



## **ИНСТИТУТ ИНТЕЛЛЕКТУАЛЬНЫХ КИБЕРНЕТИЧЕСКИХ СИСТЕМ**

### **Кафедра №42 «Криптология и кибербезопасность»**

---

*Федеральное государственное автономное образовательное  
учреждение высшего образования*

**«Национальный исследовательский ядерный университет «МИФИ»»**

**ЛАБОРАТОРНАЯ РАБОТА №2-4:**

**«Аутентификация и базовый контроль доступа.»**

Аверин Владислав

Группа: Б19-505

Ноябрь, 2022

## Содержание

1. SCHEMA-ONLY пользователь .....	4
2. Аутентификация средствами ОС .....	7
3. Аутентификация посредством радиус-сервера .....	10
4. Использование представлений для разграничения доступа .....	14
Выводы: .....	16

## *Цель работы*

Рассмотреть различные подходы к аутентификации пользователей. Рассмотреть примитивные механизмы разграничения доступа к столбцам и записям базы данных.

## *Ход работы*

1. Создать schema-only пользователя, добавить один или несколько объектов в его схему данных, убедиться в их успешном создании и работоспособности. Обосновать, почему (не) планируется использовать пользователя такого типа для хранения объектов базы данных в разрабатываемой схеме;
2. Создать пользователя, проходящего аутентификацию средствами операционной системы. Важно: имя пользователя должно начинаться с OS AUTHENT PREFIX (по умолчанию 'OP\$'). Если работа выполняется с учётной записи администратора, необходимо создать ещё одну учётную запись в операционной системе, так как административная учётная запись уже связана с SYSDBA;
3. (дополнительное кармическое задание) Развернуть RADIUS-сервер. Создать пользователя, который проходит аутентификацию посредством RADIUS-сервера. Важно: настройки сервера СУБД для работы с RADIUS-сервером могут конфликтовать с настройками для аутентификации средствами операционной системы. Необходимо убедиться, что возможно войти в учётную запись администратора без использования этого механизма;
4. Ограничить доступ пользователей/ролей к особо важным данным за счёт использования представлений. Убедиться в работоспособности решения;
5. Оформить отчёт.

## 1. SCHEMA-ONLY пользователь

Пользователь данной категории хоть и может иметь привилегии на подключение, но, по сути, не может подключаться к БД, т.к. для него не настроено ни одного способа аутентификации.

Порядок действий (не уверен, что верный, но вроде работает):

1. Создание обычного пользователя и выдача ему необходимых для администрирования собственных таблиц привилегий:

```
SQL> CREATE USER lab24 IDENTIFIED BY 1234
      QUOTA UNLIMITED ON users;

SQL> GRANT CREATE SESSION, CREATE TABLE TO lab24;
```

Подключение к нему и создание от его лица таблицы, с выдачей необходимых привилегий другому пользователю:

```
SQL> CREATE TABLE ExampleT (
      some_id NUMBER(3,0) NOT NULL,
      info VARCHAR2(100),
      CONSTRAINT lab24_pk PRIMARY KEY (some_id)
    );

SQL> GRANT
      SELECT,
      INSERT,
      DELETE
      ON ExampleT TO Skinner;
```

Как видно, привилегий ALTER и DROP TABLE у схемы Skinner нет, поэтому сторонний пользователь сможет только модифицировать данные таблицы, но не саму таблицу:

```
SQL> INSERT INTO LAB24.examplet (some_id, info)
      VALUES (5, '234rew');

1 row inserted.

SQL> DROP TABLE lab24.ExampleT;
```

```
Error starting at line : 6 in command -
DROP TABLE lab24.ExampleT
Error report -
ORA-01031: привилегий недостаточно
01031. 00000 - "insufficient privileges"
*Cause:      An attempt was made to perform a database operation without
              the necessary privileges.
*Action:      Ask your database administrator or designated security
              administrator to grant you the necessary privileges
```

Меняем от лица sysdba режим

```
connect Query Builder
ALTER USER lab24 NO AUTHENTICATION;
```

User LAB24 altered.

40	SYS\$UMF	EXPIRED & LOCKED	11G 12C	PASSWORD
41	LAB24	OPEN	(null)	NONE
42	MORGAN	OPEN	11G 12C	PASSWORD

Попытки подключиться приведут к ошибке пароля: способа аутентификации (и самого пароля) то нет

```
SQL> conn lab24/somepasswd
ERROR:
ORA-01017: неверный логин/пароль; неверный логин/пароль

Warning: You are no longer connected to ORACLE.
SQL> _
```

(Note: насколько я понял, к нему можно подключаться через CONNECT THROUGH: но опять же, для этого нужны соответствующие привилегии, которых ни у кого, кроме sysdba по идее, быть не должно.)

Механизм schema-only пользователя, насколько я понимаю, введен для обеспечения безопасности. Если каждая схема пользователя может владеть совокупностью объектов, а каждый объект должен принадлежать какой-либо схеме (а-ля один ко многим), то при несанкционированном доступе к данной схеме (даже простым брутотом пароля, если

администратор неправильно настроил СУБД и IDS) злоумышленник может просто удалить таблицу и возможно ее бекапы (хотя, удалить все данные из самой таблицы все еще никто не мешает). Централизованное же управление всеми объектами сужает вектор атаки: возможность поломки данных и самой БД появляется только при взломе данного пользователя или sysdba. И если в случае с sysdba уже класть на всю защиту, это фактически полный доступ ко всему, то исключение подключения к владеющей таблицами схеме уменьшает этот вектор до одного администратора. А взломать schema-only пользователя нельзя: в него технически нельзя зайти, пока это не изменит системный администратор. Правда, непонятно, почему все таблицы в таком случае не создавать от имени sysdba, если все равно его взлом означает полный контроль над БД (можно просто изменить AUTHENTICOM для schema-only пользователя и подключиться к нему). Возможно, дело в квоте памяти и производительности, а также для удобства, когда таблиц слишком много и они загромождают пространство главного администратора. Поэтому если предположить, например, что администратор управляет сразу несколькими БД, то для сегментации памяти каждой базы данных логичнее было бы создать своих schema-only пользователей.

Более того, обеспечение частичного доступа к объектам для всех пользователей системы защищает кроме как атак извне, и от атак изнутри. Если какой-либо инсайдер из числа доверенных лиц (если не брать самого системного администратора) окажется очень “хорошим” (или очень криворуким) человеком, то навредить самим объектам настолько критично (будь то хоть бекапы или индексы с различными ролями) он не сможет.

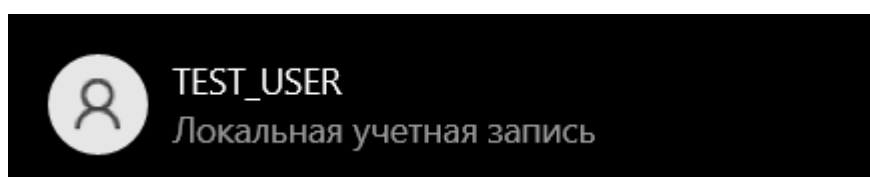
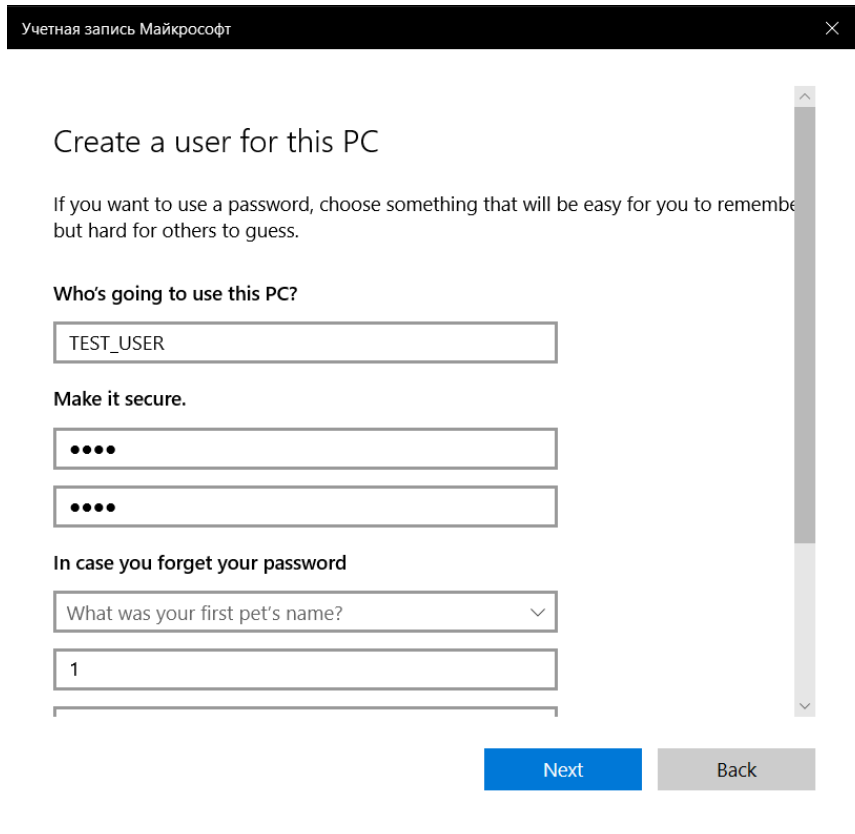
Механизм включения привилегий входа в систему, насколько я знаю, организованы во многих других продуктах, будь то разные ОС, другие СУБД или сервера. Но за достаточно простой структурой БД использование таких пользователей в наших лабах не видится рентабельным (я и с наличием schema-only пользователя все равно справлюсь с поломкой СУБД :))

## 2. Аутентификация средствами ОС

Информация взята из: <https://oracle-base.com/articles/misc/os-authentication>

Для реализации доступа средствами операционной системы, создадим нового пользователя в Windows:

ВАЖНО! Лично у меня не получалось подключиться к пользователю, если его имя было указано в lowercase. Скорее всего это из-за того, что внутри БД пользователи хранятся в верхнем регистре.



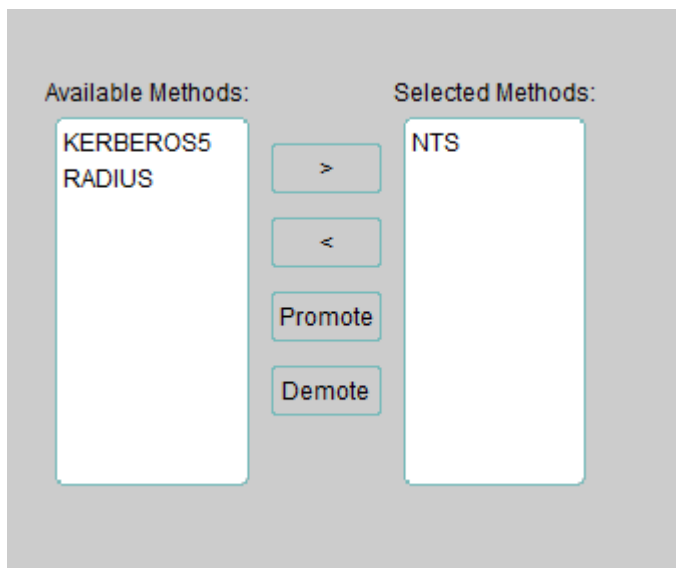
Проверим значение параметра инициализации для аутентификации средствами ОС:

```
-SQL> SHOW PARAMETER os_authent_prefix
```

NAME	TYPE	VALUE
os_authent_prefix	string	OPS\$

```
SQL>
```

Проверим x2, что способ аутентификации NTS (раз мы используем Windows) активен:



Ну или прописать напрямую в файле:

```
# sqlnet.ora Network Configuration File: C:\app\vladi\product\18.0.0\dbhomeXE\NETWORK\ADMIN\sqlnet.ora
# Generated by Oracle configuration tools.

# This file is actually generated by netca. But if customers choose to
# install "Software Only", this file wont exist and without the native
# authentication, they will not be able to connect to the database on NT.

SQLNET.AUTHENTICATION_SERVICES= (BEQ, TCPS, NTS)

ADR_BASE = C:\app\vladi\product\18.0.0\dbhomeXE\log
```

Проверим x3, что выбран контейнер XEPDB1, т.к. при использовании NTS (вход по “sqlplus / as sysdba” он автоматом перекидывает в корневой контейнер):

```
SQL> show con_name

CON_NAME
-----
CDB$ROOT
SQL> ALTER SESSION SET CONTAINER=XEPDB1;

Session altered.

SQL> show con_name

CON_NAME
-----
XEPDB1
SQL>
```



И только теперь можем создавать пользователя с именем: "OPS\$DOMAIN-NAME\TEST\_USER"; вместо DOMAIN\_NAME в случае, если компьютер (пользователь) находится не в домене, указывается имя компьютера:

```
SQL> CREATE USER "OPS$DESKTOP-F1F19FM\TEST_USER" IDENTIFIED EXTERNALLY;
User created.

SQL> GRANT CREATE SESSION TO "OPS$DESKTOP-F1F19FM\TEST_USER";
Grant succeeded.

SQL> _
```

Зайдем из-под имени TEST\_USER и проверим, что оно так работает:

```
C:\Users\TEST_USER>sqlplus /

SQL*Plus: Release 18.0.0.0.0 - Production on Fri Dec 2 16:16:20 2022
Version 18.4.0.0.0

Copyright (c) 1982, 2018, Oracle. All rights reserved.

Connected to:
Oracle Database 18c Express Edition Release 18.0.0.0.0 - Production
Version 18.4.0.0.0

SQL> show user
USER is "OPS$DESKTOP-F1F19FM\TEST_USER"
SQL> _
```

### 3. Аутентификация посредством радиус-сервера

Изначально меня почему-то переклинило на то, что в задании было написано про IDENTIFIED GLOBALLY (т.е. про вход через Windows AD). А так как мы уже делали в этом семестре по одной из дисциплин, связанных с разворачиванием домена в Microsoft Active Directory, то я начал пытаться развернуть на том windows server радиус сервер, и добавить СУБД туда. Спойлер: ниче не вышло :-). Ибо в лабораторной у нас была только самая тривиальная последовательная настройка домена для мартышек (чтобы познакомиться с СЗИ Secret Net Studio). Поэтому не мудрствуя лукаво я просто взял свою старую гостевую Убунту и конечно же сам, без помощи всяких запрещенных BitTorrent порталов, которыми пользоваться категорически нельзя и вообще, пиратство это плохо (тем более, что по факту, никаких прав нарушено не было), поднял гостевую ОС Oracle Linux 8.5 с установленной и настроенной Oracle EX 21с. Обе ОС (и убунту, и Оракл) запускались через гипервизор Virtual Box с настройками сетевого моста (просто чтобы они могли видеть друга). В качестве радиус сервера был выбран FreeRADIUS. Собственно, информация для установки и конфигурировании серверов оракла и freeradius была взята из документации и еще пары источников ниже (Спойлер x2: из задания ниче не вышло x2, так что можно Зий пункт пропускать :-)):

<https://docs.oracle.com/database/121/DBSEG/asoradus.htm#DBSEG9633>

<https://www.dmosk.ru/miniinstruktions.php?mini=freeradius-centos8>

<https://blog.pythian.com/using-freeradius-to-authorize-oracle-connections/>

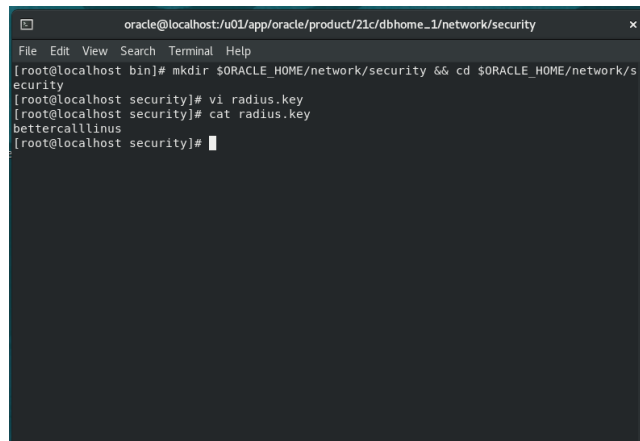
#### 1. Настройка радиус-сервера.

Для начала нужно было установить на обе машины freeradius (на oracle linux еще freeradius-utils, хотя может и не надо было). После добавим какого-нибудь пользователя в /etc/raddb/users и новый хост (нашу гостевую убунту) в /etc/raddb/clients.conf (в большинстве rpm ориентированных сборок freeradius лежит в /etc/freeradius/'номер версии'/, но в оракле почему-то была просто папка etc/raddb):

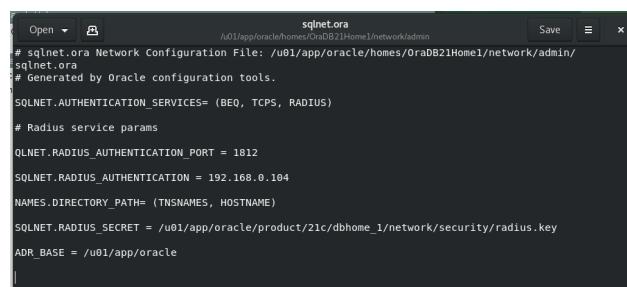


## 2. Конфигурация Радиус авторизации на сервере СУБД Oracle (да-да, дословный перевод названия 2ого пункта из документации оракла)

Собственно, делаем то, что написано в первых двух пунктах: добавляем в SQLNET.AUTHENTICATION\_SERVICES метод аутентификации RADIUS и radius.key секрет нашего созданного пользователя.



```
oracle@localhost:/u01/app/oracle/product/21c/dbhome_1/network/security
File Edit View Search Terminal Help
[root@localhost bin]# mkdir $ORACLE_HOME/network/security && cd $ORACLE_HOME/network/s
ecurity
[root@localhost security]# vi radius.key
[root@localhost security]# cat radius.key
bettercallilinus
[root@localhost security]#
```



```
sqlnet.ora
/u01/app/oracle/homes/oraDB21Home1/network/admin/
# sqlnet.ora Network Configuration File: /u01/app/oracle/homes/oraDB21Home1/network/admin/
# Generated by Oracle configuration tools.

SQLNET.AUTHENTICATION_SERVICES= (BEQ, TCPS, RADIUS)

# Radius service params
SQLNET.RADIUS_AUTHENTICATION_PORT = 1812

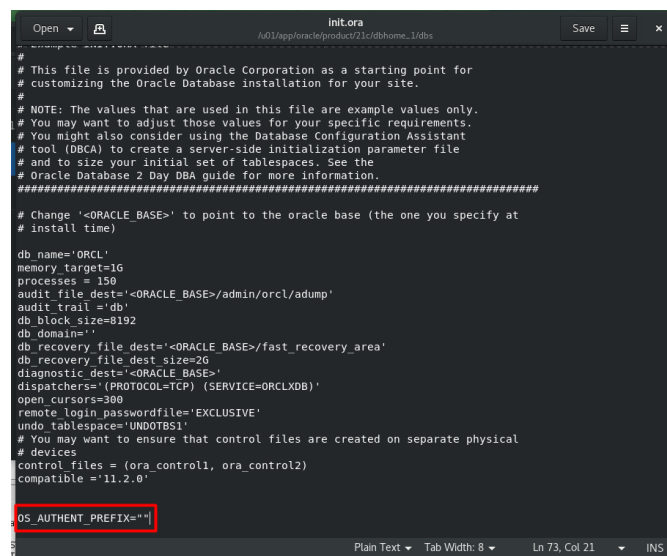
SQLNET.RADIUS_AUTHENTICATION = 192.168.0.104

NAMES.DIRECTORY_PATH= (TNSNAMES, HOSTNAME)

SQLNET.RADIUS_SECRET = /u01/app/oracle/product/21c/dbhome_1/network/security/radius.key

ADR_BASE = /u01/app/oracle
```

Добавляем параметр аутентификации:



```
init.ora
/u01/app/oracle/product/21c/dbhome_1/dbs

# This file is provided by Oracle Corporation as a starting point for
# customizing the Oracle Database installation for your site.
#
# NOTE: The values that are used in this file are example values only.
# You may want to adjust those values for your specific requirements.
# You might also consider using the Database Configuration Assistant
# tool (DBCA) to create a server-side initialization parameter file
# and to size your initial set of tablespaces. See the
# Oracle Database 2 Day DBA guide for more information.
#
#####
# Change '<ORACLE_BASE>' to point to the oracle base (the one you specify at
# install time)

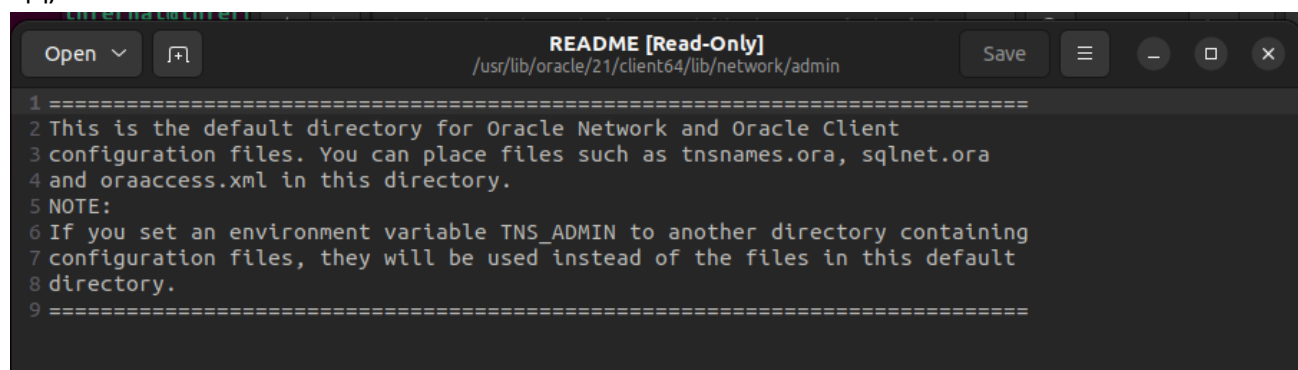
db_name='ORCL'
memory_target=1G
processes = 150
audit_file_dest='<ORACLE_BASE>/admin/orcl/adump'
audit_trail = 'db'
db_block_size=8192
db_domain=''
db_recovery_file_dest='<ORACLE_BASE>/fast_recovery_area'
db_recovery_file_dest_size=2G
diagnostic_dest='<ORACLE_BASE>'
dispatchers='(PROTOCOL=TCP) (SERVICE=ORCLXDB)'
open_cursors=300
remote_login_passwordfile='EXCLUSIVE'
undo_tablespace='UNDOTBS1'
# You may want to ensure that control files are created on separate physical
# devices
control_files = (ora_control1, ora_control2)
compatible = '11.2.0'

OS_AUTHENT_PREFIX='#'
```

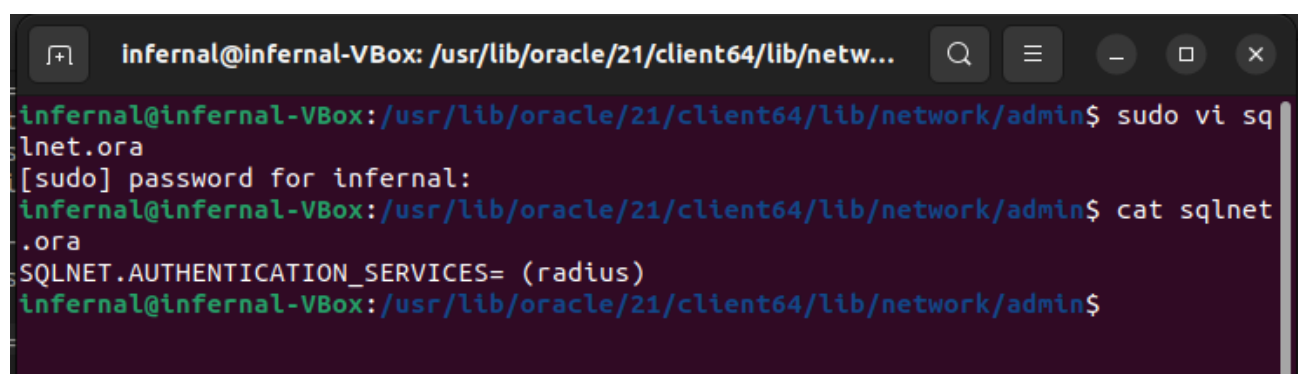
Устанавливаем Oracle Instant Client на Ubuntu:

<https://www.foxinfotech.in/2019/03/how-to-install-sqlplus-in-linux-ubuntu.html>

Единственное, что немного отличается от этого мануала, это то, что самого файла sqlnet.ora по умолчанию не было (с другой стороны, откуда ему там взяться без установленного экземпляра БД):

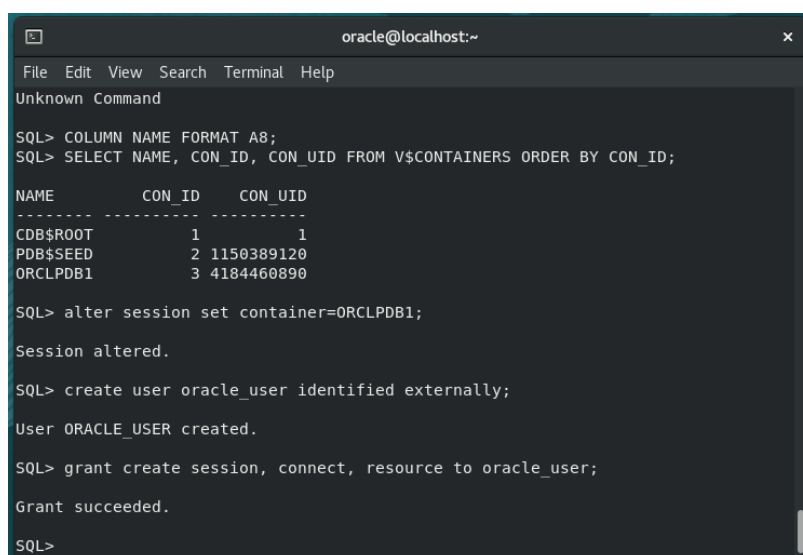


```
1 =====
2 This is the default directory for Oracle Network and Oracle Client
3 configuration files. You can place files such as tnsnames.ora, sqlnet.ora
4 and oraaccess.xml in this directory.
5 NOTE:
6 If you set an environment variable TNS_ADMIN to another directory containing
7 configuration files, they will be used instead of the files in this default
8 directory.
9 =====
```



```
infernal@infernal-VBox: /usr/lib/oracle/21/client64/lib/netw...
infernal@infernal-VBox:/usr/lib/oracle/21/client64/lib/network/admin$ sudo vi sq
lnet.ora
[sudo] password for infernal:
infernal@infernal-VBox:/usr/lib/oracle/21/client64/lib/network/admin$ cat sqlnet
.ora
SQLNET.AUTHENTICATION_SERVICES= (radius)
infernal@infernal-VBox:/usr/lib/oracle/21/client64/lib/network/admin$
```

Теперь создаем пользователя для авторизации с параметром IDENTIFIED EXTERNALLY:



```
oracle@localhost:~
File Edit View Search Terminal Help
Unknown Command

SQL> COLUMN NAME FORMAT A8;
SQL> SELECT NAME, CON_ID, CON_UID FROM V$CONTAINERS ORDER BY CON_ID;

NAME          CON_ID  CON_UID
-----
CDB$ROOT       1         1
PDB$SEED       2 1150389120
ORCLPDB1       3 4184460890

SQL> alter session set container=ORCLPDB1;
Session altered.

SQL> create user oracle_user identified externally;
User ORACLE_USER created.

SQL> grant create session, connect, resource to oracle_user;
Grant succeeded.

SQL>
```

И.... Дальше я просто запутался (На самом деле, у меня возникли проблемы с самим freeradius, и я в течение написания этих лаб поломал свою убунту, так что я просто сдался)

Далее, по идее, нужно настроить freeradius на работу с oracle, поднять какой-нибудь веб-интерфейс (через апач или нджинкс), но скорее всего, не в этом семестре, простите :(

#### 4. Использование представлений для разграничения доступа

Создадим для примера представление, ограничивающее доступ к данным для пользователей, которые являются бухгалтерами. Например, им незачем знать подробности дел (будем считать, что им нужна только информация о статусе дела и связанных датах), поэтому атрибут уровня доступа и ссылки на дело можно скрыть от них:

```
CREATE OR REPLACE VIEW cases_view AS
SELECT Cases.case_id, Cases.case_name, StatusStates.description, Cases.start_date, Cases.close_date
FROM Cases
INNER JOIN StatusStates
ON Cases.status_id = StatusStates.status_id;
```

View CASES\_VIEW created.

Изменим привилегии роли Accounting\_dep, забрав возможность работы напрямую с Cases, и дав право на использование созданного представления:

```
REVOKE
SELECT,
INSERT ON CasesPs FROM Accounting_dep;

GRANT SELECT ON Cases_view TO Accounting_dep;
```

Revoke succeeded.

Grant succeeded.

Переключимся на пользователя Nadya (которая с ролью accounting\_dep) и попробуем обратиться к таблице Cases:

```
SELECT * FROM CasesPs;

SELECT * FROM Infernal.Cases;
```

ORA-00942: таблица или представление пользователя не существует  
 00942. 00000 - "table or view does not exist"  
 \*Cause:  
 \*Action:  
 Error at Line: 3 Column: 24

А вот созданное представление она видит, и может задавать необходимые запросы:

```
SELECT * FROM Cases_view
WHERE start_date > '10.10.2021';
```

SQL   All Rows Fetched: 10 in 0,001 seconds					
CASE_ID	CASE_NAME	DESCRIPTION	START_DATE	CLOSE_DATE	
1	2 Обращение административного учреждения	Открыто - дело находится в работе.	23.11.21 00:00:00	(null)	
2	4 Порча имущества	Открыто - дело находится в работе.	29.11.21 00:00:00	(null)	
3	10 Подпольный игорный бизнес	Открыто - дело находится в работе.	15.01.22 00:00:00	(null)	
4	18 Пропажа ребенка	Открыто - дело находится в работе.	25.03.22 00:00:00	(null)	
5	26 Финансовые биржевые махинации	Открыто - дело находится в работе.	07.11.21 00:00:00	(null)	
6	32 Угон общественного транспорта	Открыто - дело находится в работе.	24.11.21 00:00:00	(null)	
7	33 ДТП с нелетальным исходом	Открыто - дело находится в работе.	02.03.22 00:00:00	(null)	
8	37 Домашняя кража	Открыто - дело находится в работе.	04.01.22 00:00:00	(null)	
9	41 Террористический акт	Открыто - дело находится в работе.	13.11.21 00:00:00	(null)	
10	1 Массовые беспорядки	Раскрыто - дело успешно расследовано, fiat iustitia, et pereat mundus!	24.02.22 00:00:00	22.04.18 00:00:00	

## **Выводы:**

В результате данной лабораторной работы были изучены и протестированы различные способы аутентификации в СУБД Oracle, а также создано представление для разграничения доступа некоторых пользователей к не делегированным им данным. Также была предпринята попытка развертывания аутентификации внешними программными средствами (посредством RADIUS-сервера), и создан schema-only пользователь, который может использоваться для безопасной настройки владения ресурсами СУБД.