Secure Access to Oracle Databases According to PCI DSS

Contents

Introduction

According to Payment Card Industry Data Security Standard (PCI DSS – see the "Payment Card Industry (PCI) Data Security Standard" document), secret data sent on the network must be encrypted:

- during administrative access to an Oracle database
- during non-administrative access if the network is not isolated by an internal network.

This document describes several types of access and setup of their encryption. For other types of access, see PCI DSS documentation as to whether they may be used and requirements to their use.

Access to a database or a server where a database is installed for its administration may be performed in the following ways:

1. Under Oracle Net (SQLNET) protocol through SqlPlus or other tools using Oracle Client
2. Java software through Oracle JDBC driver
3. Console access under SSH protocol or another type of access through an SSH tunnel
4. Through X Window (X11) – graphic access from a remote client under XDMCP protocol, e.g. to install an Oracle patch
5. Access to the DB Console (a web console for Oracle administration) through HTTPS

When data encryption is required, access methods that do not assume encryption and do not use an encrypted tunnel are forbidden and must be switched off. This includes telnet, rlogin, vnc, and Oracle client and server versions that do not support encryption.

Chapter 1. Data Encryption

Oracle Net and Oracle JDBC Data

Encryption setup is described in the Oracle® Database Advanced Security Administrator's Guide in the section "Configuring Network Data Encryption and Integrity for Oracle Servers and Clients" (the name for Oracle 10g Release 2).

To simplify configuring switching on encryption of database connections (for Oracle Net and Oracle JDBC), mandatory encryption of all connections can be set. To do so, set the following parameters on the database server in the "sqlnet.ora" file manually or using Oracle Net Manager (see the above sections of Oracle's documentation):

SQLNET.ENCRYPTION_SERVER = required

SQLNET.ENCRYPTION_TYPES_SERVER = (<list of encryption algorithms>)

where <list of encryption algorithms> is the list of necessary algorithms of the ones described in the documentation. For example, SQLNET.ENCRYPTION_TYPES_SERVER = (RC4_256, RC4_128).

After the parameters are set, all database connections of Oracle Net and Oracle JDBC clients that support encryption will be encrypted and connections of clients that do not support encryption will terminate with the "ORA-12650" or "ORA-12660" error.

For Oracle 9i clients, it will probably be necessary to add the following parameter in each client file "sqlnet.ora":

SQLNET.CRYPTO_SEED = <seed>

where <seed> is 10 to 70 random characters. Otherwise, a client's connection attempt may result in the "ORA-12645: Parameter does not exist" error because of an Oracle 9 bug).

To check how a connection is encrypted, execute a request to v$session_connect_info by session id (SID). As a result, strings with the names of the used algorithms will be returned. A string not containing an algorithm name does not mean that encryption is used. For example:

Oracle Advanced Security: RC4_256 encryption … – algorithm RC4_256 is used

Oracle Advanced Security: encryption… – does not contain an algorithm name and does not show whether data is encrypted

SSH Data

An SSH protocol server is by default set up for data encryption – in this case, it does not need to be set up. Otherwise, set up encryption according to your SSH server documentation.

Oracle Database Control, Application Server Control and Grid Control Access

To encrypt access, switch on HTTPS support and switch off HTTP support, as specified in Oracle's documentation.

Encryption setup for Oracle Grid Control 10g Release 2 is described in the "Oracle® Enterprise Manager Advanced Configuration 10g Release 2 (10.2)" document, section 4: "Enterprise Manager Security", subsection 4.2 "Configuring Security for Grid Control".

Encryption setup for Oracle Database Control is described in the Oracle Database 10g Release 1 manual. Note that the Release 2 manual does not contain the corresponding item.

Encryption setup for Oracle Application Server Control is described in the Oracle Application Server documentation.

X11 Encryption

Direct network access to X11 around SSH must be forbidden (SSH access for X11 looks like local access). For this, e.g. in Red Hat Linux, remove all lists of allowed hosts and strings containing the '*' character in the "/etc/X11/xdm/Xaccess" file and leave the local host only. In the Gnome graphic shell is used, specify string "Enable=false" in section [xdmcp] of the Gnome configuration file "/etc/X11/gdm/gdm.conf".

To switch on access through an encrypted channel (if remote access through X11 is necessary), use traffic tunnelling through SSH. For this, proceed as follows:

1. Switch on X11 port forwarding on the SSH server (e.g. specify "ForwardX11 yes" in the "/etc/ssh/ssh_config" file)
2. Switch on X11 port forwarding on the SSH client (for SecureCRT, option "Connection->Port forwarding->X11->Forward X11 Packets")

To switch on access through a configured SSH tunnel, proceed as follows:

1. Start an X server on the client in passive mode (e.g. XManager – Passive)
2. Connect to the server using an SSH client and start a graphic application ("xclock" may be used for testing). The application window must appear on the screen of the computer where the client is started.

In this mode, the value of the DISPLAY variable may usually not be changed in the SSH console (this may result in non-encrypted traffic or non-operability of graphic applications) or to switch users (by commands "su", "login", etc.).

X11 must not be used for network access to a database server without tunnelling.