

# Oracle Audit Vault and Database Firewall

POC Training

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



**SECURITY  
INSIDE  
OUT**

ORACLE®

Copyright © 2014 Oracle and/or its affiliates. All rights reserved. |

# 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

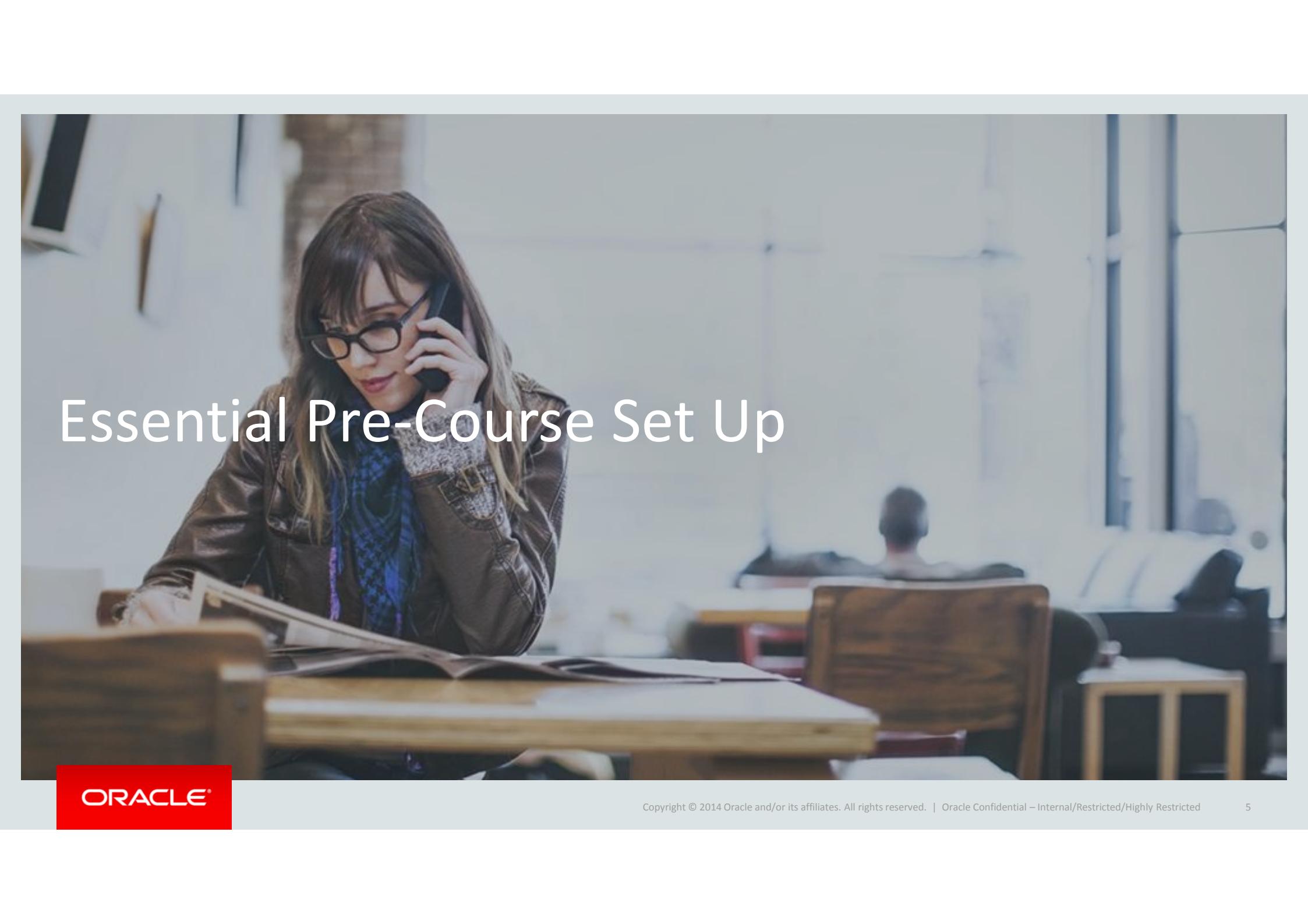
## 1 Lesson 1 – 5

- 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

A photograph of a young woman with long brown hair and glasses, wearing a brown leather jacket over a patterned top. She is sitting at a wooden desk in a library, looking down at an open book. Behind her, other students are seated at their desks. The background shows large windows and bookshelves.

# Essential Pre-Course Set Up

ORACLE®

Copyright © 2014 Oracle and/or its affiliates. All rights reserved. | Oracle Confidential – Internal/Restricted/Highly Restricted

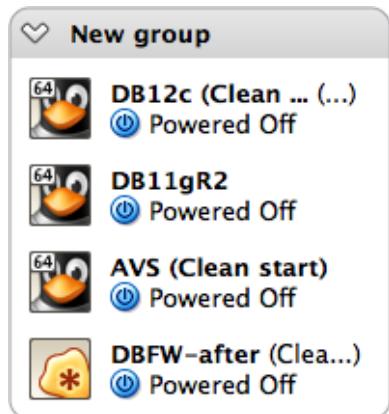
# Environment Requirements

- 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

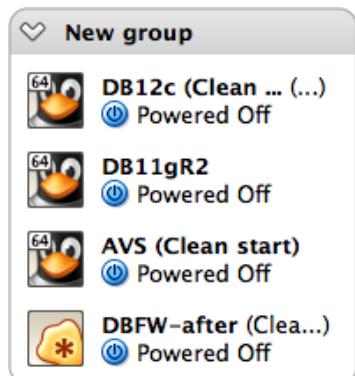
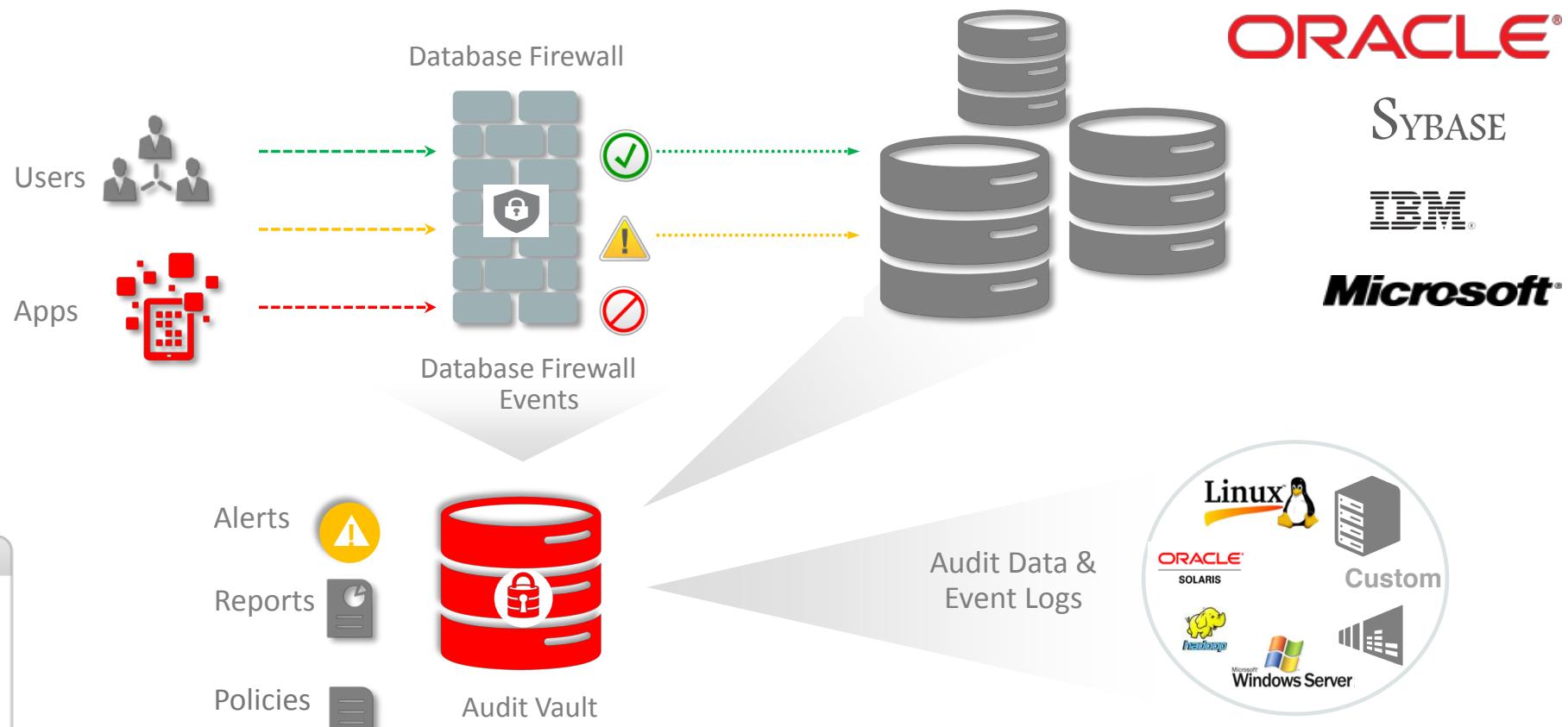
The password for all accounts is **Manager\_1**

**ORACLE®**

**SYBASE**

**IBM®**

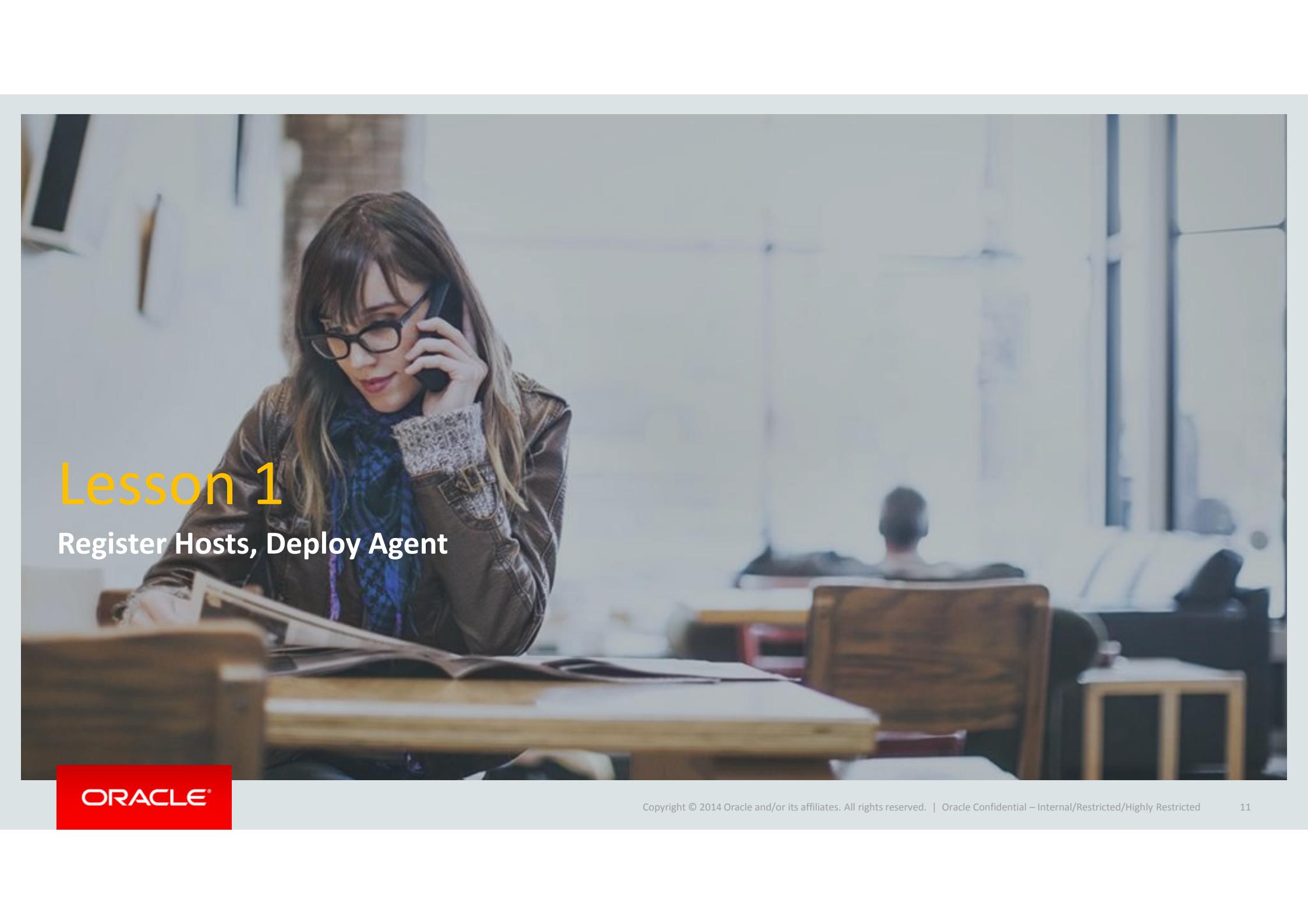
**Microsoft®**



**ORACLE®**

# 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

A photograph of a woman with long brown hair and glasses, wearing a brown leather jacket over a blue patterned top. She is sitting at a wooden desk, looking down at some papers. In the background, there are other people in what appears to be a library or study room.

# Lesson 1

Register Hosts, Deploy Agent

ORACLE®

Copyright © 2014 Oracle and/or its affiliates. All rights reserved. | Oracle Confidential – Internal/Restricted/Highly Restricted

11

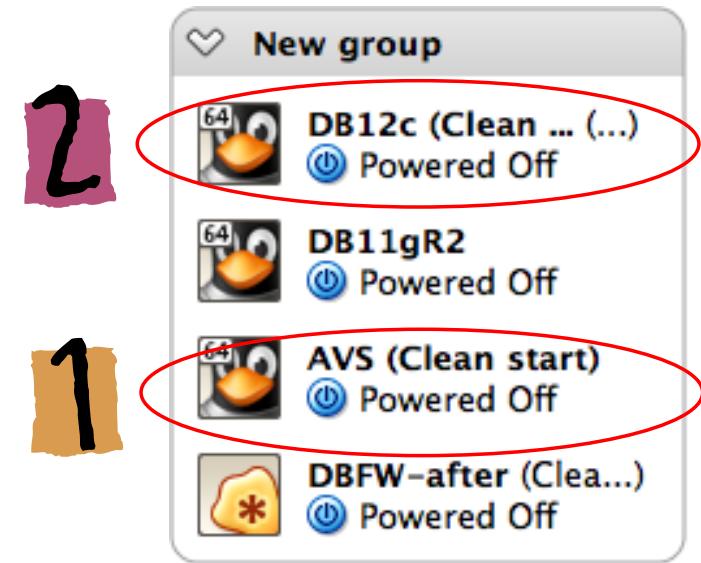
## Lesson Overview

- 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**

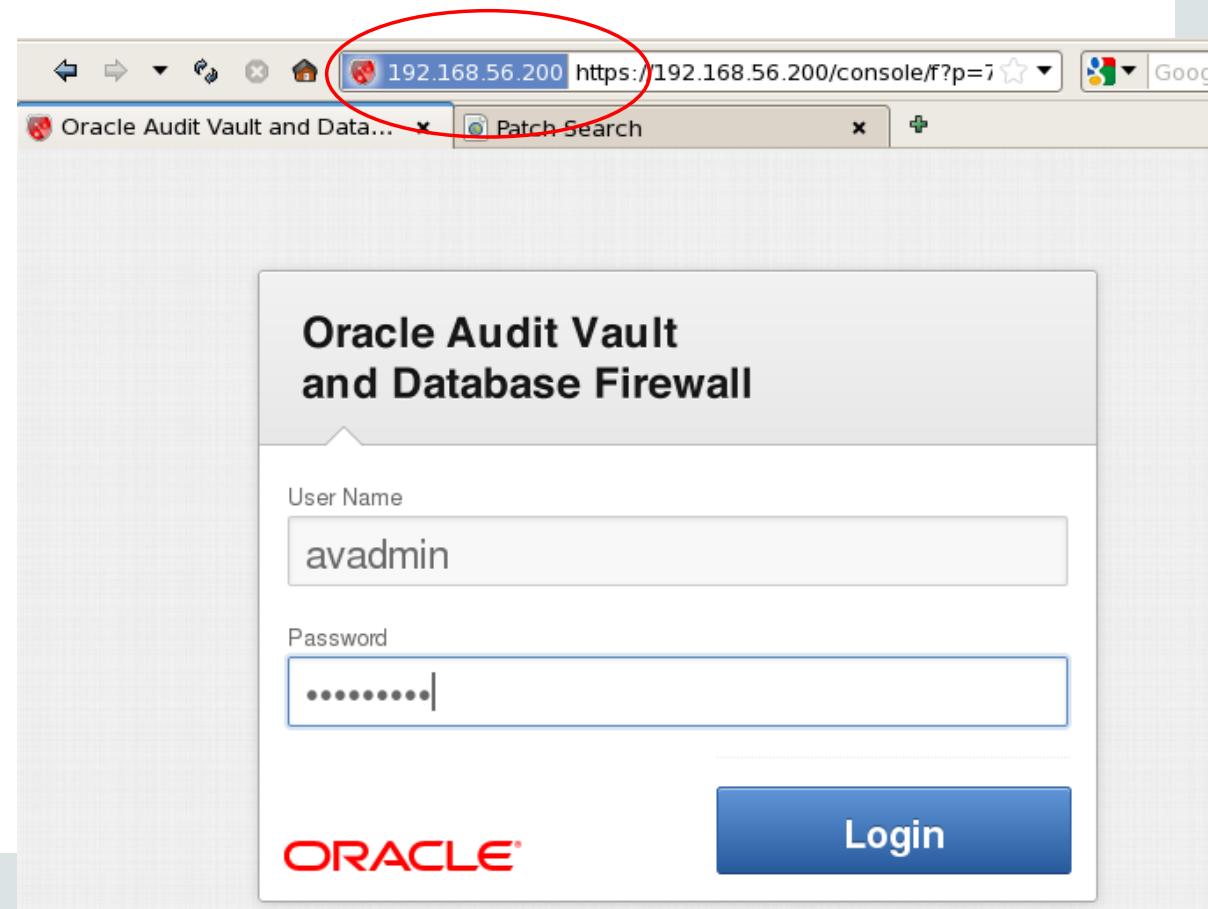


# Log In to AVS Management Console

[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

The screenshot shows the Oracle Audit Vault Server interface. The top navigation bar includes the Oracle logo, user 'avadmin', and links for Help and Logout. Below the navigation bar, a secondary menu bar has tabs for Home, Secured Targets, Firewalls, **Hosts**, Settings, and a search field. The 'Hosts' tab is selected. A breadcrumb trail indicates the current location: Home > Hosts > Register Host. On the left, a sidebar has 'Hosts' selected under the 'Hosts' category. The main content area displays a 'Register Host' dialog box. It contains two input fields: 'Host Name \*' with the value 'HostMachineOf12c' and 'Host IP \*' with the value '192.168.56.101'. There are 'Cancel' and 'Save' buttons at the bottom right of the dialog. At the bottom of the page, there is an Oracle logo and copyright information: Copyright © 2014 Oracle and/or its affiliates. All rights reserved. | Oracle Confidential – Internal/Restricted/Highly Restricted.

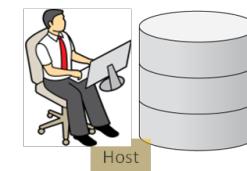
Hosts								Activate	Deactivate	Delete	Register	
								Actions ▾				
<input type="checkbox"/>	Host Name	Host IP	Agent Status	Agent Version	Agent Activation Key	Agent Activation Time	Agent Location	Platform				
<input type="checkbox"/>	HostMachineOf12c	192.168.56.101	Activated		WT29-W60E-KOY0-LPK0-O186	12/1/2014 2:08:36 PM						
<input type="checkbox"/>	Oracle11gR2	192.168.56.10	Unreachable	Release 12.1.2.0.0 (2014-07-17 22:39:56.652 +0000)	L0Q2-21OO-EA9J-SSIG-1F6A	7/17/2014 3:34:02 PM	/home/oracle /app/oracle/product /avagent	Linux x86-64				

# 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]$
```

Hosts										<a href="#">Activate</a>	<a href="#">Deactivate</a>	<a href="#">Delete</a>	<a href="#">Register</a>
	Host Name ▲	Host IP	Agent Status	Agent Version	Agent Activation Key	Agent Activation Time	Agent Location	Platform		Actions ▾	Go	Search	
<input type="checkbox"/>	HostMachineOf12c	192.168.56.101	Activated		WT29-W60E-KOY0-LPK0-O186	12/1/2014 2:08:36 PM							
<input type="checkbox"/>	Oracle11gR2	192.168.56.10	Unreachable	Release 12.1.2.0.0 (2014-07-17 22:39:56.652 +0000)	L0Q2-21OO-EA9J-SSIG-1F6A	7/17/2014 3:34:02 PM	/home/oracle /app/oracle/product /avagent	Linux x86-64					

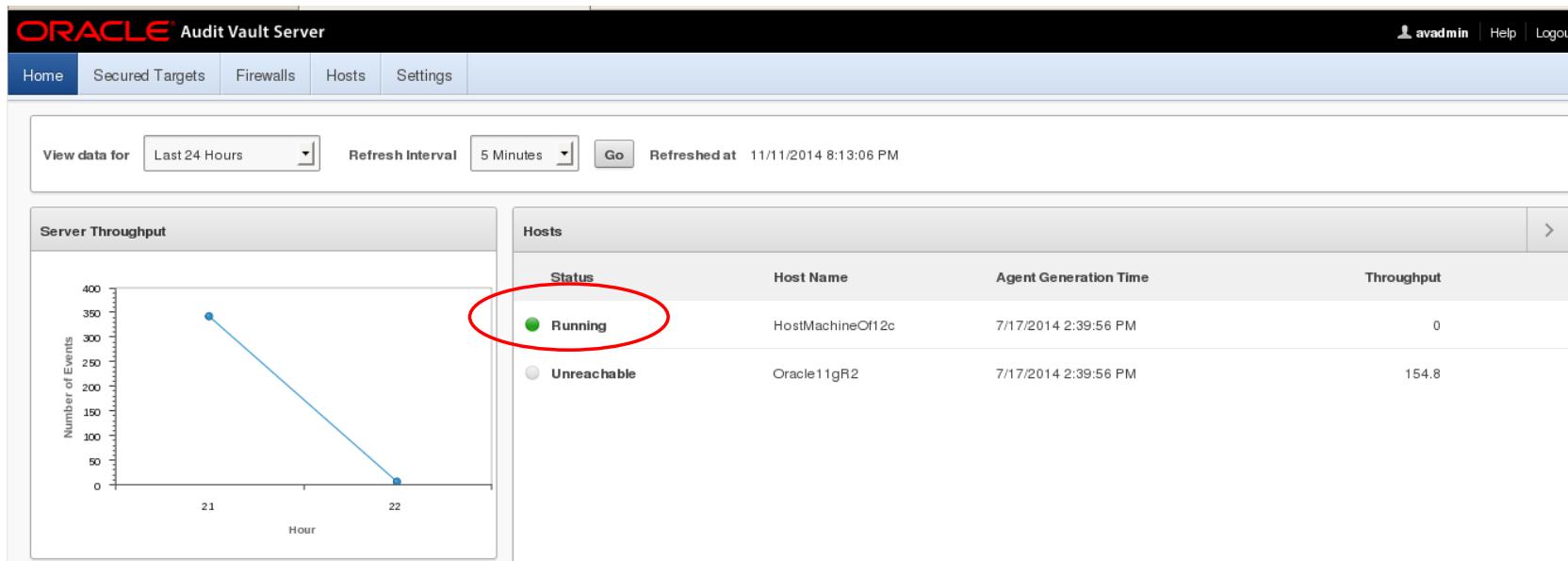
Obtain the key from Hosts page

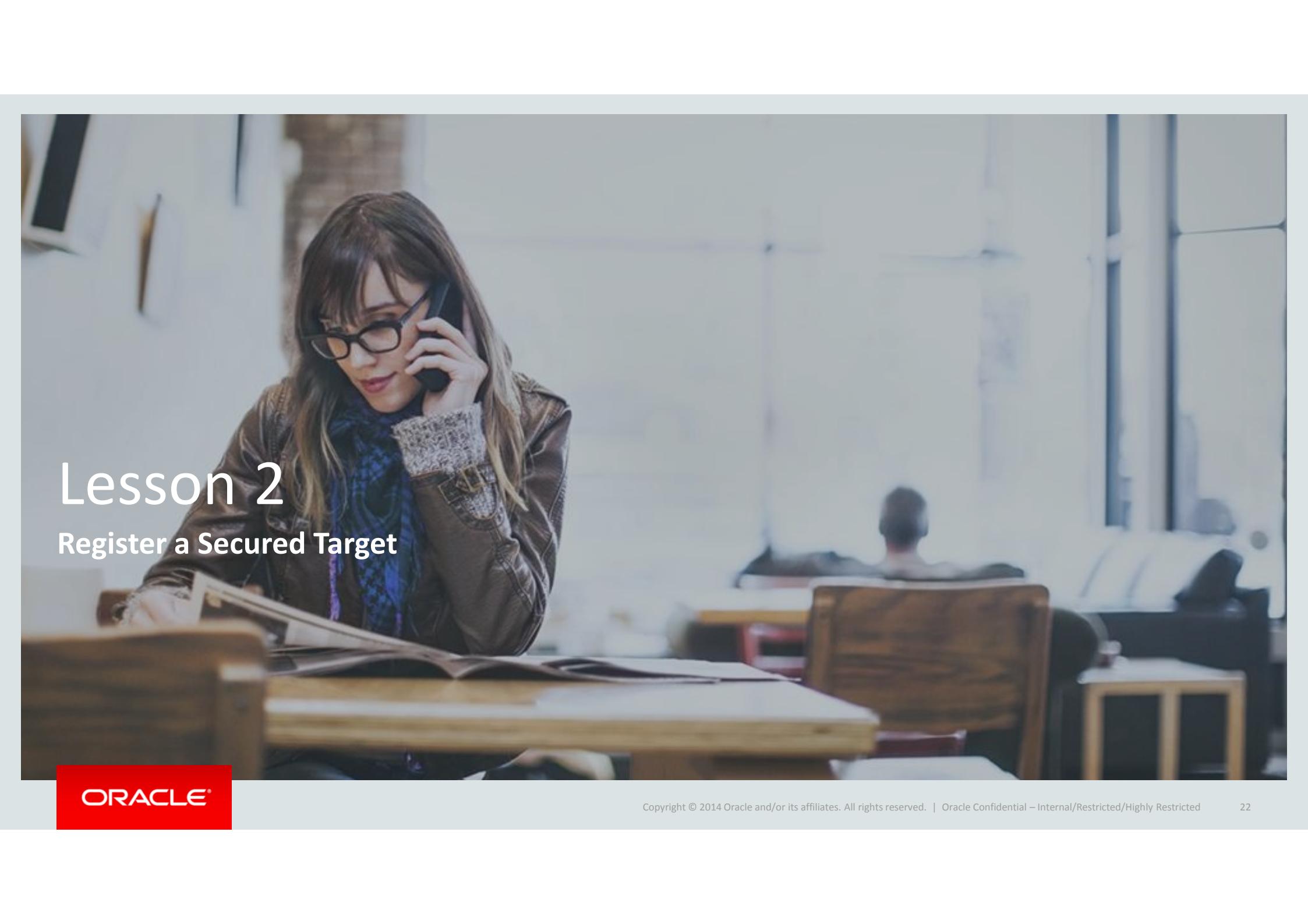
Hosts										<a href="#">Activate</a>	<a href="#">Deactivate</a>	<a href="#">Delete</a>	<a href="#">Register</a>
	Host Name ▲	Host IP	Agent Status	Agent Version	Agent Activation Key	Agent Activation Time	Agent Location	Platform		Actions ▾	Go	Search	
<input type="checkbox"/>	HostMachineOf12c	192.168.56.101	Running	Release 12.1.2.0.0 (2014-07-17 22:39:56.652 +0000)	WT29-W60E-KOY0-LPK0-O186	12/1/2014 2:08:36 PM	/u01/app/oracle /product/avagent	Linux x86-64					
<input type="checkbox"/>	Oracle11gR2	192.168.56.10	Unreachable	Release 12.1.2.0.0 (2014-07-17 22:39:56.652 +0000)	L0Q2-21OO-EA9J-SSIG-1F6A	7/17/2014 3:34:02 PM	/home/oracle /app/oracle/product /avagent	Linux x86-64					

ORACLE®

# Installing Agent

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



A photograph of a woman with long brown hair and glasses, wearing a brown leather jacket over a blue patterned top. She is sitting at a wooden desk, holding a black telephone receiver to her ear with her right hand. Her left hand is resting on a stack of papers or books on the desk. In the background, there is a window with a view of a city skyline, and another person is visible sitting at a desk further back.

# Lesson 2

## Register a Secured Target

ORACLE®

Copyright © 2014 Oracle and/or its affiliates. All rights reserved. | Oracle Confidential – Internal/Restricted/Highly Restricted

22

# 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 options
```

```
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 options
```

```
[oracle@lap-db12102 config]$
```

# Register 12c Database Secured Target

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

Register Secured Target

New Secured Target Name \*

Description

Secured Target Type \*

Add Secured Target Location

Basic  Advanced

Host Name / IP Address \*

Port \*

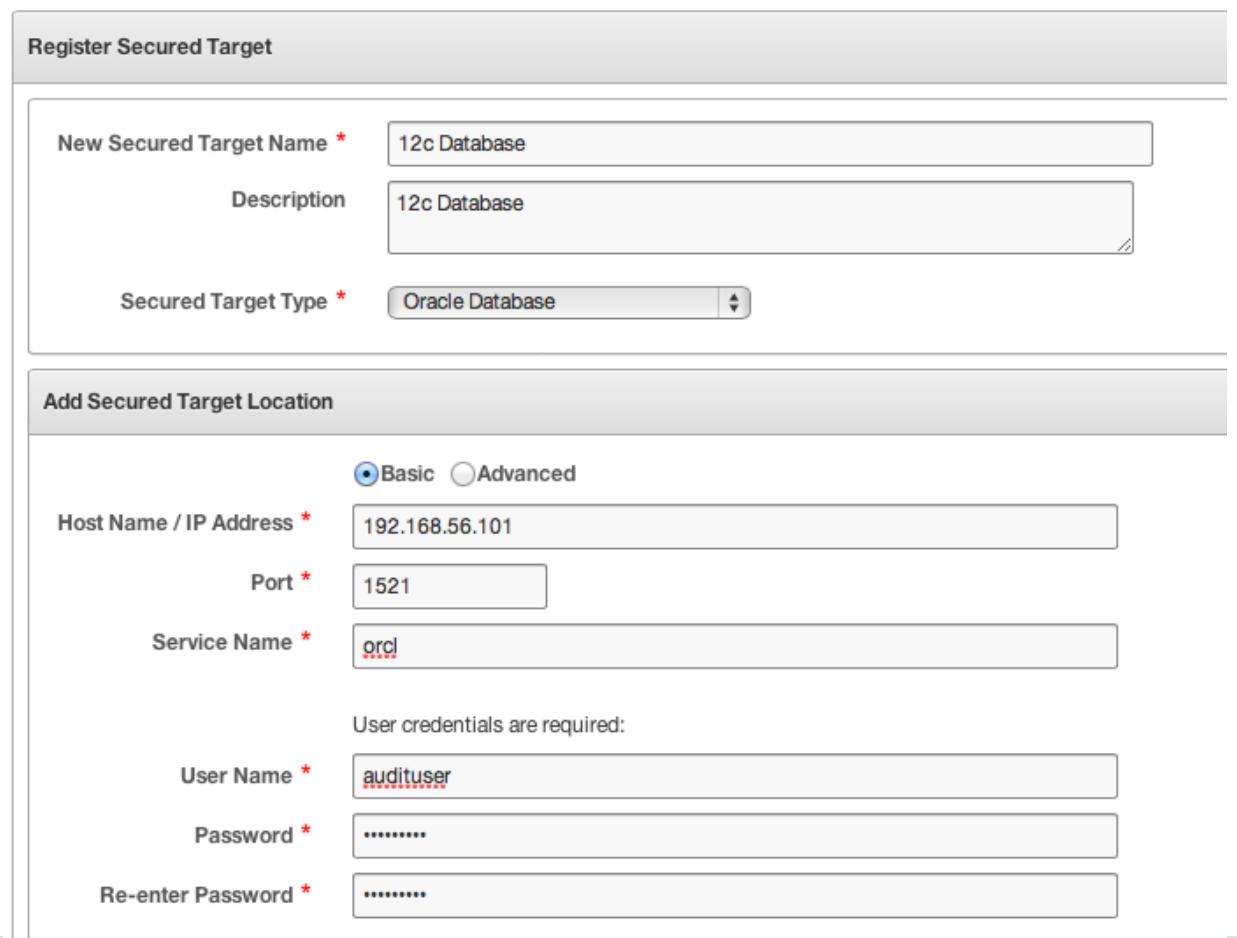
Service Name \*

User credentials are required:

User Name \*

Password \*

Re-enter Password \*



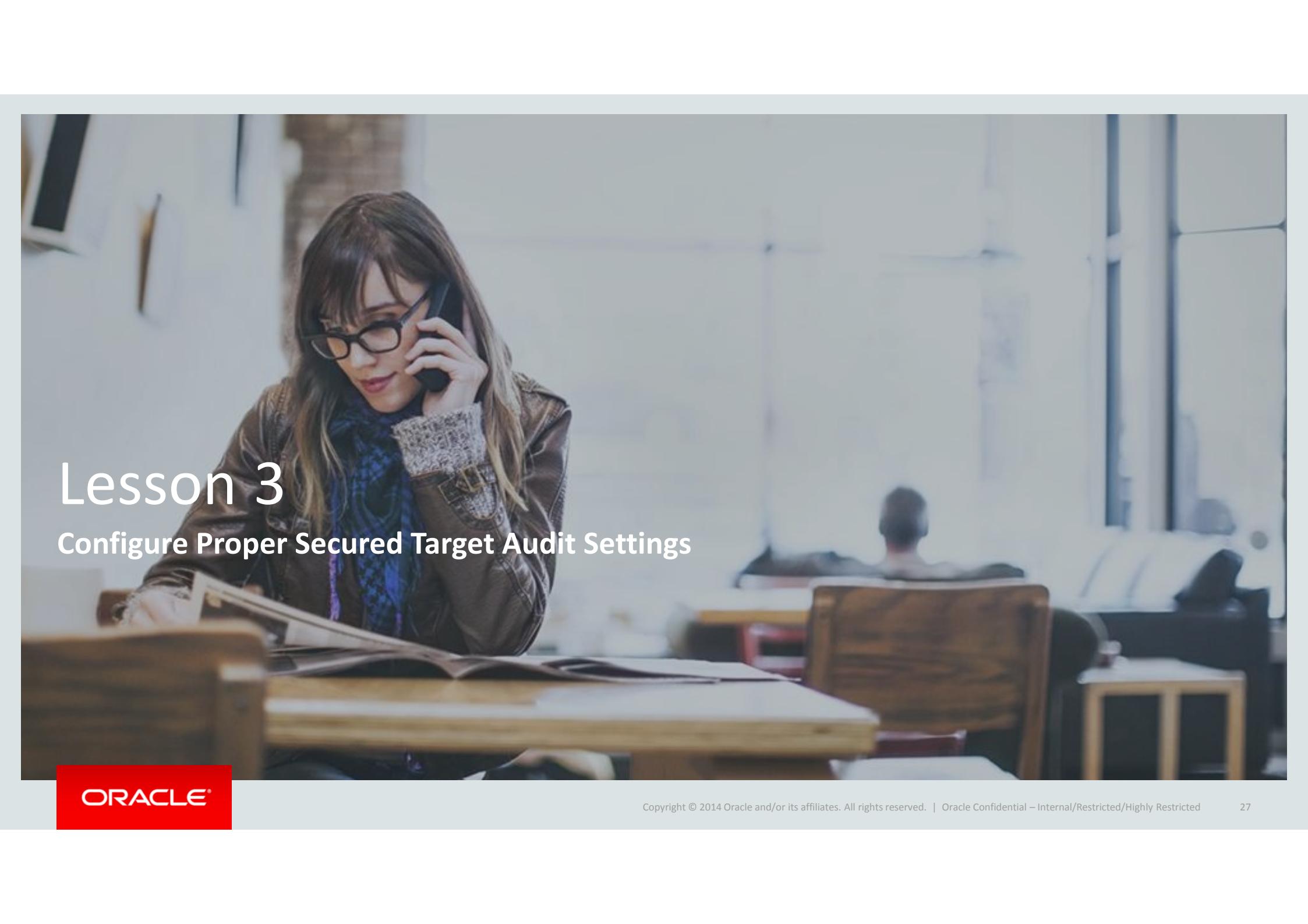
# Register 12c Database Secured Target - continued

## Optional Step

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

Modify Collection Attributes

Attribute Name	Attribute Value	Add	Remove
<input type="checkbox"/> AV.COLLECTOR.CHPNTPWINDOW	8760	Add	Remove



# Lesson 3

## Configure Proper Secured Target Audit Settings

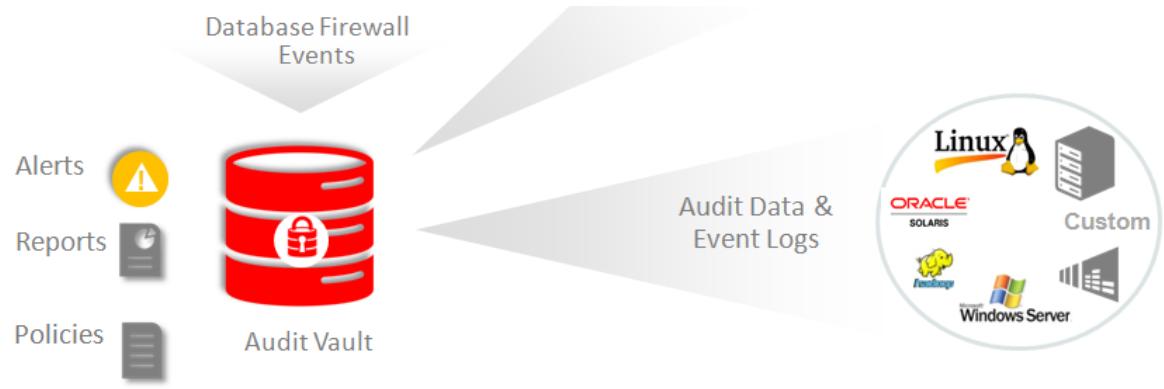
ORACLE®

Copyright © 2014 Oracle and/or its affiliates. All rights reserved. | Oracle Confidential – Internal/Restricted/Highly Restricted

27

# 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**

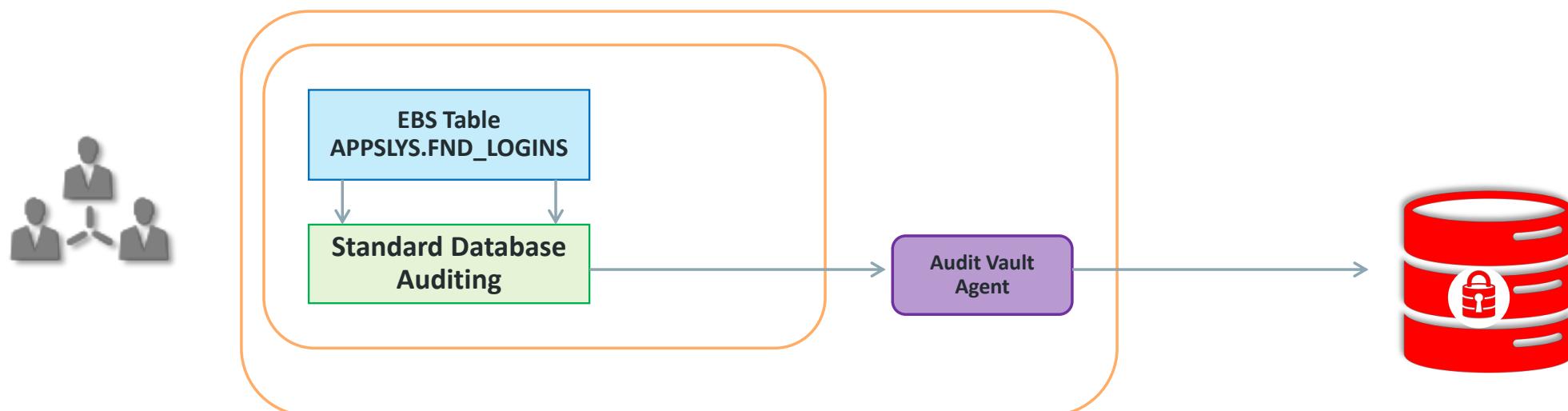
## *4. Audit privileged accounts*

```
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

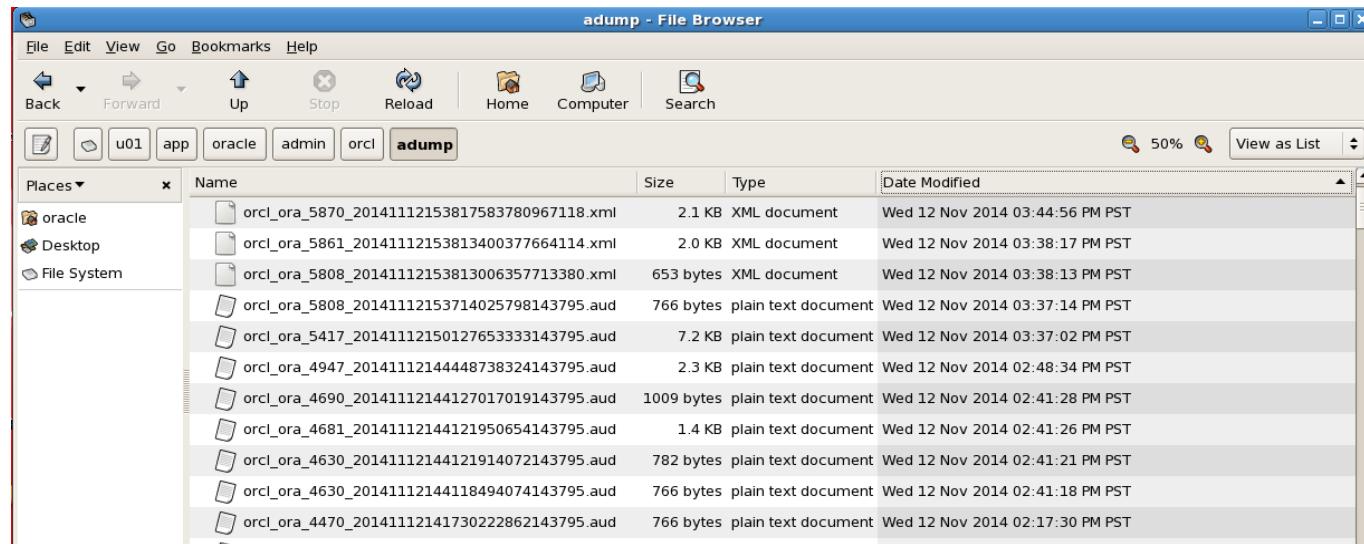
- Sqlplus / as sysdba
- Show parameter audit
- *alter system set audit\_trail=XML, EXTENDED audit\_sys\_operations=true scope=spfile;*
- Shutdown immediate;
- Startup;

```
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

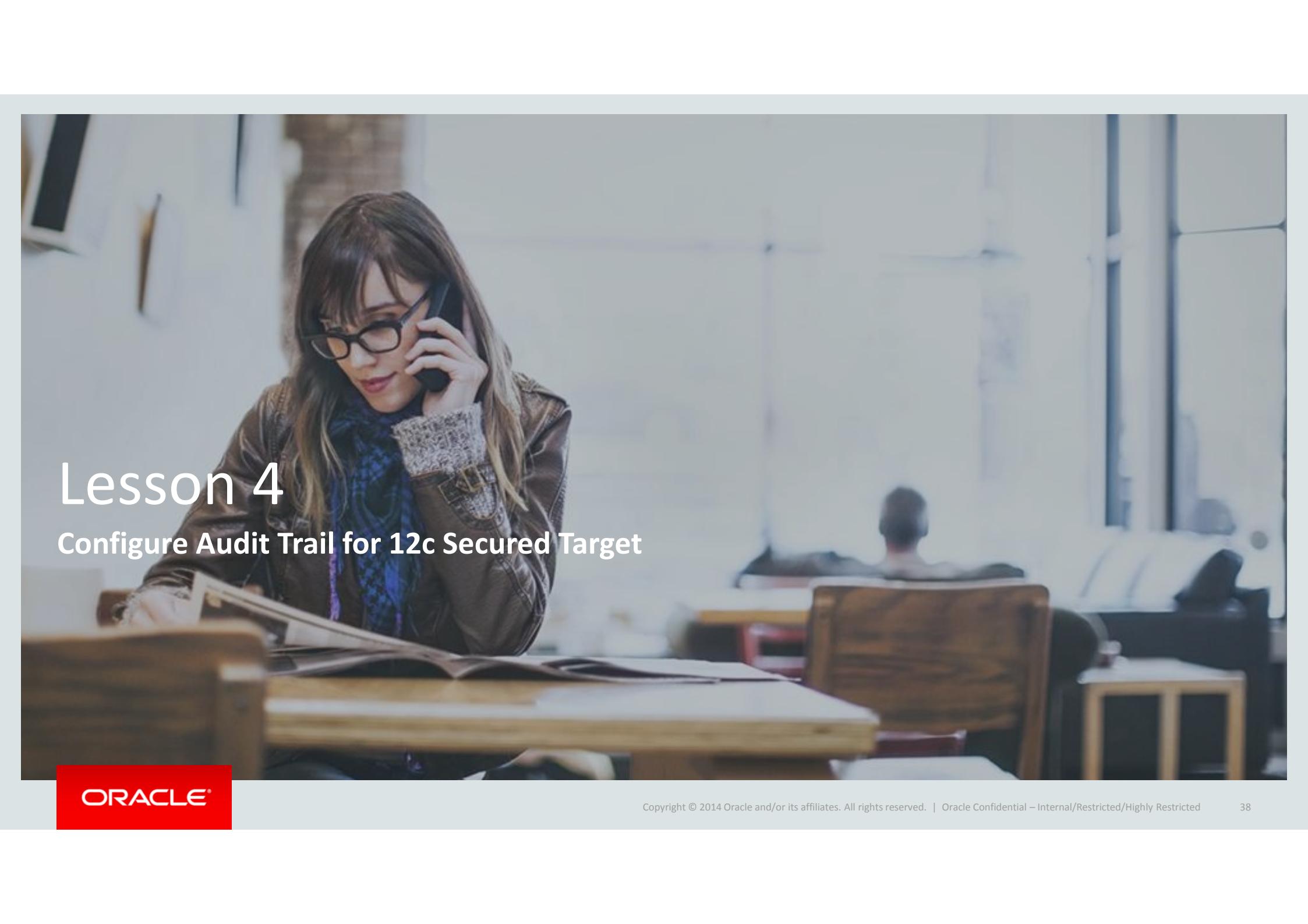
- XML files will show up in `/u01/app/oracle/admin/orcl/adump` directory



*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]

A photograph of a woman with long brown hair and glasses, wearing a brown leather jacket over a blue patterned top. She is sitting at a wooden desk, looking down at some papers. In the background, there are other people in what appears to be a library or study area.

# 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

The screenshot shows the 'Add Audit Trail' dialog box. It contains the following fields:

- Audit Trail Type: DIRECTORY
- Collection Host: HostMachineOf12c
- Secured Target: 12c Database
- Trail Location: /u01/app/oracle/admin/orcl/adump
- Collection Plug-in: com.oracle.av.plugin.oracle

At the top right of the dialog are 'Cancel' and 'Save' buttons.

# 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

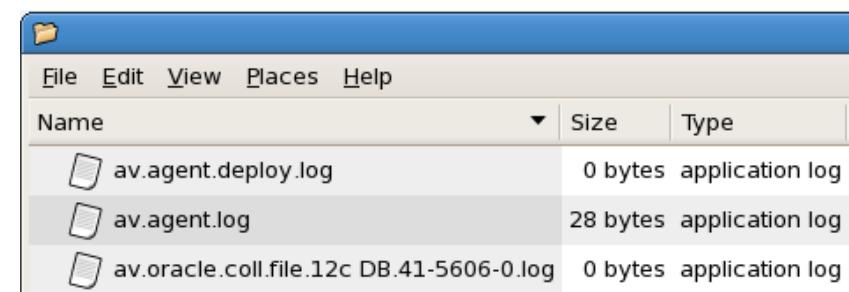
Audit Trails						
		Actions				
<input type="checkbox"/>	Collection Status	Collection Host	Trail Location	Audit Trail Type	Secured Target Name	Secured Target Type
<input type="checkbox"/>		HostMachineOf12c	/u01/app/oracle/admin/orcl/adump	DIRECTORY	12c Database	Oracle Database
<input type="checkbox"/>		HostMachineOf12c	/var/log/audit/audit.log	DIRECTORY	Linux Operating System	Linux
<input type="checkbox"/>		Oracle11gR2	SYS.AUD\$	TABLE	Oracle11gR2DB	Oracle Database
<input type="checkbox"/>		Oracle11gR2	/u01/app/oracle/admin/db02/adump	DIRECTORY	Oracle11gR2DB	Oracle Database

## 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

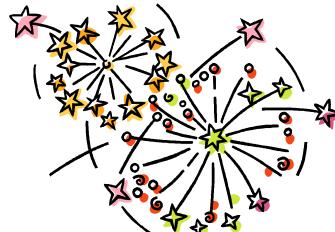
# Register Secured Targets Troubleshooting

- 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

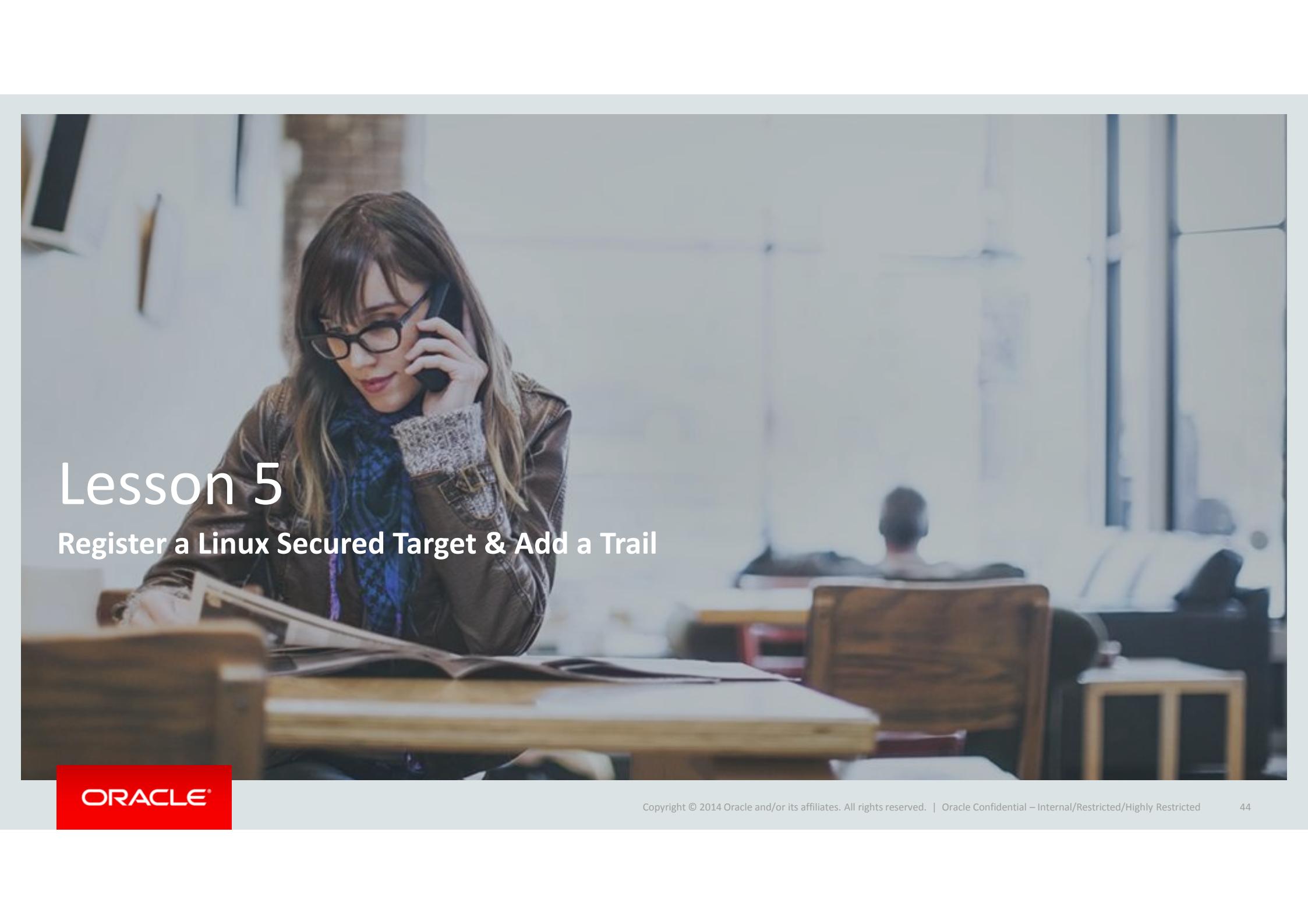


Name	Size	Type
av.agent.deploy.log	0 bytes	application log
av.agent.log	28 bytes	application log
av.oracle.coll.file.12c DB.41-5606-0.log	0 bytes	application log

You are done with 12c secured target.



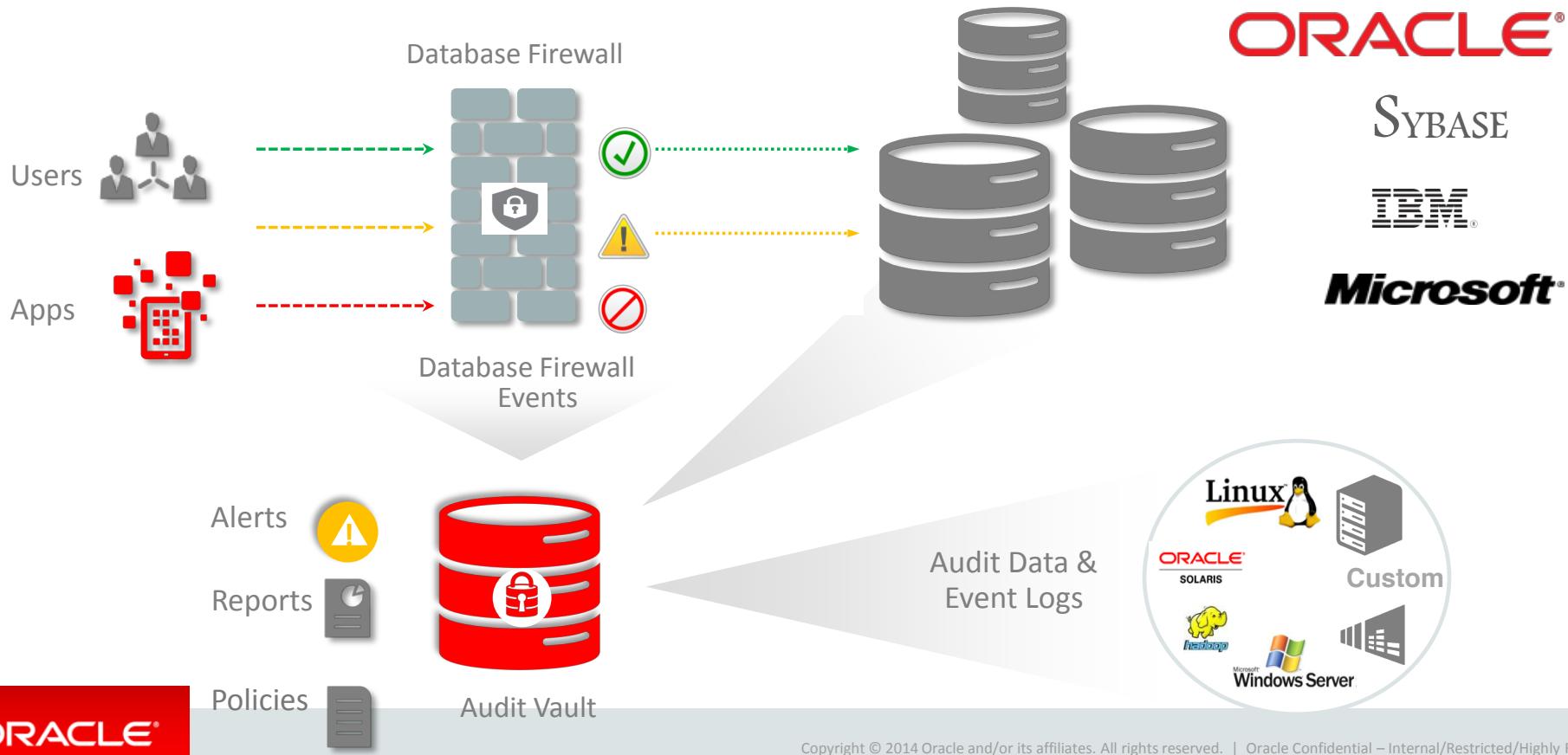
*Now let's go register a Linux secured target.*

A photograph of a young woman with long brown hair and glasses, wearing a brown leather jacket over a blue patterned top. She is sitting at a wooden desk in what appears to be a library or study room, looking down at some papers or books. In the background, other people are seated at desks, and large windows are visible.

# 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

Register Secured Target

New Secured Target Name \*

Description

Secured Target Type \*

## Add Secured Target Location

Host Name / IP Address \*

# Add a Trail

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

Add Audit Trail

Audit Trail Type \* DIRECTORY

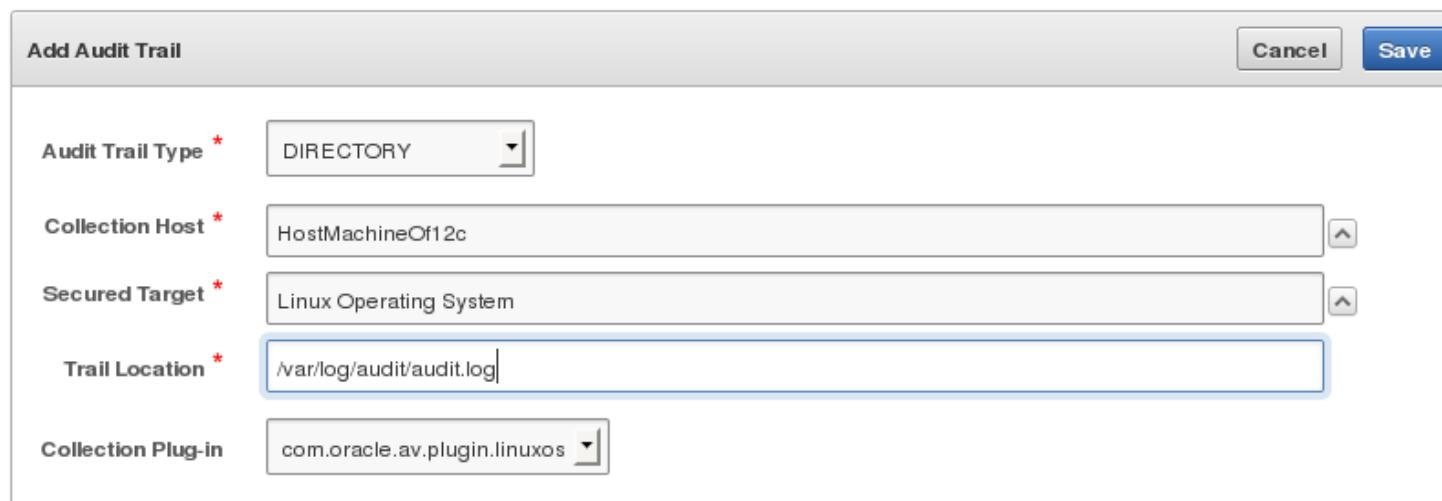
Collection Host \* HostMachineOf12c

Secured Target \* Linux Operating System

Trail Location \* /var/log/audit/audit.log

Collection Plug-in com.oracle.av.plugin.linuxos

Cancel Save



# Start the Newly Added Linux Trail

Audit Trails						
				Actions ▾		
<input type="checkbox"/>	Collection Status	Collection Host	Trail Location	Audit Trail Type	Secured Target Name ▲	Secured Target Type
<input type="checkbox"/>	⬆️	HostMachineOf12c	/u01/app/oracle/admin /orcl/adump	DIRECTORY	12c Database	Oracle Database
<input type="checkbox"/>	⬆️	HostMachineOf12c	/var/log/audit/audit.log	DIRECTORY	Linux Operating System	Linux
<input type="checkbox"/>	⬇️	Oracle11gR2	SYS.AUD\$	TABLE	Oracle11gR2DB	Oracle Database
<input type="checkbox"/>	⬇️	Oracle11gR2	/u01/app/oracle/admin /db02/adump	DIRECTORY	Oracle11gR2DB	Oracle Database

1 - 4

# 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

The screenshot shows the Oracle Audit Vault Server web interface. The top navigation bar includes links for Home, Secured Targets (which is the active tab), Firewalls, Hosts, and Settings, along with user authentication (avadmin) and navigation links (Help, Logout). The left sidebar contains links for Secured Targets (Targets, Groups, Access Rights), Monitoring (Audit Trails), and Enforcement Points (Enforcement Points). The main content area is titled "Secured Targets" and displays a list of targets with columns for Name, Type, Description, and Connect String. The list includes:

	Name	Type	Description	Connect String
<input type="checkbox"/>	12cDatabase	Oracle Database	192.168.56.101 - 12c database	jdbc:oracle:thin:@//192.168.56.101:1521/orcl
<input type="checkbox"/>	Linux Operating System	Linux	linux on 192.168.56.101	192.168.56.101
<input type="checkbox"/>	LinuxOS	Linux	Linux on 192.168.56.10	192.168.56.10
<input type="checkbox"/>	Oracle11gR2DB	Oracle Database	192.168.56.10 - 11gR2 DB resides	jdbc:oracle:thin:@//192.168.56.10:1521/db02.oracle.com

Pagination at the bottom right indicates 1 - 4.

# 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

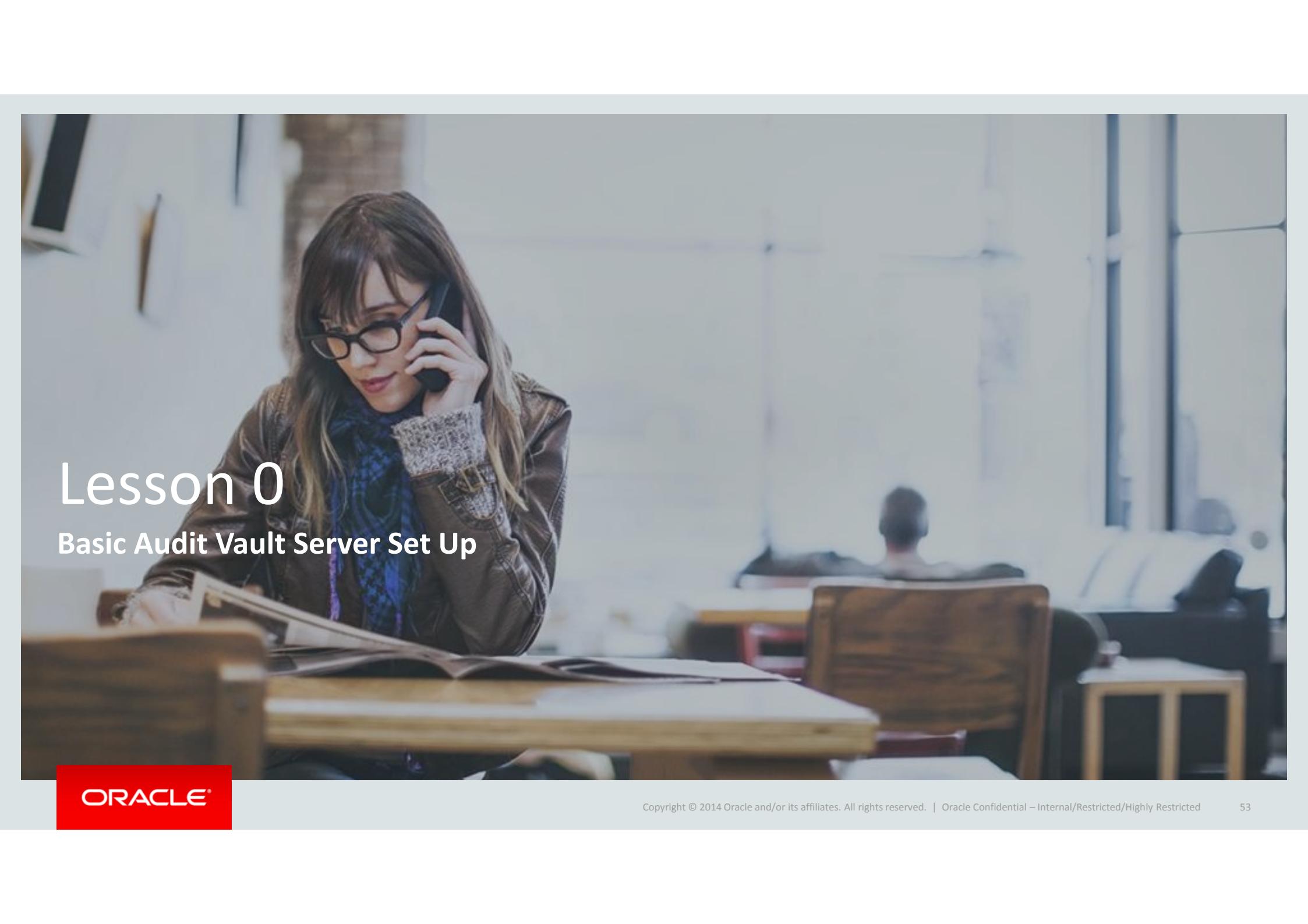
Audit Trails

Start Stop Delete Add

Go Actions ▾

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

1 - 8



# Lesson 0

## Basic Audit Vault Server Set Up

ORACLE®

Copyright © 2014 Oracle and/or its affiliates. All rights reserved. | Oracle Confidential – Internal/Restricted/Highly Restricted

53

# 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

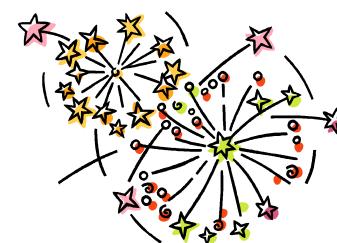
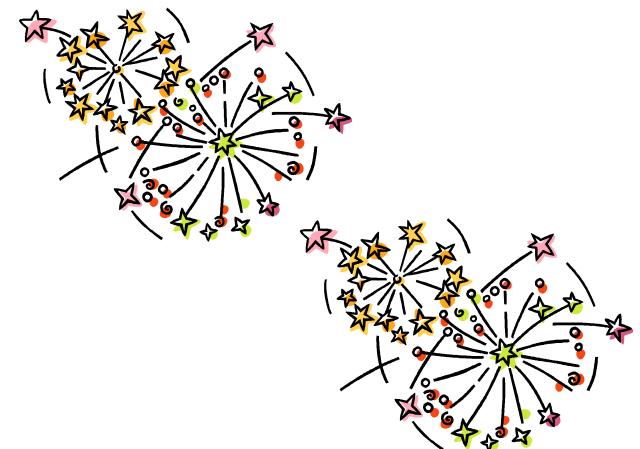
[this is already done for you]

# Setting Up Audit Vault Server

- Enable all services :
  - DNS (not using this during the class)
  - Web GUI
  - SSH console access
  - SNMP access
- In POC, further lock down access by specifying IP addresses

[this is already done for you]

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

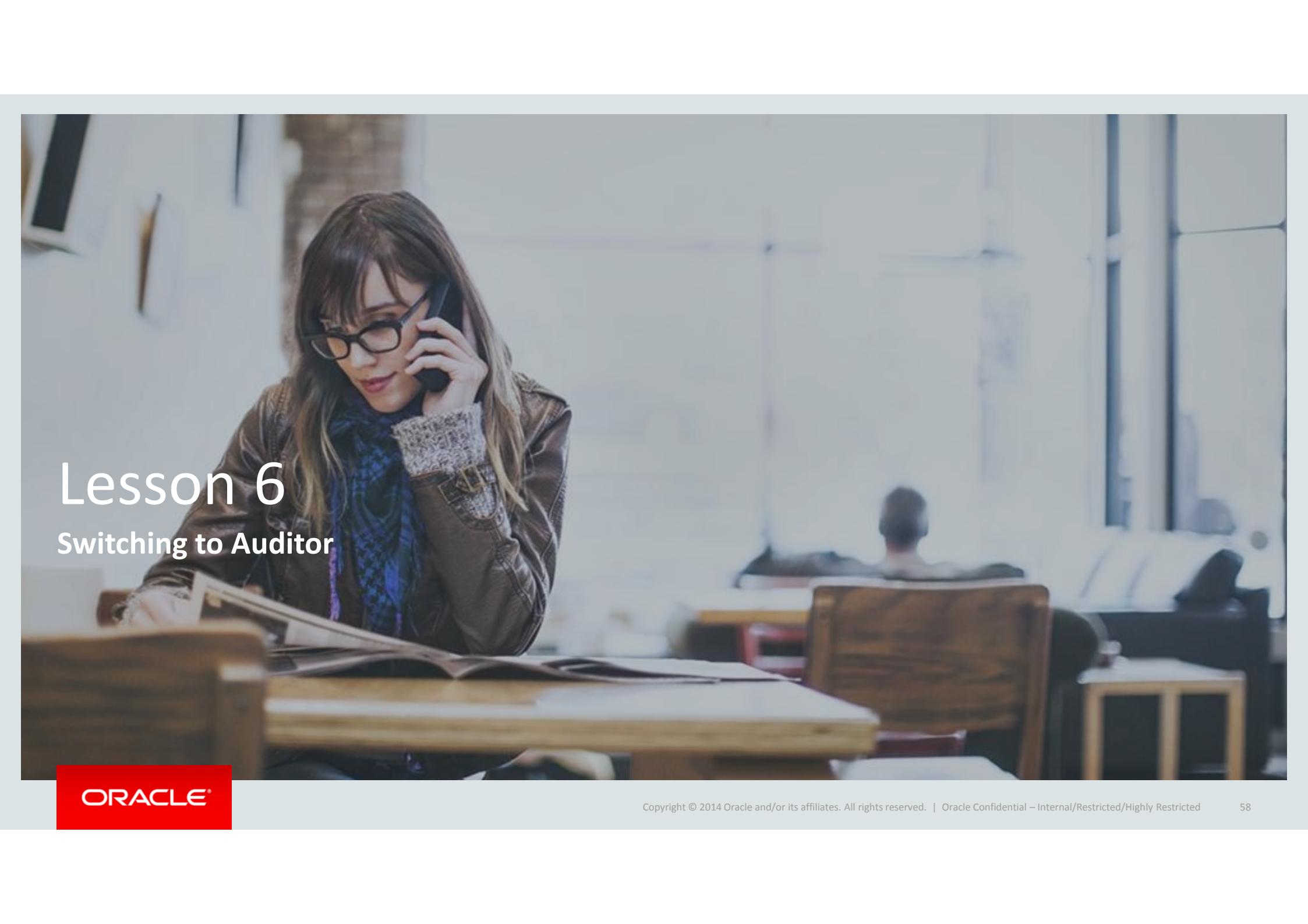


# Program Agenda

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



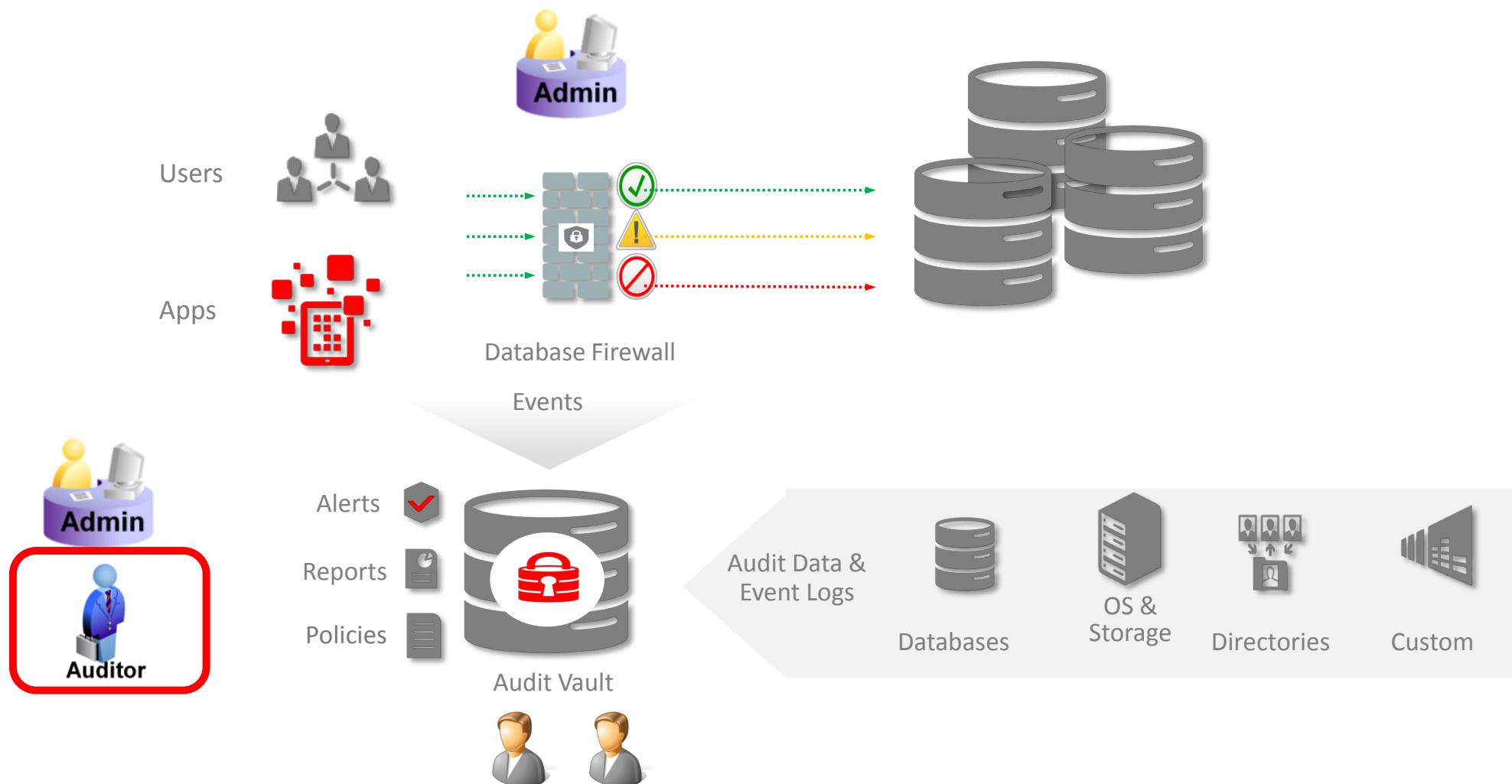
# Lesson 6

## Switching to Auditor

ORACLE®

Copyright © 2014 Oracle and/or its affiliates. All rights reserved. | Oracle Confidential – Internal/Restricted/Highly Restricted

58



# 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

The screenshot shows the ORACLE Audit Vault Server interface. The top navigation bar includes links for Home, Secured Targets, Reports, Policy, and Settings, with Settings being the active tab. Below the navigation is a breadcrumb trail: Home > Settings > Create Auditor. On the left, a sidebar under the heading 'Security' lists Manage Auditors, Manage Access, and Change Password. Under 'Notifications', it lists Distribution Lists and Email Templates. A red banner at the bottom left contains the word 'ORACLE'. The main content area displays a 'Create Auditor' dialog box with fields for User Name (AVAUDITOR\_PCI), Password (redacted), Re-type Password (redacted), and Type (Auditor). Buttons for Cancel and Save are at the top right of the dialog.

# 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**

The screenshot shows the ORACLE Audit Vault Server interface. The top navigation bar includes Home, Secured Targets, Reports, Policy, Settings, and a user dropdown (avauditor). The left sidebar has links for Security, Manage Auditors (selected), Manage Access, Change Password, Notifications, Distribution Lists, Email Templates, Quick Links, Audit Trails, Enforcement Points, System, and Jobs. The main content area is titled 'Modify Auditor AVAUDITOR\_PCI'. It shows a table of targets and groups, with a checkbox for 'Access' and a red 'X' icon next to each entry. The table columns are Access, Name, Type, and Description. The 'PCI' row has its 'Access' checkbox checked. Buttons for 'Cancel' and 'Save' are at the top right of the modal.

Access	Name	Type	Description
<input type="checkbox"/>	12c Database	Secured Target	192.168.56.101 - 12c database
<input type="checkbox"/>	DPA	Group	Data Protection Act (DPA) related targets
<input type="checkbox"/>	GLBA	Group	Gramm-Leach-Bliley Act (GLBA) related targets
<input type="checkbox"/>	HIPAA	Group	Health Insurance Portability and Accountability Act (HIPAA) related targets
<input type="checkbox"/>	Linux Operating System	Secured Target	linux on 192.168.56.101
<input type="checkbox"/>	LinuxOS	Secured Target	Same host as where the 11gR2 database resides
<input type="checkbox"/>	Oracle11gR2DB	Secured Target	
<input checked="" type="checkbox"/>	PCI	Group	Payment Card Industry (PCI) related targets
<input type="checkbox"/>	Production	Group	

# Assign Secured Target Member to PCI Group

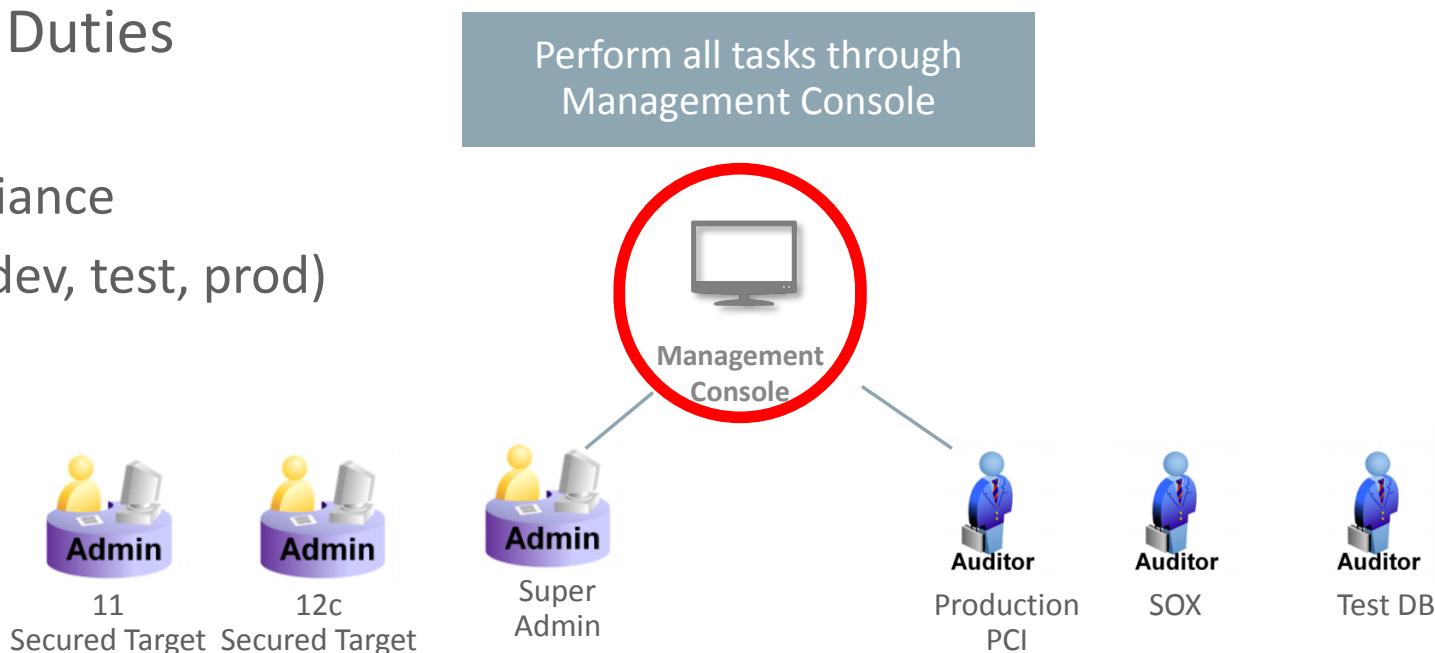
- Secured Target > Group > PCI
- Select 12c database + Linux OS
- **Add Members + Save**
- Go back to PCI page and make sure 2 members are added

The screenshot shows the Oracle Audit Vault Server interface. The top navigation bar includes links for Home, Secured Targets (which is selected), Reports, Policy, and Settings. The top right corner shows the user 'avauditor' and links for Help and Logout. The main content area has a breadcrumb trail: Home > Secured Targets > Groups > Modify Secured Target Group. On the left, a sidebar titled 'Manage' lists 'Targets', 'Groups' (which is selected and highlighted in blue), 'Access Rights', 'Entitlement Snapshots', 'Manage Snapshots', and 'Manage Labels'. Under 'Quick Links', there are 'Audit Trails' and 'Enforcement Points'. The main panel is titled 'Modify Secured Target Group'. It contains fields for 'Name \*' (set to 'PCI') and 'Description' (set to 'Payment Card Industry (PCI) related targets'). Below this is a 'Members' section with a search bar and buttons for 'Actions', 'Add Members', and 'Remove Members'. A table lists four members:

	Member	Name ▲	Description	Secured Target Type
<input type="checkbox"/>	✓	12cDatabase	192.168.56.101 - 12c database	Oracle Database
<input type="checkbox"/>	✗	Linux Operating System	linux on 192.168.56.101	Linux
<input type="checkbox"/>	✓	LinuxOS	Same host as where the 11gR2 database resides	Linux
<input type="checkbox"/>	✗	Oracle11gR2DB		Oracle Database

# 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

Manage Admins

Delete Create

Q Go Actions ▾

	User Name ▲	Type	Target Access	Group Access	Status	Password Expiry Date
<input type="checkbox"/>	AVADMIN	Super Admin	- All -	- All -	OPEN	5/17/2015
<input type="checkbox"/>	FAZHONG	Admin			OPEN	5/19/2015
<input type="checkbox"/>	KYLE	Admin			EXPIRED & LOCKED	11/18/2014
<input type="checkbox"/>	TEMP	Admin			EXPIRED	11/19/2014

1 - 4

## Reset Expired Password

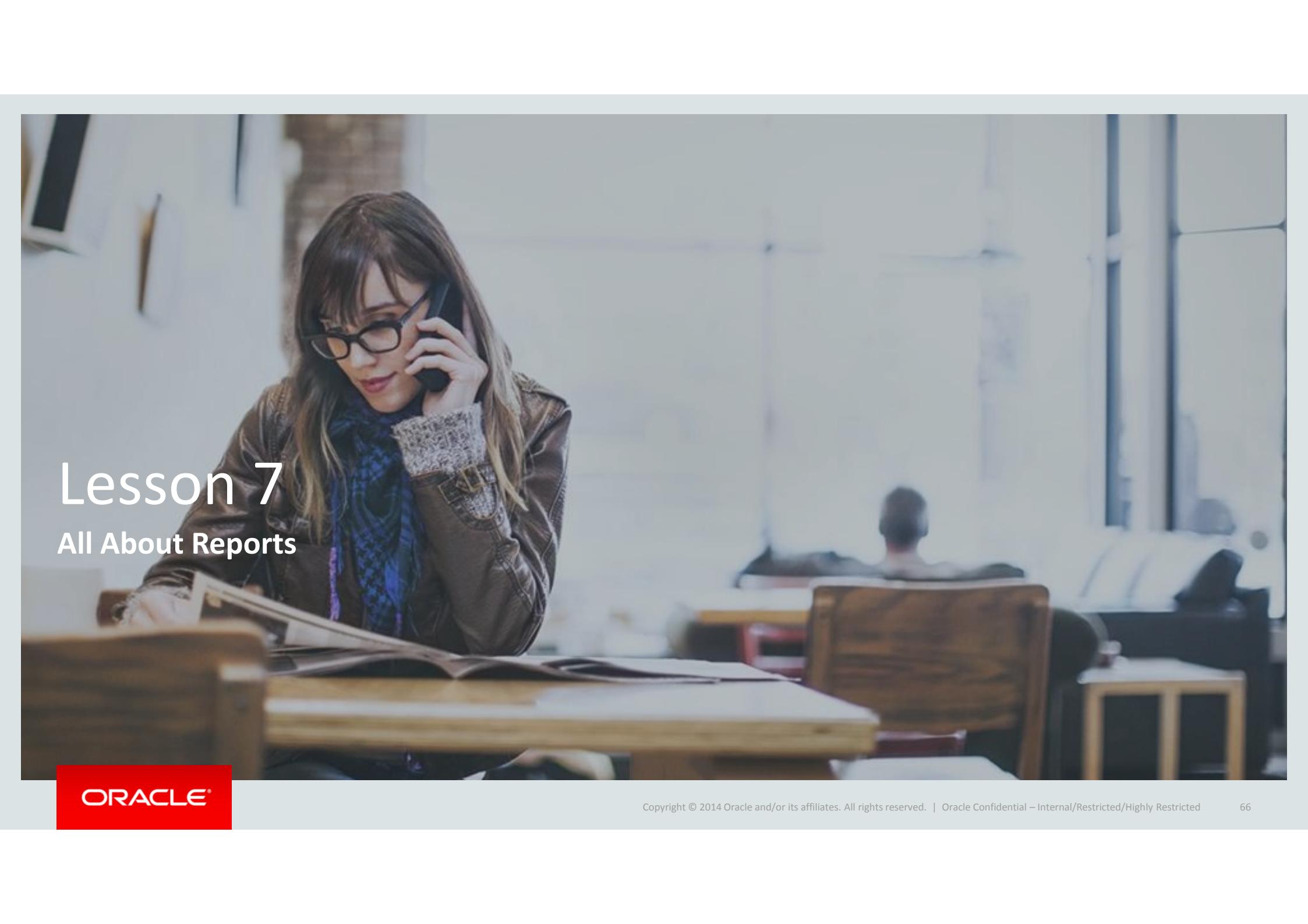
kyle, your password has expired.

Old password

New password

Confirm new password

**Submit** **Cancel**



# Lesson 7

## All About Reports

ORACLE®

Copyright © 2014 Oracle and/or its affiliates. All rights reserved. | Oracle Confidential – Internal/Restricted/Highly Restricted

66

# Browsing Reports

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

The screenshot shows the Oracle Audit Vault Server interface. At the top, there is a navigation bar with links for Home, Secured Targets, Reports (which is the active tab), Policy, and Settings. On the far right of the top bar are user profile, Help, and Logout options. Below the top bar, the page title is "ORACLE Audit Vault Server". Underneath the title, the breadcrumb navigation shows "Home > Reports". A sidebar on the left is titled "Built-in Reports" and contains links for "Audit Reports" (which is highlighted in blue), "Compliance Reports", "Specialized Reports", "Custom Reports", "Uploaded Reports", and "Interactive Reports". To the right of the sidebar, there is a list of report categories: "Activity Reports", "Alert Reports", "Entitlement Reports", and "Stored Procedure Audit Reports". Each category item has a small circular icon with a right-pointing arrow to its left.

[Home](#)[Secured Targets](#)[Reports](#)[Policy](#)[Settings](#)[Home](#) > [Reports](#) > [Compliance Reports](#)**Built-in Reports**

Audit Reports

Compliance Reports

Specialized Reports

**Custom Reports**

Uploaded Reports

Interactive Reports

[Payment Card Industry \(PCI\) Reports](#)[Gramm-Leach-Bliley Act \(GLBA\) Reports](#)[Health Insurance Portability and Accountability Act \(HIPAA\) Reports](#)[Sarbanes-Oxley Act \(SOX\) Reports](#)[Data Protection Act \(DPA\) Reports](#)[Home](#)[Secured Targets](#)[Reports](#)[Policy](#)[Settings](#)[Home](#) > [Reports](#) > [Specialized Reports](#)**Built-in Reports**

Audit Reports

Compliance Reports

Specialized Reports

**Custom Reports**

Uploaded Reports

Interactive Reports

[Database Firewall Reports](#)[Policy Reports](#)[F5 Reports](#)

**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**

**Pre-configured Reports**

Report Name	Report Description	Category	Action
Data Access	Details of audited read access to data for a specified period of time	Activity Overview	<a href="#">Download Report</a>
Activity Overview	Digest of all captured audit events for a specified period of time	Activity Overview	<a href="#">Download Report</a>
Data Modification	Details of audited data modifications for a specified period of time	Activity Overview	<a href="#">Download Report</a>

**ORACLE® Audit Vault Server**

avauditor | Help | Logout

Home > Reports > Interactive Reports

**Built-in Reports**

- Audit Reports
- Compliance Reports
- Specialized Reports

**Custom Reports**

- Uploaded Reports
- Interactive Reports

**Interactive Reports**

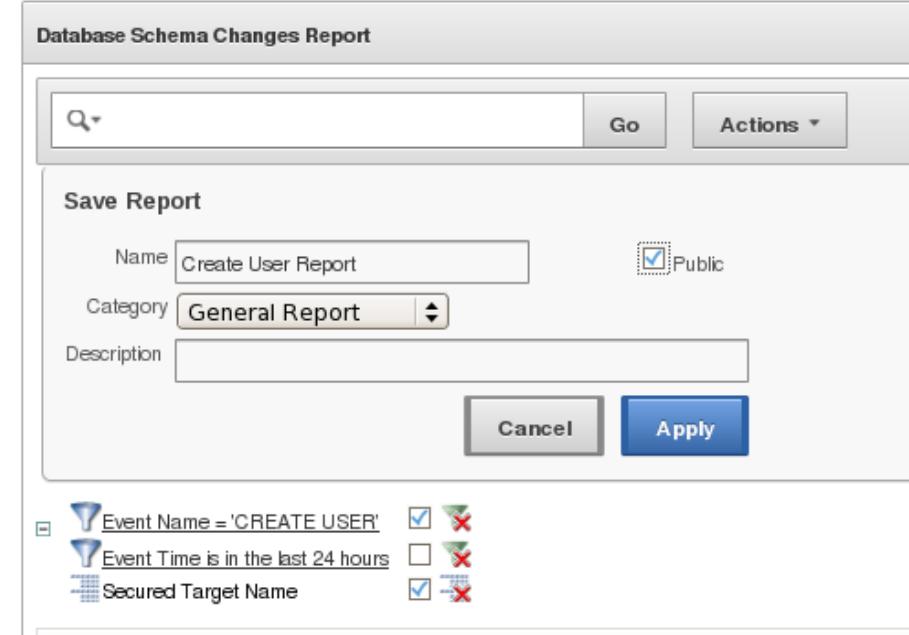
**Category : Investigation Report**

	Report Name	Description	Created By
<input type="checkbox"/>	3 days before Debra left	Activities during 3 days before Debra left the company	AVAUDITOR
<input type="checkbox"/>	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

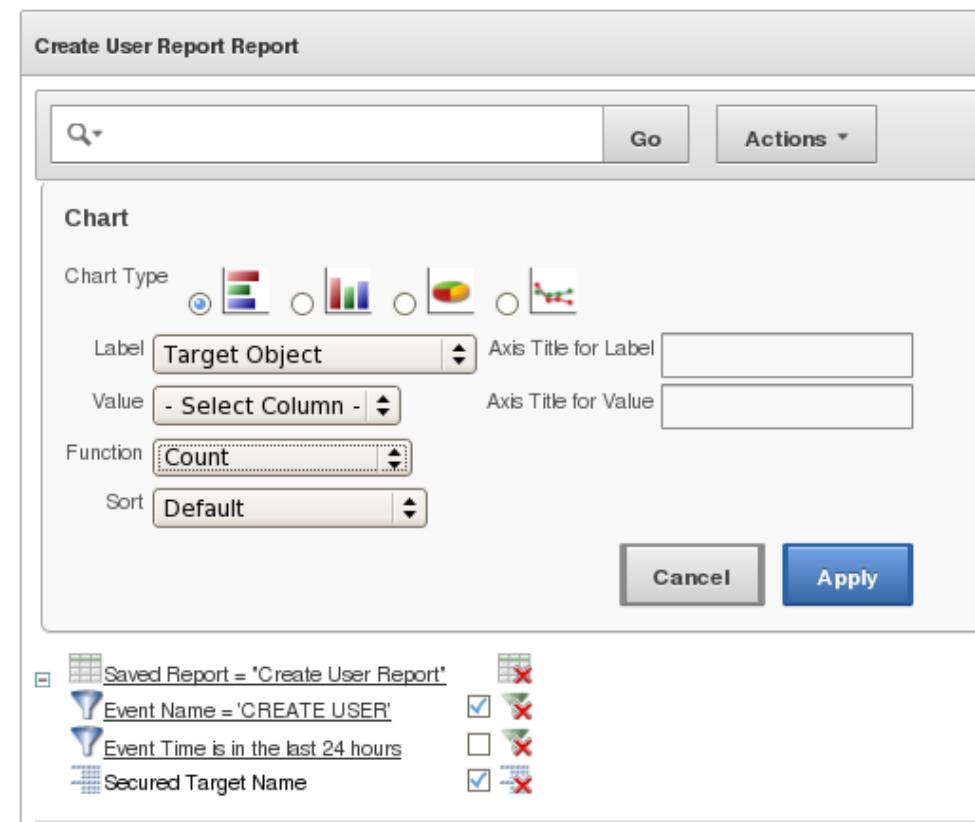


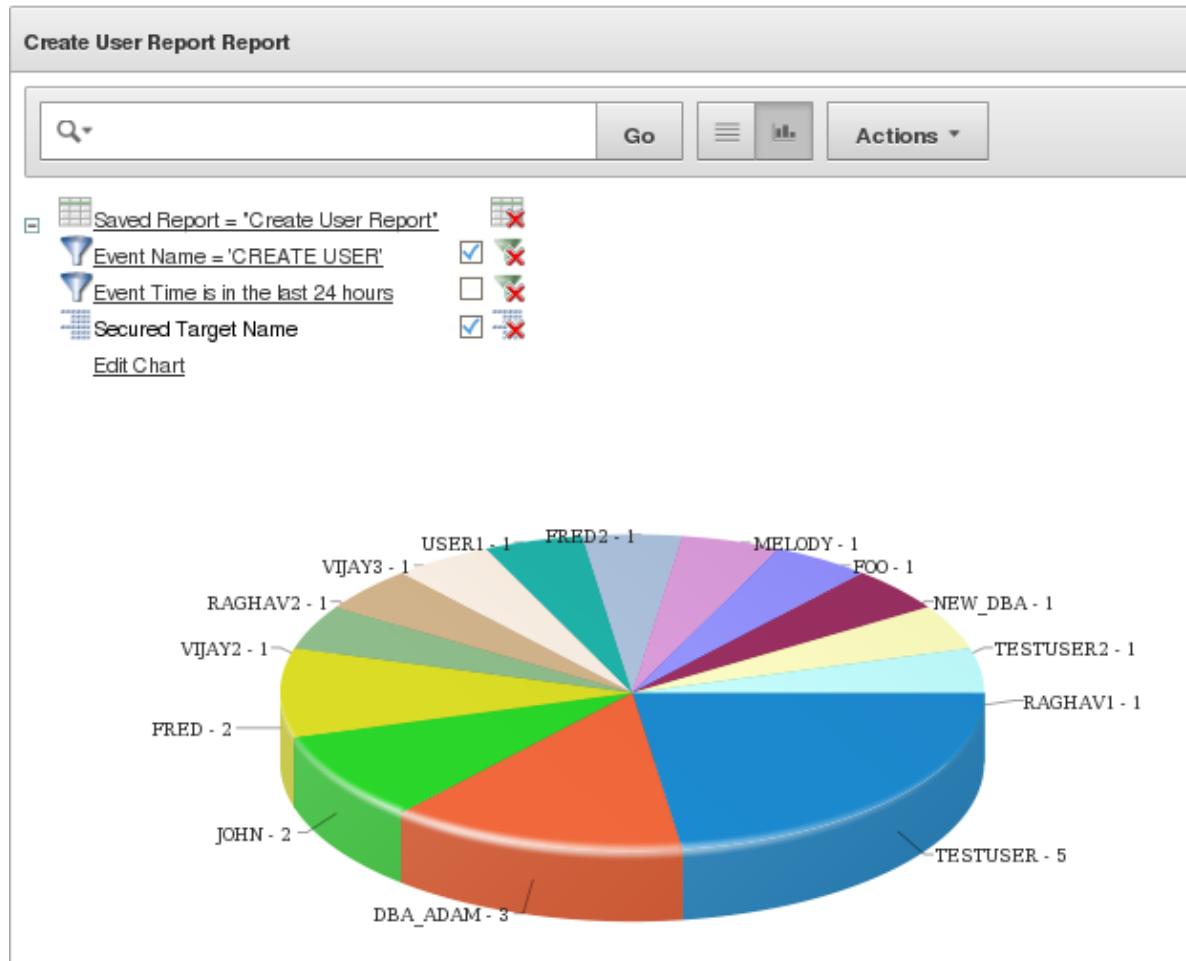
The screenshot shows the Oracle Database Schema Changes Report interface. At the top, there is a search bar with a magnifying glass icon and a 'Go' button, followed by an 'Actions' dropdown menu. Below this is a 'Save Report' dialog box. The dialog has fields for 'Name' (set to 'Create User Report'), 'Category' (set to 'General Report'), and 'Description'. There is a checked checkbox for 'Public'. At the bottom of the dialog are 'Cancel' and 'Apply' buttons. Below the dialog, there is a section with three checkboxes:

- Event Name = 'CREATE USER': Checked (green checkmark)
- Event Time is in the last 24 hours: Unchecked (red X)
- Secured Target Name: Checked (green checkmark)

# 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

Schedule Report

Category Name: Access Reports    Report Name: Failed Logins    Report Format:  PDF  XLS

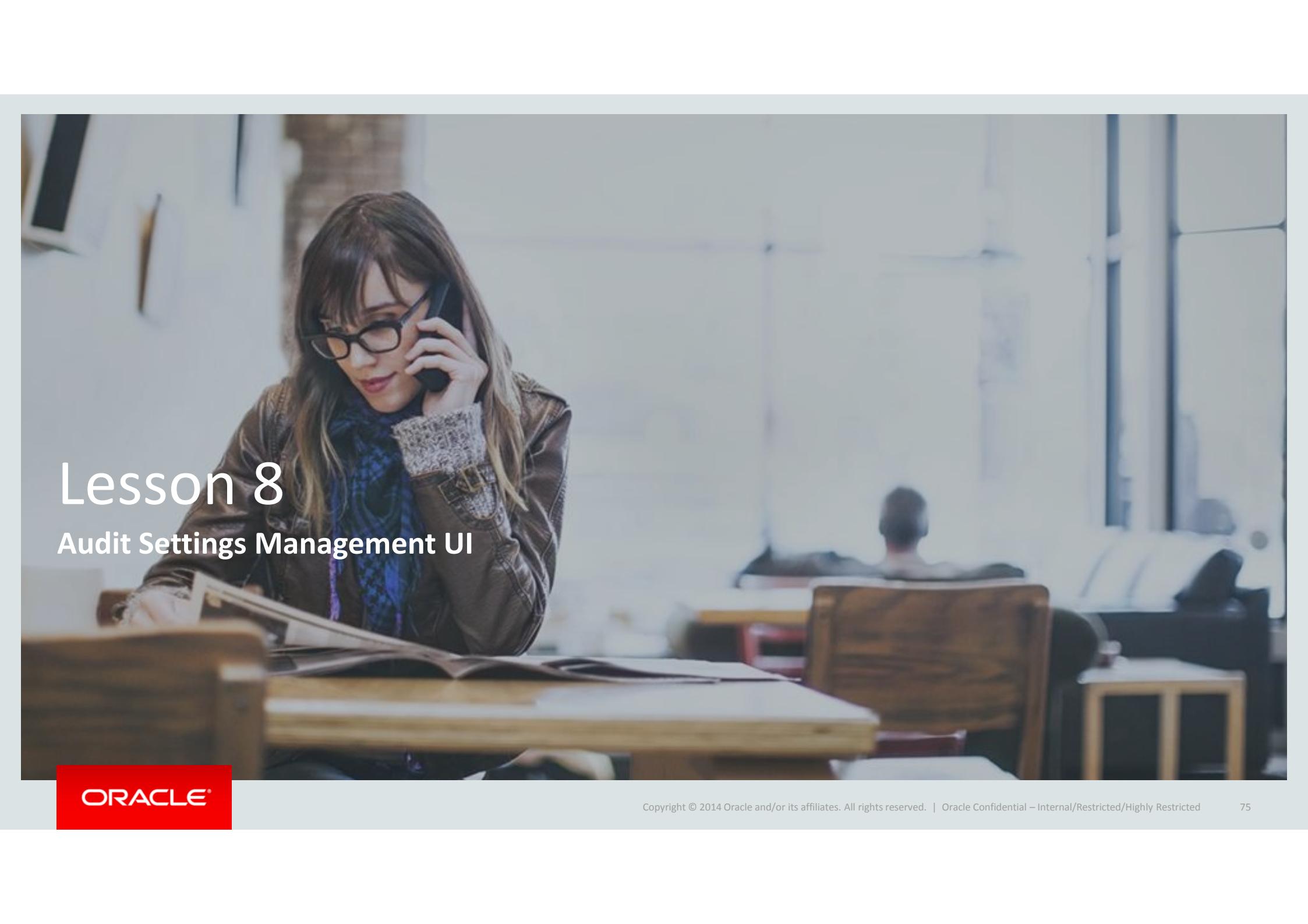
Report Filters

Row Limit: 20000  
Event Time: is in the last  days   
Secured Target Name: All

Schedule

Run \*  Immediately  Specify Schedule

**ORACLE®**



# Lesson 8

## Audit Settings Management UI

ORACLE®

Copyright © 2014 Oracle and/or its affiliates. All rights reserved. | Oracle Confidential – Internal/Restricted/Highly Restricted

75

# 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

**Secured Target Details**

Name	12c DB
Type	Oracle Database
Description	
Location	jdbc:oracle:thin:@//192.168.56.101:1521/orcl

**Audit Trails**

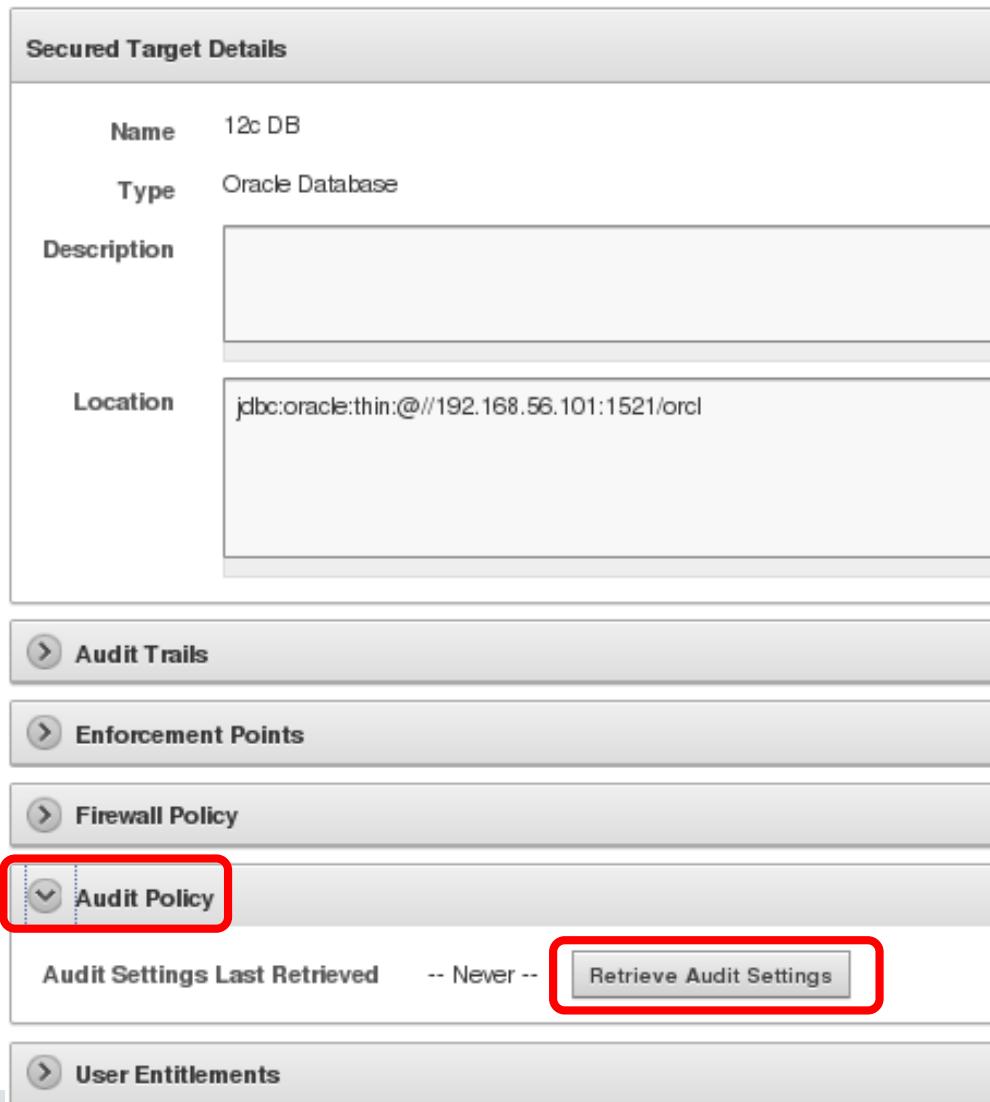
**Enforcement Points**

**Firewall Policy**

**Audit Policy** (highlighted)

**Audit Settings Last Retrieved** -- Never -- (highlighted) **Retrieve Audit Settings** (highlighted)

**User Entitlements**



# Step 1: Review

- \* When Job Completes, Policy > Audit Policy > 12c DB and you will see 0 Needed
- \* Select Object and “Set as Needed”

Audit Settings Last Retrieved	12/6/2014 10:41:27 AM		
Audit SYS	Yes		
Extended Audit Trail	Yes		
Audit Type	In Use	Needed	Problem
Statement	9	0	9
Object	6	0	6
Privilege	32	0	32
FGA	0	0	0
Capture Rule	2	0	2

Object Audit Settings									
		Setting	In Use	Needed	Object Type	Object Owner Name	Object Name	Audit Granularity	Execution Condition
<input checked="" type="checkbox"/>	▼	ALTER	▲	▼	TABLE	HR	JOBS	ACCESS	FAILURE
<input checked="" type="checkbox"/>	▼	DELETE	▲	▼	TABLE	HR	JOBS	ACCESS	FAILURE
<input checked="" type="checkbox"/>	▼	UPDATE	▲	▼	TABLE	HR	JOBS	ACCESS	BOTH
<input checked="" type="checkbox"/>	▼	SELECT	▲	▼	TABLE	HR	JOBS	ACCESS	BOTH
<input checked="" type="checkbox"/>	▼	UPDATE	▲	▼	TABLE	HR	EMPLOYEES	ACCESS	BOTH
<input checked="" type="checkbox"/>	▼	GRANT	▲	▼	TABLE	HR	JOBS	ACCESS	FAILURE

ORACLE®

## Step 2 : Create new settings

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

The screenshot shows the 'Object Audit Settings' dialog box. At the top right are 'Cancel' and 'Save' buttons. The 'Object Type \*' dropdown is set to 'TABLE' (highlighted with a red box). The 'Object \*' dropdown shows 'HR.EMPLOYEES (TABLE)'. Below these are 'Object Execution Condition \*' (set to 'Failure') and 'DML Audit Granularity \*' (set to 'Access'). A large section titled 'Select Settings' contains a 'Statements Audit Type \*' list on the left and a 'SELECT' statement editor on the right. The statements list includes: ALTER, AUDIT, COMMENT, DELETE, EXECUTE, FLASHBACK, GRANT, INDEX, INSERT, and LOCK. The 'SELECT' statement is currently selected in the editor.

## Step 2 : Create New Settings

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

Object Audit Settings									
<input type="button" value="Set as Needed"/> <input type="button" value="Set as Not Needed"/> <input type="button" value="Create"/>									
<input type="text" value="Search"/> <input type="button" value="Go"/> <input type="button" value="Actions"/>									
1 - 7									
<input type="checkbox"/>	<input type="checkbox"/>	Setting	In Use	Needed	Object Type	Object Owner Name	Object Name	Audit Granularity	Execution Condition
<input type="checkbox"/>	<input type="checkbox"/>	ALTER			TABLE	HR	JOBS	ACCESS	FAILURE
<input type="checkbox"/>	<input type="checkbox"/>	DELETE			TABLE	HR	JOBS	ACCESS	FAILURE
<input type="checkbox"/>	<input type="checkbox"/>	GRANT			TABLE	HR	JOBS	ACCESS	FAILURE
<input type="checkbox"/>	<input type="checkbox"/>	UPDATE			TABLE	HR	JOBS	ACCESS	BOTH
<input type="checkbox"/>	<input type="checkbox"/>	SELECT			TABLE	HR	JOBS	ACCESS	BOTH
<input type="checkbox"/>		UPDATE			TABLE	HR	EMPLOYEES	ACCESS	BOTH
<input type="checkbox"/>		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

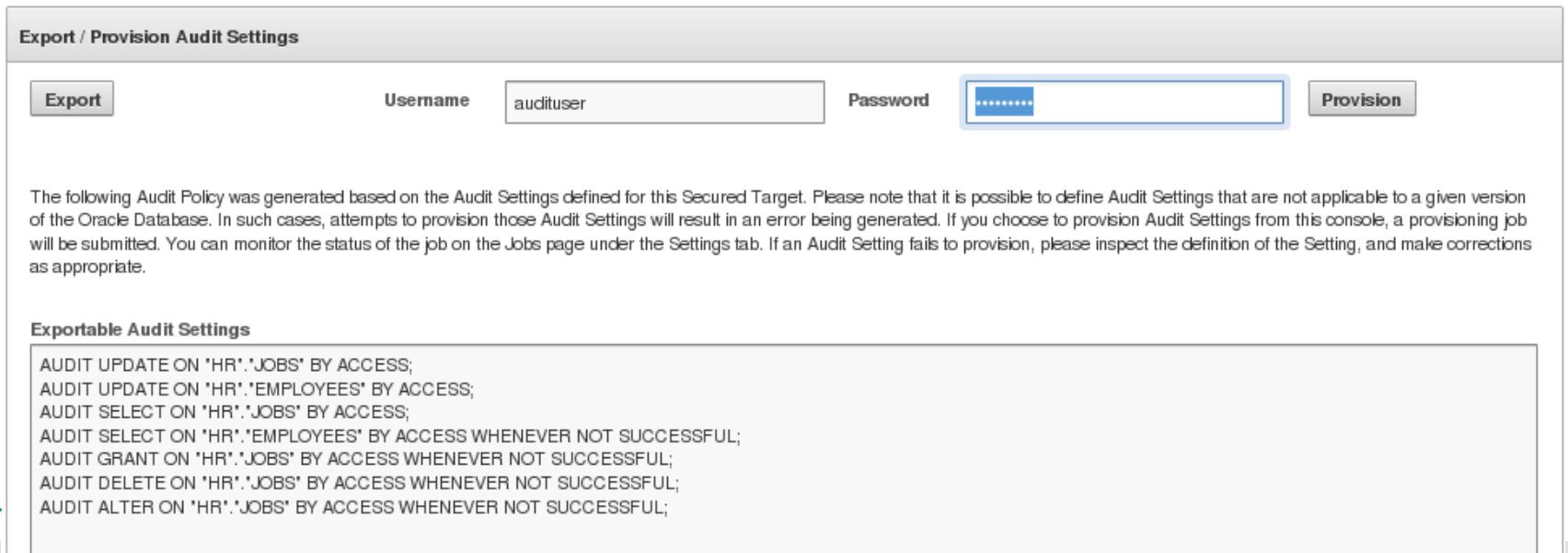
**Export / Provision Audit Settings**

**Export**      Username: audituser      Password: **\*\*\*\*\***      **Provision**

The following Audit Policy was generated based on the Audit Settings defined for this Secured Target. Please note that it is possible to define Audit Settings that are not applicable to a given version of the Oracle Database. In such cases, attempts to provision those Audit Settings will result in an error being generated. If you choose to provision Audit Settings from this console, a provisioning job will be submitted. You can monitor the status of the job on the Jobs page under the Settings tab. If an Audit Setting fails to provision, please inspect the definition of the Setting, and make corrections as appropriate.

**Exportable Audit Settings**

```
AUDIT UPDATE ON "HR"."JOBS" BY ACCESS;  
AUDIT UPDATE ON "HR"."EMPLOYEES" BY ACCESS;  
AUDIT SELECT ON "HR"."JOBS" BY ACCESS;  
AUDIT SELECT ON "HR"."EMPLOYEES" BY ACCESS WHENEVER NOT SUCCESSFUL;  
AUDIT GRANT ON "HR"."JOBS" BY ACCESS WHENEVER NOT SUCCESSFUL;  
AUDIT DELETE ON "HR"."JOBS" BY ACCESS WHENEVER NOT SUCCESSFUL;  
AUDIT ALTER ON "HR"."JOBS" BY ACCESS WHENEVER NOT SUCCESSFUL;
```

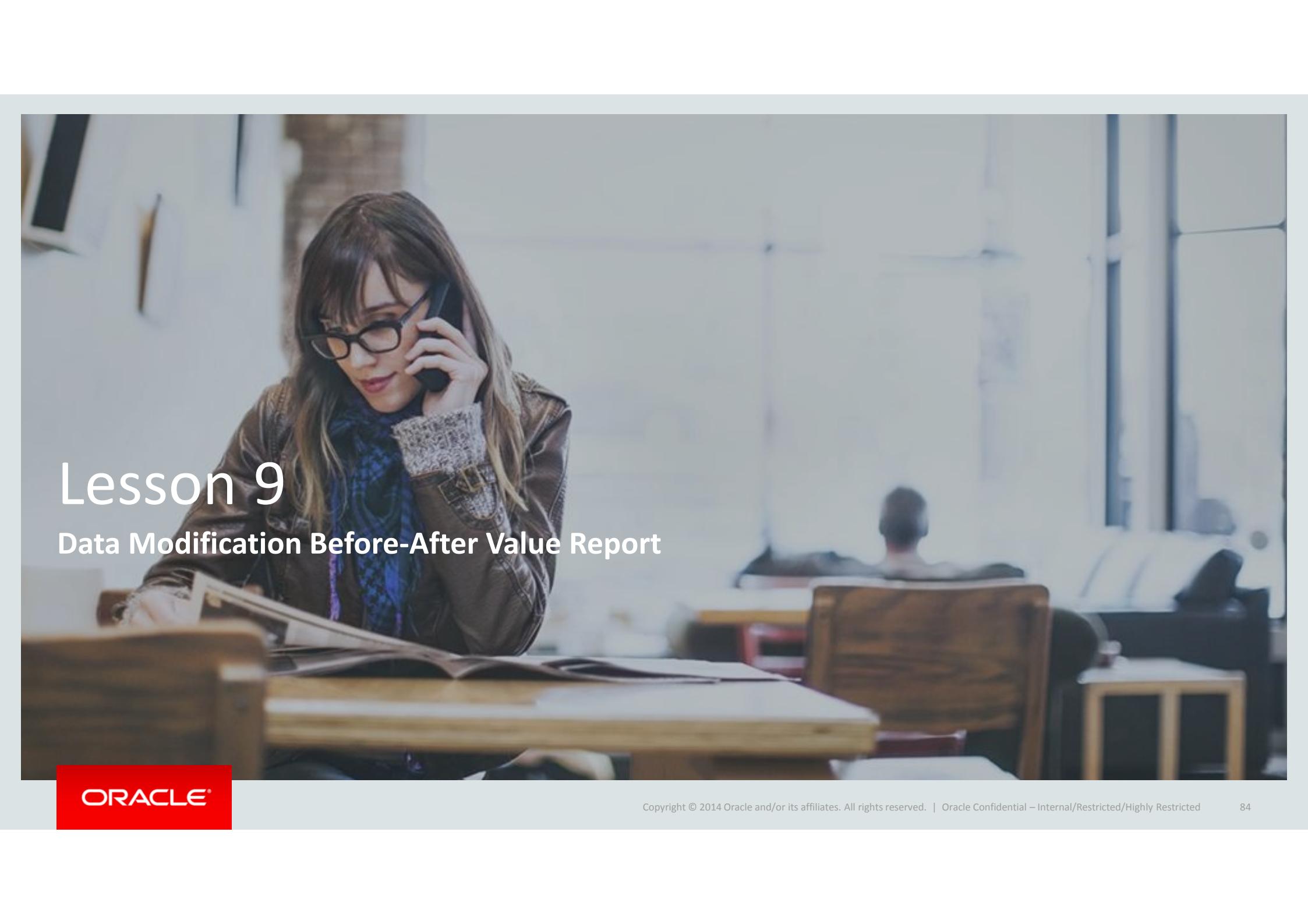


Object Audit Settings								
□	▼	Setting	In Use	Needed	Object Type	Object Owner Name	Object Name	Audit Granularity
□		ALTER	▲	▲	TABLE	HR	JOBS	ACCESS
□		DELETE	▲	▲	TABLE	HR	JOBS	ACCESS
□		GRANT	▲	▲	TABLE	HR	JOBS	ACCESS
□		UPDATE	▲	▲	TABLE	HR	JOBS	ACCESS
□		SELECT	▲	▲	TABLE	HR	JOBS	ACCESS
□		UPDATE	▲	▲	TABLE	HR	EMPLOYEES	ACCESS
□		SELECT	▲	▲	TABLE	HR	EMPLOYEES	ACCESS

When done, do the same for all other settings

# Problems? No Problem ☺





# Lesson 9

## Data Modification Before-After Value Report

ORACLE®

Copyright © 2014 Oracle and/or its affiliates. All rights reserved. | Oracle Confidential – Internal/Restricted/Highly Restricted

84

# 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

Add Audit Trail

Audit Trail Type \* TRANSACTION LOG

Collection Host \* HostMachineOf12c

Secured Target \* 12cDatabase

Collection Plug-in com.oracle.av.plugin.oracle

Cancel Save

- Create Capture Rule  
As AVAUDITOR
    - Audit Policy > Capture Rule
- [this is done for you]

Capture Rule Settings

Set as Needed Set as Not Needed Create

Actions ▾

1 - 2

		Rule Type	In Use	Needed	Secured Target Schema	Secured Target Table	Statement Type
<input type="checkbox"/>	▼	TABLE_RULE	▲	▲	HR	EMPLOYEES	DML
<input type="checkbox"/>		TABLE_RULE	▲	▲	HR	EMPLOYEES	DDL

1 - 2

# Generate Before-After Value Report

SQL>UPDATE HR.EMPLOYEES set salary=19000 where last\_name='Higgins';

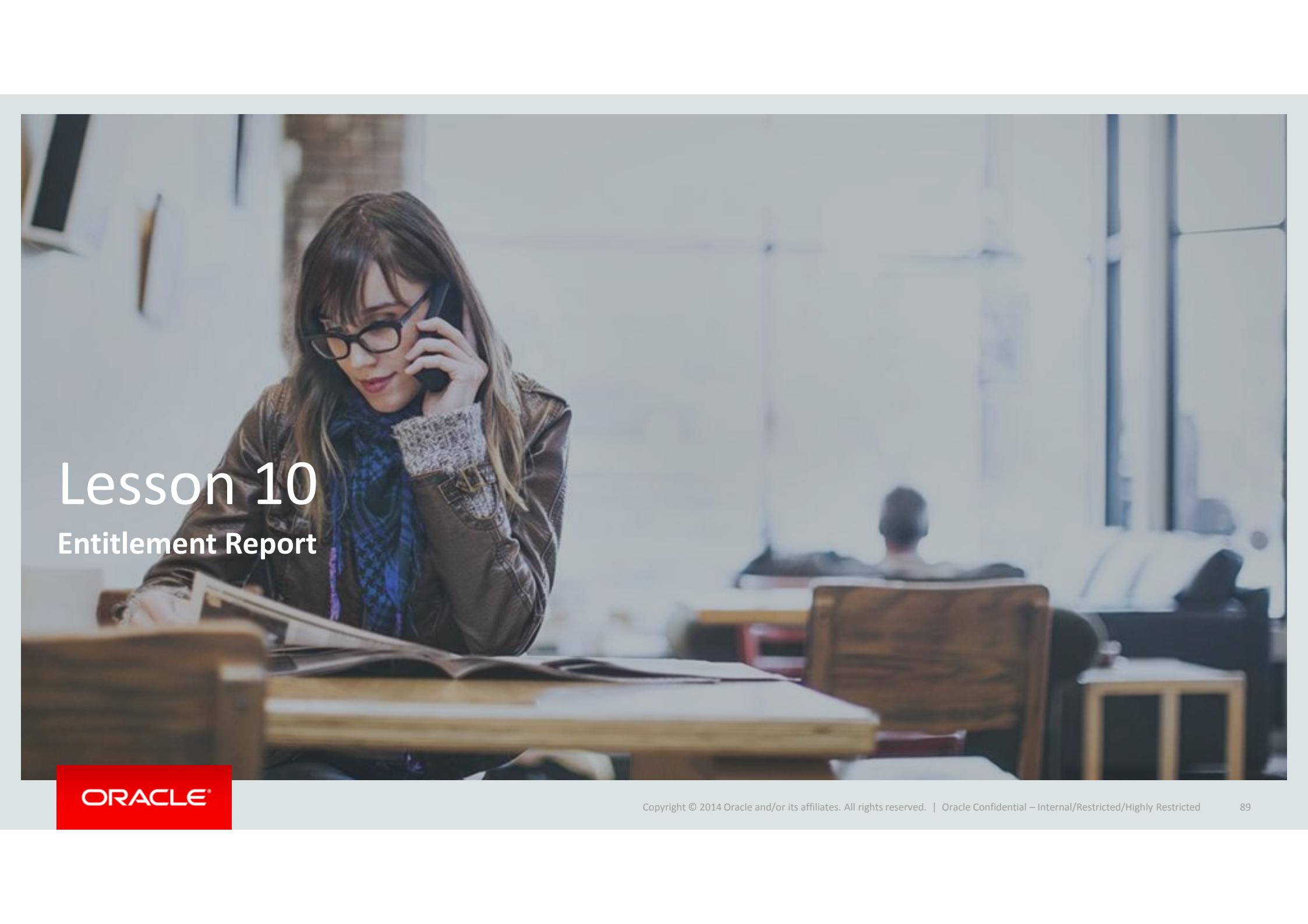
Data Modification Before-After Values Report

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

ORACLE®

Copyright © 2014 Oracle and/or its affiliates. All rights reserved. | Oracle Confidential – Internal/Restricted/Highly Restricted

89

# 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

Privileged Users by Secured Target - Changes

Secured Target: Oracle11gR2DB | Snapshot: 8/22/2014 2:06:01 PM | compare: 8/25/2014 12:19:16 PM

Actions: Go, Actions ▾

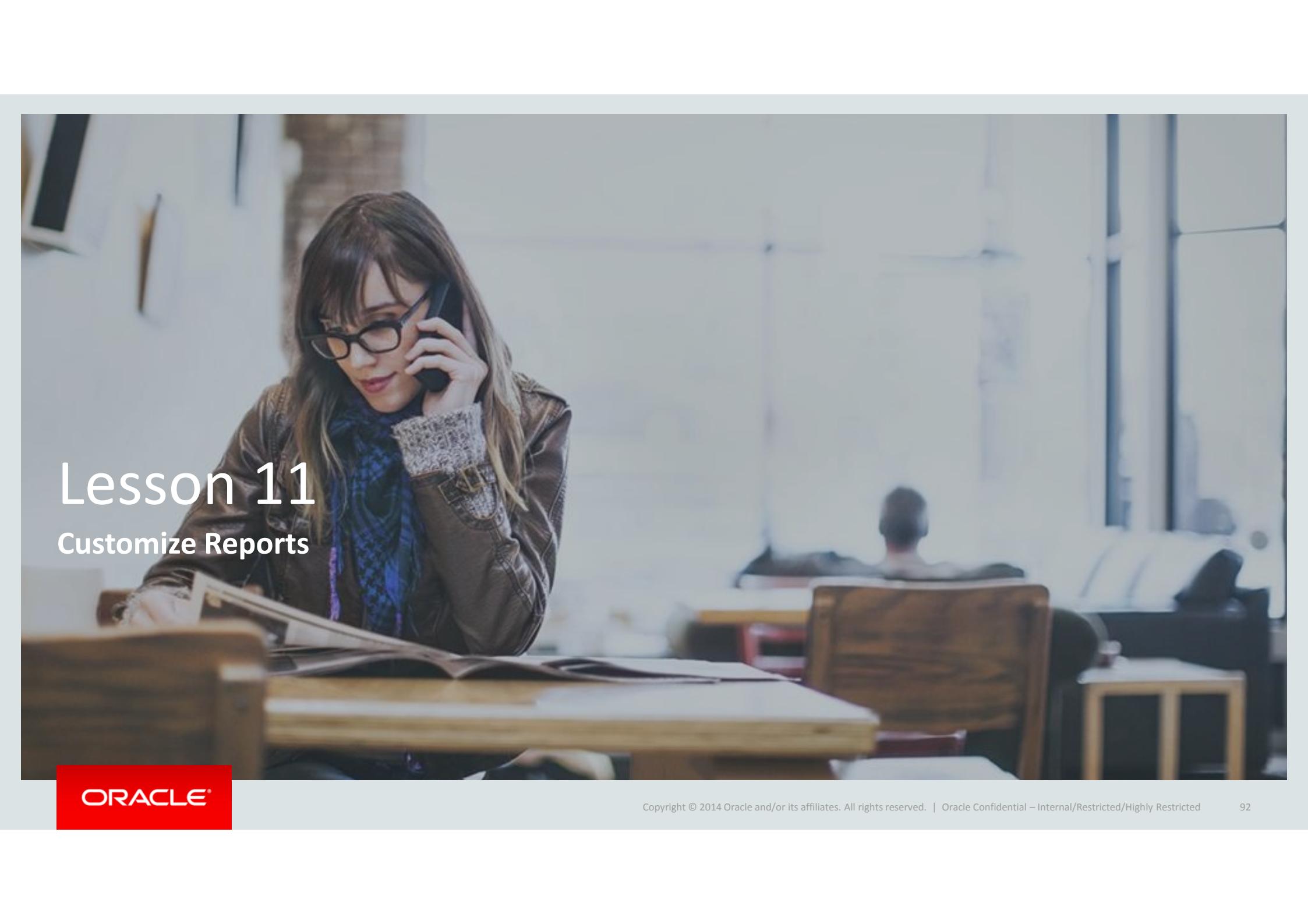
Admin Option	User	Privilege	Change Category
YES	JSMITH	UNLIMITED TABLESPACE	UNCHANGED
YES	JSMITH	UNLIMITED TABLESPACE	UNCHANGED
YES	JTAYLOR	UNLIMITED TABLESPACE	UNCHANGED
YES	JTAYLOR	UNLIMITED TABLESPACE	UNCHANGED
YES	PJONES	UNLIMITED TABLESPACE	UNCHANGED
YES	PJONES	UNLIMITED TABLESPACE	UNCHANGED

Privileged Users by Secured Target - Changes

Secured Target: Oracle11gR2DB | Snapshot: 8/22/2014 2:06:01 PM | compare: 8/25/2014 12:19:16 PM

Actions: Go, Actions ▾

Admin Option	User	Privilege	Change Category
YES	JSMITH	UNLIMITED TABLESPACE	UNCHANGED
YES	JSMITH	UNLIMITED TABLESPACE	UNCHANGED
YES	JTAYLOR	UNLIMITED TABLESPACE	UNCHANGED
YES	JTAYLOR	UNLIMITED TABLESPACE	UNCHANGED
YES	PJONES	UNLIMITED TABLESPACE	UNCHANGED
YES	PJONES	UNLIMITED TABLESPACE	UNCHANGED



# Lesson 11

## Customize Reports

ORACLE®

Copyright © 2014 Oracle and/or its affiliates. All rights reserved. | Oracle Confidential – Internal/Restricted/Highly Restricted

92

# 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)

Database Schema Changes - Microsoft Word

Home Insert Page Layout References Mailings Review View Developer Design Layout

Albany WT 16 A A A B I U abe x x Aa ab A

Font Paragraph Styles

AaBbCcDd AaBbCcDd AaBbCc AaBbCc AaB AaB Change Styles Title

Normal No Spacing Heading 1 Heading 2

Clipboard Find Replace Select Editing

**Database Schema Changes**

Report period : TIME\_FROM to TIME\_TO  
Run by : REPORT\_USER  
Report records limit : ROW\_LIMIT  
Secured Target(s) : SECURED\_TARGET

<?if:(TLQR/ROW)?>groupROWbySECURED\_TARGET

Secured Target : <?SECURED\_TARGET?>

Event Time	Event Name	Event Status	User Name	Target Object	Client IP	Client Program	Event Source
FC EVENT_TIME	EVENT_NAME	EVENT_STATUS	USER_NAME	TARGET_OBJECT	CLIENT_IP	CLIENT_PROGRAM	EVENT_SOURCE
C COMMAND_TEXT E							

Number of records for Secured Target <?SECURED\_TARGET?> : sec\_count

endROWby SECURED\_TARGET

<?endif?><if not:(TLQR/ROW)?>

Total number of records : total\_count

ORACLE®

# Customize Report

## Step 3 : Upload BOTH RTF + XML

The screenshot shows the Oracle Audit Vault Server interface. The top navigation bar includes the Oracle logo, user 'avauditor', and links for Help and Logout. The main menu bar has options: Home, Secured Targets, Reports (which is selected), Policy, and Settings. Below the menu, a breadcrumb trail shows: Home > Reports > Uploaded Reports > Upload Custom Report. On the left, a sidebar under 'Custom Reports' shows 'Uploaded Reports' as the active tab, along with other options like Audit Reports, Compliance Reports, and Specialized Reports. The main content area is titled 'Upload Custom Report' with 'Cancel' and 'Save' buttons. It contains fields for 'Report Template file' (set to '/home/oracle/Desktop/Database Schema Changes.rtf') and 'Report Definition file' (set to '/home/oracle/Desktop/Database Schema Changes.xml'). A 'Description' field contains the text 'Newly updated RFT with new company logo'. The 'Save' button is highlighted in blue.

# Customize Report

## Step 4 : Testing results

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

The screenshot shows the Oracle Audit Vault Server interface. The top navigation bar includes links for Home, Secured Targets, Reports (which is the active tab), Policy, Settings, and user account information. The main content area displays a breadcrumb trail: Home > Reports > Uploaded Reports. On the left, there's a sidebar with sections for Built-in Reports (Audit Reports, Compliance Reports, Specialized Reports) and Custom Reports (Uploaded Reports, Interactive Reports, Report Workflow). The main panel is titled 'Uploaded Reports' and contains a search bar, a 'Go' button, and an 'Actions' dropdown. A table lists one report entry:

	Report Name	Report Description	Category	Schedule Report	Download Report Template	Download Report Definition
<input type="checkbox"/>	Database Schema Changes	Newly updated RFT with new company logo	Uploaded Reports			

At the bottom right of the main panel, it says '1 - 1 of 1'. The bottom left corner features the Oracle logo.

Database Schema Changes-2.pdf

File Edit View Go Help

Previous Next 1 of 296 Fit Page Width

## Database Schema Changes

Report period : 10/19/2014 2:44:09 AM to 11/18/2014 2:44:09 AM  
Run by : AVAUDITOR  
Report records limit : 20000  
Secured Target(s) : All



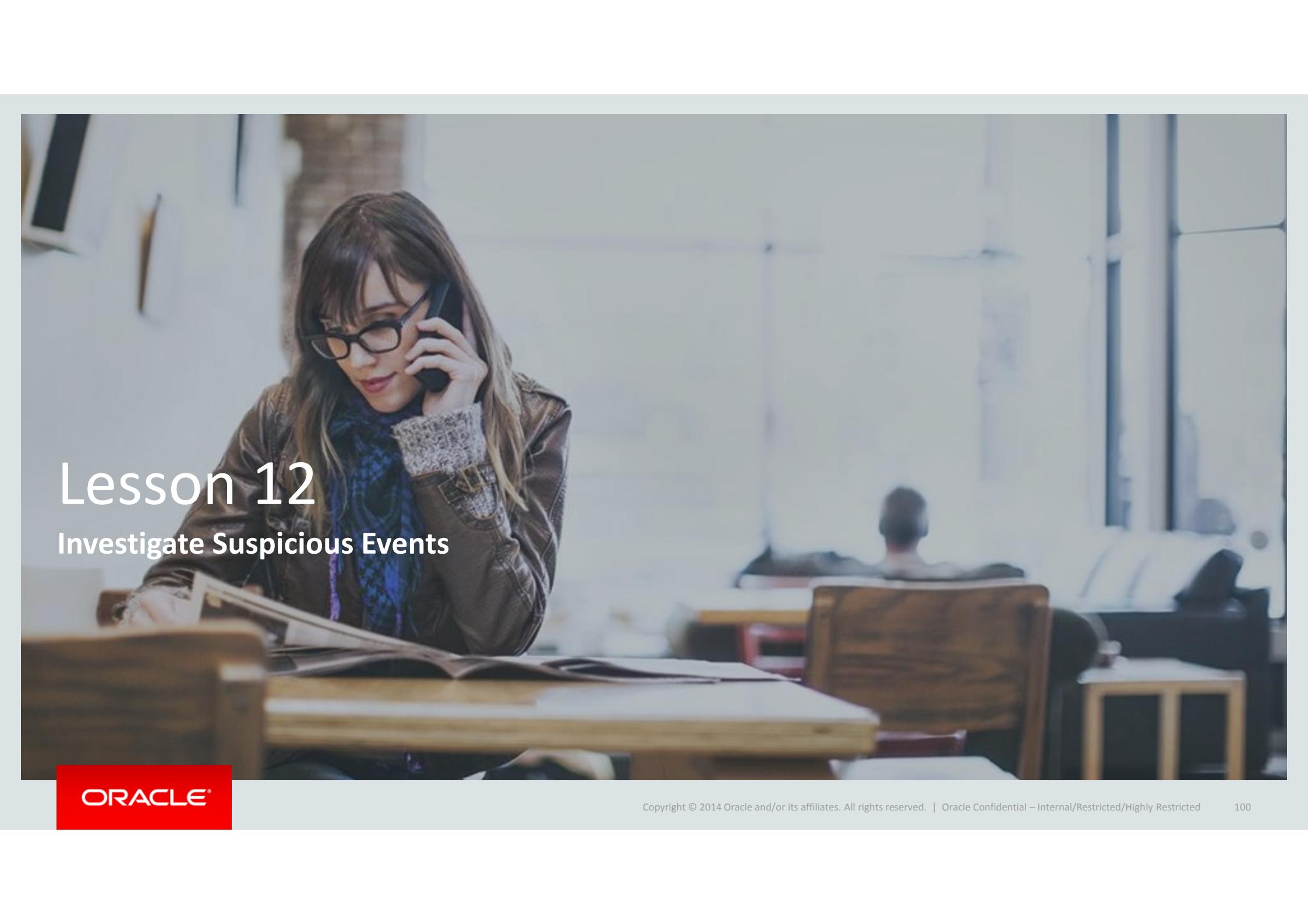
Secured Target : 12cDatabase

Event Time	Event Name	Event Status	User Name	Target Object	Client IP	Client Program	Event Source
Command Text							
11/12/2014 10:45:12 PM	SUPER USER DDL	SUCCESS	/				AUDIT TRAIL
drop user dba_debra cascade							
11/12/2014 10:47:28 PM	SUPER USER DDL	SUCCESS	/				AUDIT TRAIL
create user dba_debra identified by * account unlock							

# 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](http://docs.oracle.com/cd/E28280_01/bi.1111/e22254/create_rft_bldr.htm#BIPRD2621)



# Lesson 12

## Investigate Suspicious Events

ORACLE®

Copyright © 2014 Oracle and/or its affiliates. All rights reserved. | Oracle Confidential – Internal/Restricted/Highly Restricted

100

## 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 22<sup>nd</sup> 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

ORACLE®

Copyright © 2014 Oracle and/or its affiliates. All rights reserved. | Oracle Confidential – Internal/Restricted/Highly Restricted

103

# Enable an Existing Alert

CreateUser, Select table, non-DEMOAPPS access table

Policy > Alerts > **Enable**

The screenshot shows the Oracle Audit Vault Server interface. The top navigation bar includes Home, Secured Targets, Reports, Policy (selected), Settings, and user information (avauditor, Help, Logout). Below the navigation is a breadcrumb trail: Home > Policy > Alerts. On the left, a sidebar menu is open under the 'Alerts' section, showing 'Alerts' (selected), 'Audit Settings', and 'Firewall Policy'. The main content area is titled 'Alerts' and contains a search bar, a 'Manage Alert Status Values' button, and buttons for 'Enable', 'Disable', 'Delete', and 'Create'. A table lists four alerts:

	Status	Alert Name	Alert Owner	Description	Secured Target Type
<input checked="" type="checkbox"/>	⬇️	CreateUser	AVAUDITOR	Alert me when a new user is created.	Oracle Database
<input type="checkbox"/>	⬆️	Database Firewall Alert	AVSYS	An alert evaluated at a Database Firewall, based on a Firewall Policy.	- All -
<input type="checkbox"/>	⬇️	non-DEMOAPPS access ORDERS table	AV_AUD_AUDREY	Alert me when non-DEMOAPPS access ORDERS table	Oracle Database
<input type="checkbox"/>	⬇️	select HR.JOBS table	AVAUDITOR	Alert me when HR.JOBS table is accessed	- All -

## Modify Alert

CancelSave

Name *	<input type="text" value="CreateUser"/>
Secured Target Type	<input type="text" value="Oracle Database"/> <input type="button" value="▼"/>
Severity *	<input type="button" value="Warning"/> <input type="button" value="▼"/>
Threshold (times) *	<input type="text" value="1"/>
Duration (min) *	<input type="text" value="0"/>
Group By (Field)	<input type="text" value="SECURED_TARGET_NAME"/> <input type="button" value="▼"/>
Status *	<input type="button" value="Enabled"/> <input type="button" value="▼"/>
Description	<p>Alert me when a new user is created.</p> <p>36 of 255</p>
Condition *	<pre>:COMMAND_CLASS='CREATE' and :TARGET_TYPE='USER' and UPPER(:EVENT_STATUS)='SUCCESS'</pre>

## Condition - Available Fields

ACTION\_TAKEN  
AV\_TIME  
CLIENT\_HOST\_NAME  
CLIENT\_IP  
CLUSTER\_TYPE  
COMMAND\_CLASS  
ERROR\_CODE  
ERROR\_MESSAGE  
EVENT\_NAME  
EVENT\_STATUS  
EVENT\_TIME  
LOCATION  
NETWORK\_CONNECTION  
OSUSER\_NAME  
SECURED\_TARGET\_CLASS  
SECURED\_TARGET\_NAME  
TARGET\_OBJECT  
TARGET\_OWNER  
TARGET\_TYPE  
THREAT\_SEVERITY  
USER\_NAME

# Firing the Alert

sqlplus DBA\_DEBRA/Manager\_1

SQL> Create user {melody} identified by Manager\_1 account unlock;

Refresh Interval “Manually” > Go

The screenshot shows the Oracle Audit Vault Server interface. At the top, there's a navigation bar with tabs: Home, Secured Targets, Reports, Policy, and Settings. Below the navigation bar, there are two dropdown menus: 'View data for' set to 'Last 24 Hours' and 'Refresh Interval' set to 'Manually'. A 'Go' button is next to the refresh interval dropdown. To the right of the 'Go' button, it says 'Refreshed at 11/18/2014 7:44:37 PM'. Below these controls, there's a section titled 'Recently Raised Alerts' containing a single entry: 'CreateUser' with a yellow exclamation mark icon. This entry is circled with a red oval. To the right of the alert list is a 'Attestation Actions' panel which displays the message 'No reports need attestation at th'. At the bottom left is the Oracle logo, and at the bottom right are copyright and page number information: 'Copyright © 2014 Oracle and/or its affiliates. All rights reserved. | Oracle Confidential – Internal/Restricted/Highly Restricted' and '106'.

# Manage Your Alerts

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

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

The screenshot shows the 'Alerts' section of the Oracle Database Audit Advisor. At the top, there is a search bar with a magnifying glass icon, a 'Go' button, and an 'Actions' dropdown menu. To the right, there is a 'Set Status to' dropdown menu with three options: 'Closed' (selected), 'In\_Review', and 'New'. A blue 'Apply' button is located next to the dropdown. Below the search bar is a table with one row of data. The columns are labeled: Alert Time, Secured Target, User Name, Name, Event Time, Alert Status, and Alert Severity. The data in the table is as follows:

Alert Time	Secured Target	User Name	Name	Event Time	Alert Status	Alert Severity
11/18/2014 7:06:23 PM	12cDatabase	DBA_DEBRA	CreateUser	11/18/2014 7:06:21 PM	New	Warning

At the bottom right of the table area, there is a page number '1 - 1'.

# Create a New Alert

Alert Me When HR.EMPLOYEES table is Updated

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

Object Audit Settings

Cancel Save

Object Type \* TABLE Object \* HR.EMPLOYEES (TABLE)

Object Execution Condition \* Both

DML Audit Granularity \* Access

Select Settings

Statements Audit Type \*

- ALTER
- AUDIT
- COMMENT
- DELETE
- EXECUTE
- FLASHBACK
- GRANT
- INDEX
- INSERT
- LOCK
- READ
- REFERENCE
- RENAME
- SELECT
- WRITE

UPDATE

The screenshot shows the 'Object Audit Settings' dialog box. In the 'Object Type' dropdown, 'TABLE' is selected. The 'Object' dropdown shows 'HR.EMPLOYEES (TABLE)'. Under 'Object Execution Condition', 'Both' is selected. Under 'DML Audit Granularity', 'Access' is selected. Below this, the 'Select Settings' section is visible, featuring a list of statements under 'Statements Audit Type'. The word 'UPDATE' is highlighted in the list, indicating it is selected. The Oracle logo is in the bottom left corner.

# 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**

Activity Overview Report

Report View < > Row 2 of 1897  Exclude Null Values  Displayed Columns

Secured Target

Secured Target Name: 12cDatabase  
Secured Target Type: Oracle Database  
Secured Target Class: Database

Event

Server Time: 11/18/2014 8:23:04 PM  
Event Time: 11/18/2014 8:22:56 PM  
User Name: DBA\_DEBRA  
Event Status: SUCCESS  
Event Name: UPDATE

Command Class: UPDATE  
Location: Audit File

Target

Target Object: EMPLOYEES  
Target Owner: HR

Client/User Information

OS User Name: oracle  
Client Host Name: lap-db12102

Statement

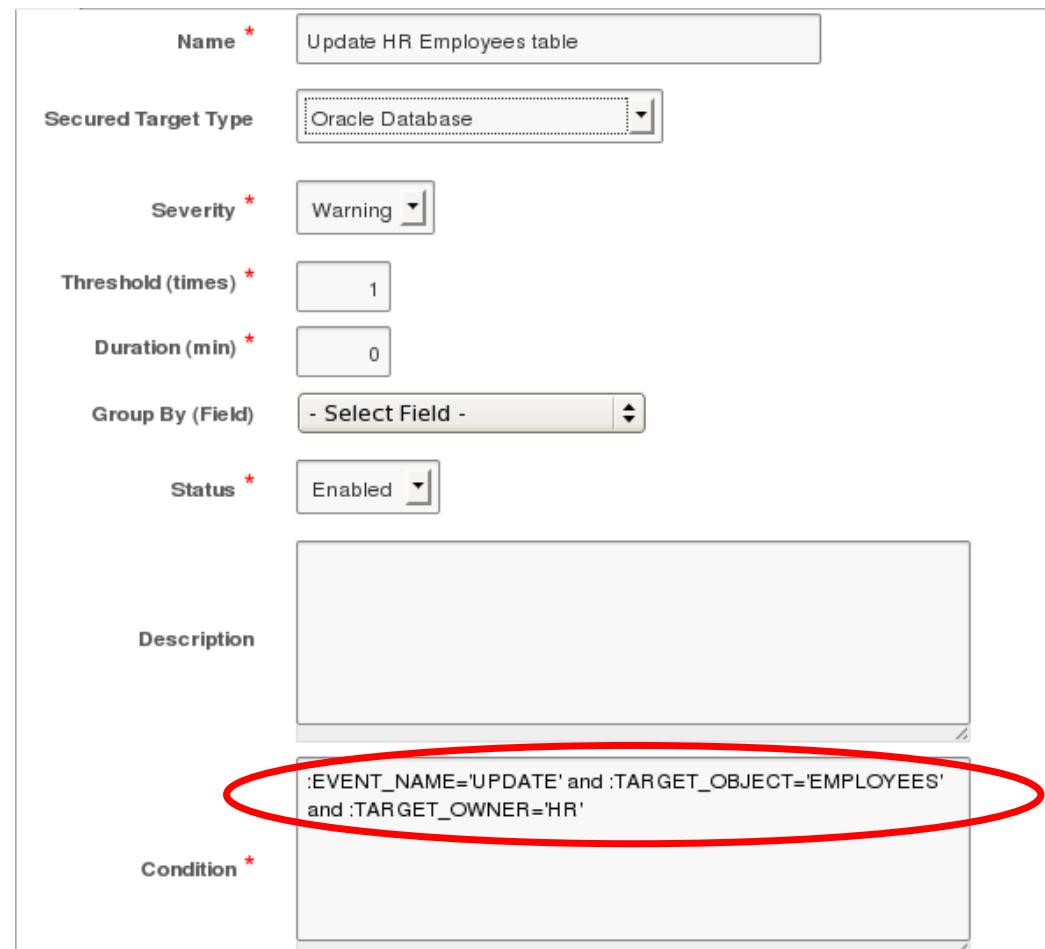
Command Text: update HR.EMPLOYEES set SALARY=12000 where LAST\_NAME='Higgins'

# Create a New Alert

## An Easier Way

### 3. Create the alert with corresponding syntax

Now fire the alert to ensure it's working



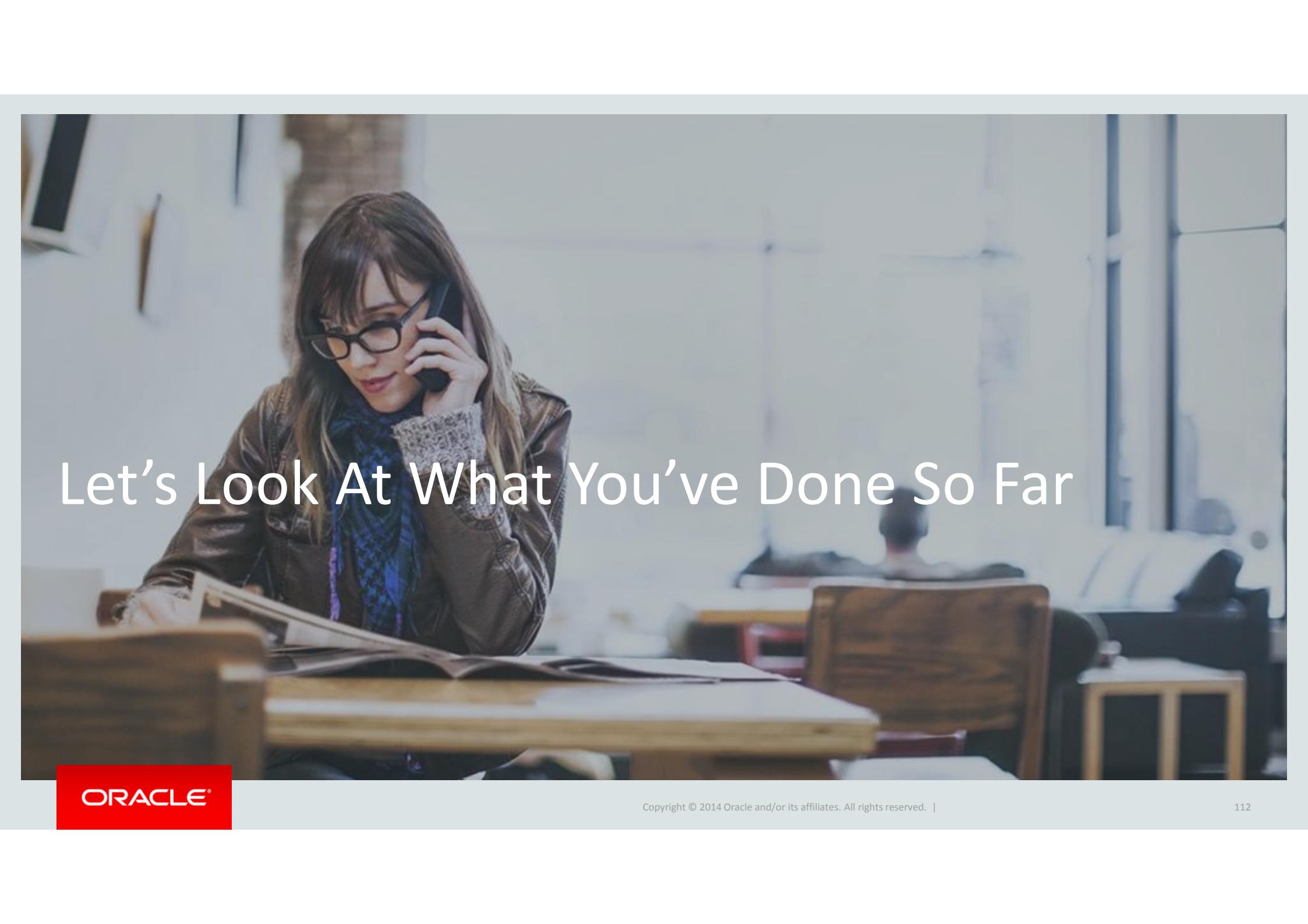
The screenshot shows the configuration of a new alert. The alert is named "Update HR Employees table". It is set to monitor an "Oracle Database" target, with a severity of "Warning", a threshold of 1, and no duration. The alert is grouped by "Field" and is currently enabled. The condition for the alert is defined as "`:EVENT_NAME='UPDATE' and :TARGET_OBJECT='EMPLOYEES' and :TARGET_OWNER='HR'`". This condition is circled in red.

Name *	Update HR Employees table
Secured Target Type	Oracle Database
Severity *	Warning
Threshold (times) *	1
Duration (min) *	0
Group By (Field)	- Select Field -
Status *	Enabled
Description	(empty text area)
Condition *	<code>:EVENT_NAME='UPDATE' and :TARGET_OBJECT='EMPLOYEES' and :TARGET_OWNER='HR'</code>

# 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



# Let's Look At What You've Done So Far

ORACLE®

Copyright © 2014 Oracle and/or its affiliates. All rights reserved. |

112

# 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 containing sensitive data such as PII, CC or stored procedure used to encryption/decryption 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

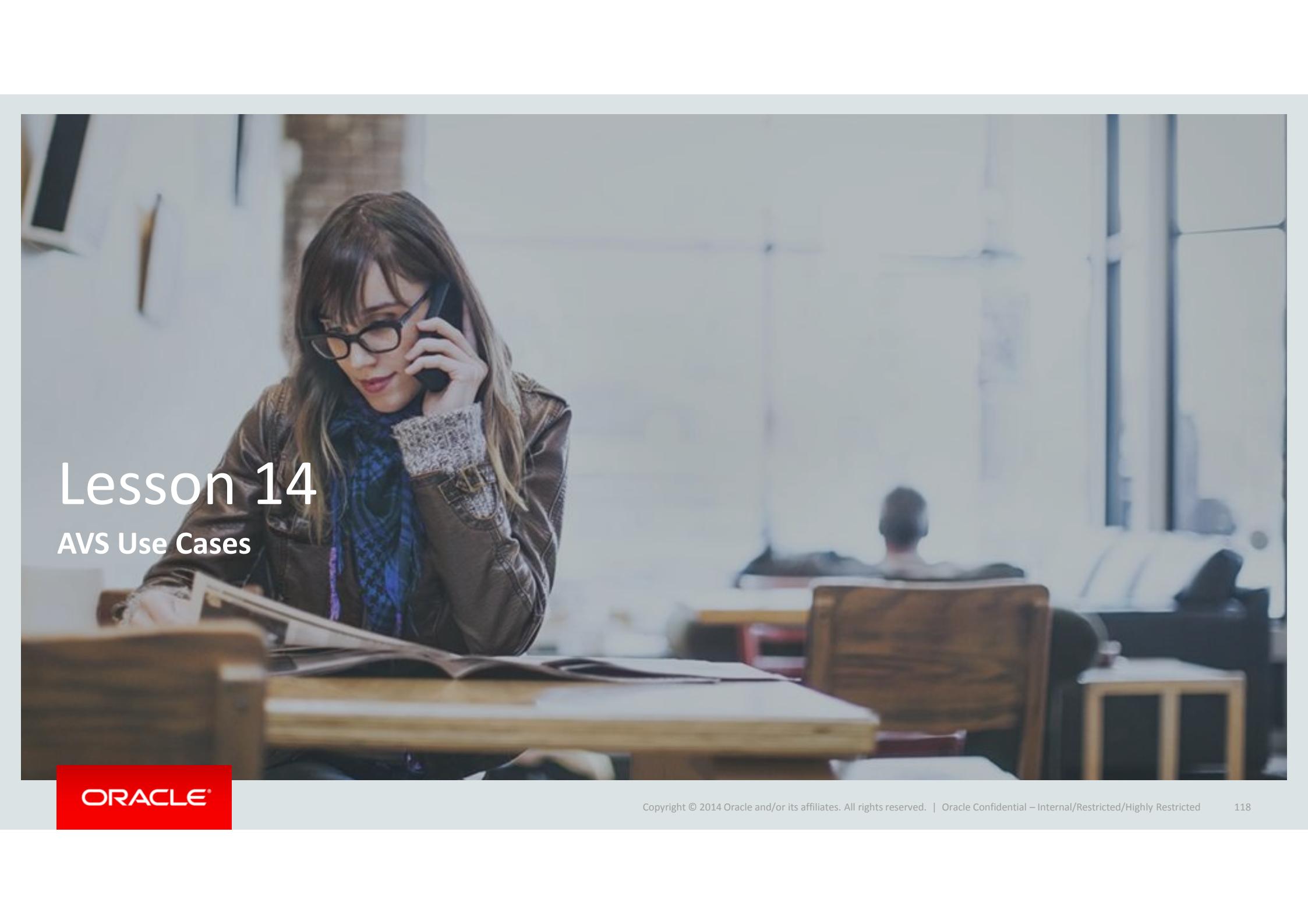
1 ➔ Lesson 1 - 5

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

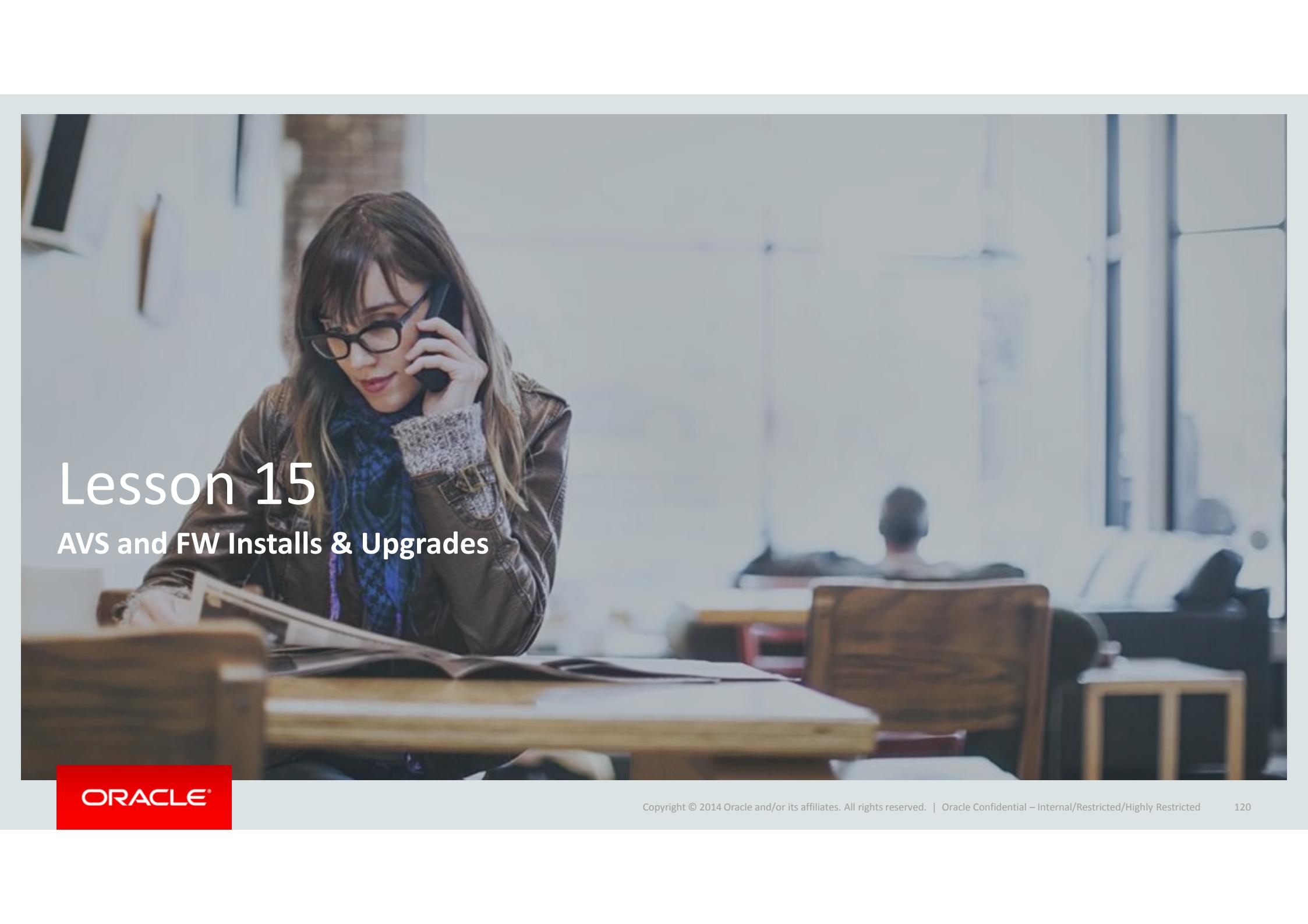
ORACLE®

Copyright © 2014 Oracle and/or its affiliates. All rights reserved. | Oracle Confidential – Internal/Restricted/Highly Restricted

118

# 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

ORACLE®

Copyright © 2014 Oracle and/or its affiliates. All rights reserved. | Oracle Confidential – Internal/Restricted/Highly Restricted

120

# 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>

**ORACLE®**  
Oracle Software Delivery Cloud

Sign Out Cloud Portal (Main) Language (English) FAQs

Terms & Restrictions Search Download

### Media Pack Search

Instructions

- Review the [License List](#) to determine which Product Pack or Packs you need to download.
- Select the Product Pack and Platform and click "Go".
- If there is only one result, you will see the download page. If there are multiple results, select one and click "Continue".

Select a Product Pack

Platform

#### Results

Select	Description	Release	Part Number	Updated	# Parts / Size
<input checked="" type="radio"/>	<a href="#">Oracle Audit Vault and Database Firewall (12.1.2.3.0), Linux x86-64</a>	12.1.2.3.0	B79779-01	NOV-14-2014	3 / 6.7G
<input type="radio"/>	<a href="#">Oracle Audit Vault and Database Firewall (12.1.2.2.0) Media Pack for Linux x86-64</a>	12.1.2.2.0	B78725-01	AUG-01-2014	3 / 6.7G
<input type="radio"/>	<a href="#">Oracle Audit Vault and Database Firewall (12.1.2.1.0) Media Pack for Linux x86-64</a>	12.1.2.1.0	B78174-01	JUN-30-2014	3 / 6.7G
<input type="radio"/>	<a href="#">Oracle Audit Vault and Database Firewall (12.1.1.5.0) Media Pack for Linux x86-64</a>	12.1.1.5.0	B79104-01	SEP-05-2014	3 / 5.7G
<input type="radio"/>	<a href="#">Oracle Audit Vault and Database Firewall (12.1.1.4.0) Media Pack for Linux x86-64</a>	12.1.1.4.0	B78426-01	JUL-14-2014	4 / 5.6G

**ORACLE®**  
Oracle Software Delivery Cloud

Sign Out Cloud Portal (Main) Language (English) FAQs

Terms & Restrictions Search Download

### Oracle Audit Vault and Database Firewall (12.1.2.3.0), Linux x86-64

**TIP** View the Readme file(s) to help decide which files you need to download.

Print this page with the list of downloadable files. It contains a list of the part numbers and their corresponding description that you may need to reference during the installation process.

Hi Melody, by clicking the download button, you agree Oracle's [Terms & Restrictions](#) apply to your use of the software on this portal. Not Melody? Do not download the software and [login with your account](#).

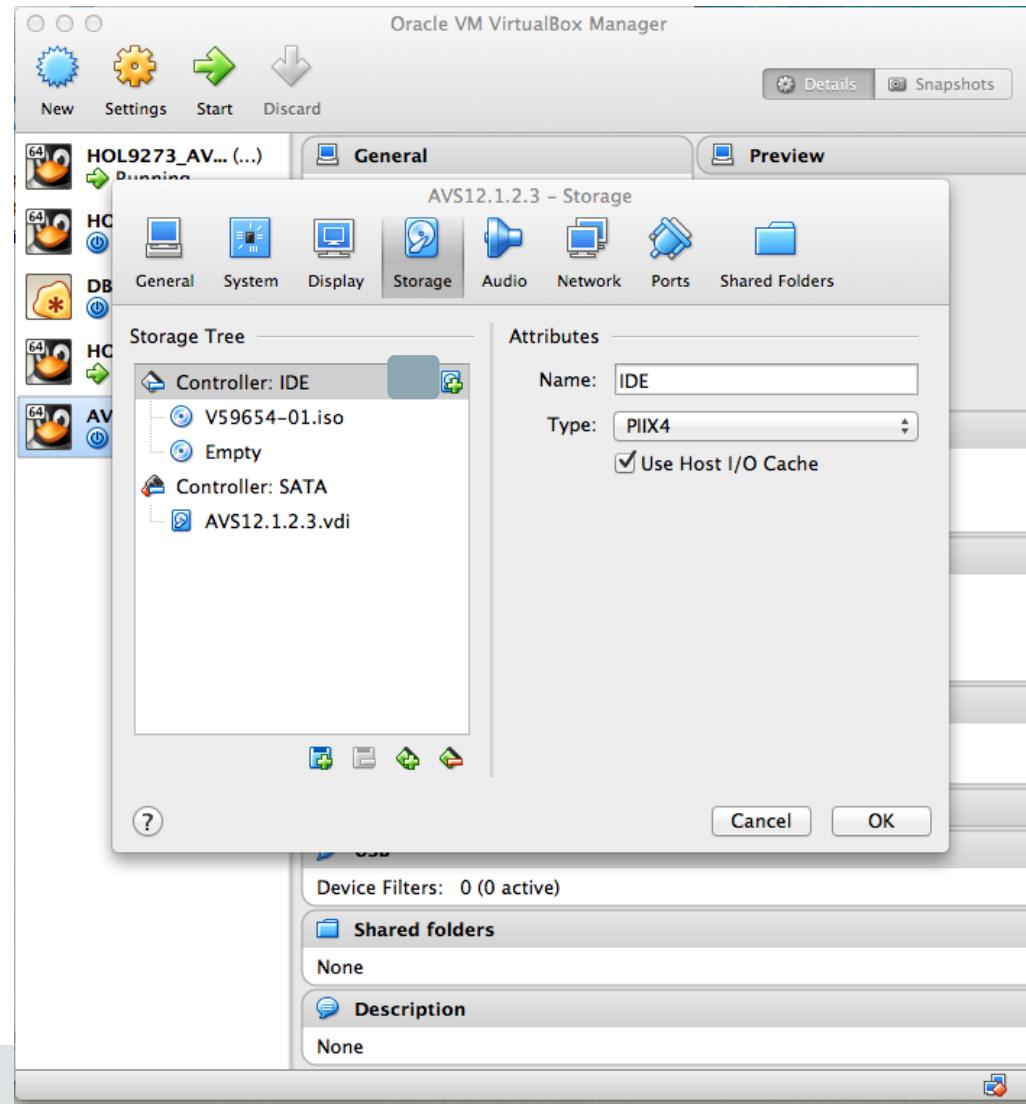
#### Oracle Audit Vault and Database Firewall (12.1.2.3.0) v1, Linux x86-64

Select	Name	Part Number	Size (Bytes)
<input type="button" value="Download"/>	Oracle Audit Vault and Database Firewall SERVER 12.1.2.3 (12.1.2 BP3)	V59654-01	4.5G
<input type="button" value="Download"/>	Database Firewall 12.1.2.3 (12.1.2 BP3)	V59655-01	2.2G
<input type="button" value="Download"/>	AVDF Utility zip 12.1.2.3 (12.1.2 BP3)	V59656-01	49K

Total: 3

Highly Restricted 122

- Mount iso file

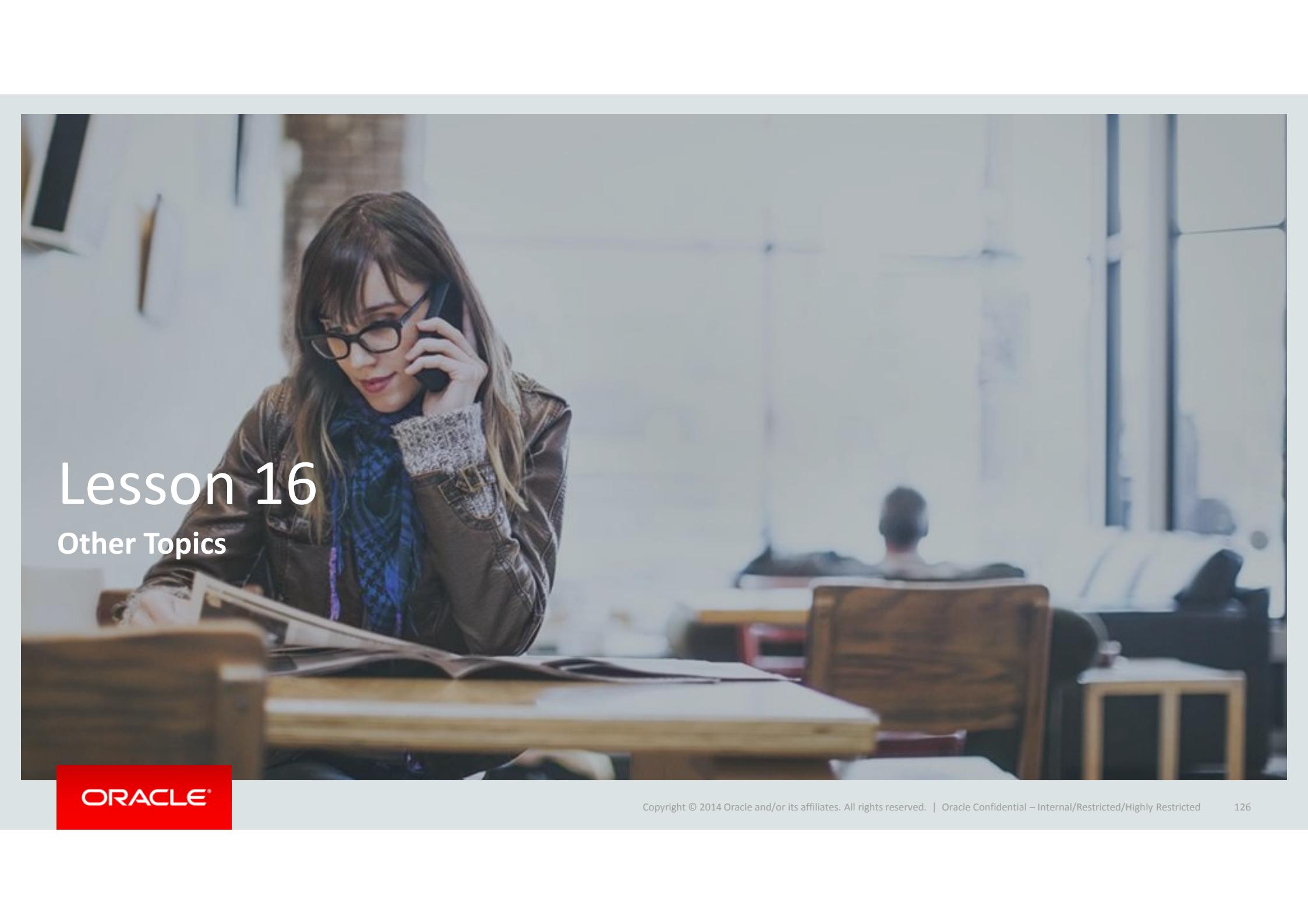


ORACLE®



# 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

ORACLE®

Copyright © 2014 Oracle and/or its affiliates. All rights reserved. | Oracle Confidential – Internal/Restricted/Highly Restricted

126

# 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 High Availability

Current status This current server (10.244.202.114) is standalone

Configure this server as \*  Primary server  Secondary server

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

Configure High Availability Save

Current status This current server (10.244.202.114) is standalone

Configure this server as \*  Primary server  Secondary server

Primary server IP address \*

Primary server certificate \*

Copyright © 2014 Oracle and/or its affiliates. All rights reserved.

Oracle Confidential – Internal/Restricted/Highly Restricted

# New HA UI

- Then prompts to switch to primary

Settings Saved

Now visit the primary server at <https://10.244.202.116> to initiate pairing.

Configure High Availability

Current status: This current server (10.244.202.114) is standalone

Configure this server as \*:  Primary server  Secondary server

Primary server IP Address \*: 10.244.202.116

"HA DOMAIN SECURED CERT" \*:

**Reset** **Save**

# 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

Configure High Availability

**Initiate Pairing**

Current status	This current server (10.244.202.114) is standalone
Configure this server as *	<input checked="" type="radio"/> Primary server <input type="radio"/> Secondary server
Please make sure the following secondary server has saved the current server's IP and certificate before pairing.	
Secondary server IP address*	<input type="text"/>
Secondary server certificate*	<input type="text"/>

## 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 :

High Availability Status	
Status	High Availability mode is enabled.
Secondary server IP address	10.244.202.117
Secondary server certificate	<pre>-----BEGIN CERTIFICATE----- MIIFlzCCA3+gAwIBAgIJANoMjhEKxZzdMA0GCSqGSIb3DQEBBQUAMDsxOTA3BgNV BAMMEFWU19DQV9DZXJ0LWE2ZDdkMD1kLTmxODAtNDNkMC04NjNkLTfMNWJjMTRi Yjg2YjAeFw0xNDA3MjEyMjMzMTzaFw0yNDA3MTgyMjMzMTzaMDsxOTA3BgNVBAMM MEFWU19DQV9DZXJ0LWE2ZDdkMD1kLTmxODAtNDNkMC04NjNkLTfMNWJjMTRiYjg2</pre>

# iSCSI SAN support for Audit Repository

**ORACLE® Audit Vault Server**

avadmin | Help | Logout

Home Secured Targets Firewalls Hosts **Settings**

Home > Settings > SAN

**Security**

- Manage Admins
- Manage Access
- Change Password

**Certificate**

**Storage**

**SAN**

Repository

Archiving

Manage Policies

Policy Usage

**SAN Servers**

Drop Register

Actions ▾

	Storage Name ▾	IP Address	Port	Method	Registered To	Action
<input type="checkbox"/>	SAN Server 1	10.240.114.221	3260	sendtargets	slc02vjp.us.oracle.com(10.240.114.150) - Standalone	Discover
<input type="checkbox"/>	SAN Server 2	10.240.114.222	3260	isns	slc02vjp.us.oracle.com(10.240.114.150) - Standalone	Discover

1 - 2 of 2

**iSCSI Initiator Name**

iqn.1988-12.com.oracle:13c619bf73c

**ORACLE®**

Copyright © 2014 Oracle and/or its affiliates. All rights reserved. | 132

# 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

**ORACLE® Audit Vault Server**

avadmin | Help | Logout

Home Secured Targets Firewalls Hosts **Settings**

Home > Settings > Manage Archive Locations > Create Archive Location

**Security**

- Manage Admins
- Manage Access
- Change Password
- Certificate

**Storage**

- SAN
- Repository

**Archiving**

- Manage Policies
- Policy Usage

**Create Archive Location**

Transfer Method  Secure Copy (scp)  Windows File Sharing (SMB)  Network File System (NFS)

Location Name \* NFS Archives

Remote Filesystem \* Create New Filesystem ▾

Address \* 10.240.114.120

Export Directory \* /nfs

Path \* /archives

**Save**

**ORACLE®**

Copyright © 2014 Oracle and/or its affiliates. All rights reserved. | 134

# 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.

The image displays two side-by-side configuration panels from the AVS (Advanced Virtual Server) software.

**Syslog Configuration:** This panel is titled "Syslog". It contains two main sections: "Syslog Destinations (UDP)" and "Syslog Destinations (TCP)". Each section has a large, empty rectangular input field for specifying a destination address. Below these fields is a "Syslog Categories" section with four checkboxes: "Alert" (checked), "Debug" (unchecked), "Info" (unchecked), and "System" (unchecked). In the top right corner of the panel is a blue "Save" button.

**HP ArcSight SIEM Configuration:** This panel is titled "HP ArcSight SIEM". It contains two sections: "Enable ArcSight event forwarding" (with an unchecked checkbox) and "ArcSight destinations (TCP)" and "ArcSight destinations (UDP)" (each with an empty rectangular input field for specifying a destination address). Below these fields is an "Event Categories" section with three checkboxes: "Debug" (unchecked), "Info" (unchecked), and "System" (unchecked). In the top right corner of the panel is a blue "Save" button.

# 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

Modify Archive Location

Transfer Method	<input checked="" type="radio"/> Secure Copy (scp) <input type="radio"/> Windows File Sharing (SMB) <input type="radio"/> Network File System (NFS)
Location Name *	Backup Server 2
Address *	192.168.56.10
Path *	/home/avbackup
Port *	22
Username *	root
Authentication Method	<input type="radio"/> Key-based Authentication <input checked="" type="radio"/> Password Authentication
Password *	[Redacted]
Confirm Password *	[Redacted]

## 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

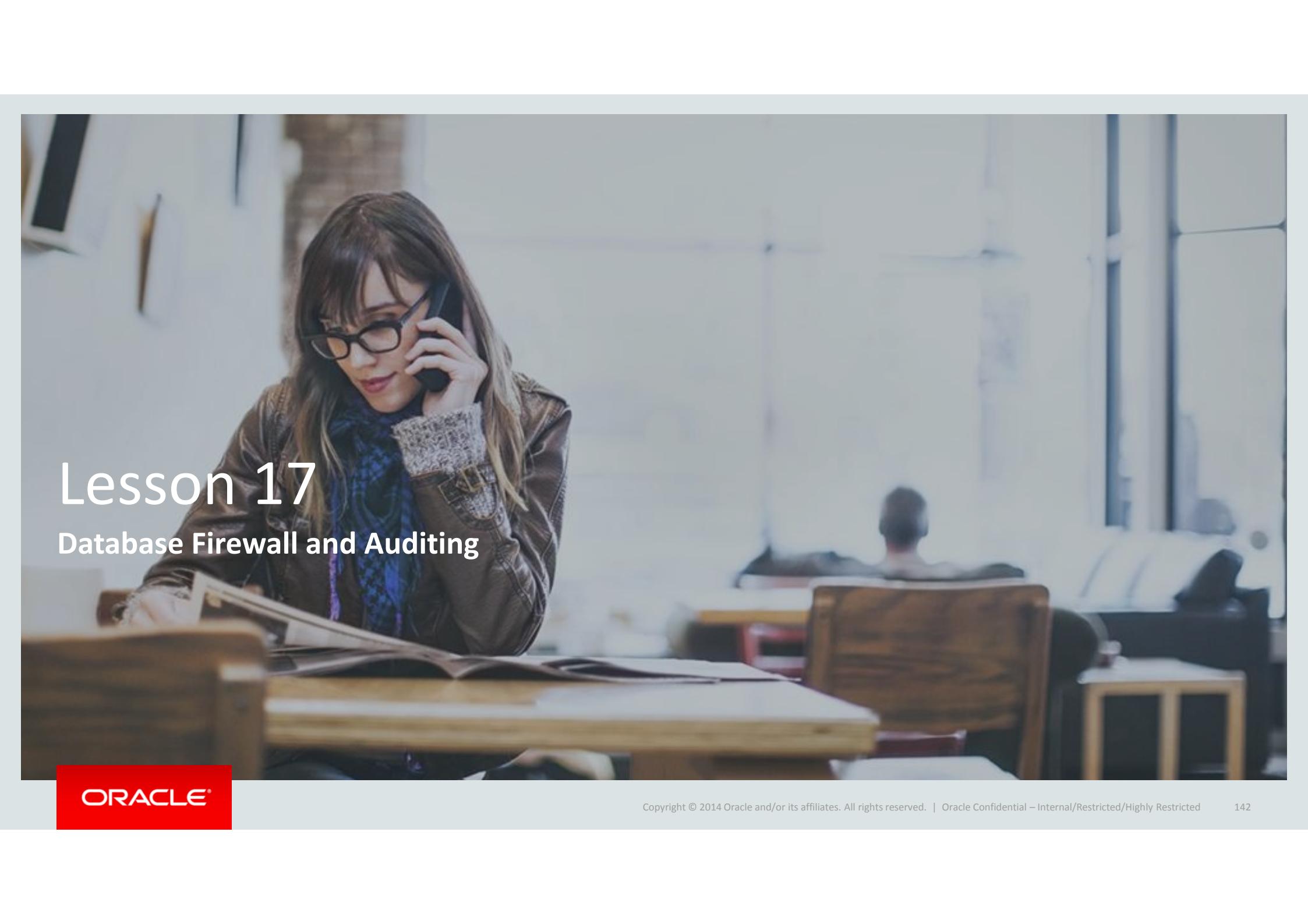
1 ➔ Lesson 1 - 5

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

ORACLE®

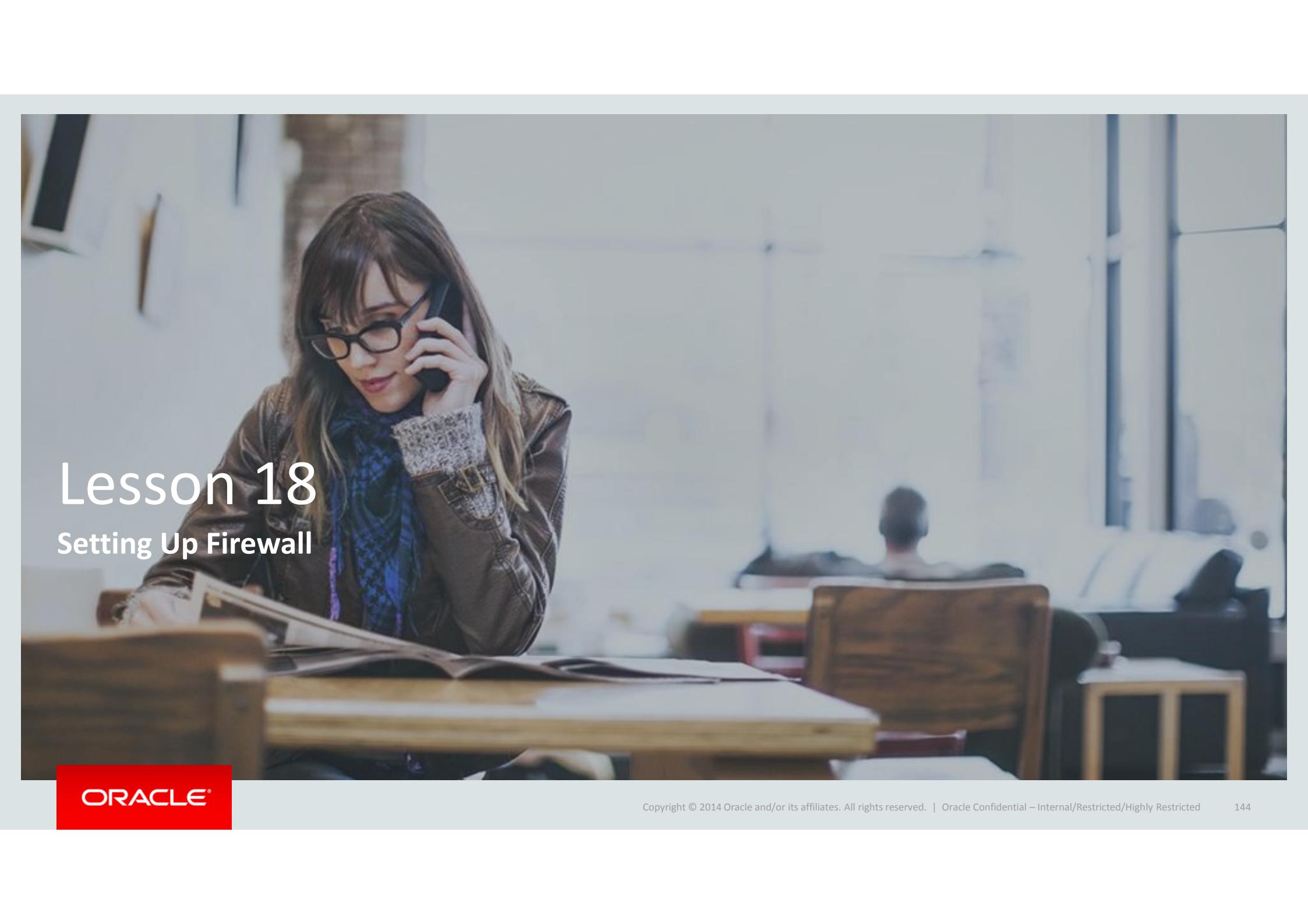
Copyright © 2014 Oracle and/or its affiliates. All rights reserved. | Oracle Confidential – Internal/Restricted/Highly Restricted

142

# Auditing & Database Firewall

## Flexible Security

	<b>Monitoring (Database Firewall)</b>	<b>Auditing</b>
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

ORACLE®

Copyright © 2014 Oracle and/or its affiliates. All rights reserved. | Oracle Confidential – Internal/Restricted/Highly Restricted

144

# 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** your 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]

Configure Network Services

Enter IP addresses to specify DNS servers. Specifying one or more DNS servers is optional, but hostnames can only be translated if at least one DNS server is specified.

DNS Server 1	disabled
DNS Server 2	disabled
DNS Server 3	disabled

Enter a space separated list of IP addresses to permit access from specific clients; enter 'all' to permit unrestricted access

Web Access	all
------------	-----

Set SSH Access to 'disabled' to block access from any IP address; enter a space separated list of IP addresses to permit access from specific clients; enter 'all' to permit unrestricted access

SSH Access	all
------------	-----

Set SNMP Access to 'disabled' to block access from any IP address; enter a space separated list of IP addresses to permit access from specific systems; enter 'all' to permit unrestricted access

SNMP Access	all
-------------	-----

# 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]

The screenshot shows the Oracle Database Firewall configuration interface. The left sidebar lists System, Network, Services, Status, Date and Time, Keyboard, Public Keys, Audit Vault Server, Connectors, Syslog, and Users. The main area has tabs for Management Interface and Proxy Ports. Under Management Interface, the Name field is set to "dbfw01.local" and is circled with a red number 1. Under Proxy Ports, a new row is being added with Traffic Source Id "15211", Port "15211", Enabled checked, and an Add button. These three items are circled with red numbers 2, 3, and 4 respectively.

Management Interface
Settings
IP Address: 192.168.56.201
Network Mask: 255.255.255.0
Gateway: 192.168.56.100
Name: dbfw01.local <span style="color:red;">1</span>
Device
MAC Address: 08:00:27:a7:68:3f
Bus Info: 0000:00:03.0
Identifier: 82540EM Gigabit Ethernet Controller
Manufacturer: Intel Corporation
Link: yes
Proxy Ports
Traffic Source Id: 15211 <span style="color:red;">2</span>
Port: 15211 <span style="color:red;">2</span>
Enabled: <input checked="" type="checkbox"/> <span style="color:red;">3</span>
Add <span style="color:red;">4</span>

# 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]

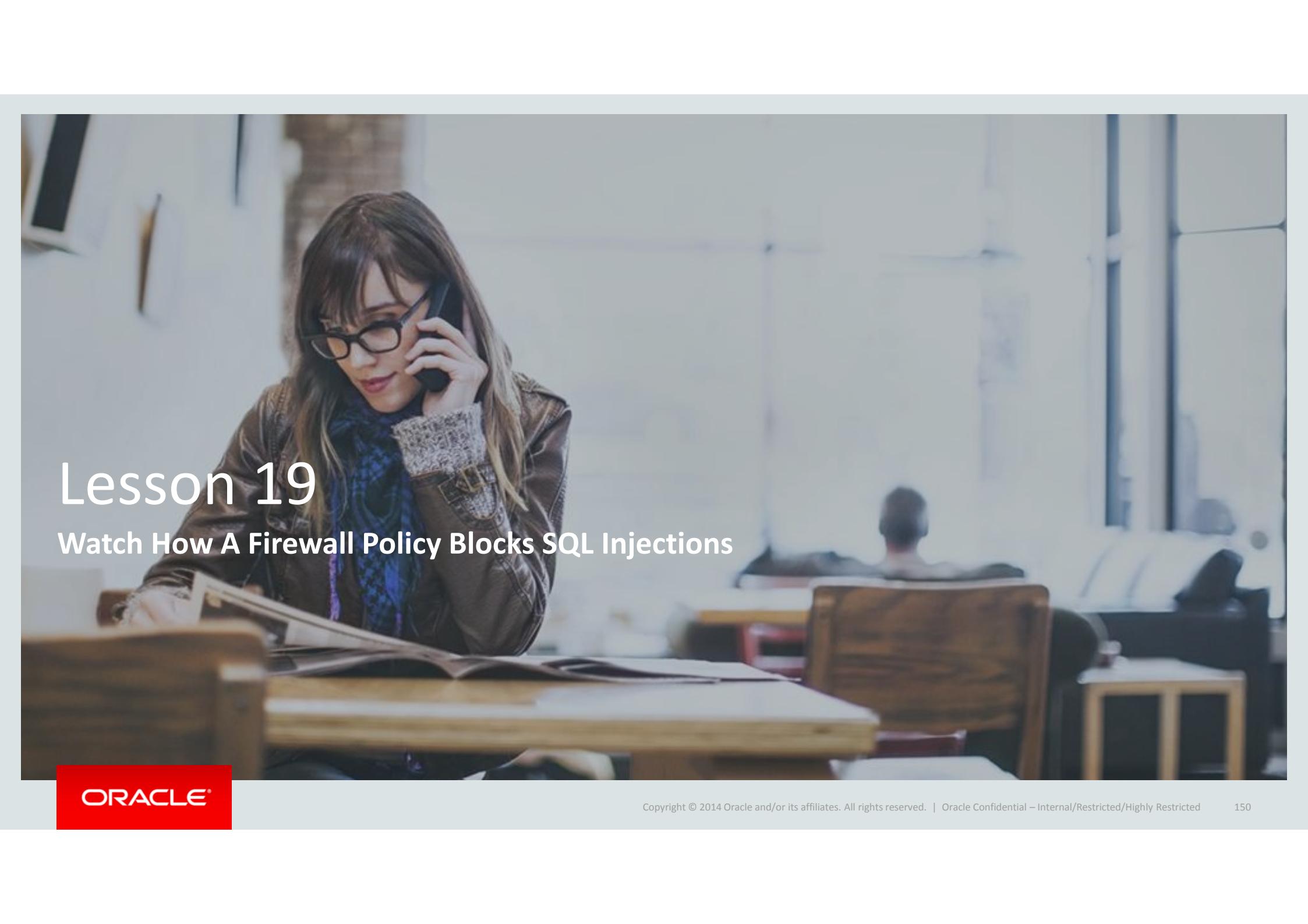
# Setting Up Firewall

## 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

```
Test Diagnostics

Checking if exists: /etc/platform.conf - OK
Checking if exists: /usr/local/dbf/w/etc/mwecsvc.conf - OK
Checking if exists: /usr/local/dbf/w/etc/pnkerpem - OK
Checking if exists: /usr/local/dbf/w/etc/cert.crt - OK
Checking if /dev/mapper/vg_root_lv_root mounted on / - OK
Checking if /dev/mapper/vg_root_lv_tm mounted on /tmp - OK
Checking if /dev/mapper/vg_root_lv_home mounted on /home - OK
Checking if /dev/mapper/vg_root_lv_local_dbfw mounted on /usr/local/dbfw - OK
Checking if /dev/mapper/vg_root_lv_local_dbfw_lmp mounted on /usr/local/dbfw/tmp - OK
Checking if /dev/mapper/vg_root_lv_var_log mounted on /var/log - OK
Checking if /dev/mapper/vg_root_lv_var_lmp mounted on /var/tmp - OK
Checking if /dev/mapper/vg_root_lv_var_www mounted on /var/www - OK
Checking if /dev/mapper/vg_root_lv_var_www_lmp mounted on /var/www/tmp - OK
Checking if /dev/mapper/vg_root_lv_oracle mounted on /var/lib/oracle - OK
Checking if /dev/mapper/vg_root_lv_var_dbfw mounted on /var/dbfw - OK
Checking if fmpfs mounted on /dev/shm - OK
Checking network address - OK
Checking network mask - OK
Checking DNS: - OK
Checking gateway - OK
Checking if certificate is valid at least for one year: - OK
Checking if backgrounddb is running: - OK
Checking if HTTP server is running: - OK
Checking if cron is running: - OK
Checking if database is running: - OK
Checking if mwecsvc is running: - OK
Checking that IPv6 is disabled - OK
Checking Oracle listener - OK
Checking Oracle database processes - OK
Checking netfilter rules - OK
Current platform: controller
Script executed as: oracle
```

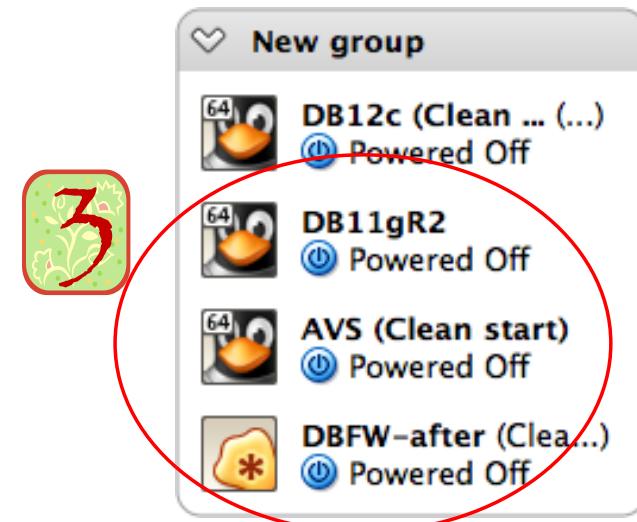
A photograph of a young woman with long brown hair and glasses, wearing a brown leather jacket over a patterned top. She is sitting at a wooden desk in what appears to be a classroom or library setting, looking down at some papers or books. In the background, other students are visible at their desks.

# 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.EMPTYTYPE, 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	<a href="#">Borst, Hugo</a>	Full-Time				Engineering	Xellerate Users
264	<a href="#">Drop, Frank</a>	Full-Time	Project Manager	<a href="#">Jansen, Henk</a>	101	Engineering	Xellerate Users
2	<a href="#">Jansen, Henk</a>	Full-Time	End-User			Engineering	Xellerate Users
4	<a href="#">Karelse, Karel</a>	Full-Time				Engineering	Xellerate Users
6	<a href="#">Koelewijn, Frans</a>	Full-Time	DBA	<a href="#">Jansen, Henk</a>	101	Engineering	Xellerate Users
129	<a href="#">Opedijk, Jeen</a>	Full-Time	Project Manager	<a href="#">Jansen, Henk</a>	101	Engineering	Xellerate Users
47	<a href="#">Stok, Frank</a>	Full-Time				Engineering	Xellerate Users
146	<a href="#">krabe, martijn</a>	Full-Time	DBA	<a href="#">Jansen, Henk</a>	101	Engineering	Xellerate Users
							Xellerate

# 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

My HR Application

Welcome Malicious Malfoy!  
Privileges: [ENGINEERING, SELECT]

Home | Help | About | Logout

**Search Employee**

HR ID	<input type="text"/>	Active	<input type="button" value="... Choose a value ..."/>
Employee Type	<input type="button" value="... Choose a value ..."/>	Position	<input type="text"/>
First Name	<input type="text" value="or 4=4—"/>	Last Name	<input type="text"/>
Department	<input type="text"/>	Organization	<input type="text"/>

**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.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' and upper(a.FIRSTNAME) like 'OR 4=4--%' order by a.LASTNAME, a.FIRSTNAME
```

HR ID	Full Name	Emp Type	Position	Manager	Cost Center	Department	Organization
264	<a href="#">Drop, Frank</a>	Full-Time	Project Manager	<a href="#">Jansen, Henk</a>	101	Engineering	Xellerate Users
244	<a href="#">y, x</a>	Full-Time	Administrator I	<a href="#">Jansen, Henk</a>	101	Corporate	Xellerate Users
245	<a href="#">x, i</a>	Full-Time	Administrator I	<a href="#">Jansen, Henk</a>	101	Corporate	Xellerate Users
190	<a href="#">ellis, harry</a>	Full-Time	DBA	<a href="#">Jansen, Henk</a>	101	Corporate	Xellerate Users
188	<a href="#">janssen, jim</a>	Full-Time	DBA	<a href="#">Jansen, Henk</a>	101	Corporate	Xellerate Users
186	<a href="#">kaptijn, joop</a>	Full-Time	DBA	<a href="#">Jansen, Henk</a>	101	Corporate	Xellerate Users
166	<a href="#">kras, frank</a>	Full-Time	Administrator I	<a href="#">Jansen, Henk</a>	101	Engineering	Xellerate Users
152	<a href="#">krabe, patrick</a>	Full-Time	DBA	<a href="#">Jansen, Henk</a>	101	Corporate	Xellerate Users
148	<a href="#">krabe, henk</a>	Full-Time	DBA	<a href="#">Jansen, Henk</a>	101	Corporate	Xellerate Users
126	<a href="#">schonis, peter</a>	Full-Time	DBA	<a href="#">Jansen, Henk</a>	101	Corporate	Xellerate Users
65	<a href="#">Forde, John</a>	Full-Time	DBA	<a href="#">Jansen, Henk</a>	101	Corporate	Xellerate Users
24	<a href="#">Kennis, Ferrie</a>	Full-Time	Documentation Clerk	<a href="#">Jansen, Henk</a>	101	Sales	Xellerate Users
6	<a href="#">Koelewin, Frans</a>	Full-Time	DBA	<a href="#">Jansen, Henk</a>	101	Engineering	Xellerate Users

**Employees**

[Search Employees](#)

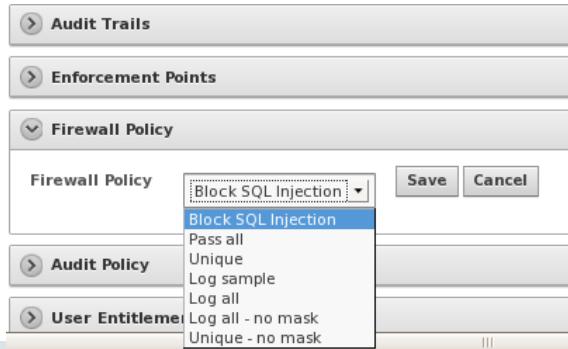
[Absence And Attendance](#)

[Timesheets](#)

[Vacation](#)

# 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**

Firewall Policies				
Search		Go	Actions ▾	
Name	Database Type	Description	Deployed	Created ▾
Block SQL Injection	Oracle Database	..	Yes	8/30/2014 2:49:30 AM
1 - 1				

- 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

The screenshot shows the Oracle Firewall Policy configuration interface. On the left, there's a sidebar with sections like 'Exception Rules', 'Analyzed SQL', 'Profile Name' (set to '-Default-'), 'Novelty Policies (Any)', 'Novelty Policies (All)', 'Default Rule', and 'Policy Controls'. The main area displays a table with columns 'Action', 'Logging Level', and 'Threat Severity'. A modal dialog box titled 'Edit Default Policy' is open in the center. It contains fields for 'Action' (set to 'Block'), 'Logging Level' (set to 'Always'), and 'Threat Severity' (set to 'Major'). Below these fields is a 'Substitution' text area containing the SQL query: 'select 100 from dual where 1=2'. At the bottom of the dialog are 'Cancel' and 'Apply Changes' buttons. The background table shows zero entries across all categories.

# Review HR App SQL using All Activity Report

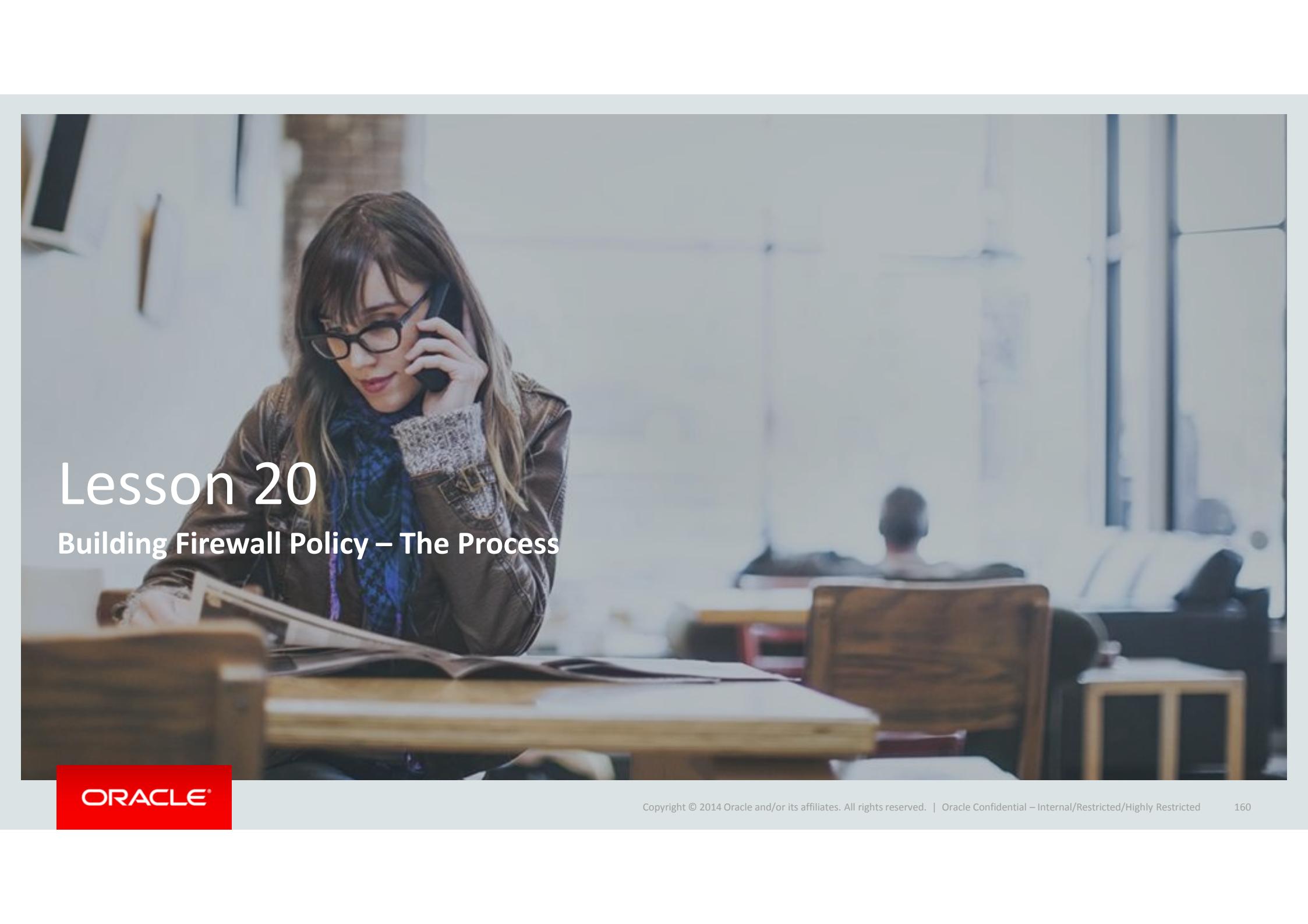
- While logged in as AVAUDITOR
- Browse All Activity Report
- Click “Action” button > ‘Select Columns’ > “Action Taken (Event)”
- Move “Action Taken (Event)” into the right window (‘Display in report’)
- Apply

The screenshot shows the Oracle Audit Vault Server interface. The top navigation bar includes Home, Secured Targets, Reports (selected), Policy, and Settings. The breadcrumb path is Home > Reports > All Activity Report. On the left, a sidebar lists Built-in Reports (Audit Reports selected), Compliance Reports, Specialized Reports, Custom Reports (Uploaded Reports, Interactive Reports), and Report Workflow (Report Schedules, Generated Reports). The main panel is titled 'All Activity Report' and contains a search bar and an 'Actions' dropdown. Below is a 'Select Columns' section. A list of columns is shown, divided into 'Do Not Display' and 'Display in Report'. The 'Action Taken(Event)' column is highlighted with a blue selection bar and is being moved from the left list to the right list using a 'Move' button. The right list includes Event Time(Event), Event Name(Event), Target Object(Target), Event Status(Event), Command Text(Statement), and Name(Event). At the bottom are 'Cancel' and 'Apply' buttons.

# 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.EMPTYTYPE, 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.EMPTYTYPE, 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

ORACLE®

Copyright © 2014 Oracle and/or its affiliates. All rights reserved. | Oracle Confidential – Internal/Restricted/Highly Restricted

160

# Building Firewall Policies

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

Firewall Policies				
Name ▾		Database Type	Description	Deployed
My Policy 3	Oracle Database	Novelty Policies	No	12/3/2014 7:23:25 PM
My Policy 2	Oracle Database	This one is "trust but verify" example	No	12/3/2014 6:50:09 PM
My Policy 1	Oracle Database	This is to build a SQL based white list example	No	12/3/2014 6:57:08 PM
Blocking SQL Injections	Oracle Database	..	No	8/30/2014 1:24:42 AM

1 - 4

# 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-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”

The screenshot shows a user interface for managing firewall policies. At the top, there's a navigation bar with tabs for 'Policy', 'Firewall Policy', 'Create Policy', 'Oracle Database', and 'My policy **1**'. Below the navigation is a section titled 'Analyzed SQL' with a 'Modify SQL' button. A message 'No clusters found.' is displayed. The main area is a large, empty text input field.

# Building A Firewall Policy - Process

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

The screenshot shows a configuration dialog with the following settings:

- Profile: Default
- Secured Target: Oracle11gR2DB
- Event Time: is in the last 1 hours
- Buttons: Apply (highlighted in blue), Cancel

Below the dialog is a toolbar with the following buttons:

- Search icon
- Go
- Actions ▾
- Set Policy
- Remove SQL

[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

The screenshot shows the 'Set Policy Controls' dialog with the following settings:

- Action: Pass
- Logging Level: Unique
- Threat Severity: Unassigned
- Escalate action after a certain number of instances?
- Buttons: Cancel, Save

# Building A Firewall Policy - Process

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



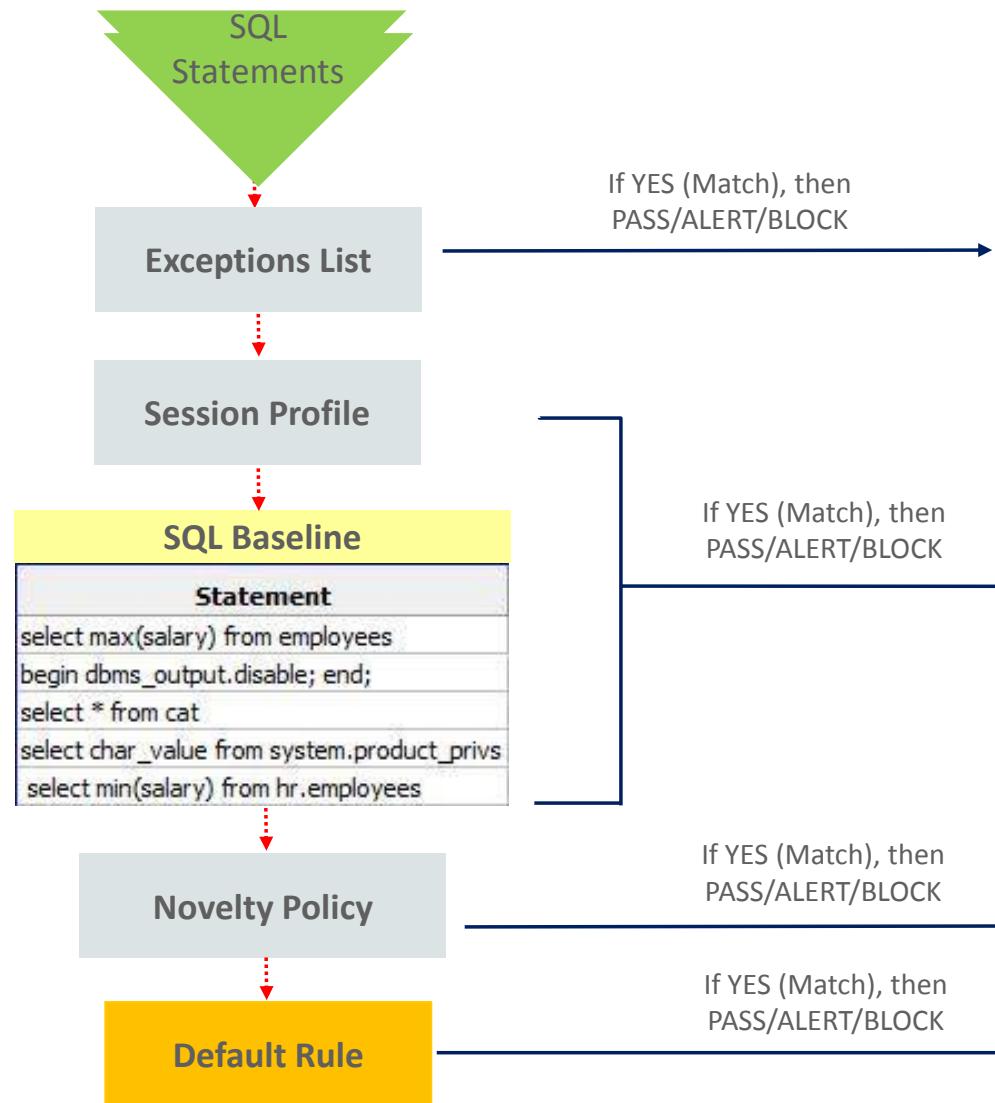
- You are done with a new Firewall Policy creation. Save + **Publish** !
  - Be sure to **Deploy** the policy !
4. Tighten access by rules for out-of-policy statements (warn, block, substitute, etc.)
    - Enforce blocking (optional) by rules for out of-policy statement
  5. Deploy in production with alert on out-of-policy activity

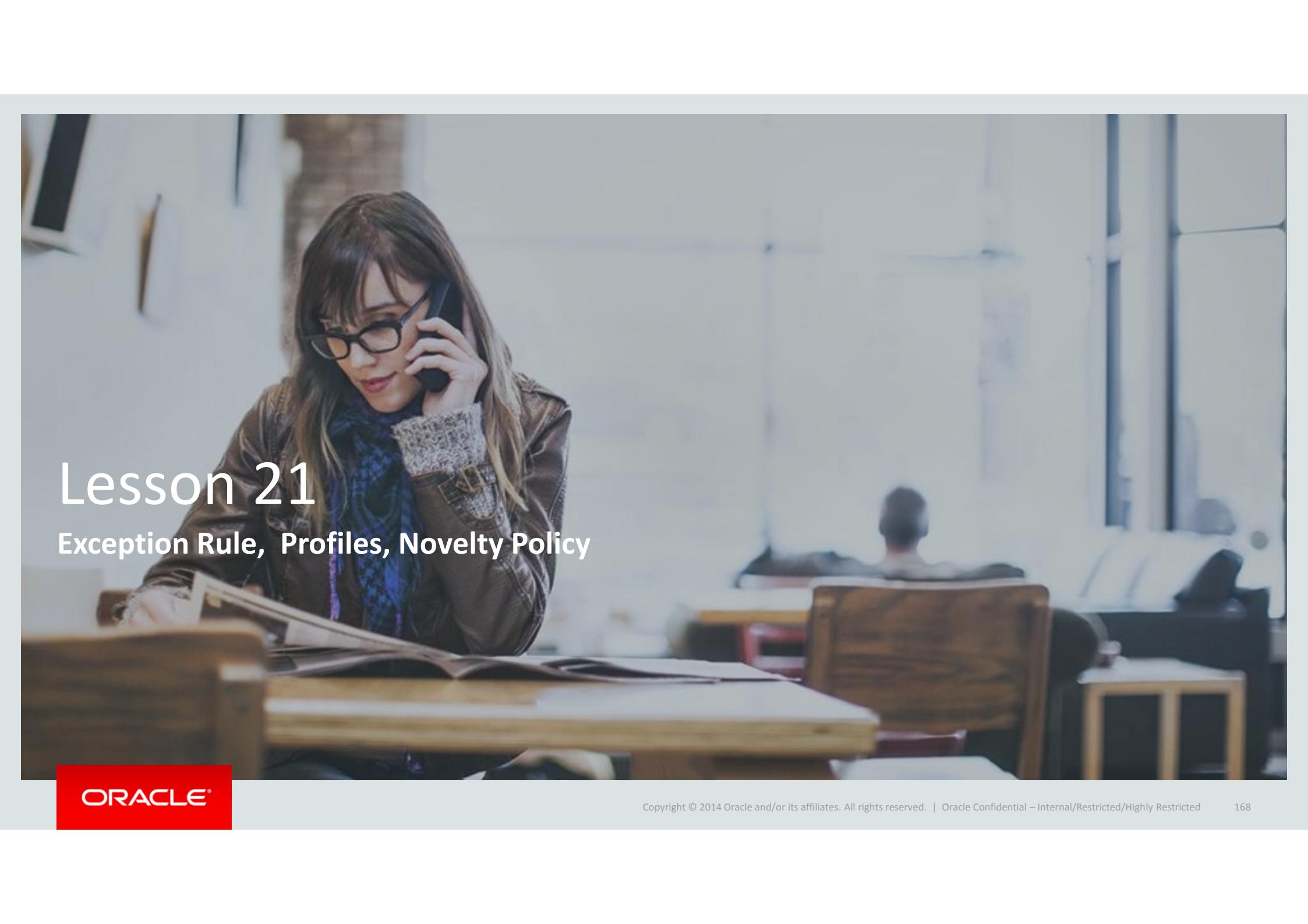
# Building A Firewall Policy - Process

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-policy statement (block)
5. Deploy policy in production with alert on out-of-policy activity

The screenshot shows the Oracle Audit Vault Server interface. At the top, there's a navigation bar with tabs: Home, Secured Targets, Reports, Policy, and Settings. The Home tab is currently selected. Below the navigation bar, there are filters for 'View data for' (set to 'Last 24 Hours') and 'Refresh Interval' (set to '5 Minutes'). A 'Go' button and a message indicating the data was 'Refreshed at 12/2/2014 7:59:06 PM'. On the left, a sidebar titled 'Recently Raised Alerts' lists two entries: 'Database Firewall Alert' from 12/2/2014 5:53:19 PM and another 'Database Firewall Alert' from 12/2/2014 5:53:06 PM. To the right of the sidebar is a section titled 'Attestation Actions' with the message 'No reports need attestation at this time.' In the bottom right corner of the interface, there's a small number '166'.

# Firewall Policy Flow





# Lesson 21

## Exception Rule, Profiles, Novelty Policy

ORACLE®

Copyright © 2014 Oracle and/or its affiliates. All rights reserved. | Oracle Confidential – Internal/Restricted/Highly Restricted

168

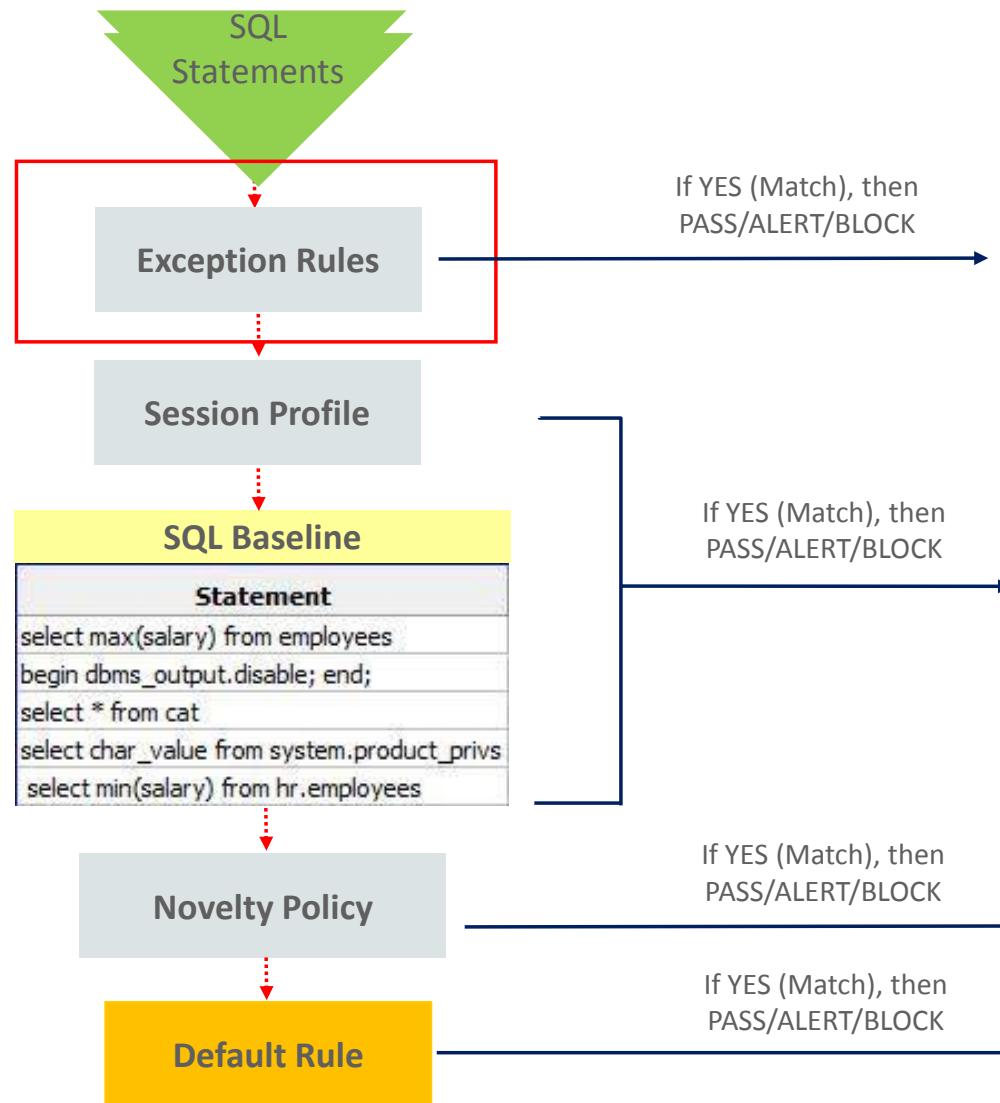
# Building More Firewall Policies

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

Firewall Policies				
Search		Go	Actions	
Name	Database Type	Description	Deployed	Created
My Policy 3	Oracle Database	Novelty Policies	No	12/3/2014 7:23:25 PM
My Policy 2	Oracle Database	This one is "trust but verify" example	No	12/3/2014 6:50:09 PM
My Policy 1	Oracle Database	This is to build a SQL based white list example	No	12/3/2014 6:57:08 PM
Blocking SQL Injections	Oracle Database	..	No	8/30/2014 1:24:42 AM

1 - 4

# Exception Rules



# 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

The dialog box has a title 'Create New Set'. It contains a 'New Set Name \*' field with the value 'VIPs'. Below it is a note: 'All sets must have at least one member. Please enter your set's first member here \*' followed by a 'melody' input field. At the bottom are 'Cancel' and 'Create Set' buttons.

- Next : apply an enforcement policy to this Set

# Exception Rules

## Exclude a new DB User Set

- Select 'Add Exception' button under Exception Rules section

Policy Overview

Name \* new policy

Database Type Oracle Database

Description ..  
2 of 2000

Exception Rules

No exception rules have been defined.

Add Exception

## 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 !

Exception Rule

Exception Rule \* Always Allow These VIPs

Profile Sets

IP Address Set	Include	-- Not Set --
DB User Set	Exclude	VIPs
OS User Set	Include	-- Not Set --
DB Client Set	Include	-- Not Set --

Policy Controls

Action	Pass	Logging Level	Don't Log	Threat Severity	Unassigned
--------	------	---------------	-----------	-----------------	------------

Escalate action after a certain number of instances?

# 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

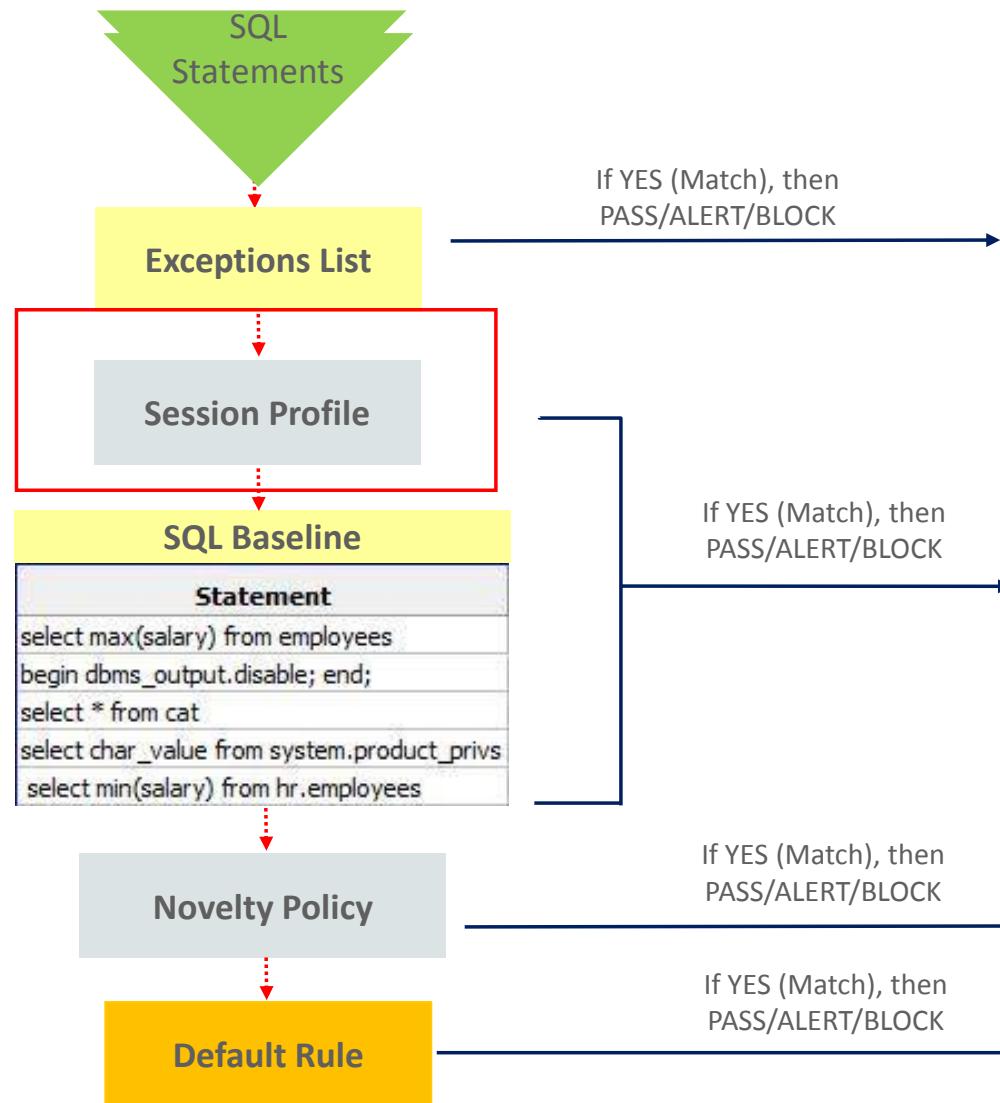
SQL*Plus: Release 11.2.0.3.0 Production on Tue Dec 9 08:36:39 2014

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

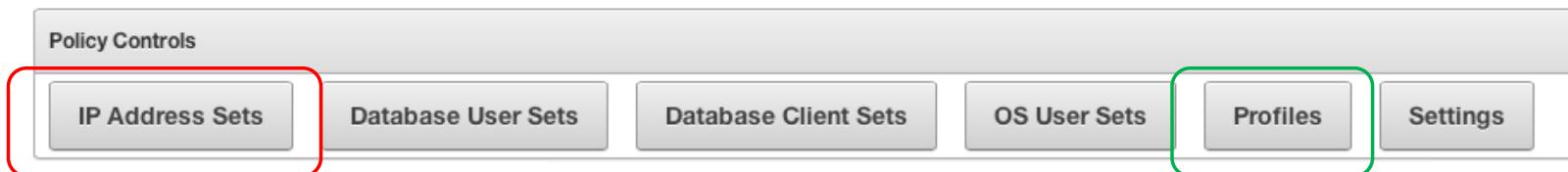
MELODY> select * from hr.jobs;
```

# Session Profile



# 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

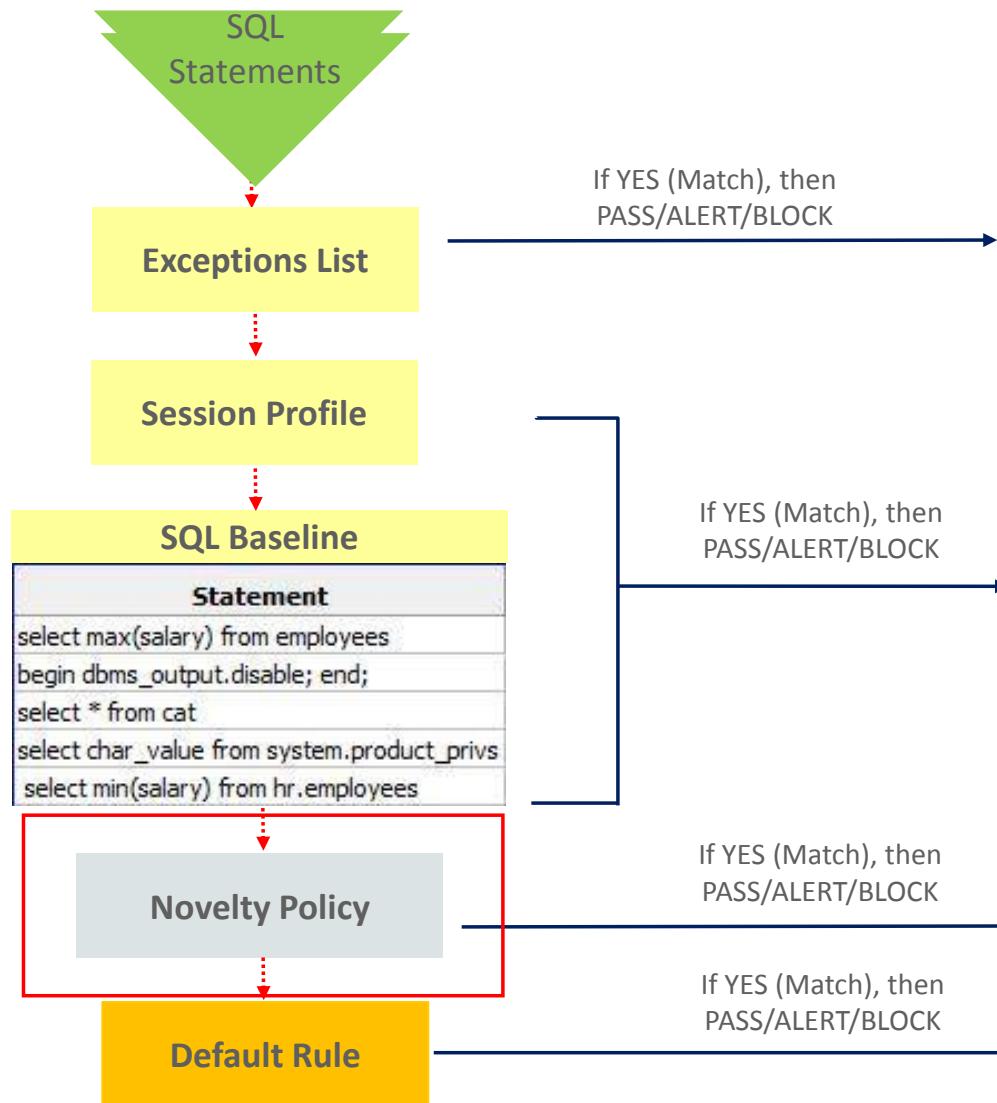
The screenshot shows a configuration dialog with the following fields:

- Profile: New Profile 1
- Secured Target: - Select -
- Event Time: is in the last 24 hours
- Change button

An arrow points from the left configuration to this dialog.

4. Now add “good SQL” to the policy

# Session Profile



# 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 Details

Novelty Rule \* Alert on all DDL

Statement Classes

Data Manipulation Readonly	<input type="checkbox"/>	Data Manipulation	<input type="checkbox"/>	Data Definition	<input checked="" type="checkbox"/>
Data Control	<input type="checkbox"/>	Procedural	<input type="checkbox"/>	Transaction	<input type="checkbox"/>
Composite	<input type="checkbox"/>	Composite with Transaction	<input type="checkbox"/>		

Policy Controls

Action	Warn	Logging Level	Always	Threat Severity	Minor
--------	------	---------------	--------	-----------------	-------

# 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 Details

Novelty Rule \* Alert on Sensitive Data Update

Statement Classes

Data Manipulation Readonly  Data Manipulation  Data Definition   
Data Control  Procedural  Transaction   
Composite  Composite with Transaction

Policy Controls

Action Warn Logging Level Always Threat Severity Major

Affected Tables

In Policy	Table Name	Secured Target Name
<input type="checkbox"/>	DEMO_HR_EMPLOYEES	Oracle11gR2DB
<input type="checkbox"/>	DBA_USERS	Oracle11gR2DB

# Novelty Policy

## 2 Rules Defined

**Policy Overview**

Name \*

Database Type Oracle Database

Description   
16 of 2000

**Exception Rules**

No exception rules have been defined.

**Analyzed SQL**

No clusters found.

**Novelty Policies (Any)**

Add Novelty Rule

Novelty Rule	Action	Logging Level	Threat Severity
<a href="#">Alert on DDL</a>	Warn	Always	Moderate
<a href="#">Alert on Sensitive Data Update</a>	Warn	Always	Moderate

ORACLE®

1 - 2

180

# Firewall Policies Created

- You start with 1 and added 3

Firewall Policies				
Search		Go	Actions ▾	
Name ▾	Database Type	Description	Deployed	Created
My Policy 3	Oracle Database	Novelty Policies	No	12/3/2014 7:23:25 PM
My Policy 2	Oracle Database	This one is "trust but verify" example	No	12/3/2014 6:50:09 PM
My Policy 1	Oracle Database	This is to build a SQL based white list example	No	12/3/2014 6:57:08 PM
Blocking SQL Injections	Oracle Database	..	No	8/30/2014 1:24:42 AM

1 - 4

# Database Firewall Use Cases

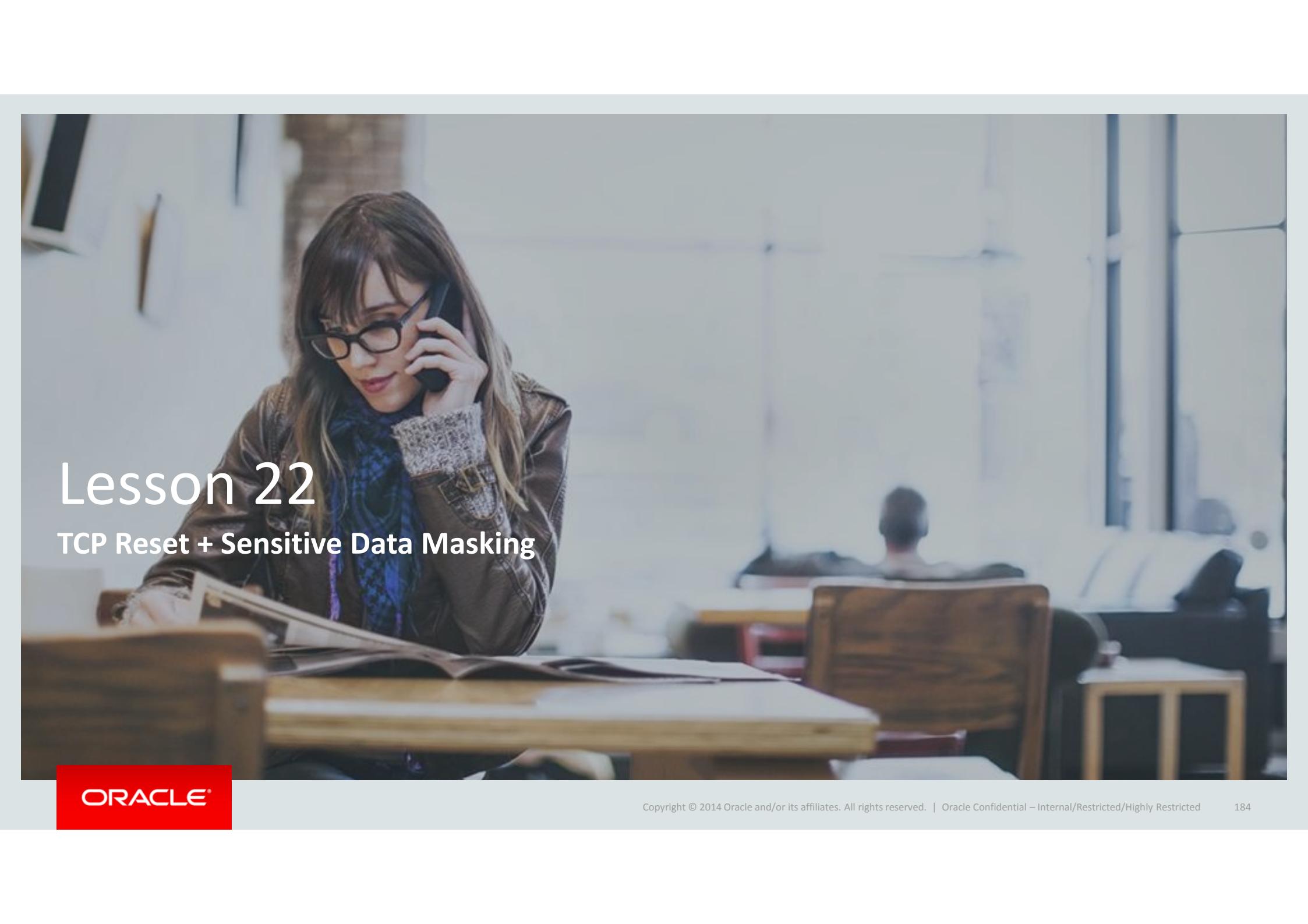
Use Case	Policy & Rule
Real time database activity monitoring	“My policy 1” – passive monitoring
Anomaly detection - Alert on unseen or suspicious events	All policy with alert control
Prevent unexpected SQL statements	“My policy 1” using whitelist
Blocking SQL Injection Threats	“Blocking SQL Injections” 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

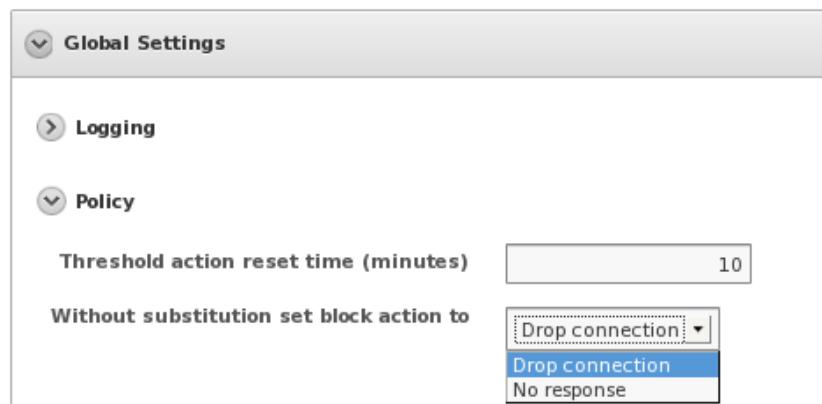
ORACLE®

Copyright © 2014 Oracle and/or its affiliates. All rights reserved. | Oracle Confidential – Internal/Restricted/Highly Restricted

184

# 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.JOB SET Max\_Salary=0000 WHERE JOB\_ID#####;

