Security Benchmarks™
A DIVISION OF CENTER FOR INTERNET SECURITY

# CIS Oracle Database Server 11g R2 on

v1.0.0

Export Date 11-20-2012

The CIS Security Benchmarks division provides consensus-oriented information security products, services, tools, metrics, suggestions, and recommendations (the "SB Products") as a public service to Internet users worldwide. Downloading or using SB Products in any way signifies and confirms your acceptance of and your binding agreement to these CIS Security Benchmarks Terms of Use.

## *CIS SECURITY BENCHMARKS TERMS OF USE*

### *BOTH CIS SECURITY BENCHMARKS DIVISION MEMBERS AND NON-MEMBERS MAY:*

- Download, install, and use each of the SB Products on a single computer, and/or
- Print one or more copies of any SB Product that is in a .txt, .pdf, .doc, .mcw, or .rtf format, but only if each such copy is printed in its entirety and is kept intact, including without limitation the text of these CIS Security Benchmarks Terms of Use.

### *UNDER THE FOLLOWING TERMS AND CONDITIONS:*

- **SB Products Provided As Is**. CIS is providing the SB Products "as is" and "as available" without: (1) any representations, warranties, or covenants of any kind whatsoever (including the absence of any warranty regarding: (a) the effect or lack of effect of any SB Product on the operation or the security of any network, system, software, hardware, or any component of any of them, and (b) the accuracy, utility, reliability, timeliness, or completeness of any SB Product); or (2) the responsibility to make or notify you of any corrections, updates, upgrades, or fixes.
- **Intellectual Property and Rights Reserved**. You are not acquiring any title or ownership rights in or to any SB Product, and full title and all ownership rights to the SB Products remain the exclusive property of CIS. All rights to the SB Products not expressly granted in these Terms of Use are hereby reserved.
- **Restrictions**. You acknowledge and agree that you may not: (1) decompile, dis-assemble, alter, reverse engineer, or otherwise attempt to derive the source code for any software SB Product that is not already in the form of source code; (2) distribute, redistribute, sell, rent, lease, sublicense or otherwise transfer or exploit any rights to any SB Product in any way or for any purpose; (3) post any SB Product on any website, bulletin board, ftp server, newsgroup, or other similar mechanism or device; (4) remove from or alter these CIS Security Benchmarks Terms of Use on any SB Product; (5) remove or alter any proprietary notices on any SB Product; (6) use any SB Product or any component of an SB Product with any derivative works based directly on an SB Product or any component of an SB Product; (7) use any SB Product or any component of an SB Product with other products or applications that are directly and specifically dependent on such SB Product or any component for any part of their functionality; (8) represent or claim a particular level of compliance or consistency with any SB Product; or (9) facilitate or otherwise aid other individuals or entities in violating these CIS Security Benchmarks Terms of Use.
- **Your Responsibility to Evaluate Risks**. You acknowledge and agree that: (1) no network, system, device, hardware, software, or component can be made fully secure; (2) you have the sole responsibility to evaluate the risks and benefits of the SB Products to your particular circumstances and requirements; and (3) CIS is not assuming any of the liabilities associated with your use of any or all of the SB Products.
- **CIS Liability**. You acknowledge and agree that neither CIS nor any of its employees, officers, directors, agents or other service providers has or will have any liability to you whatsoever (whether based in contract, tort, strict liability or otherwise) for any direct, indirect, incidental, consequential, or special damages that arise out of or are connected in any way with your use of any SB Product.
- **Indemnification**. You agree to indemnify, defend, and hold CIS and all of CIS's employees, officers, directors, agents and other service providers harmless from and against any liabilities, costs and expenses incurred by any of them in connection with your violation of these CIS Security Benchmarks Terms of Use.
- **Jurisdiction**. You acknowledge and agree that: (1) these CIS Security Benchmarks Terms of Use will be governed by and construed in accordance with the laws of the State of Maryland; (2) any action at law or in equity arising out of or relating to these CIS Security Benchmarks Terms of Use shall be filed only in the courts located in the State of Maryland; and (3) you hereby consent and submit to the personal jurisdiction of such courts for the purposes of litigating any such action.
- **U.S. Export Control and Sanctions laws**. Regarding your use of the SB Products with any non-U.S. entity or country, you acknowledge that it is your responsibility to understand and abide by all U.S. sanctions and export control laws as set from time to time by the U.S. Bureau of Industry and Security (BIS) and the U.S. Office of Foreign Assets Control (OFAC).

***SPECIAL RULES FOR CIS MEMBER ORGANIZATIONS:*** CIS reserves the right to create special rules for: (1) CIS Members; and (2) Non-Member organizations and individuals with which CIS has a written contractual relationship. CIS hereby grants to each CIS Member Organization in good standing the right to distribute the SB Products within such Member's own organization, whether by manual or electronic means. Each such Member Organization acknowledges and agrees that the foregoing grants in this paragraph are subject to the terms of such Member's membership arrangement with CIS and may, therefore, be modified or terminated by CIS at any time.

# Table of Contents

# Overview

This document is intended to address the recommended security settings for the Oracle 11g, r2 Database ©, running on either an x86 (32-bit) or x64 (64-bit) AMD/Intel chip platform. Specifically, the requirements included in this document have been designed for and tested against the Intel x64 chip running a 64-bit version of Oracle Linux © 2.6.18-194 configured as a stand-alone system, running as a "Database server," including all Oracle CPUs up through April 15, 2012. Future Oracle 11g r2 critical patch updates (CPUs) may impact the recommendations included in this document.

To obtain the latest version of this guide, please visit http://benchmarks.cisecurity.org. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

## *Intended Audience*

This benchmark is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate Oracle Database Server 11g R2 on Oracle Linux 5.

## *Consensus Guidance*

This benchmark was created using a consensus review process comprised of volunteer and contract subject matter experts. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS benchmark undergoes two phases of consensus review. The first phase occurs during initial benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the benchmark. This discussion occurs until consensus has been reached on benchmark recommendations. The second phase begins after the benchmark has been released to the public Internet. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the benchmark. If you are interested in participating in the consensus review process, please send us a note to feedback@cisecurity.org.

## *Typographical Conventions*

The following typographical conventions are used throughout this guide:

| Convention | Meaning |
|---|---|
| `Stylized Monospace font` | Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented. |
| `Monospace font` | Used for inline code, commands, or examples. Text should be interpreted exactly as presented. |
| *<italic font in brackets>* | Italic texts set in angle brackets denote a variable requiring substitution for a real value. |
| *Italic font* | Used to denote the title of a book, article, or other publication. |
| **Note** | Additional information or caveats |

## *Scoring Information*

A scoring status indicates whether compliance with the given recommendation impacts the assessed target's benchmark score. The following scoring statuses are used in this benchmark:

**Scored**
Failure to comply with "Scored" recommendations will decrease the final benchmark score. Compliance with "Scored" recommendations will increase the final benchmark score.

**Not Scored**
Failure to comply with "Not Scored" recommendations will not decrease the final benchmark score. Compliance with "Not Scored" recommendations will not increase the final benchmark score.

## *Profile Definitions*

The following configuration profiles are defined by this Benchmark:

- **Level 1 - 11.2 on Oracle Linux 5**

  Items in this profile intend to:

  - be practical and prudent;
  - provide a clear security benefit; and
  - not negatively inhibit the utility of the technology beyond acceptable means.
- **Level 2 - 11.2 on Oracle Linux 5**

  This profile extends the "Level 1" profile. Items in this profile exhibit one or more of the following characteristics:

  - are intended for environments or use cases where security is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.
- **Level 1 - 11.x on any platform**

  Items in this profile intend to:

  - be practical and prudent;
  - provide a clear security benefit; and
  - not negatively inhibit the utility of the technology beyond acceptable means.
- **Level 1 - 11.2 on any platform**

  Items in this profile intend to:

  - be practical and prudent;
  - provide a clear security benefit; and
  - not negatively inhibit the utility of the technology beyond acceptable means.
- **Level 1 - 11.2 on Windows**

  Items in this profile intend to:

  - be practical and prudent;
  - provide a clear security benefit; and
  - not negatively inhibit the utility of the technology beyond acceptable means.

# *Acknowledgements*

This benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

**Author**
Alexander Kornbrust
Alan Covell

**Contributor**
Andy McConnell
Johan Verbrugghen
Don Granaman , *Solutionary*
Andre van Winssen CISSP, CISA, CEH, Oracle Certified Master 10g/11g
Stephen Suddeth
Andy Peters
Alf-Ivar Holm
Surachart Opun
Don Granaman , *Solutionary*
Ron Reidy
Louis Lam

**Editor**
Paul Wright OCP and GSOC
Stephen Willis

# Recommendations

## 1 Oracle Database Installation and Patching Requirements

One of the best ways to ensure secure Oracle security is to implement Critical Patch Updates (CPUs) as they come out, along with any applicable OS patches that will not interfere with system operations.

## 1.1 Change the Oracle default account passwords

Depending from the chosen installation method, Oracle 11gR2 creates a number of well-known, default accounts with default passwords, which are normally locked and expired. The majority of these default accounts are powerful and allow to overtake the database if the account is open. That's why the passwords of these accounts should be changed immediately to avoid that unlocking and unexpiring the account opens a security hole in the database.

Any of these accounts that are not required can potentially be deleted, but extensive testing should be should be done in a non-Production environment prior to removing a default account, to avoid breaking critical processes associated with legacy applications.

A password change in Oracle 11 could be done using 4 different ways (alter user, grant, OCI password call and direct update on SYS.USER$ (unsupported)). The disadvantage of the alter user and grant syntax is that the password is transferred in cleartext over the network.

The SQL*Plus password command is transferring the encrypted password over the network but the Oracle client has to be compatible to the database (e.g. 11.2.0.2 client can't use the password against 11.2.0.3 due to API changes in the appropriate OCI call).

If the alter user syntax is used, the command should be executed on the database server itself.

### 1.1.1 Change the default password for 'APEX_040000' (Scored)

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The APEX_040000 account owns the greatest part of the objects created by the database during the installation of Oracle Database Application Express (ODAE).

**Rationale:**

Some pre-installed versions of APEX 4.0 come with a default password and can provide a point for database access/control by unauthorized users, opening up the tables, views, etc..

**Audit:**

```
select 'defaultpwd' as defaultpassword
from sys.user$
where name='APEX_040000'
      and
substr(spare4,3,40)=rawtohex(utl_raw.cast_to_varchar2(sys.dbms_crypto.hash(utl_raw.cas
t_to_raw('oracle')||hextoraw(substr(spare4,43,20)), 3)))
union
select 'defaultpwd' from sys.user$ where name='APEX_040000' and
password='EE7785338B8FFE3D';
```

**Remediation:**

```
Execute the following command to change the password
SQL> password apex_040000

Enter the new password twice:
Changing password for apex_040000
New password:
Retype new password:
Password changed
```

## *1.1.2 Change the default password for 'APPQOSSYS' (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The `APPQOSSYS` account manages/owns all Quality of Service objects and provides an intuitive, policy-driven system to manage service level requirements.

**Rationale:**

As the default `APPQOSSYS` account created by Oracle has a well-known password and can provide a point for database access by unauthorized users if left at the default setting, this value should be changed according to the needs of the organization.

**Audit:**

```
select 'defaultpwd' as defaultpassword
from sys.user$
where name='APPQOSSYS'
      and
substr(spare4,3,40)=rawtohex(utl_raw.cast_to_varchar2(sys.dbms_crypto.hash(utl_raw.cas
t_to_raw('appqossys')||hextoraw(substr(spare4,43,20)), 3)))
union
select 'defaultpwd' from dba_users_with_defpwd where username='APPQOSSYS';
```

**Remediation:**

```
Execute the following command to change the password
SQL> password appoqssys

Enter the new password twice:
Changing password for appqossys
New password:
Retype new password:
Password changed
```

## *1.1.3 Change the default password for 'CTXSYS' (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The `CTXSYS` is used to administer Oracle Text.

**Rationale:**

As the default `CTXSYS` account created by Oracle has a well-known password and can provide a point for database access by unauthorized users if left at the default setting, this value should be changed according to the needs of the organization.

**Audit:**

```
select 'defaultpwd' as defaultpassword
from sys.user$
where name='CTXSYS'
      and
substr(spare4,3,40)=rawtohex(utl_raw.cast_to_varchar2(sys.dbms_crypto.hash(utl_raw.cas
t_to_raw('ctxsys')||hextoraw(substr(spare4,43,20)), 3)))
union
select 'defaultpwd' as defaultpassword
from sys.user$
where name='CTXSYS'
      and
substr(spare4,3,40)=rawtohex(utl_raw.cast_to_varchar2(sys.dbms_crypto.hash(utl_raw.cas
t_to_raw('change_on_install')||hextoraw(substr(spare4,43,20)), 3)))
```

```
union
select 'defaultpwd' from dba_users_with_defpwd where username='CTXSYS';
```

**Remediation:**

```
Execute the following command to change the password
SQL> password ctxsys

Enter the new password twice:
Changing password for ctxsys
New password:
Retype new password:
Password changed
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/server.112/e10575/tdpsg_user_accounts.htm#TDPSG20030

## *1.1.4 Change the default password for 'DBSNMP' (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The `DBSNMP` account is used by the Oracle Enterprise Manager to monitor and manage the database.

**Rationale:**

Depending from the installation, the default `DBSNMP` account created by Oracle could have a well-known password and can be potentially used to retrieve the Oracle password hashes.

**Audit:**

```
select 'defaultpwd' as defaultpassword
from sys.user$
where name='DBSNMP'
      and
substr(spare4,3,40)=rawtohex(utl_raw.cast_to_varchar2(sys.dbms_crypto.hash(utl_raw.cas
t_to_raw('dbsnmp')||hextoraw(substr(spare4,43,20)), 3)))
union
select 'defaultpwd' from dba_users_with_defpwd where username='DBSNMP';
```

**Remediation:**

```
Execute the following command to change the password
SQL> password dbsnmp
```

```
Enter the new password twice:
Changing password for dbsnmp
New password:
Retype new password:
Password changed
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/server.112/e10575/tdpsg_user_accounts.htm#TDPSG20030

## *1.1.5 Change the default password for 'DIP' (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The `DIP` account supports the operation of the Oracle Internet Directory and Oracle Label Security.

**Rationale:**

As the default `DIP` account created by Oracle has a well-known password and can provide a point for database access by unauthorized users if left at the default setting, this value should be changed according to the needs of the organization.

**Audit:**

```
select 'defaultpwd' as defaultpassword
from sys.user$
where name='DIP'
      and
substr(spare4,3,40)=rawtohex(utl_raw.cast_to_varchar2(sys.dbms_crypto.hash(utl_raw.cas
t_to_raw('dip')||hextoraw(substr(spare4,43,20)), 3)))
union
select 'defaultpwd' from dba_users_with_defpwd where username='DIP';
```

**Remediation:**

```
Execute the following command to change the password
SQL> password dip

Enter the new password twice:
Changing password for dip
New password:
Retype new password:
Password changed
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/server.112/e25513/statviews_5082.htm#REFRN23725

## *1.1.6 Change the default password for 'EXFSYS' (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The `EXFSYS` account accesses the `EXFSYS` schema, which facilitates use of the Rules Manager and Expression Filter feature and allows the user to build complex PL/SQL rules and expressions.

**Rationale:**

As the default `EXFSYS` account created by Oracle has a well-known password and can provide a point for database access by unauthorized users if left at the default setting, this value should be changed according to the needs of the organization.

**Audit:**

```
select 'defaultpwd' as defaultpassword
from sys.user$
where name='EXFSYS'
      and
substr(spare4,3,40)=rawtohex(utl_raw.cast_to_varchar2(sys.dbms_crypto.hash(utl_raw.cas
t_to_raw('exfsys')||hextoraw(substr(spare4,43,20)), 3)))
union
select 'defaultpwd' from dba_users_with_defpwd where username='EXFSYS';
```

**Remediation:**

```
Execute the following command to change the password
SQL> password exfsys

Enter the new password twice:
Changing password for exfsys
New password:
Retype new password:
Password changed
```

## *1.1.7 Change the default password for 'MDDATA' (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The MDDATA account owns the schema used by Oracle Spatial for storing Geocoder and router data, which allows the plotting of datapoints, such as market locations/types, against latitude and longitude on a map, in a way similar to a GPS presentation.

**Rationale:**

As the default MDDATA account created by Oracle has a well-known password and can be potentially corrupted to allow the installation of malware disguised as a business process, this value should be reset according to the needs of the organization.

**Audit:**

```
select 'defaultpwd' as defaultpassword
from sys.user$
where name='MDDATA'
      and
substr(spare4,3,40)=rawtohex(utl_raw.cast_to_varchar2(sys.dbms_crypto.hash(utl_raw.cas
t_to_raw('mddata')||hextoraw(substr(spare4,43,20)), 3)))
union
select 'defaultpwd' from dba_users_with_defpwd where username='MDDATA';
```

**Remediation:**

```
Execute the following command to change the password
SQL> password mddata

Enter the new password twice:
Changing password for mddata
New password:
Retype new password:
Password changed
```

## *1.1.8 Change the default password for 'MDSYS' (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The MDSYS is the user in that operationalizes the Oracle Multimedia Locator, which serves as part of the storage, management, and retrieval of audio/video images.

**Rationale:**

As the default MDSYS account created by Oracle has a well-known password and can be potentially corrupted to allow the installation of malware disguised and AV plugins, this value should be reset according to the needs of the organization.

**Audit:**

```
select 'defaultpwd' as defaultpassword
from sys.user$
where name='MDSYS'
      and
substr(spare4,3,40)=rawtohex(utl_raw.cast_to_varchar2(sys.dbms_crypto.hash(utl_raw.cas
t_to_raw('sys')||hextoraw(substr(spare4,43,20)), 3)))
union
select 'defaultpwd' as defaultpassword
from sys.user$
where name='MDSYS'
      and
substr(spare4,3,40)=rawtohex(utl_raw.cast_to_varchar2(sys.dbms_crypto.hash(utl_raw.cas
t_to_raw('mdsys')||hextoraw(substr(spare4,43,20)), 3)))
union
select 'defaultpwd' from dba_users_with_defpwd where username='MDSYS';
```

**Remediation:**

```
Execute the following command to change the password
SQL> password mdsys

Enter the new password twice:
Changing password for mdsys
New password:
Retype new password:
Password changed
```

## *1.1.9 Change the default password for 'LBACSYS' (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The LBACSYS account administers the Oracle Label Security (OLS) feature.

**Rationale:**

As the default LBACSYS account created by Oracle has a well-known password and can provide a point for database access/control by unauthorized users, opening up the tables, views, etc. This value should be changed according to the needs of the organization.

**Audit:**

```
select 'defaultpwd' as defaultpassword
from sys.user$
where name='LBACSYS'
      and
substr(spare4,3,40)=rawtohex(utl_raw.cast_to_varchar2(sys.dbms_crypto.hash(utl_raw.cas
t_to_raw('lbacsys')||hextoraw(substr(spare4,43,20)), 3)))
```

```
union
select 'defaultpwd' from dba_users_with_defpwd where username='LBACSYS';
```

**Remediation:**

```
Execute the following command to change the password
SQL> password lbacsys

Enter the new password twice:
Changing password for lbacsys
New password:
Retype new password:
Password changed
```

## *1.1.10 Change the default password for 'OLAPSYS' (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The `OLAPSYS` account owns the online analytical processing (OLAP) catalog. OLAP applications are developed/operate to use business intelligence and data warehousing systems and OLAP is optimized for this type of application.

**Rationale:**

As the default `OLAPSYS` account created by Oracle has a well-known password and can be potentially corrupted to allow the installation of malware disguised as a business process, this value should be reset according to the needs of the organization.

**Audit:**

```
select 'defaultpwd' as defaultpassword
from sys.user$
where name='OLAPSYS'
      and
substr(spare4,3,40)=rawtohex(utl_raw.cast_to_varchar2(sys.dbms_crypto.hash(utl_raw.cas
t_to_raw('manager')||hextoraw(substr(spare4,43,20)), 3)))
union
select 'defaultpwd' from dba_users_with_defpwd where username='OLAPSYS';
```

**Remediation:**

```
Execute the following command to change the password
SQL> password olapsys

Enter the new password twice:
Changing password for olapsys
New password:
```

```
Retype new password:
Password changed
```

## *1.1.11 Change the default password for 'ORACLE_OCM' (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The `ORACLE_OCM` account supports the operation of the Configuration Manager with the instance and MyOracleSupport.

**Rationale:**

As the default `ORACLE_OCM` account created by Oracle has a well-known password and can provide a point for database access by unauthorized users if left at the default setting, this value should be changed according to the needs of the organization.

**Audit:**

```
select 'defaultpwd' as defaultpassword
from sys.user$
where name='ORACLE_OCM'
      and
substr(spare4,3,40)=rawtohex(utl_raw.cast_to_varchar2(sys.dbms_crypto.hash(utl_raw.cas
t_to_raw('oracle_ocm')||hextoraw(substr(spare4,43,20)), 3)))
union
select 'defaultpwd' from dba_users_with_defpwd where username='ORACLE_COM';
```

**Remediation:**

```
Execute the following command to change the password
SQL> password oracle_ocm

Enter the new password twice:
Changing password for oracle_ocm
New password:
Retype new password:
Password changed
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/server.112/e25513/statviews_5082.htm#REFRN23725

## *1.1.12 Change the default password for 'ORDDATA' (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The ORDDATA user operationalizes/owns the Oracle Multimedia DICOM modality: Digital Imaging and Communications in Medicine (DICOM), which is the industry standard for medical imaging, enables the Database to store, manage, and manipulate all DICOM format medical content.

**Rationale:**

As the default ORDDATA account created by Oracle has a well-known password and can be potentially corrupted to allow the installation of malware disguised as AV plugins, or cause a Denial-of-Service condition by deleting the account, this value should be reset according to the needs of the organization.

**Audit:**

```
select 'defaultpwd' as defaultpassword
from sys.user$
where name='ORDDATA'
      and
substr(spare4,3,40)=rawtohex(utl_raw.cast_to_varchar2(sys.dbms_crypto.hash(utl_raw.cas
t_to_raw('orddata')||hextoraw(substr(spare4,43,20)), 3)))
union
select 'defaultpwd' from dba_users_with_defpwd where username='ORDDATA';
```

**Remediation:**

```
Execute the following command to change the password
SQL> password orddata

Enter the new password twice:
Changing password for orddata
New password:
Retype new password:
Password changed
```

## *1.1.13 Change the default password for 'ORDPLUGINS' (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The ORDPLUGINS provide the plugins to enable the database to store, manage, and retrieve audio/video images, such as the DICOM medical data format.

**Rationale:**

As the default ORDPLUGINS account created by Oracle has a well-known password and can be potentially corrupted to allow the installation of malware disguised and AV plugins, this value should be reset according to the needs of the organization.

**Audit:**

```
select 'defaultpwd' as defaultpassword
from sys.user$
where name='ORDPLUGINS'
      and
substr(spare4,3,40)=rawtohex(utl_raw.cast_to_varchar2(sys.dbms_crypto.hash(utl_raw.cas
t_to_raw('ordplugins')||hextoraw(substr(spare4,43,20)), 3)))
union
select 'defaultpwd' from dba_users_with_defpwd where username='ORDPLUGINS';
```

**Remediation:**

```
Execute the following command to change the password
SQL> password ordplugins

Enter the new password twice:
Changing password for ordplugins
New password:
Retype new password:
Password changed
```

## *1.1.14 Change the default password for 'ORDSYS' (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The ORDSYS user functions as the Oracle Multimedia administrator. DICOM modality: Digital Imaging and Communications in Medicine (DICOM), which is the industry standard for medical imaging, enables the Database to store, manage, and manipulate all DICOM format medical content.

**Rationale:**

As the default ORDDATA account created by Oracle has a well-known password and can be potentially corrupted to allow the installation of malware disguised as AV plugins, or cause a Denial-of-Service condition by deleting the account, this value should be reset according to the needs of the organization.

**Audit:**

```
select 'defaultpwd' as defaultpassword
from sys.user$
```

```
where name='ORDSYS'
      and
substr(spare4,3,40)=rawtohex(utl_raw.cast_to_varchar2(sys.dbms_crypto.hash(utl_raw.cas
t_to_raw('ordsys')||hextoraw(substr(spare4,43,20)), 3)))
union
select 'defaultpwd' from dba_users_with_defpwd where username='ORDSYS';
```

**Remediation:**

```
Execute the following command to change the password
SQL> password ordsys

Enter the new password twice:
Changing password for ordsys
New password:
Retype new password:
Password changed
```

## *1.1.15 Change the default password for 'OUTLN' (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The `OUTLN` user helps preserve application stability by preventing changes to the database environment from overly impacting system performance characteristics.

**Rationale:**

As the default `OUTLN` account created by Oracle has a well-known password and can provide a point for database access by unauthorized users if left at the default setting, this value should be changed according to the needs of the organization.

**Audit:**

```
select 'defaultpwd' as defaultpassword
from sys.user$
where name='OUTLN'
      and
substr(spare4,3,40)=rawtohex(utl_raw.cast_to_varchar2(sys.dbms_crypto.hash(utl_raw.cas
t_to_raw('outln')||hextoraw(substr(spare4,43,20)), 3)))
union
select 'defaultpwd' from dba_users_with_defpwd where username='OUTLN';
```

**Remediation:**

```
Execute the following command to change the password
SQL> password outln

Enter the new password twice:
```

```
Changing password for outln
New password:
Retype new password:
Password changed
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/server.112/e25513/statviews_5082.htm#REFRN23725

## *1.1.16 Change the default password for 'OWBSYS_AUDIT' (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The `OWBSYS_AUDIT` account handles access to the OWBSYS audit/logging tables, which record Warehouse Builder workspace and user analysis/query operations.

**Rationale:**

As the default `OWBSYS_UDIT` account created by Oracle has a well-known password and can be potentially used to take alter the audit/logging tables to alter/delete forensic data that can reveal unauthorized access/alteration of data, this value should be reset according to the needs of the organization.

**Audit:**

```
select 'defaultpwd' as defaultpassword
from sys.user$
where name='OWBSYS_AUDIT'
      and
substr(spare4,3,40)=rawtohex(utl_raw.cast_to_varchar2(sys.dbms_crypto.hash(utl_raw.cas
t_to_raw('owbsys_audit')||hextoraw(substr(spare4,43,20)), 3)))
union
select 'defaultpwd' from dba_users_with_defpwd where username='OWBSYS_AUDIT';
```

**Remediation:**

```
Execute the following command to change the password
SQL> password owbsys_audit

Enter the new password twice:
Changing password for owbsys_audit
New password:
Retype new password:
Password changed
```

## *1.1.17 Change the default password for 'OWBSYS' (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The `OWBSYS` account handles Oracle Warehouse Builder database administrative tasks, which is created during installation and defines the language of repository for the Warehouse Builder workspaces and user analysis/query operations.

**Rationale:**

As the default `OWBSYS` account created by Oracle has a well-known password and can be potentially used to take over the database warehouse structures or access user queries, this value should be reset according to the needs of the organization.

**Audit:**

```
select 'defaultpwd' as defaultpassword
from sys.user$
where name='OWBSYS'
      and
substr(spare4,3,40)=rawtohex(utl_raw.cast_to_varchar2(sys.dbms_crypto.hash(utl_raw.cas
t_to_raw('owbsys')||hextoraw(substr(spare4,43,20)), 3)))
union
select 'defaultpwd' from dba_users_with_defpwd where username='OWBSYS';
```

**Remediation:**

```
Execute the following command to change the password
SQL> password owbsys

Enter the new password twice:
Changing password for owbsys
New password:
Retype new password:
Password changed
```

## *1.1.18 Change the default password for 'SI_INFORMTN_SCHEMA' (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The SI_INFORMTN_SCHEMA functions as the location for storing plugins supplied by Oracle and all other third-party plugins.

**Rationale:**

As the default SI_INFORMTN_SCHEMA account created by Oracle has a well-known password and can be potentially corrupted to allow the installation of malware disguised as third-party multimedia plugins, this value should be reset according to the needs of the organization.

**Audit:**

```
select 'defaultpwd' as defaultpassword
from sys.user$
where name='SI_INFORMTN_SCHEMA'
      and
substr(spare4,3,40)=rawtohex(utl_raw.cast_to_varchar2(sys.dbms_crypto.hash(utl_raw.cas
t_to_raw('si_informtn_schema')||hextoraw(substr(spare4,43,20)), 3)))
union
select 'defaultpwd' from dba_users_with_defpwd where username='SI_INFORMTN_SCHEMA';
```

**Remediation:**

```
Execute the following command to change the password
SQL> password si_informtn_schema

Enter the new password twice:
Changing password for si_informtn_schema
New password:
Retype new password:
Password changed
```

## *1.1.19 Change the default password for 'SPATIAL_CSW_ADMIN_USR' (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The SPATIAL_CSW_ADMIN_USR account owns the Catalog Services for the Web (CSW) capabilities, which are used by Oracle to load record-type metadata and instances from the DB into the main memory when these records are cached.

**Rationale:**

As the default SPATIAL_CSW_ADMIN_USR account created by Oracle has a well-known password and can be potentially corrupted to allow the installation of malware disguised as a business process, this value should be reset according to the needs of the organization.

**Audit:**

```
select 'defaultpwd' as defaultpassword
from sys.user$
where name='SPATIAL_CSW_ADMIN_USR'
      and
substr(spare4,3,40)=rawtohex(utl_raw.cast_to_varchar2(sys.dbms_crypto.hash(utl_raw.cas
t_to_raw('spatial_csw_admin_usr')||hextoraw(substr(spare4,43,20)), 3)))
union
select 'defaultpwd' from dba_users_with_defpwd where username='SPATIAL_CSW_ADMIN_USR';
```

**Remediation:**

```
Execute the following command to change the password
SQL> password spatial_csw_admin_usr

Enter the new password twice:
Changing password for spatial_csw_admin_usr
New password:
Retype new password:
Password changed
```

## *1.1.20 Change the default password for 'SPATIAL_WFS_ADMIN_USR' (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The SPATIAL_WFS_ADMIN_USR account owns the Web Feature Service (WFS) capabilities, which are used by Oracle to load feature instance/metadata from the DB into the main memory when these are pulled from a cache.

**Rationale:**

As the default SPATIAL_WFS_ADMIN_USR account created by Oracle has a well-known password and can be potentially corrupted to allow the installation of malware disguised as a business process, this value should be reset according to the needs of the organization.

**Audit:**

```
select 'defaultpwd' as defaultpassword
from sys.user$
```

```
where name='SPATIAL_WFS_ADMIN_USR'
      and
substr(spare4,3,40)=rawtohex(utl_raw.cast_to_varchar2(sys.dbms_crypto.hash(utl_raw.cas
t_to_raw('spatial_wfs_admin_usr')||hextoraw(substr(spare4,43,20)), 3)))
union
select 'defaultpwd' from dba_users_with_defpwd where username='SPATIAL_WFS_ADMIN_USR';
```

**Remediation:**

```
Execute the following command to change the password
SQL> password spatial_wfs_admin_usr

Enter the new password twice:
Changing password for spatial_wfs_admin_usr
New password:
Retype new password:
Password changed
```

## *1.1.21 Change the default password for 'SYS' (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The `SYS` account is the highest level user created by the database installation.

**Rationale:**

Older versions of Oracle had a well-known password and with the "SYS and SYSDBA" login provides the most powerful a point for an unauthorized user if left at the default setting, this value should be changed according to the needs of the organization.

**Audit:**

```
select 'defaultpwd' as defaultpassword
from sys.user$
where name='SYS'
      and
substr(spare4,3,40)=rawtohex(utl_raw.cast_to_varchar2(sys.dbms_crypto.hash(utl_raw.cas
t_to_raw('manager')||hextoraw(substr(spare4,43,20)), 3)))
union
select 'defaultpwd' as defaultpassword
from sys.user$
where name='SYS'
      and
substr(spare4,3,40)=rawtohex(utl_raw.cast_to_varchar2(sys.dbms_crypto.hash(utl_raw.cas
t_to_raw('change_on_install')||hextoraw(substr(spare4,43,20)), 3)))
union
select 'defaultpwd' as defaultpassword
from sys.user$
where name='SYS'
```

```
      and
substr(spare4,3,40)=rawtohex(utl_raw.cast_to_varchar2(sys.dbms_crypto.hash(utl_raw.cas
t_to_raw('d_syspw')||hextoraw(substr(spare4,43,20)), 3)))
union
select 'defaultpwd' from dba_users_with_defpwd where username='SYS';
```

**Remediation:**

```
Execute the following command to change the password
SQL> password sys

Enter the new password twice:
Changing password for sys
New password:
Retype new password:
Password changed
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/server.112/e25513/statviews_5082.htm#REFRN23725
2. http://www.oracleforensics.com/wordpress/index.php/2012/10/24/sys_throttler-and-distributed-database-forensics/

## *1.1.22 Change the default password for 'SYSTEM' (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The `SYSTEM` user is created for administrative purposes during the database installation.

**Rationale:**

In older versions of Oracle the default `SYSTEM` account had a well-known password and can provide a point for full dba access by unauthorized users if left at the default setting, this value should be changed according to the needs of the organization.

**Audit:**

```
select 'defaultpwd' as defaultpassword
from sys.user$
where name='SYSTEM'
      and
substr(spare4,3,40)=rawtohex(utl_raw.cast_to_varchar2(sys.dbms_crypto.hash(utl_raw.cas
t_to_raw('manager')||hextoraw(substr(spare4,43,20)), 3)))
union
select 'defaultpwd' as defaultpassword
from sys.user$
```

```
where name='SYSTEM'
      and
substr(spare4,3,40)=rawtohex(utl_raw.cast_to_varchar2(sys.dbms_crypto.hash(utl_raw.cas
t_to_raw('d_systpw')||hextoraw(substr(spare4,43,20)), 3)))
union
select 'defaultpwd' from dba_users_with_defpwd where username='SYSTEM';
```

**Remediation:**

```
Execute the following command to change the password
SQL> password system

Enter the new password twice:
Changing password for system
New password:
Retype new password:
Password changed
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/server.112/e25513/statviews_5082.htm#REFRN23725

## *1.1.23 Change the default password for 'WK_TEST' (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The `WK_TEST` account handles access to Oracle Ultrasearch

**Rationale:**

As the default `WK_TEST` account created by Oracle has a well-known password and can be potentially used to take alter the tables or alter/delete forensic data, this value should be reset according to the needs of the organization.

**Audit:**

```
select 'defaultpwd' as defaultpassword
from sys.user$
where name='WK_TEST'
      and
substr(spare4,3,40)=rawtohex(utl_raw.cast_to_varchar2(sys.dbms_crypto.hash(utl_raw.cas
t_to_raw('wk_test')||hextoraw(substr(spare4,43,20)), 3)))
union
select 'defaultpwd' from dba_users_with_defpwd where username='WK_TEST';
```

**Remediation:**

```
Execute the following command to change the password
SQL> password wk_test

Enter the new password twice:
Changing password for wk_test
New password:
Retype new password:
Password changed
```

## *1.1.24 Change the default password for WKPROXY (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The `WKPROXY` account handles the Oracle 9i Application Ultra Search.

**Rationale:**

As the default WKPROXY account created by Oracle has a well-known password and can be potentially used to take alter the tables or alter/delete forensic data, this value should be reset according to the needs of the organization.

**Audit:**

```
select 'defaultpwd' as defaultpassword
from sys.user$
where name='WKPROXY'
      and
substr(spare4,3,40)=rawtohex(utl_raw.cast_to_varchar2(sys.dbms_crypto.hash(utl_raw.cas
t_to_raw('change_on_install')||hextoraw(substr(spare4,43,20)), 3)))
union
select 'defaultpwd' as defaultpassword
from sys.user$
where name='WKPROXY'
      and
substr(spare4,3,40)=rawtohex(utl_raw.cast_to_varchar2(sys.dbms_crypto.hash(utl_raw.cas
t_to_raw('wkproxy')||hextoraw(substr(spare4,43,20)), 3)))
union
select 'defaultpwd' from dba_users_with_defpwd where username='WKPROXY';
```

**Remediation:**

```
Execute the following command to change the password
SQL> password wkproxy

Enter the new password twice:
Changing password for wkproxy
New password:
```

```
Retype new password:
Password changed
```

## *1.1.25 Change the default password for 'WKSYS' (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The `WKSYS` account is the Ultra Search administrator.

**Rationale:**

As the default `WKSYS` account created by Oracle has a well-known password and can provide a point for database access by unauthorized users if left at the default setting, this value should be changed according to the needs of the organization.

**Audit:**

```
select 'defaultpwd' as defaultpassword
from sys.user$
where name='WKSYS'
      and
substr(spare4,3,40)=rawtohex(utl_raw.cast_to_varchar2(sys.dbms_crypto.hash(utl_raw.cas
t_to_raw('wksys')||hextoraw(substr(spare4,43,20)), 3)))
union
select 'defaultpwd' from dba_users_with_defpwd where username='WKSYS';
```

**Remediation:**

```
Execute the following command to change the password
SQL> password wksys

Enter the new password twice:
Changing password for wksys
New password:
Retype new password:
Password changed
```

## *1.1.26 Change the default password for 'WMSYS' (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The WMSYS account stores manages all metadata for the Workspace manager, which provides a virtual environment to isolate workspaces, such as a collection of changes to production data, or keep a changes history, allowing the creation of "what if" scenarios.

**Rationale:**

As the default WMSYS account created by Oracle has a well-known password and can provide a point for database access by unauthorized users if left at the default setting, this value should be changed according to the needs of the organization.

**Audit:**

```
select 'defaultpwd' as defaultpassword
from sys.user$
where name='WMSYS'
      and
substr(spare4,3,40)=rawtohex(utl_raw.cast_to_varchar2(sys.dbms_crypto.hash(utl_raw.cas
t_to_raw('wmsys')||hextoraw(substr(spare4,43,20)), 3)))
union
select 'defaultpwd' from dba_users_with_defpwd where username='WMSYS';
```

**Remediation:**

```
Execute the following command to change the password
SQL> password wmsys

Enter the new password twice:
Changing password for wmsys
New password:
Retype new password:
Password changed
```

## *1.1.27 Change the default password for 'XDB' (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The XDB account enables high-performance storage and retrieval of XML data.

**Rationale:**

As the default XDB account created by Oracle has a well-known password and can provide a point for database access by unauthorized users if left at the default setting, this value should be changed according to the needs of the organization.

**Audit:**

```
select 'defaultpwd' as defaultpassword
from sys.user$
where name='XDB'
      and
substr(spare4,3,40)=rawtohex(utl_raw.cast_to_varchar2(sys.dbms_crypto.hash(utl_raw.cas
t_to_raw('xdb')||hextoraw(substr(spare4,43,20)), 3)))
union
select 'defaultpwd' as defaultpassword
from sys.user$
where name='XDB'
      and
substr(spare4,3,40)=rawtohex(utl_raw.cast_to_varchar2(sys.dbms_crypto.hash(utl_raw.cas
t_to_raw('change_on_install')||hextoraw(substr(spare4,43,20)), 3)))
union
select 'defaultpwd' from dba_users_with_defpwd where username='XDB';
```

**Remediation:**

```
Execute the following command to change the password
SQL> password xdb

Enter the new password twice:
Changing password for xdb
New password:
Retype new password:
Password changed
```

## *1.2 Remove Oracle Sample Users*

Oracle sample schema are not needed for the operation of the database. That's why the Oracle sample users (BI,HR,OE,PM,IX,SH, SCOTT) should be removed after checking the the schema are really sample schema.

### *1.2.1 Remove the sample user 'BI' (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The `BI` account owns the Business Intelligence (BI) sample schema.

**Rationale:**

As the default `BI` account created by Oracle has a well-known password and can be potentially used to alter the database to launch exploits against Production to gain unauthorized access to user data, this value should be reset according to the needs of the organization.

**Audit:**

```
SQL> SELECT username||' ['||created||']' FROM ALL_USERS WHERE USERNAME='BI';
```

**Remediation:**

```
SQL> DROP USER BI CASCADE;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/server.112/e10575/tdpsg_user_accounts.htm#TDPSG20303

## *1.2.2 Remove the sample user 'HR' (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The `HR` account is used to manage the HR (Human Resources) sample schema.

**Rationale:**

As the default `HR` account created by Oracle has a well-known password and can be potentially used to alter the database to launch exploits against Production to gain unauthorized access to user data, this value should be reset according to the needs of the organization.

**Audit:**

```
SQL> SELECT username||' ['||created||']' FROM ALL_USERS WHERE USERNAME='HR';
```

**Remediation:**

```
SQL> DROP USER HR CASCADE;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/server.112/e10831/scripts.htm#autoId3

## *1.2.3 Remove the sample user 'IX' (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The IX account is used to manage the Information eXchange (IX) sample schema.

**Rationale:**

As the default IX account created by Oracle has a well-known password and can be potentially used to alter the database to launch exploits against Production to gain unauthorized access to user data, this value should be reset according to the needs of the organization.

**Audit:**

```
SQL> SELECT username||' ['||created||']' FROM ALL_USERS WHERE USERNAME='IX';
```

**Remediation:**

```
SQL> DROP USER IX CASCADE;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/server.112/e10831/scripts.htm#autoId9

## *1.2.4 Remove the sample user 'OE' (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The OE account is used to manage the Order Entry (OE) sample schema.

**Rationale:**

As the default OE account created by Oracle has a well-known password and can be potentially used to alter the database to launch exploits against Production to gain unauthorized access to user data, this value should be reset according to the needs of the organization.

**Audit:**

```
SQL> SELECT username||' ['||created||']' FROM ALL_USERS WHERE USERNAME='OE';
```

**Remediation:**

```
SQL> DROP USER OE CASCADE;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/server.112/e10831/scripts.htm#autoId5

## *1.2.5 Remove the sample user 'PM' (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The `PM` account is used to manage the product media (PM) sample schema for Business-to-Business.

**Rationale:**

As the default `PM` account created by Oracle has a well-known password and can be potentially used to alter the database to launch exploits against Production to gain unauthorized access to user data, this value should be reset according to the needs of the organization.

**Audit:**

```
SQL> SELECT username||' ['||created||']' FROM ALL_USERS WHERE USERNAME='PM';
```

**Remediation:**

```
SQL> DROP USER PM CASCADE;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/server.112/e10831/scripts.htm#autoId7

## *1.2.6 Remove the sample user 'SCOTT' (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The `SCOTT` account is used in examples throughout the Oracle database.

**Rationale:**

As the default SCOTT account created by Oracle has a well-known password and can be potentially used to alter the database or to launch exploits against Production to gain unauthorized access to user data, this value should be reset according to the needs of the organization.

**Audit:**

```
SQL> SELECT username||' ['||created||']' FROM ALL_USERS WHERE USERNAME='SCOTT';
```

**Remediation:**

```
SQL> DROP USER SCOTT CASCADE;
```

## *1.2.7 Remove the sample user 'SH' (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The SH account is used to manage the SH sales schema, which stores business data.

**Rationale:**

As the default SH account created by Oracle has a well-known password and can be potentially used to alter the database to launch exploits against Production to gain unauthorized access to user data, this value should be reset according to the needs of the organization.

**Audit:**

```
SQL> SELECT username||' ['||created||']' FROM ALL_USERS WHERE USERNAME='SH';
```

**Remediation:**

```
SQL> DROP USER SH CASCADE;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/server.112/e10831/scripts.htm#autoId11

## *1.3 Ensure the latest version/patches for Oracle software is installed (Not Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The Oracle installation version, along with the patch level, should be the most recent that is compatible with the organizations' operational needs.

There are two ways to detect the patch level. Opatch is (only) checking if the files at the operating system level is patched properly. The view DBA_REGISTRY_HISTORY shows if the database related part was applied. If the result from DBA_REGISTRY_HISTORY is empty no (security) patch was applied

To be on the safe side, the view DBA_REGISTRY history should be queried.

**Rationale:**

As using the most recent Oracle database software, along with all applicable patches can help limit the possibilities for vulnerabilities in the software, the installation version and/or patches applied during setup should be established according to the needs of the organization.

**Audit:**

```
# opatch lsinventory -detail
```

and

```
SQL> select DBA_REGISTRY_HISTORY;
```

**Remediation:**

```
Download the apropriate patch (PSU, CPU) and apply it against the database. See
readme.txt for more details.
```

**References:**

1. http://www.oracle.com/us/support/assurance/fixing-policies/index.html
2. http://www.oracle.com/technetwork/topics/security/alerts-086861.html

### *1.4 Lock the Oracle software owner account (Not Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The Oracle installation requires a software account owner (often called oracle). This account should be locked.

**Rationale:**

The Oracle user should not be accessed remotely (e.g. SSH, telnet, FTP). Use a personalized user account and use sudo to run commands as user Oracle.

**Audit:**

```
$ grep oracle /etc/passwd
```

**Remediation:**

```
# sudo usermod --lock --shell /bin/nologin oracle
```

## *2 Oracle Directory and File Permissions*

The role of access control through file ownership and permissions is self-evident--the major difficulty with Oracle is determining which files it is critical to control OS-based access to. In the below, the names **"orauser"** and **"oragroup"** will substitute for whatever the organization has chosen for the primary Oracle user/group names. The primary criterion for compliance in this regard is that the instance has had the user/group names changed from the default values given by Oracle.

### *2.1 Verify/set ownership of the $ORACLE_HOME/bin directory (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The `ORACLE_HOME/bin` directory contains all the primary system binaries.

**Rationale:**

As lax permissions on this directory could allow unauthorized users to alter/substitute the directory contents to launch exploits, access should be restricted according to the needs of the organization.

**Audit:**

```
$ ls -ald $ORACLE_HOME/bin
$ drwxr-xr-x 2 orauser oragrp 12288 $ORACLE_HOME /bin
```

**Remediation:**

```
$ chown orauser $ORACLE_HOME/bin
$ chgrp oragrp $ORACLE_HOME/bin
$ chmod 755 $ORACLE_HOME/bin/*
```

## *2.2 Verify/set the umask for the oracle user (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The `umask` setting can be in a number of places, such as the users' "`*.rc`" shells, to set the default permissions for all files created by that user or in `/etc/profile`, to provide a basic umask for all users.

**Rationale:**

As lax umask settings could allow access to unauthorized users who could alter/substitute the contents of any with the wrong permissions file to launch exploits, this value should be set according to the needs of the organization.

**Audit:**

**$ umask**

**Remediation:**

$ sed -e 's/umask 022/umask 027/' </etc/profile> /etc/profile.new mv /etc/profile.new /etc/profile

OR

If the above Audit script produced no output use:

$ echo umask 027 >> /etc/profile

If using sed is discouraged, the vi text editor can add the "umask 027" value to the /etc/profile or the /etc/skel/.bashrc

**References:**

1. http://docs.oracle.com/cd/E11882_01/network.112/e16543/guidelines.htm#DBSEG501

## *2.3 Verify/set permissions for the init.ora file (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The `init.ora` file contains all the primary system startup (`init`) settings. This file is stored in the `$ORACLE_HOME/dbs` directory and can have between 200-300 instance startup parameters.

**Rationale:**

As lax permissions on this file could allow unauthorized users to alter/substitute the contents of the file to launch exploits, access should be restricted according to the needs of the organization.

**Audit:**

```
$ ls -ald $ORACLE_HOME/dbs/init.ora
$ -rw-r--r-- 1 orauser oragrp (truncated)
```

**Remediation:**

```
$ chown orauser $ORACLE_HOME/dbs/init.ora
$ chgrp oragrp $ORACLE_HOME/dbs/init.ora
$ chmod 644 $ORACLE_HOME/dbs/init.ora
```

## *2.4 Verify/set permissions for the database datafiles (*.dbs) (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The ORACLE_HOME/dbs directory contains configuration files, such as the "`/u01/oracle/prod/rbs01.dbs`," "`/u01/oracle/prod/users01.dbs`,"and "`/u01/oracle/prod/temp01.dbs`," which hold sensitive user information.

**Rationale:**

As lax permissions on this directory could allow unauthorized users to overwrite the files to launch exploits, access should be restricted according to the needs of the organization.

**Audit:**

```
$ ls -ald $ORACLE_HOME/dbs
$ drwxr-xr-x 2 oracle oracle
```

**Remediation:**

```
$ chmod 750 $ORACLE_HOME/dbs
$ chown orauser $ORACLE_HOME/dbs/*
$ chgrp oragroup $ORACLE_HOME/dbs/*
```

## *2.5 Verify/set permissions for the audit_file_dest file target (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The `audit_file_dest` log file in `init.ora` target specifies the location where the DB instance's audit dump files are kept, which is set to `$ORACLE_BASE/admin/orcl/adump` by default. It is also the location where the `audit_sys_operations`, records for the full auditing of SYS, are written.

**Rationale:**

As lax permissions on `audit_file_dest` file target could allow unauthorized users to overwrite the file(s) and launch exploits to corrupt the log files, access to the log file should be restricted according to the needs of the organization.

**Audit:**

```
$ ls -ald $ORACLE_BASE/admin/orcl/adump
$ drwxr-x--- 2 orauser oragrp  (output truncated)
```

**Remediation:**

```
$ chmod 750 $ORACLE_BASE/admin/orcl/adump
```

## *2.6 Verify/set permissions for the diagnostic_dest file target (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The `diagnostic_dest` directory parameter identifies the location of the Automatic Diagnostic Repository (ADR), which contains data such as the alert log, dumps, [db health] monitor reports, and traces and is set to the `$ORACLE_BASE` directory by default. In Oracle 11gR2 the Diagnostic Destination replaces the initialization parameter settings for background dump, user dump, and core dump destinations.

**Rationale:**

As lax permissions on `diagnostic_dest` directory target could allow unauthorized users to overwrite the file(s) and launch exploits to corrupt the log files, access to the log file should be restricted according to the needs of the organization.

**Audit:**

```
$ ls -ald $ORACLE_BASE
$ drwxr-xr-x 9 orauser oragrp  (output truncated)
```

**Remediation:**

```
$ chmod 750 $ORACLE_BASE
```

## *2.7 Verify/set permissions for the control_files file target (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The database `control_files` parameter sets the "physical" structure of the database in the way a complex building's creation is specified by engineering drawings. The `*.ctl` file's contents are absolutely essential to the DB's operation and may contain, but are not limited to the following:

- Archive log mode setting,
- Archive log history,
- DB information (RESETLOGS SCN and their time stamp),
- DB name,
- Redo log threads, and
- Tablespace/datafile records -- checkpoints, filenames, on/offline, etc.

**Rationale:**

As lax permissions on the `control_files` file targets could allow unauthorized users to overwrite the file(s) and launch exploits to corrupt/destroy the database, access to the control files should be restricted according to the needs of the organization.

**Audit:**

```
SQL: SELECT NAME FROM V$CONTROLFILE;
  (Then check the resulting file paths from the SQL CLI)
$ ls -al /control/file/path/name(s)
```

**Remediation:**

```
$ chown orauser /control/file/names(s)
$ chgrp oragrp /control/file/names(s)
$ chmod 750 /control/file/names(s)
```

## *2.8 Verify/set permissions on the $ORACLE_HOME/network/admin/ directory files (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The `$ORACLE_HOME/network/admin` directory holds all the files that are restricted to the `dba` group.

**Rationale:**

As lax permissions on the `$ORACLE_HOME/network/admin` directory files could allow unauthorized users to overwrite these file(s) and launch exploits to corrupt/destroy the database, directory access should be restricted according to the needs of the organization.

**Audit:**

```
$ ls-ald $ORACLE_HOME/network/admin/*
```

**Remediation:**

```
$ chmod 644 $ORACLE_HOME /network/admin/*
$ chown orauser.oragrp $ORACLE_HOME /network/admin/*
```

## *2.9 Verify/set permissions on the log_directory_server= target (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The `sqlnet.ora` file contains many database and system parameters, including the `log_directory_server=`(directory target) to specify the database server's trace file destination directory.

**Rationale:**

As lax permissions on the `log_directory_server=`(directory target) could allow unauthorized users to overwrite the database server's log file(s) and corrupt/obscure any forensic evidence within it, access to this file target should be restricted according to the needs of the organization.

**Audit:**

```
$ grep log_directory_server  \ $ORACLE_HOME/network/admin/sqlnet.ora
$ log_directory_server=dirpath
```

**Remediation:**

```
$ chmod 750 dirpath
$ chown orauser.oragrpoup log_directory_server dirpath
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/network.112/e10835/sqlnet.htm#NETRF187

## *2.10 Verify/set permissions on the trace_directory_server target (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The `sqlnet.ora` file contains many database and system parameters, including the `log_directory_server=`(directory target) to specify the database server's trace file destination directory.

**Rationale:**

As lax permissions on the `log_directory_server=`(directory target) could allow unauthorized users to overwrite the database server's trace file(s) and corrupt/obscure any forensic evidence within it, access to this file target should be restricted according to the needs of the organization.

**Audit:**

```
$ grep log_directory_server \
  $ORACLE_HOME/network/admin/sqlnet.ora
$ trace_directory_server=dirpath
```

**Remediation:**

```
$ chmod 750 dirpath
$ chown orauser.oragrp trace_directory_server dirpath
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/network.112/e10835/sqlnet.htm#NETRF243

## *2.11 Verify/set permissions on the listener.ora file (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The `listener.ora` file contains the name of the listener file and the network protocol/ address combinations offered by the database services.

**Rationale:**

As lax permissions on the `listener.ora` file could allow unauthorized users access to obtain, corrupt, or obscure any forensic evidence within it, access to this target should be restricted according to the needs of the organization.

**Audit:**

```
$ ls -al $ORACLE_HOME/network/admin/listener.ora
```

**Remediation:**

```
$ chmod 660 $ORACLE_HOME/network/admin/listener.ora
$ chown orauser.oragrp $ORACLE_HOME/network/admin/listener.ora
```

## *2.12 Verify/set permissions on the log_file_listener file (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The `log_file_listener=`( filename) is the name of the listener log file.

**Rationale:**

As lax permissions on the `log_file_listener=`( file target) could allow unauthorized users to corrupt/obscure any forensic evidence within it, access to this target should be restricted according to the needs of the organization.

**Audit:**

```
$ grep log_file_listener \
  $ORACLE_HOME/network/admin/listener.ora
$ log_file_listener=$ORACLE_HOME/network/log/listener.log
  (This is the default value)
```

**Remediation:**

```
$ chmod 750 orauser.oragrp log_file_listener filename
```

## *2.13 Verify/set permissions on the trace_directory_listener_name directory target (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The `trace_directory_listener_name=`(directory target) is the location of the directory for listener trace file.

**Rationale:**

As lax permissions on the `trace_directory_file_listener_name=`(directory target) could allow unauthorized users to corrupt/obscure any forensic evidence within it, access to this target should be restricted according to the needs of the organization.

**Audit:**

```
$ grep trace_directory_listener_name \ $ORACLE_HOME/network/admin/listener.ora
$ TRACE_DIRECTORY_listener=$ORACLE_HOME/network/admin/tracedir
```

**Remediation:**

```
$ chmod 660 $ORACLE_HOME/network/admin/tracedir
$ chown orauser.oragrp $ORACLE_HOME/network/admin/tracedir
```

## *2.14 Verify/set permissions on the trace_file_listener_name file target (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The trace_file_listener_name=( file target) is the location/name of the listener for the trace file.

**Rationale:**

As lax permissions on the trace_file_listener_name=( file target) could allow unauthorized users to corrupt/obscure any forensic evidence within it, access to this target should be restricted according to the needs of the organization.

**Audit:**

```
$ grep trace_file_listener_name \
  $ORACLE_HOME/network/admin/listener.ora
$ $ORACLE_HOME/network/trace/list.trc (default) $ ls -al (resulting file path)
```

**Remediation:**

```
$ chown orauser.oragrp (resulting file path)
$ chmod 660 (resulting file path)
```

# 3 Oracle Parameter Settings

The operation of the Oracle database instance is governed by numerous parameters that are set in specific configuration files and are instance-specific in scope. As alterations of these parameters can cause problems ranging from denial -of-service to theft of proprietary information, these configurations should be carefully considered and maintained.

**Note:**

For all files that have parameters that can be modified with the OS and/or SQL commands/scripts, these will both be listed where appropriate.

## 3.1 listener.ora settings

Settings for the TNS Listener listener.ora

### 3.1.1 Setting for the 'inbound_connect_timeout_listener_name' parameter (Scored)

**Profile Applicability:**

- Level 2 - 11.2 on Oracle Linux 5

**Description:**

The `inbound_connect_timeout_<listener_name>` setting in the `listener.ora` file determines how long "half-open" connections will be maintained before the connection is closed by the database.

**Rationale:**

As the maintenance of half-open connections uses up database networking resources and can ultimately result in a denial-of-service condition, this value should be set according to the needs of the organization.

**Audit:**

```
$ grep -i inbound_connect $ORACLE_HOME/network/admin/listener.ora
$ (not set by default)
```

**Remediation:**

Set the INBOUND_CONNECT_TIMEOUT_<listener_name> to the appropriate value.

**References:**

1. http://docs.oracle.com/cd/E11882_01/network.112/e10835/sqlnet.htm#NETRF210

## *3.1.2 Setting for 'secure_control_listener_name' parameter (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The `SECURE_CONTROL_listener_name` setting determines the type of control connection the Oracle server requires for remote configuration of the listener.

**Rationale:**

As listener configuration changes via unencrypted remote connections can result in unauthorized users sniffing the control configuration information from the network, these control values should be set according to the needs of the organization.

**Audit:**

```
$ grep  -i SECURE_CONTROL \
$ORACLE_HOME/network/admin/listener.ora
```

**Remediation:**

Set the SECURE_CONTROL_<listener_name> to the appropriate value.

**References:**

1. http://docs.oracle.com/cd/E11882_01/network.112/e10835/listener.htm#NETRF327

## *3.1.3 Setting for 'extproc_dlls' parameter (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The `EXTPROC_DLLS` setting determines whether or not the Oracle server will allow external DLLs and/or libraries to be loaded into the database when external procedures are called. These external procedures work through external routines and allow communication with external applications through PL/SQL.

**Rationale:**

As allowing external DLLs and/or libraries to be loaded into the database when external procedures are called could allow system security protocols to be overwritten or corrupted, this capability should be restricted/disabled according to the needs of the organization.

**Audit:**

```
$ grep  -i extproc_dlls \
  $ORACLE_HOME/network/admin/listener.ora
```

**Remediation:**

```
Use a text editor such as vi to set the EXTPROCS_DLLS =ONLY value along with absolute
pathnames, to set values such as
ENV="EXTPROC_DLLS=ONLY:<custom_dll_directory>/<custom_shared
_library>,LD_LIBRARY_PATH=<oracle_home_directory>/lib")
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/network.112/e10836/advcfg.htm#NETAG0132

## *3.1.4 extproc configuration in listener.ora (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

Oracle Extproc allows to run procedures from operating system libraries. These library calls can allow to run any operating system command.

**Rationale:**

Extproc should be removed from the listener.ora to avoid that attackers are abusing the external procedure feature.

**Audit:**

```
$ grep  -i extproc \
  $ORACLE_HOME/network/admin/listener.ora
```

**Remediation:**

Remove extproc from the listener.ora.

**References:**

1. http://docs.oracle.com/cd/E11882_01/network.112/e10836/advcfg.htm#NETAG0132

### *3.1.5 Setting for 'secure_register_listener_name' parameter (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The `SECURE_REGISTER_<listener_name>` setting determines the type of protocol the Oracle server requires for remote registration connections to the listener.

**Rationale:**

As registration connections to the listener via unencrypted remote connections can result in unauthorized users sniffing the registration information from the network, these protocol values should be set according to the needs of the organization.

**Audit:**

```
$ grep  -i SECURE_REGISTER \
  $ORACLE_HOME/network/admin/listener.ora
```

**Remediation:**

Set the SECURE_REGISTER_<listener_name> to the appropriate value.

**References:**

1. http://docs.oracle.com/cd/E11882_01/network.112/e10835/listener.htm#NETRF328

## *3.1.6 Setting for 'secure_protocol_listener_name' parameter (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The `SECURE_PROTOCOL_<listener_name>` setting determines the type of protocol the Oracle server requires for remote administrative connections to the listener.

**Rationale:**

As administrative connections to the listener via unencrypted remote connections can result in unauthorized users sniffing the administrative information from the network, these protocol values should be set according to the needs of the organization.

**Audit:**

```
$ grep -i  SECURE_PROTOCOL \
  $ORACLE_HOME/network/admin/listener.ora
```

**Remediation:**

Set the SECURE_PROTOCOL_<listener_name> to the appropriate value.

**References:**

1. http://docs.oracle.com/cd/E11882_01/network.112/e10835/listener.htm#NETRF329

### *3.1.7 Setting for the 'admin_restrictions_listener_name' parameter (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The `admin_restrictions_<listener_name>` setting in the `listener.ora` file can require that any attempted real-time alteration of the parameters in the `listener` via the `set` command file be refused unless the `listener.ora` file is manually altered then restarted by a privileged user.

**Rationale:**

As blocking unprivileged users from making alterations of the `listener.ora` file, where remote data/services are specified, will help protect data confidentiality, this value should be set to the needs of the organization.

**Audit:**

```
$ grep -i admin_restrictions  \
  $ORACLE_HOME/network/admin/listener.ora
$ (not set by default)
```

**Remediation:**

Set the ADMIN_RESTRICTIONS_<listener_name> to the value ON.

**References:**

1. http://docs.oracle.com/cd/E11882_01/network.112/e10835/listener.htm#NETRF310

### *3.1.8 Setting for the 'logging_listener_name' parameter (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The `logging_<listener_name>` setting in the `listener.ora` file requires that all listener actions be logged to create an audit trail.

**Rationale:**

As the logging of all actions by the listener will create an audit trail that is invaluable to forensic investigations of unauthorized activities, this value should be set to the needs of the organization.

**Audit:**

```
$ grep -i logging $ORACLE_HOME/network/admin/listener.ora $ (not set by default)
```

**Remediation:**

Set the logging_<listener_name> to the appropriate value.

**References:**

1. http://docs.oracle.com/cd/E11882_01/network.112/e10835/listener.htm#NETRF1914

## *3.1.9 Setting for 'passwords_listener_name' parameter (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The Oracle `listener` provides network connections to the database with the name of the connection, protocol addresses, and services offered by the database. In database versions prior to 11gr2, there was an option to include a password in the `listener.ora` file or to have OS-based authentication for `listener` connections; now only OS-based authentication is allowed and `listener.ora` file password use has been deprecated.

**Rationale:**

As using the default OS-based authentications for `listener` connections can remove the need to include a clear-text password in the `listener.ora` file, any password in this file should be removed according to the needs of the organization.

**Audit:**

```
grep -i PASSWORDS_=
 $ORACLE_HOME/network/admin/listener.ora file
```

**Remediation:**

Remove the PASSWORDS_<listener_name> from the listener.ora.

**References:**

1. http://docs.oracle.com/cd/E11882_01/network.112/e10836/listenercfg.htm#NETAG459

## *3.1.10 Change the default port numbers that connect to Oracle (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The Oracle installation creates a number of well-known ports for connections to the `listener` service; these ports which are often targeted by unauthorized users' automated exploits.

**Rationale:**

As the default ports created by Oracle can provide a target for exploits by unauthorized users, the ports should be changed according to the needs of the organization.

**Audit:**

```
$ grep 1521 $ORACLE_HOME/network/admin/listener.ora
```

**Remediation:**

(new port example is "1527")

```
$ sed -e 's/1521/1527/' <$ORACLE_HOME/network/admin/listener.ora>
$ORACLE_HOME/network/admin/listener.ora.new  mv
$ORACLE_HOME/network/admin/listener.ora.new $ORACLE_HOME/network/admin/listener.ora;
fi
```

### *3.1.11 Setting for parameter 'secure_register_listener_name' parameter (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The `SECURE_REGISTER_<listener_name>` setting specifies the protocols which are used to connect to the TNS listener.

**Rationale:**

As listener configuration changes via unencrypted remote connections can result in unauthorized users sniffing the control configuration information from the network, these control values should be set according to the needs of the organization.

**Audit:**

```
$ grep -i SECURE_REGISTER \
$ORACLE_HOME/network/admin/listener.ora
```

**Remediation:**

```
Use a text editor such as vi to set the SECURE_REGISTER_listener_name=TCPS or
SECURE_REGISTER_listener_name=IPC under the SECURE_REGISTER_listenername= parameter
found in $ORACLE_HOME/network/admin/listener.ora
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/network.112/e10835/listener.htm#NETRF328
2. https://support.oracle.com/epmos/faces/ui/km/DocumentDisplay.jspx?id=1453883.1
3. https://support.oracle.com/epmos/faces/ui/km/DocumentDisplay.jspx?id=1340831.1
4. http://www.joxeankoret.com/download/tnspoison.pdf

### *3.1.12 Setting for 'ADR_BASE_listener_name' parameter (Not Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The ADR_BASE_<*listener_name*> setting specifies the ADR location where the log and traces files are generated.

**Rationale:**

The location of the ADR_BASE files should be in a safe location using secure Linux permissions.

**Audit:**

```
$ grep -i ADR_BASE \
$ORACLE_HOME/network/admin/listener.ora
```

**Remediation:**

Set the ADR_BASE_<listener_name> to the appropriate value.

**References:**

1. http://www.acehints.com/2012/02/purpose-of-adrbaselistener.html

## *3.2 sqlnet.ora settings*

Settings for sqlnet.ora

### *3.2.1 Setting for the 'sqlnet.expire_time' parameter (Scored)*

**Profile Applicability:**

- Level 2 - 11.2 on Oracle Linux 5

**Description:**

The `sqlnet.expire_time` setting in the `sqlnet.ora` file determines how long database connections that are inactive remain open, before the connection is expired by the database.

**Rationale:**

As the maintenance of open connections uses up database networking resources and can ultimately result in a denial-of-service condition, this value should be set according to the needs of the organization.

**Audit:**

```
$ grep -i sqlnet.expire_time \
  $ORACLE_HOME/network/admin/sqlnet.ora
$ (not set by default)
```

**Remediation:**

```
$ if [ `grep '^sqlnet.expire_time =.*' $ORACLE_HOME/network/admin/sqlnet.ora` ]; then
awk '/^ sqlnet.expire_time/ {$1 = "sqlnet.expire_time=10"} {print}'
<$ORACLE_HOME/network/admin/sqlnet.ora>  $ORACLE_HOME/network/admin/sqlnet.ora.new; mv
$ORACLE_HOME/network/admin/sqlnet.ora.new  $ORACLE_HOME/network/admin/sqlnet.ora; else
echo sqlnet.expire_time=10 >> $ORACLE_HOME/network/admin/sqlnet.ora; fi
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/network.112/e10835/sqlnet.htm#NETRF209

## *3.2.2 Setting for the 'sqlnet.inbound_connect_timeout' parameter (Scored)*

**Profile Applicability:**

- Level 2 - 11.2 on Oracle Linux 5

**Description:**

The `sqlnet.inbound_connect_timeout` setting in the `sqlnet.ora` file determines how long "half-open" connections will be maintained, awaiting the completion of authentication, before the connection is closed by the database.

**Rationale:**

As the maintenance of half-open connections uses up database networking resources and can ultimately result in a denial-of-service condition, this value should be set according to the needs of the organization.

**Audit:**

```
$ grep -i sqlnet.inbound_connect_timeout / $ORACLE_HOME/network/admin/sqlnet.ora
$ (not set by default)
```

**Remediation:**

```
$ if [ `grep '^sqlnet.inbound_connect_timeout=.*'
$ORACLE_HOME/network/admin/sqlnet.ora` ]; then awk '/^ sqlnet.inbound_connect_timeout
/ {$1 = " sqlnet.inbound_connect_timeout=3"} {print}'
```

```
<$ORACLE_HOME/network/admin/sqlnet.ora>  $ORACLE_HOME/network/admin/sqlnet.ora.new; mv
$ORACLE_HOME/network/admin/sqlnet.ora.new  $ORACLE_HOME/network/admin/sqlnet.ora; else
echo sqlnet.inbound_connect_timeout=3 >> $ORACLE_HOME/network/admin/sqlnet.ora; fi
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/network.112/e10835/sqlnet.htm#NETRF210

### *3.2.3 Setting for the 'sqlnet.allowed_logon_version' parameter (Scored)*

**Profile Applicability:**

- Level 2 - 11.2 on Oracle Linux 5

**Description:**

The setting for the `SQLNET.ALLOWED_LOGON_VERSION` setting in the `sqlnet.ora` file specifies the versions of the Oracle client that are allowed login privileges.

**Rationale:**

As the pre-11versions of the Oracle client do not use strong authentication for client login and could allow unauthorized users to break credentials sniffed from the network, this value should be set according to the needs of the organization.

**Audit:**

```
$ grep -i SQLNET.ALLOWED_LOGON_VERSION  $ORACLE_HOME/network/admin/sqlnet.ora
```

**Remediation:**

```
$ if [ `grep '^sqlnet.allowed_logon_version=.*' $ORACLE_HOME/network/admin/sqlnet.ora`
]; then awk '/^ sqlnet.allowed_logon_version/ {$1 = "
sqlnet.allowed_logon_version=11"} {print}' <$ORACLE_HOME/network/admin/sqlnet.ora>
$ORACLE_HOME/network/admin/sqlnet.ora.new; mv
$ORACLE_HOME/network/admin/sqlnet.ora.new  $ORACLE_HOME/network/admin/sqlnet.ora; else
echo sqlnet.allowed_logon_version=11 >> $ORACLE_HOME/network/admin/sqlnet.ora; fi
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/network.112/e10835/sqlnet.htm#NETRF196
2. http://marcel.vandewaters.nl/oracle/security/cryptographic-flaws-in-oracle-database-authentication-protocol
3.

## 3.2.4 Setting for the 'tcp.validnode_checking' parameter (Scored)

**Profile Applicability:**

- Level 2 - 11.2 on Oracle Linux 5

**Description:**

The *tcp.validnode_checking* setting in the sqlnet.ora file allow for the testing of incoming connections to see if these match the "invited" and "excluded" systems list.

**Rationale:**

As limiting connections to system by listing invited and excluded hosts will sharply limit the number of systems that can connect to the instance, this value should be set according to the needs of the organization.

**Audit:**

```
$ grep -i tcp.validnode $ORACLE_HOME/admin/network/sqlnet.ora
$ (not set by default)
```

**Remediation:**

```
$ if [ `grep '^tcp_validnode_checking=.*' $ORACLE_HOME/network/admin/sqlnet.ora` ];
then awk '/^tcp_validnode_checking/ {$1 = "tcp_validnode_checking=YES"} {print}'
<$ORACLE_HOME/network/admin/sqlnet.ora> $ORACLE_HOME/network/admin/sqlnet.ora.new; mv
$ORACLE_HOME/network/admin/sqlnet.ora.new $ORACLE_HOME/network/admin/sqlnet.ora; else
echo tcp_validnode_checking=YES >> $ORACLE_HOME/network/admin/sqlnet.ora; fi
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/network.112/e10835/sqlnet.htm#NETRF238

## 3.2.5 Setting for the 'tcp.excluded_nodes' parameter (Scored)

**Profile Applicability:**

- Level 2 - 11.2 on Oracle Linux 5

**Description:**

The tcp.excluded_nodes setting in the sqlnet.ora file provides a list, based on hostname and/or ip addresses, of nodes not allowed to make incoming connections to the Oracle listener.

**Rationale:**

As limiting connections to the system by listing excluded nodes will sharply limit the number of systems that can connect to the instance, thus reducing attack surfaces, this value should be set according to the needs of the organization.

**Audit:**

```
$ grep -i tcp.excluded_nodes $OACLE_HOME/network/admin/sqlnet.ora
$ (not set by default)
```

**Remediation:**

```
$ if [ `grep '^tcp.excluded_nodes=.*' $ORACLE_HOME/network/admin/sqlnet.ora` ]; then
awk '/^ tcp.excluded_nodes/ {$1 = " tcp.excluded_nodes=your_org_ips"} {print}'
<$ORACLE_HOME/network/admin/sqlnet.ora>  $ORACLE_HOME/network/admin/sqlnet.ora.new; mv
$ORACLE_HOME/network/admin/sqlnet.ora.new  $ORACLE_HOME/network/admin/sqlnet.ora; else
echo tcp.ecluded_nodes=(your_org_ips) >> $ORACLE_HOME/network/admin/sqlnet.ora; fi
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/network.112/e10835/sqlnet.htm#NETRF236

## *3.3 Setting for the 'audit_sys_operations' parameter (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on any platform

**Description:**

The `AUDIT_SYS_OPERATIONS` setting provides for the auditing of all user activities conducted under the `SYSOPER` and `SYSDBA` accounts.

**Rationale:**

If the parameter `AUDIT_SYS_OPERATIONS` is FALSE all statements except of Startup/Shutdown and Logon by SYSDBA/SYSOPER users are not audited.

**Audit:**

```
SQL> select value from v$parameter where upper(name)='AUDIT_SYS_OPERATIONS';
```

**Remediation:**

```
SQL> ALTER SYSTEM SET AUDIT_SYS_OPERATIONS = true SCOPE=SPFILE;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/server.112/e25513/initparams015.htm#REFRN10005

## *3.4 Setting for the 'audit_trail' parameter (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The `audit_trail` setting determines whether or not Oracle's basic audit features are enabled. These can be set to "Operating System"(OS), "DB,", "DB,EXTENDED", "XML" or "XML,EXTENDED".

**Rationale:**

As enabling the basic auditing features for the Oracle instance permits the collection of data to troubleshoot problems, as well as providing value forensic logs in the case of a system breach, this value should be set according to the needs of the organization.

**Audit:**

```
SQL> select value
 from v$parameter
 where upper(name)='AUDIT_TRAIL';
```

**Remediation:**

```
SQL> alter system set audit_trail = DB,EXTENDED scope = spfile;
```

or

```
SQL> alter system set audit_trail = OS scope = spfile;
```

or

```
SQL> alter system set audit_trail = XML,EXTENDED scope = spfile;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/server.112/e25513/initparams017.htm#REFRN10006

2. http://www.oracle.com/technetwork/database/audit-vault/learnmore/twp-security-auditperformance-166655.pdf

## *3.5 Setting for the 'global_names' parameter (Scored)*

**Profile Applicability:**

- Level 2 - 11.2 on Oracle Linux 5

**Description:**

The `global_names` setting requires that the name of a database link matches that of the remote database it will connect to.

**Rationale:**

As not requiring database connections to match the domain that is being called remotely could allow unauthorized domain sources to potentially connect via brute-force tactics, this value should be set according to the needs of the organization.

**Audit:**

```
SQL> select value from v$parameter where upper(name)='GLOBAL_NAMES';
```

**Remediation:**

```
SQL> alter system set global_names = true scope = spfile;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/server.112/e25513/initparams096.htm#REFRN10065

## *3.6 Setting for the 'local_listener' parameter (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The `local_listener` setting specifies a network name that resolves to an address of the Oracle TNS listener.

**Rationale:**

The TNS poisoning attack allows to redirect TNS network traffic to another system by registering a listener to the TNS listener. This attack can be performed by unauthorized users with network access. By specifying the IPC protocol it is no longer possible to register listeners via TCP/IP.

**Audit:**

```
SQL> select value from v$parameter a where upper(name) = 'LOCAL_LISTENER';
```

**Remediation:**

```
SQL> alter system set local_listener='(DESCRIPTION=(ADDRESS=
(PROTOCOL=IPC)(KEY=REGISTER))' scope = both;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/server.112/e25513/initparams118.htm#REFRN10082
2. https://support.oracle.com/epmos/faces/ui/km/DocumentDisplay.jspx?id=1453883.1
3. https://support.oracle.com/epmos/faces/ui/km/DocumentDisplay.jspx?id=1340831.1
4. http://www.joxeankoret.com/download/tnspoison.pdf

## *3.7 Setting for the 'remote_listener' parameter (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on any platform

**Description:**

The `remote_listener` setting determines whether or not a valid listener can be established on a system separate from the database instance.

**Rationale:**

As permitting a remote listener for connections to the database instance can allow for the potential spoofing of connections and that could compromise data confidentiality and integrity, this value should be disabled/restricted according to the needs of the organization.

**Audit:**

```
SQL> select value from v$parameter a where upper(name) = 'LOCAL_LISTENER';
```

**Remediation:**

```
SQL> alter system set remote_listener ='' scope = spfile;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/server.112/e25513/initparams208.htm#REFRN10183

## *3.8 Setting for the 'o7_dictionary_accessibility' parameter (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The `O7_dictionary_accessibility` setting is a database initializations parameter that allows/disallows with the EXECUTE ANY PROCEDURE and SELECT ANY DICTIONARY access to objects in the SYS schema; this functionality was created for the ease of migration from Oracle 7 databases to later versions.

**Rationale:**

As leaving the SYS schema so open to connection could permit unauthorized access to critical data structures, this value should be set according to the needs of the organization.

**Audit:**

```
SQL> select value from v$parameter where upper(name)='O7_DICTIONARY_ACCESSIBILITY';
```

**Remediation:**

```
SQL> ALTER SYSTEM SET O7_DICTIONARY_ACCESSIBILITY=FALSE scope=spfile;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/server.112/e25513/initparams157.htm#REFRN10133

## *3.9 Setting for the 'os_roles' parameter (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The `os_roles` setting permits externally created groups to be applied to database management.

**Rationale:**

As allowing the OS use external groups for database management could cause privilege overlaps and generally weaken security, this value should be set according to the needs of the organization.

**Audit:**

```
SQL> select value from v$parameter where upper(name)='OS_ROLES';
```

**Remediation:**

```
SQL> ALTER SYSTEM SET OS_ROLES=false SCOPE=SPFILE;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/server.112/e25513/initparams175.htm#REFRN10153

## *3.10 Setting for the 'remote_os_roles' parameter (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The remote_os_roles setting permits remote users' OS roles to be applied to database management.

**Rationale:**

As allowing remote clients OS roles to have permissions for database management could cause privilege overlaps and generally weaken security, this value should be set according to the needs of the organization.

**Audit:**

```
SQL> select value from v$parameter a where upper(name) = 'REMOTE_OS_ROLES';
```

**Remediation:**

```
SQL> ALTER SYSTEM SET REMOTE_OS_ROLES=false SCOPE=SPFILE;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/server.112/e25513/initparams211.htm#REFRN10186

## *3.11 Setting for the 'remote_os_authent' parameter (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The `remote_os_authent` setting determines whether or not OS 'roles' with the attendant privileges are allowed for remote client connections.

**Rationale:**

As permitting OS roles for database connections to can allow the spoofing of connections and permit granting the privileges of an OS role to unauthorized users to make connections, this value should be restricted according to the needs of the organization.

**Audit:**

```
SQL> select value from v$parameter where upper(name)='REMOTE_OS_AUTHENT';
```

**Remediation:**

```
SQL> alter system set remote_os_authent = false scope = spfile;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/server.112/e25513/initparams210.htm#REFRN10185

## *3.12 Setting for the 'remote_login_passwordfile' parameter (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on any platform

**Description:**

The `remote_login_passwordfile` setting specifies whether or not Oracle checks for a password file during login and how many databases can use the password file.

**Rationale:**

As the use of this sort of password login file could permit unsecured, privileged connections to the database, this value should be set according to the needs of the organization.

**Audit:**

```
SQL> select value from v$parameter where upper(name)='REMOTE_LOGIN_PASSWORDFILE';
```

**Remediation:**

```
SQL> ALTER SYSTEM SET remote_login_passwordfile = none scope = spfile;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/server.112/e25513/initparams209.htm#REFRN10184

## *3.13 Setting for the 'utl_file_dir' parameter (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The `utl_file_dir` setting allows packages like utl_file to access (read/write/modify/delete) files specified in utl_file_dir. (This is deprecated but usable in 11g.)

**Rationale:**

As using the `utl_file_dir` to create directories allows the manipulation of files in these directories.

**Audit:**

```
SQL> select value from v$parameter where upper(name)='UTL_FILE_DIR';
```

**Remediation:**

```
SQL> ALTER SYSTEM SET UTIL_FILE_DIR = '' SCOPE=SPFILE;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/server.112/e25513/initparams266.htm#REFRN10230

## *3.14 Setting for the 'sec_return_server_release_banner' parameter (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The information about patch/update release number provides information about the exact patch/update release that is currently running on the database.

**Rationale:**

As allowing the database to return information about the patch/update release number could facilitate unauthorized users' attempts to gain access based upon known patch weaknesses , this value should be set according to the needs of the organization.

**Audit:**

```
SQL> select value from v$parameter where
upper(name)='SEC_RETURN_SERVER_RELEASE_BANNER';
```

**Remediation:**

```
SQL> ALTER SYSTEM SET sec_return_server_release_banner=false scope=spfile;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/server.112/e25513/initparams226.htm#REFRN10275

## *3.15 Setting for the 'sec_case_sensitive_logon' parameter (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on any platform

**Description:**

The SEC_CASE_SENSITIVE_LOGON information determines whether or not case-sensitivity is required for passwords during login. Due to the security bug CVE-2012-3137 it is recommended to set this parameter to FALSE.

**Rationale:**

Oracle 11g databases without CPU October 2012 patch or later are vulnerable to CVE-2012-3137 if case-sensisitve SHA-1 password hashes are used. To avoid this kind of attack the old DES-hashes have to be used.

**Audit:**

```
SQL> select value from v$parameter where upper(name)='SEC_CASE_SENSITIVE_LOGON';
```

**Remediation:**

```
SQL> ALTER SYSTEM SET SEC_CASE_SENSITIVE_LOGON=FALSE scope=spfile;
```

**Impact:**

If SEC_CASE_SENSITIVE_LOGON is FALSE, all user with SHA-1 hashes only ("select name,password,spare4 from sys.user$ where password is null and spare4 is not null") are no longer able to connect to the database. In this case the password for all users without DES hash have to set again.

**References:**

1. http://docs.oracle.com/cd/E11882_01/server.112/e25513/initparams222.htm#REFRN10299
2. https://support.oracle.com/epmos/faces/DocumentDisplay?id=1492721.1
3. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3137

## *3.16 Setting for the 'sec_max_failed_login_attempts' parameter (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The SEC_MAX_FAILED_LOGIN_ATTEMPTS parameter determines how many failed login attempts are allowed before Oracle closes the login connection.

**Rationale:**

As allowing an unlimited number of login attempts for a user connection can facilitate both brute-force login attacks and the occurrence of Denial-of-Service, this value (10) should be set according to the needs of the organization.

**Audit:**

```
SQL> select value from v$parameter where upper(name)='SEC_MAX_FAILED_LOGIN_ATTEMPTS';
```

**Remediation:**

```
SQL> ALTER SYSTEM SET SEC_MAX_FAILED_LOGIN_ATTEMPTS = 10 scope=spfile;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/server.112/e25513/initparams223.htm#REFRN10274

## *3.17 Setting for the 'sec_protocol_error_further_action' parameter (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The `SEC_PROTOCOL_ERROR_FURTHER_ACTION` setting determines the Oracle's server's response to bad/malformed packets received from the client.

**Rationale:**

As bad packets received from the client can potentially indicate packet-based attacks on the system, such as "TCP SYN Flood" or "Smurf" attacks, which could result in a Denial-of-Service condition, this value should be set according to the needs of the organization.

**Audit:**

```
SQL> select value from v$parameter where
upper(name)='SEC_PROTOCOL_ERROR_FURTHER_ACTION';
```

**Remediation:**

```
SQL> ALTER SYSTEM SET SEC_PROTOCOL_ERROR_FURTHER_ACTION = delay,3 scope=spfile ;
```

```
OR

SQL> ALTER SYSTEM SET SEC_PROTOCOL_ERROR_FURTHER_ACTION = drop,3 scope=spfile ;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/server.112/e25513/initparams224.htm#REFRN10282

## *3.18 Setting for the 'sec_protocol_error_trace_action' parameter (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The `SEC_PROTOCOL_ERROR_TRACE_ACTION` setting determines the Oracle's server's logging response level to bad/malformed packets received from the client, by generating `ALERT`, `LOG`, or `TRACE` levels of detail in the log files.

**Rationale:**

As bad packets received from the client can potentially indicate packet-based attacks on the system, such as "TCP SYN Flood" or "Smurf" attacks, which could result in a Denial-of-Service condition, this diagnostic/logging value for `ALERT`, `LOG`, or `TRACE` conditions should be set according to the needs of the organization.

**Audit:**

```
SQL> select value from v$parameter where
upper(name)='SEC_PROTOCOL_ERROR_TRACE_ACTION';
```

**Remediation:**

```
SQL> ALTER SYSTEM SET SEC_PROTOCOL_ERROR_TRACE_ACTION=LOG scope=spfile;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/server.112/e25513/initparams225.htm#REFRN10283

## *3.19 Setting for the 'sql92_security' parameter (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The `sql92_security parameter` setting `FALSE` allows to grant only `UPDATE` or `DELETE` privileges without the need to grant SELECT privileges.

**Rationale:**

The default value FALSE of the parameter `sql92_security` is secure out-of-the-box. Several security guides recommend the unsecure setting TRUE. This unsecure setting TRUE allows users which need only UPDATE/DELETE privileges to select data directly instead of guessing it.

**Audit:**

```
SQL> select value from v$parameter where upper(name)='SQL92_SECURITY';
```

**Remediation:**

```
SQL> ALTER SYSTEM SET sql92_security=FALSE SCOPE=SPFILE;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/server.112/e25513/initparams246.htm#REFRN10210

## *3.20 Setting for undocumented '_trace_files_public' parameter (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The `_trace_files_public` setting determines whether or not the system's trace file is world readable.

**Rationale:**

As permitting the unix read permission to other anyone can read the instance's trace files file which could contain sensitive information about instance operations, this value should be restricted according to the needs of the organization.

**Audit:**

```
SQL>  select value
 from v$parameter where lower(name)='_trace_files_public';
```

**Remediation:**

```
SQL> alter system set "_trace_files_public"=false scope=spfile;
```

**References:**

1. http://asktom.oracle.com/pls/asktom/f?p=100:11:0::::P11_QUESTION_ID:4295521746131

# 4 Oracle client/user connection and login restrictions

The restrictions on Client/User connections to the Oracle database help block unauthorized access to data and services by setting access rules; these security measures help to ensure that successful logins cannot be easily made through brute-force password attacks or intuited by clever social engineering exploits. By the use of the base profile, e.g. "DEFAULT," then assigning this profile to a client, the database administrator can set a standard policy for password security/resource use to all users assigned the 'DEFAULT' profile; however, this policy can still be overridden by local policy. All values assigned below are the recommended minimums or maximums; higher, more restrictive values can be applied at the discretion of the organization by creating a separate profile to assign to a different user group.

## 4.1 Rejected - Database Profile

Set and define database profiles for the different use cases (personal user vs. technical account vs. DBA account

## 4.2 Restrictions on failed login attempts via the default DB profile (Scored)

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The `failed_login_attempts` setting determines how many failed login attempts are permitted before the system locks the user's account. While different profiles can have

different and more restrictive settings, such as USERS and APPS, the minimum(s) recommended here should be set on the DEFAULT profile.

**Rationale:**

As repeated failed login attempts can indicate the initiation of a brute-force login attack, this value should be set according to the needs of the organization (see **warning** below on a known bug that can make this security measure backfire).

**Audit:**

```
SQL> SELECT PROFILE, RESOURCE_NAME, LIMIT FROM DBA_PROFILES WHERE PROFILE='DEFAULT'
AND RESOURCE_NAME='FAILED_LOGIN_ATTEMPTS';
```

**Remediation:**

```
SQL> ALTER PROFILE DEFAULT LIMIT FAILED_LOGIN_ATTEMPTS 5;
```

## *4.3 Requirements for account locking via on the default DB profile (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The `PASSWORD_LOCK_TIME` setting determines how many days must pass for the user's account to be unlocked after the set number of failed login attempts has occurred.

**Rationale:**

As locking the user account after repeated failed login attempts can block further brute-force login attacks, but can create administrative headaches as this account unlocking process always requires DBA intervention, this value should be set according to the needs of the organization.

**Audit:**

```
SQL> SELECT PROFILE, RESOURCE_NAME, LIMIT FROM DBA_PROFILES WHERE PROFILE='DEFAULT'
AND RESOURCE_NAME='PASSWORD_LOCK_TIME';
```

**Remediation:**

```
SQL> ALTER PROFILE DEFAULT LIMIT PASSWORD_LOCK_TIME 1;
```

## *4.4 Restrictions on password duration via the default DB profile (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The `password_life_time` setting determines how long a password may be used before the user is required to be change it.

**Rationale:**

As allowing passwords to remain unchanged for long periods makes the success of brute-force login attacks more likely, this value should be set according to the needs of the organization.

**Audit:**

```
SQL> SELECT PROFILE, RESOURCE_NAME, LIMIT FROM DBA_PROFILES WHERE PROFILE='DEFAULT'
AND RESOURCE_NAME='PASSWORD_LIFE_TIME';
```

**Remediation:**

```
SQL> ALTER PROFILE DEFAULT LIMIT PASSWORD_LIFE_TIME 90;
```

## *4.5 Restrictions on password history via the default DB profile (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The `password_reuse_max` setting determines how many different passwords must be used before the user is allowed to reuse a prior password.

**Rationale:**

As allowing reuse of a password within a short period of time after the password's initial use can make the success of both social-engineering and brute-force password-based attacks more likely, this value should be set according to the needs of the organization.

**Audit:**

```
SQL> SELECT PROFILE, RESOURCE_NAME, LIMIT FROM DBA_PROFILES WHERE PROFILE='DEFAULT'
AND RESOURCE_NAME='PASSWORD_REUSE_MAX';
```

**Remediation:**

```
SQL> ALTER PROFILE DEFAULT LIMIT PASSWORD_REUSE_MAX 20;
```

## *4.6 Restrictions on password use (reuse) via a DB profile (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The `password_reuse_time` setting determines the amount of time in days that must pass before the same password may be reused.

**Rationale:**

As reusing the same password after only a short period of time has passed makes the success of brute-force login attacks more likely, this value should be set according to the needs of the organization.

**Audit:**

```
SQL> SELECT PROFILE, RESOURCE_NAME, LIMIT FROM DBA_PROFILES WHERE PROFILE='DEFAULT'AND
RESOURCE_NAME='PASSWORD_REUSE_TIME';
```

**Remediation:**

```
SQL> ALTER PROFILE DEFAULT PASSWORD_REUSE_TIME 365;
```

## *4.7 Requirements for account locking (grace time) via a DB profile (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The `password_grace_time` setting determines how many days can pass after the user's password expires before the user's login capability is automatically locked out.

**Rationale:**

As locking the user account after the expiration of the password change requirement's grace period can help prevent password-based attack against a forgotten or disused accounts, while still allowing the account and its information to be accessible by DBA intervention, this value should be set according to the needs of the organization.

**Audit:**

```
SQL> SELECT PROFILE, RESOURCE_NAME, LIMIT FROM DBA_PROFILES WHERE PROFILE='DEFAULT'AND
RESOURCE_NAME='PASSWORD_GRACE_TIME';
```

**Remediation:**

```
SQL> ALTER PROFILE DEFAULT PASSWORD_GRACE_TIME 5;
```

## *4.8 Requirements for limiting EXTERNAL user login capability (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The `password='EXTERNAL'` setting determines whether or not a user can be authenticated by a remote OS to allow access to the database with full authorization.

**Rationale:**

As allowing remote OS authentication of a user to the database can potentially allow supposed "privileged users" to connect as "authenticated," even when the remote system is compromised, these logins should be disabled/restricted according to the needs of the organization.

**Audit:**

```
SQL> SELECT USERNAME FROM DBA_USERS WHERE AUTHENTICATION_TYPE='EXTERNAL';
```

**Remediation:**

```
SQL> ALTER USER username IDENTIFIED BY password;
```

## *4.9 Requirement for setting the password verification function (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The `password_verify_function` determines password settings requirements when a user password is changed at the SQL command prompt. This applies not for users managed by the Oracle password file

**Rationale:**

As requiring users to apply the 11gr2 security features in password creation, such as forcing mixed-case complexity, the blocking of simple combinations, and change/history settings can potentially thwart logins by unauthorized users, this function should be applied/enabled according to the needs of the organization.

**Audit:**

```
SQL> SELECT PROFILE, RESOURCE_NAME FROM DBA_PROFILES WHERE
RESOURCE_NAME='PASSWORD_VERIFY_FUNCTION';
```

**Remediation:**

Create a custom password verification function which fulfills the password requirements of the organization.

## *4.10 Requirements for limiting the number of sessions per user (Scored)*

**Profile Applicability:**

- Level 2 - 11.2 on Oracle Linux 5

**Description:**

The `SESSIONS_PER_USER` (Number of sessions allowed) determines the maximum number of user sessions that are allowed to be open concurrently.

**Rationale:**

As limiting the number of the `SESSIONS_PER_USER` can help prevent memory resource exhaustion by poorly formed requests or intentional Denial-of-Service attacks, this value should be set according to the needs of the organization.

**Audit:**

```
SQL>  SELECT PROFILE, RESOURCE_NAME, LIMIT FROM DBA_PROFILES WHERE
RESOURCE_NAME='SESSIONS_PER_USER' AND PROFILE='DEFAULT';
```

**Remediation:**

```
SQL> ALTER PROFILE DEFAULT LIMIT SESSIONS_PER_USER 10;
```

# 5 Oracle user access and authorization restrictions

The capability to use database resources at a given level, or user authorization rules, allows for user manipulation of the various parts of the Oracle database; these authorizations must be structured to block unauthorized use and/or corruption of vital data and services, by setting restrictions on user capabilities, particularly those of the user PUBLIC; these security measures help to ensure that successful logins cannot be easily redirected.

## 5.1 Default Public Privileges for Packages and Object Types

Revoke default public execute privileges from powerful packages and object types

### 5.1.1 Limit public access to the DBMS_ADVISOR package (Scored)

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The Oracle database DBMS_ADVISOR package can be used to write files located on the server where the Oracle instance is installed.

**Rationale:**

As use of the `DBMS_ADVISOR` package could allow an unauthorized user to corrupt operating system files on the instance's host, use of this package should be restricted according to the needs of the organization.

**Audit:**

```
SQL> SELECT GRANTEE, TABLE_NAME FROM DBA_TAB_PRIVS where TABLE_NAME='DBMS_ADVISOR' AND
GRANTEE ='PUBLIC';
```

**Remediation:**

```
SQL> REVOKE EXECUTE ON DBMS_ADVISOR FROM PUBLIC;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/appdev.112/e25788/d_advis.htm

### *5.1.2 Limit public access to the DBMS_CRYPTO package (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The `DBMS_CRYPTO` settings provide a toolset that determines the strength of the encryption algorithm used to encrypt application data and is part of the SYS schema. The DES (56-bit key), 3DES (168-bit key), 3DES-2KEY (112-bit key), AES (128/192/256-bit keys), and RC4 are available.

**Rationale:**

As execution of these cryptography procedures by the user PUBLIC can potentially endanger portions of or all of the data storage, this value should be set according to the needs of the organization.

**Audit:**

```
SQL> SELECT GRANTEE, PRIVILEGE, TABLE_NAME FROM DBA_TAB_PRIVS WHERE
TABLE_NAME='DBMS_CRYPTO';
```

**Remediation:**

```
SQL> REVOKE EXECUTE ON DBMS_CRYPTO FROM PUBLIC;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/appdev.112/e25788/d_crypto.htm#ARPLS664

### *5.1.3 Limit public access to the DBMS_JAVA package (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The Oracle database `DBMS_JAVA` package can xxx.

**Rationale:**

As use of the `DBMS_JAVA` package xxx.

**Audit:**

```
SQL> SELECT GRANTEE, TABLE_NAME FROM DBA_TAB_PRIVS where TABLE_NAME='DBMS_JAVA' AND
GRANTEE = 'PUBLIC';
```

**Remediation:**

```
SQL> REVOKE EXECUTE ON DBMS_JAVA FROM PUBLIC;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/java.112/e10588/appendixa.htm#JJDEV13000

### *5.1.4 Limit public access to the DBMS_JAVA_TEST package (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The Oracle database `DBMS_JAVA_TEST` package can xxx.

**Rationale:**

As use of the `DBMS_JAVA_TEST` package xxx.

**Audit:**

```
SQL> SELECT GRANTEE, TABLE_NAME FROM DBA_TAB_PRIVS where TABLE_NAME='DBMS_JAVA_TEST'
AND GRANTEE ='PUBLIC';
```

**Remediation:**

```
SQL> REVOKE EXECUTE ON DBMS_JAVA_TEST FROM PUBLIC;
```

**References:**

1. http://www.databasesecurity.com/HackingAurora.pdf

### *5.1.5 Limit public access to the DBMS_JOB package (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The Oracle database `DBMS_JOB` package schedules and manages the jobs sent to the job queue and has been superseded by the `DBMS_SCHEDULER` package, even though `DBMS_JOB` has been retained for backwards compatibility.

**Rationale:**

As use of the `DBMS_JOB` package could allow an unauthorized user to disable or overload the job queue and has been superseded by the `DBMS_SCHEDULER` package, this package should be disabled or restricted according to the needs of the organization.

**Audit:**

```
SQL> SELECT GRANTEE, TABLE_NAME FROM DBA_TAB_PRIVS WHERE TABLE_NAME='DBMS_JOB' AND
GRANTEE='PUBLIC';
```

**Remediation:**

```
SQL> REVOKE EXECUTE ON DBMS_JOB FROM PUBLIC;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/appdev.112/e25788/d_job.htm

## *5.1.6 Limit public access to the DBMS_LDAP package (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The Oracle database `DBMS_LDAP` package can be used to create specially crafted error messages or send information via DNS to the outside.

**Rationale:**

As use of the `DBMS_LDAP` package xxx.

**Audit:**

```
SQL> SELECT GRANTEE, TABLE_NAME FROM DBA_TAB_PRIVS where TABLE_NAME='DBMS_LDAP' AND
GRANTEE ='PUBLIC';
```

**Remediation:**

```
SQL> REVOKE EXECUTE ON DBMS_LDAP FROM PUBLIC;
```

**References:**

1. http://docs.oracle.com/cd/E23943_01/oid.1111/e10186/dbmsldap_ref.htm#OIMAD009

## *5.1.7 Limit public access to the DBMS_LOB package (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The Oracle database `DBMS_LOB` package provides subprograms that can manipulate and read/write on BLOBs, CLOBs, NCLOBs, BFILEs, and temporary LOBs.

**Rationale:**

As use of the `DBMS_LOB` package could allow an unauthorized user to manipulate BLOBs, CLOBs, NCLOBs, BFILEs, and temporary LOBs on the instance, either destroying data or causing a Denial-of-Service condition due to corruption of disk space, use of this package should be restricted according to the needs of the organization.

**Audit:**

```
SQL> SELECT GRANTEE, TABLE_NAME FROM DBA_TAB_PRIVS where TABLE_NAME='DBMS_LOB' AND
GRANTEE = 'PUBLIC';
```

**Remediation:**

```
SQL> REVOKE EXECUTE ON DBMS_LOB FROM PUBLIC;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/appdev.112/e25788/d_lob.htm

## *5.1.8 Limit public access to the DBMS_OBFUSCATION_TOOLKIT package (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The DBMS_OBFUSCATION_TOOLKIT settings provide one of the tools that determine the strength of the encryption algorithm used to encrypt application data and is part of the SYS schema. The DES (56-bit key) and 3DES (168-bit key) are the only two types available.

**Rationale:**

As allowing the PUBLIC user privileges to access this capability can be potentially harm the data storage, this access should be set according to the needs of the organization.

**Audit:**

```
SQL> SELECT GRANTEE, PRIVILEGE, TABLE_NAME FROM DBA_TAB_PRIVS WHERE
TABLE_NAME='DBMS_OBFUSCATION_TOOLKIT';
```

**Remediation:**

```
SQL> REVOKE EXECUTE ON DBMS_OBFUSCATION_TOOLKIT FROM PUBLIC;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/appdev.112/e25788/d_obtool.htm#ARPLS028

## *5.1.9 Limit public access to the DBMS_RANDOM package (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The Oracle database DBMS_RANDOM package is used for generating random numbers but should not be used for cryptographic purposes.

**Rationale:**

As assignment of use of the DBMS_RANDOM package can allow the unauthorized application of the random number-generating function, this capability should be restricted according to the needs of the organization.

**Audit:**

```
SQL> SELECT GRANTEE FROM DBA_TAB_PRIVS WHERE TABLE_NAME= 'DBMS_RANDOM' AND
GRANTEE='PUBLIC';
```

**Remediation:**

```
SQL> REVOKE EXECUTE ON DBMS_BACKUP_RESTORE FROM PUBLIC;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/appdev.112/e25788/d_random.htm

## 5.1.10 Limit public access to the DBMS_SCHEDULER package (Scored)

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The Oracle database `DBMS_SCHEDULER` package schedules and manages the jobs .

**Rationale:**

As use of the `DBMS_JOB` package could allow an unauthorized user to disable or overload the job queue and has been superseded by the `DBMS_SCHEDULER` package, this package should be disabled or restricted according to the needs of the organization.

**Audit:**

```
SQL> SELECT GRANTEE, TABLE_NAME FROM DBA_TAB_PRIVS WHERE TABLE_NAME='DBMS_SCHEDULER'
AND GRANTEE='PUBLIC';
```

**Remediation:**

```
SQL> REVOKE EXECUTE ON DBMS_SCHEDULER FROM PUBLIC;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/appdev.112/e25788/d_sched.htm

## 5.1.11 Limit public access to the DBMS_SQL package (Scored)

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The Oracle database `DBMS_SQL` package is used for running dynamic SQL statements.

**Rationale:**

The DBMS_SQL package could allow privilege escalation if the input validation is not done properly.

**Audit:**

```
SQL> SELECT GRANTEE, TABLE_NAME FROM DBA_TAB_PRIVS where TABLE_NAME='DBMS_SQL' and
GRANTEE='PUBLIC';
```

**Remediation:**

```
SQL> REVOKE EXECUTE ON DBMS_SQL FROM PUBLIC;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/appdev.112/e25788/d_sql.htm

### *5.1.12 Limit public access to the DBMS_XMLGEN package (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The DBMS_XMLGEN package takes an arbitrary SQL query as input, converts it to XML format, and returns the result as a CLOB.

**Rationale:**

The package DBMS_XMLGEN can be used to search the entire database for critical information like creditcard numbers, ...

**Audit:**

```
SQL> SELECT GRANTEE, TABLE_NAME FROM DBA_TAB_PRIVS where TABLE_NAME='DBMS_XMLGEN' AND
GRANTEE='PUBLIC';
```

**Remediation:**

```
SQL> REVOKE EXECUTE ON DBMS_XMLGEN FROM PUBLIC;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/appdev.112/e25788/d_xmlgen.htm
2. http://www.red-database-security.com/wp/confidence2009.pdf

## *5.1.13 Limit public access to the DBMS_XMLQUERY package (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The Oracle package DBMS_XMLQUERY takes an arbitrary SQL query, converts it to XML format, and returns the result. This package is similar to DBMS_XMLGEN.

**Rationale:**

The package DBMS_XMLQUERY can be used to search the entire database for critical information like creditcard numbers, ...

**Audit:**

```
SQL> SELECT GRANTEE, TABLE_NAME FROM DBA_TAB_PRIVS where TABLE_NAME='DBMS_XMLQUERY'
AND GRANTEE='PUBLIC';
```

**Remediation:**

```
SQL> REVOKE EXECUTE ON DBMS_XMLQUERY FROM PUBLIC;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/appdev.112/e25788/d_xmlque.htm

## *5.1.14 Limit public access to the UTL_FILE package (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The Oracle database `UTL_FILE` package can be used to read/write files located on the server where the Oracle instance is installed.

**Rationale:**

As use of the `UTL_FILE` package could allow an user to read files at the operating system. These files could contain sensitive information (e.g. passwords in .bash_history).

**Audit:**

```
SQL> SELECT GRANTEE, TABLE_NAME FROM DBA_TAB_PRIVS where TABLE_NAME='UTL_FILE' AND
GRANTEE = ('PUBLIC');
```

**Remediation:**

```
SQL> REVOKE EXECUTE ON UTL_FILE FROM PUBLIC;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/appdev.112/e25788/u_file.htm#ARPLS70896

## *5.1.15 Limit public access to the UTL_INADDR package (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The Oracle database `UTL_INADDR` package can be used to create specially crafted error messages or send information via DNS to the outside.

**Rationale:**

As use of the `UTL_INADDR` package is often used in SQL Injection attacks from the web it should be revoked from public.

**Audit:**

```
SQL> SELECT GRANTEE, TABLE_NAME FROM DBA_TAB_PRIVS where TABLE_NAME='UTL_INADDR' AND
GRANTEE ='PUBLIC';
```

**Remediation:**

```
SQL> REVOKE EXECUTE ON UTL_INADDR FROM PUBLIC;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/appdev.112/e25788/u_inaddr.htm

## *5.1.16 Limit public access to the UTL_TCP package (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The Oracle database `UTL_TCP` package can be used to read/write file to TCP sockets on the server where the Oracle instance is installed.

**Rationale:**

As use of the `UTL_TCP` package could allow an unauthorized user to corrupt the TCP stream used for carry the protocols that communicate with the instance's external communications, use of this package should be restricted according to the needs of the organization.

**Audit:**

```
SQL> SELECT GRANTEE, TABLE_NAME FROM DBA_TAB_PRIVS WHERE TABLE_NAME='UTL_TCP' AND
GRANTEE = 'PUBLIC';
```

**Remediation:**

```
SQL> REVOKE EXECUTE ON UTL_TCP FROM PUBLIC;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/appdev.112/e25788/u_tcp.htm#ARPLS71533

## *5.1.17 Limit public access to the UTL_MAIL package (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The Oracle database `UTL_MAIL` package can be used to send email from the server where the Oracle instance is installed.

**Rationale:**

As use of the `UTL_MAIL` package could allow an unauthorized user to corrupt the SMTP function to accept or generate junk mail that can result in a Denial-of-Service condition due to network saturation, use of this package should be restricted according to the needs of the organization.

**Audit:**

```
SQL> SELECT GRANTEE, TABLE_NAME FROM DBA_TAB_PRIVS where TABLE_NAME='UTL_MAIL' and
GRANTEE ='PUBLIC';
```

**Remediation:**

```
SQL> REVOKE EXECUTE ON UTL_MAIL FROM PUBLIC;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/appdev.112/e25788/u_mail.htm

## *5.1.18 Limit public access to the UTL_SMTP package (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The Oracle database `UTL_SMTP` package can be used to send email from the server where the Oracle instance is installed.

**Rationale:**

As use of the `UTL_SMTP` package could allow an unauthorized user to corrupt the SMTP function to accept or generate junk mail that can result in a Denial-of-Service condition due to network saturation, use of this package should be restricted according to the needs of the organization.

**Audit:**

```
SQL> SELECT GRANTEE, TABLE_NAME FROM DBA_TAB_PRIVS where TABLE_NAME='UTL_SMTP' and
GRANTEE = 'PUBLIC';
```

**Remediation:**

```
SQL> REVOKE EXECUTE ON UTL_SMTP FROM PUBLIC;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/appdev.112/e25788/u_smtp.htm

## *5.1.19 Limit public access to the UTL_DBWS package (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The Oracle database `UTL_DBWS` package can be used to read/write file to web-based applications on the server where the Oracle instance is installed.

**Rationale:**

As use of the `UTL_DBWS` package could allow an unauthorized user to corrupt the HTTP stream used for carry the protocols that communicate with the instance's web-based external communications, use of this package should be restricted according to the needs of the organization.

**Audit:**

```
SQL> SELECT GRANTEE, TABLE_NAME FROM DBA_TAB_PRIVS where TABLE_NAME='UTL_DBWS' AND
GRANTEE ='PUBLIC';
```

**Remediation:**

```
SQL> REVOKE EXECUTE ON UTL_DBWS FROM 'PUBLIC';
```

**References:**

1. http://docs.oracle.com/cd/B19306_01/appdev.102/b14258/u_dbws.htm

## *5.1.20 Limit public access to the UTL_ORAMTS package (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The Oracle database UTL_ORAMTS package can be used to perform HTTP-requests. This could be used to send information to the outside.

**Rationale:**

As use of the `UTL_ORAMTS` package could be used to send (sensitive) information to external websites. The use of this package should be restricted according to the needs of the organization.

**Audit:**

```
SQL> SELECT GRANTEE, TABLE_NAME FROM DBA_TAB_PRIVS where TABLE_NAME='UTL_ORAMTS' AND
GRANTEE ='PUBLIC';
```

**Remediation:**

```
SQL> REVOKE EXECUTE ON UTL_ORAMTS FROM PUBLIC;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/win.112/e26104/recovery.htm#NTMTS139

## *5.1.21 Limit public access to the UTL_HTTP package (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The Oracle database `UTL_HTTP` package can be used to perform HTTP-requests. This could be used to send information to the outside.

**Rationale:**

As use of the UTL_HTTP package could be used to send (sensitive) information to external websites. The use of this package should be restricted according to the needs of the organization.

**Audit:**

```
SQL> SELECT GRANTEE, TABLE_NAME FROM DBA_TAB_PRIVS where TABLE_NAME='UTL_HTTP' AND
GRANTEE = 'PUBLIC';
```

**Remediation:**

```
SQL> REVOKE EXECUTE ON UTL_HTTP FROM PUBLIC;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/appdev.112/e25788/u_http.htm

## *5.1.22 Limit public access to the HTTPURITYPE object type (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The Oracle database `HTTPURITYPE` object type can be used to perform HTTP-requests. This could be used to send information to the outside.

**Rationale:**

tbd.

**Audit:**

```
SQL> SELECT GRANTEE, TABLE_NAME FROM DBA_TAB_PRIVS where TABLE_NAME='HTTPURITYPE' AND
GRANTEE ='PUBLIC' ;
```

**Remediation:**

```
SQL> REVOKE EXECUTE ON HTTPURITYPE FROM PUBLIC;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/appdev.112/e25788/t_dburi.htm#ARPLS71705

## 5.2 Non-Default Public Privileges for Packages and Object Types

Non-Default Public Privileges for Packages and Object Types

### 5.2.1 Limiting public user access to the DBMS_SYS_SQL package (Scored)

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The Oracle database `DBMS_SYS_SQL` package is shipped as undocumented.

**Rationale:**

As use of the `DBMS_SYS_SQL` package could allow an user to run code as a different user without entering user credentials.

**Audit:**

```
SQL> SELECT GRANTEE, TABLE_NAME FROM DBA_TAB_PRIVS where TABLE_NAME='DBMS_SYS_SQL' and
grantee='PUBLIC';
```

**Remediation:**

```
SQL> REVOKE EXECUTE ON DBMS_SYS_SQL FROM PUBLIC;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/network.112/e16543/guidelines.htm#DBSEG499
2. http://asktom.oracle.com/pls/asktom/f?p=100:11:0::::P11_QUESTION_ID:1325202421535

## *5.2.2 Limit public access to the DBMS_BACKUP_RESTORE package (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The Oracle database `DBMS_BACKUP_RESTORE` package is used for applying PL/SQL commands to the native RMAN sequences.

**Rationale:**

As assignment of use of the `DBMS_BACKUP_RESTORE` package can allow to access file permissions on operating system level.

**Audit:**

```
SQL> SELECT GRANTEE FROM DBA_TAB_PRIVS WHERE TABLE_NAME= 'DBMS_BACKUP_RESTORE' and
grantee='PUBLIC';
```

**Remediation:**

```
SQL> REVOKE EXECUTE ON DBMS_BACKUP_RESTORE FROM PUBLIC;
```

**References:**

1. http://psoug.org/reference/dbms_backup_restore.html
2. http://davidalejomarcos.wordpress.com/2011/09/13/how-to-list-files-on-a-directory-from-oracle-database/

## *5.2.3 Limiting public user access to the DBMS_AQADM_SYSCALLS package (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The Oracle database `DBMS_AQADM_SYSCALLS` package is shipped as undocumented and allows to run SQL commands as user SYS.

**Rationale:**

As use of the `DBMS_AQADM_SYSCALLS` package could allow an unauthorized user `to run SQL commands as user SYS.`

**Audit:**

```
SQL> SELECT GRANTEE, TABLE_NAME FROM DBA_TAB_PRIVS where
TABLE_NAME='DBMS_AQADM_SYSCALLS' and grantee='PUBLIC';
```

**Remediation:**

```
SQL> REVOKE EXECUTE ON DBMS_AQADM_SYSCALLS FROM PUBLIC;
```

**References:**

1. http://www.databasesecurity.com/dbsec/ohh-indirect-privilege-escalation.pdf

## *5.2.4 Limiting public user access to the DBMS_REPACT_SQL_UTL package (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The Oracle database `DBMS_REPACT_SQL_UTL` package is shipped as undocumented and allows to run SQL commands as user SYS.

**Rationale:**

As use of the `DBMS_REPACT_SQL_UTL` package could allow an unauthorized user to run SQL commands as user SYS.

**Audit:**

```
SQL> SELECT GRANTEE, TABLE_NAME FROM DBA_TAB_PRIVS where
TABLE_NAME='DBMS_REPACT_SQL_UTL' and grantee='PUBLIC';
```

**Remediation:**

```
SQL> revoke execute on DBMS_REPACT_SQL_UTL from PUBLIC;
```

**References:**

1. http://www.databasesecurity.com/dbsec/ohh-indirect-privilege-escalation.pdf

## *5.2.5 Limiting public user access to the INITJVMAUX package (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The Oracle database `INITJVMAUX` package is shipped as undocumented and allows to run SQL commands as user SYS.

**Rationale:**

As use of the `INITJVMAUX` package could allow an unauthorized user to run SQL commands as user SYS.

**Audit:**

```
SQL> SELECT GRANTEE, TABLE_NAME FROM DBA_TAB_PRIVS where TABLE_NAME='INITJVMAUX' and
grantee='PUBLIC';
```

**Remediation:**

```
SQL> Revoke execute on INITJVMAUX from PUBLIC;
```

**References:**

1. http://www.databasesecurity.com/dbsec/ohh-indirect-privilege-escalation.pdf

## *5.2.6 Limiting public user access to the DBMS_STREAMS_ADM_UTL package (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The Oracle database `DBMS_STREAMS_ADM_UTL` package is shipped as undocumented and allows to run SQL commands as user SYS.

**Rationale:**

As use of the `DBMS_STREAMS_ADM_UTL` package could allow an unauthorized user to run SQL commands as user SYS.

**Audit:**

```
SQL> SELECT GRANTEE, TABLE_NAME FROM DBA_TAB_PRIVS where
TABLE_NAME='DBMS_STREAMS_ADM_UTL' and grantee='PUBLIC';
```

**Remediation:**

```
SQL> Revoke execute on DBMS_STREAMS_ADM_UTL from PUBLIC;
```

**References:**

1. http://www.databasesecurity.com/dbsec/ohh-indirect-privilege-escalation.pdf

## *5.2.7 Limiting public user access to the DBMS_AQADM_SYS package (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The Oracle database `DBMS_AQADM_SYS` package is shipped as undocumented and allows to run SQL commands as user SYS.

**Rationale:**

As use of the `DBMS_AQADM_SYS` package could allow an unauthorized user to run SQL commands as user SYS.

**Audit:**

```
SQL> SELECT GRANTEE, TABLE_NAME FROM DBA_TAB_PRIVS where TABLE_NAME='DBMS_AQADM_SYS'
and grantee='PUBLIC';
```

**Remediation:**

```
SQL> Revoke execute on DBMS_AQADM_SYS from PUBLIC;
```

**References:**

1. http://www.google.de/#hl=de&safe=off&sclient=psy-ab&q=DBMS_STREAMS_ADM_UTL&oq=DBMS_STREAMS_ADM_UTL&gs_l=serp.3..0i10i30.38260.38260.0.38463.1.1.0.0.0.0.105.105.0j1.1.0...0.0...1c.2.1-46wqcQeow&pbx=1&bav=on.2,or.r_gc.r_pw.r_cp.r_qf.&fp=2569366ac9a6532d&bpc

## *5.2.8 Limiting public user access to the DBMS_STREAMS_RPC package (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The Oracle database `DBMS_STREAMS_RPC` package is shipped as undocumented and allows to run SQL commands as user SYS.

**Rationale:**

As use of the `DBMS_STREAMS_RPC` package could allow an unauthorized user to run SQL commands as user SYS.

**Audit:**

```
SQL> SELECT GRANTEE, TABLE_NAME FROM DBA_TAB_PRIVS where TABLE_NAME='DBMS_STREAMS_RPC'
and grantee='PUBLIC';
```

**Remediation:**

```
SQL> Revoke execute on DBMS_STREAMS_RPC from PUBLIC;
```

**References:**

1. http://www.databasesecurity.com/dbsec/ohh-indirect-privilege-escalation.pdf

## *5.2.9 Limiting public user access to the DBMS_AQADM_SYS package (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The Oracle database `DBMS_AQADM_SYS` package is shipped as undocumented and allows to run SQL commands as user SYS.

**Rationale:**

As use of the `DBMS_AQADM_SYS` package could allow any user to run SQL commands as user SYS.

**Audit:**

```
SQL> SELECT GRANTEE, TABLE_NAME FROM DBA_TAB_PRIVS where TABLE_NAME='DBMS_AQADM_SYS'
and grantee='PUBLIC';
```

**Remediation:**

```
SQL> Revoke execute on DBMS_AQADM_SYS from PUBLIC;
```

## *5.2.10 Limiting public user access to the DBMS_PRVTAQIM package (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The Oracle database `DBMS_PRVTAQIM` package is shipped as undocumented and allows to run SQL commands as user SYS.

**Rationale:**

As use of the `DBMS_PRVTAQIM` package could allow an unauthorized user to xxx.

**Audit:**

```
SQL> SELECT GRANTEE, TABLE_NAME FROM DBA_TAB_PRIVS where TABLE_NAME='DBMS_PRVTAQIM'
and grantee='PUBLIC';
```

**Remediation:**

```
SQL> Revoke execute on DBMS_PRVTAQIM from PUBLIC;
```

**References:**

1. http://www.databasesecurity.com/dbsec/ohh-indirect-privilege-escalation.pdf

### *5.2.11 Limiting public user access to the LTADM package (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The Oracle database `LTADM` package is shipped as undocumented and xxx

**Rationale:**

As use of the `LTADM` package could allow an unauthorized user to xxx.

**Audit:**

```
SQL> SELECT GRANTEE, TABLE_NAME FROM DBA_TAB_PRIVS where TABLE_NAME='LTADM' and
grantee='PUBLIC';
```

**Remediation:**

```
SQL> Revoke execute on LTADM from PUBLIC;
```

**References:**

1. http://www.databasesecurity.com/dbsec/ohh-indirect-privilege-escalation.pdf

### *5.2.12 Limiting public user access to the WWV_DBMS_SQL package (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The Oracle database `WWV_DBMS_SQL` package is shipped as undocumented and allows Oracle Application Express to run dynamic SQL statements.

**Rationale:**

As use of the `WWV_DBMS_SQL` package could allow an unauthorized user to run SQL statements as Application Express (APEX) user.

**Audit:**

```
SQL> SELECT GRANTEE, TABLE_NAME FROM DBA_TAB_PRIVS where TABLE_NAME='WWV_DBMS_SQL' and
grantee='PUBLIC';
```

**Remediation:**

```
SQL> Revoke execute on WWV_DBMS_SQL from PUBLIC;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/install.112/e12196/trouble.htm#HTMIG267

## *5.2.13 Limiting public user access to the WWV_EXECUTE_IMMEDIATE package (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The Oracle database `WWV_EXECUTE_IMMEDIATE` package is shipped as undocumented and allows Oracle Application Express to run dynamic SQL statements.

**Rationale:**

As use of the `WWV_EXECUTE_IMMEDIATE` package could allow an unauthorized user to run SQL statements as Application Express (APEX) user.

**Audit:**

```
SQL> SELECT GRANTEE, TABLE_NAME FROM DBA_TAB_PRIVS where
TABLE_NAME='WWV_EXECUTE_IMMEDIATE' and grantee='PUBLIC';
```

**Remediation:**

```
SQL> Revoke execute on WWV_EXECUTE_IMMEDIATE from PUBLIC;
```

**References:**

1. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-1811
2. https://forums.oracle.com/forums/thread.jspa?threadID=953790

## *5.2.14 Limiting public user access to the DBMS_IJOB package (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The Oracle database `DBMS_IJOB` package is shipped as undocumented and allows to run database jobs in the context of another user.

**Rationale:**

As use of the DBMS_IJOB package could allow an attacker to change identities by using a different username to execute a database job.

**Audit:**

```
SQL> SELECT GRANTEE, TABLE_NAME FROM DBA_TAB_PRIVS where TABLE_NAME='DBMS_IJOB' and
grantee='PUBLIC';
```

**Remediation:**

```
SQL> Revoke execute on DBMS_IJOB from PUBLIC;
```

## *5.2.15 Limiting public user access to the DBMS_FILE_TRANSFER package (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The Oracle database `DBMS_FILE_TRANSFER` package allows to transfer files from one database server to another.

**Rationale:**

As use of the DBMS_FILE_TRANSFER package could allow to transfer files from one database server to another.

**Audit:**

```
SQL> SELECT GRANTEE, TABLE_NAME FROM DBA_TAB_PRIVS where
TABLE_NAME='DBMS_FILE_TRANSFER' and GRANTEE='PUBLIC';
```

**Remediation:**

```
SQL> Revoke execute on DBMS_FILE_TRANSFER from PUBLIC;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/appdev.112/e25788/d_ftran.htm#ARPLS095

## *5.3 System Privileges*

Revoke system privileges

### *5.3.1 Limiting users by restricting the SELECT ANY DICTIONARY privilege (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The Oracle database `SELECT ANY DICTIONARY` privilege allows the designated user to access SYS schema objects.

**Rationale:**

The Oracle database `SELECT ANY DICTIONARY` privilege allows the designated user to access SYS schema objects. The Oracle password hashes are part of the SYS schema and can be selected using SELECT ANY DICTIONARY privileges.

**Audit:**

```
SQL> SELECT GRANTEE, PRIVILEGE FROM DBA_SYS_PRIVS where PRIVILEGE='SELECT ANY
DICTIONARY' AND GRANTEE NOT IN
('DBA','DBSNMP','OEM_MONITOR','OLAPSYS','ORACLE_OCM','SYSMAN','WMSYS');
```

**Remediation:**

```
SQL>REVOKE SELECT_ANY_DICTIONARY from <grantee>;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/network.112/e16543/authorization.htm#BABHFJFJ

2. http://docs.oracle.com/cd/E11882_01/server.112/e25513/initparams157.htm#REFRN10133
3. http://arup.blogspot.de/2011/07/difference-between-select-any.html

### *5.3.2 Limiting users by restricting the SELECT ANY TABLE privilege (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The Oracle database `SELECT ANY TABLE` privilege allows the designated user to open any table, except of SYS, to view it.

**Rationale:**

As assignment of the `SELECT ANY TABLE` privilege can allow the unauthorized viewing of sensitive data, this capability should be restricted according to the needs of the organization.

**Audit:**

```
SQL> SELECT GRANTEE, PRIVILEGE FROM DBA_SYS_PRIVS where PRIVILEGE='SELECT_ANY_TABLE';
```

**Remediation:**

```
SQL> REVOKE SELECT_ANY_TABLE from <grantee>;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/server.112/e26088/statements_10002.htm#SQLRF01702

### *5.3.3 Limiting users by restricting the AUDIT SYSTEM privilege (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The Oracle database `AUDIT SYSTEM` privilege allows the change auditing activities on the system.

**Rationale:**

As assignment of the `AUDIT SYSTEM` privilege can allow the unauthorized alteration of system audit activities, disabling the creation of audit trails, this capability should be restricted according to the needs of the organization.

**Audit:**

```
SQL> SELECT GRANTEE, PRIVILEGE FROM DBA_SYS_PRIVS where
PRIVILEGE='AUDIT SYSTEM' AND GRANTEE NOT IN
('DBA','DATAPUMP_IMP_FULL_DATABASE','IMP_FULL_DATABASE','SYS');
```

**Remediation:**

```
SQL> REVOKE AUDIT SYSTEM from <grantee>;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/server.112/e26088/statements_4007.htm#SQLRF01107

## *5.3.4 Limiting users by restricting the EXEMPT ACCESS POLICY (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The Oracle database `EXEMPT ACCESS POLICY` keyword provides the user the capability to access all the table rows regardless of row-level security lockouts.

**Rationale:**

As assignment of the `EXEMPT ACCESS POLICY` privilege can allow an unauthorized user to potentially access/change confidential data, this capability should be restricted according to the needs of the organization.

**Audit:**

```
SQL> SELECT * FROM DBA_SYS_PRIVS WHERE PRIVILEGE='EXEMPT ACCESS POLICY';
```

**Remediation:**

```
SQL> REVOKE EXEMPT ACCESS POLICY FROM <grantee>;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/network.112/e16543/auditing.htm#DBSEG419
2. http://docs.oracle.com/cd/E11882_01/network.112/e16543/vpd.htm#DBSEG309

## *5.3.5 Limiting users by restricting the BECOME USER privilege (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The Oracle database `BECOME USER` privilege allows the designated user to inherit the rights of another user.

**Rationale:**

As assignment of the `BECOME USER` privilege can allow the unauthorized use of another user's privileges, this capability should be restricted according to the needs of the organization.

**Audit:**

```
SQL> SELECT GRANTEE, PRIVILEGE FROM DBA_SYS_PRIVS where PRIVILEGE='BECOME USER' AND
GRANTEE NOT IN ('DBA','SYS','IMP_FULL_DATABASE');
```

**Remediation:**

```
SQL> REVOKE BECOME USER from <grantee>;
```

**References:**

1. http://docs.oracle.com/cd/B19306_01/network.102/b14266/cfgaudit.htm

## *5.3.6 Limiting users by restricting the CREATE PROCEDURE privilege (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The Oracle database `CREATE PROCEDURE` privilege allows the designated user to create a stored procedure that will fire when given the correct command sequence.

**Rationale:**

As assignment of the `CREATE PROCEDURE` privilege can lead to severe problems in unauthorized hands, such as rogue procedures facilitating data theft or Denial-of-Service by corrupting data tables, this capability should be restricted according to the needs of the organization.

**Audit:**

```
SQL> SELECT GRANTEE, PRIVILEGE FROM DBA_SYS_PRIVS where PRIVILEGE='CREATE PROCEDURE'
and GRANTEE NOT IN (
'DBA','DBSNMP','MDSYS','OLAPSYS','OWB$CLIENT','OWBSYS','RECOVERY_CATALOG_OWNER','SPATI
AL_CSW_ADMIN_USR','SPATIAL_WFS_ADMIN_USR','SYS','APEX_030200','APEX_040000','APEX_0401
00','APEX_040200');
```

**Remediation:**

```
REVOKE CREATE_PROCEDURE from <grantee>;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/server.112/e26088/statements_6009.htm#SQLRF01309

## *5.3.7 Limiting users by restricting the ALTER SYSTEM privilege (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The Oracle database `ALTER SYSTEM` privilege allows the designated user to dynamically alter the instance's running operations.

**Rationale:**

As assignment of the `ALTER SYSTEM` privilege can lead to severe problems, such as the instance's session being killed or the stopping of redo log recording, which would make transactions unrecoverable, this capability should be severely restricted according to the needs of the organization.

**Audit:**

```
SQL> SELECT GRANTEE, PRIVILEGE FROM DBA_SYS_PRIVS WHERE PRIVILEGE='ALTER SYSTEM' and
GRANTEE NOT IN
('SYS','SYSTEM','APEX_030200','APEX_040000','APEX_040100','APEX_040200');
```

**Remediation:**

```
SQL> REVOKE ALTER SYSTEM from <grantee>;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/server.112/e26088/statements_2014.htm#SQLRF00902

## *5.3.8 Limiting users by restricting the CREATE ANY LIBRARY privilege (Not Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The Oracle database `CREATE (ANY) LIBRARY` privilege allows the designated user to create objects that are associated to the shared libraries.

**Rationale:**

As assignment of the `CREATE (ANY) LIBRARY` privilege can allow the creation of numerous library-associated objects and potentially corrupt the libraries' integrity, this capability should be restricted according to the needs of the organization.

**Audit:**

```
SQL> SELECT * FROM DBA_SYS_PRIVS where (PRIVILEGE='CREATE LIBRARY'
or PRIVILEGE='CREATE ANY LIBRARY') AND GRANTEE NOT IN ('SYS','SYSTEM','DBA');
```

**Remediation:**

```
SQL> REVOKE CREATE LIBRARY FROM <grantee>;
SQL> REVOKE CREATE ANY LIBRARY FROM <grantee>;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/server.112/e26088/statements_6001.htm#SQLRF01301
2. http://docs.oracle.com/cd/E18283_01/server.112/e17120/manproc007.htm

### *5.3.9 Limiting users by restricting GRANT ANY OBJECT PRIVILEGE privilege (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The Oracle database `GRANT ANY OBJECT PRIVILEGE` keyword provides the grantee the capability to grant access to any single or multiple combinations of objects to any grantee in the catalog of the database.

**Rationale:**

As authorization to use the `GRANT ANY OBJECT PRIVILEGE` capability can allow an unauthorized user to potentially access/change confidential data or damage the data catalog due to potential complete instance access, this capability should be restricted according to the needs of the organization.

**Audit:**

```
SQL> SELECT * FROM DBA_SYS_PRIVS WHERE PRIVILEGE='GRANT ANY OBJECT PRIVILEGE' AND
GRANTEE NOT IN ('DBA','SYS','IMP_FULL_DATABASE','DATAPUMP_IMP_FULL_DATABASE');
```

**Remediation:**

```
SQL> REVOKE GRANT ANY OBJECT PRIVILEGE FROM <grantee>;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/network.112/e16543/authorization.htm#DBSEG99914

### *5.3.10 Limiting users by restricting GRANT ANY ROLE privilege (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The Oracle database `GRANT ANY ROLE` keyword provides the grantee the capability to grant any single role to any grantee in the catalog of the database.

**Rationale:**

As authorization to use the GRANT ANY ROLE capability can allow an unauthorized user to potentially access/change confidential data or damage the data catalog due to potential complete instance access, this capability should be restricted according to the needs of the organization.

**Audit:**

```
SQL> SELECT * FROM DBA_SYS_PRIVS WHERE PRIVILEGE='GRANT ANY ROLE' AND GRANTEE NOT IN
('DBA','SYS','DATAPUMP_IMP_FULL_DATABASE','IMP_FULL_DATABASE','SPATIAL_WFS_ADMIN_USR',
'SPATIAL_CSW_ADMIN_USR');
```

**Remediation:**

```
SQL> REVOKE GRANT ANY ROLE FROM <grantee>;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/network.112/e16543/authorization.htm#DBSEG99903

## *5.3.11 Limiting users by restricting GRANT ANY PRIVILEGE privilege (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The Oracle database GRANT ANY PRIVILEGE keyword provides the grantee the capability to grant any single privilege to any item in the catalog of the database.

**Rationale:**

As authorization to use the GRANT ANY PRIVILEGE capability can allow an unauthorized user to potentially access/change confidential data or damage the data catalog due to potential complete instance access, this capability should be restricted according to the needs of the organization.

**Audit:**

```
SQL> SELECT * FROM DBA_SYS_PRIVS WHERE PRIVILEGE='GRANT ANY PRIVILEGE' AND GRANTEE NOT
IN ('DBA','SYS','IMP_FULL_DATABASE','DATAPUMP_IMP_FULL_DATABASE');
```

**Remediation:**

```
SQL> REVOKE GRANT ANY PRIVILEGE FROM <grantee>;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/network.112/e16543/authorization.htm#DBSEG99876

## 5.4 Role Privileges

Revoke powerful roles

### 5.4.1 Limiting user authorizations for the DELETE_CATALOG_ROLE (Not Scored)

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The Oracle database `DELETE_CATALOG_ROLE` provides `DELETE` privileges for the records in the system's audit table (`AUD$`).

**Rationale:**

As permitting unauthorized access to the `DELETE_CATALOG_ROLE` can allow the destruction of audit records vital to the forensic investigation of unauthorized activities, this capability should be restricted according to the needs of the organization.

**Audit:**

```
SQL> SELECT *  FROM DBA_ROLE_PRIVS where granted_role='DELETE_CATALOG_ROLE' and
grantee not in ('DBA','SYS');
```

**Remediation:**

```
SQL> REVOKE DELETE_CATALOG_ROLE FROM <grantee>;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/network.112/e16543/authorization.htm#DBSEG99873
2. http://docs.oracle.com/cd/E11882_01/network.112/e16543/authorization.htm#DBSEG4414

## *5.4.2 Limiting user authorizations for the SELECT_CATALOG_ROLE (Not Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The Oracle database `SELECT_CATALOG_ROLE` provides `SELECT` privileges on all data dictionary views held in the `SYS` schema.

**Rationale:**

As permitting unauthorized access to the `SELECT_CATALOG_ROLE` can allow the disclosure of all dictionary data, this capability should be restricted according to the needs of the organization.

**Audit:**

```
SQL> SELECT *  FROM DBA_ROLE_PRIVS where granted_role='SELECT_CATALOG_ROLE' and
grantee not in ('DBA','SYS','IMP_FULL_DATABASE','EXP_FULL_DATABASE','OEM_MONITOR');
```

**Remediation:**

```
SQL> REVOKE SELECT_CATALOG_ROLE FROM <grantee>;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/network.112/e16543/authorization.htm#DBSEG99873
2. http://docs.oracle.com/cd/E11882_01/network.112/e16543/authorization.htm#DBSEG4414

## *5.4.3 Limiting user authorizations for the EXECUTE_CATALOG role (Not Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The Oracle database `EXECUTE_CATALOG_ROLE` provides `EXECUTE` privileges for a number of packages and procedures in the data dictionary in the `SYS` schema.

**Rationale:**

As permitting unauthorized access to the `EXECUTE_CATALOG_ROLE` can allow the disruption of operations by initialization of rogue procedures, this capability should be restricted according to the needs of the organization.

**Audit:**

```
SQL> SELECT *  FROM DBA_ROLE_PRIVS where granted_role='EXECUTE_CATALOG_ROLE' and
grantee not in ('DBA','SYS','IMP_FULL_DATABASE','EXP_FULL_DATABASE');
```

**Remediation:**

```
SQL> REVOKE EXECUTE_CATALOG_ROLE FROM <grantee>;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/network.112/e16543/authorization.htm#DBSEG99873
2. http://docs.oracle.com/cd/E11882_01/network.112/e16543/authorization.htm#DBSEG4414

### *5.4.4 Limiting users by restricting the DBA role (Not Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The Oracle database DBA role is the default database administrator role provided for the allocation of administrative privileges.

**Rationale:**

As assignment of the `DBA` role to an ordinary user can provide a great number of unnecessary privileges to that user and opens the door to data breaches, integrity violations, and Denial-of-Service conditions, application of this role should be restricted according to the needs of the organization.

**Audit:**

```
SQL> SELECT GRANTEE, GRANTED_ROLE FROM DBA_ROLE_PRIVS WHERE GRANTED_ROLE='DBA' AND
GRANTEE NOT IN ('SYS','SYSTEM');
```

**Remediation:**

```
SQL> REVOKE DBA from <grantee>;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/network.112/e16543/authorization.htm#DBSEG4414

## 5.5 Table and View privileges

Revoke table and view privileges

### 5.5.1 Limiting authorizations for the SYS.AUD$ table (Scored)

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The Oracle database `SYS.AUD$` table contains all the audit records for the database of the non-Data Manipulation Language (DML) events, such as `ALTER`, `DROP`, `CREATE`, and so forth. (DML changes need trigger-based audit events to record data alterations.)

**Rationale:**

As permitting non-privileged users the authorization to manipulate the `SYS_AUD$` table can allow distortion of the audit records, hiding unauthorized activities, this capability should be restricted according to the needs of the organization.

**Audit:**

```
SQL> SELECT GRANTEE, PRIVILEGE FROM DBA_TAB_PRIVS WHERE TABLE_NAME='AUD$' and grantee
not in ('DELETE_CATALOG_ROLE');
```

**Remediation:**

```
SQL> REVOKE ALL ON AUD$ FROM <grantee>;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/network.112/e16543/auditing.htm#CEGDGIAF

### 5.5.2 Limiting authorizations for the SYS.USER_HISTORY$ table (Scored)

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The Oracle database `SYS.USER_HISTORY$` table contains all the audit records for the user's password change history. (This table gets updated by password changes if the user has an assigned profile that has password reuse limit set, e.g., `PASSWORD_REUSE_TIME` set to other than `UNLIMITED`.)

**Rationale:**

As permitting non-privileged users the authorization to manipulate the records in the `SYS.USER_HISTORY$` table can allow distortion of the audit trail, potentially hiding unauthorized data confidentiality attacks or integrity changes, this capability should be restricted according to the needs of the organization.

**Audit:**

```
SQL> SELECT GRANTEE, PRIVILEGE FROM DBA_TAB_PRIVS WHERE TABLE_NAME='USER_HISTORY$';
```

**Remediation:**

```
SQL> REVOKE ALL ON USER_HISTORY$ FROM <username>;
```

**References:**

1. http://marcel.vandewaters.nl/oracle/database-oracle/password-history-reusing-a-password

## *5.5.3 Limiting authorizations for the SYS.LINK$ table (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The Oracle database `SYS.LINK$` table contains all the user's password information and data table link information.

**Rationale:**

As permitting non-privileged users to manipulate or view the `SYS.LINK$` table can allow capture of password information and/or corrupt the primary database linkages, this capability should be restricted according to the needs of the organization.

**Audit:**

```
SQL> SELECT GRANTEE, PRIVILEGE FROM DBA_TAB_PRIVS WHERE TABLE_NAME='LINK$';
```

**Remediation:**

```
SQL> REVOKE ALL ON LINK$ FROM <grantee>;
```

## *5.5.4 Limiting authorizations for the SYS.USER$ table (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The Oracle database `SYS.USER$` table contains the users' hashed password information.

**Rationale:**

As permitting non-privileged users the authorization to open the `SYS.USER$` table can allow the capture of password hashes for the later application of password cracking algorithms to breach confidentiality, this capability should be restricted according to the needs of the organization.

**Audit:**

```
SQL> SELECT GRANTEE, PRIVILEGE FROM DBA_TAB_PRIVS WHERE TABLE_NAME='USER$' and grantee
not in ('CTXSYS','XDB','APEX_030200', 'APEX_040000','APEX_040100','APEX_040200');
```

**Remediation:**

```
SQL> REVOKE ALL ON SYS.USER$ FROM <username>;
```

**References:**

1. http://dba.stackexchange.com/questions/17513/what-do-the-columns-in-sys-user-represent

## *5.5.5 Limiting user authorizations for the DBA_% views (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The Oracle database DBA_ views show all information which is relevant to administrative accounts.

**Rationale:**

As permitting users the authorization to manipulate the DBA_ views can expose sensitive data.

**Audit:**

```
SQL> SELECT * FROM dba_tab_privs WHERE TABLE_NAME LIKE 'DBA_%' and grantee not in
('APEX_030200','APPQOSSYS','AQ_ADMINISTRATOR_ROLE','CTXSYS','EXFSYS','MDSYS','OLAP_XS_
ADMIN','OLAPSYS','ORDSYS','OWB$CLIENT','OWBSYS','SELECT_CATALOG_ROLE','WM_ADMIN_ROLE',
'WMSYS','XDBADMIN') and table_name not in
('DBA_SDO_MAPS','DBA_SDO_STYLES','DBA_SDO_THEMES') ;
```

**Remediation:**

```
SQL> REVOKE ALL ON DBA_<view_name> FROM <Non-DBA/SYS grantee>;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/server.112/e25789/datadict.htm#autoId2

## *5.5.6 Limiting user authorizations for the $V_ views (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The Oracle database $V_ views provide a continually updated look at internal database statistics, with 467 possible views in Oracle 11gr2, including all SQL statements running: The V$ views are sometimes referred to as "Dynamic performance views or tables" for this reason.

**Rationale:**

As permitting users the authorization to read the $V_ views can expose sensitive database operations that hold information that can facilitate system attacks, this capability should be restricted according to the needs of the organization.

**Audit:**

```
SQL> SELECT GRANTEE,PRIVILEGE, TABLE_NAME FROM DBA_TAB_PRIVS WHERE TABLE_NAME LIKE
'V$_%' AND GRANTEE NOT IN ('DBA') and table_name not in ('V$OBJECT_USAGE');
```

**Remediation:**

```
SQL> REVOKE ALL ON TABLENAME LIKE 'V$_' FROM <Non-DBA grantee>;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/server.112/e25789/datadict.htm#CNCPT1220

## *5.5.7 Limiting authorizations for the SCHEDULER$_CREDENTIAL table (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The Oracle database `SCHEDULER$_CREDENTIAL` table contains the database scheduler credential information.

**Rationale:**

As permitting non-privileged users the authorization to open the `SYS.SCHEDULER$_CREDENTIAL` table.

**Audit:**

```
SQL> SELECT GRANTEE, PRIVILEGE FROM DBA_TAB_PRIVS WHERE
TABLE_NAME='SCHEDULER$_CREDENTIAL';
```

**Remediation:**

```
SQL> REVOKE ALL ON SYS.SCHEDULER$_CREDENTIAL FROM <username>;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/appdev.112/e25788/d_sched.htm#ARPLS72292
2. http://berxblog.blogspot.de/2012/02/restore-dbmsschedulercreatecredential.html

## *5.5.8 Drop table sys.user$mig (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

The table sys.user$mig is created during the migration and contains the Oracle password hashes before the migration starts.

**Rationale:**

The table sys.user$mig is not deleted after the migration. An attacker could access this table containing the Oracle password hashes.

**Audit:**

```
select  owner,table_name from all_tables where owner='SYS' and table_name='USER$MIG';
```

**Remediation:**

```
drop table sys.user$mig;
```

## *5.6 Other Privileges*

Revoke other privileges

### *5.6.1 Access to ACL privileges (Not Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

Review access to Oracle network ACLs.

**Rationale:**

Oracle network ACLs control who can connect to which port/ip.

**Audit:**

**Remediation:**

Revoke unneeded privileges.

## *5.7 Limiting user authorizations for the SYSTEM tablespace (Scored)*

**Profile Applicability:**

- Level 2 - 11.2 on Oracle Linux 5

**Description:**

The `SYSTEM` tablespace contains all the basic system objects for the database, such as the data dictionary tables.

**Rationale:**

As allowing any user other than SYS to use the SYSTEM tablespace can potentially allow disk resource exhaustion (Denial-of-Service) conditions to occur or data dictionary corruption, requiring a tablespace reconstruction from backups, authorization to use the SYSTEM tablespace should limited according to the needs of the organization.

**Audit:**

```
SQL> SELECT USERNAME, DEFAULT_TABLESPACE FROM DBA_USERS WHERE
DEFAULT_TABLESPACE='SYSTEM' and username not in ('SYSTEM','SYS','MGMT_VIEW','OUTLN');
```

**Remediation:**

```
SQL> ALTER user DEFAULT_TABLESPACE tablename;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/server.112/e25494/create004.htm#ADMIN11092

## *5.8 Limiting basic user privileges to restrict the ANY keyword (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The Oracle database `ANY` keyword provides the user the capability to alter any item in the catalog of the database.

**Rationale:**

As authorization to use the ANY expansion of a privilege can allow an unauthorized user to potentially change confidential data or damage the data catalog, this capability should be restricted according to the needs of the organization.

**Audit:**

```
SQL> SELECT * FROM DBA_SYS_PRIVS WHERE PRIVILEGE LIKE '%ANY%' AND GRANTEE NOT IN
('AQ_ADMINISTRATOR_ROLE','DBA',
'DBSNMP','EXFSYS','EXP_FULL_DATABASE','IMP_FULL_DATABASE','DATAPUMP_IMP_FULL_DATABASE'
,'JAVADEBUGPRIV','MDSYS','OEM_MONITOR','OLAPSYS','OLAP_DBA','ORACLE_OCM','OWB$CLIENT',
'OWBSYS','SCHEDULER_ADMIN','SPATIAL_CSW_ADMIN_USR','SPATIAL_WFS_ADMIN_USR','SYS','SYSM
AN','SYSTEM','WMSYS','APEX_030200','APEX_040000','APEX_040100','APEX_040200');
```

**Remediation:**

```
REVOKE ALL ON '<ANY Privilege>' FROM <grantee>;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/network.112/e16543/authorization.htm#DBSEG99877

## *5.9 Limiting users by restricting the WITH_ADMIN privilege (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The Oracle database WITH_ADMIN privilege allows the designated user to grant another user the same privileges.

**Rationale:**

As assignment of the WITH_ADMIN privilege can allow the granting of a restricted privilege to an unauthorized user, this capability should be restricted according to the needs of the organization.

**Audit:**

```
SQL> SELECT * FROM DBA_SYS_PRIVS WHERE ADMIN_OPTION='YES' and GRANTEE not in
('AQ_ADMINISTRATOR_ROLE','DBA','OWBSYS', 'SCHEDULER_ADMIN','SYS','SYSTEM','WMSYS');
```

**Remediation:**

```
SQL> REVOKE <privilege> FROM <grantee>;
```

## *5.10 Limit direct privileges for proxy user (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

Do not grant privileges directly to proxy users

**Rationale:**

A proxy user should only have the ability to connect to the database.

**Audit:**

SQL> select * from dba_role_privs where grantee in (select proxy from dba_proxies) and granted_role not in ('CONNECT');

SQL> select * from dba_sys_privs where grantee in (select proxy from dba_proxies) and privilege not in ('CREATE SESSION');

SQL> select * from dba_tab_privs where grantee in (select proxy from dba_proxies);

**Remediation:**

SQL> revoke privilege from <proxy_user>;

## *5.11 Revoke execute any procedure from user OUTLN (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

Remove unneeded privileges from OUTLN

**Rationale:**

Migrated OUTLN users have more privileges than required.

**Audit:**

```
SQL> SELECT * FROM DBA_SYS_PRIVS where privilege='EXECUTE ANY PROCEDURE' and
grantee='OUTLN';
```

**Remediation:**

```
SQL> revoke EXECUTE ANY PROCEDURE from OUTLN;
```

### *5.12 Revoke execute any procedure from user DBSNMP (Scored)*

**Profile Applicability:**

- Level 1 - 11.x on any platform

**Description:**

Remove unneeded privileges from DBSNMP

**Rationale:**

Migrated DBSNMP users have more privileges than required.

**Audit:**

```
SQL> SELECT * FROM DBA_SYS_PRIVS where privilege='EXECUTE ANY PROCEDURE' and
grantee='DBSNMP';
```

**Remediation:**

```
SQL> revoke EXECUTE ANY PROCEDURE from DBSNMP;
```

## *6 Audit/Logging Policies and Procedures*

The ability to audit system logs, to determine the result of user actions that have potentially resulted in the loss or violations of availability, confidentiality, and/or integrity is among the most important of all database security features. Decisions must be made regarding the breadth/depth of the logging activity, as greater detail produces larger log files. Measures must also be taken to protect the log files themselves, for these may be targeted for alteration or destruction to hide unauthorized activity. There are numerous command sequences for AUDIT, some of which are applicable to most database objects,

such as CREATE, ALTER, DROP, while others are limited to a few database objects, such as GRANT, TRUNCATE, SET, SYSTEM AUDIT, and SYSTEM GRANT. The commands that apply to larger numbers of objects will be addressed object by object after the primary connection commands are dealt with.

## *6.1 Audit all CREATE SESSION (logon/logoff) activities (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The logging of all `CREATE SESSION` activities, the logon/logoff equivalent to remote database access , will provide an audit trail of user connection; this is the minimum privilege required to request access to run operations against the database.

**Rationale:**

As the logging of user connections to the database via logon/logoff activity can provide forensic evidence of the initiation of a pattern of unauthorized activities, this capability should be set according to the needs of the organization.

**Audit:**

```
SQL> SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE
PRIVILEGE='CREATE SESSION';
```

**Remediation:**

```
SQL> AUDIT CREATE SESSION;
```

## *6.2 Audit all CREATE USER object activities/requests (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The `USER` object for the Oracle database is a specification of an object which is an account through which either a human or an application can connect to, via a JDBC or log into, via a CLI, and interact with the database instance according to the roles and privileges allotted to account.

**Rationale:**

As the logging of user activities involving the creation, alteration, or dropping of a USER can provide forensic evidence about a pattern of suspect/unauthorized activities, the audit capability should be set according to the needs of the organization.

**Audit:**

```
SQL> select USER_NAME, SUCCESS, FAILURE from DBA_STMT_AUDIT_OPTS where AUDIT_OPTION in
('CREATE USER','USER');
```

**Remediation:**

```
SQL> AUDIT CREATE USER;
```

## *6.3 Audit all ALTER USER object activities/requests (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The `USER` object for the Oracle database is a specification of an object which is an account through which either a human or an application can connect to, via a JDBC or log into, via a CLI, and interact with the database instance according to the roles and privileges allotted to account.

**Rationale:**

As the logging of user activities involving the creation, alteration, or dropping of a USER can provide forensic evidence about a pattern of suspect/unauthorized activities, the audit capability should be set according to the needs of the organization.

**Audit:**

```
SQL> select USER_NAME, SUCCESS, FAILURE from DBA_STMT_AUDIT_OPTS where AUDIT_OPTION in
('ALTER USER', 'USER');
```

**Remediation:**

```
SQL> AUDIT ALTER USER;
```

## *6.4 Audit all DROP USER object activities/requests (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The `USER` object for the Oracle database is a specification of an object which is an account through which either a human or an application can connect to, via a JDBC or log into, via a CLI, and interact with the database instance according to the roles and privileges allotted to account.

**Rationale:**

As the logging of user activities involving the creation, alteration, or dropping of a USER can provide forensic evidence about a pattern of suspect/unauthorized activities, the audit capability should be set according to the needs of the organization.

**Audit:**

```
SQL> select USER_NAME, SUCCESS, FAILURE from DBA_STMT_AUDIT_OPTS where AUDIT_OPTION in
('DROP USER','USER');
```

**Remediation:**

```
SQL> AUDIT DROP USER;
```

## *6.5 Audit all user ROLE activities/requests (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The ROLE object allows for the creation of a set of privileges that can be granted to users/ other roles, both for application connection and database administrative purposes.

**Rationale:**

As the logging of user activities involving the creation, alteration, setting or dropping of a ROLE can provide forensic evidence about a pattern of suspect/unauthorized activities, the audit capability should be set according to the needs of the organization.

**Audit:**

```
SQL> select USER_NAME, SUCCESS, FAILURE from DBA_STMT_AUDIT_OPTS where AUDIT_OPTION in
('ROLE');
```

**Remediation:**

```
SQL> AUDIT ROLE;
```

## *6.6 Audit all user GRANT ROLE activities/requests (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The system grant allows to audit all type of grants and revokes.

**Rationale:**

As the logging of all grant and revokes (roles and system privileges) can provide forensic evidence about a pattern of suspect/unauthorized activities, the audit capability should be set according to the needs of the organization.

**Audit:**

```
SQL> select USER_NAME, SUCCESS, FAILURE from DBA_STMT_AUDIT_OPTS where
AUDIT_OPTION='SYSTEM GRANT';
```

**Remediation:**

```
SQL> AUDIT SYSTEM GRANT;
```

## 6.7 Audit all user CREATE PROFILE activities/requests (Scored)

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The `PROFILE` object allows for the creation of a set of database resource limits that can be assigned to a user, so that that user cannot exceed those resource limitations.

**Rationale:**

As the logging of user activities involving the creation, alteration, or dropping of a `PROFILE` can provide forensic evidence about a pattern of unauthorized activities, the audit capability should be set according to the needs of the organization.

**Audit:**

```
SQL> select USER_NAME, SUCCESS, FAILURE from DBA_STMT_AUDIT_OPTS where AUDIT_OPTION in
('CREATE PROFILE','PROFILE');
```

**Remediation:**

```
SQL> AUDIT CREATE PROFILE;
```

## 6.8 Audit all user ALTER PROFILE activities/requests (Scored)

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The `PROFILE` object allows for the creation of a set of database resource limits that can be assigned to a user, so that that user cannot exceed those resource limitations.

**Rationale:**

As the logging of user activities involving the creation, alteration, or dropping of a `PROFILE` can provide forensic evidence about a pattern of unauthorized activities, the audit capability should be set according to the needs of the organization.

**Audit:**

```
SQL> select USER_NAME, SUCCESS, FAILURE from DBA_STMT_AUDIT_OPTS where AUDIT_OPTION in
('ALTER PROFILE','PROFILE');
```

**Remediation:**

```
SQL> AUDIT ALTER PROFILE;
```

## *6.9 Audit all user DROP PROFILE activities/requests (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The `PROFILE` object allows for the creation of a set of database resource limits that can be assigned to a user, so that that user cannot exceed those resource limitations.

**Rationale:**

As the logging of user activities involving the creation, alteration, or dropping of a `PROFILE` can provide forensic evidence about a pattern of unauthorized activities, the audit capability should be set according to the needs of the organization.

**Audit:**

```
SQL> USER_NAME, SUCCESS, FAILURE from DBA_STMT_AUDIT_OPTS where AUDIT_OPTION in ('DROP
PROFILE','PROFILE');
```

**Remediation:**

```
SQL> AUDIT DROP PROFILE;
```

## *6.10 Audit all DATABASE LINK activities/requests (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

All activities on database links should be audited.

**Rationale:**

As the logging of user activities involving the creation or dropping of a `DATABASE LINK` can provide forensic evidence about a pattern of unauthorized activities, the audit capability should be set according to the needs of the organization.

**Audit:**

```
SQL> select * from dba_stmt_audit_opts where audit_option='DATABASE LINK';
```

**Remediation:**

```
SQL> AUDIT DATABASE LINK;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/server.112/e26088/statements_4007.htm#SQLRF01107

## *6.11 Audit all PUBLIC DATABASE LINK activities/requests (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The `PUBLIC DATABASE LINK` object allows for the creation of a public link for an application-based "user" to access the database for connections/session creation .

**Rationale:**

As the logging of user activities involving the creation, alteration, or dropping of a `PUBLIC DATABASE LINK` can provide forensic evidence about a pattern of unauthorized activities, the audit capability should be set according to the needs of the organization.

**Audit:**

```
select * from dba_stmt_audit_opts where audit_option='PUBLIC DATABASE LINK';
```

**Remediation:**

```
SQL> audit public database link;
```

## *6.12 Audit all PUBLIC SYNONYM activities/requests (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The `PUBLIC SYNONYM` object allows for the creation of an alternate description of an object and public synonyms are accessible by all users that have the appropriate privileges to the underlying object.

**Rationale:**

As the logging of user activities involving the creation or dropping of a `PUBLIC SYNONYM` can provide forensic evidence about a pattern of unauthorized activities, the audit capability should be set according to the needs of the organization.

**Audit:**

```
SQL> select * from dba_stmt_audit_opts where audit_option='PUBLIC SYNONYM';
```

**Remediation:**

```
SQL> AUDIT PUBLIC SYNONYM;
```

## *6.13 Audit all user SYNONYM activities/requests (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The SYNONYM operation allows for the creation of a an alternative name for a database object such as a Java class schema object, materialized view, operator, package, procedure, sequence, stored function, table, view, user-defined object type, even another synonym; this synonym puts a dependency on its target and is rendered invalid if the target object is changed/dropped.

**Rationale:**

As the logging of user activities involving the creation or dropping of a SYNONYM can provide forensic evidence about a pattern of suspect/unauthorized activities, the audit capability should be set according to the needs of the organization.

**Audit:**

```
SQL> select * from dba_stmt_audit_opts where audit_option='SYNONYM';
```

**Remediation:**

```
SQL> AUDIT SYNONYM;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/server.112/e26088/statements_4007.htm#SQLRF01107

## *6.14 Audit all grants and revokes of privileges on directories (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The DIRECTORY object allows for the creation of a directory object that specifies an alias for a directory on the server file system, where the external binary file LOBs (BFILEs)/ table data are located.

**Rationale:**

As the logging of user activities involving the creation or dropping of a DIRECTORY can provide forensic evidence about a pattern of unauthorized activities, the audit capability should be set according to the needs of the organization.

**Audit:**

```
SQL> select * from dba_stmt_audit_opts where audit_option='GRANT DIRECTORY';
```

**Remediation:**

```
SQL> AUDIT GRANT DIRECTORY;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/server.112/e26088/statements_4007.htm#SQLRF01107

## *6.15 Audit all user SELECT ANY DICTIONARY activities/requests (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The `SELECT ANY DICTIONARY` capability allows the user to view the definitions of all schema objects in the database.

**Rationale:**

As the logging of user activities involving the capability to access the description of all schema objects in the database can provide forensic evidence about a pattern of unauthorized activities, the audit capability should be set according to the needs of the organization.

**Audit:**

```
SQL> SELECT * FROM DBA_STMT_AUDIT_OPTS WHERE AUDIT_OPTION='SELECT ANY DICTIONARY';
```

**Remediation:**

```
SQL> AUDIT SELECT ANY DICTIONARY;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/server.112/e26088/statements_4007.htm#SQLRF01107

## *6.16 Audit all user GRANT ANY OBJECT PRIVILEGE activities/requests (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The `GRANT ANY OBJECT PRIVILEGE` allows for the granting of any OBJECT privilege, which includes directories, flashbacks, mining models, etc.

**Rationale:**

As the logging of privilege grants that can lead to the creation, alteration, or dropping of tables, users and other critical system components is critical to forensic investigations, this audit capability should be set according to the needs of the organization.

**Audit:**

```
SQL> select * from DBA_PRIV_AUDIT_OPTS where privilege='GRANT ANY OBJECT PRIVILEGE';
```

**Remediation:**

```
SQL> AUDIT GRANT ANY OBJECT PRIVILEGE;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/server.112/e26088/statements_4007.htm#SQLRF01107

## *6.17 Audit all user GRANT ANY PRIVILEGE activities/requests (Not Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The `GRANT ANY PRIVILEGE` allows for the granting of any privilege, including those at the DBA level, so that the entire range of DBA capabilities is open to to the grantee.

**Rationale:**

As the logging of privilege grants that can lead to the creation, alteration, or dropping of tables, users and other critical system components, this audit capability should be set according to the needs of the organization.

**Audit:**

```
SQL> select * from DBA_PRIV_AUDIT_OPTS where privilege='GRANT ANY PRIVILEGE';
```

**Remediation:**

```
SQL> AUDIT GRANT ANY PRIVILEGE;
```

**References:**

1. http://docs.oracle.com/cd/E11882_01/server.112/e26088/statements_4007.htm#SQLRF01107

## *6.18 Audit all user CREATE PROCEDURE activities/requests (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The `AUDIT PROCEDURE` audit command allows for the tracking a number of user activities, including the:

`FUNCTION`, the creation/dropping of a standalone stored function or a "Call specification" that is like a procedure, except functions return values to its original environment and can be in Java or other 3GL languages;

`LIBRARY`, which is the creation/dropping of a schema object associated with an operating-system shared library;

`PACKAGE`, which is the creation/dropping of a locally stored collection of related procedures, functions, and potentially other program objects stored together; and

`PROCEDURE`, which is the creation/dropping of a procedure--this is a subprogram that performs a specified action that is stored in the database.

**Rationale:**

As the logging of user activities involving the creation, alteration, or dropping of a PROCEDURE and its related activities can provide forensic evidence about a pattern of unauthorized activities, this audit capability should be set according to the needs of the organization.

**Audit:**

```
SQL> SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE
PRIVILEGE='CREATE PROCEDURE';
```

**Remediation:**

```
SQL> AUDIT CREATE PROCEDURE;
```

## *6.19 Audit all user CREATE ANY PROCEDURE activities/requests (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The `AUDIT CREATE ANY PROCEDURE` command is auditing the creation of procedures in other schema.

**Rationale:**

As the logging of user activities involving the creation, alteration, or dropping of a PROCEDURE and its related activities can provide forensic evidence about a pattern of unauthorized activities, this audit capability should be set according to the needs of the organization.

**Audit:**

```
SQL> select * from dba_stmt_audit_opts where audit_option = 'CREATE ANY PROCEDURE';
```

**Remediation:**

```
SQL> AUDIT CREATE ANY PROCEDURE;
```

## *6.20 Audit all user ALTER ANY PROCEDURE activities/requests (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The `AUDIT ALTER ANY PROCEDURE` command is auditing the alteration of procedures in other schema.

**Rationale:**

As the logging of user activities involving the creation, alteration, or dropping of a PROCEDURE and its related activities can provide forensic evidence about a pattern of unauthorized activities, this audit capability should be set according to the needs of the organization.

**Audit:**

```
SQL> select * from dba_stmt_audit_opts where audit_option = 'ALTER ANY PROCEDURE';
```

**Remediation:**

```
SQL> AUDIT ALTER ANY PROCEDURE;
```

## *6.21 Audit all user DROP ANY PROCEDURE activities/requests (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The `AUDIT DROP ANY PROCEDURE` command is auditing the creation of procedures in other schema.

**Rationale:**

Dropping procedures of another user could be part of an privilege escalation exploit and should be audited.

**Audit:**

```
SQL> select * from dba_stmt_audit_opts where audit_option = 'DROP ANY PROCEDURE';
```

**Remediation:**

```
SQL> AUDIT DROP ANY PROCEDURE;
```

## *6.22 Audit all user CREATE ANY LIBRARY activities/requests (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The AUDIT CREATE ANY LIBRARY command is auditing the creation of libraries.

**Rationale:**

As the logging of user activities involving the creation, alteration, or dropping of a PROCEDURE and its related activities can provide forensic evidence about a pattern of unauthorized activities, this audit capability should be set according to the needs of the organization.

**Audit:**

```
SQL> select * from dba_stmt_audit_opts where audit_option='PROCEDURE' or audit_option
= 'CREATE ANY LIBRARY' or audit_option = 'CREATE LIBRARY';
```

**Remediation:**

```
SQL> AUDIT CREATE ANY LIBRARY;
```

## *6.23 Audit all user DROP ANY LIBRARY activities/requests (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The AUDIT PROCEDURE audit command allows for the tracking a number of user activities, including the:

FUNCTION, the creation/dropping of a standalone stored function or a "Call specification" that is like a procedure, except functions return values to its original environment and can be in Java or other 3GL languages;

LIBRARY, which is the creation/dropping of a schema object associated with an operating-system shared library;

PACKAGE, which is the creation/dropping of a locally stored collection of related procedures, functions, and potentially other program objects stored together; and

PROCEDURE, which is the creation/dropping of a procedure--this is a subprogram that performs a specified action that is stored in the database.

**Rationale:**

As the logging of user activities involving the creation, alteration, or dropping of a PROCEDURE and its related activities can provide forensic evidence about a pattern of unauthorized activities, this audit capability should be set according to the needs of the organization.

**Audit:**

```
SQL> SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='DROP
ANY LIBRARY';
```

**Remediation:**

```
SQL> AUDIT DROP ANY LIBRARY;
```

## *6.24 Audit all user CREATE ANY TRIGGER activities/requests (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

Auditing CREATE ANY TRIGGER allows to monitor who is creating trigger in other schema.

**Rationale:**

Trigger in other schema can be used to escalate privileges.

**Audit:**

```
SQL> SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE
PRIVILEGE='CREATE ANY TRIGGER';
```

**Remediation:**

```
SQL> AUDIT CREATE ANY TRIGGER;
```

## 6.25 Audit all user ALTER ANY TRIGGER activities/requests (Scored)

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

Auditing ALTER ANY TRIGGER allows to monitor who is altering trigger code in other schema.

**Rationale:**

Trigger in other schema can be used to escalate privileges.

**Audit:**

```
SQL> SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE
PRIVILEGE='ALTER ANY TRIGGER';
```

**Remediation:**

```
SQL> AUDIT ALTER ANY TRIGGER;
```

## 6.26 Audit all user DROP ANY TRIGGER activities/requests (Scored)

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

Auditing DROP ANY TRIGGER allows to monitor who is dropping trigger in other schema.

**Rationale:**

Dropping Trigger in other schema can be used to remove restrictions on a schema or an object.

**Audit:**

```
SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE PRIVILEGE='DROP ANY
TRIGGER';
```

**Remediation:**

```
AUDIT DROP ANY TRIGGER BY ACCESS;
```

## *6.27 Set AUDIT ALL ON SYS.AUD$ activities (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

The logging of attempts to alter the audit trail in the `SYS.AUD$` table (open for read/update/delete/view) will provide a record of any activities that may indicate unauthorized attempts to access the audit trail.

**Rationale:**

As the logging of attempts to alter the `SYS.AUD$` table can provide forensic evidence of the initiation of a pattern of unauthorized activities, this logging capability should be set according to the needs of the organization.

**Audit:**

```
SQL> SELECT * from DBA_OBJ_AUDIT_OPTS where OBJECT_NAME='AUD$';
```

**Remediation:**

```
SQL> AUDIT ALL on SYS.AUD$;
```

## *6.28 Audit all user ALTER SYSTEM activities/requests (Scored)*

**Profile Applicability:**

- Level 1 - 11.2 on Oracle Linux 5

**Description:**

Auditing ALTER SYSTEM allows to modify the database settings.

**Rationale:**

Alter system allows one to change instance settings, including security settings and auditing options. Additionally alter system can be used to run operating system commands using undocumented Oracle functionality.

## Audit:

```
SQL> SELECT USER_NAME, SUCCESS, FAILURE FROM DBA_PRIV_AUDIT_OPTS WHERE
PRIVILEGE='ALTER SYSTEM';
```

## Remediation:

```
SQL> AUDIT ALTER SYSTEM;
```

# Appendix: Change History

| Date | Version | Changes for this version |
|---|---|---|
| 11-15-2012 | 1.0.0 | Initial release. |