Evaluated Configuration for

Oracle Database 11*g* Release 2 (11.2.0.2)

November 2011

Security Evaluations
Oracle Corporation
500 Oracle Parkway
Redwood Shores, CA 94065

Evaluated Configuration for Oracle Database 11*g*

Release 2 (11.2.0.2)

November 2011

Author: Saad Syed, modifications made by Courtney Cavness, Trang Huynh

Contributors: Peter Goatly, Shaun Lee, Sebastian Mayer

This document is based on the equivalent document for Oracle11g Release 1, Issue 0.7 [ECD_10] used in the last Common Criteria Evaluation of Oracle11g. The contributions of the many authors of the precursors to this document are acknowledged.

Contents

CHAPTER

1 Introduction

The Target of Evaluation (TOE) is the Oracle Database 11g Release 2 (11.2.0.2) Object-Relational Database Management System (O-RDBMS) Standard and Enterprise Edition.

The TOE is hosted on the following operating system platforms, all of which have been evaluated for compliance with the Controlled Access Protection Profile [CAPP], which is required by the TOE:

- Oracle Enterprise Linux Edition Version 5 (Update 5)
- Red Hat Enterprise Linux 5 (Release 5)
- SuSE Linux Enterprise Server 11

This *Evaluated Configuration for Oracle Database 11g* document explains the manner in which the TOE must be configured along with the host operating system and network services so as to provide the security functionality and assurance as required under the Common Criteria for Information Technology Security Evaluation [CC].

The assumptions and procedures stated in the document are all (by and large) intended to remove potential vulnerabilities or attack paths from the TOE in its environment.

The Evaluation Assurance Level for the TOE is EAL4 augmented with ALC_FLR.3. The Protection Profile used for the evaluation of the TOE is the Database Management Systems in Basic Robustness Environments, Version 1.3 [BR-DBMSPP]. The Security Target used for the evaluation of the TOE is [ST].

Note: This guide supersedes any other guidance documentation in case of conflicting statements.

1.1 Intended Audience

The intended audience for this document includes evaluators of the TOE, system integrators who will be integrating the TOE into systems, and accreditors of the systems into which the TOE has been integrated.

1.2 Organization

This document is composed of the following sections:

Chapter 1	contains the introduction to the document;
Chapter 2	provides an overview of the security functionality of the TOE;
Chapter 3	describes the physical environment of the TOE and the network services required to support the TOE;
Chapter 4	describes the host operating system, network services, and client application configurations required to support the TOE;
Chapter 5	describes the configuration of the TOE, and all TOE-related network services and applications;
Chapter 6	contains a step by step guide to installation of the TOE in its evaluated configuration;
Annex A	details the password management controls that must be implemented in all user profiles;
Annex B	lists the software components installed as per chapter 5;
Annex C	describes logon trigger examples; and
Annex D	lists the references that are used in this document.

1.3 Format

Assertions for the physical, host, and Oracle configurations are given identifiers to the left of each evaluation configuration requirement in bold Arial font, e.g. **[A-1]**.

The names of the identifiers have not changed from one release to the next even when some assertions have been removed because they are no longer applicable.

Mandatory evaluation configuration requirements use the words “must” and/or “shall” in each assertion.

Strongly recommended evaluation configuration requirements use the words “should” in each assertion.

1.4 Physical Delivery of the TOE

To determine that the physical media has not been tampered with, check that:

1. the original packaging material with Oracle logo is being used.
2. the way bill contains both the order reference and the tracking number previously announced by Oracle.
3. the CD envelops in the package are sealed and that the correct version (11.2.0.1) has been shipped.
4. See section 1.5.1 for electronic download of the required updates/patches.
   Note: to upgrade to TOE version 11.2.0.2, you are required to download and install the patch # 10098816. See section 1.5.1 for instructions to obtain this patch. This patch will install a complete Database version 11.2.0.2 – for a fresh installation, it is not required to install 11.2.0.1 first.

1.5 Electronic Delivery of the TOE

To receive an electronic delivery of the TOE, complete the following steps: using the instructions in section 1.5.1, go to the Oracle patch set website: https://support.oracle.com and directly download patch 10098816.

Note: This patch will install a complete Database version 11.2.0.2 – for a fresh installation, it is not required to install 11.2.0.1 first.

Also, see section 1.5.1 (step 14) for electronic download of the additional required updates/patches.

1.5.1 For Patch and Critical Patch Updates (CPU/PSU)

1. Access the Oracle patch set website: https://support.oracle.com
2. Click Login To metaLink. Note: First time users must first register by clicking Register For MetaLink.
3. Enter your user information and click Sign In.
4. Select the Patches and Updates tab and click Simple Search.
5. Search by Patch Number/name: 10098816
   Note: Patch # 10098816 contains a full installation of Oracle Database 11.2.0.2.
6. Click Go.
7. Verify the search results returned the Oracle Database Patch Set necessary to achieve the TOE (11.2.0.2) for your operating system platform.
8. Click View Readme to access and/or print (recommended) the patch set notes.
9. Contact Oracle Support to obtain the password in order to download the patch(es).
10. Click the View Digest button. A popup window displays with all available checksum values (e.g., SHA-1). Take a note of the SHA-1 checksum value provide for the desired download.
11. Close the View Digest popup window.
12. Download the desired patch set..
13. Verify that the checksum for your download matches the checksum on the Oracle download page. For example, to calculate the SHA-1 has value of the download, execute the following command (a built-in tool in most Unix-based operating systems):
    "sha1sum file_name.zip"

    where *file_name.zip* is the name of the file that was transferred. This will generate a hexadecimal number that can be compared to the checksum value you noted above. If differences exist, corruption to the download may have occurred and the download cannot be trusted.

14. Repeat steps 1 to 13 for the Patch Number/name 12419331 and 12828071

Note: Patch 12419331 is a July PSU that contains July CPU plus additional patches. It is not required to apply a separate July CPU (12319321). Patch 12828071 is an October 2011 CPU.

1.6 Verification of guidance documentation

The consumers can verify the authenticity of the guidance documents by:

1. Request the exact version of the guidance documents that were subject to evaluation from the developer's published email address, seceval_us@oracle.com.

2. Download the support note titled *Common Criteria Oracle Database 11gR2 (11.2.0.2) Enterprise Edition, Standard Edition and Standard Edition 1 Support Note* from support.oracle.com that contains SHA-1 hash sums for those guidance documents. support.oracle.com, which is also used to deliver patches for the TOE, provides hash sums for the downloads offered that are transmitted via an SSL connection with the option to verify Oracle's server certificates.

3. When selecting the Support Note for download on the Oracle support website, obtain its checksum value by clicking the View Digest button. A popup window displays with all available checksum values (e.g., SHA-1). Take note of the SHA-1 checksum provided for the downloaded Support Note.

4. After downloading the Support Note, verify its checksum using the following instructions:

    a. If you do not always have a SHA-1 file hash tool, download an appropriate SHA-1 tool to verify SHA-1 checksums. SHA-1 tools are available for any platform.
    b. Verify that the checksum for your download matches the checksum shown on the Oracle download page. For example, to calculate the SHA-1 has value of the download, execute the following command (a built-in tool in most Unix-based) operating systems):

        "shalsum *file_name.zip"*

        where *file_name.zip* is the name of the file that was transferred. This will generate a hexadecimal number that can be compared to the checksum value you noted above. If differences exist, corruption to the download may have occurred and the download cannot be trusted.

5. Similarly, verify the guidance documents have correct versions, i.e., take a guidance document, make sure that it is the right version as identified in the Support Note, and then generate and compare hashes as follows:

a. To calculate the SHA-1 has value of the guidance document, execute the following command (a built-in tool in most Unix-based) operating systems):
"shalsum *file_name.pdf*"

where *file_name.pdf* is the name of the guidance document. This will generate a hexadecimal number that can be compared to the checksum value specified in the Support Note. If differences exist, the file cannot be trusted.

1.7 Overview of Security Functionality

This section provides an overview of the TOE security functionality. For more detailed information of the security functionality provided by the TOE, see chapter 6 of [ST].

1.7.1 Identification and Authentication

The TOE provides unique identification for each user and authentication via password, configurable controls on passwords, LOGON triggers to restrict user login to specific days of the week and/or specific times of the day.

1.7.2 Resource Control

The TOE provides resource control for database resources so that only authorised users can alter a Resource Profile for a database and/or assign Resource Profiles to users, users are limited to a specified maximum number of concurrent sessions, the TOE will terminate a session if the user exceeds the specified connect time or idle time, or terminate an operation if the user exceeds the specified resource limits for a single SQL statement.

1.7.3 Object Access Control

The TOE provides discretionary access control, label-based access control, implements user roles that can be assigned privileges to access database objects, and determines whether privileges are effective in a user session.

1.7.4 Audit and Accountability

The TOE writes an audit record at start-up, shut-down, and when connection is made through keywords AS SYSDBA or SYSOPER, as well as by specific audit configuration including enabling standard auditing for a specific instance. The TOE also allows authorised users to specify events which are auditable and/or delete or update audit records.

1.7.5 Data Consistency

When accessing the database dictionary (tables and views containing reference information about the database, its structures, and its users), the TOE will ensure that cache entries designated to hold dictionary data are marked dirty when updated and are written back to disk before being overwritten. When the TOE is configured with RAC, a cache-to-cache block transfer mechanism known as Cache Fusion is used to transfer read-consistent images of blocks from one instance to another.

This Page Intentionally Blank

CHAPTER

2 Physical Configuration and Procedural Requirements

This chapter describes the physical and procedural requirements for maintaining the security of the TOE.

2.1 Physical Environmental Assumptions

[A-1] The processing resources of the TOE shall be located within controlled access facilities which will prevent unauthorized physical access to the TOE by unprivileged users. Only authorized DBA or operator users (i.e. users who are allowed corresponding SYSDBA or SYSOPER access rights within the database) shall have physical access to the server machines.

[A-2] The processing resources of the underlying operating system required to support the TOE shall be located within controlled access facilities which will prevent unauthorized physical access.

[A-3] The processing resources of the network services required to support the TOE shall be located within controlled access facilities which will prevent unauthorized physical access.

[A-4] The media on which authentication data for the underlying operating system data resides shall not be physically removable from the underlying operating system by unauthorized users.

[A-5] The media on which the TOE audit data resides shall not be physically removable from the underlying operating.

[A-6] Any on-line and/or off-line storage media on which security relevant data resides shall be

located within controlled access facilities which will prevent unauthorized physical access.

2.2 Supporting Procedures

Procedures for the administration of TOE security shall be established based on the contents of this document, the Security Target [ST]. In particular, the following procedures are best practices that shall be established such that:

- users must not disclose their operating system passwords to other individuals;
- operating system or database passwords generated by the system administrator shall be distributed in a secure manner;
- procedures and/or mechanisms shall assure that, after system failure or other discontinuity, recovery without a protection (i.e. security) compromise is obtained;
- the on-line and off-line storage media on which security related data (such as operating system backups, database backups and transaction logs, and audit trails) are held shall be properly stored and maintained, and routinely checked to ensure the integrity and availability of the security related data;
- the media on which database-related files (including database files, export files, redo log files, control files, trace files, and dump files) have been stored shall be purged prior to being re-used for any non-database purpose;
- the predefined normal users `SYS`, `SYSTEM`, and users who connect as `SYSDBA` or `SYSOPER`, are highly trusted users, who are required by the architecture of the TOE to be able to perform privileged database operations for which the TOE records only limited information. It is assumed that appropriate personnel and procedural measures (such as procedural two-person control) will be provided to ensure that operations performed under these trusted user accounts conform to the system security policy.

  For more routine administration tasks it is recommended that alternative, less privileged, database user accounts are configured and used to perform a more restricted set of privileged database operations.

  After installation, the TOE has the following default audit behaviour:

  - the TOE allows only `SYS` and `SYSTEM`, and users connected `AS SYSDBA`, to set and alter the audit configuration, and to update/delete records from the audit trail.
  - the TOE always audits instance startup and shutdown, and connections from users with administrative privileges.
  - in a RAC environment: RAC-related errors are written to alert and trace files on each instance (see [RACADG] Appendix B “Troubleshooting Oracle Real Application Clusters”). In addition, the Oracle Enterprise Manager Database Control is cluster-aware and gathers alert messages that allow to monitor cluster performance, and to detect when instances are not reachable.

- a user who grants the `REFERENCES` privilege on one or more columns of a table shall understand the possible interactions between database referential integrity controls and access controls. Specifically, a referential constraint has the following implications:
- if the referential constraint specifies `DELETE RESTRICT` then a user will not be able to

delete referenced parent rows even though the user has `DELETE` access on the parent table;

- if the referential constraint specifies `SET TO NULL` or `SET TO DEFAULT` then when a parent row is deleted from the parent table the corresponding child row(s) will be updated regardless of whether the deleting user has UPDATE access on that child table.
- if the referential constraint specifies `DELETE CASCADE` then when a parent row is deleted from the parent table the corresponding child row(s) will be deleted from the child table regardless of whether the deleting user has `DELETE` access on that child table.
- Administrators shall understand the limitations of resource limits. The TOE can control certain resources such as user sessions and connect time directly, but 'system' resources such as CPU time and logical reads can only be controlled in relation to statements that the database has to process (i.e. SQL and PL/SQL statements). For example, the O-RDBMS can run Java code internally, but as this is a separate server mechanism the program code itself is not subject to resource limits. However any database calls (SQL) made from the Java code are sent from the Java Engine to the database SQL engine, then processed in the normal way and are subject to all applicable resource limits.
- Administrators, through the use of password limits in profiles, shall ensure that password controls for all users (including trusted administrative users) are strong enough to satisfy the TOE's CC Strength of Function rating of SOF-*high*.
- Administrators should be aware, when creating new profiles or when changing the default profile, of the factors influencing the strength of user passwords. **[DB.IA-18]** ensures that certain limits are set in every profile (although it does offer a choice to administrators), however the other password controls available can both strengthen and weaken the TOE's overall password mechanism strength. In general, any further elaboration of the complexity check function (beyond that suggested in this document) will **weaken** the strength of passwords since it would narrow the choice available. The other controls are however generally strengthening measures. A password_lock_time in conjunction with failed_login_attempts will delay any password-guessing attacks (although a lockout time of at least 1 minute, and a failed logins count of <10 is recommended). Setting a password_life_time (in conjunction with password_grace_time) will limit the opportunity of an attacker to guess a particular password. Also, using the password_reuse_time limit will enforce the use of different passwords, again limiting the opportunity for a particular password to be guessed. To prevent the same password being supplied at the end of a password life-time period, administrators should set password_reuse_time greater than password_life_time.
  Note that "password_reuse_time" should be interpreted as the time between the last successful user password change to a given value and the next attempt to change the user's password to that same value.
- The `LOGON` trigger function can be used to restrict the ability of a user to login on specific days of the week and specific times of the day. (Note: triggers are functions the database calls upon specific events. Login is one of the those events a trigger can be assigned to.) See annex C.
- Administrators shall not open databases in read-only mode. The read-only database open feature provides the ability for users to query an open database without the potential for on-line data contents modification. This mode of operation deactivates some security features including password changing, account lockout, and database auditing.
- Views created using a version and patch level prior to the evaluated one by others than a

trusted user should be recompiled before they are allowed to be used by regular users.

This Page Intentionally Blank

CHAPTER

3 Host Configuration

This chapter describes the configuration requirements for the operating system platforms, the network services and the client platforms. It also covers the use of operating system facilities to protect the TOE.

3.1 Operating System

[OS-1] The TOE shall only be used with operating system platforms listed in this section, which have all met Common Criteria security requirements for assurance level EAL 4.

[OS-2] The operating system administrator shall ensure that only designated users are able to perform administrative tasks in the operating system.

In addition, the only local operating system user accounts on the server shall be those for the DBA administrators and OS administrators.

[OS-3] There are no general-purpose computing capabilities (e.g., compilers or user applications) available on DBMS servers, other than those services necessary for the operation, administration and support of the DBMS.

[OS-4] Authentication by the host operating system and use of digital certificates are not in the evaluated configuration.

3.1.1 Red Hat Enterprise Linux 5 (Release 5) and Oracle Enterprise Linux Version 5 (Update 5)

The following instructions apply to both, the Red Hat and Oracle Enterprise Linux.

[RH-3] Red Hat Linux shall be installed and operated in the manner described in [ORHEL], [ECGR] and chapter 3 of this document.

[RH-4] The ext3 filesystem shall be used on all host machines supporting the TOE.

During the Red Hat Enterprise Linux installation, change the keyboard and timezone settings as appropriate, and set “selinux=off.”

After installing the Red Hat Enterprise Linux, you may need to make the following changes to the OS:

- If you plan to get your files via NFS or FTP, you do not need to mount a CD ROM. However, if you want to read CDs, add the cdrom to /etc/fstab:
- echo "/dev/cdrom iso 9660 ro, noauto 0 0">>/etc/fstab
- To run the Oracle Installer remotely, install the "xorg-x11-xauth" package which is located on the RedHat installer CDs (or available via FTP from RedHat) using rpm -i <*package file*> in a root shell. For example:
- rpm -i xorg-x11-xauth-6.8.2-1.EL.13.20.rpm
- To run the Oracle GUI programs remotely, edit the ssh-config file to allow X11 forwarding to run the Oracle GUI programs remotely.

3.1.2 SuSE Linux Enterprise Server 11

[SU-1] SuSE Linux shall be installed and operated in a manner described in [SLES] and chapter 3 of this document.

During the SuSE Linux installation, change the keyboard and timezone settings as appropriate. You must choose to install "xinetd" (which is described in the installation guide as optional, but is necessary for EAL4 hardening).

During installation you are asked to edit the sysctl.conf file. Note that to enable the sysctl.conf changes, you must set "chkconfig boot.sysctl on" and then reboot.

3.1.3 Identification and Authentication

[OS.IA-6] No non-administrative users (existing or newly created) shall belong to the administrative groups on either the host machine on which the TOE is installed, or on their local (client) machines from which they will connect to the TOE.

See [OS-2] for guidance about such administrative groups. F.IA.IDE

[OS.IA-8] All normal operating system users shall have a non-administrative primary group set, such as `USERS` or `ORA_USERS`.

3.1.4 Protection of Resources

[OS.PR-1] The operating system shall protect all of the installed TOE-related files and directories by means of its Discretionary Access Control mechanisms to ensure that they are accessible to authorized users only.

Oracle Universal Installer, Database Configuration Assistant and Database Upgrade Assistant set file permissions when Oracle software is installed, so no further action is required.

[SG, 2-6: Restrict Operating System Access] describes best practice in restricting operating system access.

[OS.PR-4] To maintain the integrity of the audit timestamp, only operating system administrators

shall have access to the operating system clock configuration. All other users shall have no access permissions for the operating system clock configuration.

[OS.PR-5] Those responsible for the TOE must ensure that users are assigned label authorisations and policy privileges commensurate with the degree of trust placed in them by the organisation that owns, or is responsible for, the information processed by or stored in the TOE.

[OS.PR-6] Authorized administrators of the TOE are non-hostile, are appropriately trained, and follow all administrator guidance.

3.1.5 Accounting and Auditing

[OS.AA-1] The operating system shall protect operating system audit trails or any other audit trails (e.g. audit log files) used by the O-RDBMS against unauthorized modification and deletion by means of its Discretionary Access Control mechanisms.

[OS.AA-2] The directory containing the TOE-generated audit log files shall have permissions set for only the local TOE administrator operating group, and no access for all other users. Note: this is located by default in the *$ORACLE_HOME/rdbms/audit* directory.

[OS.AA-3] The operating system administrator shall include procedures that support the archiving of operating system audit trails and audit log files prior to audit trail or disk space exhaustion.

Note: If you receive error ORA-02002 while writing to the audit trail, it is because the auditing facility is unable to write to the `AUDIT_TRAIL` table. If this error occurs, SQL statements that are currently being audited may also fail. This error will occur if the `SYSTEM` tablespace runs out of disk space.

If you receive this error, you must add space to the `SYSTEM` tablespace or delete rows from the AUDIT_TRAIL table. If these operations fail or do not eliminate the problem, shut down and restart Oracle with auditing disabled. This is done by setting the initialization parameter `AUDIT_TRAIL` to `FALSE`.

3.1.6 Underlying Systems

[OS.US-1] The directory server used by the TOE must provide protection mechanisms against unauthorized access to TSF data stored in the directory. In addition, queries must be properly authenticated, the TSF data stored in the directory must be protected by the access control mechanisms of the directory server, the TSF data in the directory server must be properly managed by the administrative personnel, and the directory server as well as its network connections must be physically and logically protected from access and interference by unauthorized persons.

[OS.US-2] The information about enterprise users stored in the directory (password verifier, password policy, global roles and privileges) must be managed correctly by authorized personnel.

[OS.US-3] Internal TSF communication as well as communication between the TOE and the

directory server must be protected from unauthorized access to the transmitted data and must ensure that the communication piers are the intended ones.

[OS.US-4] The TOE-external LDAP compliant directory server Oracle Internet Directory 10g (9.0.4) or higher must be used to authenticate Enterprise users, and must be restricted to password based authentication only. Other authentication options (e.g., using digital certificates) are not supported. Other LDAP-compliant directory services are supported by using Oracle Internet Directory Integration Platform to synchronize them with Oracle Internet Directory.

[OS.US-5] The Oracle Internet Directory 10g (9.0.4) must be configured appropriately as described in [IDAG]. The following are generic statements about what the TOE requires in the directory server configuration:

- Enforces the directory access control policy on users of the directory as subjects and TOE security functionality data for users of the TOE as objects and all operations that create, read, modify or delete those objects.
- Enforces the directory access control policy to objects based on successful authentication of any users of the directory.
- Enforces the following rules to determine if an operation among a controlled subject and a controlled object is allowed:
    - If the user has the role of an enterprise security manager, and has the required discretionary access rights to the directory entries he wants to access, access is allowed;
    - Otherwise, access is denied.
- Explicitly authorizes access of subjects to objects based on the following additional rules: NONE.
- Explicitly denies access of subjects to objects based on the following additional rules: NONE.
- Provides a mechanism to verify that secrets (passwords for TOE users managed in the directory) meet reuse, lifetime, and content metrics as defined by an authorized administrative user.
- Requires each directory user to be successfully authenticated before allowing any other directory TOE security functionality-mediated actions on behalf of that directory user.
- Requires each directory user to identify itself before allowing any other directory TOE security functionality-mediated actions on behalf of that directory user.
- Enforces the directory access control policy to restrict the ability to query, modify, or delete the security attributes of Enterprise Users and the LDAP server to the Enterprise Security Manager (and other authorized identified roles). Note that it is left up to the directory server to define the roles that are allowed to perform those operations or define additional controlled operations.
- Enforces the directory access control policy to provide appropriate default values for security attributes that are used to enforce the security functional specifications.
- Allows authorized roles to specify alternative initial values to override the default

values when an object or information is created.

- Is capable of performing the security management functions provided by the directory TOE security functionality.
- Maintains the roles Enterprise Security Manager and other authorized, identified roles.
- Is able to associate users with roles.

[OS.US-6] The environment must provide protection mechanisms that prohibit unauthorized access to data the TOE transfers over communication links. This applies to data the TOE transmits to another part of itself as well as data exchanged between the TOE and the external directory server. This protection may be provided by physical protection, logical protection or a combination of both.

3.2 Network Services

[OS.NS-3] In a distributed environment, the underlying network services shall be based on the available secure communication protocols which ensure the authenticity of the operating system users.

[OS.NS-4] Only administrative users shall be able to modify the network services configuration parameters.

[OS.NS-5] Real Application Clusters (RAC) uses only Automatic Storage Management (ASM) for the management of the shared disk storage.

3.3 Client Applications

[OS.CA-1] No applications shall be permitted to run on any client machines which access the network, unless they have been shown not to compromise the TOE's security objectives stated in the [BR-DBMSPP] and the [ST].

[OS.CA-2] Client applications are developed in accordance with Oracle's application development documentation and do not use any undocumented interfaces of the client part of the TOE.

This Page Intentionally Blank

CHAPTER

4 Oracle Configuration

The TOE consists of software only. The TOE contains no hardware or firmware components and there are no hardware or firmware dependencies which affect the evaluation.

The TOE shall be installed, configured and maintained in accordance with this document and with the instructions provided in [INST_LINUX11g] and [ORHEL]. See the next chapter for additional TOE installation information.

4.1 O-RDBMS Server

4.1.1 Identification and Authentication

In the evaluated configuration, only the O-RDBMS mode of Identification and Authentication is supported, as well as authentication for Enterprise Users via a TOE-external LDAP compliant directory server (e.g., Oracle Internet Directory) which is restricted to password-based authentication only. Otherwise, OS Authentication should not be enabled on either of these platforms.

[DB.IA-1] The TOE shall be configured to use O-RDBMS or TOE-external LDAP compliant directory server I&A for all users connecting to the TOE, i.e. all database users must have a *database password.*

[DB.IA-2] Administrators who create normal users within the O-RDBMS or TOE-external LDAP compliant directory server shall create appropriately privileged accounts for those users in the operating system as well. See **[OS.IA-8]** for details.

[DB.IA-3] Database administrators shall set the initialization parameter as follows:

```
o7_dictionary_accessibility = FALSE
```

This ensures that if you need to access objects in the SYS schema, explicit object privilege must be granted to you. System privileges that allow access to objects in "any schema" do not allow access to objects in SYS schema.

[DB.IA-4] After creating and setting up a database, all database user accounts must be configured as per **[DB.IA-1].** All pre-defined accounts (such as `SYS, MDSYS, SYSTEM` etc.) and any demonstration accounts (such as `SCOTT`) created during installation should have their passwords changed.

[DB.IA-7] Database administrators shall set the initialization parameter as follows:

```
sql92_security = TRUE
```

This ensures that the user must have `SELECT` privilege on a table when executing an `UPDATE` or `DELETE` statement that references table column values in a `WHERE` or `SET` clause.

[DB.IA-11] Normal database users may belong to one or more of the following operating system local groups.

```
ora_user
ora_<sid>_user
```

This step is discretionary, it may help distinguish database users from other users, however it is not necessary for users to belong to this user group in order to connect to the database.

[DB.IA-14] To connect to the O-RDBMS as a privileged database user such as a database administrator, the following parameter shall be set in the appropriate initialization file:

```
remote_login_passwordfile = EXCLUSIVE
```

This allows two types of privileged connection. Privileged connections (i.e. `AS SYSDBA, AS SYSOPER`) are permitted either by having an entry in the password file (having been granted the appropriate permissions in the database). See **[DB.NS-6]** for an additional parameter required to be initialized to permit such connections.

[DB.IA-15] Database administrators who are required to use the CONNECT / AS SYSOPER syntax to connect to an O-RDBMS shall belong to the following operating system local group:

```
dba
```

Note that the *dba* group gives both sysdba and sysoper privileges.

[DB.IA-16] Database administrators who are required to use the `CONNECT / AS SYSDBA` syntax to connect to an O-RDBMS shall belong to the following operating system local group:

```
dba
```

Note that the *dba* group gives both sysdba and sysoper privileges.

[DB.IA-18] After creating and setting up a database, the default profile must be changed as described in Annex A of this document. Annex A provides a choice of two profiles, which implement password limits that enable the TOE to satisfy its CC Strength of Function claim. Database administrators must also employ this change to all new profiles created, to ensure that all users (including administrative users) are subject to strong password controls at all times. The guidance in section 2.2 should be followed when modifying or creating profiles.

[DB.IA-19] Administrators wishing to limit password reuse (for example to prevent the same password being supplied at the end of a password life-time period), should use the profile setting password_reuse_time, perhaps in conjunction with password_life_time and

password_grace_time (with password_reuse_time being set greater than password_life_time). The profile setting password_reuse_max should not be used.

[DB.IA-20] In the evaluated configuration, roles shall not be protected by an associated password.

[DB.IA-21] In the evaluated configuration, the operating system does not authenticate remote users nor perform role associations. Therefore, database administrators shall set the following parameters:

```
remote_os_authent = FALSE
os_roles = FALSE
remote_os_roles = FALSE
```

4.1.2 Accounting and Auditing

[DB.AA-2] In the evaluated configuration for a specific O-RDBMS, the `audit_trail` parameter in the appropriate initialization parameter file for that O-RDBMS shall be assigned in one of the following two ways:

```
audit_trail = OS
audit_trail = DB
```

[DB.AA-5] Database administrators shall create database audit trail views for all other appropriately privileged O-RDBMS users to be able to read and analyse database audit trail data.

Pre-defined database audit trail views are automatically created during the installation and creation of the database.

Only highly trusted users shall have the privilege which allows them to:

- set or alter the audit trail configuration for the database;
- alter or delete any audit record in the database audit trail.

[DB.AA-6] Database administrators shall perform regular archiving of database and operating system audit trails before audit trail exhaustion to ensure sufficient free space for continued auditing operations. See section 3.1.5 for details.

[DB.AA-7] Database administrators shall ensure that session auditing is enabled at all times by issuing the statement

```
audit session;
```

By enabling session auditing at all times, all user sessions are recorded with their sessionid and method of authentication. This information can then be used to identify whether actions in a particular session were undertaken by a proxy user

[DB.AA-9] Database administrators shall ensure that changes to the database audit trail are audited, by issuing the statement

```
audit insert, update, delete
on system.aud$
by access;
```

[DB.AA-9] Since fine-grained auditing is supported only with cost-based optimization, database administrators shall ensure that the cost-based optimization mode is used when using

fine-grained auditing. This can be achieved by setting the `optimization_mode` parameter in the appropriate initialization parameter file in one of the following ways:

`optimizer_mode = first_rows_n` (where n = 1, 10, 100 or 1000), or
`optimizer_mode = all_rows`

[DB.AA-13] The database administrator shall ensure that modifications to the roles of a user are audited, by issuing the statement:

```
audit grant;
```

4.1.3 Availability and Reliability

[DB.AR-1] Only privileged O-RDBMS /Enterprise users such as database administrators shall be permitted to perform privileged O-RDBMS operations such as backup and recovery, and enforce tablespace quotas and resource profiles.

[DB.AR-2] **[DB.AR-1]** should be accomplished by ensuring that only privileged O-RDBMS / Enterprise users have the necessary administrative system privileges to perform these types of operations.

[DB.AR-3] Administrative system privileges shall not be granted to normal O-RDBMS users directly or through the use of database roles. See section 4.1.5 for details.

For example, a normal O-RDBMS user must not be granted the `ALTER PROFILE` system privilege either directly or through a database role.

[DB.AR-4] Each user of the TOE must be configured with appropriate tablespace quotas that are

- sufficiently permissive to allow the user to perform the operations for which the user has access rights;
- sufficiently restrictive that the user cannot abuse the access rights and thereby waste or monopolise resources.

4.1.4 DAC Access Controls

[DB.AC-5] If the UTL_FILE PL/SQL package is used to provide database access to host OS files the configuration parameter `UTL_FILE_DIR` must not be set to "*", but to explicit values so as to protect against overriding the operating system DAC mechanisms.

[DB.AC-6] Each database link must be defined such that users who refer to the link are connected to an identically named normal user account in the secondary or remote database, that is the database link must be defined without reference to a single normal user account to which all users referencing the link would otherwise be connected.

[DB.AC-7] The EXECUTE privilege on the `DBMS_JOB, DBMS_LOB, DBMS_JAVA, DBMS_JAVA_TEST, UTL_SMTP, UTL_TCP, UTL_HTTP, UTL_FILE, DBMS_RANDOM, XFSYS.DBMS_EXPFIL, SYS.OWA_OPT_LOCK, XDB.DBMS_XDB, CTXSYS.DRILOAD, MDSYS.PRVT_IDX, SYS.DBMS_CDC_DPUTIL, SYS.DBMS_EXPORT_EXTENSION, SYS.DBMS_TRANSFORM_EXIMP, XDB.XDB_PITRIG_PKG` PL/SQL packages is granted to PUBLIC by default. This should be revoked by executing the following SQL statements from an administrative connection to the database:

```
revoke execute on <package_name> from public;
```

Additionally, the INSERT privilege on the MDSYS.USER_SDO_GEOM_METADATA and MDSYS.USER_SDO_LRS_METADATA tables is granted to PUBLIC by default. This should be revoked by executing the following SQL statements from an administrative connection to the database:

```
revoke insert on <table_name> from public;
```

.

[DB.AC-10] Normal users shall not be granted access to objects in the SYSTEM schemas.

[DB.AC-11] The recycle bin feature must to be disabled.

4.1.5 Security Administration and Management

In the evaluated configuration, the TOE supports and implements Security Administration and Management by the use of over ninety distinct and separately managed object and system privileges.

System privileges which are administrative in nature such as those which allow database-wide object, role, user, privilege, and profile manipulation shall not be granted to normal O-RDBMS users or Enterprise users either directly or through database roles.

[DB.SAM-1] Only highly trusted O-RDBMS users / Enterprise users and database administrators should be allowed to possess system privileges which are administrative in nature.

Examples of such privileges (if Oracle Database Vault is not installed) are the ALTER PROFILE and ALTER USER system privileges which can be used to alter any user profile, or any user in the O-RDBMS. The latter gives full access to other users' accounts, either through altering their passwords or through the ability to proxy as them.

[DB.SAM-2] Object privileges and other system privileges (which are non-administrative in nature) are required by normal O-RDBMS users and Enterprise users to perform their tasks under the *Principle of Least Privilege.*

The privileges described above should be grouped together into database roles and granted to normal O-RDBMS users or Enterprise users.

An example of these types of privileges is the CREATE TABLE privilege which by default allows O-RDBMS users or Enterprise users to create and modify tables within their own schema, but not in any other user schema.

[DB.SAM-3] The system privileges of SYSDBA and SYSOPER shall not be granted to any normal O-RDBMS / Enterprise user, including the user SYSTEM.

Database administrators are authenticated as described by **DB.IA-14** above. Only database administrators should be granted these system privileges, or given membership of the OS groups described in **DB.IA-15** and **DB.IA-16**.

[DB.SAM-5] The CREATE LIBRARY and CREATE ANY LIBRARY system privileges shall not be granted to any user of the TOE.

This restriction is imposed so as to prevent the use of libraries which would enable callouts to external C programs which could be misused against the TOE's security features.

[DB.SAM-6] The CREATE SNAPSHOT, CREATE MATERIALIZED VIEW, CREATE ANY

SNAPSHOT, CREATE ANY MATERIALIZED VIEW, ALTER ANY SNAPSHOT or ALTER ANY MATERIALIZED VIEW privileges shall only be assigned to trusted (e.g. DBA) users.

[DB.SAM-7] In the evaluated configuration the use of Java packages is not supported. Database Administrators shall make regular checks to ensure that users do not use Java packages.

[DB.SAM-8] LBAC user authorisations are required by normal O-RDBMS users and Enterprise users to perform their tasks under the Principle of Least Privilege.

[DB.SAM-12] The roles CONNECT and RESOURCE shall not be granted to normal users or Enterprise users of the TOE. These roles are only provided to maintain compatibility with previous versions of Oracle and may not be provided in future versions of Oracle. Instead, the privileges which make up these roles should individually be granted to users or to a role as needed by the user. See [SG].

[DB.SAM-13] The EXEMPT ACCESS POLICY system privilege shall only be given to users who have legitimate reasons for by-passing fine-grained security enforcement of VPD policies.

[DB.SAM-14] Because system privileges are so powerful, administrators must take great care when granting ANY system privileges to non-DBA users (such as UPDATE ANY TABLE). Such privileges shall only be given to users who have legitimate reasons for their use.

In particular, CREATE ANY TRIGGER shall not be granted to non-DBA users. This is because it allows a user to create a trigger on any database table and hence to capture data from any transaction performed on that table.

[DB.SAM-15] [ADG, 15]: Database Administration Tasks Before Using Flashback Features] describes how DBAs should set up a database for flashback queries. DBAs should only grant the FLASHBACK ANY TABLE privilege or EXECUTE on the DBMS_FLASHBACK package to trusted users who have legitimate reasons for their use, because this allows such users to access data that existed in the past in tables that they can currently access. This would be a problem if the owner of a table had deleted rows that held sensitive information before granting other users privileges to access the table.

For the same reason, DBAs should refuse requests from normal users or Enterprise users to be granted the FLASHBACK privilege on a table that they do not own. They should, instead, ask such a user to request the owner of the table to grant them the FLASHBACK privilege.

[DB.SAM-16] As described in **[DB.SAM-15]**, DBAs should refuse requests from normal users or Enterprise users to be granted the FLASHBACK privilege on a table that they do not own. They should, instead, ask such a user to request the owner of the table to grant them the FLASHBACK privilege. The owner of a table which is protected by VPD policies should refuse requests from normal users or Enterprise users to be granted the FLASHBACK privilege on the table unless the administrators for these VPD policies have given their approval. The reason for this is that otherwise there would be a problem if a row in a table protected by a VPD policy has had data in a column updated to make access to the row via the policy more restricted, because a flashback query could allow a user access to the row when the VPD policy should not permit it.

[DB.SAM-17] As described in **[DB.SAM-15],** DBAs should refuse requests from normal users or Enterprise users to be granted the FLASHBACK privilege on a table that they do not own. They should, instead, ask such a user to request the owner of the table to grant them the FLASHBACK privilege. **[DB.SAM-19]** The System Global Area (SGA) API is not available to users other than trusted (e.g. DBA) users in the evaluated configuration.

[DB.SAM-21] Revoke the `CREATE EXTERNAL JOB` privilege (for running jobs on the operating system outside the database) from all users who do not need it.

4.1.6 Secure Data Exchange

[DB.SAM-21] Database administrators shall ensure that any system privilege (directly or through the use of roles) required to implement database import and export be only granted to O-RDBMS users or Enterprise users who are trusted to perform these operations, and who normally do not have the appropriate privileges for read and write access to such data.

4.1.7 Secure Distributed Processing and Databases

The TOE can be operated in standalone, client/server and server/server configurations. Database links may be used to connect between different O-RDBMS servers over a network. The TOE provides site autonomy which implies that each server participating in a distributed environment is administered independently from other servers in the distributed system.

[DB.SDD-1] Database administrators should implement a site-specific security policy according to their security requirements.

The Transparent Data Encryption (including its key management) may be used in the evaluated configuration, but no claims about the effectiveness of the protection using encryption has been made in the [ST], and therefore no analysis has been made for this function within the evaluation.

4.1.8 Muli-tier environments

[DB.MT-1] To ensure accountability in multi-tier environments, any middle-tier(s) must pass the original client ID through to the TOE.

4.1.9 External and Subsystem Interfaces

[DB.EI-1] Oracle's heterogeneous option (HO), which provides gateway functionality to non-Oracle databases, is not included in the evaluated configuration.

[DB.EI-2] Java interfaces should not be used in the evaluated configuration.

[DB.EI-3] The following historical Oracle interfaces are being phased out and are not included in the evaluated configuration:

- "old" (version 7 and earlier) Oracle Call Interface (OCI) (for external interface to the Oracle Database)
- UPI (a private interface, for Oracle application use only)

[DB.EI-3] The JDBC thin client should not be used in the evaluated configuration.

4.2 Oracle Network Services

[DB.NS-3] Only operating system or database administrators shall be able to modify the installed network services configuration parameters.

[DB.NS-4] No other user should be permitted to modify any network services configuration parameter in the O-RDBMS network configuration files such as `TNSNAMES.ORA`, `LISTENER.ORA` and `SQLNET.ORA`.

[DB.NS-5] The network services configuration files specified in DB.NS-4 are located in *$ORACLE_HOME*/network/admin. Permissions on this directory should be restricted so that administrative users have full access, but all other operating system users have read-only access.

[DB.NS-7] The parameters in the network configuration files specified in DB.NS-4 shall use a consistent O-RDBMS naming convention; this helps ensure database uniqueness throughout the domain.

[DB.NS-8] The SQL-NET.ALLOWED_LOGON_VERSION parameter must be set to the value 10 in the sql-net.ora file to enforce password encryption over Oracle Net using the AES algorithm.

4.3 Unsupported features in the evaluated configuration

The Oracle Database features specified in this section are not supported, therefore, must be disabled or not used in the evaluated configuration.

4.3.1 Cluster Time Synchronization Service (CTSS)

It is not necessary to disable this feature. CTSS runs in passive mode as long as the Network Time Protocol (NTP) is configured for the machines on which the TOE is running.

4.3.2 Role-Separated Management

By default, this feature is not implemented during installation. Therefore, it should remain disabled in the evaluated configuration.

4.3.3 Application Express

This feature should be disabled in the evaluated configuration. According to the Oracle® Application Express Installation Guide Release 3.2 section 1 “Oracle Application Express Installation Overview” the Oracle Application Express is installed with Oracle Database 11g or later.

To remove the Application Express from the database, see the Oracle® Application Express Installation Guide Release 3.2, section A.3.2 “Removing oracle Application Express from the Database”.

4.3.4 Java Stored Procedures

This feature should not be used in the evaluated configuration. For more information, see oracle Database Concepts 11g Release 2, section “Java Stored Procedures”.

4.3.5 XML DB

This feature should be disabled in the evaluated configuration. For more information, see Oracle XML DB Developer’s Guide 11g Release 2, section 1

“Introduction to Oracle XML DB.

This Page Intentionally Blank

CHAPTER

5 Step by Step Guide

This chapter contains a step by step guide to installing the TOE in its evaluated configuration.

Readers unfamiliar with Oracle products should read this section in conjunction with [DAG]. Note that in some cases changes are not effective until the database is restarted or, for membership of an OS user group, until the user has logged out and logged in again.

5.1 Operating System Installation / Configuration

Ensure that the intended physical environment is in accordance with the assumptions **[A-1]** to **[A-6]** listed in section 2.1 of this document.

5.1.1 Installation of Oracle Enterprise Linux Version 5 Update 5

Install Oracle Enterprise Linux Version 5 Update 1 as discussed in Red Hat Enterprise Linux AS (Release 5) as discussed in section 3.1.1 of this document.

5.1.2 Installation of Red Hat Enterprise Linux 5 (Release 5)

Install Red Hat Enterprise Linux AS (Release 5) as discussed in section 3.1.1 of this document.

5.1.3 Installation of SuSE Linux Enterprise Server 11

Install SuSE Linux Enterprise Server 10 as discussed in section 3.1.2 of this document.

5.2 Oracle Database 11g Server Installation / Configuration

5.2.1 Additional Tasks

Note that if mandated to install GNU C and/or C++ compilers (for example, package name compat-gcc or compat-gcc-c++) by the Oracle Database Installation Guide for your platform, the compilers must be installed so that only administrators can execute them.

5.2.1.1 Additional Tasks for Red Hat Enterprise Linux 5 (Release 5)

Additional changes to the Red Hat Enterprise Linux AS (Release 5) installation are either

requested by the Oracle Universal Installer or required and described in [INST_LINUX_11g] and [ORHEL].

5.2.1.2 Additional Tasks for SuSE Linux Enterprise Server 11

5.2.2 Installation of Oracle Database 11g Release 2 (11.2.0.2)

You can choose from the following installation types when installing Oracle Database 11g:

- Enterprise Edition: Installs licensable Oracle Database options and database configuration and management tools in addition to all of the products that are installed during a Standard Edition installation. It also installs products most commonly used for data warehousing and transaction processing. For the evaluated configuration, the Enterprise Edition is installed following the Custom Installation option.
- Standard Edition: Installs an integrated set of management tools, full distribution, replication, Web features, and facilities for building business-critical applications.

This section should be used in conjunction with the relevant installation manuals and assumes any prior installations of Oracle Database 11 O-RDBMS have been subsequently removed. Some screens only appear during the first installation of the Oracle Database on a system.

Important: After installation of the software, you must then install the necessary patches as described in the following sections to duplicate the evaluated configuration of Oracle Database 11g.

5.2.2.1 Enterprise Edition

To install the Database Enterprise Edition in the evaluated configuration, follow the installation steps in [INST_LINUX_11g] but choose the installation options below:

- Do not supply support credentials
- Skip software updates
- Select create and configure a database
- Select server class
- Select single instance database installation
- On the installation type dialog, choose advanced installation
    - Choose English language only
    - Choose Enterprise Edition
    - Select options for “Oracle Partitioning” only.
- Specify pathnames for the database, SID, global identifiers, etc.
- On the page with “Memory”, “Character Sets”, “Security” and “Sample Schemas”,

select the default values for each of them.

- Use Enterprise Manager Console
- Store data on filesystem
- Do not enable automated backup
- When choosing passwords for the database accounts, specify either all different or all the same.
- Select OS groups and users
- Perform OS checks (kernel params, packages), configure OS for the checks to succeed
- Proceed to install.

5.2.2.2 Standard Edition

No evaluation-specific installation steps are required.

5.2.3 Exclusions

This document implicitly excludes certain components by specifying the installation options that comprise the TOE boundary. Additionally, the guidance and configuration steps contained in this document prohibit the use of certain other facilities.

Administrators should also be aware of facilities that should not be used during development of database applications in the evaluated configuration. These are the iFS (internet File System), the OCI internet cache, the KG platform (which implements PL/SQL metadata sharing in applications), the Thin JBDC driver (which provides java applets with a non-OCI interface to the database), the Oracle Intelligent Agent and the new Java RepAPI protocol for snapshots (which is similar to the thin Java client interface).

5.3 Installation of Patch Set for Oracle Database 11g (11.2.0.2)

Install the Oracle Database 11g Patch Set (11.2.0.2) in accordance with the instructions given in the Oracle Database 11g Patch Set Notes [PSN-Linux], which are obtained as described in “Electronic Delivery of the TOE in section 1.5.

5.4 Installation of Critical Patch Updates July 2011 and October 2011

Install the Oracle Database 11g Patch Set (11.2.0.2) Critical Patch Updates (patch number in accordance with the instructions given in patch update note, which is part of the patch files obtained as described in “Electronic Delivery of the TOE” in section 1.5.

5.5 Configuration of Oracle Database 11g RDBMS

5.5.1 Protection of database files

Protect the database files from unauthorized access as per **[OS.PR-1]** of section 3.1.4. Network files shall be protected as per **[DB.NS-3]** to **[DB.NS-5]** of section 4.2.

5.5.2 Setting up the Evaluated Configuration

The following steps must be completed to comply with the Evaluated Configuration.

5.5.2.1 As required for **[DB.IA-14]**, database administrators shall set the following initialization parameter:

```
o7_dictionary_accessibility = FALSE
```

5.5.2.2 As required for **[DB.IA-7],** database administrators shall set the following initialization parameter:

```
sql92_security = TRUE
```

5.5.2.3 As required for **[DB.IA-14],** database administrators shall set the following initialization parameter

```
remote_login_passwordfile = EXCLUSIVE
```

5.5.2.4 As required for **[DB.AA-2]**, the audit_trail parameter in the appropriate initialization parameter file for that O-RDBMS shall be assigned in one of the following two ways:

```
audit_trail = OS
audit_trail = DB
```

5.5.2.5 As required for **[DB.AA-10],** if fine-grained auditing is in use then database administrators shall set the `optimizer_`mode initialization parameter in set in one of the following ways:

```
optimizer_mode = first_rows_n (where n =
1,10,100,1000), or
optimizer_mode = all_rows
```

5.5.2.6 As required for **[DB.AA-7]**, database administrators shall ensure that session auditing is enabled at all times, by issuing the following statement from an administrative connection to the database:

```
audit session;
```

5.5.2.7 As required for **[DB.AC-7],** the following SQL statements shall be executed from an administrative connection to the database:

```
revoke execute on DBMS_JOB from public;
```

```
revoke execute on DBMS_LOB from public;
revoke execute on DBMS_JAVA from public;
revoke execute on DBMS_JAVA_TEST from public;
revoke execute on DBMS_XMLGEN from public;
revoke execute on utl_smtp from public;
revoke execute on utl_tcp from public;
revoke execute on utl_http from public;
revoke execute on utl_file from public;
revoke execute on dbms_random from public;
revoke execute on EXFSYS.DBMS_EXPFIL from public;
revoke execute on SYS.OWA_OPT_LOCK from public;
revoke execute on XDB.DBMS_XDB from public;
revoke execute on CTXSYS.DRILOAD from public;
revoke execute on MDSYS.PRVT_IDX from public;
revoke execute on SYS.DBMS_CDC_DPUTIL from public;
revoke execute on SYS.DBMS_EXPORT_EXTENSION from
public;
revoke execute on SYS.DBMS_TRANSFORM_EXIMP from
public;
revoke execute on XDB.XDB_PITRIG_PKG from public;
revoke insert on mdsys.user_sdo_geom_metadata from
public;
revoke insert on mdsys.user_sdo_lrs_metadata from
public
```

5.5.2.8 As required for **[DB.IA-1],** on Red Hat Linux systems, the administrator shall ensure OS authentication is not configured for any user connecting to the TOE, i.e. all database users must be configured to have a database password. This can be checked at any time by executing:

```
select username from dba_users where
 password='EXTERNAL';
```

If no records are selected, then all users are authenticating via a database password.

5.5.2.9 As required for **[DB.IA-4],** all pre-defined accounts (such as `SYS, MDSYS, SYSTEM` etc.) and any demonstration accounts (such as `SCOTT`) created during installation shall have their passwords changed.

If the account is not to be used, then it shall be locked and expired. To prevent inappropriate access to the data dictionary tables or other tampering with the database, the passwords set for `SYS and SYSTEM` shall be divulged only to the group of

administrators who are intended to use them.

5.5.2.10 As required for **[DB.IA-4],** the following SQL statements shall be executed from an administrative connection to the database:

```
alter user dbsnmp account lock password expire;
```

5.5.2.11 As required for **[DB.IA-18],** after creating and setting up a database, the default profile must be changed as described in Annex A.

5.5.2.12 As required for **[DB.IA-21],** database administrators shall set the following initialization parameter:

```
remote_os_authent = 'FALSE'
os_roles = 'FALSE'
remote_os_roles = 'FALSE'
```

5.5.2.13 As required for **[DB.AC-11],** the recycle bin feature must be disabled. For detailed instructions, see [DVG] Appendix D "Security Considerations for the Recycle Bin".

5.5.2.14 As required for **[DB.AA-13],** the database administratur shall set the following audit option:

```
audit grant;
```

5.5.2.15 As required for **[DB.AA-14]**, the database administratur shall set the following audit option:

```
audit system grant whenever not successful;
audit grant on <object> whenever not successful;
audit drop role whenever not successful;
```

5.5.2.16 Maintaining the Evaluated Configuration

The above steps are necessary for achieving an initial evaluated configuration. The remaining configuration requirements in this document (section 4.1.2 section 4.1.3, section 4.1.4, section 4.1.5, section 4.1.6, section 4.1.7, section 4.8, and **[DB.NS-7]**) cover the general administration of the TOE in order that the evaluated configuration is maintained.

5.6 Configuration of Real Application Clusters (RAC)

Standard Edition One supports up to 400 users, and does not support Real Application Clusters. Standard Edition supports up to 1,000 users, and up to 4 CPUs (including CPUs in a cluster used with Real Application Clusters).

For Standard Edition users, to bind up to 4 servers together so they operate as a single system, the TOE must be configured with Real Application Clusters (RAC). For more

information on RAC, see [RACADG]. For RAC installation instructions, see [RACLINUX].

The `GC_FILES_TO_LOCKS` parameter is at the default value upon installation, and should remain unchanged for the evaluated configuration of the TOE.

5.7 Client Installation

The TOE scope does not include any Oracle client software, but to set up the environment for the evaluated configuration, client installation was completed as follows:

- Install the host operating system as described in section 5.1 above;
- Install the client Oracle software as described in section 5.9 below;
- Configure the network services configuration parameters as described in **[DB.NS-3]** and **[DB.NS-4]**;
- Protect the client applications from unauthorized use by setting the appropriate access control permissions.

Note that untrusted users of the TOE are not expected to be administrators of their local machines.

5.8 Oracle Client Applications

[DB.CA-1] In the environment for the evaluated configuration, the client applications shall be installed using the Oracle Universal Installer. The following software components shall be selected and installed using the Custom Installation option:

Oracle Database Utilities 11.2.x.x
SQL*Plus 11.2.x.x
Oracle Call Interface 11.2.x.x

Annex B contains a complete list of all the software components that are then installed by the Oracle Universal Installer.

[DB.CA-2] No database applications except those based on OCI (e.g. SQL*Plus) shall be permitted to run on any client or server host machines which access the network, unless they have been shown not to compromise the TOE's security objectives as stated in the [BR-DBMSPP] and the [ST] (see **[OS.CA-1]**).

This Page Intentionally Blank

ANNEX

A Password Profile Controls

This Annex specifies the password control requirements that must be applied to all profiles in the evaluated configuration of the TOE. Assertion **[DB.IA-18]** states that the password control limits specified in this Annex must be applied to the default profile as part of the installation task, and then to all new profiles created subsequently.

This Annex does however provide database administrators with a choice of two profiles, both of which provide password controls that are strong enough to meet the claimed CC Strength of Function rating of SOF-*high*. Both choices can also be strengthened further, if necessary, however administrators should see the guidance in section 2.2 of this document, and carefully consider their security requirements and the implications of the profile changes before implementing any such changes.

The two profiles suggested below, entitled ProfileA and ProfileB, require creation via a SQL script (which could be achieved by modifying an example script supplied with the TOE), as well as execution of the script and a SQL statement in the database. The steps are explained fully in sections A.3 and A.4. A rationale for the two choices available is provided in section A.2.

ProfileA and ProfileB were used during the evaluation of the TOE, along with variants of them that added strengthened password controls. Any installation of the TOE can remain within the TOE's Evaluated Configuration provided that ProfileA or ProfileB are used or, if variants of them are used, then it must be possible to show that the changes have added strengthened password controls.

A.1 Password for Enterprise Users

A.1.1 Selecting Passwords

Since passwords for Enterprise Users are used to authenticate a user on several systems, they should be selected carefully to prohibit guessing or a dictionary attack. Creating

passwords that are hard to guess but somewhat easy to remember is the challenge.

A password policy similar to the one defined for the TOE may be also defined for Oracle Internet Directory. This ensures that all passwords defined for Enterprise Users must pass the same tests as passwords defined for local users. In addition it is advised to use the following mechanism to create strong passwords that can also be memorized.

The idea is to create 4 "pseudo" words each 4 character long. A pseudo-word may start with any character from the alphabet followed by a character that would also follow the first character in a valid syllable. FIPS-181 defines a way to create such words based on a random number generator. Implementations of FIPS 181 compatible password generation algorithms can be found on the web.

A combination of 4 randomly generated "words", each 4 character long creates a very strong password. If the password policy also requires at least one digit in a password, the digit as well as its location within the password can also be randomly selected and the character at the selected location in the generated password can by exchanged with the digit.

This procedure is able to produce passwords that are more easy to memorize than pure random passwords but still are very hard to guess or break using a dictionary attack.

A.1.2 Password Controls

In the case of an Enterprise User, the configurable controls on passwords are enforced by the directory as part of the TOE environment. A security administrator for the directory can define the restrictions below as part of the password policy enforced for enterprise users.

a) the number of days the same password can be used before expiring,

b) the number of days before which a password cannot be reused,

c) the number of password changes required before the current password can be reused,

d) the number of days of grace period after a password expires before the user account is locked,

e) a password complexity check to screen passwords selected by the user.

For recommended settings of these restrictions, see section 2.2.

A.2 Rationale

ProfileA specifies a complexity check function that enforces a minimum password length of 8 characters, plus a 1 second lockout whenever 3 consecutive failed log in attempts are made. It is intended that this profile achieves the required strength by enforcement of password length, thereby presenting an attacker with an unreasonably large password space to search. This type of profile may be preferred by administrators who do not wish to use any unreasonable lockout on user accounts, i.e. for availability reasons.

Profile B specifies a complexity check function that enforces a minimum password length of 6 characters, plus a 1 minute lockout whenever 3 consecutive failed log in attempts are made. The rationale for this profile is that administrators may not want to mandate a length of 8 for user passwords, but by reducing this to a length of 6 the profile is strengthened by introducing a temporary lockout.

The type of lockout (used for Profile A and B) works extremely effectively against automated attacks by almost nullifying the speed advantage they would have over manual attacks. The temporary nature of the lockout (one second or one minute is suggested as being sufficient, although a longer time would strengthen the profiles) counters a denial of service attack, since the accounts automatically re-enable themselves after the lockout time expires.

The complexity check function for both profiles will do the following checks:

- Check that the password supplied is not the same as the username;
- Check the length of the password meets the minimum requirement;
- Raise application errors if either of these two checks fail.

The two sections for ProfileA and ProfileB below both specify in full the `CREATE FUNCTION` statement that will create a PL/SQL function to be the complexity check. This function can either be created by entering the full creation statement into the database, or by putting it into a SQL script and executing this within the database. The ProfileA and ProfileB sections also specify the SQL statement that can then be used to modify or create profiles to incorporate the new complexity check function.

As a further alternative to creating a script from scratch (by using a text editor), the example complexity check function supplied with the TOE can be modified. The example script supplied is called *utlpwdmg.sql*, and instructions for modifying this (as an alternative to using the scripts in sections A.3 and A.4) are given in A.5 below.

A.3 ProfileA

To implement ProfileA, the complexity check function needs to be created, and then assigned to the profile.

Section A.3.1 supplies a listing for a SQL script that, when executed, will create the function. Note, the function can also be entered directly into the database if required (omit the `Rem` statements), however a script is recommended as this will preserve the function definition for future use or modification.

A.3.1 Script Listing

```
Rem Oracle Database 11g Release 1 (11.1.0) evaluated configuration
Rem Password complexity check (ProfileA)

CREATE OR REPLACE FUNCTION profilea

(username varchar2,

  password varchar2,

  old_password varchar2)

 RETURN boolean IS

BEGIN

-- Check if the password is the same as the username

   IF password = username THEN

   raise_application_error(-20001, 'Password same as user');
```

```
   END IF;
-- Check for the minimum length of the password
   IF length(password) < 8 THEN
      raise_application_error(-20002, 'Password length less than
8');
   END IF;
RETURN(TRUE);
END;
/
```

A.3.2 Database commands

To create the function from a script, the script must be executed in the database by an administrator (e.g. *sys*) as follows:

```
sqlplus> @profilea.sql
```

Once the complexity check function (called `profilea`) is created, then the default profile can be amended as follows:

```
alter profile default limit
failed_login_attempts 3
password_lock_time 1/86400
password_verify_function profilea;
```

A.4 ProfileB

To implement ProfileB, the complexity check function needs to be created, and then assigned to the profile in conjunction with other profile limits.

Section A.4.1 supplies a listing for a SQL script that, when executed, will create the function. Note, the function can also be entered directly into the database if required (omit the `Rem` statements), however a script is recommended as this will preserve the function definition for future use or modification.

A.4.1 Script Listing

```
Rem Oracle Database 11g Release 1 (11.1.0) evaluated configuration
Rem Password complexity check (ProfileB)
CREATE OR REPLACE FUNCTION profileb
(username varchar2,
  password varchar2,
  old_password varchar2)
  RETURN boolean IS
BEGIN
-- Check if the password is the same as the username
   IF password = username THEN
     raise_application_error(-20001, 'Password same as user');
```

```
   END IF;
-- Check for the minimum length of the password
   IF length(password) < 6 THEN
      raise_application_error(-20002, 'Password length less than
6');
   END IF;
RETURN(TRUE);
END;
/
```

A.4.2 Database Commands

To create the function from a script, the script must be executed in the database by an administrator (e.g. *sys*) as follows:

```
sqlplus> @profileb.sql
```

Once the complexity check function (called `profileb`) is created, then the default profile can be amended as follows:

```
alter profile default limit
failed_login_attempts 3
password_lock_time 1/1440
password_verify_function profileb;
```

A.5 Modifying utlpwdmg.sql

As an alternative to creating the function using the scripts described above, it is also possible to modify the *utlpwdmg.sql* script as described below.

1. In the check for minimum length of password, modify the value of '4' to either '8' (for ProfileA) or '6' (for ProfileB). Ensure this value is changed in two places - the line commencing `IF length`... and the line commencing

   `raise_application_error`.

2. Comment out all checks except the first two checks (the code for the first two checks ensures that the password is not the same as the username, and that the minimum length of password is met). Note, all lines of code under every check description should be commented out by placing the word "Rem" at the start of the line.

3. Ensure that having commented out every check underneath the first two, that the following lines at the end of the function remain un-commented out:

   ```
   RETURN(TRUE);
   END;
   /
   ```

4. Comment out all the lines of the `ALTER PROFILE` statement at the end of the script by placing the word "Rem" at the start of each line.

5. Save the modified script (it is recommended that a different filename is used e.g. `profilea.sql` or `profileb.sql`). Then using a tool such as SQL*PLUS, connect as a privileged user (e.g. *sys*) and run the script to create the complexity

check function as follows:

```
sqlplus> @profilea.sql
```

6. The default profile can then be modified to include the complexity check function as follows:

```
sqlplus> alter profile default limit
password_verify_function profilea;
```

ANNEX

B TOE Components

To obtain a list of TOE components installed on your platform, run the opatch lsinventory -detail command. For example:

```
# /opt/oracle/app/oracle/OPatch/opatch lsinventory -detail
```

The following is an exemplary listing of all the software components installed on an SuSE Enterprise Linux following the installation notes described in chapter 5 of this document:

This Page Intentionally Blank

ANNEX

C Logging Trigger Examples

Oracle has provided example logon triggers as .sql programs available online at http://www.oracle.com/technology/deploy/security/seceval/oracle-common-criteria-evaluated.html. These programs allow you to establish a trigger (or hook) that is executed after logon. The triggers use a database table where the logical expression is stored. The content of that table is then evaluated to allow or deny the logon.

Note: It is important to note that the triggers are executed after logon, and therefore you must be careful when applying logon triggers because as the rules become complex you can inadvertently lock out users (for example, user SYS).

The available .sql programs are:

- install.sql - installs logon triggers
- deinstall.sql - removes logon triggers
- audit_trail.sql - enables you to view relevant audit logs
- package.sql - the package required by install.sql

These programs can be executed by an administrator who has the privileges necessary to install triggers.

> **Note**: The contents of each .sql package are reproduced in the corresponding subsections in this annex.

C.1 Restricting session establishment by time of day and day of week

To restrict session establishment by time of day and day of the week, Oracle provides a set of packages that can be used to implement this requirement via an "after-logon" trigger. This section explains how to install/deinstall this function, and how to use it.

C.1.1 Installation

To install the trigger, the install.sql package is used. Before executed, modify the install.sql and deinstall.sql scripts according to your needs:

- id of the new user (’tsf’ by default)
- default tablespace (’sysaux’ by default)
- passwords of the new user (placeholder ’<tsfpass>’)

The after-logon trigger is then executed with the privileges of this new user.

When created, the new user gets the following privileges assigned:

- Create session
- Create procedure
- Create table
- Administer database trigger
- Create trigger
- Select, insert and update on table sys.aud$
- Select, insert and update on table system.aud$
- Create role

A new role 'SECURITY_ADMIN' is created and assigned to the new user. To activate the functions, the install package will shutdown and restart the database.

Note: Execution of this install package will replace any existing after-logon triggers as well as any existing before-ddl triggers. Also note that the created tsf account is normally not used afterwards, so that you might decide to expire the tsf account:

alter user tsf account lock password expire;

C.1.2 Usage

Once installed, the package allows the definition of a rule used by the after-logon trigger to determine if session establishment is allowed by day of the week or time of the day. The management functions available for a user with the role of SECURITY_ADMIN are:

- add_event_rule (event, rule_expression)

  which allows adding a new rule

- update_event_rule (event, rule_expression)

  which allows updating an existing rule

- delete_event_rule (event)

  which allows deleting an existing rule

ADD_EVENT_RULE Procedure

This procedure adds an event rule that is associated with a specific event. The rule is evaluated by a trigger function asso eciated with the event.

Syntax

```
ADMIN.ADD_EVENT_RULE (
 event                          IN VARCHAR2,
 rule_expression        IN VARCHAR2);
```

Parameters:

event	a string of maximum 100 characters that specifies the event. **Note**: this parameter must be set to the value 'LOGIN' to define a rule that is evaluated by the after-logon trigger.
rule_expression	a string of less than 3900 character that defines the rule to be evaluated. See the section below for details on how to define rules.

MODIFY_EVENT_RULE Procedure

This procedure adds an event rule that is associated with a specific event. The rule is evaluated by a trigger function associated with the event.

Syntax

```
ADMIN.MODIFY_EVENT_RULE (
 event          IN VARCHAR2,
 rule_expression        IN VARCHAR2);
```

Parameters:

event	a string of maximum 100 characters that specifies the event. **Note**: this parameter must be set to the value 'LOGIN' to define a rule that is evaluated by the after-logon trigger.
rule_expression	a string of less than 3900 character that defines the rule to be evaluated. See the section below for details on how to define rules.

DELETE_EVENT_RULE Procedure

This procedure adds an event rule that is associated with a specific event. The rule is

evaluated by a trigger function associated with the event.

Syntax

```
ADMIN.DELETE_EVENT_RULE (
 event              IN VARCHAR2);
```

Parameters:

event	a string of maximum 100 characters that specifies the event. **Note**: this parameter must be set to the value 'LOGIN' to define a rule that is evaluated by the after-logon trigger.

C.1.2.1 How to define an event rule

To restrict login by day of the week, the rule must be constructed in the following way:

USER IN ({List of users that are not restricted by the rule})
OR
(RTRIM(TO_CHAR(SYSDATE, "DAY")) IN ({List of days of the week a user is allowed to login}) AND
RTRIM(TO_CHAR(LOCALTIMESTAMP,"HH24")) IN ({List of hours a user is allowed to login}))

{List of users that are not restricted by the rule}:
a comma separated list of strings where each string is the ID of a user that is not restricted by the rule.

Example: 'SYS' , 'TSF'
In this example the users SYS and TSF would not be restricted by the rule

{List of days of the week a user is allowed to login}:
A comma separated list of days of the week where users are allowed to login

Example: 'MONDAY' , 'TUESDAY , 'WEDNESDAY' , 'THURSDAY' , 'FRIDAY'
This example list would not allow users (other than the ones in the list above) to login on Saturdays and Sundays.

{List of hours a user is allowed to login}:
A comma separated list of hours of the day where users are allowed to login.

Example: '08', '09', '10', '11', '12', '13', '14', '15', '16', '17'
This example list would allow users to login at a time where the hour value at the time of login (in 24 hour format) is between 8 and 17 (i. e. between 8:00am and 5:59pm).

C.1.2.2 Examples

Adding a rule with the values in the example can be done with the following call to admin.add_event_rule:

```
DECLARE
    l_rule_admin_users  varchar2(200) := 'USER IN ("TSF","SYS")';
    l_rule_days_allowed varchar2(200) :=
    'RTRIM(TO_CHAR(SYSDATE,"DAY")) IN ("MONDAY", "TUESDAY ,
    "WEDNESDAY" , "THURSDAY" , "FRIDAY")';
    l_rule_hours_allowed varchar2(200) :=
    'RTRIM(TO_CHAR(LOCALTIMESTAMP,"HH24")) IN ("08", "09", "10",
    "11", "12", "13", "14", "15", "16", "17")';
BEGIN
    ADMIN.ADD_EVENT_RULE('LOGIN', l_rule_admin_users || ' OR ( ' ||
    l_rule_days_allowed || ' AND ' || l_rule_hours_allowed || ')');
END
/
```

This example allows users 'SYS' and 'TSF' to login at all days and all time. All other users are allowed to login only Monday to Friday and only between 8:00 am and 5:59 pm.

Note: If the trigger disallows a user to login, an Oracle error 1031 "insufficient privileges" is raised.

Note: The logon trigger will attach the following string at the beginning of the rule specified:
'select count(*) from sys.dual where '
and execute this as an sql statement within the after-logon trigger. Login is allowed when the statement found a match or when no rule exists. It is therefore possible to define significantly more complex rules than given in this example.

Note: Care should be taken when defining rules to not lock out all users! It is therefore strongly advised to define rules always in such a way that database administrators are allowed to login at all time.

C.1.3 Obtaining Information on Logins

To obtain information about the time and location of the last successful login and the number of unsuccessful login attempts since the last successful login, a user can call the procedure tsf_logon_status. This provides the information in the form:

Welcome <userid>. Your last logon was on "DD-MMM-YY HH.MM.SS.mmmm AM/PM +HH:MM";

from host "<host-id>" on terminal "<terminal-id>".

There have been <n> unsuccessful logon attempts since your last logon.

Where <userid> is the name of the user calling the procedure, <host-id> is the Client host machine name where the last successful login was performed from and <terminal-id> is the identifier of the terminal used for the last successful login.

The number of unsuccessful login attempts is counted since the last successful login.

This allows a user to check if someone has used his account or has unsuccessfully attempted to logon using his account.

The ability to use this function requires the successful installation of the logon trigger as described in section C.1.1 as well as session auditing being enabled as described in section 4.1.2.

C.2 install.sql

```
Rem
Rem Copyright (c) 2007, Oracle, USA. All rights reserved.
Rem    NAME
Rem      install.sql
Rem
Rem    DESCRIPTION
Rem      Installs objects and packages for rules-based login control
Rem      for FTA_THA_EXP.1
Rem
Rem    NOTES
Rem       sqlplus /nolog
Rem       @install
Rem
Rem    MODIFIED (MM/DD/YY)
Rem    sgaetjen  05/11/07 - created
Rem    sec       09/12/07 - adapted for FTA_THA_EXP.1
Rem    smayer 07/03/09 - added password placeholder
Rem

set echo on

connect / as sysdba

create user tsf identified by <tsfpass>
 default tablespace sysaux;
alter user tsf quota 5m on sysaux;

grant create session to tsf;
grant create procedure to tsf;
grant create table to tsf;
grant administer database trigger to tsf;
grant create trigger to tsf;
grant select , insert, update on sys.aud$ to tsf ;
-- if OLS installed
grant select, insert, update on system.aud$ to tsf ;
grant select, insert, update on sys.dba_audit_trail to tsf ;
grant select, insert, update on sys.dba_audit_session to tsf ;
grant create role to tsf;

connect tsf/<tsfpass>;
```

```
create role security_admin;

-- Note: you could extend the concept of the event rule to have audit codes
-- and audit messages so the auditing is more customizable
create table security_criteria (
     event_name   varchar2(100) not null
   , event_rule varchar2(4000)  not null
);
alter table security_criteria add constraint security_criteria_pk
primary key (event_name) enable ;

@@package.sql


create or replace trigger after_logon_trigger after logon on database
begin
   admin.evaluate_rule('LOGIN');
exception
   when others then
      raise;
end;
/

connect / as sysdba
grant execute on tsf.logon_status to public;
grant execute on tsf.logon_last_host to public;
grant execute on tsf.logon_last_terminal to public;
grant execute on tsf.logon_last_date to public;
grant execute on tsf.logon_unsuccessful_count to public;
create or replace public synonym tsf_logon_status for tsf.logon_status;
create or replace public synonym tsf_logon_last_host for tsf.logon_last_host;
create or replace public synonym tsf_logon_last_terminal for tsf.logon_last_terminal;
create or replace public synonym tsf_logon_last_date for tsf.logon_last_date;
create or replace public synonym tsf_logon_unsuccessful_count for
tsf.logon_unsuccessful_count;
alter system set audit_trail = db scope = spfile ;
alter system set audit_sys_operations = true scope = spfile ;

AUDIT CREATE SESSION BY ACCESS WHENEVER SUCCESSFUL;
AUDIT CREATE SESSION BY ACCESS WHENEVER NOT SUCCESSFUL;
```

C.3 deinstall.sql

Note: The following deinstalls only the default user that was assigned during install (see "install.sql"). If you defined a user other than the default, you must modify the script below to deinstall the defined user.

```
Rem
Rem Copyright (c) 2007, Oracle, USA. All rights reserved.
Rem    NAME
Rem      deinstall.sql
Rem
```

```
Rem    DESCRIPTION
Rem      De-install rules-based login control for FTA_THA_EXP.1
Rem
Rem    NOTES
Rem
Rem    MODIFIED (MM/DD/YY)
Rem    sgaetjen  05/11/07 - created
Rem    sec       09/12/07 - adapted for FTA_THA_EXP.1
Rem

connect / as sysdba
drop public synonym tsf_logon_status;
drop public synonym tsf_logon_last_host;
drop public synonym tsf_logon_last_terminal;
drop public synonym tsf_logon_last_date;
drop public synonym tsf_logon_unsuccessful_count;
drop user tsf cascade;
drop user tsfuser cascade;
drop role security_admin;
```

C.4 audit_trail.sql

```
Rem
Rem Copyright (c) 2007, Oracle, USA. All rights reserved.
Rem    NAME
Rem      audit_trail.sql
Rem
Rem    DESCRIPTION
Rem      Display for audit trail of rules-based login control
Rem
Rem    NOTES
Rem
Rem    MODIFIED (MM/DD/YY)
Rem    sgaetjen  05/11/07 - created
Rem
column action_name format a15
column username format a15
column comment_text format a30
select to_char(cast(extended_timestamp as date),'DD-MON-YYYY HH24:MI:SS')
   , username,action,action_name,returncode
from dba_audit_trail
where extended_timestamp > (sysdate-1)
   and action_name like 'LOG%'
order by extended_timestamp
/
```

C.5 package.sql

```
Rem
Rem Copyright (c) 2007, Oracle, USA. All rights reserved.
```

```
Rem    NAME
Rem      package.sql
Rem
Rem    DESCRIPTION
Rem      Package rules-based login control for FTA_THA_EXP.1
Rem
Rem    NOTES
Rem
Rem    MODIFIED (MM/DD/YY)
Rem    sgaetjen  05/11/07 - created
Rem    sec       09/12/07 - adapted for FTA_THA_EXP.1
Rem

set echo on

create or replace package admin as
   procedure add_event_rule ( event varchar2, rule_expression varchar2 );
   procedure update_event_rule ( event varchar2, rule_expression varchar2 );
   procedure delete_event_rule ( event varchar2  );
   procedure evaluate_rule ( event varchar2  );
   procedure logon_status;
   function logon_last_date return varchar2;
   function logon_last_host return varchar2;
   function logon_last_terminal return varchar2;
   function logon_unsuccessful_count return number;
   function session_has_role ( role_name varchar2 ) return number ;
end;
/
show errors

create or replace package body admin as

   c_is_10203 boolean := false;
   -------------------------------------------------
   procedure raise_error ( msg in varchar2 ) is
   begin
       raise_application_error(-20106, msg, false);
   end;
   -------------------------------------------------
   procedure set_is10203 is
   begin
      for c in ( select banner from v$version where banner like 'Oracle Database%'  ) loop
         if instr(c.banner,'10.2.0.3') > 0 OR instr(c.banner,'10.2.0.4') > 0 then
            c_is_10203 := true ;
            exit;
         end if;
      end loop;
   end;
   -------------------------------------------------
   procedure raise_1031 is
     raise_1031_exception exception;
```

```
  pragma exception_init(raise_1031_exception, -1031);
begin
   raise raise_1031_exception;
end;
-------------------------------------------------
procedure validate_event_rule ( event varchar2, rule_expression varchar2 ) is
begin
   if (event is null) or (length(event) > 100) then
      raise_error('invalid event specified');
   end if ;
   if (rule_expression is null) or (length(rule_expression) > 4000) then
      raise_error('invalid rule expression specified');
   end if ;
end;
-------------------------------------------------
function session_has_role ( role_name varchar2) return number is
   l_count number := 0;
begin
   select count(*)
   into l_count
   from session_roles
   where role = upper(role_name);
   if l_count = 0 then
      select count(*)
      into l_count
      from user_role_privs
      where username = user and granted_role = upper(role_name);
   end if;
   return l_count;
end;
-------------------------------------------------
procedure validate_admin_session is
   l_count number;
begin
   if session_has_role('SECURITY_ADMIN') = 0 then
      raise_1031;
   end if;
end;
-------------------------------------------------
procedure add_event_rule ( event varchar2, rule_expression varchar2 ) is
begin
   validate_event_rule(event,rule_expression);
   validate_admin_session;
   insert into security_criteria values ( upper(event), rule_expression);
   commit;
end;
-------------------------------------------------
procedure update_event_rule ( event varchar2, rule_expression varchar2 ) is
begin
   validate_event_rule(event,rule_expression);
   validate_admin_session;
```

```
    update security_criteria set event_rule = rule_expression
    where event_name = upper(event);
    commit;
  end;
  ------------------------------------------------
  procedure delete_event_rule ( event varchar2  ) is
  begin
    validate_event_rule(event,'DUMMY');
    validate_admin_session;
    delete security_criteria where event_name = upper(event);
    commit;
  end;
  ------------------------------------------------
  procedure update_audit_login(sess_id number) is
    pragma autonomous_transaction;
    a_rec sys.aud$%rowtype;
    cursor c_aud (sess number) is select * from sys.aud$
        where sessionid = sess and action# = 100;
  begin
    open c_aud(sess_id);
    loop
      fetch c_aud into a_rec;
      exit when c_aud%notfound;
      a_rec.action# := 101;
      a_rec.returncode := 1031;
      a_rec.comment$text := 'ORA-01031: insufficient privileges';
      insert into sys.aud$ values a_rec;
    end loop;
    commit;
  end;
  ------------------------------------------------
  function logon_last_date return varchar2 is
        l_username varchar2(30) := sys_context('userenv', 'session_user');
        l_date varchar2(50) := 'n/a';
  begin
        begin
                select extended_timestamp into l_date from sys.dba_audit_session
                where username = l_username and returncode = 0 and
extended_timestamp =
                (select max(extended_timestamp) from sys.dba_audit_session where
username = l_username
                 and returncode = 0 and extended_timestamp <
                 (select max(extended_timestamp) from sys.dba_audit_session where
username = l_username
                  and returncode = 0));
        exception
                when others then
                        null;
        end;
        return l_date;
  end;
```

```
   ------------------------------------------------
   function logon_last_host return varchar2 is
           l_username varchar2(30) := sys_context('userenv', 'session_user');
           l_host varchar2(128) := 'n/a';
   begin
           begin
                   select userhost into l_host from sys.dba_audit_session
                   where username = l_username and returncode = 0 and
extended_timestamp =
                   (select max(extended_timestamp) from sys.dba_audit_session where
username = l_username
                    and returncode = 0 and extended_timestamp <
                    (select max(extended_timestamp) from sys.dba_audit_session where
username = l_username
                     and returncode = 0));
           exception
                   when others then
                           null;
           end;
           return l_host;
   end;
   ------------------------------------------------
   function logon_last_terminal return varchar2 is
           l_username varchar2(30) := sys_context('userenv', 'session_user');
           l_term varchar2(255) := 'n/a';
   begin
           begin
                   select terminal into l_term from sys.dba_audit_session
                   where username = l_username and returncode = 0 and
extended_timestamp =
                   (select max(extended_timestamp) from sys.dba_audit_session where
username = l_username
                    and returncode = 0 and extended_timestamp <
                    (select max(extended_timestamp) from sys.dba_audit_session where
username = l_username
                     and returncode = 0));
           exception
                   when others then
                           null;
           end;
           return l_term;
   end;
   ------------------------------------------------
   function logon_unsuccessful_count return number is
           l_username varchar2(30) := sys_context('userenv', 'session_user');
           l_unsucc number := 0;
   begin
           begin
                   select count(*) into l_unsucc from sys.dba_audit_session
                   where username = l_username and returncode > 0 and
extended_timestamp >=
```

```
                (select max(extended_timestamp) from sys.dba_audit_session where
username = l_username
                 and returncode = 0 and extended_timestamp <
                 (select max(extended_timestamp) from sys.dba_audit_session where
username = l_username
                  and returncode = 0));
        exception
                when others then
                        null;
        end;
        return l_unsucc;
    end;
    ------------------------------------------------
    procedure logon_status is
        l_username varchar2(30) := sys_context('userenv', 'session_user');
        l_unsucc number := 0;
        l_date varchar2(50) := 'n/a';
        l_term varchar2(255) := 'n/a';
        l_host varchar2(128) := 'n/a';
    begin
        -- select last logon date, host, terminal
        begin
                select extended_timestamp, userhost, terminal into l_date, l_host,
l_term from sys.dba_audit_session
                where username = l_username and returncode = 0 and
extended_timestamp =
                (select max(extended_timestamp) from sys.dba_audit_session where
username = l_username
                 and returncode = 0 and extended_timestamp <
                 (select max(extended_timestamp) from sys.dba_audit_session where
username = l_username
                  and returncode = 0));
        exception
                when others then
                        null;
        end;
        -- select unsuccessful logon count
        begin
                select count(*) into l_unsucc from sys.dba_audit_session
                where username = l_username and returncode > 0 and
extended_timestamp >=
                (select max(extended_timestamp) from sys.dba_audit_session where
username = l_username
                 and returncode = 0 and extended_timestamp <
                 (select max(extended_timestamp) from sys.dba_audit_session where
username = l_username
                  and returncode = 0));
        exception
                when others then
                        null;
        end;
```

```
            dbms_output.put_line('Welcome '||l_username||'. Your last logon was on
'''||l_date||''';');
            dbms_output.put_line('from host '''||l_host||''' on terminal '''||l_term||'''.');
            dbms_output.put_line('There have been '||l_unsucc||' unsuccessful logon attempts
since your last logon.');
   end;
   ------------------------------------------------
   procedure evaluate_rule ( event varchar2  ) is
      l_count number := NULL ;
      l_sql varchar2(4000);
   begin
      begin
         validate_event_rule(event,'DUMMY');
         for c in ( select event_rule
               from security_criteria
               where event_name = upper(event) ) loop
            l_sql := 'select count(*) from sys.dual where ' || c.event_rule ;
            execute immediate l_sql into l_count;
            exit;
         end loop;
      exception
         when others then
            if ( event = 'LOGIN') then
               update_audit_login(sys_context('userenv','sessionid'));
            end if;
            raise_1031;
      end;

      if (l_count is not null) and (l_count = 0) then
         if ( event = 'LOGIN') then
            update_audit_login(sys_context('userenv','sessionid'));
         end if;
         raise_1031;
      end if;
   end;
   ------------------------------------------------
begin
  set_is10203;
end;
/
show errors

create or replace procedure logon_status is
begin
   admin.logon_status;
end;
/
show errors
create or replace function logon_last_host return varchar2 is
begin
   return admin.logon_last_host;
```

```
end;
/
show errors
create or replace function logon_last_terminal return varchar2 is
begin
   return admin.logon_last_terminal;
end;
/
show errors
create or replace function logon_last_date return varchar2 is
begin
   return admin.logon_last_date;
end;
/
show errors
create or replace function logon_unsuccessful_count return varchar2 is
begin
   return admin.logon_unsuccessful_count;
end;
/
show errors
```

[redacted]

ANNEX

D References

[ADG] *Oracle Database Application Developer's Guide - Fundamentals*, 11g, Release 2 (11.2), Oracle Corporation.

[BR-DBMSPP] *U.S. Government Protection Profile for Database Management Systems in Basic Robustness Environments*, Version 1.3, December 24, 2010

[CAPP] *Controlled Access Protection Profile*, Version 1.d, 8 October 1999, Information Assurance Directorate, National Security Agency.

[CC] *Common Criteria for Information Technology Security Evaluation*, Version 3.1, CCMB-2009-07-001, July 2009.

[CON] *Oracle Database Concepts, 11g Release 2 (11.2)*, Oracle Corporation.

[DAG] *Oracle Database Administrator's Guide*, 11g *Release 2 (11.2)*, Oracle Corporation.

http://www.oracle.com/technology/deploy/security/seceval/pdf/OEL-CAPP-EAL4-Configuration-Guide-v1.3.pdf

[EUA] *Oracle Database Enterprise User Administrator's Guide, 11g Release 2 (11.2),* Oracle Corporation.

[ICG] *Oracle Database Installation and Configuration Guide, 11g Release 2 (11.2),* Oracle Corporation.

[IDAG] *Oracle Internet Directory Administrator's Guide Release 2.1.1,* Oracle Corporation.

[INST_LINUX_11g] *Oracle Database Installation Guide 11g Release 2 (11.2) for Linux,* Oracle Corporation.

[OCI] *Oracle Database Call Interface Programmers Guide, 11g Release 2 (11.2),* Oracle Corporation.

[ORHEL] *Deploying Oracle® Database 11g R1 Enterprise Edition, Dell,* April 2008 Available from http://www.RedHat.com.

[PLS] *PL/SQL User's Guide and Reference, 11g Release 2 (11.21),* Oracle Corporation.

[PSN-Linux] *Oracle Database Patch Set Notes, 11g Release 2(11.2.x.x),Patch Set 1 for Linux x86*-64, Oracle Corporation. Available from https://metalink.oracle.com via Patches and Updates tab.

[RACADG] *Oracle Clusterware and Oracle Real Application Clusters Administration and Deployment Guide, 11g Release 2 (11.2),* Oracle Corporation.

[RACLINUX] *Oracle Clusterware and Oracle Real Application Clusters Installation Guide, 11g Release 2 (11.2) for Linux,* Oracle Corporation.

[ST] *Security Target for Oracle Database 11g, Release 2 (11.2.x.x),* Oracle Corporation.

[SG] *Oracle Database Security Guide, 11g Release 2(11.2.x.x),* Oracle Corporation.

[SQL] *Oracle Database SQL Reference, 11g Release 2(11.2),* Oracle Corporation.

[SQL92] *Database Language SQL, ISO/IEC 9075:1992 and ANSI X3.135-1992*.