*УДК 681.3*

**М.Карпінський[1], докт. техн. наук; М.Сальніков[2]**
[1] *Тернопільський державний технічний університет імені Івана Пулюя*
[2] *Технологічний університет Поділля (м.Хмельницький)*

# МЕТОДИ БЕЗПЕЧНОЇ РОБОТИ ПРИ ВИКОРИСТАННІ SQL-СЕРВЕРА ORACLE

*Розглядається задача адміністрування баз даних розрахованих на велику кількість користувачів. Наводяться рекомендації щодо створення нових користувачів та налагодження їх безпечної роботи в середовищі Oracle 8i Server, Release 8.1.5. Висвітлені можливості, що надаються середовищем Oracle 8i Server при роботі у відкритих мережах.*

У сучасних умовах розв'язання будь-якої проблеми вимагає отримання повного обсягу достеменної інформації. Для організації доступу та зберігання структурованої інформації зручною є система управління базами даних (СУБД), що підтримує структуровану мову запитів (SQL – Structured Query Language) [1].

Проте інформаційна система, в якій передбачено використання баз даних (БД), майже ніколи не розрахована на одного користувача. Тому, якщо з БД працює велика кількість користувачів, то цілком виправданим є застосування технології "клієнт-сервер". Її перевагою є те, що адміністратор БД може встановлювати права для кожного користувача БД залежно від його потреб.

До однієї з найпотужніших та гнучких СУБД, побудованих за технологією "клієнт-сервер", належить Oracle8i Server, Release 8.1.5 [2]. Однак при цьому постає питання, як можна забезпечити безпеку БД за наявності великої кількості користувачів з різними рівнями привілеїв.

Більшість прав користувачам надається при їх створенні системним адміністратором.

Створення користувача <user_name> з паролем <user_password>:

create user <user_name> ideltified by <user_password>.

Надання права для користувача на під'єднання до БД і на створення таблиць:

grant create session, create table to <user_name>.

Тоді користувач вже може працювати у системі, однак не може використовувати її ресурсів. У середовищі Oracle8i користувач повинен мати щонайменше дві робочі області, зокрема:

- область користувача;
- тимчасову область.

Для їх визначення необхідно не тільки вказати, що користувач має доступ до цих областей, а й обмежити їх обсяг. Це виконується так:

alter user user_name
default tablespace system
temporary tablespace temp
quota <розмір> K on system
quota <розмір> K on temp

При замовчуванні використовуються табличні ресурси system та temp, однак системний адміністратор може призначати кожному користувачеві свої табличні ресурси. Розмір вказує на обсяг робочого простору для користувача у кілобайтах (К) або мегабайтах (М). Користувач може працювати тільки з даними, що знаходяться в активному табличному просторі.

Користувач може створювати, наповнювати, змінювати, вилучати створені ним таблиці. Звичайно користувачеві може знадобитися доступ до таблиць, створених іншими користувачами. Тому адміністратор SQL-сервера повинен цей доступ надати. Це робиться так:

grant <перелік_прав> on <ім'я_власника>.<ім'я_таблиці>
to <ім'я_користувача>;

Права користувачеві можуть як надаватися, так і скасовуватися. Для цього використовується оператор Revoke з відповідними опціями. Вилучення користувача із системи відбувається за допомогою оператора Drop user.

Вище було розглянуто створення та надання прав одному користувачеві. Але досить часто, наприклад, для виконання цих задач для бухгалтерських потреб або навчання студентів виникає необхідність створення великої кількості користувачів з ідентичними правами. Це може займати досить багато часу навіть за наявності відповідних сценаріїв. Тому в СУБД Oracle8i Server передбачене розширення стандартної структурованої мови запитів SQL, що дозволяє створювати набори привілеїв і надавати або скасовувати їх за допомогою лише одного оператора. Це ролі БД. Крім того, ролі дозволяють адміністраторові БД надавати і скасовувати набори привілеїв таким чином, щоб користувач володів лише одним активним набором.

Створення ролей та надання їх користувачеві виконується так:

1) створення ролі

create role <ім'я_ролі> identified by <пароль>;

2) надання привілеїв для ролі

grant <перелік_привілеїв> to <ім'я_ролі>.

Привілеї можуть поширюватися на декілька таблиць кількох користувачів. Деякі права ролям надаватися не можуть, зокрема index, references;

3) надання ролей користувачам та їх активація

grant <ім'я_ролі> to <ім'я_користувача>.

Роль буде активізована при вході користувача в систему.

Інколи виникає потреба надати користувачеві, що працює над декількома задачами, різні набори привілеїв для кожної задачі. Тоді створюються так звані стандартні ролі. Це робиться так:

alter user <ім'я_користувача> default role <ім'я_ролі>.

З міркувань безпеки недоцільно включати до стандартного набору більш ніж одну роль, оскільки тоді права права користувача комбінуватимуться.

Вилучення ролі із стандартного набору відбувається так:

alter user <ім'я_користувача> default role none.

Користувач може сам активізовувати ролі, що належать йому. Це виконується так:

set role <ім'я_ролі>.
Аналогічно роль деактивується:

set role none.

Ще одним потужним засобом, що надає додаткових можливостей для управління відображенням інформації, є представлення. Вони дозволяють обмежувати кількість стовпчиків або рядків, з якими користувач може працювати.

Створюються представлення за допомогою оператора Select, а саме:

create view <ім'я_представлення> as
select <перелік> from <ім'я_таблиці> where <умови>.

Складність представлення залежатиме від того, як написаний оператор Select. Якщо в <перелік> вказати декілька стовпчиків, то користувач матиме доступ лише до них. Звичайно, ефективнішим з точки зору швидкодії є використання команди Grant замість представлення, проте для забезпечення доступу до певних рядків можуть використовуватися лише представлення.

Отже, використовуючи привілеї, що надаються користувачеві, ролі та представлення, можна забезпечити гнучку систему безпеки даних при роботі великої кількості користувачів у середовищі SQL-сервера (СУБД) Oracle8i Server, Release 8.1.5.

Все вищенаведене стосується захисту об'єктів БД при роботі у захищеній локальній мережі. У зв'язку з поширенням електронної комерції та розширеним використанням Web-програм обов'язки адміністратора СУБД щодо захисту даних стали значно складнішими. Мережі тепер перестали бути внутрішніми закритими зонами. Вони безпосередньо включені до мережі Інтернет, що дозволяє кожному отримувати доступ до найважливішої інформації. Для створення захищеного розподіленого обчислювального середовища використовуються засоби ASO (Advanced Security Option – розширені засоби захисту). Пакет ASO – це комплекс програмних засобів, що дозволяють забезпечити конфіденційність, цілість та доступність комп'ютерної системи.

Конфіденційність транзакцій забезпечується завдяки аутентифікації користувачів та серверів, що організовують такі транзакції. Аутентифікація користувачів забезпечується використанням паролів, а аутентифікація БД та серверів – за допомогою цифрових підписів.

Основні функціональні можливості Oracle ASO:

- шифрування даних та обчислення контрольної суми. При використанні ASO можна гарантувати безпеку даних при передаванні їх лініями зв'язку, забезпечуючи шифрування потоку даних між користувачем і сервером. Також можна захистити дані від модифікації при переміщенні між користувачем та сервером, забезпечивши передачу контрольної суми разом з пакетами даних;
- аутентифікація та вхід до системи. ASO дозволяють інтегрувати середовище Oracle з іншими засобами аутентифікації і входу в систему. Net8 підтримує адаптери для Kerberos, CyberSAFE, Identix TouchNet II та SecurID. Крім того, новий сервер Oracle Security підтримуватиме служби аутентифікації для існуючих ресурсів Oracle. Спільно зі службою SSL (Secured Socket Layer) можуть використовуватися цифрові сертифікати X.509V3;

- аутентифікація користувачів за допомогою протоколу RADIUS (Remote Authentification Dual-In User Service);
- застосування протоколу SSL;
- використання Oracle Wallet. Дана функція дозволяє керувати інфраструктурою PKI (Public Key Infrastructure).

Для шифрування даних ASO використовує стандарт RSA Data Security RC4 або DES (Data Encription Standart). Для захисту всього мережевого трафіку використовується ключ, що випадково генерується для кожного сеансу Net8.

Допустимі типи шифрування такі:

- R.C4_40: RSA RC4 (40-розрядний розмір ключа) — внутрішній та міжнародний;
- RC4_56: RSA RC4 (56-розрядний розмір ключа) — тільки внутрішній для США та Канади;
- RC4_128: RSA RC4 (128-розрядний розмір ключа) — тільки внутрішній для США та Канади;
- DES: стандарт DES (56-розрядний розмір ключа) — тільки внутрішній для США та Канади;
- DES40: DES40 (40-розрядний розмір ключа) — внутрішній та міжнародний;
- 3DES: потрійний DES з використанням SSL.

Підтримка протоколу RADIUS дозволяє використовувати разом з Oracle продукти сторонніх виробників засобів аутентифікації. Коли клієнт виконує передбачену ASO процедуру реєстрації на сервері БД, останній звертається на сервер RADIUS для аутентифікації цього запиту. Сервер RADIUS приймає або відхиляє запит. Відповідь передається на сервер БД Oracle8i, який виконує відповідні дії. Таким чином, сервер Oracle8i підтримує повністю прозору та захищену процедуру аутентифікації.

Додаткові функції ASO щодо застосування протоколу RADIUS містять використання схеми аутентифікації та обліку типу “пароль-відповідь” з такою послідовністю виконання (рис. 1):

1) сервер RADIUS передає пароль серверові додатків;
2) сервер додатків передає пароль комп’ютерові клієнта;
3) пароль відображається для кінцевого користувача;
4) користувач вносить відповідь на отриманий пароль;
5) значення відповіді повертається на сервер RADIUS;
6) сервер RADIUS порівнює отримане значення, а потім передає на сервер додатків відповідь з вказівкою прийняти або відхилити запит на сполучення з даним користувачем.

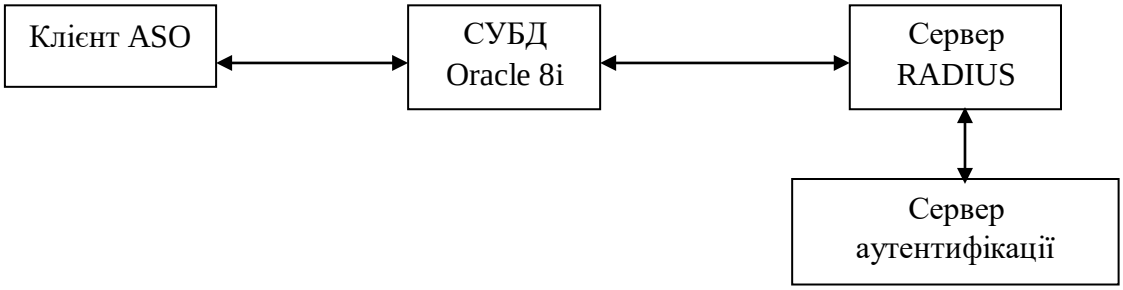


Рис. 1. Використання протоколу RADIUS у середовищі Oracle.

Підтримка протоколу SSL безпосередньо вбудована в середовище БД Oracle8i та ASO. Протокол SSL підтримує аутентифікацію з використанням цифрових сертифікатів X.509, а також шифрування мережевого трафіку. Якщо всі компоненти роботи в мережі Інтернет застосовують протокол SSL, то це забезпечує повну захищеність усіх

процесів. Основною вимогою є використання протоколу SSL усіма рівнями сеансу мережі Інтернет. А саме – рівень клієнта, рівень Web-сервера та рівень БД.

Гарантія цілості даних досягається завдяки використанню комплектів шифрів. Як клієнт, так і сервер, мають набори комплектів шифрів і спочатку домовляються, який з комплектів використовуватметься для даної транзакції (рис. 2).

При розробці системи захисту БД, до яких є доступ з мережі Інтернет, доцільно дотримуватися трирівневої схеми побудови додатків. Вона передбачає роботу з так званими "тонкими клієнтами", призначеними лише для під'єднання до Web-сервера, що самостійно встановлює з'єднання з БД (рис. 3). На ньому клієнтом БД є Web-сервер. Слід пам'ятати, що клієнтом може бути як Web-сервер, так і традиційна програма-клієнт для комп'ютера.

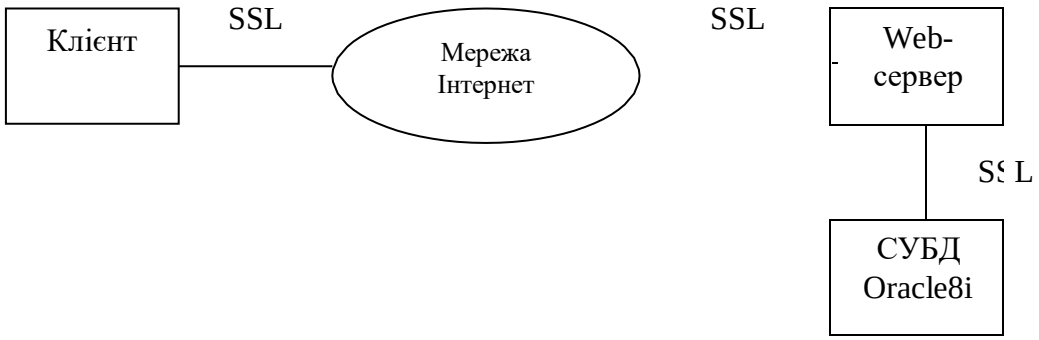


Рис. 2. Архітектура використання протоколу SSL.

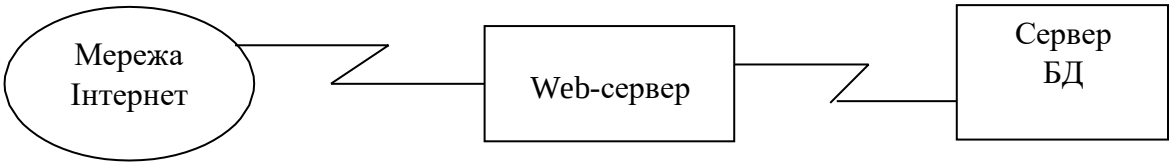


Рис. 3. Трирівнева схема побудови додатків.

Здебільшого комп'ютерний порушник, який хоче отримати конфіденційну інформацію, намагається зламати спочатку перший рівень захисту, а саме – отримати доступ до Web-сервера. Для захисту Web-серверів використовуються брандмауери. Вони призначені для ізоляції захищених об'єктів від потенційно небезпечного середовища, яким є мережа Інтернет. У типовому випадку використання брандмауерів схема передбачає його встановлення як проміжного пункту між Web-сервером та сервером БД (рис. 4).

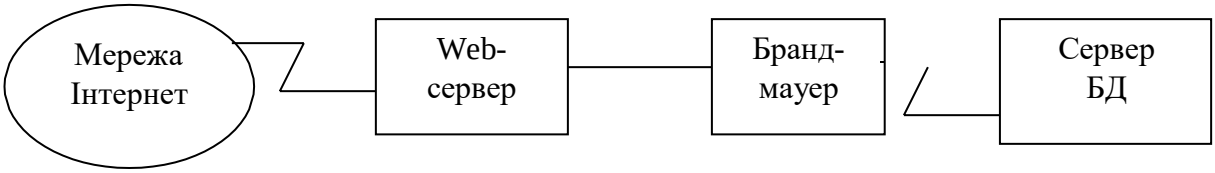


Рис. 4. Схема використання брандмауерів.

Мета використання брандмауерів:

- закриття портів, пов'язаних з обчислювальними ресурсами;
- обмеження мережевого трафіку від одного ресурсу мережі до іншого;
- обмеження щодо напрямку руху трафіка, тобто дозвіл на проходження мережевого трафіку лише в одному напрямку;
- обмеження допустимих типів взаємодії між Web-сервером та сервером БД.

Висновок: безпеку БД слід забезпечувати не тільки на рівні користувачів, а й на рівні програмних додатків та апаратного забезпечення. Середовище Oracle8i надає всі можливості для цього. Але при організації системи безпеки треба порівнювати вартість

розгортання такої системи та втрати, що виникнуть при знищенні інформації, для якої ця система може розгортатися.

*In this article some aspects of administration of the large databases with number users is considered. Also are instructions on creation of the new users and adjustment of their safe work in Oracle 8i Server environment. The opportunities of the Oracle 8i Server connected with work in open networks are shown too.*

## Література

1. Ладани Х. SQL. Энциклопедия пользователя / Пер. с англ. – К.: ДиаСофт, 1998. – 624 с.
2. Пейдж В.Дж. Использование Oracle 8™/8i™: Специальное издание / Пер. с англ. – М.: Вильямс, 1999. – 1024 с.

*Одержано 20.11.2001 р.*