오라클 데이터베이스 서버 운영

테이블 조회 권한
(WITH GRANT OPTION)

AAA

뷰 조회 권한

테이블 스페이스
확장 요청

ROLE 부여

SERVER

DDD

프로파일 설정
(로그인 시도 제한)

유저생성 권한
(WITH ADMIN OPTION)

BBB

유저 생성 권한

프로파일 설정
(세션접속 가능시간 제한)

EEE

CCC

테이블 조회 권한
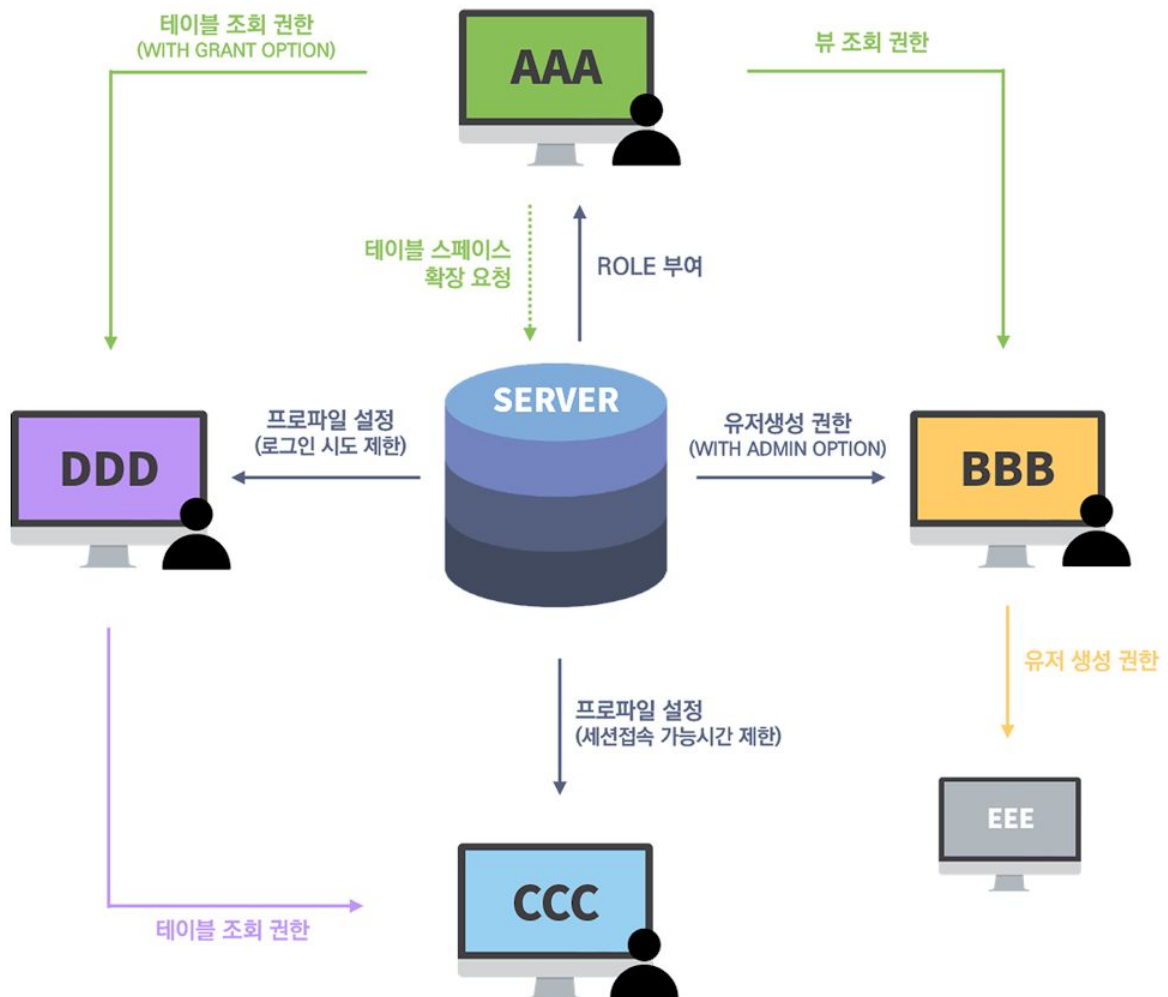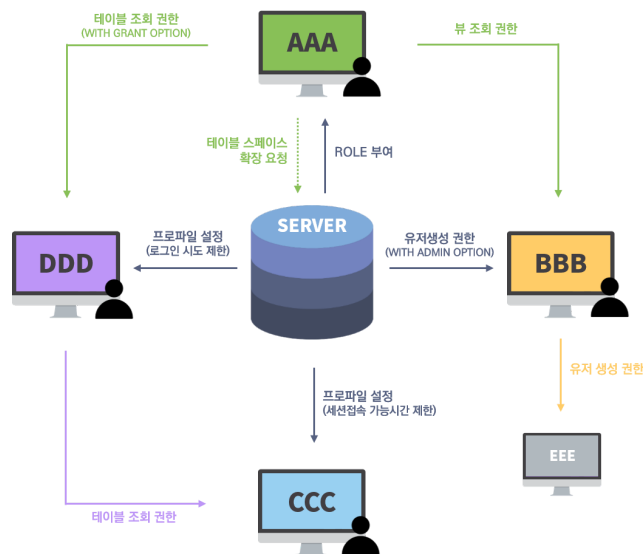
Portfolio 01. 오라클 데이터베이스 서버 운영

1. 프로젝트 목적

1) DB 액세스 관리 (권한과 롤의 부여)
2) 데이터베이스 공간 관리 (테이블 스페이스 관리)
3) 유저 보안 관리 (PROFILE 생성)

2. 프로젝트 작업 환경

1) OS : Linux (OEL 5.4)
2) DB : Oracle 12c

3. 역할 할당

역할	계정	작업내용
사수	SYS	– 유저 생성, PROFILE 생성 – 테이블 스페이스 관리 – 부사수에게 롤, 권한 부여
부사수	AAA	– 테이블 EMP 생성 – 뷰 V_EMP 생성
	BBB	– 유저 EEE 생성
	CCC	– 세션접속 제한 확인
	DDD	– 테이블 EMP 조회 권한 CCC에게 부여 – 로그인 시도 2회 실패

PART 1. DB 액세스 관리

유저 생성

```
SYS@JEON>create user aaa
  2   identified by aaa
  3   default tablespace project;

User created.

SYS@JEON>create user bbb
  2   identified by bbb
  3   default tablespace project;

User created.

SYS@JEON>create user ccc
  2   identified by ccc
  3   default tablespace project;

User created.

SYS@JEON>create user ddd
  2   identified by ddd
  3   default tablespace project;

User created.
```

세션 접근 권한 부여

```
SYS@JEON>grant create session to aaa;
Grant succeeded.

SYS@JEON>grant create session to bbb;
Grant succeeded.

SYS@JEON>grant create session to ccc;
Grant succeeded.

SYS@JEON>grant create session to ddd;
Grant succeeded.
```

AAA에게 MANAGER 롤 부여

```
SYS@JEON>create role manager;
Role created.

SYS@JEON>grant create table, create view, drop any table to manager;
Grant succeeded.

SYS@JEON>grant manager to aaa;
Grant succeeded.
```

1) WITH GRANT OPTION

※ 참고

with admin option	with grant option
시스템 권한	오브젝트 권한
재할당 가능	재할당 가능
연쇄 회수 X	연쇄 회수 O

 AAA 유저가 SCOTT 스키마의 테이블에 접근하여 CTAS로 테이블을 생성할 수 있도록 권한 부여

```
SYS@JEON>grant select on scott.emp to aaa;
Grant succeeded.
```

AAA) 작업할 테이블 생성 (EMP)

```
AAA@JEON>create table emp
  2  as
  3  select *
  4  from scott.emp;
Table created.
```

AAA) DDD에게 테이블 EMP를 조회할 권한을 WITH GRANT OPTION으로 부여

```
AAA@JEON>grant select on emp to ddd with grant option;
Grant succeeded.

AAA@JEON>select grantor, grantee, table_name, privilege, grantable
  2  from user_tab_privs
  3  where grantor = 'AAA';

GRANTOR  GRANTEE    TABLE_NAME PRIVILEGE           GRA
-------- ---------- ---------- ------------------- ---
AAA      DDD        EMP        SELECT              YES
AAA      PUBLIC     AAA        INHERIT PRIVILEGES  NO

2 rows selected.
```

AAA) 데이터 수정

```
AAA@JEON>update emp set ename = 'JEON' where ename = 'KING';
1 row updated.
```

DDD) 조회할 권한만 받았기 때문에 데이터 수정 불가

```
DDD@JEON>select * from aaa.emp where ename = 'JEON';

     EMPNO ENAME      JOB          MGR       SAL       COMM     DEPTNO
---------- ---------- --------- ------- --------- ---------- ----------
      7839 JEON       PRESIDENT            5000                     10
```

```
DDD@JEON>update aaa.emp set ename = 'KIM' where ename = 'FORD';
update aaa.emp set
            *
ERROR at line 1:
ORA-01031: insufficient privileges

DDD@JEON>select grantor, grantee, privilege, table_name, grantable
  2  from user_tab_privs;


GRANTOR  GRANTEE    PRIVILEGE            TABLE_NAME GRA
-------- ---------- ------------------- ---------- ---
AAA      DDD  SELECT                    EMP        NO
DDD      PUBLIC     INHERIT PRIVILEGES  DDD        NO
```

```
DDD@JEON>grant select on aaa.emp to ccc;
Grant succeeded.
```

CCC) 권한 확인

```
CCC@JEON>select grantor, grantee, privilege, table_name, grantable
  2  from user_tab_privs;

GRANTOR  GRANTEE    PRIVILEGE            TABLE_NAME GRA
-------- ---------- ------------------- ---------- ---
DDD      CCC  SELECT                    EMP        NO
CCCC     PUBLIC     INHERIT PRIVILEGES  CCC        NO

2 rows selected.
```

AAA) 권한 회수

```
AAA@JEON>revoke select on emp from ddd;
Revoke succeeded.
```

DDD) 권한 회수 확인

```
DDD@JEON>select * from aaa.emp;
select * from aaa.emp
                *
ERROR at line 1:
ORA-00942: table or view does not exist
```

CCC) 연쇄적으로 권한이 회수 되었는지 확인

```
CCC@JEON>select * from aaa.emp;
select * from aaa.emp
                *
ERROR at line 1:
ORA-00942: table or view does not exist
```

2) WITH ADMIN OPTION

BBB에게 유저생성 권한을 WITH ADMIN OPTION 으로 부여

```
SYS@JEON>grant create user to bbb with admin option;
Grant succeeded.
```

BBB) EEE 유저를 생성하고 권한 재부여

```
BBB@JEON>select * from user_sys_privs;

USERNAME   PRIVILEGE          ADM COM
---------  -----------------  --- ---
BBB        CREATE SESSION     NO  NO
BBB        CREATE USER        YES NO

2 rows selected.

BBB@JEON>create user eee identified by eee;
User created.

BBB@JEON>grant create user to eee;
Grant succeeded
```

BBB의 권한 회수

```
SYS@JEON>revoke create user from bbb;
Revoke succeeded.
```

BBB) 권한 조회

```
BBB@JEON>select * from user_sys_privs;

USERNAME   PRIVILEGE          ADM COM
---------  -----------------  --- ---
BBB        CREATE SESSION     NO  NO

1 rows selected.
```

EEE) 권한 조회

```
※ EEE에 접속하려면 SYS에서 권한을 부여해야 한다.
SYS@JEON>grant create session to eee;
Grant succeeded.

EEE@JEON>select * from user_sys_privs;

USERNAME   PRIVILEGE                            ADM COM
---------  ----------------------------------   --- ---
EEE        CREATE USER                          NO  NO
EEE        CREATE SESSION                       NO  NO

2 rows selected.
```

3) VIEW 조회 권한

AAA) 뷰 생성 후 조회

```
AAA@JEON>create or replace view v_emp
 2  as
 3  select ename, sal, deptno
 4  from emp
 5  where deptno in (10, 20);

View created.

AAA@JEON>select * from v_emp;

ENAME            SAL     DEPTNO
---------- ---------- ----------
SMITH            800         20
JONES           2975         20
CLARK           2450         10
SCOTT           3000         20
JEON            5000         10
ADAMS           1100         20
FORD            3000         20
MILLER          1300         10

8 rows selected.
```

AAA) BBB에게 뷰 조회 권한 부여

```
AAA@JEON>grant select on v_emp to bbb;
Grant succeeded.
```

BBB) 뷰 조회

```
BBB@JEON>select * from aaa.v_emp;

ENAME            SAL     DEPTNO
---------- ---------- ----------
SMITH            800         20
JONES           2975         20
CLARK           2450         10
SCOTT           3000         20
JEON            5000         10
ADAMS           1100         20
FORD            3000         20
MILLER          1300         10

8 rows selected.
```

PART 2. 데이터베이스 공간 관리

테이블 스페이스 확장 시뮬레이션

기존 테이블 스페이스 조회

```
SYS@JEON>select tablespace_name, status
  2  from dba_tablespaces;

TABLESPACE_NAME           STATUS
----------------------    -------
SYSTEM             ONLINE
SYSAUX             ONLINE
UNDOTBS1                  ONLINE
TEMP                      ONLINE
USERS                     ONLINE
EXAMPLE                   ONLINE

6 rows selected.


SYS@JEON>select tablespace_name, file_name
  2  from dba_data_files;

TABLESPACE_NAME           FILE_NAME
----------------------    ----------------------------------------
USERS                     /u01/app/oracle/oradata/JEON/users01.dbf
UNDOTBS1                  /u01/app/oracle/oradata/JEON/undotbs01.dbf
SYSTEM             /u01/app/oracle/oradata/JEON/system01.dbf
SYSAUX             /u01/app/oracle/oradata/JEON/sysaux01.dbf
EXAMPLE                   /u01/app/oracle/oradata/JEON/example01.dbf

5 rows selected.
```

테이블 스페이스 'PROJECT' 생성

```
SYS@JEON>create tablespace project
  2  datafile '/u01/app/oracle/oradata/JEON/project.dbf' size 1M;
Tablespace created.


SYS@JEON>select tablespace_name, file_name, bytes/1024/1024 MB, status
  2 from dba_data_files;

TABLESPACE_NAME FILE_NAME                                     MB  STATUS
-------------- --------------------------------------- -------- ---------
USERS     /u01/app/oracle/oradata/JEON/users01.dbf          5  AVAILABLE
UNDOTBS1  /u01/app/oracle/oradata/JEON/undotbs01.dbf      155  AVAILABLE
SYSTEM/u01/app/oracle/oradata/JEON/system01.dbf         790  AVAILABLE
SYSAUX/u01/app/oracle/oradata/JEON/sysaux01.dbf         690  AVAILABLE
EXAMPLE   /u01/app/oracle/oradata/JEON/example01.dbf  1243.75  AVAILABLE
PROJECT   /u01/app/oracle/oradata/JEON/project.dbf          1  AVAILABLE

6 rows selected.
```

AAA) 작업할 테이블 생성 (TEST)

```
AAA@JEON>create table test(col1 varchar(30), col2 number);
Table created.
```

ORA-01950 에러 발생 시

```
AAA@JEON>create table emp
  2  as
  3  select *
  4  from scott.emp;
from scott.emp
              *
ERROR at line 4:
ORA-01950: no privileges on tablespace 'PROJECT'

SYS@JEON>alter user aaa default tablespace project quota unlimited on project;
User altered.
```

생성된 유저에게 PROJECT 테이블스페이스의 영역을 얼마만큼 할당할 것인지 정해지지 않은 상태이기 때문이다. 해당 테이블 스페이스에 대한 공간을 정해주면 되는데, unlimited는 제한을 두지 않고 할당한다는 의미이다.

AAA) TEST 테이블에 INSERT 작업 반복

```
AAA@JEON>insert into test(col1, col2)
  2  select object_name, object_id
  3  from all_objects
  4  where rownum <= 100;

100 rows created.

.
.
.

AAA@JEON>r
  1  insert into test(col1, col2)
  2  select object_name, object_id
  3  from all_objects
  4* where rownum <= 100000
insert into test(col1, col2)
            *
ERROR at line 1:
ORA-01653: unable to extend table AAA.TEST by 8 in tablespace PROJECT
```

참고) 테이블 스페이스의 총 용량과 남은 공간을 조회할 때

```
SYS@JEON>select a.tablespace_name, a.total "TOTAL(MB)", b.free "FREE(MB)"
  2  from (select file_id, tablespace_name, sum(bytes/1024/1024) TOTAL
  3  from dba_data_files
  4  group by file_id, tablespace_name) a,
  5  (select file_id, tablespace_name, sum(bytes/1024/1024) FREE
  6  from dba_free_space
  7  group by file_id, tablespace_name) b
  8  where a.file_id = b.file_id

TABLESPACE_NAME                 TOTAL(MB)   FREE(MB)
----------------------------- ----------  ---------
SYSTEM                          790         4.25
EXAMPLE                         1243.75    24.6875
SYSAUX                          690       41.6875
PROJECT                           1          .4375
USERS                             5         3.3125
UNDOTBS1                        155          5.875

6 rows selected.
```

해결방법 1) 기존의 데이터 파일 크기를 늘려준다.

```
SYS@JEON>alter database datafile '/u01/app/oracle/oradata/JEON/project.dbf'
 2 resize 2M;
Database altered.


SYS@JEON>select tablespace_name, file_name, bytes/1024/1024 MB, status
  2  from dba_data_files

TABLESPACE_NAME FILE_NAME                                          MB   STATUS
--------------- ----------------------------------------- -------  ---------
USERS           /u01/app/oracle/oradata/JEON/users01.dbf       5   AVAILABLE
UNDOTBS1        /u01/app/oracle/oradata/JEON/undotbs01.dbf   155   AVAILABLE
SYSTEM    /u01/app/oracle/oradata/JEON/system01.dbf        790   AVAILABLE
SYSAUX    /u01/app/oracle/oradata/JEON/sysaux01.dbf        690   AVAILABLE
EXAMPLE         /u01/app/oracle/oradata/JEON/example01.dbf 1243.75  AVAILABLE
PROJECT         /u01/app/oracle/oradata/JEON/project.dbf          2  AVAILABLE

6 rows selected.
```

AAA) TEST 테이블에 INSERT 작업 반복

```
AAA@JEON>r
  1  insert into test(col1, col2)
  2  select object_name, object_id
  3  from all_objects
  4* where rownum <= 10000
insert into test(col1, col2)
          *
ERROR at line 1:
ORA-01653: unable to extend table AAA.TEST by 128 in tablespace PROJECT
```

해결방법 2) 테이블 스페이스 autoextend 옵션을 on으로 설정한다.

※ autoextend 옵션 확인

```
SYS@JEON>select file_name, tablespace_name, bytes, autoextensible
  2  from dba_data_files
  3  where tablespace_name = 'PROJECT';

FILE_NAME                                      TABLESPACE_NAME BYTES      AUT
---------------------------------------------- --------------- ---------- ---
/u01/app/oracle/oradata/JEON/project.dbf       PROJECT         2097152    NO


SYS@JEON>alter database datafile '/u01/app/oracle/oradata/JEON/project.dbf'
  2 autoextend on next 1M;
Database altered.
```

AAA) TEST 테이블에 INSERT 작업 반복

```
AAA@JEON>r
  1  insert into test(col1, col2)
  2  select object_name, object_id
  3  from all_objects
  4* where rownum <= 10000

10000 rows created.
```

※ 테스트 종료 후 TEST 테이블 삭제

```
AAA@JEON>drop table test;
Table dropped.
```

PART 3. 유저 보안 관리

프로파일 생성

```
SYS@JEON>create profile conn_ccc limit
  2  connect_time 5;
Profile created.

SYS@JEON>create profile conn_ddd limit
  2  failed_login_attempts 2;
Profile created.

SYS@JEON>select *
  2  from dba_profiles
  3  where profile in ('CONN_CCC', 'CONN_DDD');

PROFILE            RESOURCE_NAME          RESOURCE       LIMIT        COM
---------------- ---------------------- ------------- ------------- ---
CONN_CCC           CONNECT_TIME           KERNEL          5           NO
CONN_DDD           FAILED_LOGIN_ATTEMPTS  PASSWORD        2           NO
...
32 rows selected.
```

프로파일 등록

```
SYS@JEON>alter user ccc profile conn_ccc;
User altered.

SYS@JEON>alter user ddd profile conn_ddd;
User altered.

SYS@JEON>select username, profile
  2  from dba_users
  3  where username in ('CCC', 'DDD');

USERNAME    PROFILE
---------- --------------------
CCC         CONN_CCC
DDD         CONN_DDD

2 rows selected.
```

CCC) 5분 후 CONNECT_TIME 프로파일이 작동하는지 확인

```
CCC@JEON>select * from aaa.emp;
select * from aaa.emp
                *
ERROR at line 1:
ORA-00604: error occurred at recursive SQL level 1
ORA-02399: exceeded maximum connect time, you are being logged off
```

DDD) 로그인 실패 2회 후 FAILED_LOGIN_ATTEMPTS 프로파일이 작동하는지 확인

```
[oracle@edydr1p1 ~]$ sqlplus ddd/aaa

ERROR:
ORA-01017: invalid username/password; logon denied

Enter user-name: ddd
Enter password: (ccc)

ERROR:
ORA-01017: invalid username/password; logon denied

Enter user-name: ddd
Enter password: (ccc)

ERROR:
ORA-28000: the account is locked
SP2-0157: unable to CONNECT to ORACLE after 3 attempts, exiting SQL*Plus
```