Защита в среде Oracle

1. Пользователи Oracle

1.1. Создание пользователя

CREATE USER *имя_ пользователя*
IDENTIFIED {BY *пароль* | EXTERNALLY}
[DEFAULT TABLESPACE *имя_табличного_пространства*]
[TEMPORARY TABLESPACE *им_временногоя_табличного_пространства*]
[QUOTA {integer [K|M] | UNLIMITED} ON *имя_табличного_пространства*] ...
[PROFILE *имя_профиля*]

CREATE USER *tom* IDENTIFIED BY *tommy*;

GRANT create sessiot TO *tom*;

1.2. Изменение параметров пользователя

ALTER USER *tom* IDENTIFIED BY *tootsie*;

1.3. Удаление пользователя

DROP USER *tom* [CASCADE];

2. Привилегии системного уровня

2.1. Виды системных привилегий

2.2. Предоставление системных привилегий

GRANT {*привилегия* | *имя_роли*} [, { *привилегия* | *имя_роли* }] ...
TO { *пользователь* | *имя_роли* | PUBLIC}
[, { *пользователь* | *имя_роли* | PUBLIC}] ...
[WITH ADMIN OPTION]

GRANT create table, create procedure, create trigger TO tom;

GRANT create table TO public;

2.3. Отмена системных привилегий

REVOKE { *привилегия* | *имя_роли* } [, { *привилегия* | *имя_роли* }] ...
FROM { *пользователь* | *имя_роли* | PUBLIC}
[, { *пользователь* | *имя_роли* | PUBLIC}] ...

REVOKE create trigger FROM tom;

2.4. Проверка системных привилегий

SELECT * FROM user_sys_privs;

3. Привилегии объектного уровня

3.1. Виды объектных привилегий

SELECT	**EXECUTE**
INSERT	**ALTER**
UPDATE	**INDEX**
DELETE	**REFERENCES**

3.2. Предоставление объектных привилегий

GRANT { *привилегия* | ALL [PRIVILEGES]} [(*колонка* [,*колонка*] ...)]
[, { *привилегия* | ALL [PRIVILEGES]} [(*колонка* [,*колонка*] ...)]]
ON [*схема*.]*объект*
TO { *пользователь* | *имя_роли* | PUBLIC}
[, { *пользователь* | *имя_роли* | PUBLIC}] ...
[WITH GRANT OPTION]

GRANT select, insert ON tab1 TO tom;

3.3. Отмена объектных привилегий

REVOKE { *привилегия* | ALL [PRIVILEGES]}
[, { *привилегия* | ALL [PRIVILEGES]}] ...
ON [*схема*.] *объект*
FROM { *пользователь* | *имя_роли* | PUBLIC}
[, { *пользователь* | *имя_роли* | PUBLIC}] ...
[CASCADE CONSTRAINTS]

REVOKE insert ON tab1 FROM tom;

3.4. Проверка объектных привилегий

USER_TAB_PRIVS
USER_COL_PRIVS
TABLE_PRIVILEGES
COLUMN_PRIVILEGES

4. Роли

4.1. Для чего нужны роли

- **Упрощение предоставления системных и объектных привилегий**
- **Возможность определить набор привилегий еще до появления пользователей**
- **Упрощенный метод разрешения и запрещения привилегий пользователя**

4.2. Создание, изменение и уничтожение ролей

CREATE ROLE *имя_роли*
[NOT IDENTIFIED | IDENTIFIED {BY *пароль* | EXTERNALLY}]

CREATE ROLE salperson ;

CREATE ROLE manager IDENTIFIED BY secret ;

ALTER ROLE *имя_роли*
[NOT IDENTIFIED | IDENTIFIED {BY *пароль* | EXTERNALLY}]

ALTER ROLE manager NOT IDENTIFIED;

DROP ROLE *имя_роли*

CREATE ROLE salperson ;

4.3. Предоставление привилегий ролям

GRANT create table, create procedure TO manager;

GRANT select, update ON delegates TO manager;

4.4. Предоставление и отмена ролей

GRANT salperson TO Tom, Mary;
GRANT manager TO Tom WITH ADMIN OPTION;

CREATE ROLE big_chief ;
GRANT manager, salperson TO big_chief;

REVOKE manager FROM big_chief;
REVOKE manager FROM Tom;

4.5. Разрешение и запрещение ролей

SET ROLE { *роль* [IDENTIFIED BY *пароль*]
[,*роль* [IDENTIFIED BY *пароль*]] ...
| ALL [EXCEPT *роль* [,*роль*] ...] | NONE }

GRANT manager, salperson TO Tom;

SET ROLE manager;
SET ROLE ALL EXCEPT salperson;
SET ROLE NONE;

4.6. Роли пользователя, заданные по умолчанию

ALTER USER Tom DEFAULT ROLE salperson;

4.7. Представления словаря данных для ролей

ROLE_ROLE_PRIVS
ROLE_SYS_PRIVS
ROLE_TAB_PRIVS
SESSION_ROLES
SESSION_PRIVS
TABLE_PRIVILEGES

4.8. Ограничения ролей

В процедурах, функциях, пакетах нельзя использовать объекты, привилегии на которые получены через роли

5. Профили

5.1. Профили, заданные по умолчанию

5.2. Создание, изменение и удаление профилей

CREATE PROFILE *имя_профиля* LIMIT
[SESSIONS_PER_USER {integer | UNLIMITED | DEFAULT}]
[CPU_PER_SESSION {integer | UNLIMITED | DEFAULT}]
[CPU_PER_CALL {integer | UNLIMITED | DEFAULT}]
[CONNECT_TIME {integer | UNLIMITED | DEFAULT}]
[IDLE_TIME {integer | UNLIMITED | DEFAULT}]
[LOGICAL_READS_PER_SESSION {integer | UNLIMITED | DEFAULT}]
[LOGICAL_READS_PER_CALL {integer | UNLIMITED | DEFAULT}]
[COMPOSITE_LIMIT {integer | UNLIMITED | DEFAULT}]
[PRIVATE_SGA {integer [K|M] | UNLIMITED | DEFAULT}]

```
CREATE PROFILE low_limits LIMIT
 CPU_PER_SESSION 2
 CPU_PER_CALL    DEFAULT
 CONNECT_TIME    UNLIMITED;
```

ALTER PROFILE *имя_профиля* LIMIT
[SESSIONS_PER_USER {integer | UNLIMITED | DEFAULT}]
[CPU_PER_SESSION {integer | UNLIMITED | DEFAULT}]
[CPU_PER_CALL {integer | UNLIMITED | DEFAULT}]
[CONNECT_TIME {integer | UNLIMITED | DEFAULT}]
[IDLE_TIME {integer | UNLIMITED | DEFAULT}]
[LOGICAL_READS_PER_SESSION {integer | UNLIMITED | DEFAULT}]
[LOGICAL_READS_PER_CALL {integer | UNLIMITED | DEFAULT}]
[COMPOSITE_LIMIT {integer | UNLIMITED | DEFAULT}]
[PRIVATE_SGA {integer [K|M] | UNLIMITED | DEFAULT}]

```
ALTER PROFILE low_limits LIMIT
 SESSIONS_PER_USER 3;
```

DROP PROFILE *имя_профиля* [CASCADE]

```
DROP PROFILE low_limits CASCADE;
```

5.3. Назначение профилей

```
ALTER USER Tom PROFILE low_limits;
```

5.4. Активизация контроля ресурсов

```
ALTER SYSTEM SET RESOURCE_LIMIT = TRUE;
```