Oracle® Health Sciences Network

Security Guide

Release 2.0.0.0

E50290-02

September 2015

1 Introduction

The main challenge sponsors face in clinical trials is the elapsed time from the start of the protocol design to the start of patient recruitment. Even with the advent of Clinical Research Organizations (CROs) streamlining research activities, processes for identifying study sites and recruiting patients remain slow. Validating protocols (inclusion and exclusion criteria) and identifying patients consumes valuable time and resources, especially if information or assumptions are dated.

Healthcare providers and academic medical centers can utilize their Electronic Medical Records (EMR) information to provide significant value to Pharmaceutical or Medical Device Companies (study sponsors) through focused searches for study candidates. In parallel, the providers can augment their value to chronic disease patients, by facilitating access to the latest research.

Oracle Health Sciences Network (HSN) Release 2.0. broadens access to more data sources and enables more scalable collaboration. For HSN services, the providers that contribute data to the network are referred to as Data Management (DM) Partners. Organizations (Sponsors, Providers, and DM Partners) can join the network by forming unique relationships with other HSN participant organizations to collaborate within a common network infrastructure. The services described by each relationship are registered within the network, ensuring the appropriate services like Protocol Validator (PV) and Patient Recruiter (PR) are enabled for the respective users from each organization. This release supports a *many-to-many* model, where one sponsor may collaborate with multiple providers on a single protocol and one provider may support recruiting patients for multiple protocols, each from different sponsors.

In combination, the PV and PR application services let users define, save, and share protocols to identify cohorts of patients that match a protocol's criteria. This release introduces workflow features to help users review the feasibility of protocol definitions as well as validate patients appropriate for study recruitment.

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 HSN database objects and database options.

2.1 Oracle Database Options

The Oracle Database has options that provide additional security features. HSN 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

HSN 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 HSN schema to the HSN user to prevent DBAs and other *superuser* accounts from accessing the data.

Note: 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 data file level to keep users from viewing the oracle data files 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 the HSN ManApp Schema.

   Execute `hsnp_post_install.sql` to remove unnecessary grants from HSN ManApp Schema. This script should be executed by a user with DBA privileges

2. Revoke unnecessary grants from the PVPR Data Model Schema.

   Execute `pvpr_post_install.sql` to remove unnecessary grants from the PVPR 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 HSN 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 HSN 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 HSN. 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 Security Guidelines for Oracle Data Integrator

While installing and configuring the Oracle Data Integrator (ODI) Server, follow the guidelines documented in section "Managing Security in Oracle Data Integrator" in the document *Oracle® Fusion Middleware Developer's Guide for Oracle Data Integrator 11g Release 1 (11.1.1).*

7 Security Guidelines for the Middle Tier

This section describes the security guidelines for the HSN middle tier.

7.1 Removing Unused Applications from WebLogic

Currently, the WebLogic Server installation includes the entire JDK and some additional WebLogic Server development utilities (for example, wlsvc). These development programs could be a security vulnerability. The following are recommendations for making a WebLogic Server installation more secure:

- Do not install the WebLogic Server sample applications.
- Delete development tools, such as the Configuration Wizard and the jCOM tools.
- Delete the Derby database, which is bundled with WebLogic Server for use by the sample applications and code examples as a demonstration database.

For more details, refer to the Determining Your Security Needs section in *Oracle® Fusion Middleware Securing a Production Environment for Oracle WebLogic Server 11g Release 1 (10.3.6)*

7.2 Enabling SSL

Enable SSL for Oracle HTTP Server to accept request for the PVPR application. Perform these steps for all servers for PVPR, HSN ManApp and SOA.

To enable SSL:

1. Log into Oracle WebLogic Server Administration Console.
2. Click the **Environment** node in the Domain Structure pane and click **Servers** in Environment table.
3. Click each of the managed servers where the application or SOA composite is deployed.
4. Click the **Configuration** tab.
5. Click the **General** tab.
6. If Save is disabled, click **Lock & Edit** in the Change Center pane.
7. Select the **SSL Listen Port Enabled** check box and enter a port number.
8. Click **Save.**
9. Click **Activate Changes** in the Change Center pane, if it is enabled.
10. Click the **Control** tab.
11. Click the **Start/Stop** tab.
12. Click **Restart SSL**
13. Click **Yes**. The following message appears.

```
SSL channels have been successfully restarted.
```

You must also configure SSL, identity, and trust. For more information, refer to *Oracle® Fusion Middleware Securing Oracle WebLogic Server 11g Release 1 (10.3.6).*

7.3 Configuring SSL

To set up SSL, perform the following steps:

1. Obtain an identity (private key and digital certificates) and trust (certificates of trusted certificate authorities) for Oracle WebLogic Server. Use the digital certificates, private keys, and trusted CA certificates provided by Oracle WebLogic Server, the CertGen utility, the keytool utility, or a reputable vendor such as Entrust or Verisign to perform this step.
2. Store the identity and trust. Private keys and trusted CA certificates which specify identity and trust are stored in keystores.
3. Configure the identity and trust keystores for Oracle WebLogic Server in the Oracle WebLogic Server Administration Console.
4. Set SSL configuration options for the private key alias and password in the Oracle WebLogic Server Administration Console. Optionally, set configuration options that require the presentation of client certificates (for two-way SSL).

For more details, refer to Configuring SSL section in *Oracle® Fusion Middleware Securing Oracle WebLogic Server 11g Release 1 (10.3.6)*.

7.4 Allowing Only Known Host

Allowing only known IPs to access the PVPR application prevents it from being crawled by search engines and only lets customers access the application. This can be done by restricting access from customer's public IPs.

For more information, see the *Access Control* section in *Oracle® Fusion Middleware Administrator's Guide for Oracle HTTP Server Release 1 (11.1.1)*. (`http://docs.oracle.com/cd/E23943_01/web.1111/e10144/security.htm#CDDBCEJI`)

7.5 Protecting User Accounts

WebLogic Server defines a set of configuration options to protect user accounts from intruders. In the default security configuration, these options are set for maximum protection. You can use the Administration Console to modify these options on the **Configuration** > **User Lockout** page.

As a system administrator, you have the option of turning off all the configuration options, increasing the number of login attempts before a user account is locked, increasing the time period in which invalid login attempts are made before locking the user account, and changing the amount of time a user account is locked. Remember that changing the configuration options lessens security and leaves user accounts vulnerable to security attacks. For more details, refer to Configuring Security for a WebLogic Domain section in *Oracle® Fusion Middleware Securing Oracle WebLogic Server 11g Release 1 (10.3.6)*.

8 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.

9 Setting Up Fine Grain Audit Policy

The HSN application has three different schemas:

- Schema for Cohort Data Mart (CDM)
- Application schema used by the HSN ManApp
- Application schema used by the PVPR application user interface

Oracle recommends that only the CDM and HSN ManApp schemas have audit policies. There is no need to log unwarranted access to the application schema. 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 the PVPR schema, 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. For a detailed description of the DBMS_FGA package, refer to the Oracle database documentation.

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.

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

10 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 that have purchased support 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 Network Security Guide, Release 2.0.0.0
E50290-02

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

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.

This software or hardware and documentation may provide access to or information about 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 unless otherwise set forth in an applicable agreement between you and Oracle. 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, except as set forth in an applicable agreement between you and Oracle.