Oracle® Health Sciences Omics Data Bank

Security Guide

Release 2.5

E41334-01

June 2013

1 Introduction

Oracle Health Sciences Omics Data Bank (ODB) is a flexible, cross-platform omics data management system that delivers meaningfully biological contents and the extreme performance required by today's translational research studies. Moreover, it is fully integrated with the Oracle Health Sciences Cohort Explorer (OHSCE), bringing both phenotypic and genotypic data to researchers and clinicians.

The data model supports reference omics information and annotation, as well as result data from each individual sample. ODB 2.5 is packaged with a set of data loaders for reference and result data, thereby reducing your adoption barrier. It also includes Oracle SecureFile as an optional file storage mechanism. This guide describes various security guidelines for the Omics Data Bank

1.1 General Security Principles

The following principles are fundamental to using any application securely.

1.1.1 Keep Software Up To Date

One of the principles of good security practice is to keep all software versions and patches up to date.

1.1.2 Keep Up To Date on Latest Security Information Critical Patch Updates

Oracle continually improves its software and documentation. Critical Patch Updates are the primary means of releasing security fixes for Oracle products to customers with valid support contracts. They are released on the Tuesday closest to the 17th day of January, April, July and October. We highly recommend customers apply these patches as soon as they are released.

1.1.3 Configuring Strong Passwords on the Database

Although the importance of passwords is well known, the following basic rule of security management is worth repeating:

Ensure all your passwords are strong passwords.

You can strengthen passwords by creating and using password policies for your organization. For guidelines on securing passwords and for additional ways to protect passwords, refer to the *Oracle® Database Security Guide* specific to the database release you are using.

You should modify the following passwords to use your policy-compliant strings:

- Passwords for the database default accounts, such as SYS and SYSTEM.
- Passwords for the database application-specific schema accounts, such as HDM.
- Password for the database listener. You should not configure a password for the database listener as that will enable remote administration. For more information, refer to the *Removing the Listener Password* section of *Oracle® Database Net Services Reference 11g Release 2 (11.2)*

1.1.4 Following the Principle of Least Privilege

The principle of least privilege states that users should be given the least amount of privilege to perform their jobs. Overly ambitious granting of responsibilities, roles, grants — especially early on in an organization's life cycle when people are few and work needs to be done quickly — often leaves a system wide open for abuse. User privileges should be reviewed periodically to determine relevance to current job responsibilities.

Before executing the DDL scripts to create Healthcare Data Warehouse Foundation (HDWF), the database user should be created with the specified limited set of privileges. DBA access should not be given to the user.

2 Security Guidelines for Database Objects and Database Options

This section describes security guidelines for ODB database objects and database options.

2.1 Omics Data Bank Objects

ODB contains database objects. You can use DDL scripts and PL/SQL procedures and functions to create database objects and DML scripts to create seed data. These files are part of the media pack.

The guidelines for installing and configuring Oracle Database Server are available here http://docs.oracle.com/cd/E11882_01/network.112/e16543/toc.htm.

2.2 Oracle Database Options

The Oracle Database has options that provide additional security features. ODB may include data that falls under HIPAA guidelines in the United States and similar guidelines elsewhere. These features can help you comply with those guidelines.

Database Vault

ODB includes data that may fall under HIPAA or other regulations outside the United States. These data are highly sensitive and only those with a need to know should have access to it. To prevent DBAs and others from seeing the data, it is recommended that Oracle Database Vault be used to limit access to the ODB schema to the ODB user to prevent DBAs and other "superuser" accounts from accessing the data. Note that Database Vault requires a separate license.

Oracle Audit Vault

Oracle Audit Vault automates the audit collection, monitoring, and reporting process, turning audit data into a key security resource for detecting unauthorized activity.

Consider using this feature to satisfy compliance regulations such as SOX, PCI, and HIPAA, and to mitigate security risks. Note that Oracle Audit Vault requires a separate license.

Transparent Data Encryption

Transparent Data Encryption is one of the three components of the Oracle Advanced Security option for Oracle Database 11g Release 2 Enterprise Edition. It provides transparent encryption of stored data to support your compliance efforts. If you employ Transparent Data Encryption, applications do not have to be modified and continue to work seamlessly as before. Data is automatically encrypted when it is written to disk and automatically decrypted when accessed by the application. Key management is built in, eliminating the complex task of creating, managing and securing encryption keys. Note that the Advanced Security Option is licensed separately from the database.

Tablespace Encryption

Tablespace Encryption is another component of the Oracle Advanced Security option for Oracle Database 11g Release 2 Enterprise Edition. Tablespace encryption facilitates encryption of the entire tablespace contents, rather than having to configure encryption on a column-by-column basis. It encrypts data at the datafile level to keep users from viewing the oracle datafiles directly. Oracle recommends that you perform tablespace encryption for maximum protection.

3 Revoking Unnecessary Grants

For security purposes, you must revoke all unnecessary grants on the schema. You need DBA privileges to perform this action.

1. Revoke unnecessary grants from Omics Data Bank Schema.

   Execute odb_revoke_grants.sql to remove unnecessary grants from Omics Data Model Schema. This script should be executed by a user with DBA privileges

4 Disabling Unnecessary Operating System Level Services

This section suggests various unused operating system level services that you can disable to improve security.

4.1 Disabling the Telnet Service

Oracle Health Sciences Cohort Explorer does not use the Telnet service.

Telnet listens on port 23 by default. If the Telnet service is available on any computer, Oracle recommends that you disable Telnet in favor of Secure Shell (SSH). Telnet, which sends clear-text passwords and user names through a log-in, is a security risk to your servers. Disabling Telnet tightens and protects your system security.

4.2 Disabling Other Unused Services

Oracle Health Sciences Omics Data Bank does not use the following services or information for any functionality:

- Simple Mail Transfer Protocol (SMTP). This protocol is an Internet standard for E-mail transmission across Internet Protocol (IP) networks.

- Identification Protocol (identd). This protocol is generally used to identify the owner of a TCP connection on UNIX.
- Simple Network Management Protocol (SNMP). This protocol is a method for managing and reporting information about different systems.
- File transfer Protocol (FTP). This protocol is used for downloading or uploading files from the file server.

Therefore, restricting these services or information does not affect the use of Oracle Health Sciences Omics Data Bank. If you are not using these services for other applications, Oracle recommends that you disable these services to minimize your security exposure. If you need SMTP, identd, or SNMP for other applications, be sure to upgrade to the latest version of the protocol to provide the most up-to-date security for your system.

5 Designing Multiple Layers of Protection

When designing a secure deployment, design multiple layers of protection. If a hacker should gain access to one layer, such as the application server, that should not automatically give them easy access to other layers, such as the database server.

Providing multiple layers of protection may include:

- Enabling only those ports required for communication between different tiers, for example, only allowing communication to the database tier on the port used for SQL*NET communications, (1521 by default).
- Placing firewalls between servers so that only expected traffic can move between servers.

6 Protecting Data

Data is vulnerable at many points in any computer system, and many security techniques and types of functionality can be employed to protect it.

7 Setting Up Fine Grain Audit Policy

The ODB application has one schema:

- Schema for Omics Data Bank (ODB)

Oracle recommends that ODB schema has audit policies. The package used to create each policy is the DBMS_FGA package. This package lets you create specific policies for each table. Oracle recommends that the policy names match each table name that is to be audited. This allows for simple identification of audit policies for each table. The audit policies must be defined for `INSERT`, `DELETE`, or `UPDATE` operations. If you plan to move PHI data in OHSCE Schema, then Oracle recommends that you have auditing enabled for `Select` operations. Also, the columns that are audited must be left `NULL` to audit all columns that are accessed. The default value for any column change must be left as is. The mode used to record information must be set to DB + extended or XML extended in order to log the exact SQL statement and bind variables. This is important to detect which data may is affected. Refer to the Oracle database documentation, for a detailed description of the DBMS_FGA package.

There are initialization parameters to specify where the audit logs are stored. Oracle recommends that the audit logs be stored in a separate tablespace and preferably on a

different disk so as to not interfere with other database operations which may need high throughput of the disks with real data. Information about parameters for audit log storage can also be found in the Oracle database documentation.

Oracle recommends that a general audit mode be set to audit each logon to the database as the actual DBA password could be compromised and you may want to disable audit policies. Setting up an audit policy to log all log on operations to the database is always a very good idea in production databases.

There is a list of tables in the ODB schema that do not need any audit policy. These tables are used as staging tables in order to move data to the final tables. All of these tables have _STG in the end of the name. No need to audit any of these tables.

Here is an example of the SQL to set up an audit policy:

```
begin
DBMS_FGA.ADD_POLICY(
object_schema=>'ODB',
object_name=>'W_EHA_GENE',
policy_name=>'W_EHA_GENE',
enable=>true,
statement_types=>'INSERT,UPDATE,DELETE'
);
end;
```

For more information on setting up the audit policy, refer to Oracle data documentation at http://www.oracle.com/pls/db112/homepage.

8 Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Oracle Health Sciences Omics Data Bank Security Guide, Release 2.5
E41334-01

Copyright © 2012, 2013, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.