7. *Нестеренко А.В.* Основы термодинамических расчётов вентиляции и кондиционирования воздуха: [Учебн. пособие]; изд. 3 доп. – М.: Высшая школа, 1971 – 460 с.
8. *Молчанов С.* Проектирование промышленной вентиляции. – Л: Стройиздат. Ленинградское отделение, 1970. – 228 с.
9. ANSYS FLUENT 12.0 User's Guide.ANSYS, Inc. is certified to ISO 9001:2008, 2009 – 2070 pp.
10. *Greenshields C.* OpenFOAM User Guide version 6. The OpenFOAM Foundation, 2018 – 237 pp.
11. Сайт Solid Works Flow Simulation https://hawkridgesys.com/solidworks/ (відкритий доступ станом на 02.10.2018)
12. Додаток до розпорядження НАЕК «Енергоатом» №137-р від 05.02.2018. Перечень разрешенных к использованию в ГП «НАЭК «Энергоатом» расчетных кодов для обоснования безопасности ядерных установок
13. *Azarenkov N.A., Rudychev V.G., Pismenetskiy S.A.* Solid and liquid waste processing and reducing of personnel doses / «Journal of Kharkiv National University»physical series «Nuclei, Particles, Fields», issue 3 /55/, 1017, 2012. – pp.117-122.
14. *Raskob W., Landman C. Trybushnyi D.* Functions of decision support systems (JRodos as an example): overview and new features and products (el source https://www.radioprotection.org/articles/radiopro/pdf/2016/03/radiopro160015-s.pdf)
15. HotSpot Health Physics Codes Version 3.0 User's Guide / National Atmospheric Release Advisory Center, LNLL, 2014 – 198 pp.
16. RASCAL 4.3 User's Guide / Ramsdell Environmental Consulting, LLC, 2013– 125 pp.
17. WinMACCS, a MACCS2 Interface for Calculating Health and Economic Consequences from Accidental Release of Radioactive Materials into the Atmosphere MACCS User's Guide / U.S. Nuclear Regulatory Commission, 2007 – 233 pp.
18. *Богорад В.І., Бєлов Я.Ю., Кириленко Ю.О.* та ін. Поєднання апаратних засобів мобільної лабораторії RanidSONNI та комп'ютерних технологій СППР RODOS для прогнозу наслідків виникнення пожежі в зоні відчуження Чорнобильської АЕС / Журнал «Ядерна та радіаційна безпека», 2018. – 3(79). – С.10-15

Поступила 17.09.2018р.

УДК 519.7-004.65

М.Ю. Комаров, Київ

ПІДСИСТЕМА УПРАВЛІННЯ ДОСТУПОМ СИСТЕМИ УПРАВЛІННЯ БАЗАМИ ДАНИХ ORACLE DATABASE 12C ENTERPRISE EDITION

Abstract. Data base; The United Energy System of Ukraine, Real Application Cluster (RAC), Automatic Control Systems.

Актуальність

Механізми безпеки інформації в системі управління базами даних (далі – СУБД) ORACLE реалізовані засобами захисту від несанкціонованого доступу

до інформації, які можуть використовуватися для реалізації функціональних послуг безпеки, описаних в НД ТЗІ 2.5-004-99.

Засоби захисту від несанкціонованого доступу до інформації реалізують ряд механізмів безпеки, що здійснюють в сукупності ідентифікацію та автентифікацію, розмежування доступу до об'єктів бази даних, реєстрацію подій і підтримку цілісності бази даних.

Постановка задачі

В даній статті пропонується провести аналіз підсистеми управління доступом СУБД ORACLE Database 12C Enterprise Edition.

Вирішення задачі

Перш ніж створити сесію СУБД завжди здійснює автентифікацію користувача.

У СУБД після стандартної установки (інсталяції) присутній деякий набір стандартних користувачів, склад якого залежить від опцій установки.

Автентифікаційні дані користувачів зберігаються в таблиці sys.user $, доступ до якої можливий тільки при вході з опцією as sysdba.

Переглянути інформацію можливо скориставшись поданням DBA_USERS. У даному поданні, складеному на підставі таблиці user $, відображені унікальні ідентифікатори та імена користувачів, однак хеш-значення їх паролів не відображаються.

При вході користувач повинен вказати ім'я, пароль та ідентифікатор екземпляра, до якого здійснює підключення. Представлений пароль перетворюється односпрямованою функцією, результат якої порівнюється з збереженим в таблиці user $ значенням.

Для виконання операцій з адміністрування екземпляру необхідно при автентифікації вказати спеціальну опцію AS SYSDBA.

Об'єкти бази даних також унікально ідентифікуються за числовим ідентифікатором, представленим в таблиці obj $ і імені об'єкта і схеми, в якій об'єкт знаходиться. Під об'єктами в даному випадку розуміються внутрішні сутності СУБД, такі як таблиці, подання, послідовності, збережені процедури і т.п. Вимоги пред'являються до ідентифікації записів і полів записів, тому в якості об'єктів ідентифікації розглядаються таблиці та подання, а також їх стовпці.

Права користувача в системі визначаються набором його привілеїв.

У СУБД виділяються два типи привілеїв.

Системні привілеї визначають права користувача на здійснення дій у системі в цілому. Прикладом такого роду привілеїв може служити CREATE SESSION або UNLIMITED TABLESPACE. Інші системні привілеї дозволяють здійснювати конкретну операцію над вказаним типом об'єктів у межах всієї бази даних. Наприклад: CREATE ANY VIEW, ALTER ANY TABLE.

Примітка:

1. CREATE SESSION – дозволяє новоствореному користувачу підключитися до бази даних.

2. UNLIMITED TABLESPACE – дозволяє користувачу використовувати необмежену кількість будь-якого табличного простору в базі даних.

3. CREATE ANY VIEW - дозволяє створити подання в будь-якій схемі.

4. ALTER ANY TABLE - дозволяє змінити будь-яку таблицю в будь-якій схемі.

Другим базовим типом привілеїв є об'єктні привілеї, що визначають права користувача щодо конкретних об'єктів БД. До об'єктних привілеїв відносяться привілеї на використання DML (Data Manipulation Language) операторів SELECT, UPDATE, INSERT і DDL (Data Definition Language) операторів ALTER, INDEX і REFERENCE. Окремо стоїть привілей EXECUTE. Привілеї INSERT і UPDATE можуть бути визначені для конкретного стовпця таблиці. При приписуванні привілеї INSERT на конкретний стовпець таблиці, у разі виконання операції, значення решти стовпців буде встановлено в NULL або значення за замовчуванням.

Примітка:

Data Manipulation Language (DML) (мова управління (маніпулювання) даними) - це сімейство комп'ютерних мов, що використовуються в комп'ютерних програмах або користувачами баз даних для отримання, вставки, видалення або зміни даних у базах даних.

Data Definition Language (DDL) (мова опису даних) - це сімейство комп'ютерних мов, що використовуються в комп'ютерних програмах для опису структури баз даних.

Поширеним механізмом управлінням доступом є подання (views). Подання містять дані, вибрані з однієї або декількох таблиць.

В рамках сесії користувач має всі системні і об'єктні привілеї, якими він наділений безпосередньо, а також привілеї суб'єкта PUBLIC і привілеї, якими володіють приписані йому ролі за замовчуванням. У ході роботи набір привілеїв може змінюватися у зв'язку з активацією або відключенням конкретної ролі, виконанням збереженої процедури або тригера. При створенні користувача, він не має привілеїв. Користувач автоматично отримує всі об'єктні привілеї до всіх об'єктів у своїй схемі. Об'єктні привілеї до об'єкта або його синоніму еквівалентні. Коли синонім видаляється, привілеї до об'єкта схеми залишаються в силі.

Примітка: PUBLIC – вказує що, системні повноваження, що визначені адміністратором надаються всім користувачам.

Інформація про привілеї зберігається в таблицях sysauth $ і objauth $.

Привілеї можуть безпосередньо даватися користувачеві операцією GRANT, або можуть попередньо групуватися в ролі, і вже ролі приписуватися користувачеві. Роль є пойменований набір привілеїв. Привілеї можуть бути як об'єктними, так і системними. Переглянути список привілеїв, асоційованих із суб'єктом (користувачем або роллю) можна через уявлення DBA_SYS_PRIVS, DBA_TAB_PRIVS і dba_role_privs.

Примітка: GRANT – оператор, який надає користувачам повноваження і ролі.

З метою зручності адміністрування передбачена можливість приписування ролі іншій ролі. Додатковий рівень контролю доступу вводиться ролями, що включаються за паролем. Для отримання привілеїв, пов'язаних з такими ролями, користувач повинен в рамках сесії явним чином активувати роль, вказавши пов'язаний з нею пароль. За замовчуванням, існують три визначені ролі:

- Connect володіє тільки привілеєм create session і дозволяє підключатися до системи;
- Resource володіє привілеями зі створення базових об'єктів;
- DBA містить всі системні привілеї з опцією WITH GRANT OPTION.

Примітка:

CREATE SESSION – привілей, якого повинні отримати всі користувачі без винятку, оскільки це право на відкриття сеансу зв'язку з сервером СУБД.

WITH GRANT OPTION – вказує, суб'єкту безпеки, що отримує дозвіл, дана можливість надання певних дозволів іншим обліковим записам безпеки.

Інформація про розмежування доступу зберігається в наступних таблицях (у табл. 1 наведені деякі з назв стовпців).

Таблиця 1

Назви стовпців

Назва	Примітка
User$	User # (код користувача) Name (ім'я користувача) Password (хеш пароля)
Profile$	Profile # (ідентифікатор профілю) Resource # (ідентифікатор ресурсу) Type # (тип ресурсу) Limit # (граничне значення ресурсу)
Profname$	Profile # (ідентифікатор профілю) Name (ім'я профілю)
Resource_map	У цій таблиці задається відображення ідентифікатора ресурсу на його ім'я, наприклад, 0 Failed_login_attempts
Sysauth$	Grant # (код користувача) Privilege # (ідентифікатор привілеї)
System_privilege_map	У цій таблиці задається відображення ідентифікатора системних привілеїв на їх ім'я
Objauth$	Obj # (ідентифікатор об'єкта) Grantor # (суб'єкт, що наділив привілеєм) Grant # (суб'єкт, наділений привілеєм) Privilege # (ідентифікатор привілеї) Col # (ідентифікатор стовпця)
Col$	Інформація про стовпцях.
Table_privilege_map	У таблиці задається відображення ідентифікатора об'єктних привілеїв на їх ім'я
Dba_roles	Подання містить існуючі в БД ролі
Role_Role_privs	Подання містить ролі предписані ролям

Беручи до уваги, що кожен суб'єкт і об'єкт унікальним чином ідентифікується СУБД, можливо сформулювати наступне:

Контроль доступу до об'єктів БД здійснюється на підставі ідентифікатора користувача, ідентифікатора власника об'єкта, системних і об'єктних привілеїв даного сеансу.

При розмежуванні доступу реалізуються наступні правила:

- якщо користувач є власником об'єкта, то доступ дозволяється;
- якщо системні і (або) об'єктні привілеї дозволяють виконання операції, то доступ дозволяється;
- якщо користувачеві приписана роль DBA, то доступ дозволяється;
- користувач може надати іншому суб'єкту об'єктний привілей, тільки якщо йому такий був надано з опцією with grant option або він є власником об'єкта;
- користувач може надати іншому суб'єкту системний привілей (або відкликати його), тільки якщо:
    - користувачеві приписана роль DBA;
    - користувач має привілей GRANT ANY PRIVILEGES;
    - користувачеві даний системний привілей був надано з опцією WITH ADMIN OPTION.

Примітка:

GRANT ANY PRIVILEGES – дозволяє користувачу надавати системні привілеї, навіть якщо він сам ними не володіє.

WITH ADMIN OPTION – дозволяє користувачу, який отримав системні повноваження і роль надавати їх надалі іншими користувачам або ролям. Таке рішення зокрема включає і можливість зміну або видалення ролі.

Налаштування формату паролів визначається характеристиками профілю DEFAULT, який за замовчуванням зв'язується з кожним користувачем. За умовчанням в базі даних існують два профілі DEFAULT і WKSYS_PROF, описані в таблицях profile $, profname $ і resource_map. Зокрема, у профілях визначаються деякі параметри, пов'язані з форматом парольної політики.

Шляхом прямої модифікації таблиць можливо встановити в профілях необхідні значення. Альтернативним підходом є створення нового профілю, в числі іншого, що встановлює формат парольної політики, і приписування його користувачам, що створюються.

Скрипт $ ORA_HOME / RDBMS / Admin / utlpwdmg.sql містить опис функції verify_function. Ця функція визначає деякі обмеження, що накладаються на пароль, зокрема:

- пароль не повинен співпадати з ім'ям користувача;
- не повинен співпадати з визначеним словом;
- повинен містити, щонайменше, один символ, одну цифру і один спецсимвол;
- повинен відрізнятися від попереднього не менш ніж у трьох позиціях;
- його довжина не повинна бути менше 4 символів.

У цьому ж скрипті задаються параметри профілю, що визначають період дії пароля, кількість невдалих спроб входу до блокування і т.п.

При створенні клієнтської сесії інформація про неї заноситься в службові таблиці, на базі яких формується подання V $ SESSION. Це подання зокрема містить NetBIOS ім'я клієнтської машини і ім'я домену / робочої групи. Крім того, отримати ідентифікатор клієнтської машини дозволяють визначені налаштування аудиту.

Опціональний компонент Oracle Database Vault (далі – ODV) дозволяє створювати в рамках БД СУБД області, що захищаються (realms), доступ до об'єктів у яких може бути обмежений для будь-яких користувачів, включаючи користувачів, яки володіють адміністративними привілеями в системі. Таким чином, можливо захистити збережені в базі дані від доступу з боку адміністратора, зберігши при цьому для нього можливість управління БД.

При розмежуванні доступу Database Vault оперує наступними сутностями:

- область, що захищається (realm) – функціональна група об'єктів бази даних, доступ до яких повинен бути обмежений. Наприклад, можливо згрупувати схеми, об'єкти і ролі, яки пов'язані з управління кадрами;
- правило виконання команд (command rule) – спеціальне правило, що дозволяє управляти виконанням користувачами всіх типів виразів: DDL і DML виразів, а також запитів SELECT. Об'єднуються в набори правил;
- фактор (factor) – іменована змінна або атрибут, які Database Vault здатний розпізнати і використовувати при перевірці доступу. Як фактор можуть виступати: IP адреса станції клієнта, ім'я користувача і т.д. Фактори можуть використовуватися для обмеження підключення до СУБД, або для створення логіки, що обмежує доступність даних;
- набір правил (rule set) – сукупність одного або більше правил, які можуть бути асоційовані з областю, що захищається, правилом команд або приписуванням фактора. Підсумкове значення набору правил («TRUE» або «FALSE») базується на обчисленні кожного правила і типі набору (All true або Any true). Правило в наборі являє собою PL/SQL вираз повертає «TRUE» або «FALSE»;
- безпечна роль додатку (Secure application role) – спеціальна роль БД, яка може бути активізована на підставі набору правил.

Примітка: PL/SQL (Procedural Language / Structured Query Language) - мова програмування, процедурне розширення мови SQL, розроблене корпорацією Oracle. Базується на мові Ада.

Для підтримки перерахованих сутностей ODV надає набір PL/SQL інтерфейсів і пакетів. Нижче перераховуються адміністративні інтерфейси ODV.

Oracle Datavault Administrator (DVA) – Java програма, яка побудована на

прикладному програмному інтерфейсі (API) ODV. За допомогою цієї програми адміністратори безпеки мають можливість керувати розмежуванням доступу через зручний графічний інтерфейс. Крім того, DVA надає набір звітів з безпеки, що розширюють стандартні можливості аудиту БД. Через інтерфейс DVA конфігурується політика розмежування доступу в термінах сутностей ODV.

Oracle Database Vault Configuration Assistant – утиліта командного рядка, що дозволяє виконувати операції з встановленим екземпляром ODV.

Схема DVSYS зберігає різного роду об'єкти БД (ролі, подання, функції і т.д.) необхідні для роботи ODV.

Схема DVF зберігає функції для обчислення в режимі реального часу значень факторів.

ODV містить набір PL/SQL пакетів, які дозволяють адміністратору СУБД або розробнику налаштовувати політику розмежування доступу потрібним чином.

Oracle Database Vault Reporting and Monitoring Tools дозволяє створювати звіти по різним типам активності. Крім того можливо відслідковувати зміну політик, конфігурації БД і спроби НСД до областей, що захищаються.

Процедура інсталяції ODV змінює деякі ініціалізацій параметри екземпляра СУБД з метою забезпечити його більшу захищеність. У табл. 2 перераховані параметри, вказані у файлі Init.ora, яки змінюються при установці опції ODV.

Таблиця 2

Параметри у файлі Init.ora

Ім'я параметра	Значення за замовчуванням	Значення після встановлення ODV	Примітка
AUDIT_SYS_ OPERATIONS	FALSE	TRUE	Ініціалізаційний параметр, відповідальний за включення аудиту для користувача SYS і користувачів мають привілеї SYSDBA і SYSOPER
OS_AUTHEN T_PREFIX	Ops$	Null	строковий параметр - це префікс що додається сервером СУБД до імені користувача при зіставленні імен.
OS_ROLES	None	FALSE	Якщо OS_ROLES =TRUE, то призначеннями ролей всім користувачам бази даних повністю управляє операційна система. Всі спроби відкликання ролей, призначених операційної

			системою, ігноруються, так само, як і будь-які ролі, призначені до цього. Значення FALSE, змушує ідентифікувати і управляти ролями базу даних
REMOTE_OS_AUTHENT	FALSE	FALSE	Ініціалізаційний параметр, при значенні TRUE надає довірчу модель мережевої автентифікації, користувачі, що мають облікові записи операційної системи можуть отримувати доступ до бази даних. Таким чином вся відповідальність автентифікації лягає на операційну систему
REMOTE_OS_ROLES	FALSE	FALSE	Параметр вказує, чи дозволено віддаленим клієнтам використовувати ролі операційної системи. Коли встановлено FALSE, СУБД визначає ролі для віддалених клієнтів і управляє цими ролями.
SQL92_SECURITY	FALSE	TRUE	Параметр визначає, чи повинен бути у користувача привілей SELECT на таблицю, при виконанні операторів UPDATE або SELECT.

Процедура інсталяції ODV також вносить зміни до складу деяких ролей за замовчуванням з метою реалізації розподілу адміністративних повноважень. У табл. 3 нижче наведений список змінених ролей та перелік привілеїв, з цих ролей відкликаних (видалених).

Таблиця 3

Список змінених ролей та перелік привілеїв

Ролі	**Привілеї**
DBA	BECOME USER (дозволяє ставати іншим користувачем (потрібна при імпорті БД)); SELECT ANY TRANSACTION (дозволяє працювати з будь якою транзакцією); CREATE ANY JOB (дозволяє створювати, змінювати і видаляти завдання, графіки і програм у будь-якій схемі, крім SYS); CREATE EXTERNAL JOB (створення робочих місць, які працюють за

	межами бази даних -ОС); EXECUTE ANY PROGRAM (дозволяє в планових завданнях використовувати програми з будь-якій схемі); EXECUTE ANY CLASS (дозволяє в планових завданнях використовувати будь яки класи роботи); MANAGE SCHEDULER (дозволяє створювати, змінювати і видаляти класи роботи, також дозволяє встановлювати і отримувати атрибути планувальника завдань); DEQUEUE ANY QUEUE (керування чергами); ENQUEUE ANY QUEUE (керування чергами); MANAGE ANY QUEUE (керування чергами);
PUBLIC	EXECUTE ON UTL_FILE (доступ до файлової системи ОС)
SYS	ALTER USER (дозволяє зміну параметрів для будь-якого користувача (пароль, кількість доступного табличного простору, призначений профіль і т.п.)); DROP USER (дозволяє видалити іншого користувача);
SYSTEM	ALTER USER (дозволяє змінювати параметри для будь-якого користувача (пароль, кількість доступного табличного простору, призначений профіль і т.п.)); DROP USER (дозволяє видалити іншого користувача); CREATE USER (дозволяє створювати користувачів, встановлювати квоти в будь-якому табличному просторі, встановлювати табличний простір за замовчуванням і тимчасовий табличний простір, надавати профілі).

Крім того, привілеї ALTER, CREATE a DROP PROFILE відкликаються (видаляються) у користувачів SYS і SYSTEM і присвоюються ролі DV_ACCTMGR.

Висновки

Проведено аналіз підсистеми управління доступом системи управління базами даних Oracle Database 12C Enterprise Edition.

За результатами проведеного аналізу встановлено, що:

- СУБД дозволяє створювати та ідентифікувати адміністраторів та користувачів з різними правами доступу до об'єктів СУБД для забезпечення зменшення потенційних збитків від навмисних або помилкових дій користувачів та обмеження авторитарності керування СУБД.

- СУБД реалізує механізми, яки забезпечують розмежування доступу користувачів до об'єктів СУБД на підставі привілеїв.

Отримані результати дозволяють констатувати можливість застосування СУБД Oracle Database 12C Enterprise Edition як основу для побудови ГІС-систем на етапах проведення науково-дослідних робіт, проектування і виготовлення устаткування енергетичних систем, його подальшого монтажу і пуско-налагоджувальних робіт.

1. *В.А. Гуреев, В.Н. Сулейманов, О.В. Сулейманова, Н. Реза*. Принципы построения информационной части модели электроэнергетики Украины. // Электропанорама, № 12, 2011.
2. *Гуреев В.А., Сулейманова О.В*. Разработка архитектуры мини базы знаний противоаварийных тренировок // Энергетика и электрификация. 1987. – № 1, С.44-46.
3. *Гуреев В.А., Редковский Н.Н., Суманенков В.Г*. Информационная технология управления сложными распределенными техническими системами. // Информационные технологии и новейшее применение теории управления (Автоматика-94): Тез. докл. 1-й Украинской конф. по авт. упр. – К.: 1994. – Ч. 1, С.230-231.
4. *Рик Гринвальд, Роберт Стаковьяк, Джонатан Стерн.* Oracle11g. Основы – Символ-Плюс, 2009. – 464 с.
5. *С. Фейерштейн, Б. Прибыл.* Oracle PL/SQL. Для профессионалов – Питер, 2011. – 800 с.
6. Oracle® SQL Developer User's Guide.

Поступила 10.09.2018р.

УДК 621.311.68

О.М. Шам, Київ

РОЗРАХУНОК ПАРАМЕТРІВ АВТОНОМНОЇ ОСВІТЛЮВАЛЬНОЇ УСТАНОВКИ ВУЛИЧНОГО ОСВІТЛЕННЯ

Abstract. The article presents the calculation of the parameters of the autonomous system of street lighting based on solar panels. Show the advantages and disadvantages of these systems.

Вступ

Рівень енергоспоживання постійно зростає, тому гостро постає проблема нестачі енергетичних ресурсів, а електричні мережі наразі не можуть скрізь забезпечити стабільність енергопостачання, та якість параметрів електричної енергії. Одним з варіантів вирішення цієї проблеми є створення власних систем енергозабезпечення для таких споживачів з використанням відновлювальних джерел енергії.

Великий відсоток електроенергії припадає на потреби вуличного освітлення, яке до того ж, має низький рівень автоматизації. Для вирішення цієї задачі пропонується модернізація вуличного освітлення, шляхом впровадження автономних систем живлення на базі фотоелектричних перетворювачів (рис. 1). Це дозволить знизити навантаження на електричну мережу, підвищити якість освітлення, та організувати зовнішнє освітлення у важкодоступних районах, без необхідності прокладки ліній електропередач.

