Oracle Database 12c Release 2 Enterprise Edition (with Database Vault and Multitenant)

Common Criteria Guidance Supplement

Evaluation Assurance Level (EAL): EAL2+

Doc No. 2030-000-D105
Version: 1.3
6 November 2018

Oracle Corporation
5000 Oracle Parkway
Redwood Shores, California
94065

Prepared by:
EWA-Canada
1223 Michael Street North, Suite 200
Ottawa, Ontario, Canada
K1J7T2

CONTENTS

1 SECURE ACCEPTANCE PROCEDURES

Secure acceptance procedures ensure that the correct version of the TOE has been received by the customer as intended by the developer. Oracle Database 12c may be downloaded by registered users from the Oracle secure delivery cloud at https://edelivery.oracle.com/. Customers must verify that the session is encrypted and must view the certificate to verify the connection before proceeding with the software download. This may be done in Firefox by clicking on the lock icon beside the URL, selecting 'Show connection details > More Information > View Certificate', and verifying that the Common Name in the certificate is www.oracle.com. In Internet Explorer, this may be done by clicking on the lock icon beside the URL, selecting 'View certificates' and verifying that the certificate was issued to www.oracle.com.

The user may then enter the base software (Oracle Database 12c), and then choose a version (12.2.0.1.0), and select this to add it to the shopping cart. The user may then click on the cart and select the platform. In the evaluated configuration, the Linux x86-64 platform is selected. The user may then select 'Continue', accept the terms and restrictions and select 'Continue' again. Before selecting 'Download', the user may view or print the digest details for the package. When the user selects 'View Digest Details', an MD5, SHA-1 and SHA-256 digest of each file is displayed. The user may select 'Print' to print this data. The user may then select 'Download' to initiate the download of the package.

Once the files are downloaded, the user may use a third-party application to verify the SHA-256 digest before proceeding to unzip and install the files. The MD5 and SHA-1 digests are not to be used when verifying the CC evaluated version of the software.

1.1 PATCH AND CRITICAL UPDATES (PPU/CSU)

Information on the October 2018 Patch/Critical Patch Update can be found at:

http://www.oracle.com/technetwork/index.html

1. To download the patch a user needs to access the Oracle support website: https://support.oracle.com.
2. Click "*Sign In*".

   Note: First time users must first register by clicking "*New User? Register here*".
3. Select the 'Patches & Updates' tab.
4. Search by Patch Number/name: 28662603
5. Click Search.
6. Select the patch for the Linux operating system and click on the Readme button to access instructions. Follow the Readme instructions.
7. Click 'Download' to download the patch.
8. Click on p28662603_122010_Linux-x86-64.zip.

Additional information about the patch can be found in My Oracle Support at:

http://www.oracle.com/technetwork/topics/security/alerts-086861.html

2 SECURE INSTALLATION PROCEDURES

This section describes the steps necessary for secure installation of the TOE and the secure preparation of the operation environment in the evaluated configuration.

2.1 SECURE PREPARATION OF THE OPERATIONAL ENVIRONMENT

The following assumptions are made with respect to the secure installation of the TOE and its operational environment:

Assumptions	Description
Physical aspects	
A.PHYSICAL	It is assumed that the IT environment provides the TOE with appropriate physical security, commensurate with the value of the IT assets protected by the TOE.
Personnel aspects	
A.AUTHUSER	Authorized users possess the necessary authorization to access at least some of the information managed by the TOE.
A.MANAGE	The TOE security functionality is managed by one or more competent administrators. The system administrative personnel are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the guidance documentation.
A.TRAINEDUSER	Users are sufficiently trained and trusted to accomplish some task or group of tasks within a secure IT environment by exercising complete control over their user data.
Procedural aspects	
A.NO_GENERAL _PURPOSE	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.
A.PEER_FUNC _&_MGT	All remote trusted IT systems trusted by the TSF to provide TSF data or services to the TOE, or to support the TSF in the enforcement of security policy decisions are assumed to correctly implement the functionality used by the TSF consistent with the assumptions defined for this functionality and to be properly managed and operate under security policy constraints compatible with those of the TOE.

Assumptions	Description
A.SUPPORT	Any information provided by a trusted entity in the IT environment and used to support the provision of time and date, information used in audit capture, user authentication, and authorization that is used by the TOE is correct and up to date.
Connectivity aspects	
A.CONNECT	All connections to and from remote trusted IT systems and between separate parts of the TSF are physically or logically protected within the TOE environment to ensure the integrity and confidentiality of the data transmitted and to ensure the authenticity of the communication end points.

Table 1 – Assumptions

The following subsections provide additional guidance required to meet the secure preparation of the operational environment.

2.1.1 OE.ADMIN

OE.ADMIN Those responsible for the TOE are competent and trustworthy individuals, capable of managing the TOE and the security of the information it contains.

Users of the Oracle DB12 database must ensure that only known, competent, trusted employees are made responsible for managing the security of the database and the data contained therein. Employees should be subject to background checks and undergo Oracle DB12 database training before being put into a position of trust.

2.1.2 OE.INFO_PROTECT

OE.INFO_PROTECT Those responsible for the TOE must establish and implement procedures to ensure that information is protected in an appropriate manner. In particular:

- All network and peripheral cabling must be approved for the transmittal of the most sensitive data transmitted over the link. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted using appropriate physical and logical protection techniques.
- DAC protections on security-relevant files (such as audit trails and authorization databases) shall always be set up correctly.
- Users are authorized to access parts of the data managed by the TOE and are trained to exercise control over their own data.

Adherence to ISO/IEC 11801 standards is required for the implementation of cabling associated with any device connected to the network which includes an

Oracle DB12 database implementation. Both copper and fibre optic cabling are permitted.

Users of the Oracle DB12 database must ensure that all implementations are fully planned prior to system installation and configuration. All access controls must be put in place before the database is populated.

The Oracle DB12 database must be implemented using a 'least privilege' approach. Users may only be permitted access to the data to which access is required in order to perform assigned functions. Only those users fully trained in the use of the Oracle DB12 database, and who have been advised of their privileges and responsibilities may be given access.

2.1.3 OE.NO_GENERAL_PURPOSE

OE.NO _GENERAL _PURPOSE There will be 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.

Installers of the database must ensure a fresh installation of the underlying operating system has been implemented and hardened in accordance with the organization's best practices prior to database installation. Access to the operating system must be strictly controlled, and no other services may be installed on the database server.

2.1.4 OE.PHYSICAL

OE.PHYSICAL Those responsible for the TOE must ensure that those parts of the TOE critical to enforcement of the security policy are protected from physical attack that might compromise IT security objectives. The protection must be commensurate with the value of the IT assets protected by the TOE.

Installers are instructed to only install the Oracle DB12 database in locations that provide physical security against possible attack in accordance with the organization's policy. Security should be increased in accordance with the value of the data to be protected within the database.

2.1.5 OE.IT_I&A

OE.IT_I&A Any information provided by a trusted entity in the environment and used to support user authentication and authorization used by the TOE is correct and up to date.

Prior to configuring an Oracle DB12 database with an external authentication mechanism, the implementers must ensure that every entry in the authentication system is correct and up to date.

2.1.6 OE.IT_REMOTE

OE.IT _REMOTE If the TOE relies on remote trusted IT systems to support the enforcement of its policy, those systems provide that the functions and any data used by the TOE in making policy decisions required by the TOE are sufficiently protected from any attack that may cause those functions to provide false results.

The implementers of the Oracle DB12 database must ensure that any system that connects to the database and provides input to the database's security policy decision making must be implemented securely and protected from possible physical attack.

2.1.7 OE.IT_TRUSTED_SYSTEM

OE.IT _TRUSTED _SYSTEM The remote trusted IT systems implement the protocols and mechanisms required by the TSF to support the enforcement of the security policy.

These remote trusted IT systems are managed according to known, accepted, and trusted policies based on the same rules and policies applicable to the TOE, and are physically and logically protected equivalent to the TOE.

The Oracle DB12 database implementation team must ensure that any system that connects to the database must be implemented securely and protected from possible physical attack. Only remote systems that are under control of those implementing the database, and subject to the same physical and access control security policies should be allowed to access the database.

2.2 INITIAL SETUP AND CONFIGURATION

Administrators should perform the initial setup and configuration of the TOE in accordance with the instructions provided in the following chapters from the *Oracle® Database Installation Guide 12c Release 2 (12.2) for Linux*:

- Chapter 1, Oracle Database Installation Checklist
- Chapter 4, Configuring Operating Systems for Oracle Database on Linux
- Chapter 5, Configuring Users, Groups and Environments for Oracle Grid Infrastructure and Oracle Database
- Chapter 11, Installing Oracle Database
- Chapter 12, Oracle Database Postinstallation Tasks

Administrators managing a multitenant environment should refer to Part VI of the *Oracle® Database Administrator's Guide 12c Release 2 (12.2)*. Initial setup and configuration is performed in accordance with the instructions provided in the following chapters:

- Chapter 36 Overview of Managing a Multitenant Environment
- Chapter 37 Creating and Configuring a CDB
- Chapter 38 Creating and Removing PDBs with SQL*Plus

Administrators using Database Vault features should refer to *Oracle® Database Vault Administrator's Guide 12c Release 2 (12.2)*, particularly Chapter 3 Getting Started with Oracle Database Vault.

2.3 PASSWORD CONFIGURATION

Administrators are required to manually enable the password complexity checking function using the `Ora12c_strong_verify_function`. Instructions on enabling this function can be found in the *Oracle® Database Security Guide 12c Release 2 (12.2)*, Section 3.2.5.6 ora12c_strong_verify_function Function Password Requirements (page 3-19).

3 OTHER PROCEDURES

This section describes the user-accessible functions and privileges that should be controlled in a secure processing environment, and includes the security-critical information and security-critical actions required for secure use of the TOE.

3.1 INITIALIZATION PARAMETERS

The following steps must be completed for the TOE to operate in the evaluated configuration.

a) To connect to the DBMS as a privileged user, such as a database administrator, the following parameters shall be set in the appropriate initialization file:

```
O7_dictionary_accessibility = FALSE;

Remote_login_passwordfile = EXCLUSIVE
```

b) The following parameter ensures that a 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:

```
sql92_security = TRUE
```

c) The `audit_trail` parameter in the appropriate initialization parameter file shall be assigned in the following ways:

```
audit_trail = DB
```

d) The following parameter enables session auditing:

```
audit session
```

e) The following parameters revoke default PUBLIC privileges:

```
revoke execute on DBMS_JOB from Public;

revoke execute on DBMS_JAVA 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 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_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
```

f) In the evaluated configuration, the operating system does not authenticate remote users nor perform role associations. Therefore, the following parameters must be set:

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

g) The following parameter ensures that modifications to the roles of a user are audited:

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

3.2 EVALUATED CONFIGURATION

For the purposes of the evaluation, DB12 was configured to demonstrate the Security Functional Requirements in the Security Target. In order to replicate the evaluated configuration, the steps shown in Section 3.2 must be followed.

3.2.1 Previous Login Information

The date and time of the last successful login are displayed when a user logs in.

In order to display the date and time of the last unsuccessful attempt to login and the number of unsuccessful attempts since the last successful login, the user must run a custom query. The user must be granted the SELECT_CATALOG_ROLE and AUDIT_VIEWER role in order to have the permissions required to run this query. The following steps provide the instructions for granting these permissions to a user, and for running the query as a test user. An organization would be required to customize these instructions to accommodate the usernames, passwords and filenames required for the organization’s own implementation. Note that the user name must be in capital letters and the password must be at least nine characters in length. Instead of using capital letters in the user name, the administrator may choose to surround the username parameter with double quotes (i.e. “&user_name”). This would be done wherever the user name appears in the script, with the exception of within the SELECT commands. It is suggested that passwords be read as a parameter from the command line. Otherwise, the correct password may be entered in the following script in place of <password>.

-- Invoke as follows: sqlplus /nolog @commoncriteria2 <dba_user_name> <dba_pwd> <test_user_name> <tns_alias>

```
-- dba_user_name can be any user with DBA privilege. This is required for provisioning the test user and DB.
-- Example: sqlplus /nolog @commoncriteria2 SYSTEM manager TESTU testdbtns

SPOOL commoncriteria2.log

SET ECHO ON
SET FEEDBACK ON

DEFINE dba_usr = &1
DEFINE dba_pwd = &2
DEFINE user_name = &3
DEFINE tns = &4

-- Setup script
-- Execute as user with DBA privilege
CONN &dba_usr/&dba_pwd@&tns
DROP USER &user_name CASCADE;
CREATE USER &user_name IDENTIFIED BY pass;
GRANT CREATE SESSION TO &user_name;
GRANT SELECT_CATALOG_ROLE, AUDIT_VIEWER TO &user_name;

-- Enable ORA_LOGON_FAILURES audit policy
AUDIT POLICY ORA_LOGON_FAILURES WHENEVER NOT SUCCESSFUL;

-- Attempt Successful logins
CONN &user_name/<password>@&tns

COLUMN login_time FORMAT a40
VAR login_timestamp varchar2(1024);
EXECUTE :login_timestamp := TO_CHAR(current_timestamp AT LOCAL);
SELECT :login_timestamp AS login_time FROM DUAL;
```

```
-- Attempt unsuccessful logins
CONN &user_name/<incorrectpassword1>@&tns
CONN &user_name/<incorrectpassword2>@&tns
CONN &user_name/<incorrectpassword3>@&tns

CONN &user_name/pass@&tns
-- Query login time
-- FTA_TAH_(EXT).1.1/FTA_TAH_(EXT).1.2
-- a. Query the date and time of the session establishment attempt of the user
COLUMN username FORMAT a30
COLUMN last_successful_login_time FORMAT a40

SELECT username, last_login AT LOCAL as last_successful_login_time FROM
dba_users WHERE username = '&user_name';

-- b. The incremental count of successive unsuccessful session establishment
attempt(s).
COLUMN unsuccessful_attempts FORMAT 9999

-- Should record 3 unsuccessful attempts.
SELECT dbusername as username, count(*) as unsuccessful_attempts
FROM unified_audit_trail
WHERE unified_audit_policies like '%ORA_LOGON_FAILURES%'
AND dbusername = '&user_name'
AND return_code = 1017
AND event_timestamp AT LOCAL >= TO_TIMESTAMP_TZ(:login_timestamp)
GROUP BY dbusername;

QUIT;
```

3.2.2 Restricting Session Establishment

There is a requirement to configure DB12 to restrict session establishment as described in the Security Target. Using the following example as a guide, use a CONNECT command rule to restrict user session establishment to certain time of day and day of week. In order to implement these restrictions, Database Vault must be enabled and the setup of the CONNECT command rule must be performed by a user with the DV_OWNER or DV_ADMIN role.

1. Create a rule checking for the allowed days of week (e.g. Not on Saturday and Sunday)

```
execute dbms_macadm.create_rule('allowed_days',
'to_char(sysdate, ''DAY'') NOT IN (''SATURDAY'', ''SUNDAY'')');
```

2. Create a rule checking for the allowed time of day (e.g. between 9 am and 6 pm):

```
execute dbms_macadm.create_rule('allowed_time',
'to_char(sysdate, ''HH24'') > 9 and to_char(sysdate, ''HH24'')
< 18');
```

3. Create a ruleset to be used for the CONNECT command rule:

```
execute
dbms_macadm.create_rule_set(rule_set_name=>'connect_ruleset',
description=>'to restrict session establishment',
enabled=>dbms_macutl.g_yes,
eval_options=>dbms_macutl.g_ruleset_eval_all,
audit_options=>dbms_macutl.g_ruleset_audit_fail,
fail_options=>2, fail_message=>'Connection not allowed at this
time', fail_code=>-20010, handler_options=>0, handler=>null);
```

4. Add the rules to the rule set:

```
execute dbms_macadm.add_rule_to_rule_set('connect_ruleset',
'allowed_days');

execute dbms_macadm.add_rule_to_rule_set('connect_ruleset',
'allowed_time');
```

5. Create a CONNECT command rule:

```
execute dbms_macadm.create_connect_command_rule('%',
'connect_ruleset', 'Y');
```

When the SYSTEM user tries to connect during a day or time that is not allowed, the user will be blocked as below:

```
SQL> connect system

Enter password:

ERROR:

ORA-47306: 20010: Connection not allowed at this time
```

3.3 NETWORK ENCRYPTION CONFIGURATION

Network encryption is outside the scope of the evaluation. However, an administrator can manually enable the encryption of data that is sent over the network. Administrators should configure the network encryption in accordance with the instructions provided in the following chapters of the *Oracle® Database Security Guide 12c Release 2 (12.2)*:

- Chapter 13, Configuring Oracle Database Network Encryption and Data Integrity
- Chapter 14, Configuring the Thin JDBC Client Network

4 REFERENCES

The following installation and administrative guides are referenced within this document:

- Oracle® Database Installation Guide 12c Release 2 (12.2) for Linux, Part Number E85758-02
- Oracle® Database Security Guide 12c Release 2 (12.2), Part Number E85682-02
- Oracle® Database Administrator's Guide 12c Release 2 (12.2), Part Number E85760-06
- Oracle® Database Vault Administrator's Guide 12c Release 2 (12.2), Part Number E85657-02