

## Настройка парольной политики в СУБД Oracle

21.07.2009

*В статье описаны пошаговые инструкции по настройке парольной политики популярной СУБД Oracle в соответствии с требованиями стандарта PCIDSS.*

*Александр Поляков, ведущий аудитор информационной безопасности компании Digital Security*

Довольно часто при проведении аудита на соответствие стандарту PCI DSS, да и аудита безопасности в целом, приходится сталкиваться с отсутствием правильно настроенных парольных политик. Собственно из-за этого в итоге мы и получаем на выходе пароли типа «12345» и прочие уже приевшиеся аудиторскому глазу наборы символов, которые потом мелькают в очередном обзоре самых популярных паролей. И если на контроллере домена худо-бедно политика настроена, да и то, в основном, потому что настраивается по умолчанию, то в СУБД мы видим довольно грустную картину. А ведь чем по сотне раз на дню объяснять пользователям кошмары про подбор паролей, не проще ли один раз внедрить адекватную парольную политику и избавиться уж как минимум от 90% популярных паролей, тем более, что в этом нет ничего сложного и весь набор технических требований раздела 8.5 стандарта, как ни странно, можно реализовать даже не прибегая к дополнительным приложениям, потратив минимальное количество времени.

Итак, не будем больше терять драгоценного времени и приступим к настройке парольной политики в СУБД Oracle. Определимся с техническими требованиями:

1. Изменение пароля пользователя не реже одного раза в 90 дней.
2. При смене пароля запрещается выбор в качестве нового какого-либо из последних четырех использовавшихся данным пользователем паролей.
3. Блокирование учетной записи после шести неудачных попыток ввода пароля.
4. Блокирование учетной записи пользователя не менее чем на 30 минут, либо пока администратор не снимет блокировку.
5. Блокирование рабочей сессии пользователя не более чем через 15 минут простоя.
6. Использование в пароле не менее семи символов.
7. Использование в пароле как цифр, так и букв.

Теперь перейдём к реализации. Собственно, основная часть требований реализуется при помощи настройки профилей:

- Создаём новый профиль для парольной политики с соответствующими значениями:

```
CREATE PROFILE BANK_USERS LIMIT
PASSWORD_LIFE_TIME 80          -- требование 1 и 2
PASSWORD_GRACE_TIME 10        -- требование 1 и 2
PASSWORD_REUSE_TIME 450       -- требование 3
```

```
PASSWORD_REUSE_MAX 4          -- требование 3
FAILED_LOGIN_ATTEMPTS 6       -- требование 4
PASSWORD_LOCK_TIME 1/48      -- требование 5
IDLE_TIME 15;                -- требование 6
```

Проверить установленные значения можно следующим запросом:

```
select PROFILE, RESOURCE_NAME from dba_profiles;
```

- Для выполнения требования 7 необходимо указать так называемую функцию проверки, в которой можно настроить более тонкие параметры и даже, при желании, внедрить любые свои функции. Пример данной функции находится по умолчанию в директории `$ORACLE_HOME/rdbms/admin/UTLPWDMG.SQL`.

Для соответствия требованиям необходимо внести в эту функцию одно изменение, а именно - найти в скрипте строку, отвечающую за длину пароля и изменить значение с 4 на 7 (от себя добавлю, что лучше поставить 9):

```
-- Check for the minimum length of the password
IF length(password) < 7 THEN
    raise_application_error(-20002, 'Password length less than 7');
END IF;
```

Для того, чтобы ввести в эксплуатацию данную функцию, необходимо запустить модифицированный в предыдущем пункте скрипт `UTLPWDMG.SQL` от имени пользователя `SYS`. После чего необходимо добавить её в наш профиль следующей командой:

```
Alter profile BANK_USERS limit PASSWORD_VERIFY_FUNCTION verify_function;
```

- Назначить каждому пользователю созданный профиль:

```
Alter user USERNAME set profile BANK_USERS;
```

Вот, в общем то и всё, что касается технических требований. Более подробно о тонких настройках парольной политики и написании своей функции проверки, а также о других настройках безопасности СУБД Oracle можно прочитать в моей книге [«Безопасность Oracle глазами аудитора: нападение и защита»](#).

## Об авторе

Александр Поляков - ведущий аудитор информационной безопасности компании Digital Security. Специализируется на проведении аудитов защищенности, тестов на проникновение, анализе защищённости бизнес приложений и исследовательской деятельности в области информационной безопасности. Является известным экспертом по безопасности бизнес приложений таких производителей как Oracle и SAP, обнаружившим и опубликовавшим информацию о большом количестве уязвимостей в приложениях данных производителей. Один из основателей и руководитель исследовательского центра Digital Security Research Group [DSecRG], занимающегося поиском и анализом уязвимостей приложений и операционных систем. Автор ряда статей и исследований по информационной безопасности, автор книги «Oracle глазами аудитора: нападение и защита».

## О стандарте PCI DSS

Стандарт PCI DSS (Payment Card Industry Data Security Standard) предназначен для обеспечения безопасности обработки, хранения и передачи данных о держателях платежных карт в информационных системах компаний, работающих с международными платежными системами Visa, MasterCard и другими. Стандарт разработан сообществом PCI Security Standards Council, в которое входят мировые лидеры на рынке платежных карт, такие как American Express, Discover Financial Services, JCB, MasterCard Worldwide и Visa International.

Под действие требований стандарта попадают банки, процессинговые центры, поставщики ИТ-услуг, торгово-сервисные предприятия, и иные организации, обрабатывающие транзакции по международным платежным картам. К части этих компаний международные платежные системы предъявляют требование о прохождении обязательного ежегодного аудита компанией, обладающей статусом QSA.

Текущая версия стандарта 1.2 выпущена 1 октября 2008 года.