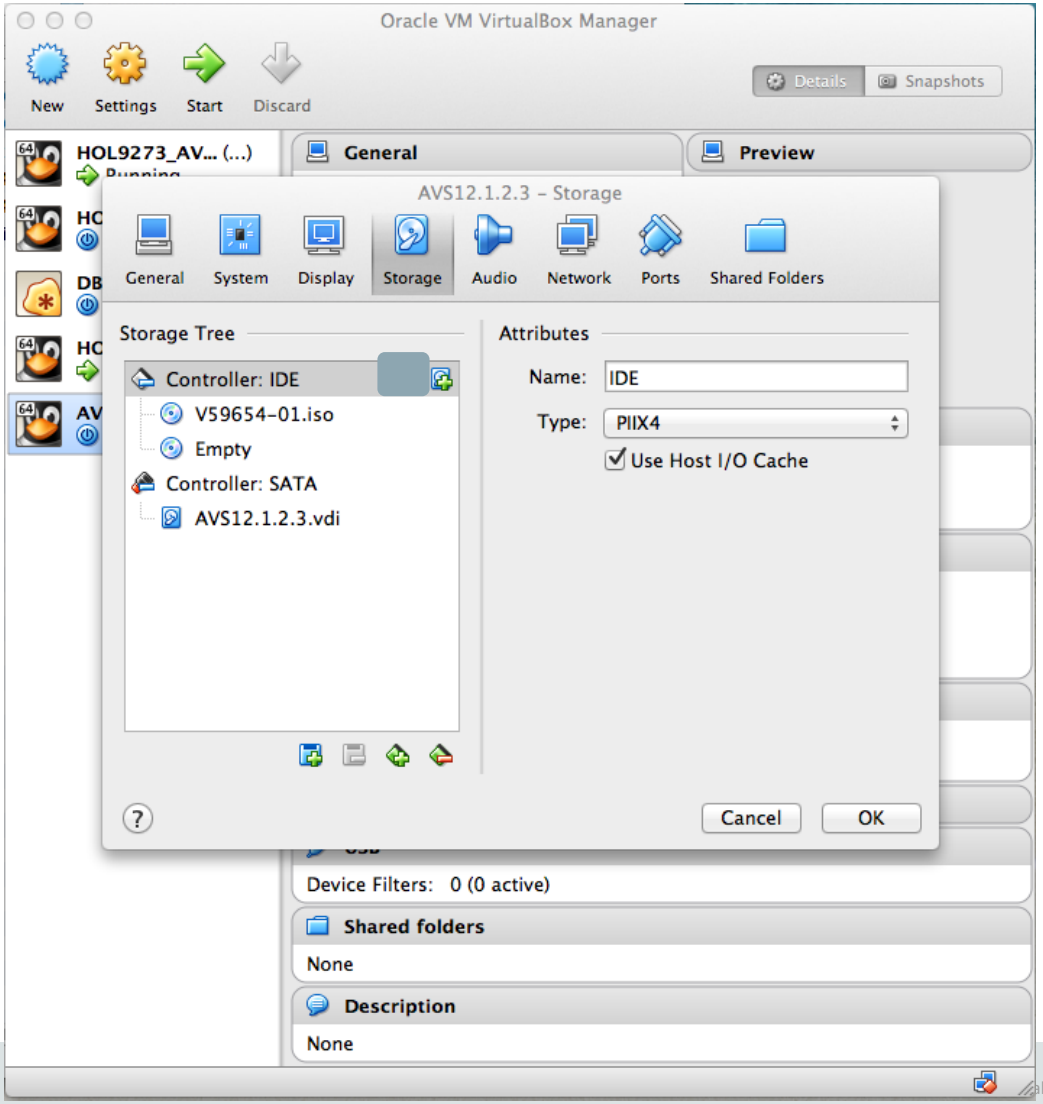
Check List

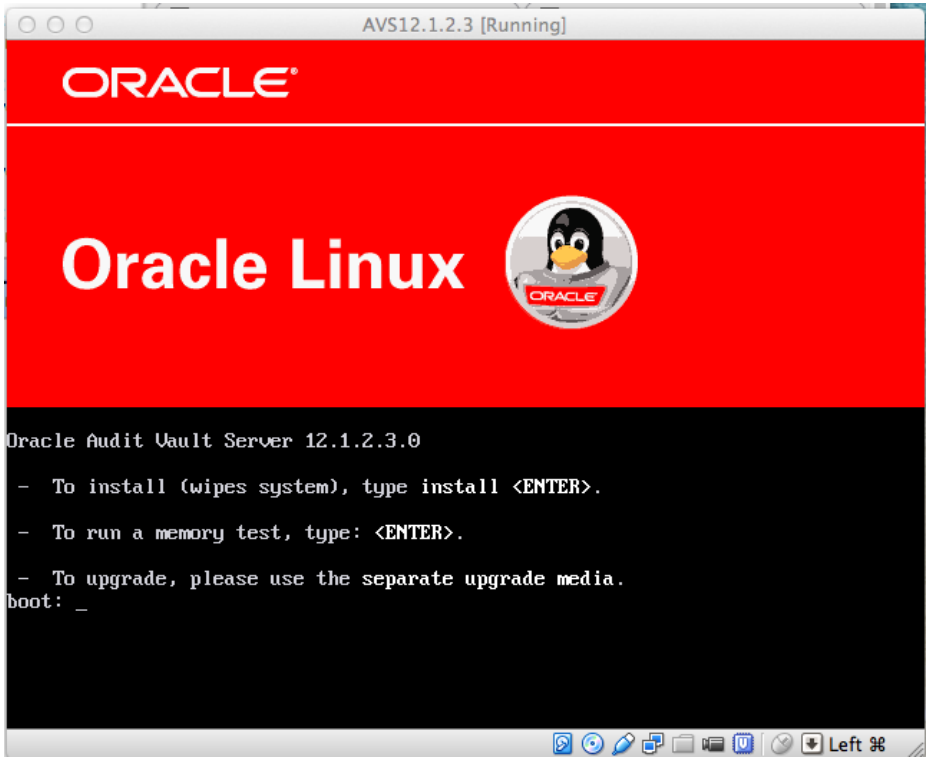
- Download ISO http://eDelivery.oracle.com





- Mount iso file





AVDF Maintenance

- AVDF releases Bundle Patches on a quarterly basis, following Oracles PSUs.
- Customers do not need to apply patches to individual components.
- How to find AVDF BP ?
  - Support site > Patches & Updates > Product or Family > Product is ‘Oracle Audit Vault and Database Firewall” + Release is “*the latest*”

Lesson 16

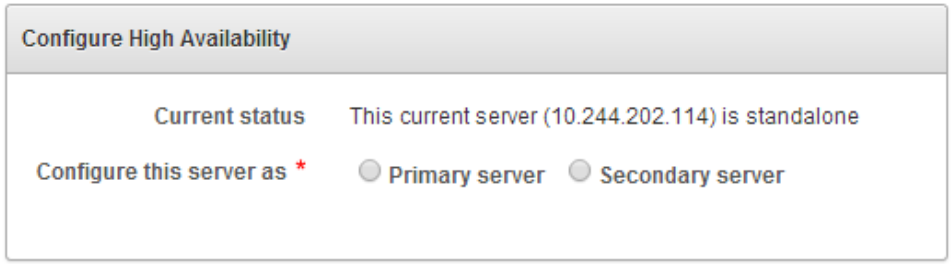
Other Topics

Other Topics

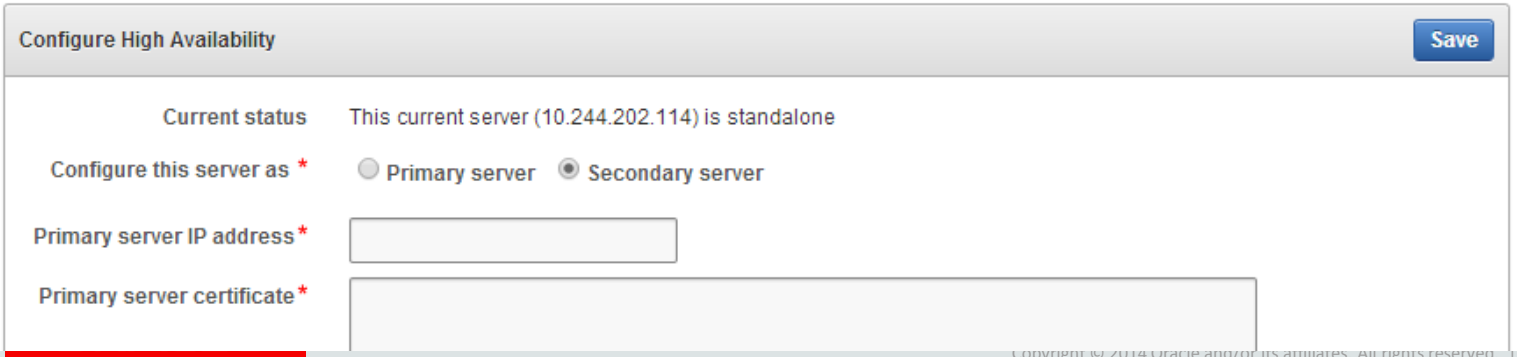
- New UI Changes on AVS HA
- SAN Storage Management and Migration
- Alerts integration with SYSLOG
- External Storage Support for both Audit Repository & Archive
- Backup & Restore Script

New HA UI

Validates all fields before HA pairing request can be submitted

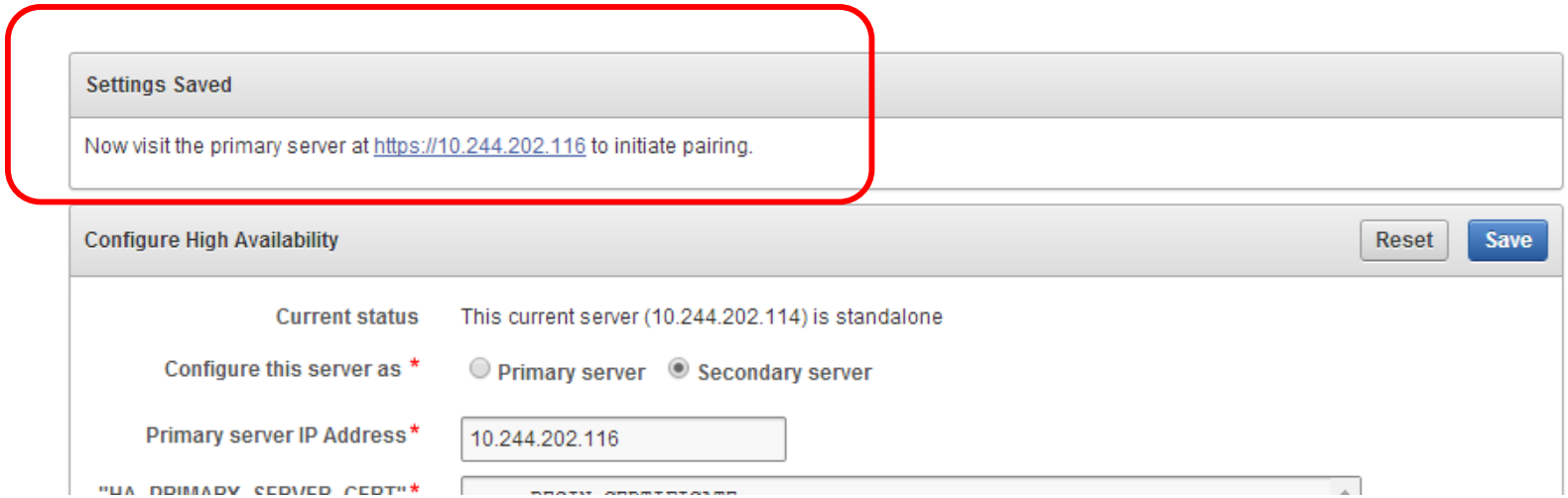


- **Configure the secondary server first**
- Validates all fields before they can be saved



New HA UI

- Then prompts to switch to primary



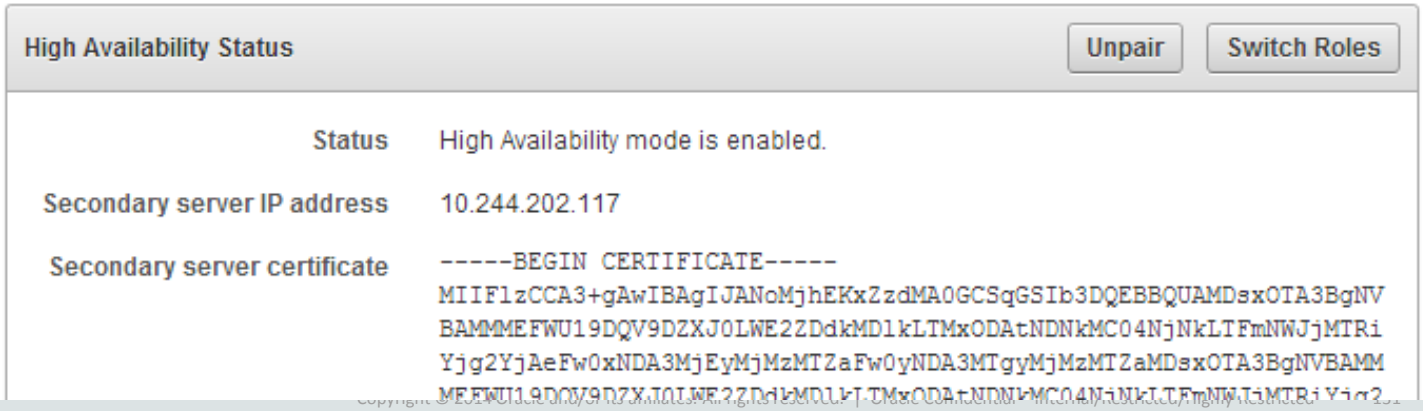
New HA UI

- Follow the link to the primary server and pick "Primary server" for "Configure this server as“
- “**Initiate Pairing**” is the only button that validates all

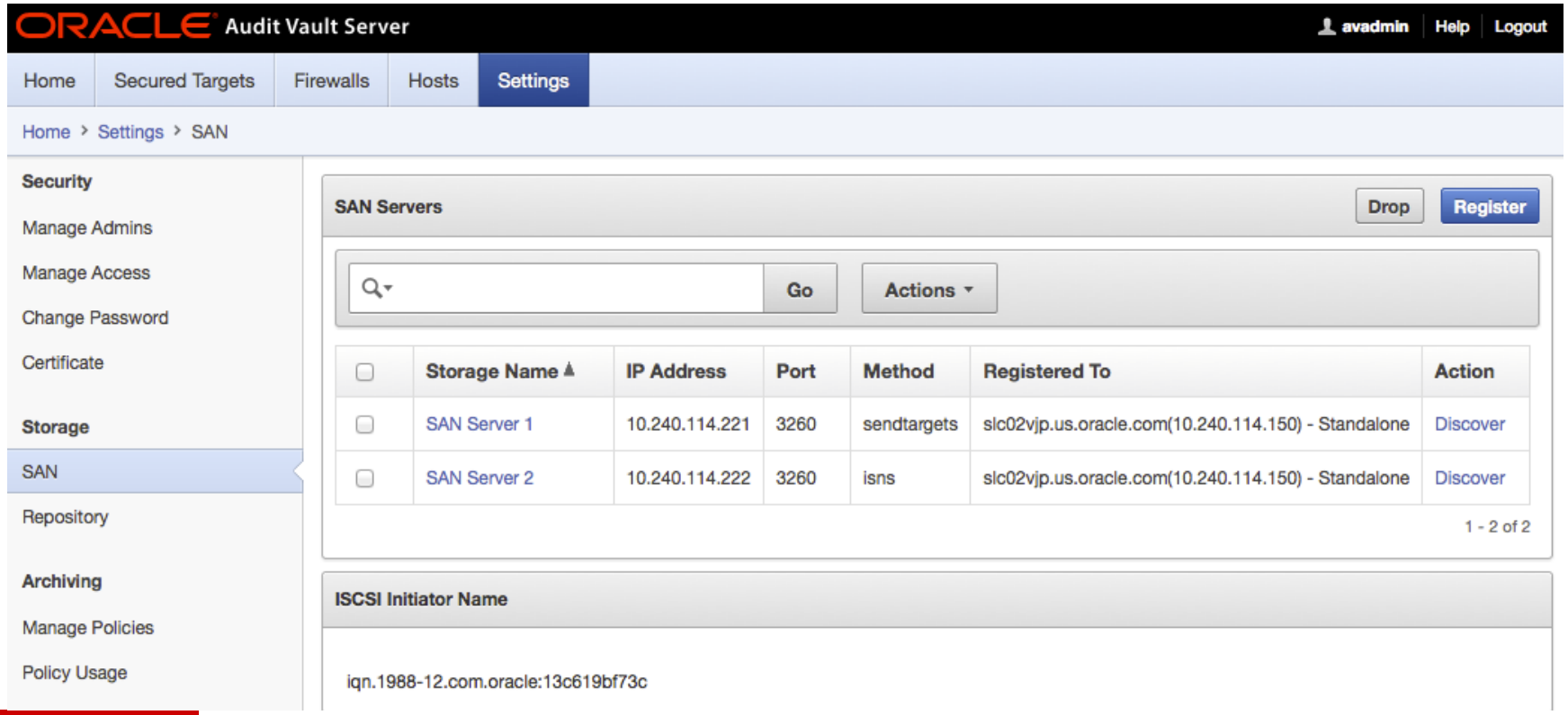
New HA UI

- When HA is being configured:
  Job in progress….HA is being configured, may take at least 10 minutes. The web console may not be available."

  The only thing visible on HA page is a "Refresh" button even when they navigate away and comes back.
- When done :



iSCSI SAN support for Audit Repository

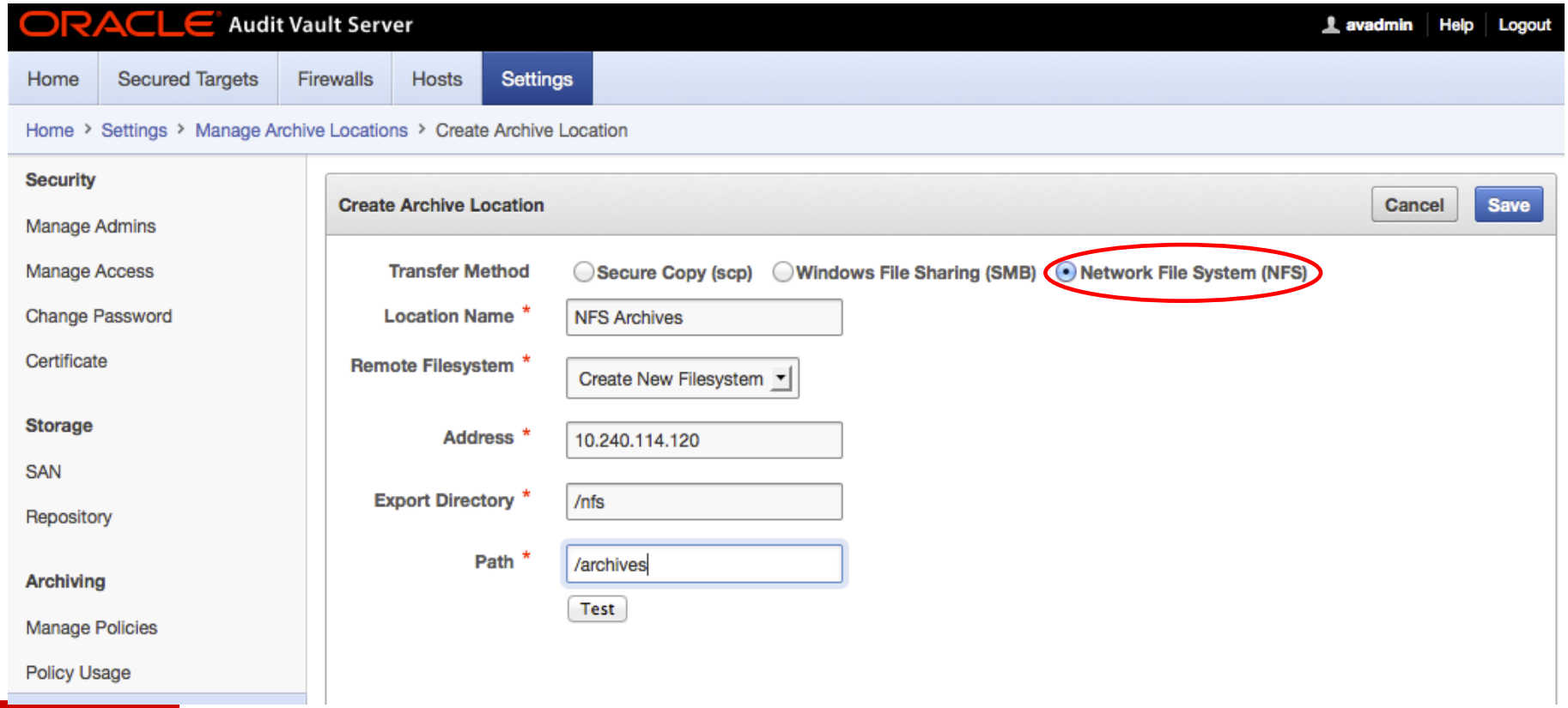


SAN Storage Best Practices

- Most straightforward way for customers is to attach/register SAN disks with the product and then do nothing.
- All newly collected data would automatically get stored on the SAN device, the ‘old’ data would eventually get out of the retention period and thus removed.

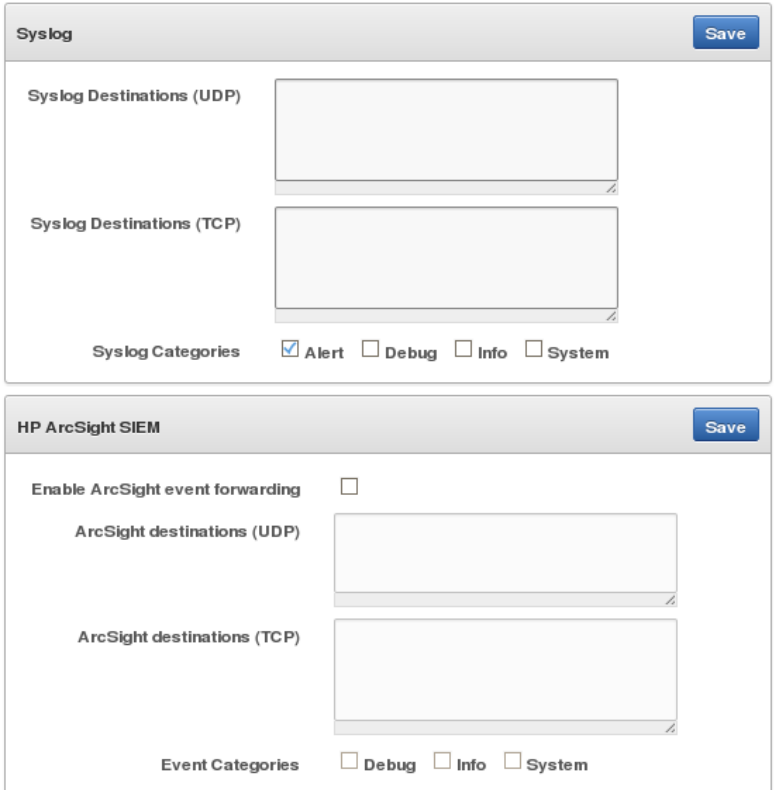
- Optionally download ZFS Vbox (+600MB – not recommended)

NFS Storage for Audit Data Archives



Configure syslog in AVS

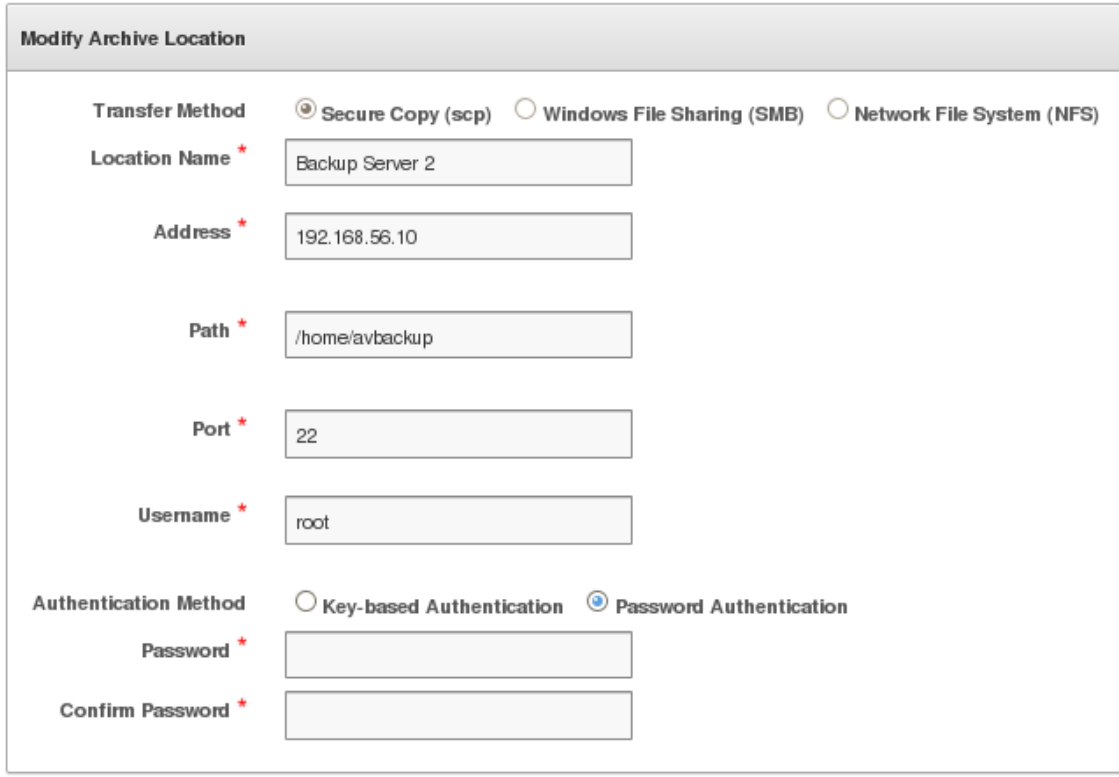
- Log in as avadmin
- Home > Settings > Connectors
- Syslog can be send to any destination TCP or UDP port. The most common ports are:
  - UDP 514 (default)
  - UDP 601
  - TCP 601
  - TCP 1522
- TCP syslog is vastly superior to UDP, because they are guaranteed to reach the syslog server, whilst UDP messages can be lost.



Configure Archive and Restore locations

- Log in as avadmin

- Settings > Manage Archive Locations
- Transfer method: SCP
- Location Name: Backup Server 2
- Address: 192.168.56.10
- Path /home/avbackup
- Port: 22
- Username: root
- Auth Method: password
- Password: Manager_1



Configure Archive and Restore locations - continued

- Open a terminal (192.168.56.10), and login as root
- Type in the commands
  - cd /home
  - mkdir /avbackups
- Check the directory exists with the command
  - ls –latr

Backup & Restore Script

MOS Note

- **Audit Vault Server Backup and Restore for Release 12.1.2.3.0 and Prior (Doc ID 1556200.1)**
- It describes how to create a manual backup of the Audit Vault Server installation and restoring that backup to new, replacement hardware using the Bash shell scripts from the **backup_restore12.1.2.3.0.tar.gz** file
- MOS note includes the tar file
- Always checks for updates from MOS
- 12.1.3 will have a wrapper to avoid manual editing of the backup script file

POC Check List

Good To Know

- Alt+F9 to watch console log while starting up AVS
- Setup a script to start agent
- Create another set of avadmin and avauditor. Use the installed user accounts ONLY as back-up accounts.
- What's my Firewall Admin userid ?
  - SQL>select username from dba_user where username like 'WUI%';
- EM integration (link to video)

Program Agenda

1. Lesson 1 - 5
2. Lesson 6 – 13
3. Lesson 14- 16
4. Lesson 17 - 22
   - Database Firewall and Auditing
   - Setting Up Firewall
   - Watch How A Firewall Policy Blocks SQL Injections
   - Building Firewall Policy – The Process
   - Exceptions Rule, Profiles and Novelty Policy
   - TCP Reset, Sensitive Data Masking

Lesson 17

Database Firewall and Auditing

Auditing & Database Firewall

Flexible Security

	Monitoring (Database Firewall)	Auditing
Information	Who, what, when where	Who, what, when, where Before/After values Full execution and application context
Pathways	Network	All: stored procedures, direct connections, scheduled jobs and operational activities
Impact on database	Completely independent	Configure database audit policies
Purpose	Prevent SQL injections and other unauthorized activity, enforce compliance with corporate data security policy	Ensure compliance, provide guaranteed audit trail to enable control

Lesson 18

Setting Up Firewall

Setting Up Your Environment

- All labs will require 3 OVMs : AVS, DBFW, 11gR2 (where HR_Application is)
- We will need DBWF only for this lab

- **Stop** you DB12.1.0.2 VM
- Keep your **AVS** VM up
- Start your **DBFW** VM

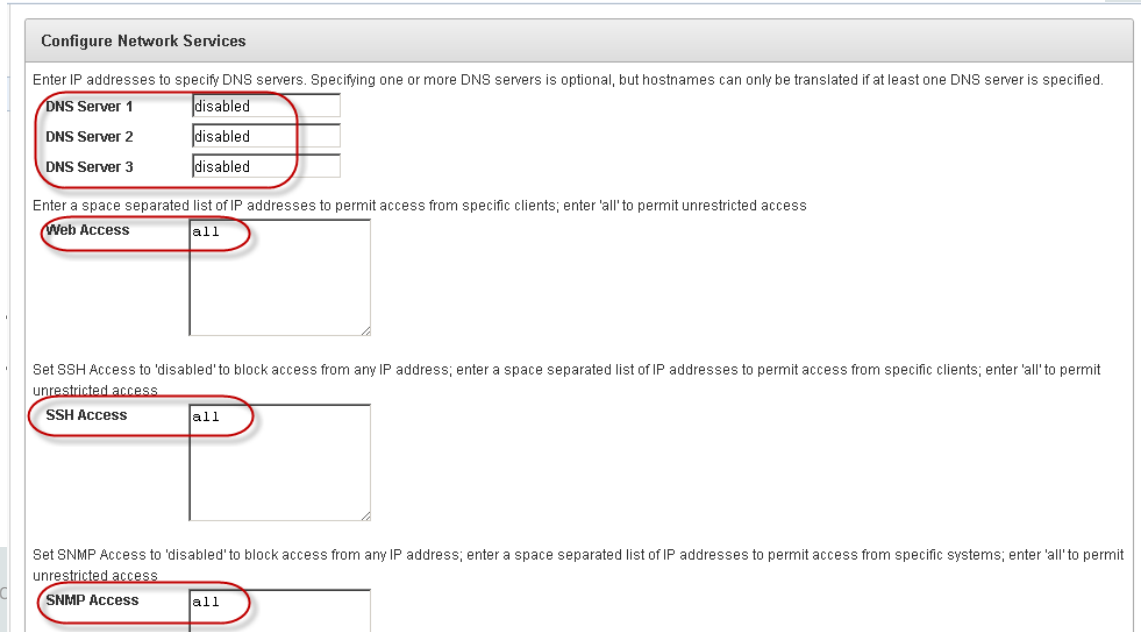
Setting Up Firewall

Enable Network Services

- From your laptop browser, go to Firewall Console :
  - https://192.168.56.12
- Log in as **FWADMIN**/Manager_1
- System > Service

[this is already done for you]

[Also check Date and Time + keyboard

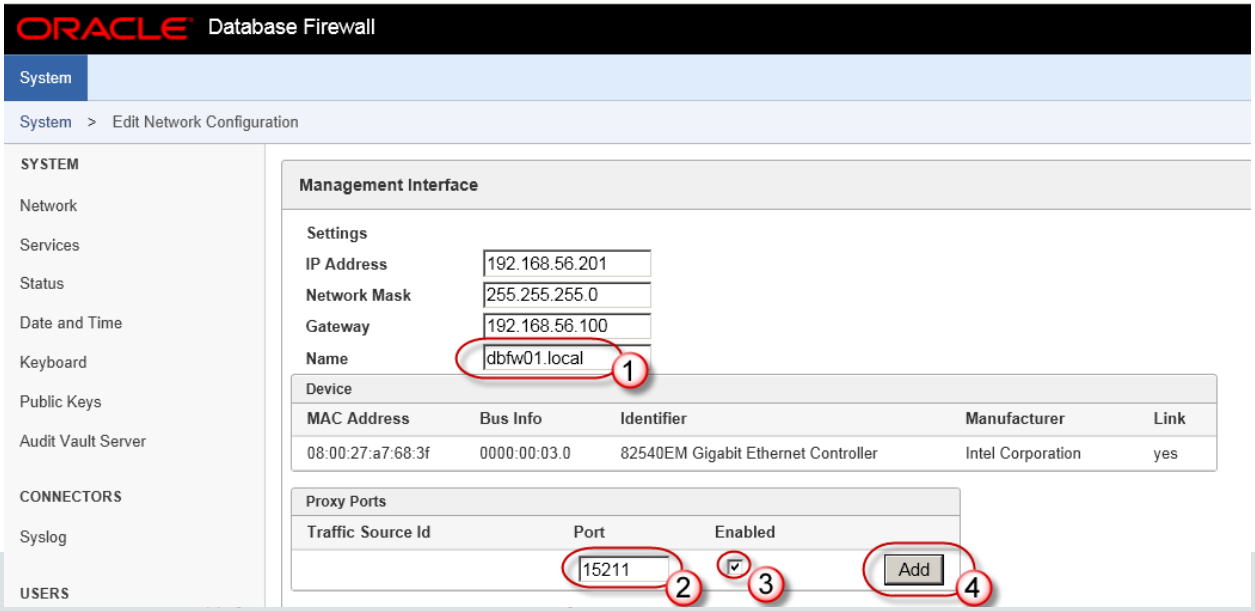


Setting Up Firewall

Configure the network interface and hostname

- System > Network
- Give it a friendly host name to your firewall
- Add a proxy port of 15211

[this is already done for you]



Setting Up Firewall

Associate Database Firewall with Audit Vault Server

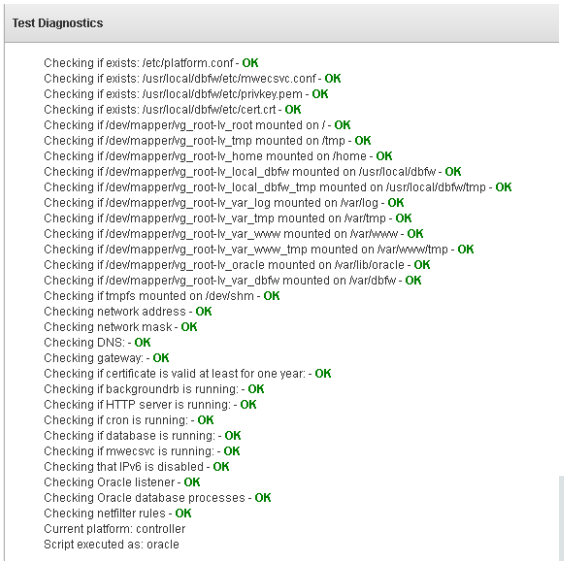
- Start another browser and log in to AVS console as AVADMIN
  - Settings > Certificate
  - Copy the certificate into your clipboard or into a text file.
  - Make sure you copy the header and footer (-----BEGIN CERTIFICATE----- and -----END CERTIFICATE-----)
- Switch to the Database Firewall administration console (FW_ADIN_ADAM)
  - System > Audit Vault Server
  - Enter the IP Address of the Audit Vault Server: 192.168.56.200
  - Paste the Audit Vault Server's Certificate in the next field

[this is already done for you]

Setting Up Firewall

Register the Firewall in AVS

- Switch to AVADMIN
- Firewall > Register
  - Enter a Name : dbfw02 and IP Address : 192.168.56.12
  - [this is already done for you so simply click dbfw02 to see the details]
- To test : Settings > Status > 'Test Diagnostics'
  - Everything should have a green **OK** next to it



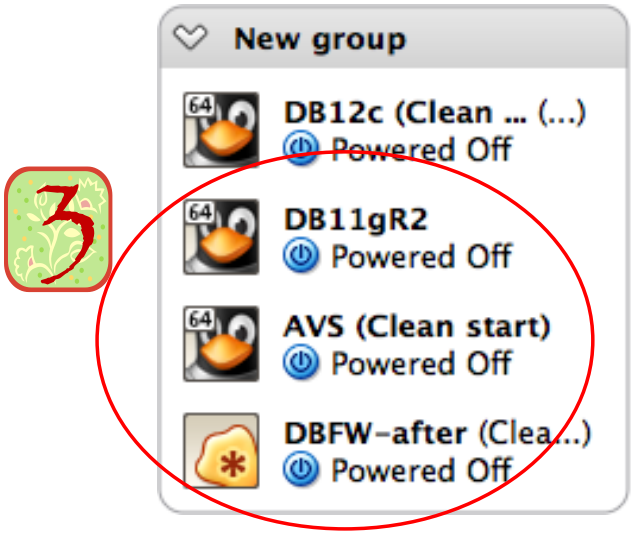
Lesson 19

Watch How A Firewall Policy Blocks SQL Injections

Setting Up Your Environment For This Lab

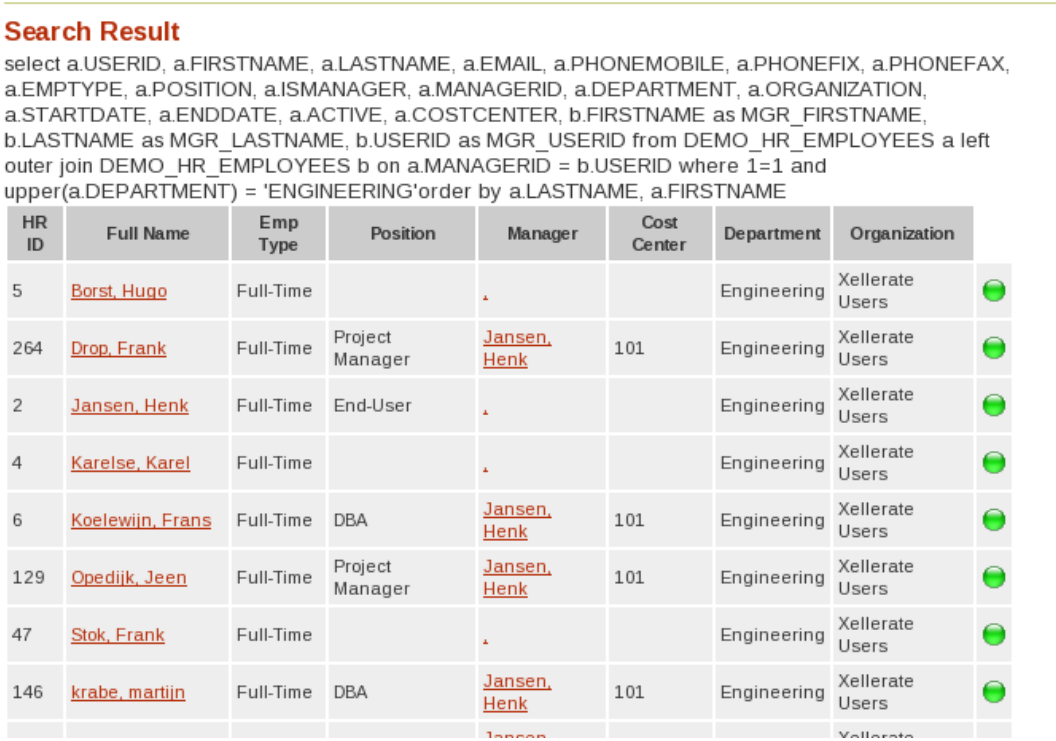
- All labs will require 3 OVMs : AVS, DBFW, 11gR2 (where HR_Application is)

- Keep your **AVS** VM up
- Keep your **DBFW** VM up
- Start your **DB11gR2** VM
  - Log in to Linux with Oracle/Manager_1
  - Run “step1 : start agent”
  - Start a browser and select ‘HR_App’ bookmark



Run ‘Search Employees’

- Click ‘Login’ link in the upper left of the window
- Use **malicious_malfoy/Manager_1** to login to the sample HR Application
- Click on ‘Search Employees’ link in the right pane
- Click “Search” button
- You will see list 10 results returned
- Optionally select “Debug” checkbox to see SQL statement executed



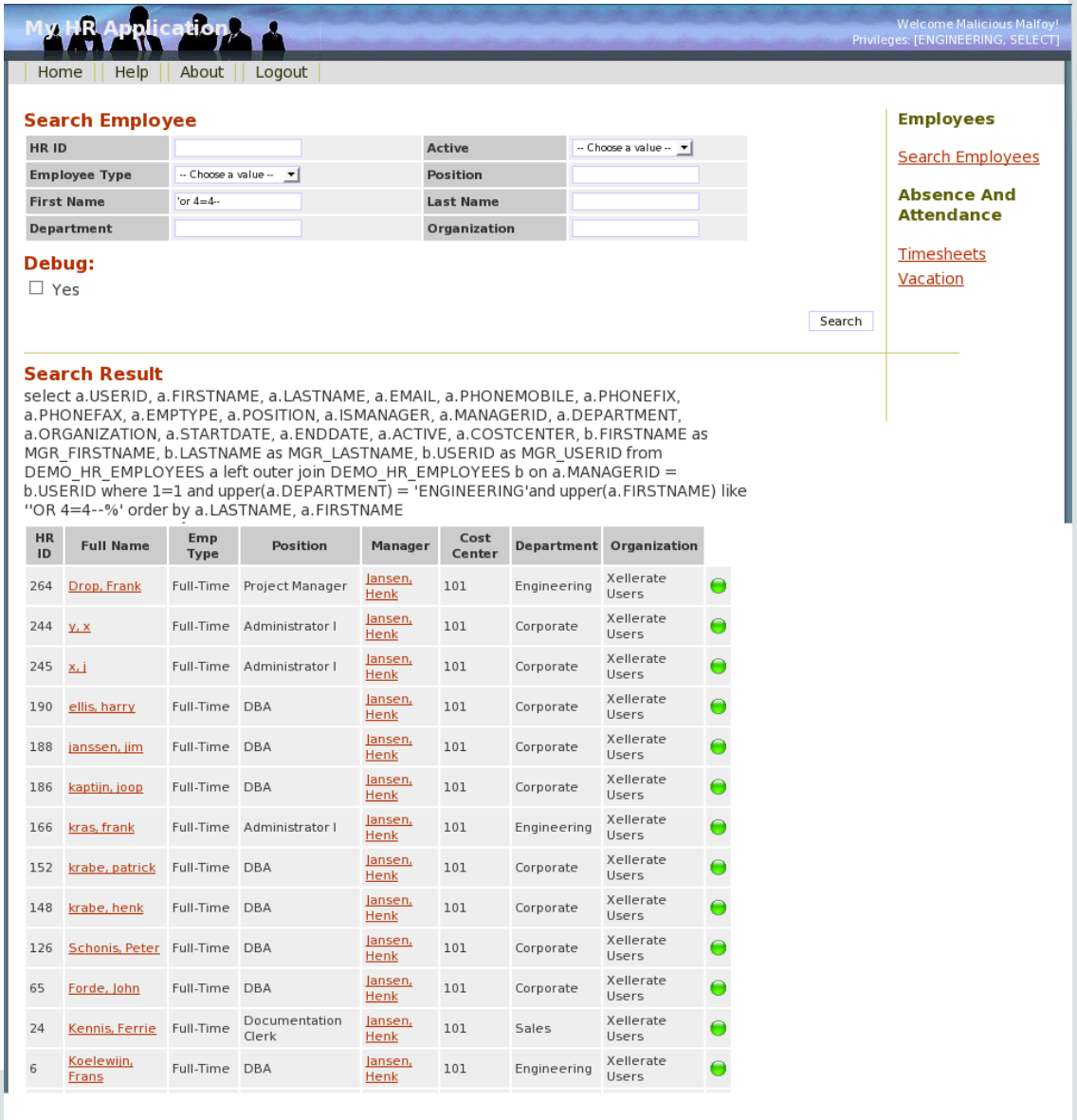
Search Result

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.ORGANIZATION, 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.DEPARTMENT) = 'ENGINEERING'order by a.LASTNAME, a.FIRSTNAME

HR ID	Full Name	Emp Type	Position	Manager	Cost Center	Department	Organization
5	Borst, Hugo	Full-Time				Engineering	Xellerate Users
264	Drop, Frank	Full-Time	Project Manager	Jansen, Henk	101	Engineering	Xellerate Users
2	Jansen, Henk	Full-Time	End-User			Engineering	Xellerate Users
4	Karelse, Karel	Full-Time				Engineering	Xellerate Users
6	Koelewijn, Frans	Full-Time	DBA	Jansen, Henk	101	Engineering	Xellerate Users
129	Opedijk, Jeen	Full-Time	Project Manager	Jansen, Henk	101	Engineering	Xellerate Users
47	Stok, Frank	Full-Time				Engineering	Xellerate Users
146	krabe, martijn	Full-Time	DBA	Jansen, Henk	101	Engineering	Xellerate Users

SQL Inject

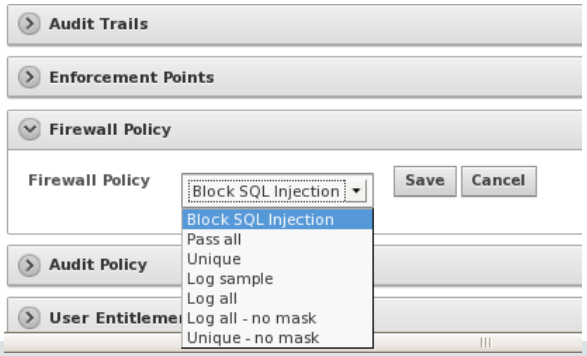
- In Last Name field, enter **'or 4=4—**
- You will see (unexpected) more results shown
- Optionally select "Debug" checkbox to see SQL statement executed



ORACLE

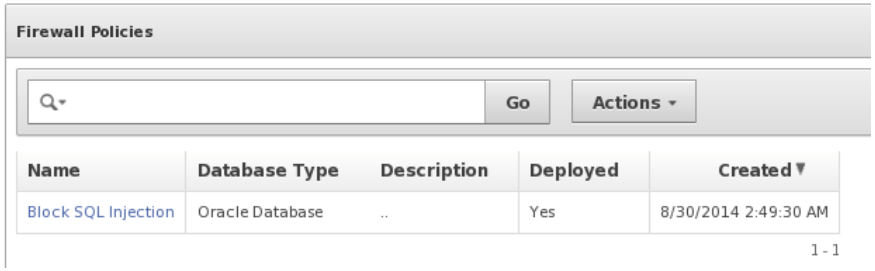
Deploy Firewall Policy and Watch Injection Blocking

- Log into AVS as AVAUDITOR > “Secured Targets” > “Oracle11gR2DB”
- Expand “Firewall Policy” section
- Click ‘Change’ button and select ‘**Block SQL Injection**’ policy in the dropdown list
- Click ‘Save’ button and you will get a message “Firewall Policy assigned successfully’



Deploy Firewall Policy and Watch Injection Blocking

- Go to Home > Policy > Firewall Policy and verify that the policy is **Deployed**



- This firewall policy will only accept SQLs on the whitelist and will substitute all unseen SQLs (potential injections) with a safe statement.
- Next, you will observe how the same injections will be blocked and substituted

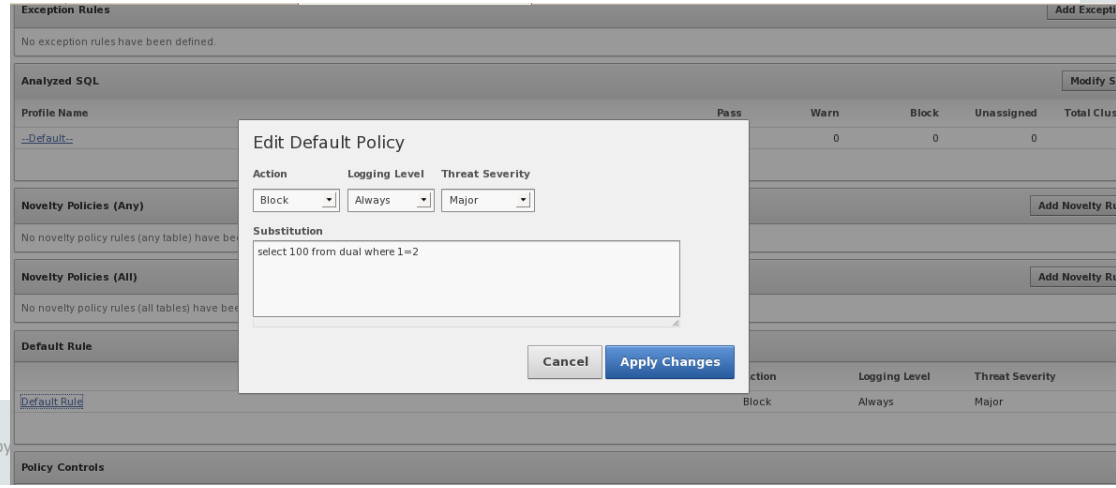
Deploy Firewall Policy and Watch Injection Blocking

- Go back to your My HR Application window and issue the same SQL Injection **‘ or 4=4—**
- Check ‘Debug’ and click on ‘Search’
- Observe that **no results** were returned even with the same injection in the SQL statement.
  - Instead you will see ‘java.sql.SQLException : ORA-00911: invalid character’ error msg
  - This is because Database Firewall blocked the SQL-injection and substituted with a harmless statement → let’s find out the harmless statement ?

Examine the Firewall Policy and Its Default Policy

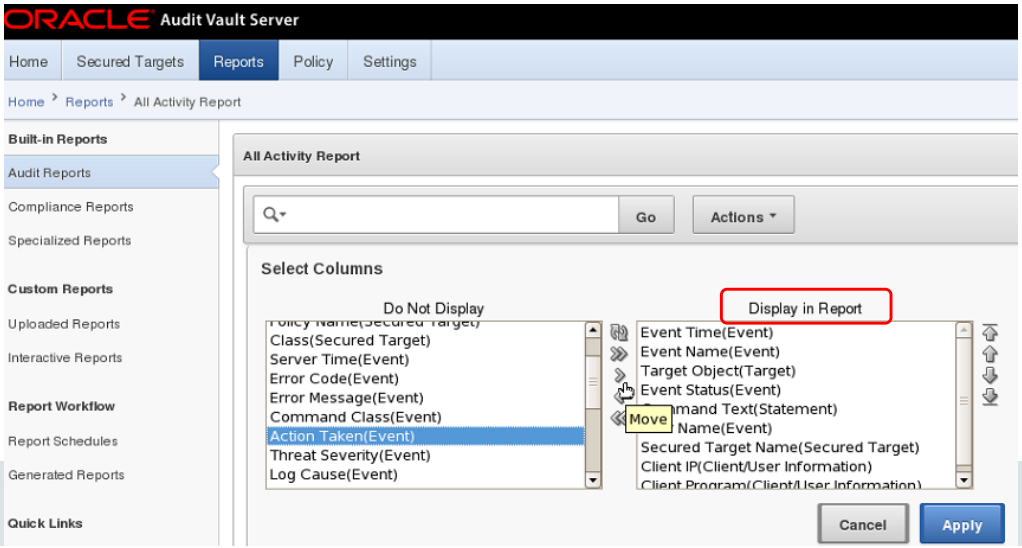
Note : a firewall policy cannot be modified while deployed

- So, first switch current policy to “Log Unique”
- Now examine “Block SQL Injection” policy :
  - Policy > Firewall Policy > “Block SQL Injections”
  - Scroll down to ‘Default Rule’ and select it
  - You will see the details



Review HR App SQL using All Activity Report

- While logged in as AVAUDITOR
- Browse All Activity Report
- Click “Action” button > ‘Select Columns’ > “Action Taken (Event)’
- Move “Action Taken (Event)’ into the right window (‘Display in report’)
- Apply



Review HR App SQL using All Activity Report

Secured Target Name : Oracle11gR2DB

	Action Taken	Event Time	Event Name	Target Object	Event Status	Command Text	User Name	Client IP	Client Program
	block	9/24/2014 3:51:21 AM	statement	DEMO_HR_EMPLOYEES		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.ORGANIZATION, 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 0=0 and upper(a.DEPARTMENT) = '############'and upper(a.FIRSTNAME) like ''OR 0=0--%' order by a.LASTNAME, a.FIRSTNAME	DEMOAPPS	192.168.56.10	JDBC Thin Client
	block	9/24/2014 3:51:21 AM	statement	DEMO_HR_EMPLOYEES		select a.USERID, a.FIRSTNAME, a.LASTNAME, a.EMAIL, a.PHONEMOBILE, a.PHONEFIX, a.PHONEFAX, a.EMPTYPE, a.POSITION, a.ISMANAGER, a.MANAGERID,	DEMOAPPS	192.168.56.10	JDBC Thin Client

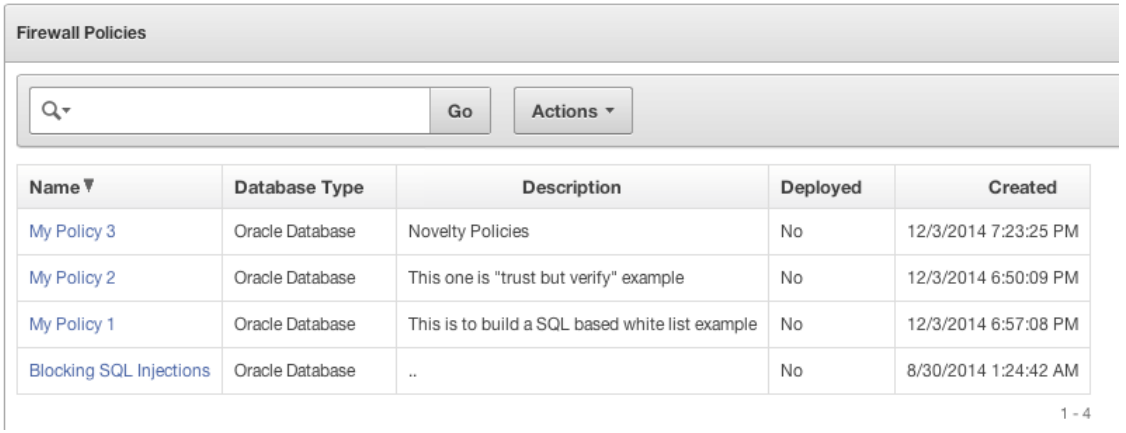
Note: you will also see firewall alert on home page.

Lesson 20

Building Firewall Policy – The Process

Building Firewall Policies

- In this exercise you will build a new policy : My Policy 1



Building A Firewall Policy - Process

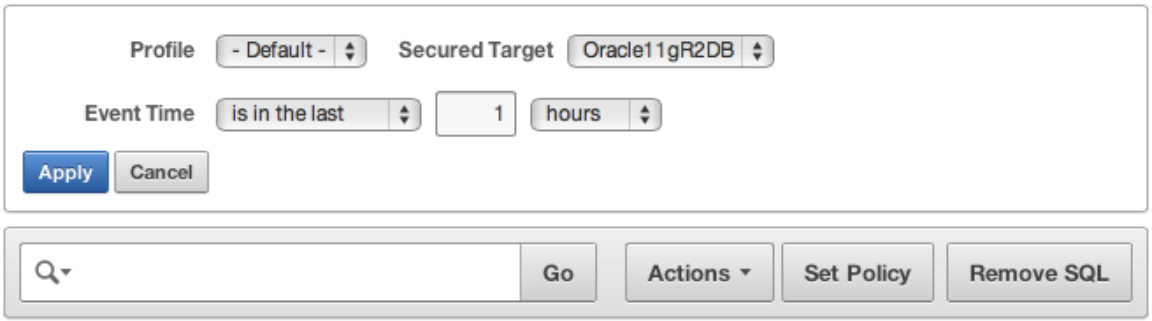
1. Start with “Log Unique” policy
2. Create a new firewall policy
3. Capture live data in Testing lab & build whitelist
4. Tighten access by rules for out-of-policy statements (log, alert, substitute)
   - Enforce blocking (optional) by rules for out of-of-policy statement (block)
5. Deploy policy in production with alert on out-of-policy activity

Building A Firewall Policy - Process

1. Start with “Log Unique” policy
2. Create a new firewall policy
   - Policy > Firewall Policy > Create Policy > Oracle Database + {My policy **1**} > Save
   - Right now there is no whitelist nor default rule yet
3. Capture live data in testing lab & build whitelist
   - Feed **good** SQLs (using HR_App and search)
   - Go back to the new policy you just created
   - Select “Modify SQL” under “ Analyzed SQL”

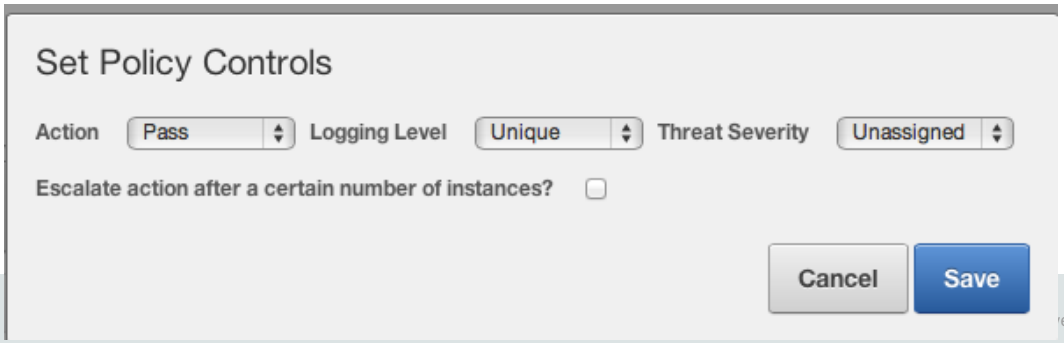
Building A Firewall Policy - Process

- Select "**Change**" button > select Secured Target : Oracle11gR2DB + Event in last hour > Apply



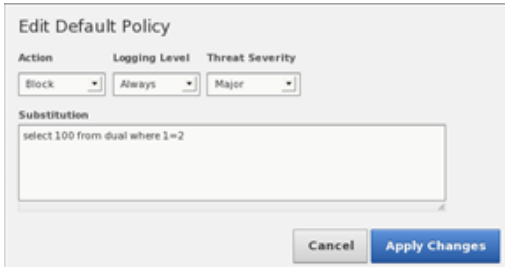
[you will see SQLs you just generated showing up]

- Check the good SQLs and click 'Set Policy' button → you just built your whitelist
- Now 'Set policy Controls' window will pop up > Action: Pass + Logging : Unique + Threat : Unassigned



Building A Firewall Policy - Process

- Select ‘Default Rule’ and set Action : Warn + Logging : Always + Threat : Major > Apply Changes

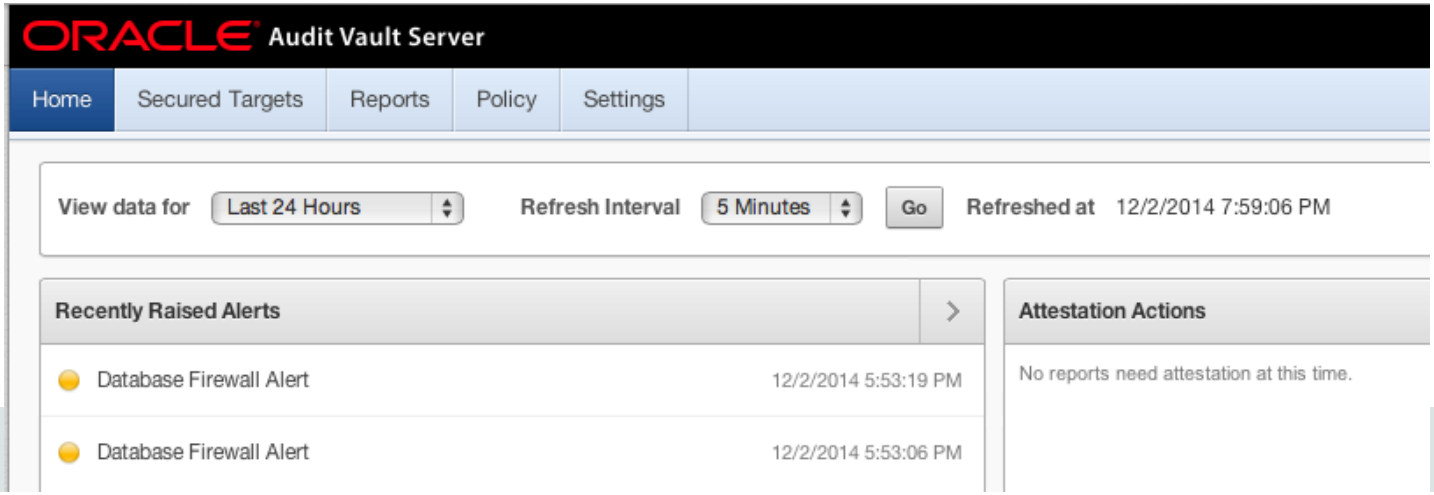


- You are done with a new Firewall Policy creation. Save + **Publish** !
- Be sure to **Deploy** the policy !

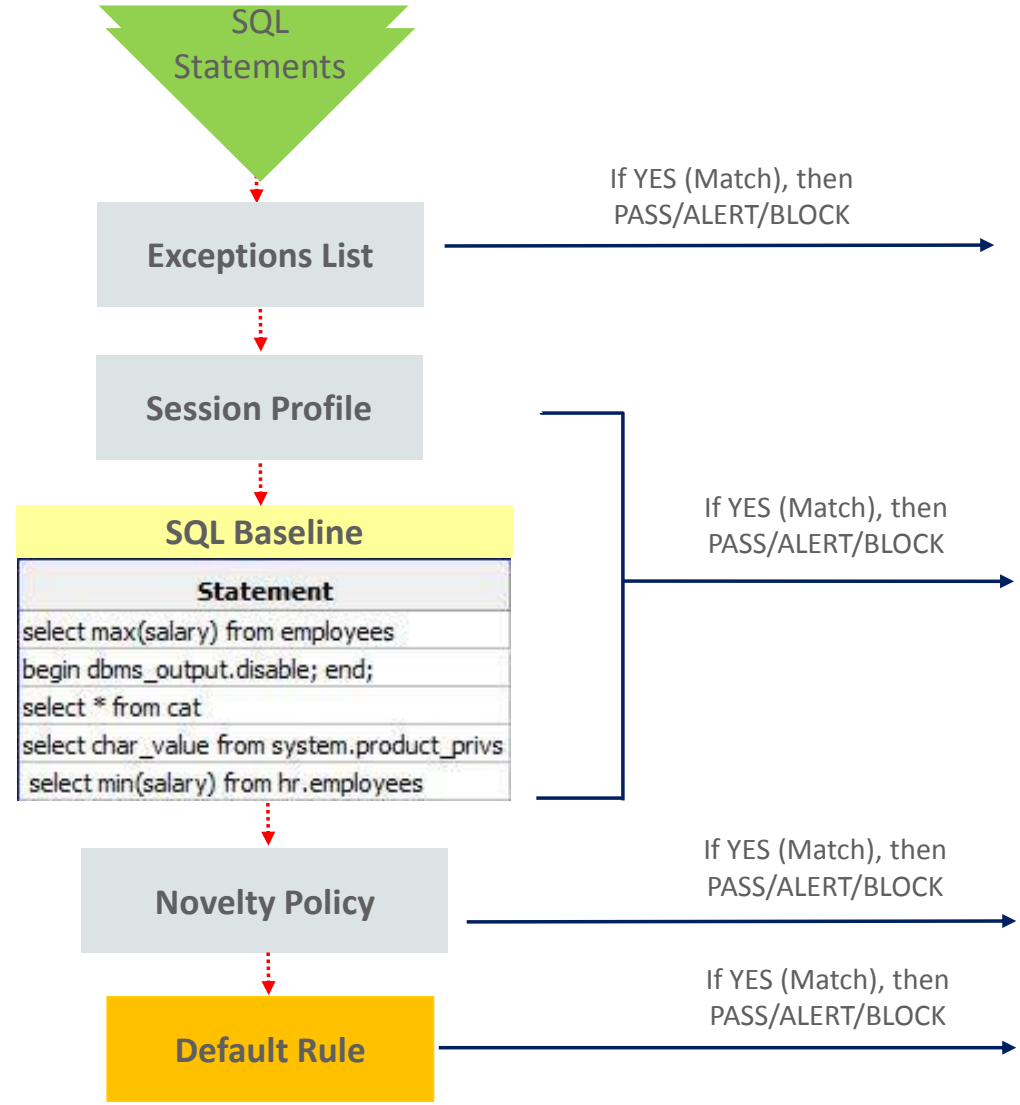
4. Tighten access by rules for out-of-policy statements (warn, block, substitute, etc.)
   - Enforce blocking (optional) by rules for out of-of-policy statement
5. Deploy in production with alert on out-of-policy activity

Building A Firewall Policy - Process

1. Start with “Log Unique” policy
2. Create a new firewall policy
3. Capture live data in Testing lab & build whitelist
4. Tighten access by rules for out-of-policy statements (pass, alert, substitute)
   - Enforce blocking (optional) by rules for out of-of-policy statement (block)
5. Deploy policy in production with alert on out-of-policy activity



Firewall Policy Flow



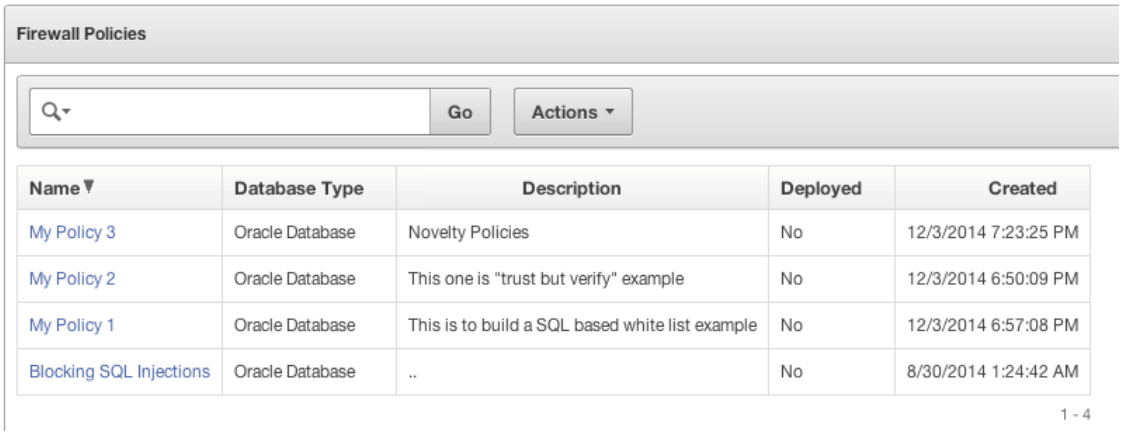
167

Lesson 21

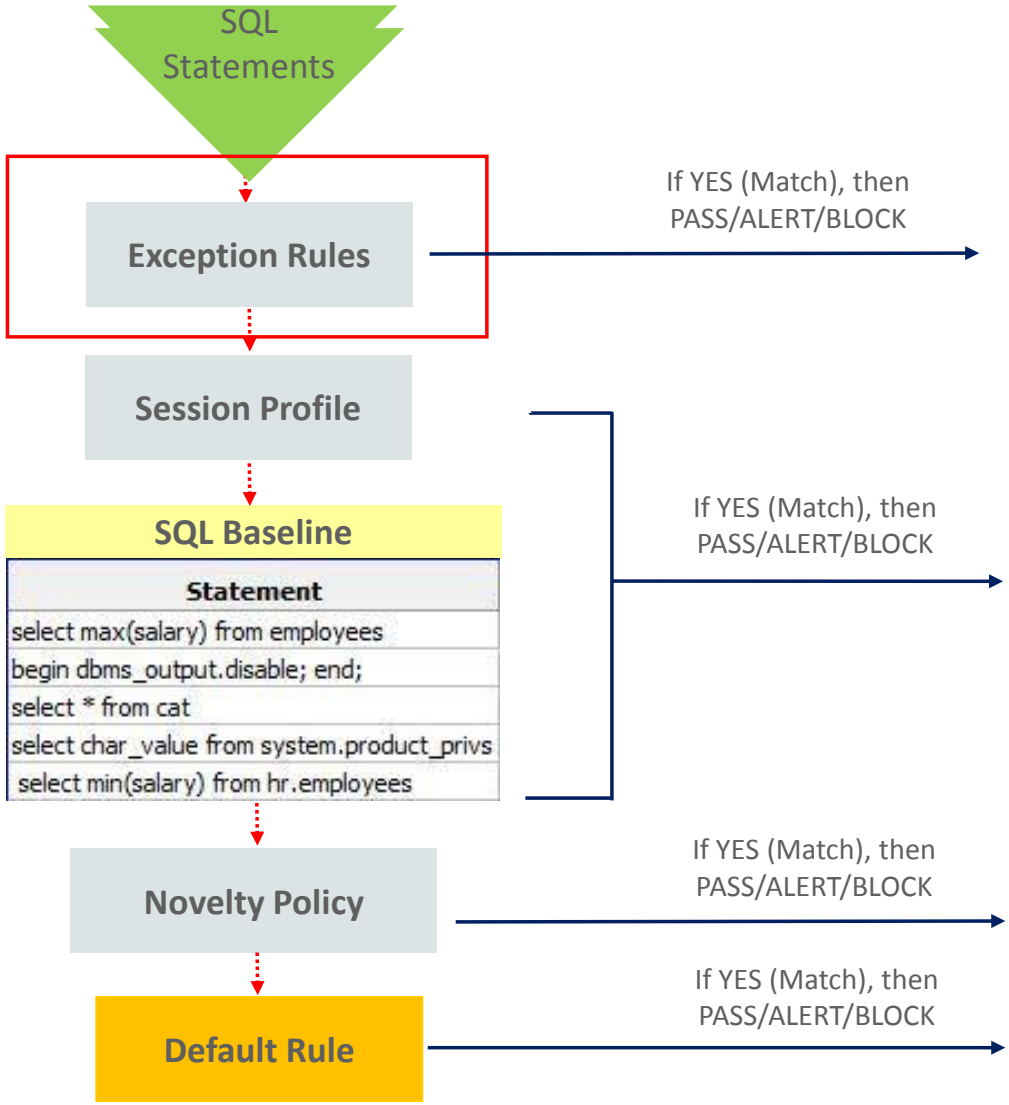
Exception Rule, Profiles, Novelty Policy

Building More Firewall Policies

- In this exercise you will build 2 new polices : My Policy 2/3
- You will also build an Session Profile for My Policy 1 you just created



Exception Rules



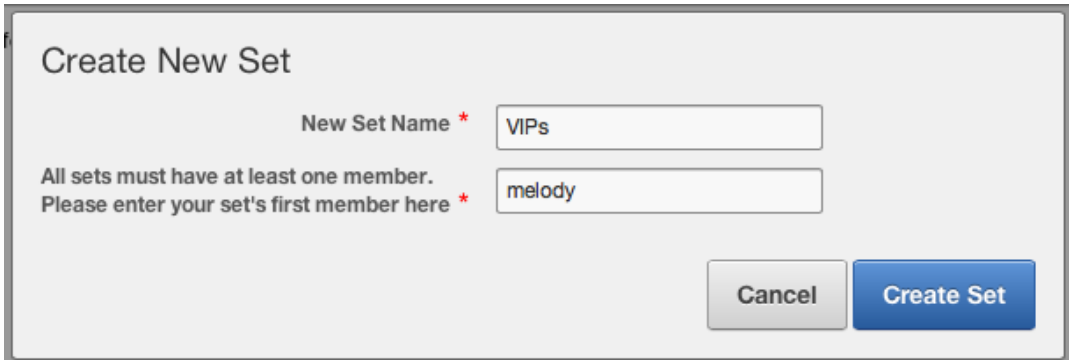
170

Exception Rules

Exclude a new ‘DB User Set’

[Create a database user melody]

- Create another new firewall policy {My Policy **2**}
- At the bottom of the screen click on ‘**Database User Sets**’ > Create New Set
- Name it ‘VIPs’ and put [Melody] here



- Next : apply an enforcement policy to this Set

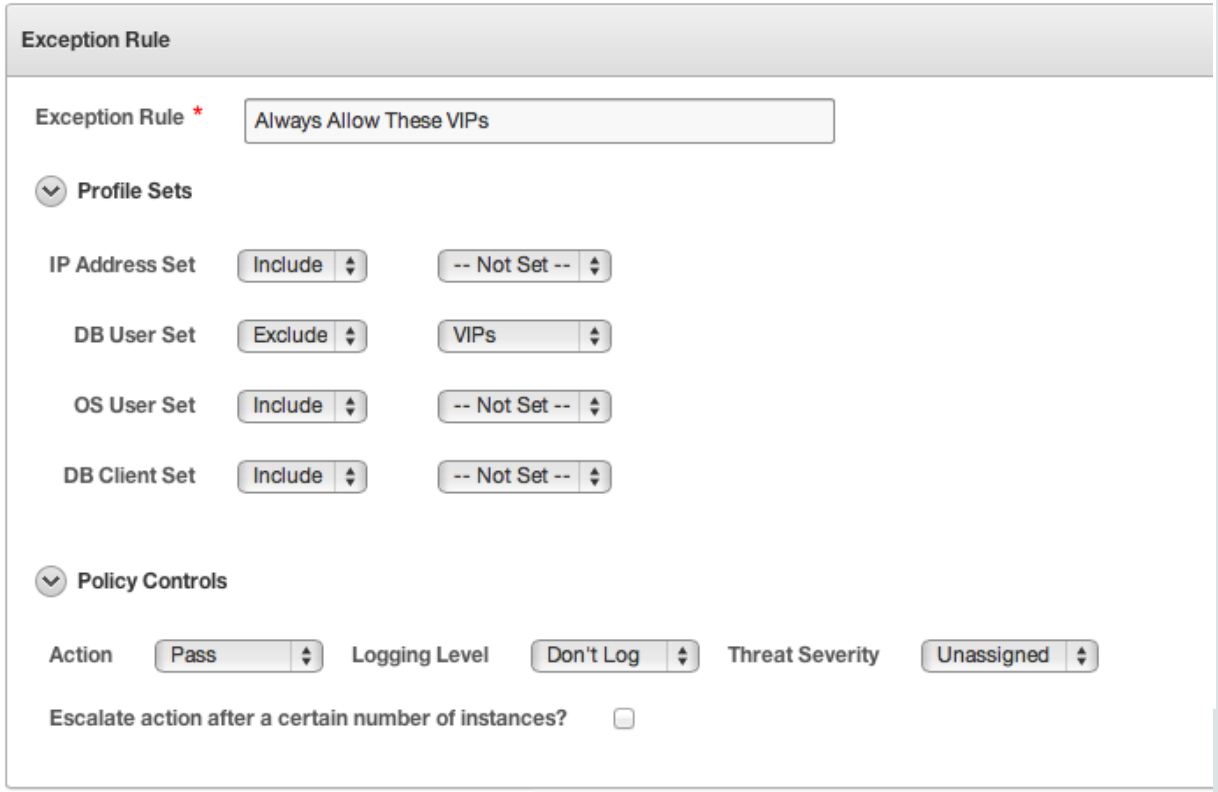
Exception Rules
Exclude a new DB User Set

- Select ‘Add Exception’ button under Exception Rules section

Exception Rule - **Trust But Verify**

- Create an exception rule called Always_Allow_These_VIPs and set the included users with these policy controls :
  - Action: Pass
  - Logging Level: **Log**
  - Threat Severity: Unassigned

Don't forget to Save + Publish Your policy after !

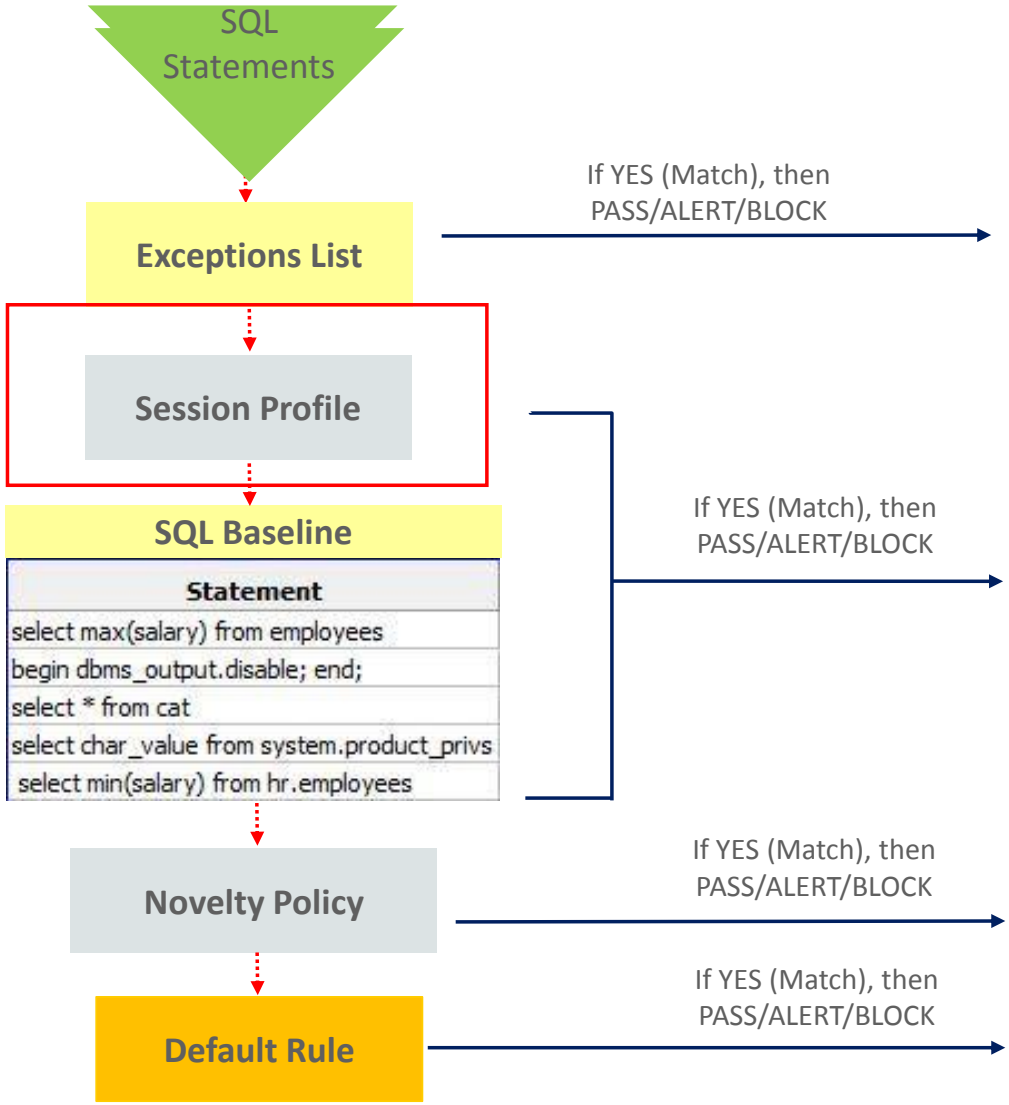


Testing the Firewall Policy

SQLPLUS melody/Manager_1@192.168.56.12:15211/db02.oracle.com

```
[oracle@db02 ~]$ sqlplus melody/Manager_1@192.168.56.12:15211/db02.oracle.com

SQL*Plus: Release 11.2.0.3.0 Production on Tue Dec 9 08:36:39 2014

Copyright (c) 1982, 2011, Oracle.  All rights reserved.


Connected to:
Oracle Database 11g Enterprise Edition Release 11.2.0.3.0 - 64bit Production
With the Partitioning, OLAP, Data Mining and Real Application Testing options

MELODY> select * from hr.jobs;
```

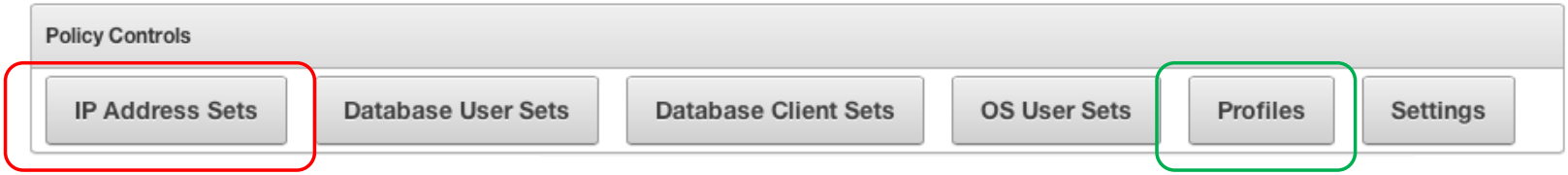
Session Profile



175

Create a New Profile

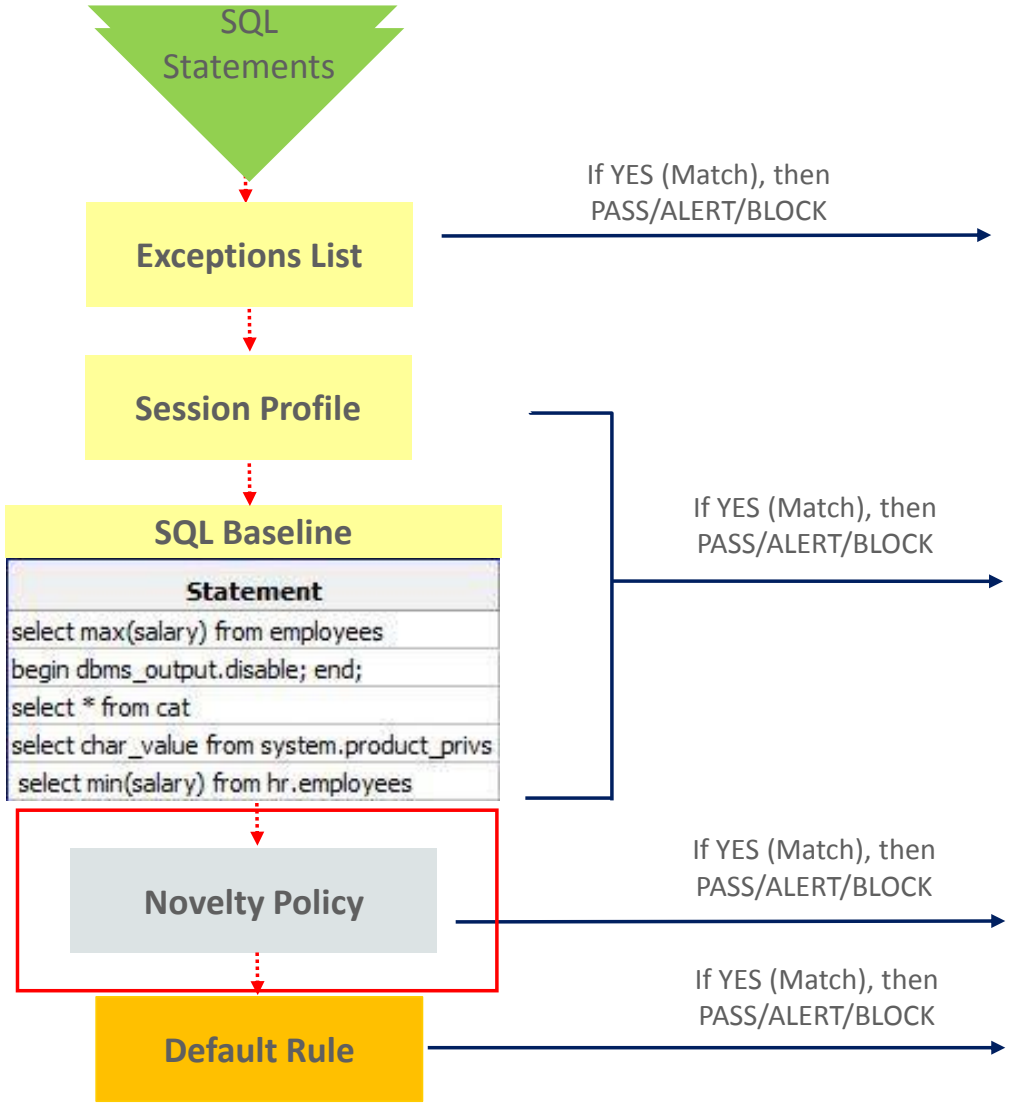
1. Created an allowed IP Address Set :192.168.56.10



2. Define **any** or **all** of above 4 Sets : Select '**Profiles**' with a new name : Profile1
3. Click on the profile and add "good" SQL to the list via **Analyzed SQL**
   - **Be sure to change profile**

4. **Now add "good SQL" to the policy**

Session Profile

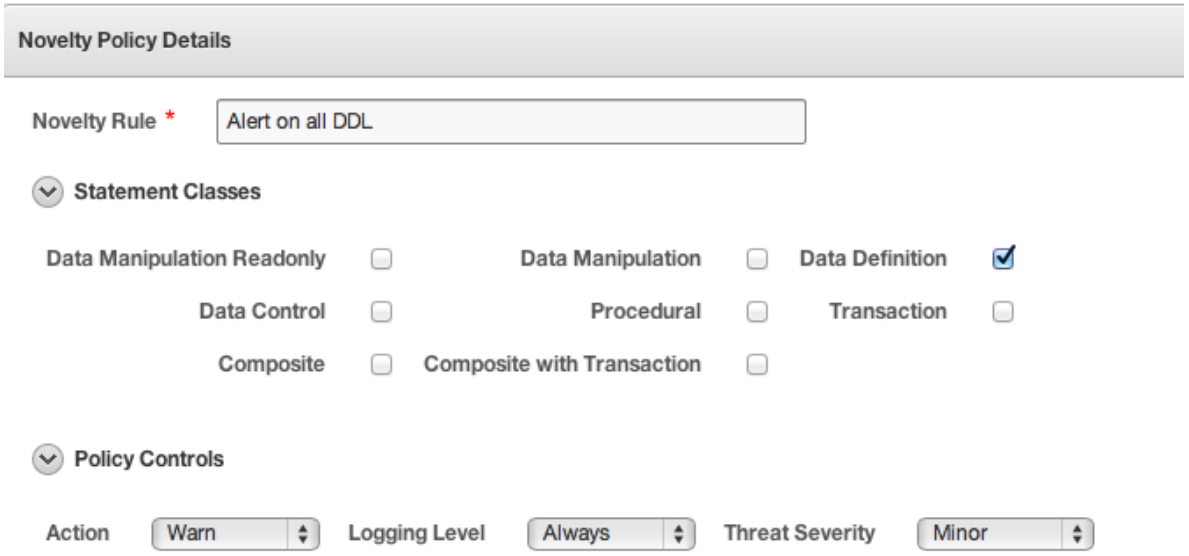


177

Novelty Policy

Alert on All DDLs

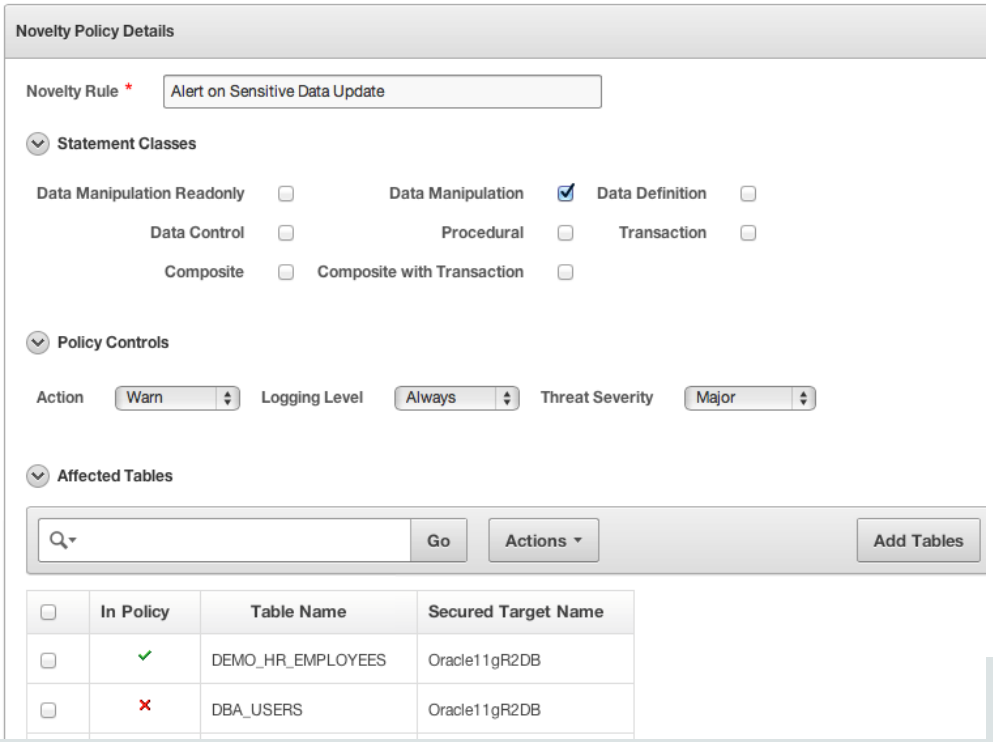
- Create a new policy {My Policy 3}
- Select Novelty Policy and create a new Rule : Alert on All DDLs



Novelty Policy

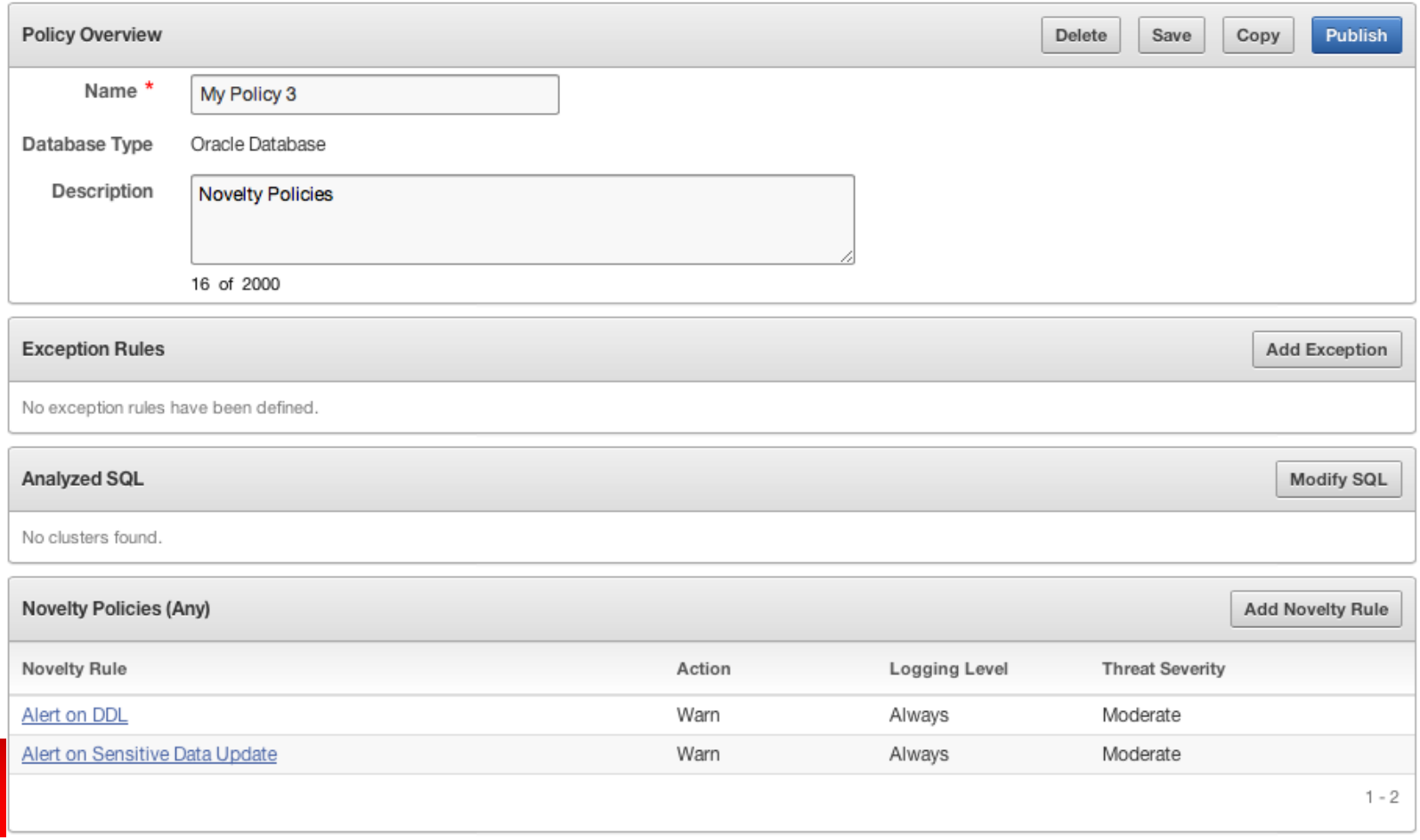
Alert on Sensitive Data Updates

- While in {My Policy 3}
- Select Novelty Policy and create a new Rule : Alert on DML Updates



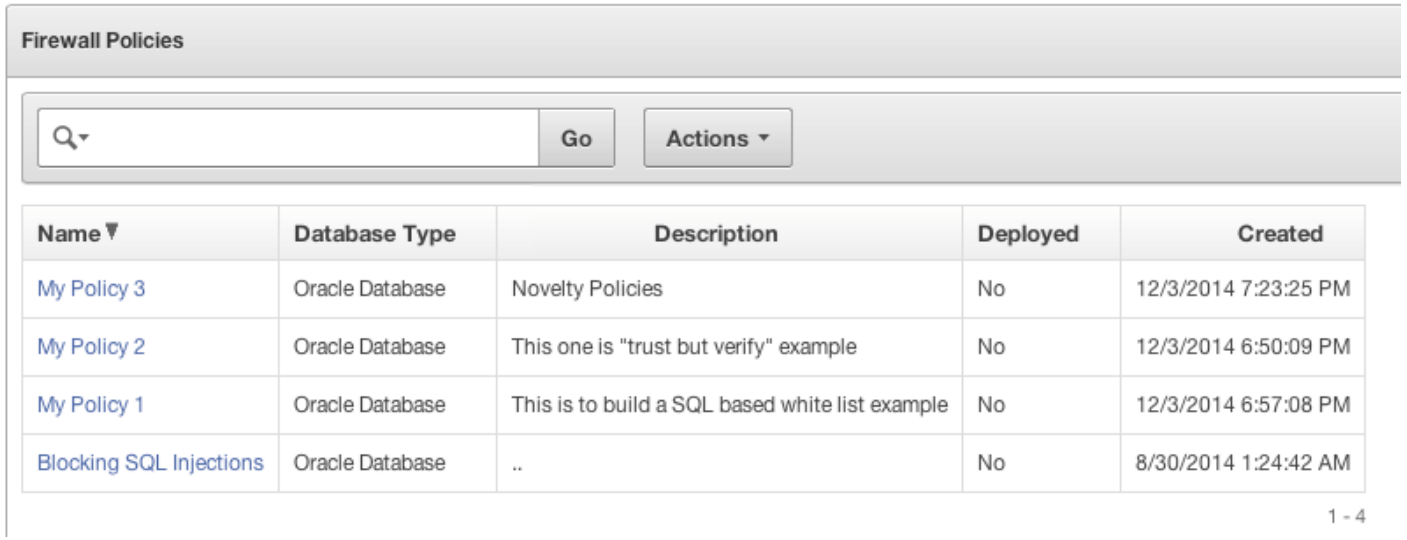
Novelty Policy

2 Rules Defined



Firewall Policies Created

- You start with 1 and added 3



Database Firewall Use Cases

Use Case	Policy & Rule
Real time database activity monitoring	“My policy 1” – passive monitoring
Anomaly detection - Alert on unseen or suspicious events	All policy with alert control
Prevent unexpected SQL statements	“My policy 1” using whitelist
Blocking SQL Injection Threats	“Blocking SQL Injections” Policy
Privileged account monitoring	“My policy 2” -using Exceptions Rule
Alert on unseen or suspicious events	“My policy 3” using Novelty Rule ½ (DDL, sensitive DML)

Database Firewall Use Cases

Dial Up Security Control As Needed

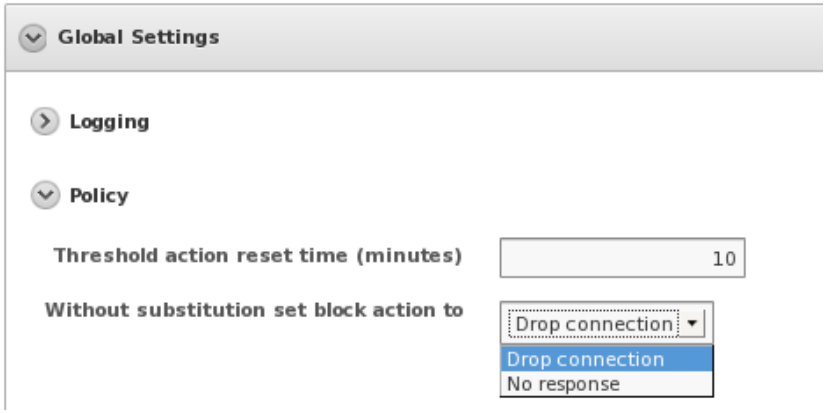
- ✓ Real time database activity monitoring (passive log unique)
- ✓ Privileged account monitoring (Exceptions, Profile)
- ✓ Anomaly detection
  - ✓ Alert on unseen or suspicious events
    - ✓ Whitelist with Profiles approach
    - ✓ Blacklist approach (Novelty Rule, Exceptions)
- ✓ Prevent unexpected SQL statements, users or objects
- ✓ Blocking SQL Injection Threats

Lesson 22

TCP Reset + Sensitive Data Masking

TCP Reset When Blocking Traffic

- While in SQL Injection Blocking Firewall Policy
- Settings > Global Settings > Policy
- Change from No response to ‘Drop connection’ – TCP reset



Sensitive Data Masking (on audited data)

- While within your Firewall Policy
- Settings > Sensitive Data Masking > Add {sensitive table or column}> Save
- Future firewall audit traffic will be masked (see it in your report)
  - UPDATE HR.JOBS SET Max_Salary=0000 WHERE JOB_ID=######;