# 사용자

자바 강의실

## 목차

# 1. 사용자 관리

- 사용자 생성
  - 회사에 새로운 사원이 입사하게 되면 시스템에 접속하도록 관리자가 계정을 하나 발급해 줍니다.
  - 지금까지는 hr사용자로 접속해서 오라클 데이터베이스를 사용했지만, 사실은 부서별이나 사원의 직무에 따라 사용 가능한 테이블을 고려해서 오라클 데이터베이스에서도 사용자 계정을 발급해야 합니다.
  - 권한은 사용자한테 부여하는 것이므로 사용자를 생성하는 것부터 살펴보도록 합시다.
  - 다음은 사용자 생성을 위한 CREATE USER 명령어의 형식입니다.

```
CREATE USER user_name
IDENTIFIED BY password;
```

# 1. 사용자 관리

- 사용자 생성
  - 사용자의 생성은 사용자의 이름과 암호를 지정하여 생성합니다.
  - 사용자를 생성하기 위해서도 권한이 필요합니다.
  - 우리가 지금까지 주로 사용해 왔던 hr 이란 사용자는 사용자를 생성할 권한이 없습니다.
  - 새로운 사용자 계정을 발급받기 전에 주의할 점이 있습니다.
  - 사용자를 생성하기 위해서는 시스템 권한을 가지고 있어야 합니다.
  - 오라클 데이터베이스를 설치할 때 자동으로 생성되는 디폴트 사용자 가운데 시스템 권한을 가진 데이터베이스 관리자인 DBA는 SYS, SYSTEM입니다.
  - 그러므로 사용자 계정을 발급 받기 위해서 시스템 권한을 가진 SYSTEM으로 접속해야 합니다.

# 1. 사용자 관리

## 예: 사용자 생성

질의 : CREATE USER 명령어를 사용하여
사용자명은 jsp
암호는 1234 로 사용자를 생성해봅시다.

# 1. 사용자 관리

**예: 사용자 생성 쿼리**

**질의 쿼리 :**

```
CREATE USER jsp IDENTIFIED BY 1234 DEFAULT TABLESPACE JSP ;
```

# 1. 사용자 관리

## 예: 사용자 비밀번호 수정

**질의 : 사용자 jsp 의 비밀번호를 변경하라**

ALTER USER jsp IDENTIFIED BY jsp2 ;

## 예: 사용자 삭제

**질의 : 사용자 jsp 를 삭제하라**

DROP USER jsp [CASCADE] ;

# 2. 보안 관리

- 데이터베이스 보안을 위한 권한
  - 기업에서 보유하고 있는 데이터들은 자료 이상의 가치가 있으므로 외부에 노출되지 않도록 보안을 해야 합니다.
  - 데이터베이스를 운영하려면 데이터베이스에 대한 적절한 보안 대책을 마련해야 합니다.
  - 오라클은 다수의 사용자들이 데이터베이스에 저장된 정보를 공유해서 사용합니다.
  - 하지만 정보의 유출이나 불법적인 접근을 방지하기 위해서 철저한 보안 대책이 필요합니다.
  - 이러한 보안 대책을 위해서 데이터베이스 관리자가 있어야 합니다.

# 2. 보안 관리

- 데이터베이스 보안을 위한 권한
  - 데이터베이스 관리자는 사용자가 데이터베이스의 객체(테이블, 뷰 등)에 대한 특정 권한을 가질 수 있도록 함으로서 다수의 사용자가 데이터베이스에 저장된 정보를 공유하면서도 정보에 대한 보안이 이루어지도록 합니다.
  - 데이터베이스에 접근하기 위해서는 사용자가 이름과 암호를 입력해서 로그인 인증을 받아야 합니다.
  - 이렇게 데이터베이스에 접속하는 사용자로부터 어떻게 데이터를 보안할 수 있을까요?
  - 사용자마다 서로 다른 권한과 롤을 부여함으로서 보안을 설정할 수 있습니다.

# 2. 보안 관리

- 권한을 부여하기
  - 사용자에게 시스템 권한 부여하기 위해서는 GRANT 명령어를 사용합니다.

```
GRANT privilege_name, …
TO user_name;
```

  - 우선 데이터베이스 관리자로 접속합니다.
  - 새로 생성된 user01에 데이터베이스에 접속할 수 있는 권한인 CREATE SESSION를 부여합니다.
  - 다시 user01 사용자로 접속을 시도하면 이번에는 데이터베이스에 성공적으로 접속하게 됩니다.

# 2. 보안 관리

## 예: 권한부여

질의 : 새로 생성된 jsp 에 데이터베이스에 접속할 수 있는 권한인
CREATE SESSION를 부여합니다.
jsp 사용자로 접속을 시도하면
이번에는 데이터베이스에 성공적으로 접속하게 됩니다.

GRANT CREATE SESSION TO jsp ;

# 2. 보안 관리

- 권한의 역할과 종류
  - 권한은 사용자가 특정 테이블을 접근할 수 있도록 하거나 해당 테이블에 SQL(SELECT/INSERT/UPDATE/DELETE) 문을 사용할 수 있도록 제한을 두는 것을 말합니다.
  - 데이터베이스 보안을 위한 권한은 시스템 권한(System Privileges)과 객체 권한(Object Privileges)으로 나뉩니다.
  - 시스템 권한은 사용자의 생성과 제거, DB 접근 및 각종 객체를 생성할 수 있는 권한 등 주로 DBA에 의해 부여되며 그 권한의 수가 80 가지가 넘기에 대표적인 시스템 권한만 정리하고 넘어갑시다.

| 시스템 권한 | 기능 |
|---|---|
| CREATE USER | 새롭게 사용자를 생성하는 권한 |
| DROP USER | 사용자를 삭제하는 권한 |
| DROP ANY TABLE | 임의의 테이블을 삭제할 수 있는 권한 |
| QUERY REWRITE | 함수 기반 인덱스를 생성하는 권한 |
| BACKUP ANY TABLE | 임의의 테이블을 백업할 수 있는 권한 |

# 2. 보안 관리

- 권한의 역할과 종류
  - 데이터베이스를 관리하는 권한으로 다음과 같은 것이 있습니다. 이러한 권한은 시스템 관리자가 사용자에게 부여하는 권한입니다

| 시스템 권한 | 기능 |
|---|---|
| CREATE SESSION | 데이터베이스에 접속할 수 있는 권한 |
| CREATE TABLE | 사용자 스키마에서 테이블을 생성할 수 있는 권한 |
| CREATE VIEW | 사용자 스키마에서 뷰를 생성할 수 있는 권한 |
| CREATE SEQUENCE | 사용자 스키마에서 시퀀스를 생성할 수 있는 권한 |
| CREATE PROCEDURE | 사용자 스키마에서 함수를 생성할 수 있는 권한 |

  - 객체 권한은 객체를 조작할 수 있는 권한입니다.
  - 객체는 우리가 학습한 것 중에서 테이블, 뷰 등을 예로 들 수 있고, 이미 학습한 시퀀스, 인덱스 등과 앞으로 배울 동의어가 모두 객체에 해당됩니다.

# 2. 보안 관리

## 예: 권한부여

**질의 : 사용자 jsp 에 데이터베이스의 모든 권한을 부여하라**

```
GRANT CONNECT, RESOURCE TO jsp ;
```

[참고]

```
SELECT * FROM DBA_SYS_PRIVS WHERE GRANTEE = 'CONNECT';
SELECT * FROM DBA_SYS_PRIVS WHERE GRANTEE = 'RESOURCE';
```

- 권한을 삭제하기
  - 사용자에게 부여한 객체 권한을 데이터베이스 관리자나 객체 소유자로부터 절회하기 위해서는 REVOKE 명령어를 사용합니다. 다음은 REVOKE 명령어의 형식입니다

```
REVOKE {privilege_name | all}
ON object_name
FROM {user_name | role_name | public};
```

- 기타 유용한 명령

```
-- 데이터베이스명
SELECT NAME, DB_UNIQUE_NAME FROM V$DATABASE;

-- SID 명
SELECT INSTANCE FROM v$thread;
```