Безопасный доступ к БД Oracle в соответствии со стандартом PCI DSS

Содержание

Введение

Для соответствия требованиям стандарта Payment Card Industry Data Security Standard (PCI DSS – см. документ "Payment Card Industry (PCI) Data Security Standard") необходимо шифровать секретные данные, передаваемые по сети, в случаях:

- при административном доступе к базе данных (БД);
- при неадминистратовном доступе, если сеть не является изолированной внутренней сетью.

Данный документ описывает некоторые виды доступа и настройку их шифрования. Для других видов доступа необходимо консультироваться с документацией стандарта PCI DSS о возможности и требованиях к их использованию.

Доступ к БД или серверу, на котором установлена БД, для ее администрирования может осуществляться следующими способами:

1. по протоколу Oracle Net (SQLNET) с помощью SqlPlus или других инструментов, использующих Oracle Client;
2. java-программы через JDBC-драйвер Oracle;
3. консольный доступ по протоколу SSH или другой доступ через SSH-туннель;
4. через X Window (X11) – доступ с использованием графического интерфейса с удаленного клиента по протоколу XDMCP, например, для установки исправлений (patch) Oracle;
5. доступ к DB Console (web-консоль администрирования Oracle) через HTTPS.

При необходимости шифрования данных способы доступа, не предусматривающие шифрования и не организованные через зашифрованный туннель, запрещены и должны быть отключены. В частности, запрещены telnet, rlogin, vnc, а также версии клиентов и серверов Oracle, не поддерживающие шифрование.

Глава 1. Шифрование данных

Данные Oracle Net и Oracle JDBC

Настройка шифрования описана в документе "Oracle® Database Advanced Security Administrator's Guide" в разделе "Configuring Network Data Encryption and Integrity for Oracle Servers and Clients" (название для Oracle 10g Release 2).

Для упрощения настройки включения шифрования соединений с БД (по Oracle Net и Oracle JDBC), можно установить обязательность шифрования всех соединений. Для этого на сервере БД необходимо сконфигурировать параметры в файле sqlnet.ora вручную или с помощью Oracle Net Manager (см. вышеуказанные разделы документации Oracle):

SQLNET.ENCRYPTION_SERVER = required

SQLNET.ENCRYPTION_TYPES_SERVER = (<список алгоритмов шифрования>)

где <список алгоритмов шифрования> – список желаемых алгоритмов, из описанных в документации. Например,
SQLNET.ENCRYPTION_TYPES_SERVER = (RC4_256, RC4_128).

После задания этих параметров все соединения к БД клиентов Oracle Net и Oracle JDBC, поддерживающих шифрование, будут шифроваться, а соединения, не поддерживающие шифрование, будут завершаться с сообщением об ошибке "ORA-12650" или "ORA-12660".

Для клиентов Oracle 9i, возможно, потребуется в каждом клиентском файле sqlnet.ora добавить параметр:

SQLNET.CRYPTO_SEED = <seed>

где <seed> – 10-70 случайных символов, иначе попытка соединения этого клиента может завершаться с сообщением об ошибке "ORA-12645: Parameter does not exist", из-за программной ошибки в Oracle 9.

Проверить, как шифруется соединение, можно, выполнив запрос к v$session_connect_info по session id (SID) и получив строки с именами используемых алгоритмов. Строка, не содержащая имени алгоритма, не указывает на использование шифрования. Например:

Oracle Advanced Security: RC4_256 encryption … – используется алгоритм RC4_256

Oracle Advanced Security: encryption… – данная строка не указывает имени алгоритма и по ней невозможно судить, шифруются ли данные.

Данные SSH

Сервер протокола SSH обычно по умолчанию настроен на шифрование данных – в этом случае его настройка не требуется. В противном случае необходимо настроить шифрование в соответствие с документацией к используемому SSH-серверу.

Доступ к web-приложениям Oracle Database Control, Application Server Control, Grid Control

Для шифрования доступа необходимо включить поддержку протокола HTTPS и отключить поддержку протокола HTTP, как указано в документации Oracle.

Настройка шифрования для Oracle Grid Control 10g Release 2 описывается в документе "Oracle® Enterprise Manager Advanced Configuration 10g Release 2 (10.2)", раздел 4: "Enterprise Manager Security", подраздел 4.2 "Configuring Security for Grid Control".

Настройка шифрования для Oracle Database Control описывается в инструкции к Oracle Database 10g Release 1, при этом инструкция к Release 2 не содержит соответствующего пункта.

Настройка шифрования для Oracle Application Server Control описываются в документации по Oracle Application Server.

Шифрование X11

Необходимо запретить прямой доступ по сети к X11 в обход SSH (доступ по SSH выглядит для X11 как локальный). Для этого, например в Red Hat Linux, в файле /etc/X11/xdm/Xaccess следует убрать все списки разрешенных хостов и строки, содержащие символ "*", оставив только localhost, а также при использовании графической оболочки Gnome в файле конфигурации Gnome /etc/X11/gdm/gdm.conf в разделе [xdmcp] указать строку Enable=false.

Для включения доступа по шифрованному каналу (если требуется удаленный доступ по X11), необходимо использовать туннелирование трафика через SSH. Для этого следует:

1. включить форвардинг портов X11 на SSH-сервере (например, в файле /etc/ssh/ssh_config указать: ForwardX11 yes
2. включить форвардинг портов X11 на SSH-клиенте (для SecureCRT опция Connection → Port forwarding → X11 → Forward X11 Packets)

Для включения доступа по настроенному SSH-туннелю следует:

1. запустить X-сервер на клиенте в пассивном режиме (например, XManager – Passive);
2. соединиться SSH-клиентом с сервером и запустить графическое приложение (для проверки можно использовать приложение xclock); на

мониторе компьютера, на котором запущен клиент, должно открыться окно приложения.

В таком режиме работы в SSH-консоли обычно нельзя менять значение переменной DISPLAY (это может привести к передаче нешифрованного трафику или неработоспособности графических приложений) или переключать текущего пользователя (командой su, login и т. п.).

Использовать X11 для доступа по сети к серверу БД без туннелирования запрещено.