Oracle® Healthcare Analytics Data Integration Application Toolkit

Security Guide

Release 3.1 for Oracle Data Integrator

E63794-01

June 2015

This document contains the following sections:

1 Introduction to Application Toolkit

The Application Toolkit is a collection of conformed dimensions, facts, and dimension hierarchies that are used for data mart creation and building analytic applications. You can use the entities provided to develop data mart that supports reporting capabilities. The following are the advantages of the Application Toolkit:

- Rapid application development
- Reuse of the data model and Extraction, Transformation, and Loading (ETLs) across multiple applications
- Enforcement of data governance
- Extension of the toolkit data model and ETLs as per your requirements
- Integration across Silo Analytics

2 General Security Principles

The following principles are fundamental to using any application securely.

2.1 Keeping Software Up to Date

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

2.2 Keeping Up to Date on the 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 to apply these patches as soon as they are released.

2.3 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, HDI, HCD, HMC and repository schemas.
- You should not configure a password for the database listener as that will enable remote administration. For more information, see the section “Removing the Listener Password” of *Oracle® Database Net Services Reference 11g Release 2 (11.2)*.

For more information, see *Oracle® Database Security Guide 11g Release 2 (11.2)*.

2.4 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.

3 Database Security Features

The following principles are fundamental to using any application securely.

3.1 About Database Vault

Oracle Database Vault restricts access to specific areas in an Oracle database from any user, including users who have administrative access. For example, you can restrict administrative access to employee salaries, customer medical records, or other sensitive information. This enables you to apply fine-grained access control to your sensitive data in a variety of ways. It hardens your Oracle Database instance and enforces industry standard best practices in terms of separating duties from traditionally powerful users. Most importantly, it protects your data from super-privileged users but still lets them to maintain your Oracle databases.

Oracle Database Vault is an integral component of your enterprise. With Oracle Database Vault, you can address the most difficult security problems remaining today, such as, protecting against insider threats, meeting regulatory compliance requirements, and enforcing separation of duty. You can configure the Oracle Database Vault to manage the security of an individual Oracle Database instance. You can install

Oracle Database Vault on standalone Oracle Database installations, in multiple Oracle homes, and in Oracle Real Application Clusters (Oracle RAC) environments.

For frequently asked questions about Oracle Database Vault, visit http://www.oracle.com/technology/deploy/security/database-security/database-vault/dbv_faq.html.

For Oracle Technology Network (OTN) information specific to Oracle Database Vault, visit http://www.oracle.com/technology/deploy/security/database-security/database-vault/index.html.

Note: The Database Vault is a separately licensed feature of the database.

3.2 About Audit Vault

Oracle Audit Vault automates the audit collection, monitoring, and reporting process. It turns 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. Audit Vault is a separately licensed component.

To know more about Oracle Audit Vault, visit http://www.oracle.com/technetwork/database/audit-vault/overview/index.html.

3.3 About Tablespace Encryption

Transparent Data Encryption is one of the three components of the Oracle Advanced Security option for the Oracle Database 11g Release 2 Enterprise Edition. It provides transparent encryption of stored data to support your compliance efforts. Applications do not have to be modified and will 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 to the Tablespace Encryption feature, eliminating the complex task of creating, managing, and securing encryption keys. The Advanced Security Option is a separately licensed component.

To know more about Oracle advance security options, visit http://www.oracle.com/technetwork/database/options/advanced-security/index.html.

3.4 Secure SQL*Net

SQL*Net enables both client-server and server-server communications across any network. With SQL*Net, databases and their applications can reside on different computers and communicate as peer applications.

Advanced Security Option or Advanced Network Option can be used for encryption of SQL*Net traffic between the database and application servers. This certification and encrypting of SQL*Net traffic is only relevant for highly secure implementations that require encryption of all network traffic. The application servers and database should be solely contained in a secure data center. Performance should be tested before implementing encryption in a production environment. Organizations with stringent security requirements would benefit from a limited deployment of encryption of all direct SQL*Net traffic from outside the data center. The Advanced Security Option (ASO) is an optional component of the Oracle Database and is an extra cost.

To know more about SQL*NET, visit http://docs.oracle.com/cd/A57673_01/DOC/net/doc/NWUS233/ch1.htm

3.5 Managing Default User Accounts

The schema owner should not be the user for normal production; instead the account should be locked after the installation.

3.6 Closing All Open Ports Not in Use

Keep only the minimum number of ports open and close all ports that are not in use.

3.7 Disabling the Telnet Service

The OHADI configuration 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.

3.8 Disabling Other Unused Services

In addition to not using Telnet, the OHADI configuration does not use the following services or information for any functionality:

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

Restricting these services or information does not affect the use of OHADI configuration. 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.

3.9 Designing for 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:

- Enable 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).
- Place firewalls between servers so that only expected traffic can move between servers.

3.10 Configuring Secure SQL NET

If the Application Toolkit Oracle Data Integrator (ODI) repository is installed in a database server other than the server having HDWF and Data Mart schema, the data transfer takes place between two different database servers over a network. As HDWF and Data Mart contains sensitive clinical and healthcare data, you must secure the communication between database servers. Use Oracle® Net Manager to configure encryption to secure communication between database servers. Oracle provides different encryption algorithms to secure communication. Select an appropriate encryption algorithm. For more information, see *Oracle® Database Advanced Security Administrator's Guide 11g Release 2 (11.2)*.

4 Configuring Proxy Schema

You can execute ETLs to load entities using a proxy user to prevent users from accidentally modifying the objects in HDM, HCD, and HMC schemas. To do this, create a proxy schema with basic permissions for accessing the HDM, HCD, and HMC objects. It is important that proxy user is created in the same DB instance where HDWF is installed.

You can also execute HCD ETLs through a proxy schema. However, this is an optional feature. To use this feature, follow the steps in Section 4.1.

4.1 Executing ETLs Using a Proxy Schema

To execute ETLs using a proxy schema, perform the following steps:

1. Create a proxy schema user with an appropriate default tablespace with requisite quotas and temporary tablespace.
2. Traverse to the HCD installed directory or etlsql folder from the command prompt.
3. Log in as HCD user (for example, HCD) in database and execute the following script:

   ```
   @HCD_PROXY_E_TABLE_SCRIPT.sql <name of the hcd schema>;
   ```

4. Log in as SYSTEM user in database and execute the following scripts.

   ```
   @HCD_PROXY_GRANT_SESSION_PREIVS.sql <name of the proxy schema>;
   ```

   ```
   @HCD_PROXY_HDWF_GRANT_PRIVILEGES.sql <name of the hdwf schema> <name of the HCD schema> <name of the metadata schema> <name of the proxy schema>;
   ```

Note: When initial load workflows are executed, the indexes are deleted and the constraints are disabled before ETL execution, and are re-created and enabled respectively after the ETL execution. To do this, the proxy user is assigned with the following privileges using the `HCD_PROXY_GRANT_SESSION_PREIVS.sql` executed in this step:

CREATE ANY INDEX

DROP ANY INDEX

ALTER ANY TABLE

You can revoke these privileges after the completion of the initial load or before starting the incremental load by logging in to the SYSTEM user and executing the following script from the command prompt:

```
@HCD_PROXY_REVOKE_PRIV_INIT.sql <name of the proxy schema>;
```

5. Log in as Metadata user (for example, HMC) in database and execute the following script:

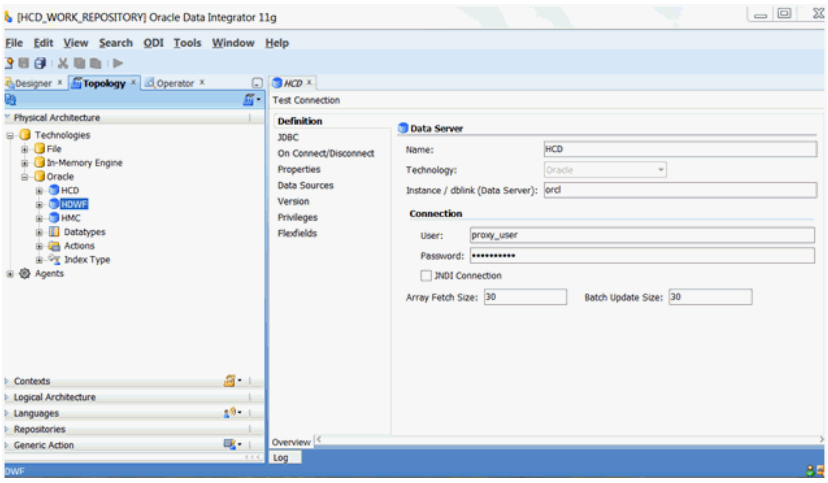
   ```
   @HCD_PROXY_UPDATE_GLBL_PARAM_TABLE.sql <name of the metadata schema>;
   ```

6. In ODI:
   a. Log in to the HCD work repository.
   b. Navigate to **Topology > Physical Architecture > Technologies > Oracle**.
   c. Click on the HCD data server.
   d. Modify the following options:

      User - <name of the proxy schema>

      Password - <password of the proxy schema>

Figure 1 Modifying Connection Details



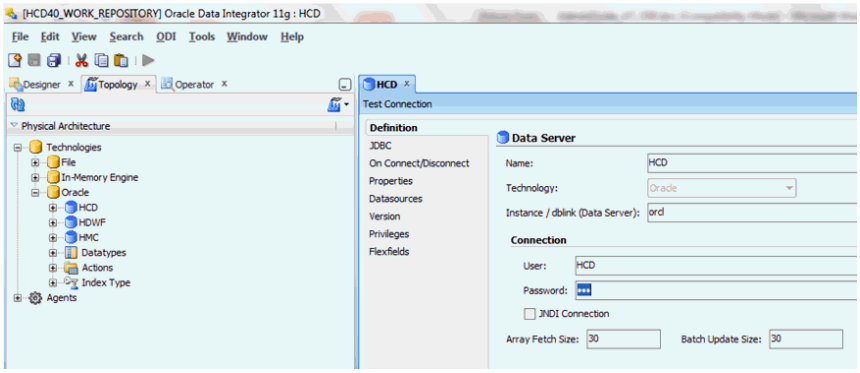
7. Modify the user and password for other data servers such as, HDWF and HMC.
8. Save the repository.
9. Execute the HCD ETLs.

5 Switching to Default Configuration from Proxy Schema Configuration

Perform the following steps to revert the proxy schema configuration and go back to the default settings:

1. In ODI, log in to HCD work repository and navigate to **Topology > Physical Architecture > Technologies > Oracle**.
2. Open the HCD data server. Modify the following options:
   a. User - <name of the HCD schema >
   b. Password - <password for the HCD schema>

Figure 2 HCD Data Server



3. Repeat step 2 for HDWF and HMC data servers.
4. Save the configuration in the repository (click **Save All** from ODI Studio).
5. Log in as SYS user in the database with the following syntax from the command prompt and execute the scripts:

   ```
   sqlplus <sys user>@"(DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)
   (HOST=<hostname>)(PORT=<port number>))(CONNECT_DATA=(SERVICE_
   NAME=<service_name>)))" as sysdba
   ```

   Enter the password when prompted.

   ```
   drop user <name of the proxy schema> cascade;
   ```

6. Log in as HMC user in the database using the following commands at the command prompt:

   ```
   sqlplus <HMC user>@"(DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)
   (HOST=<hostname>)(PORT=<port number>))(CONNECT_DATA=(SERVICE_
   NAME=<service_name>)))"
   ```

   Enter the password when prompted.

   ```
   @ HCD_PROXY_REVERT_GLBL_PARAM_TABLE.sql <name of the HMC schema>;
   ```

6 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 Healthcare Analytics Data Integration Application Toolkit Security Guide, Release 3.1 for Oracle Data Integrator
E63794-01