ORACLE®

Privileged Database User Security Best Practices

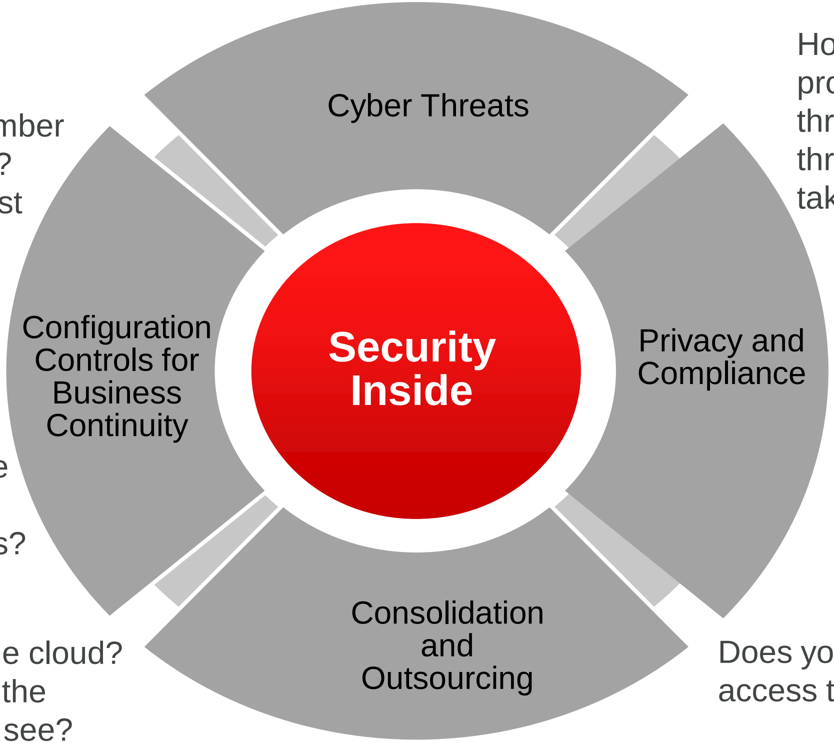
Morana Kobal Butković
Principal Sales Consultant
Oracle Hrvatska

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Cyber Threats and Risk Factors

Are you trying to minimize the number of privileges given to applications? How would you determine the least privilege model?

How is your application data protected against Cyber threats? If you detect a cyber threat, what steps would you take to protect your data?


Cyber Threats
Configuration Controls for Business Continuity
Security Inside
Privacy and Compliance
Consolidation and Outsourcing

Do you need to control ad-hoc access to the application and the database? How do you prevent intentional or accidental changes?

Do you have sensitive customer data access to which is regulated? Do you have valuable intellectual property that might be targeted?

Do you host information in the cloud? Do you know who maintains the database and what can they see?

Does your DBA have default access to sensitive data?

Control Strategies

- Minimize Attack surface
- Add environment-based access control
- Enforce separation of duty
- Restrict DBA unlimited powers
- Control configuration changes

Oracle Database 12*c*

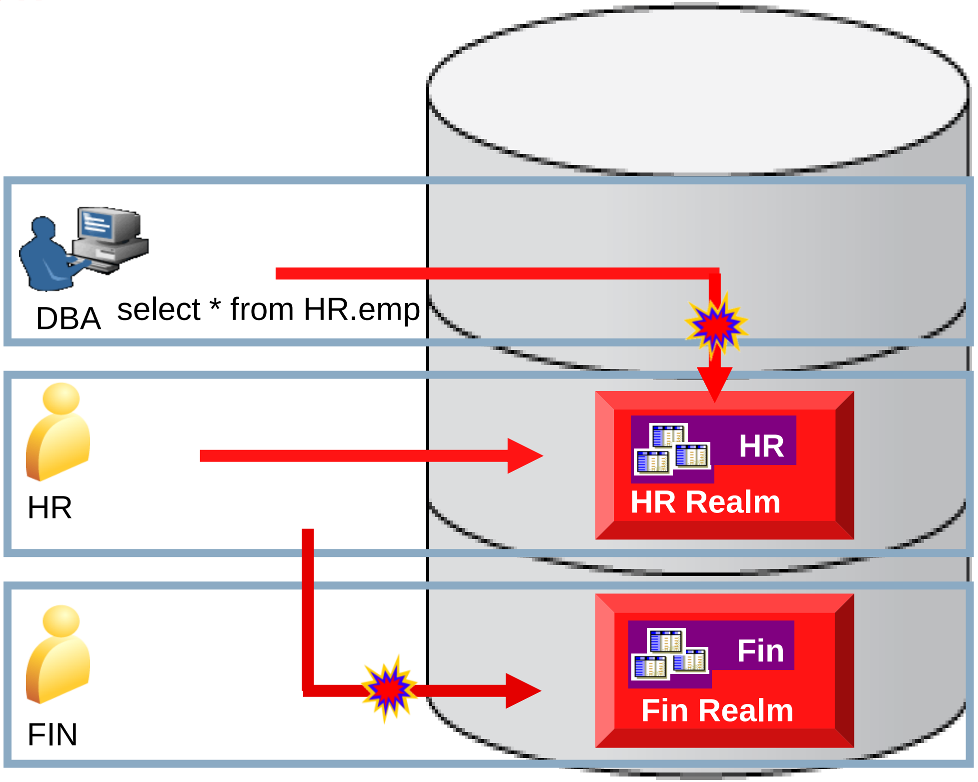
Control Solutions

- Privilege Analysis helps minimize attack surface *New*
- Multi-factor authorization for environment-based access control
- SYSKM, SYSDG and SYSBACKUP *(New)*, in addition to Security Admin and Accounts Admin to enforce separation of duty
- Realms restrict DBA unlimited powers
- Mandatory Realms restrict application DBA unlimited powers *New*
- Command Controls enforce configuration control standards

Realms Restrict DBA Unlimited Powers

Database Vault Controls Overview

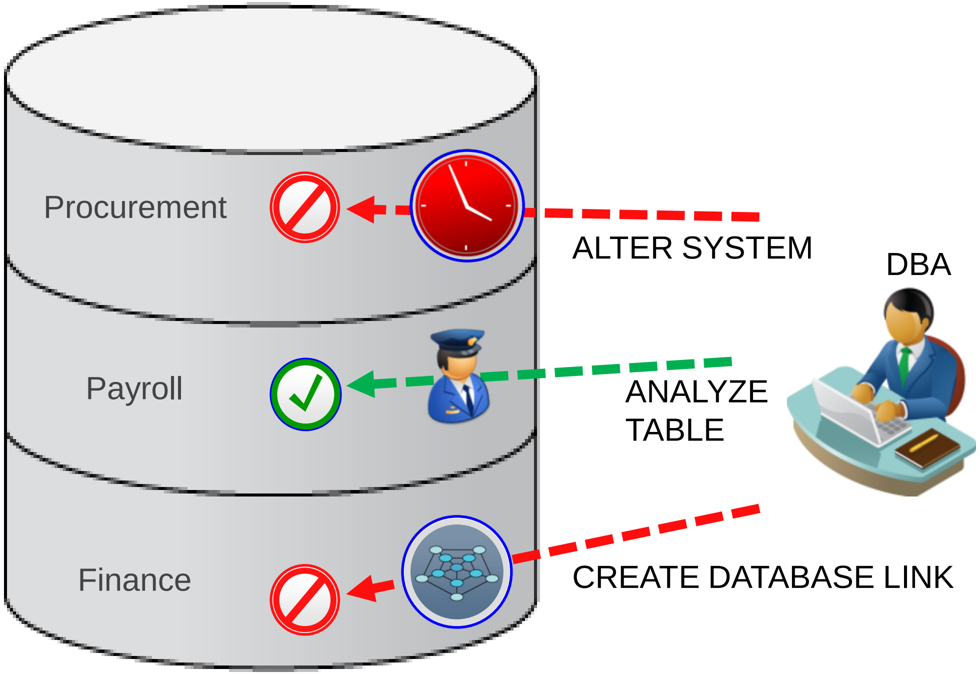
- Block threats from compromised privileged accounts
- Block privileged insiders from accessing application data
- Block privileged application from accessing other application data
- Securely consolidate and use private or public cloud computing



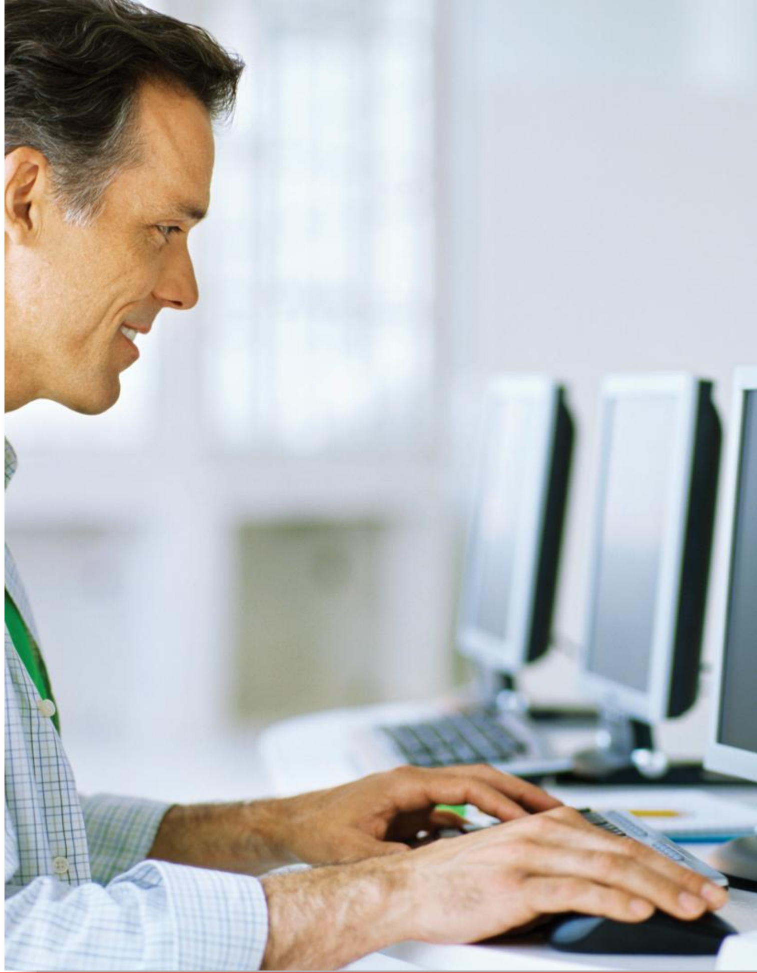
Multi-Factor Authorization & Command Controls

Database Vault Controls Overview

- Protect application data and prevent application by-pass
- Control database configuration changes for security, compliance, and business continuity
- Enforce who, where, when, and how data can be accessed using environment-based factors such as time, IP address, and program name

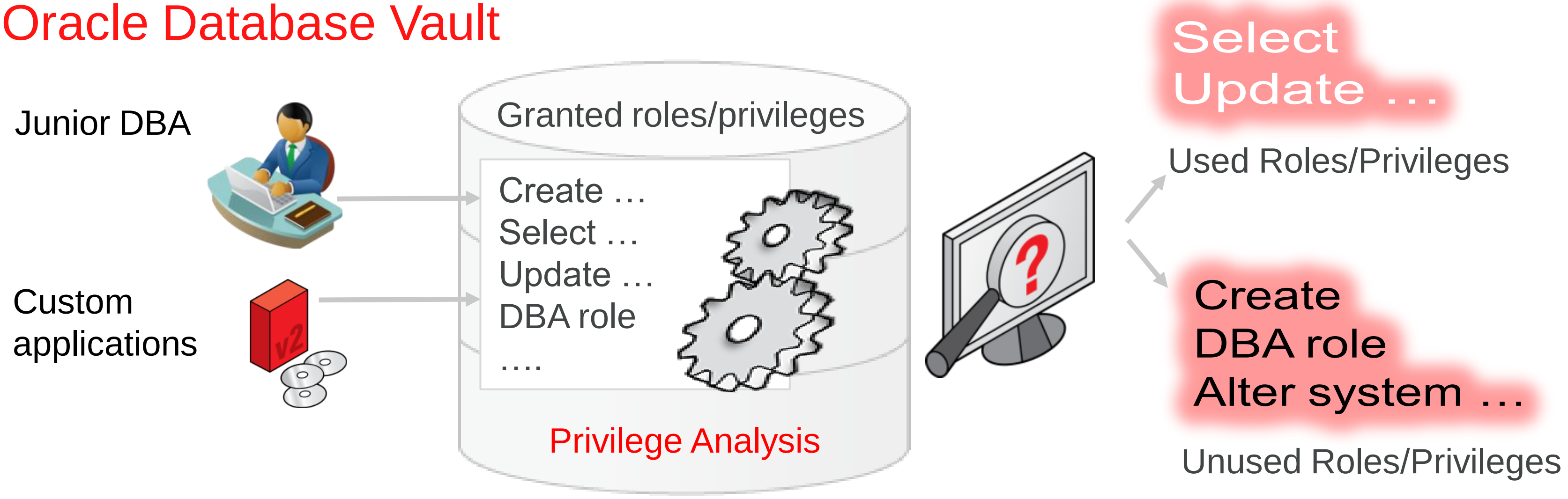


New Database Vault Privilege Analysis: Minimize Attack Surface



Privilege Analysis Overview

Oracle Database Vault



- Identify over-privileged users and applications
- Report on actual privileges / roles used in the database
- Reduce attack surface by reducing privileges and roles to what is needed

Privilege Analysis Features

Oracle Database Vault

- Scope: database, role, user, IP address, …
- Applies across all database sessions and remains active even after database restarts
- Minimal performance overhead - run on production systems < 5%
- Captures direct and indirect role grants
- Database Vault installed by default but not enabled
- Privilege Analysis can be used without enabling Database Vault controls (i.e. SoD, Realm controls, Command Controls …)

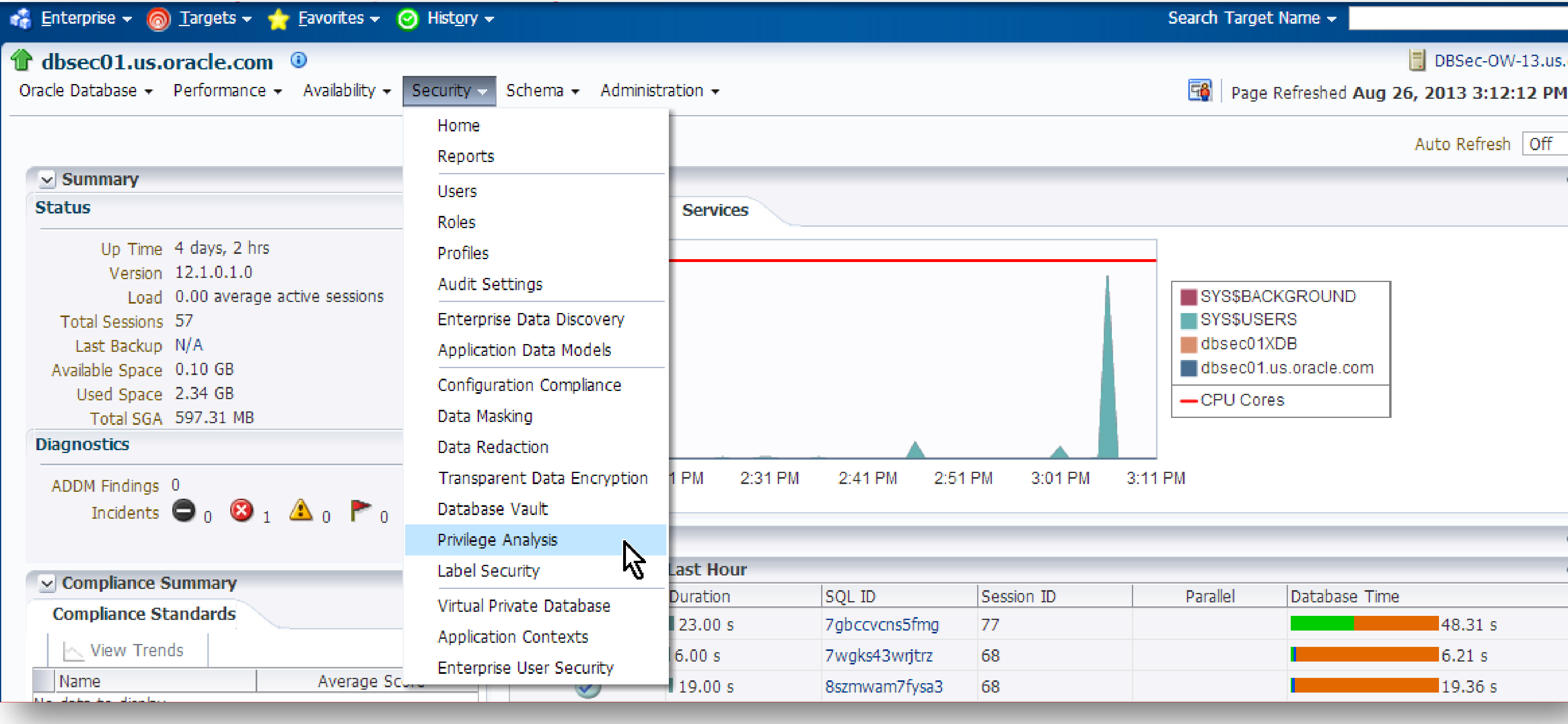
Oracle Database Vault

Privilege Analysis

```
DBMS_PRIVILEGE_CAPTURE.CREATE_CAPTURE (
  name              => ‘DBA Tuning Privilege Analysis',
  description       => ‘Analyze Privileges needed for a database tuning DBA',
  type              =>  DEFAULT DBMS_PRIVILEGE_CAPTURE. G_CONTEXT,
  condition         => 'SYS_CONTEXT(''USERENV'','‘USER'') ='‘DBA_USER_12''‘);

DBMS_PRIVILEGE_CAPTURE.ENABLE_CAPTURE (‘DBA Tuning Privilege Analysis‘);
```

Privilege Analysis For Applications



Page Refreshed **Aug 26, 2013 3:12:12 PM**

Auto Refresh Off

Up Time	4 days, 2 hrs
Version	12.1.0.1.0
Load	0.00 average active sessions
Total Sessions	57
Last Backup	N/A
Available Space	0.10 GB
Used Space	2.34 GB
Total SGA	597.31 MB

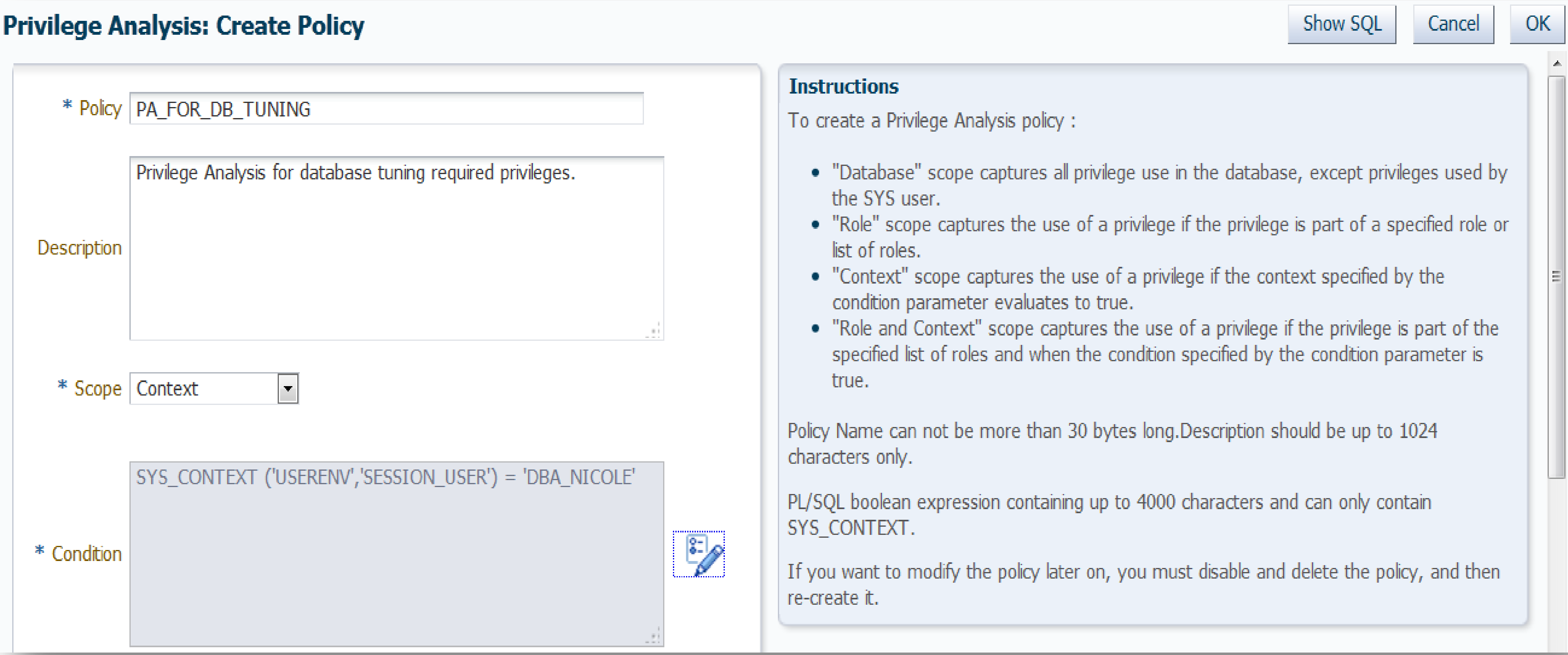
ADDM Findings 0

Incidents 0 1 0 0

Name	Average Sc

Duration	SQL ID	Session ID	Parallel	Database Time
23.00 s	7gbccvcns5fmg	77		48.31 s
6.00 s	7wgks43wrjtrz	68		6.21 s
19.00 s	8szmwam7fysa3	68		19.36 s

Privilege Analysis Create Policy



Privilege Analysis: Create Policy

* Policy	PA_FOR_DB_TUNING
Description	Privilege Analysis for database tuning required privileges.
* Scope	Context
* Condition	SYS_CONTEXT ('USERENV','SESSION_USER') = 'DBA_NICOLE'

Instructions

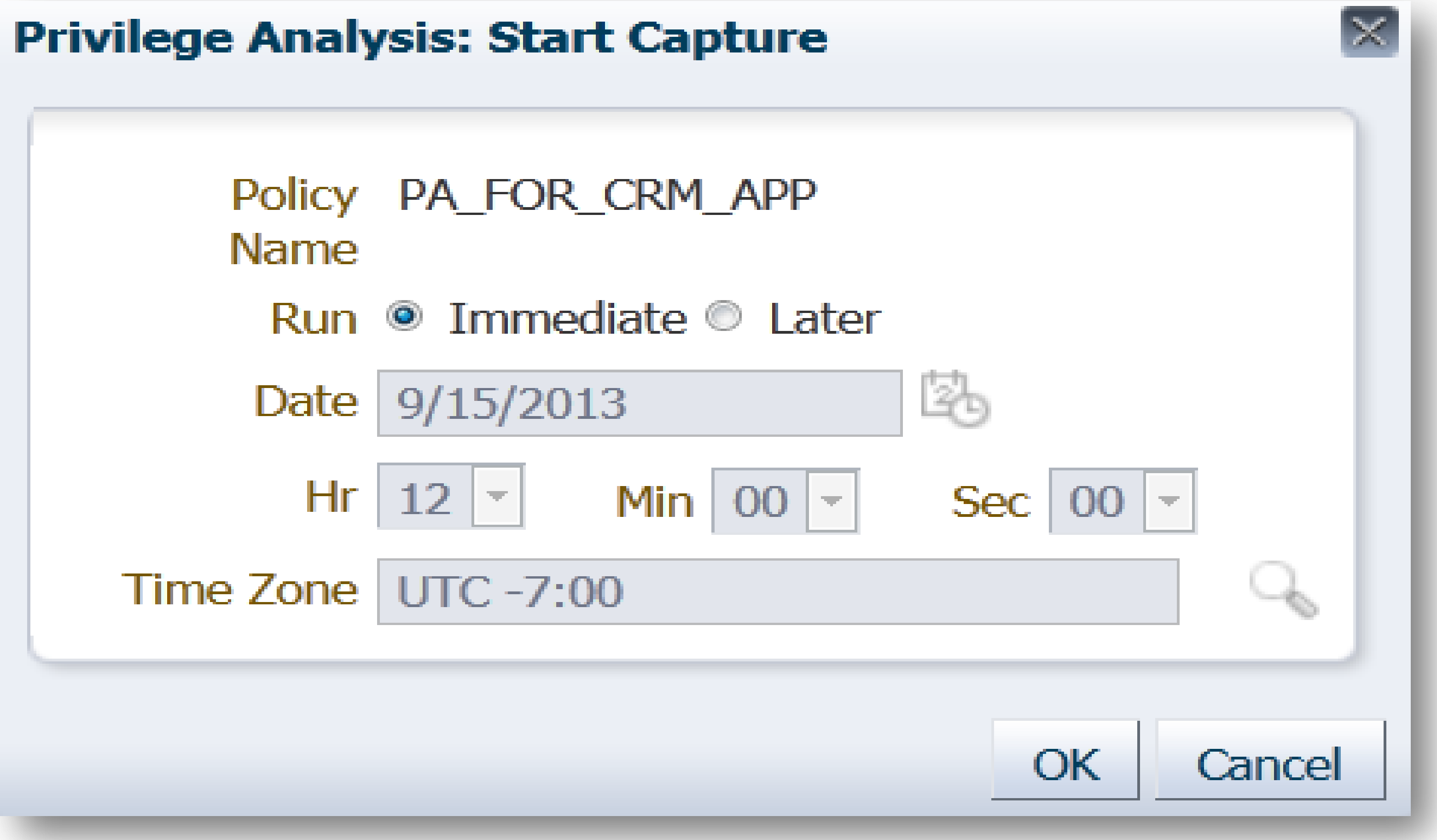
To create a Privilege Analysis policy :

- "Database" scope captures all privilege use in the database, except privileges used by the SYS user.
- "Role" scope captures the use of a privilege if the privilege is part of a specified role or list of roles.
- "Context" scope captures the use of a privilege if the context specified by the condition parameter evaluates to true.
- "Role and Context" scope captures the use of a privilege if the privilege is part of the specified list of roles and when the condition specified by the condition parameter is true.

Policy Name can not be more than 30 bytes long.Description should be up to 1024 characters only.

PL/SQL boolean expression containing up to 4000 characters and can only contain SYS_CONTEXT.

If you want to modify the policy later on, you must disable and delete the policy, and then re-create it.



Privilege Analysis: Start Capture

Policy Name PA_FOR_CRM_APP

Run ● Immediate ○ Later

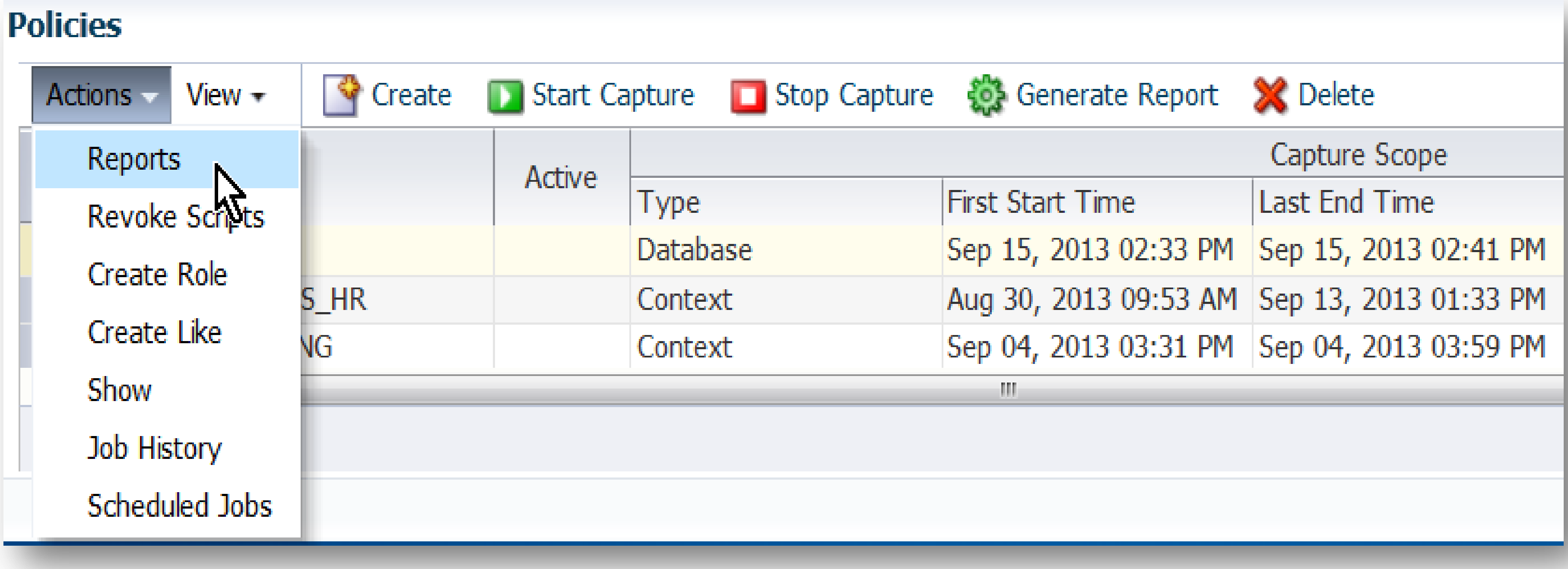
Date 9/15/2013

Hr 12 Min 00 Sec 00

Time Zone UTC -7:00

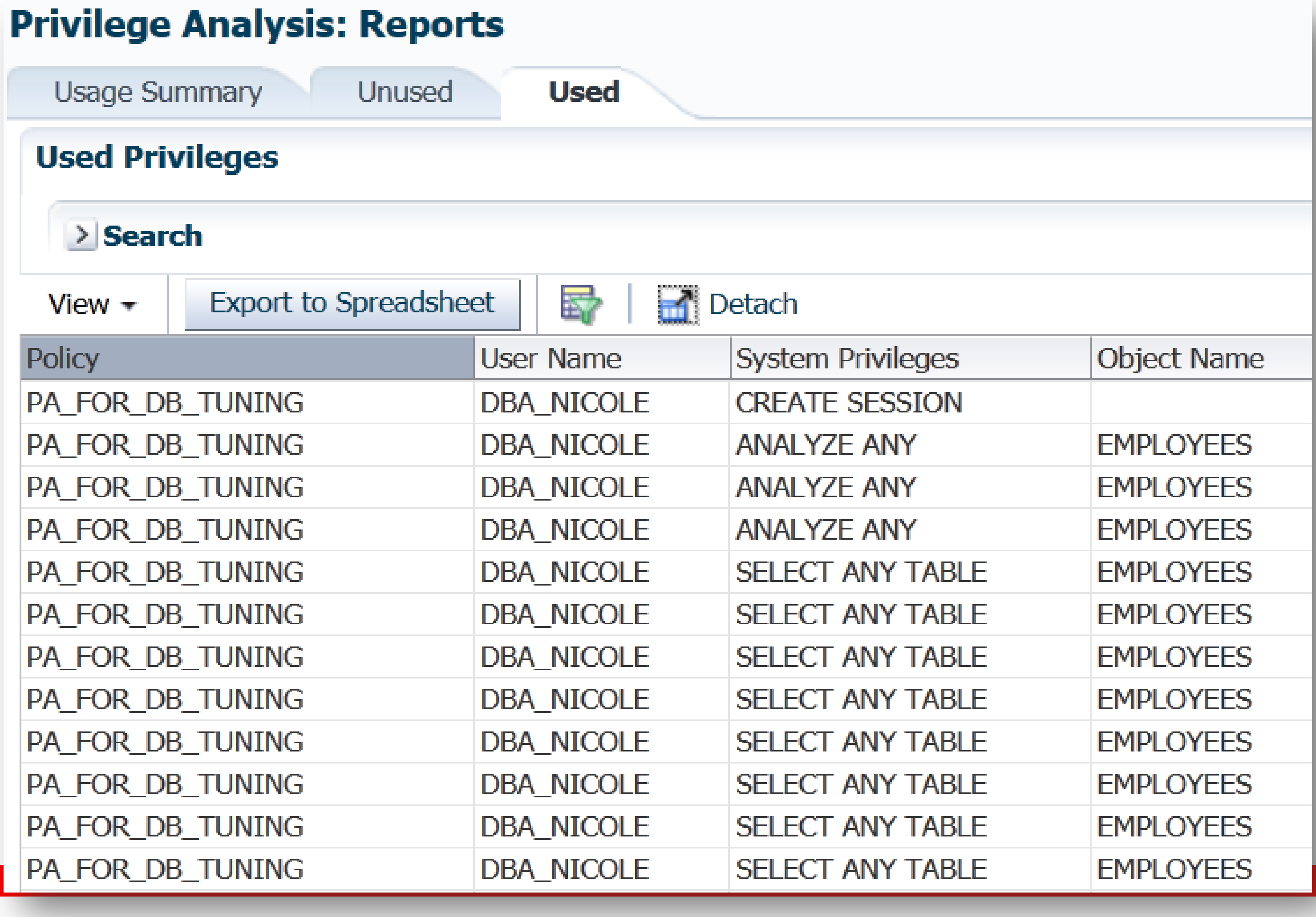
Privilege Analysis

Oracle Database Vault



Policies

	Active	Capture Scope		
		Type	First Start Time	Last End Time
		Database	Sep 15, 2013 02:33 PM	Sep 15, 2013 02:41 PM
S_HR		Context	Aug 30, 2013 09:53 AM	Sep 13, 2013 01:33 PM
NG		Context	Sep 04, 2013 03:31 PM	Sep 04, 2013 03:59 PM

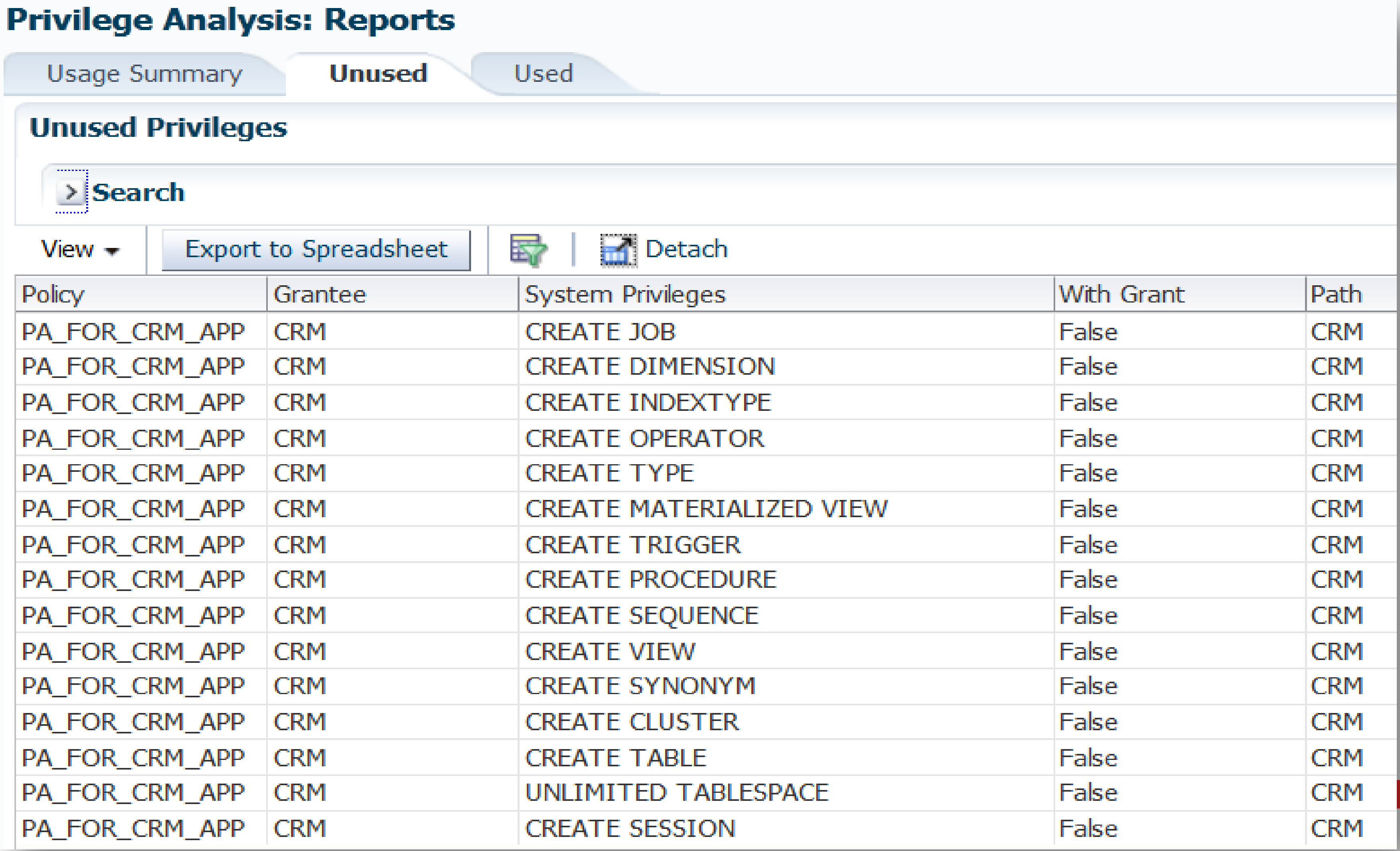


Privilege Analysis: Reports

Used Privileges

Policy	User Name	System Privileges	Object Name
PA_FOR_DB_TUNING	DBA_NICOLE	CREATE SESSION	
PA_FOR_DB_TUNING	DBA_NICOLE	ANALYZE ANY	EMPLOYEES
PA_FOR_DB_TUNING	DBA_NICOLE	ANALYZE ANY	EMPLOYEES
PA_FOR_DB_TUNING	DBA_NICOLE	ANALYZE ANY	EMPLOYEES
PA_FOR_DB_TUNING	DBA_NICOLE	SELECT ANY TABLE	EMPLOYEES
PA_FOR_DB_TUNING	DBA_NICOLE	SELECT ANY TABLE	EMPLOYEES
PA_FOR_DB_TUNING	DBA_NICOLE	SELECT ANY TABLE	EMPLOYEES
PA_FOR_DB_TUNING	DBA_NICOLE	SELECT ANY TABLE	EMPLOYEES
PA_FOR_DB_TUNING	DBA_NICOLE	SELECT ANY TABLE	EMPLOYEES
PA_FOR_DB_TUNING	DBA_NICOLE	SELECT ANY TABLE	EMPLOYEES
PA_FOR_DB_TUNING	DBA_NICOLE	SELECT ANY TABLE	EMPLOYEES
PA_FOR_DB_TUNING	DBA_NICOLE	SELECT ANY TABLE	EMPLOYEES

ORACLE



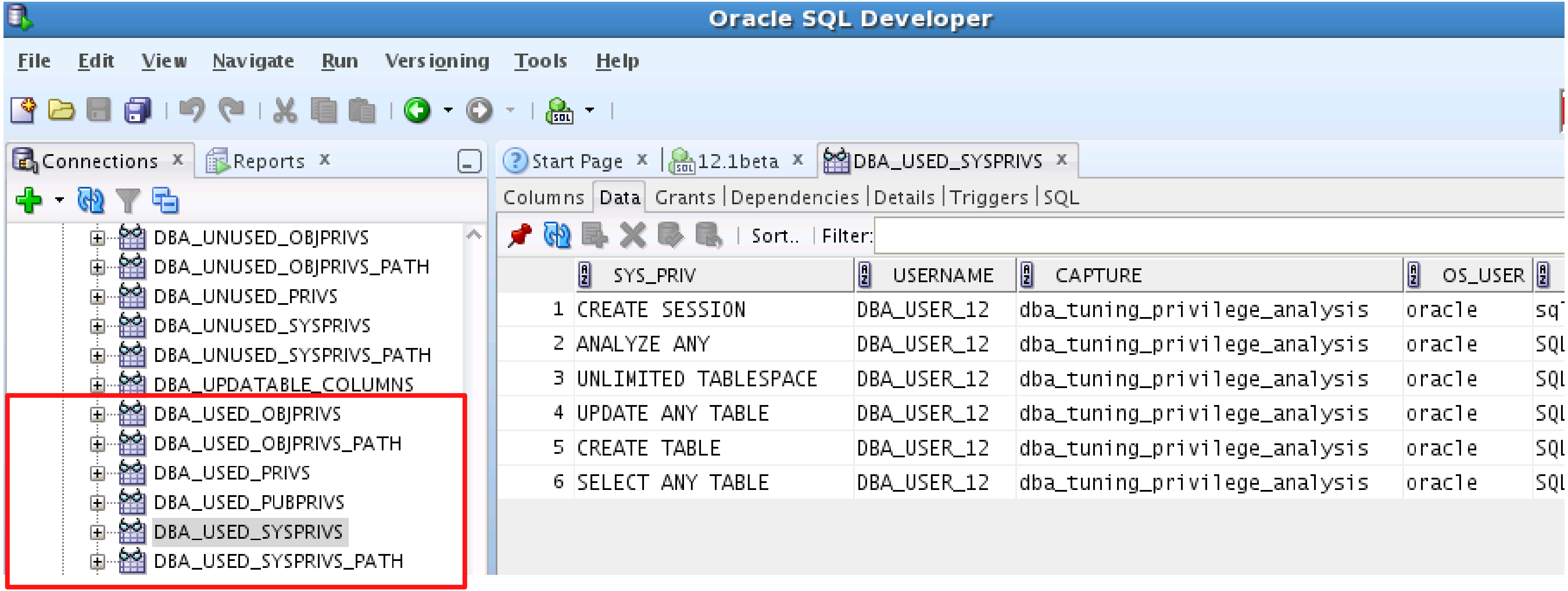
Privilege Analysis: Reports

Unused Privileges

Policy	Grantee	System Privileges	With Grant	Path
PA_FOR_CRM_APP	CRM	CREATE JOB	False	CRM
PA_FOR_CRM_APP	CRM	CREATE DIMENSION	False	CRM
PA_FOR_CRM_APP	CRM	CREATE INDEXTYPE	False	CRM
PA_FOR_CRM_APP	CRM	CREATE OPERATOR	False	CRM
PA_FOR_CRM_APP	CRM	CREATE TYPE	False	CRM
PA_FOR_CRM_APP	CRM	CREATE MATERIALIZED VIEW	False	CRM
PA_FOR_CRM_APP	CRM	CREATE TRIGGER	False	CRM
PA_FOR_CRM_APP	CRM	CREATE PROCEDURE	False	CRM
PA_FOR_CRM_APP	CRM	CREATE SEQUENCE	False	CRM
PA_FOR_CRM_APP	CRM	CREATE VIEW	False	CRM
PA_FOR_CRM_APP	CRM	CREATE SYNONYM	False	CRM
PA_FOR_CRM_APP	CRM	CREATE CLUSTER	False	CRM
PA_FOR_CRM_APP	CRM	CREATE TABLE	False	CRM
PA_FOR_CRM_APP	CRM	UNLIMITED TABLESPACE	False	CRM
PA_FOR_CRM_APP	CRM	CREATE SESSION	False	CRM

Oracle Database Vault

Privilege Analysis Demo



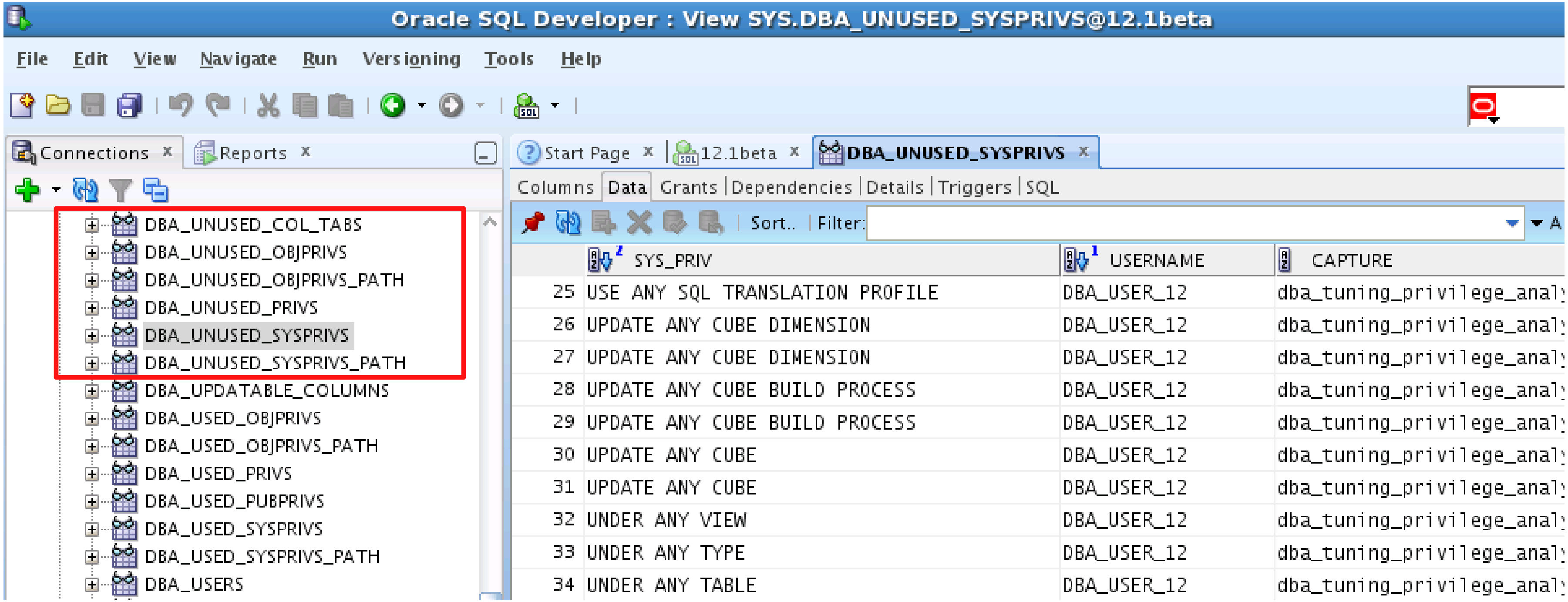
Oracle SQL Developer
File Edit View Navigate Run Versioning Tools Help
Connections
Reports
Start Page
12.1beta
DBA_USED_SYSPRIVS
Columns Data Grants Dependencies Details Triggers SQL
Sort..
Filter:

- DBA_UNUSED_OBJPRIVS
- DBA_UNUSED_OBJPRIVS_PATH
- DBA_UNUSED_PRIVS
- DBA_UNUSED_SYSPRIVS
- DBA_UNUSED_SYSPRIVS_PATH
- DBA_UPDATABLE_COLUMNS
- DBA_USED_OBJPRIVS
- DBA_USED_OBJPRIVS_PATH
- DBA_USED_PRIVS
- DBA_USED_PUBPRIVS
- DBA_USED_SYSPRIVS
- DBA_USED_SYSPRIVS_PATH

	SYS_PRIV	USERNAME	CAPTURE	OS_USER	
1	CREATE SESSION	DBA_USER_12	dba_tuning_privilege_analysis	oracle	sq
2	ANALYZE ANY	DBA_USER_12	dba_tuning_privilege_analysis	oracle	SQl
3	UNLIMITED TABLESPACE	DBA_USER_12	dba_tuning_privilege_analysis	oracle	SQl
4	UPDATE ANY TABLE	DBA_USER_12	dba_tuning_privilege_analysis	oracle	SQl
5	CREATE TABLE	DBA_USER_12	dba_tuning_privilege_analysis	oracle	SQl
6	SELECT ANY TABLE	DBA_USER_12	dba_tuning_privilege_analysis	oracle	SQl

Oracle Database Vault

Privilege Analysis Demo



Oracle SQL Developer : View SYS.DBA_UNUSED_SYSPRIVS@12.1beta
File Edit View Navigate Run Versioning Tools Help
Connections
Reports
Start Page
12.1beta
DBA_UNUSED_SYSPRIVS
Columns Data Grants Dependencies Details Triggers SQL
Sort..
Filter:

- DBA_UNUSED_COL_TABS
- DBA_UNUSED_OBJPRIVS
- DBA_UNUSED_OBJPRIVS_PATH
- DBA_UNUSED_PRIVS
- DBA_UNUSED_SYSPRIVS
- DBA_UNUSED_SYSPRIVS_PATH
- DBA_UPDATABLE_COLUMNS
- DBA_USED_OBJPRIVS
- DBA_USED_OBJPRIVS_PATH
- DBA_USED_PRIVS
- DBA_USED_PUBPRIVS
- DBA_USED_SYSPRIVS
- DBA_USED_SYSPRIVS_PATH
- DBA_USERS

	SYS_PRIV	USERNAME	CAPTURE
25	USE ANY SQL TRANSLATION PROFILE	DBA_USER_12	dba_tuning_privilege_anal
26	UPDATE ANY CUBE DIMENSION	DBA_USER_12	dba_tuning_privilege_anal
27	UPDATE ANY CUBE DIMENSION	DBA_USER_12	dba_tuning_privilege_anal
28	UPDATE ANY CUBE BUILD PROCESS	DBA_USER_12	dba_tuning_privilege_anal
29	UPDATE ANY CUBE BUILD PROCESS	DBA_USER_12	dba_tuning_privilege_anal
30	UPDATE ANY CUBE	DBA_USER_12	dba_tuning_privilege_anal
31	UPDATE ANY CUBE	DBA_USER_12	dba_tuning_privilege_anal
32	UNDER ANY VIEW	DBA_USER_12	dba_tuning_privilege_anal
33	UNDER ANY TYPE	DBA_USER_12	dba_tuning_privilege_anal
34	UNDER ANY TABLE	DBA_USER_12	dba_tuning_privilege_anal

Privilege Analysis Best Practices

Oracle Database Vault

- Run full applications tests to capture all used privileges and roles
- Applications may use certain privileges only monthly or quarterly
  - Capture privileges long enough to allow all operations to happen
  - Or capture multiple times over different periods
- For unused privileges, consider auditing their use before revoking
- Look for the ADMIN OPTION when analyzing used or unused privileges
  - Keep these privileges if the user is responsible for granting them to others

Privilege Analysis Best Practices

Oracle Database Vault

- For used privileges, consider replacing powerful system privileges with direct object privileges
  - For example, replace SELECT ANY with direct object SELECT privilege
- If you feel there is a privilege or role that is shown as being used but should not be, then turn on auditing to monitor that privilege or role
- Consider creating a new custom role for the used privileges to make it easier to grant to others
- Information gathered can be applied to 11.2 databases

Privilege Analysis Benefits

Oracle Database Vault

- Helps achieve least privilege which makes applications more secure by reducing attack surface
- Shows a definite list of used / unused Roles and System and Object privileges and how they were obtained
- For unused privileges: keep, create a custom role, audit, or revoke

Demonstration:

Oracle Database Vault Privilege Analysis