



SQL 활용

사용자 관리



한국기술교육대학교
온라인평생교육원

학습내용

- 보안
- 권한 부여

학습목표

- 보안에 대한 기본 개념을 설명할 수 있다.
- 사용자 권한 부여를 위한 DCL문을 작성할 수 있다.

● 보안

1. 통제

◆ 보안

- 불법적인 데이터의 폭로나 변경 또는 파괴로부터 데이터베이스를 보호하는 것

◆ 보안에 대한 통제

- ① 법적, 윤리적 통제
 - 법, 윤리 ⇨ 심리적 보안
- ② 행정, 관리적 통제
 - 오용을 탐지하고 방지함
- ③ 물리적 통제
 - 적극적, 물리적 보안으로 위반을 예방, 탐지함
- ④ 기술적 통제
 - 하드웨어 통제
 - 소프트웨어 통제
 - 데이터베이스 통제
 - DBMS 보안 서브 시스템 ⇨ 접근 제어

● 보안

2. 접근 제어

◆ 권한이 부여되지 않은 데이터의 검색이나 변경을 방지함

① 직접 접근 제어

- 사용자 신분증 확인(ID)
- 신분증 본인 확인을 위한 인증(PASSWORD)
- 요청 데이터 객체에 대한 요청 연산 권한(권한 부여)

② 간접 접근 제어

- 한 장소에서 다른 장소로의 데이터 흐름 제어
- 개인의 비밀 데이터로부터 작성된 통계정보에 대한 추론 제어
- 전송이나 저장 데이터의 암호화 시스템 작동과 사용자 상호작용의 감시

◆ 접근 제어 구조

● 신분증

- 지문, 성문, ID

● 인증

- 권한 부여 테이블
 - 사용자, 접근 가능한 데이터와 연산
- 데이터베이스 정보
- 요구되는 연산
 - 메인 메모리에 있는 권한 부여 테이블
 - 사용자 활동 로깅

◆ 권한 부여 규정

- 권한 부여 규정은 DCL로 명세함
- 명세된 규정은 데이터 딕셔너리(Data Dictionary)에서 관리함

● 권한 부여

1. 뷰 기반 기법

◆ 뷰 기반 기법이란?

- 뷰를 이용한 권한 부여
- 특정 뷰에 대하여 특정 사용자만 보도록 지정함
- 민감한 데이터를 권한이 없는 사용자로부터 은닉할 수 있음
- 릴레이션의 수직적 / 수평적 서브셋을 제한할 수 있음

◆ 뷰 기반 기법의 문제점

```
CREATE VIEW ST1
AS SELECT SNO, NAME, SAL
FROM STUDENT
WHERE YEAR ≤ 4
```

◆ 튜플 삽입의 제약

```
INSERT INTO S1(SNO, NAME, YEAR): <'E5', 'LEE', 5>
```

◆ 뷰 기반 기법의 문제점

- 알려진 값의 NULL 값
 - ST는 DEPTNO가 12인 뷰인데 삽입될 때는 12대신 NULL이 들어감

```
CREATE VIEW ST2
AS SELECT SNO, YEAR
FROM STUDENT
WHERE DEPTNO = 12

INSERT INTO ST2 (SNO, YEAR):
<'E5', 2>
```

● 권한 부여

2. GRANT / REVOKE 기법

◆ GRANT / REVOKE

- 특정 데이터와 연산을 특정 사용자만 수행할 수 있도록 권한 부여하는 DCL 문
 - GRANT문
 - 자신에게 허용된 권한을 다른 사용자에게 부여하는 구문
 - REVOKE문
 - 다른 사용자에게 허용한 권한을 철회하는 구문
 - DENY문
 - 다른 사용자에게 특정 권한을 불허하는 구문

◆ GRANT 구문

GRANT [권한|ALL] ON 데이터객체 TO 사용자

- 데이터객체가 테이블 또는 뷰일 경우
 - 권한 : SELECT, INSERT, UPDATE, DELETE, REFERENCE 등 사용 권한
- 데이터객체가 데이터베이스일 경우
 - 권한 : CREATE [DB, TABLE, VIEW] 등의 권한
 - 주의점 : DROP 권한은 일반적으로 생성자(주인)만 가짐
- ALL : 모든 권한을 말함

◆ REVOKE / DENY 구문

REVOEK 권한 ON 데이터객체 TO 사용자

DENY 권한 ON 데이터객체 TO 사용자

● 권한 부여

3. MS-SQL에서의 권한 부여

◆ 인증 모드

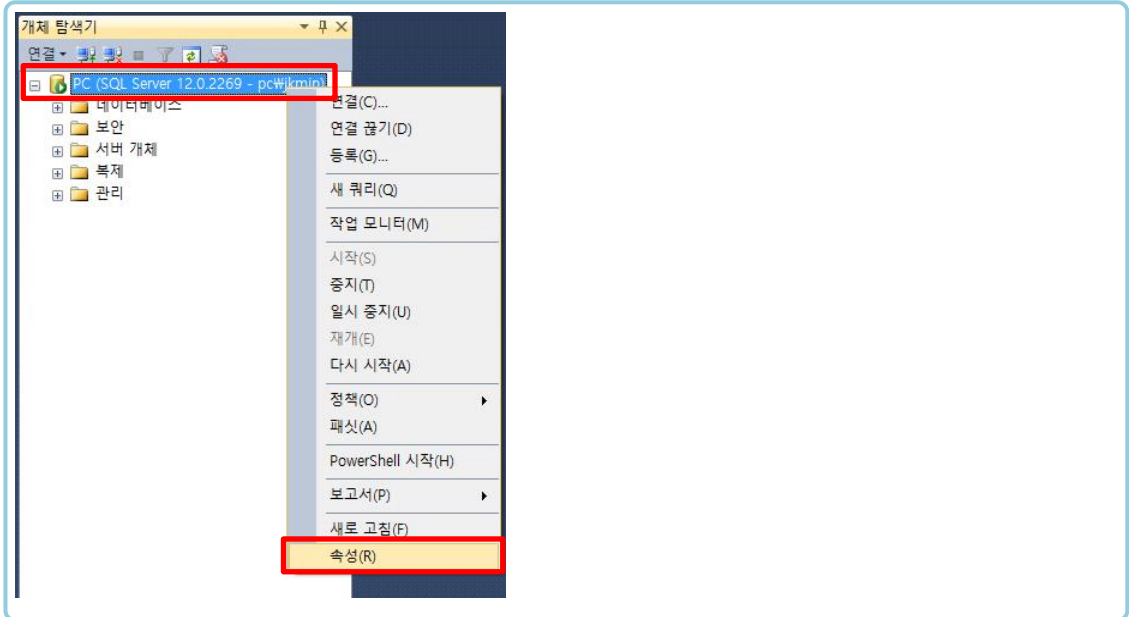
- MS-SQL은 인증과 권한 부여가 분리되어 있음
 - **인증**을 위해서는 로그인 객체가 필요함
 - ⇒ 인증 : MS-SQL Sever에 접속할 수 있다는 것
 - **권한 부여**를 위해서는 사용자 객체가 필요함
 - 인증되었다고 모든 객체(테이블 등)을 접근할 수 있다는 것은 아님
 - 사용자 마다 다른 권한을 가질 수 있음
- 윈도우 인증
 - 별도의 ID나 비밀번호 없이 Windows에 접속한 사용자로 MS-SQL에 연결할 수 있도록 하는 인증방식
- SQL-Server 인증
 - 윈도우 인증과는 무관하게 SQL-Server에 등록된 로그인 계정으로 인증
 - Windows 운영체제의 보완과는 상관없이 SQL-Server 계정으로 접속 가능
 - 보안의 취약성으로 MS사에서는 권장하지 않음
 - 실무에서는 SQL-Server 인증을 빈번히 사용함
 - 보안이 상대적으로 취약하지만 외부 컴퓨터에서 SQL-Server에 접근하여 사용하려면 SQL-Server 인증이 보다 편리함

- 권한 부여

3. MS-SQL에서의 권한 부여

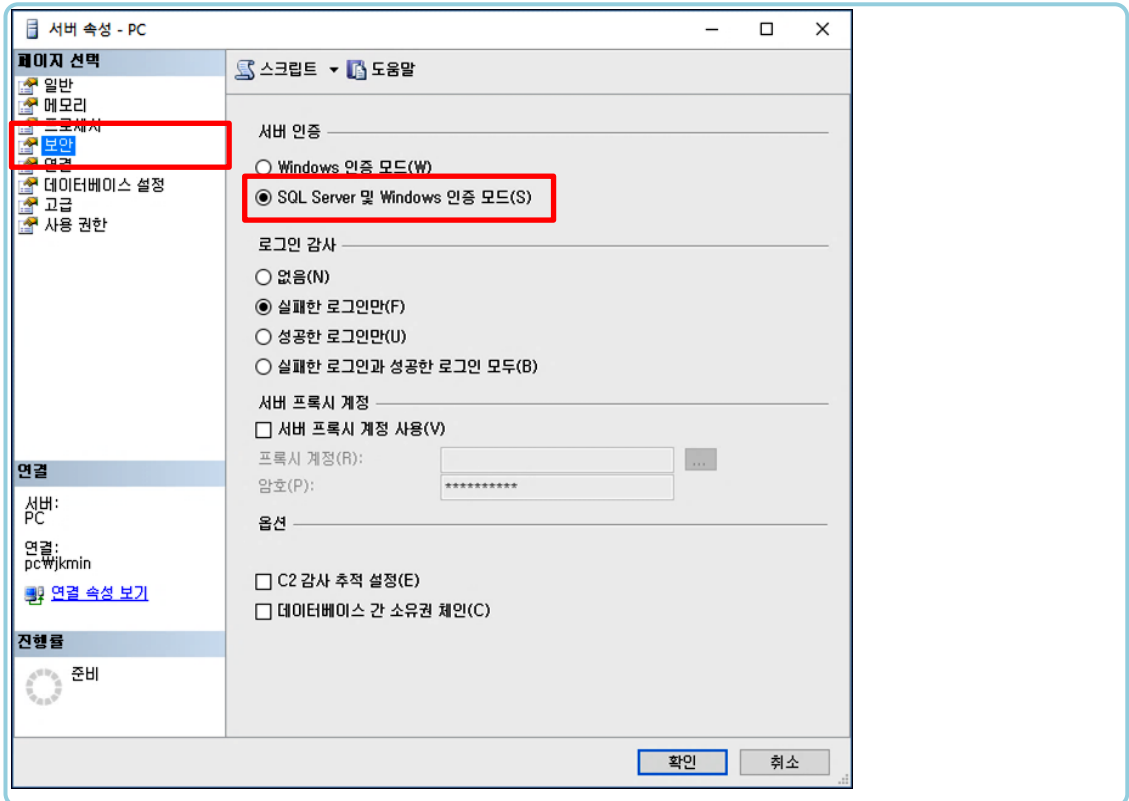
- ◆ 인증 모드

- 인증모드 변경



- 인증모드 변경

⇒ 이후 컴퓨터 재시작 필수



● 권한 부여

3. MS-SQL에서의 권한 부여

◆ DB 사용자

- 로그인 되었다고 MS-SQL Server가 관리하는 모든 데이터베이스들을 자동 접근할 수 있다면 심각한 보안 위협이 됨



데이터베이스 별로 사용자 등록을 해야 함

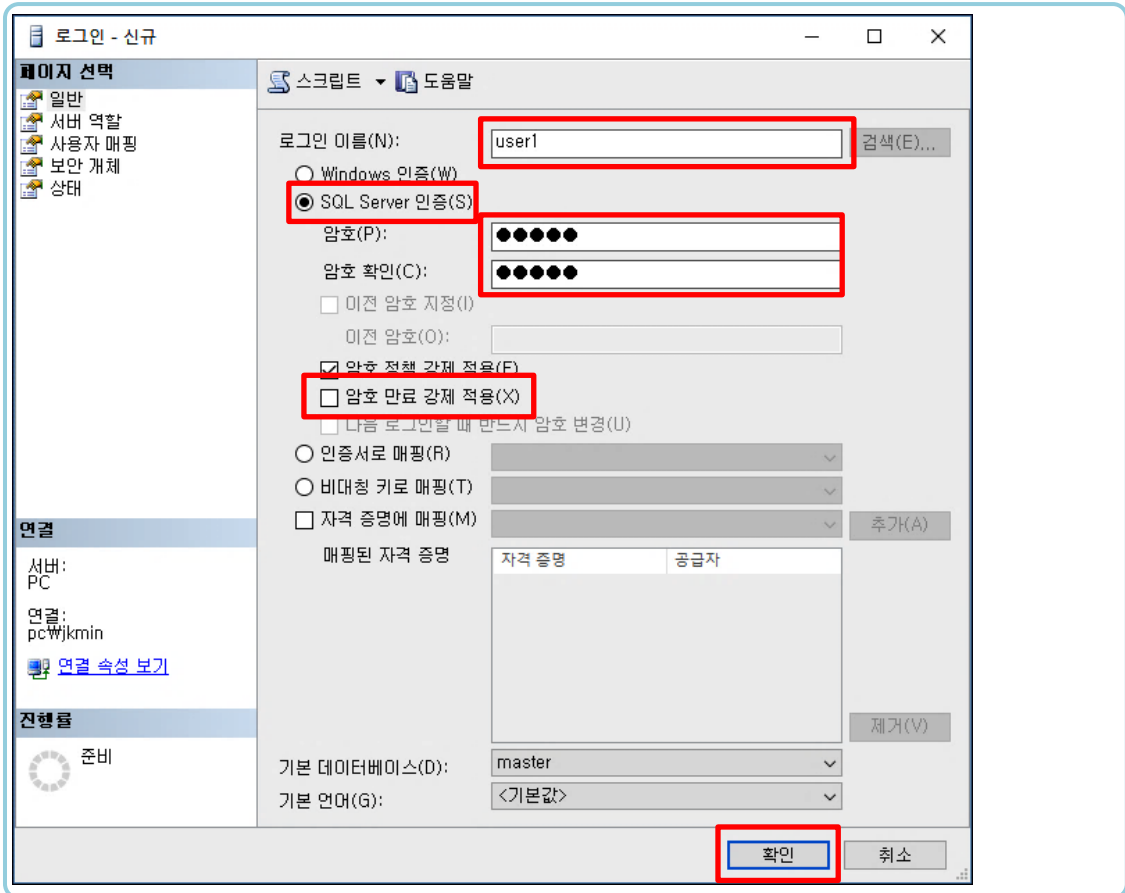
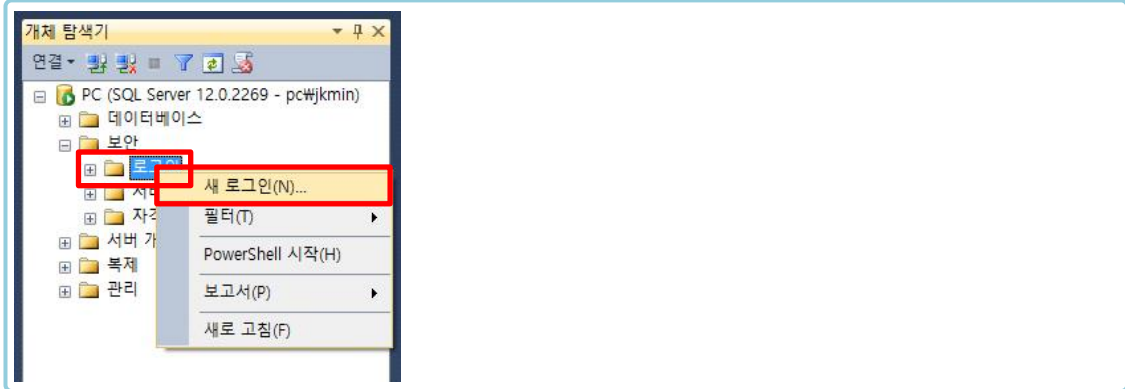
◆ Login 객체 생성 및 사용자 등록

- SSMS를 이용하여 user1 로그인 객체를 생성하고 MagicCorp 데이터베이스에 사용자를 등록함
 - SQL-Server 인증 방식으로 만듦

● 권한 부여

3. MS-SQL에서의 권한 부여

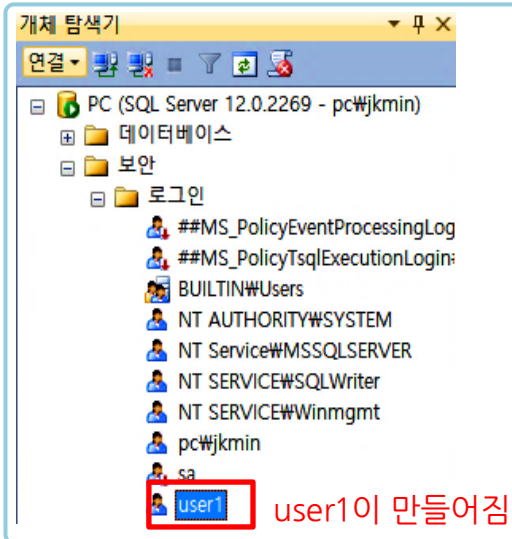
① Login 객체 생성



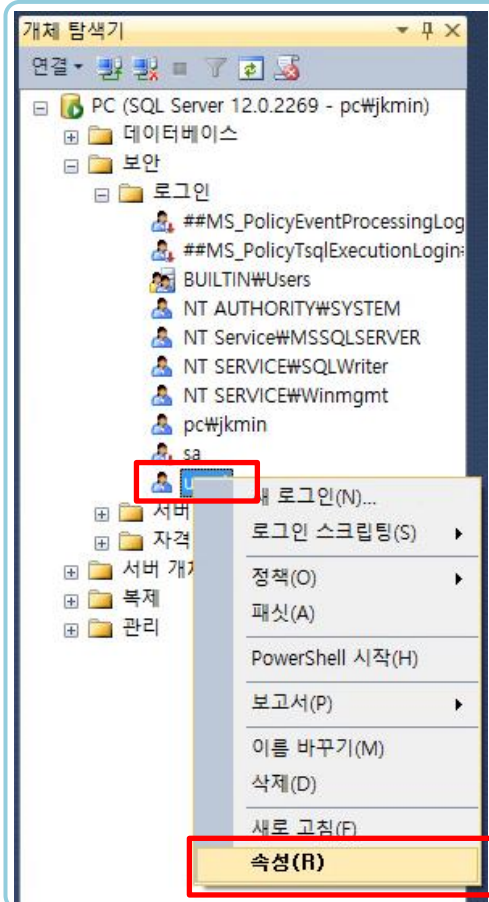
● 권한 부여

3. MS-SQL에서의 권한 부여

① Login 객체 생성



② 사용자 등록

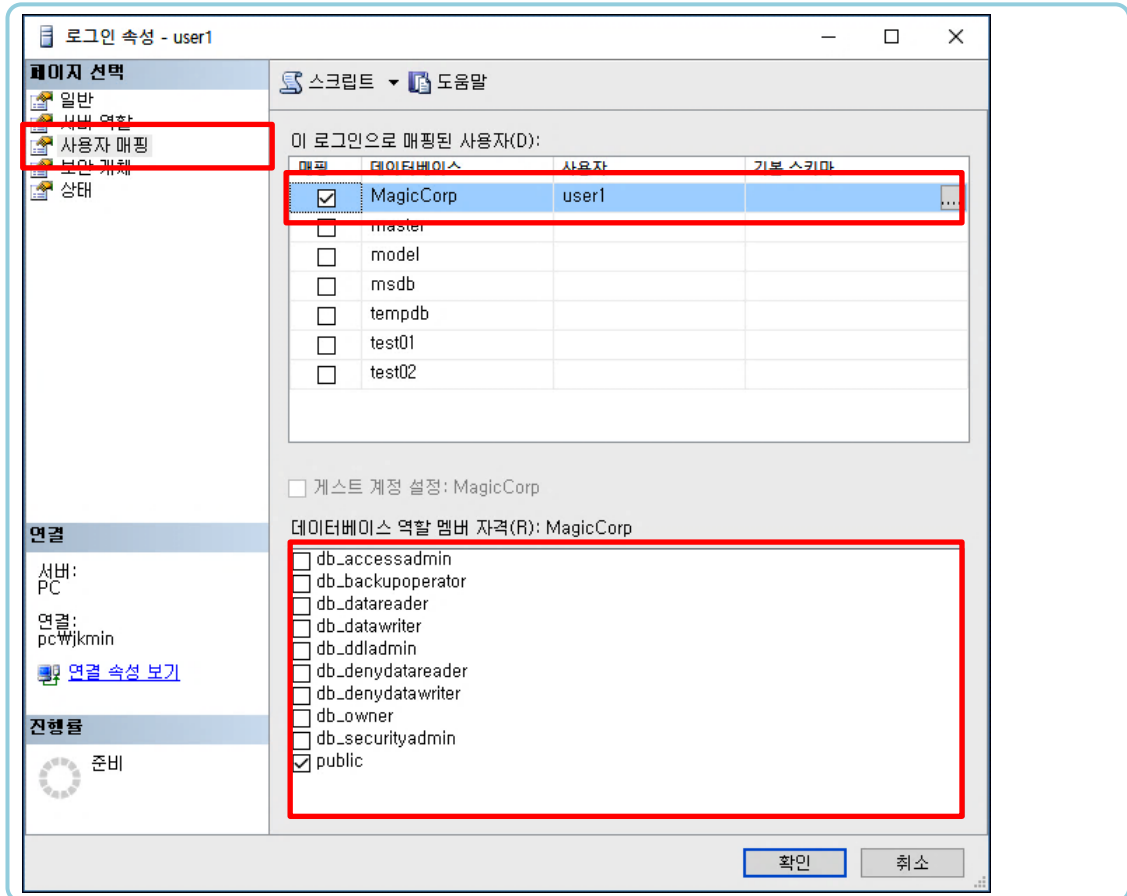


● 권한 부여

3. MS-SQL에서의 권한 부여

② 사용자 등록

- 데이터베이스 역할(Rule) 멤버 자격
 - 사용자가 해당 DB에 어떤 역할인지 지정함

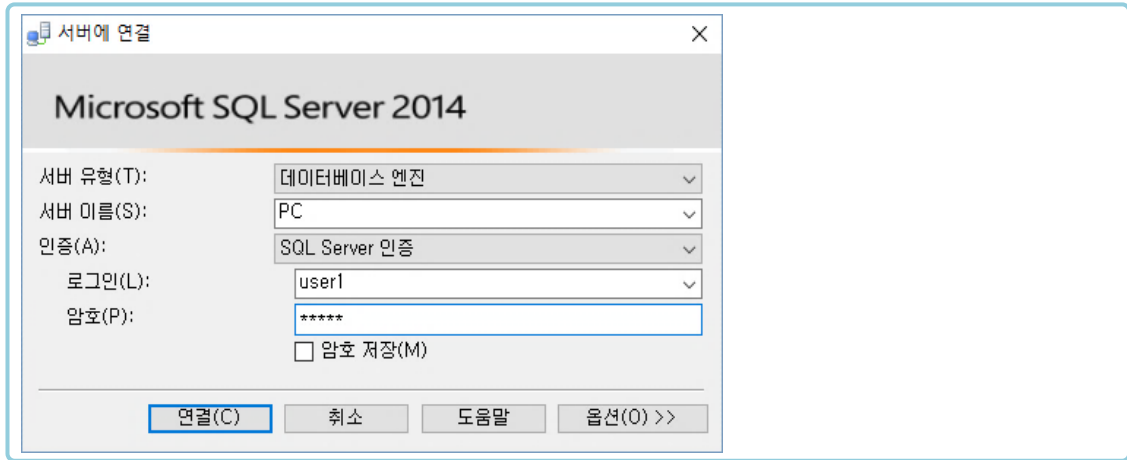


- 데이터베이스 역할(Rule) 멤버 자격
 - 주요 역할 멤버
 - db_accessadmin : 로그인에 대한 추가나 제거 권한
 - db_owner : DB의 모든 구성 및 유지 작업 가능
 - public : 디폴트로 부여되는 최소한의 권한

● 권한 부여

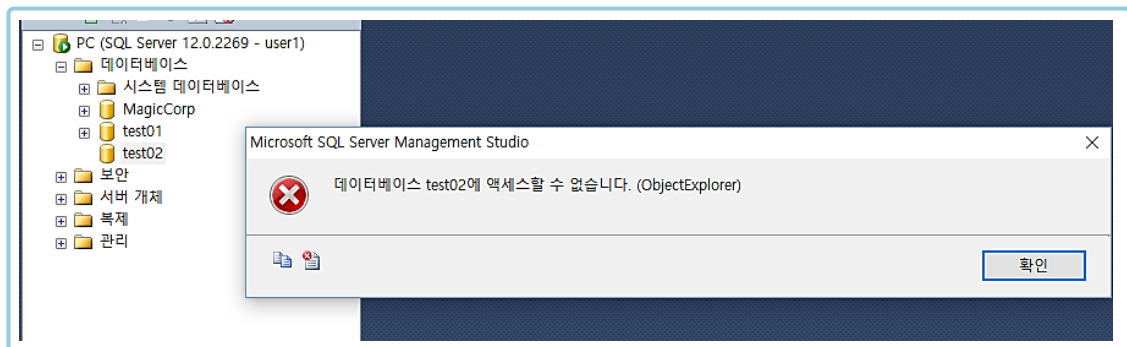
3. MS-SQL에서의 권한 부여

③ MS-SQL 재 시작 후 SQL-Server 인증 방식으로 해서 user1 로그인

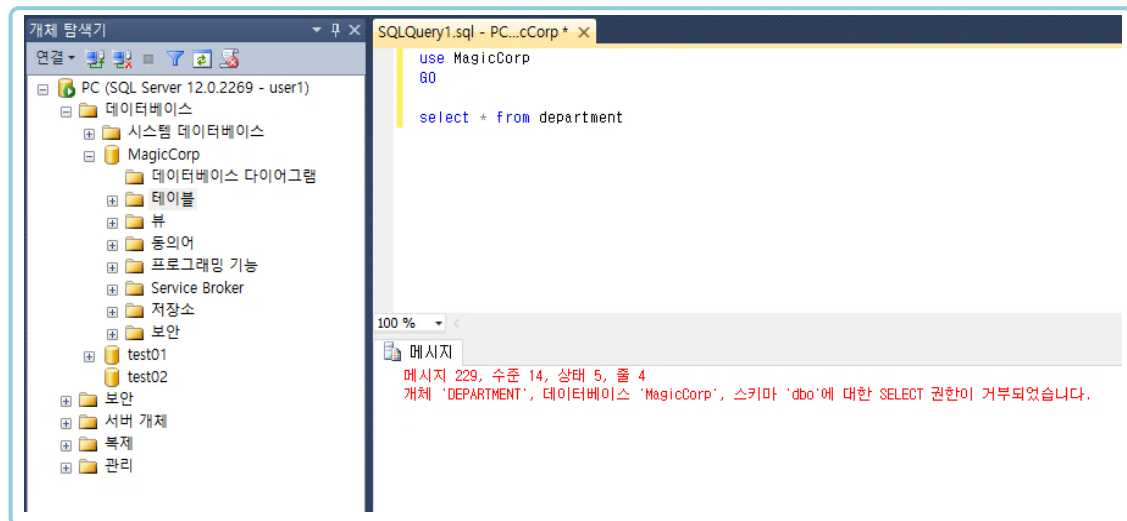


④ user1 로그인

● test02 DB에는 역할이 없으므로 접근 불가



● MagicCorp에 접근은 가능하지만 권한 부여된 것이 없어서 테이블 접근은 불가능함



● 권한 부여

3. MS-SQL에서의 권한 부여

- ⑤ T-SQL을 이용한 로그인 객체와 사용자 등록
 - MS-SQL을 종료하고 재 시작함
 - Windows 인증 모드로 연결하여 관리자가 되어야 함
 - user3 계정을 만들

```
USE master
GO

CREATE LOGIN [user3]
WITH PASSWORD = '12345',
DEFAULT_DATABASE = [master],
CHECK_POLICY = ON,
CHECK_EXPIRATION = OFF
GO

USE MagicCorp
GO

CREATE USER [user3]
FOR LOGIN [user3]
GO
```

100 % <

메시지
명령이 완료되었습니다.

- ⑥ user3에게 DEPARTMENT 테이블에 대한 검색(Select) 및 수정(Update) 권한 부여(T-SQL 이용)
 - 허가를 거부하거나 해지하려면 DENY 또는 REVOKE를 씀

```
use MagicCorp
GO

GRANT select, update
ON department
to user3
GO
```

100 % <

메시지
명령이 완료되었습니다.

● 권한 부여

3. MS-SQL에서의 권한 부여

⑦ user3로 로그인하여 DEPARTMENT 검색



```
SQLQuery1.sql - PC...cCorp * X
use MagicCorp
GO

select * from DEPARTMENT
```

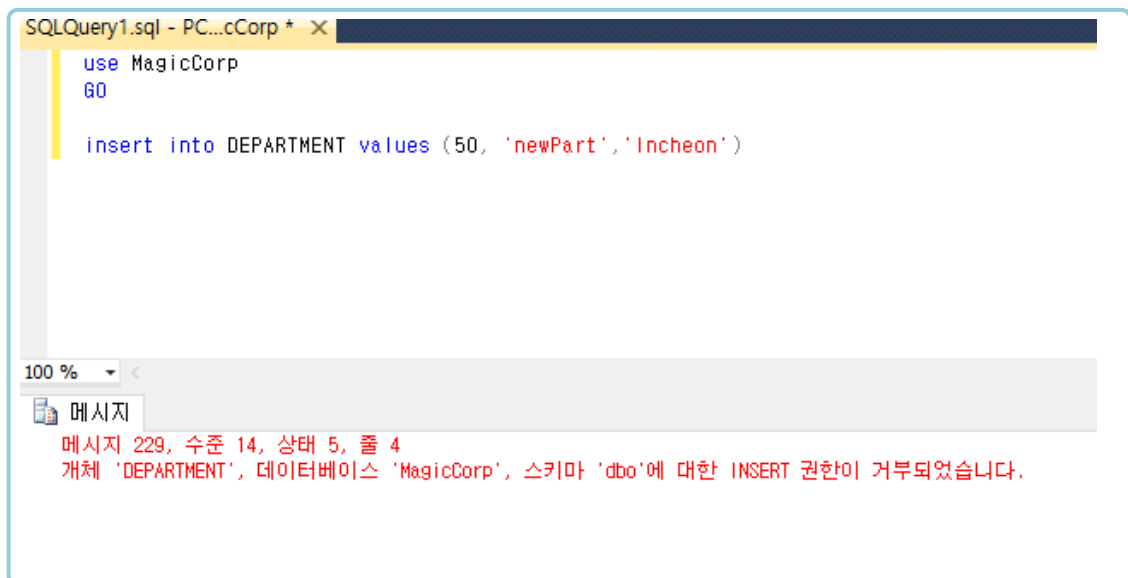
100 % <

결과 메시지

	DNO	DNAME	LOC
1	10	Accounting	Seoul
2	20	Human	Incheon
3	30	Sales	Yungin
4	40	Computing	Suwon

⑧ user3로 로그인하여 DEPARTMENT에 새로운 튜플 삽입

- insert 권한이 없음으로 삽입이 불가능 함



```
SQLQuery1.sql - PC...cCorp * X
use MagicCorp
GO

insert into DEPARTMENT values (50, 'newPart', 'Incheon')
```

100 % <

메시지

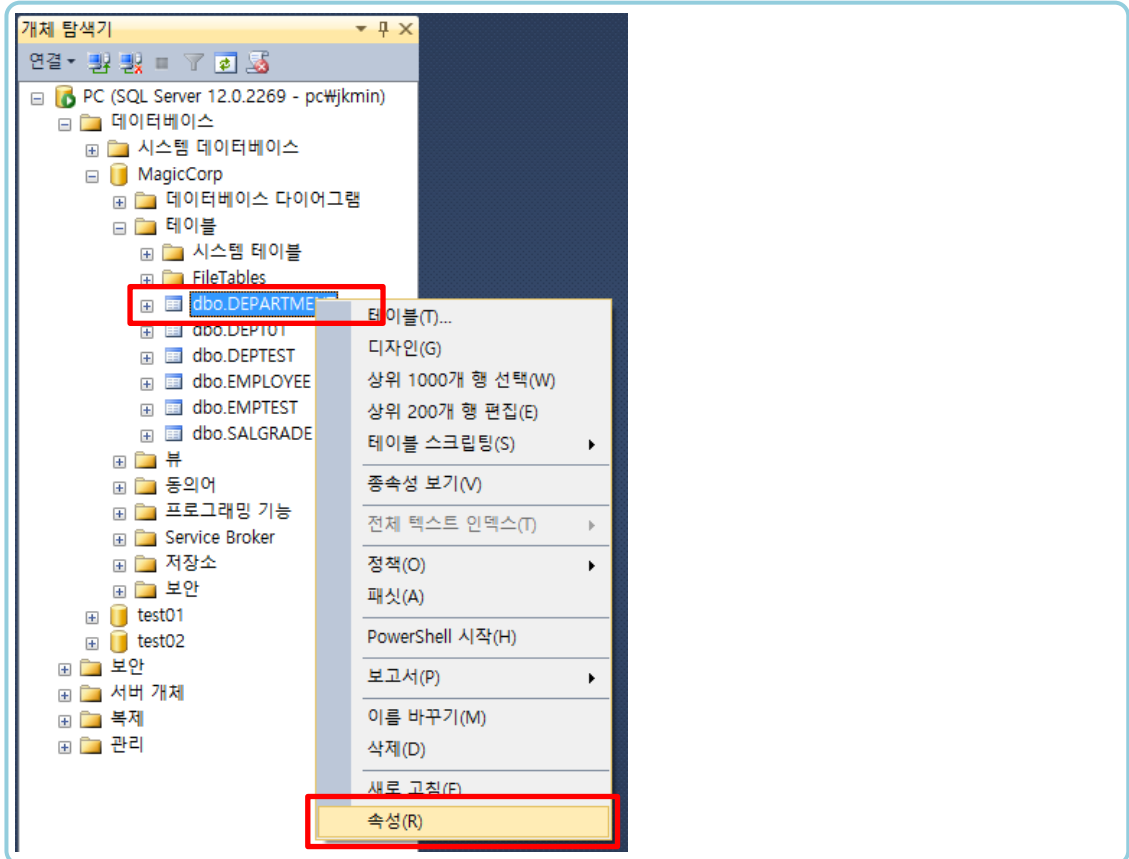
메시지 229, 수준 14, 상태 5, 줄 4
개체 'DEPARTMENT', 데이터베이스 'MagicCorp', 스키마 'dbo'에 대한 INSERT 권한이 거부되었습니다.

- 권한 부여

3. MS-SQL에서의 권한 부여

⑨ 관리자로 로그인하여 user3의 DEPARTMENT 테이블에 insert 권한 추가 부여

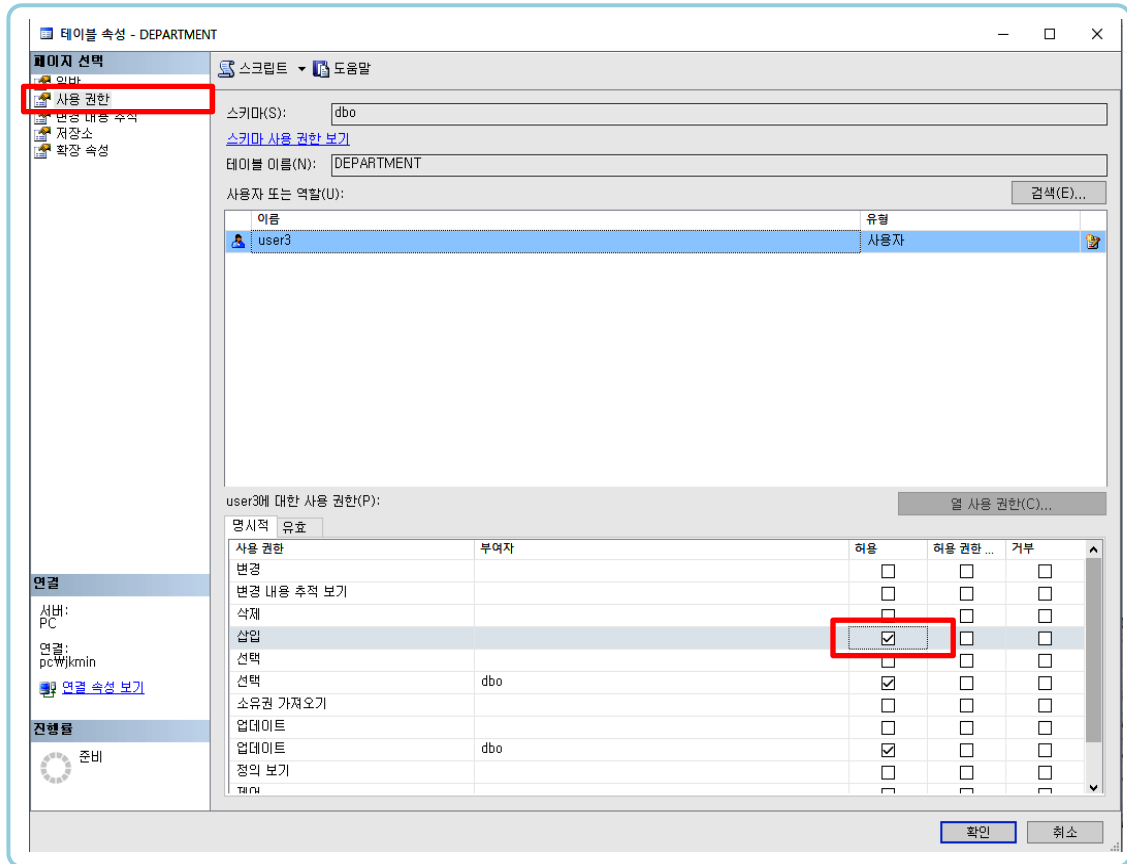
- insert 권한이 없음으로 삽입이 불가능 함



● 권한 부여

3. MS-SQL에서의 권한 부여

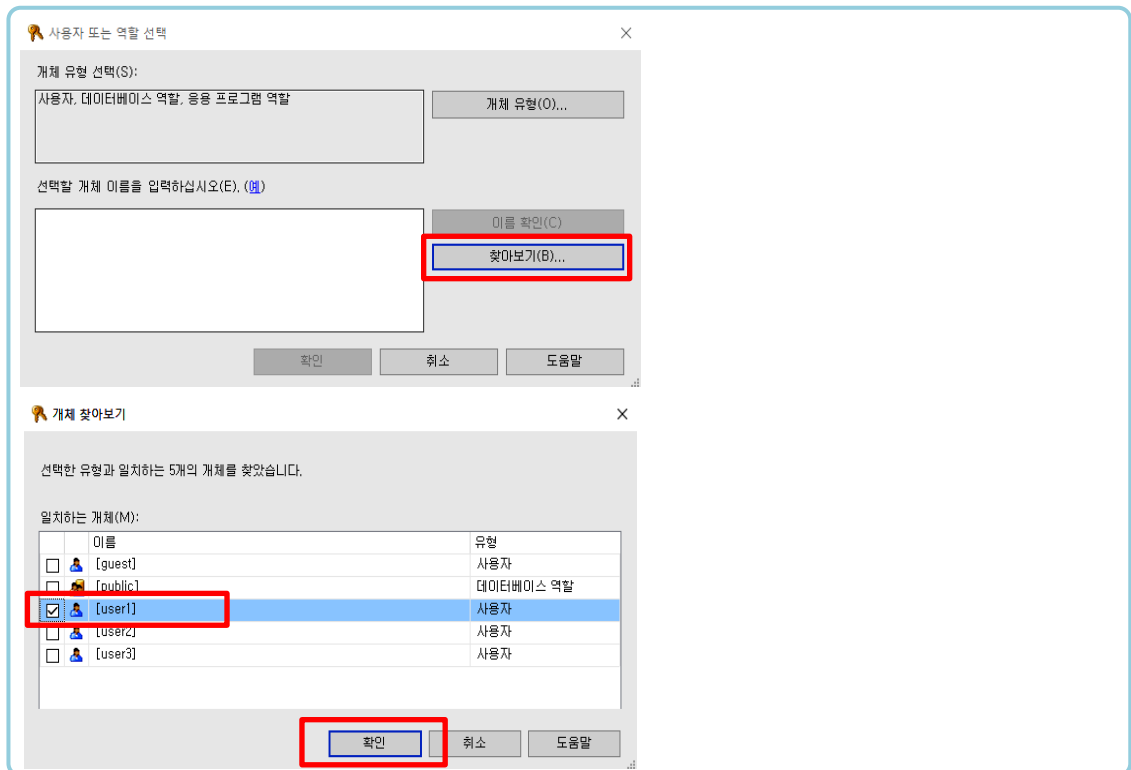
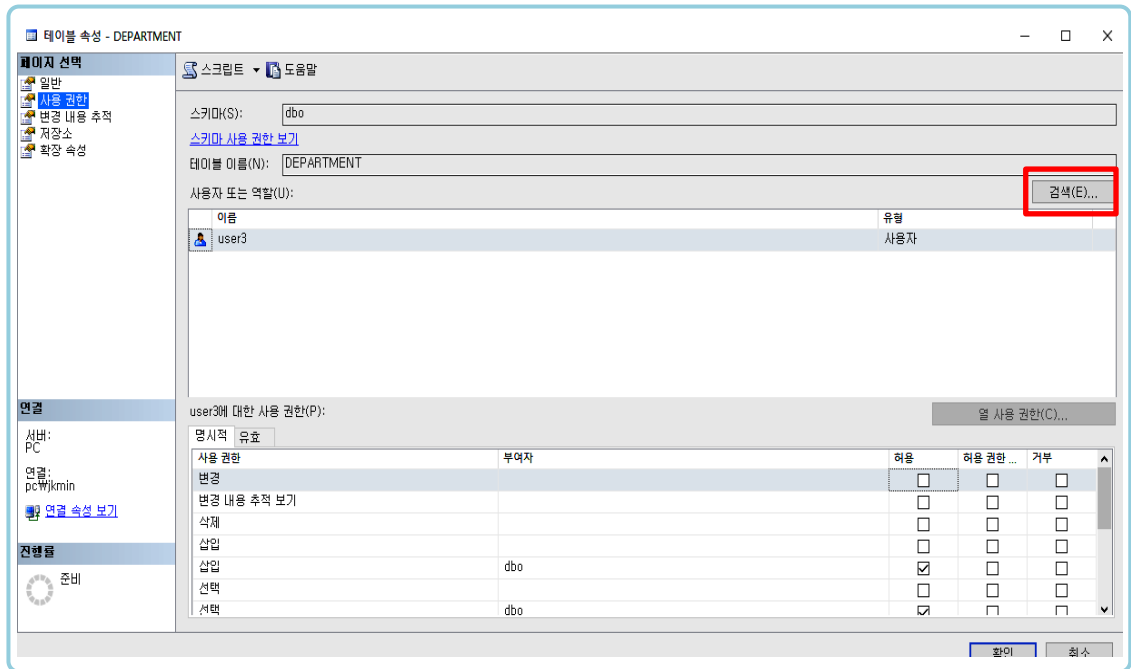
⑨ 관리자로 로그인하여 user3의 DEPARTMENT 테이블에 insert 권한 추가 부여



● 권한 부여

3. MS-SQL에서의 권한 부여

- ⑩ 관리자로 로그인하여 user1에게도 DEPARTMENT 테이블에 select insert 권한 추가 부여



● 권한 부여

3. MS-SQL에서의 권한 부여

- ⑩ 관리자로 로그인하여 user1에게도 DEPARTMENT 테이블에 select insert 권한 추가 부여

사용자 또는 역할(U):

이름	유형
user1	사용자
user3	사용자

user1에 대한 사용 권한(P):

명시적	유효	부여자	허용	허용 권한 ...	거부
사용 권한			<input type="checkbox"/>	<input type="checkbox"/>	
변경			<input type="checkbox"/>	<input type="checkbox"/>	
변경 내용 추적 보기			<input type="checkbox"/>	<input type="checkbox"/>	
삭제			<input type="checkbox"/>	<input type="checkbox"/>	
삽입			<input checked="" type="checkbox"/>	<input type="checkbox"/>	
선택			<input checked="" type="checkbox"/>	<input type="checkbox"/>	
소유권 가져오기			<input type="checkbox"/>	<input type="checkbox"/>	
업데이트			<input type="checkbox"/>	<input type="checkbox"/>	

확인

- ⑪ 이후 user1, user3로 로그인 시 DEPARTMENT 테이블에 대한 검색 / 삽입이 가능해짐

핵심요약

1. 보안

■ 통제

■ 보안

- 테이블을 구성하는 튜플 집합에 대한 테이블의 부분 집합을 결과로 반환하는 연산자

■ 보안에 대한 통제

① 법적, 윤리적 통제

- 법, 윤리 ⇨ 심리적 보안

② 행정, 관리적 통제

- 오용을 탐지하고 방지함

③ 물리적 통제

- 적극적, 물리적 보안으로 위반을 예방, 탐지함

④ 기술적 통제

- 하드웨어 통제
- 소프트웨어 통제
- 데이터베이스 통제 : DBMS 보안 서브 시스템 ⇨ 접근 제어

핵심요약

1. 보안

■ 접근 제어

- 권한이 부여되지 않은 데이터의 검색이나 변경을 방지함

① 직접 접근 제어

- 사용자 신분증 확인(ID)
- 신분증 본인 확인을 위한 인증(PASSWORD)
- 요청 데이터 객체에 대한 요청 연산 권한(권한 부여)

② 간접 접근 제어

- 한 장소에서 다른 장소로의 데이터 흐름 제어
- 개인의 비밀 데이터로부터 작성된 통계정보에 대한 추론 제어
- 전송 이나 저장 데이터의 암호화 시스템 작동과 사용자 상호작용의 감시

■ 접근 제어 구조

- 신분증 : 지문, 성문, ID
- 인증 : 권한 부여 테이블(사용자, 접근 가능한 데이터와 연산)

데이터베이스 정보

요구되는 연산(메인 메모리에 있는 권한 부여 테이블, 사용자 활동 로깅)

■ 권한 부여 규정

- 권한 부여 규정은 DCL로 명세함
- 명세된 규정은 데이터 디렉터리에서 관리함

핵심요약

2. 권한 부여

■ 뷰 기반 기법

■ 뷰 기반 기법이란?

- 뷰를 이용한 권한 부여
- 특정 뷰에 대하여 특정 사용자만 보도록 지정함
- 민감한 데이터를 권한이 없는 사용자로부터 은닉할 수 있음
- 릴레이션의 수직적 / 수평적 서브셋을 제한할 수 있음

■ 뷰 기반 기법의 문제점

```
CREATE VIEW ST1
AS SELECT SNO, NAME, SAL
FROM STUDENT
WHERE YEAR = 4
```

- 튜플 삽입의 제약

```
INSERT INTO S1(SNO, NAME, YEAR): <'E5', 'LEE', 5>
```

■ 뷰 기반 기법의 문제점

- 알려진 값의 NULL값 : ST는 DEPTNO가 12인 뷰인데 삽입될 때는 12대신 NULL이 들어감

```
CREATE VIEW ST2
AS SELECT SNO, YEAR
FROM STUDENT
WHERE DEPTNO = 12
```

```
INSERT INTO ST2 (SNO, YEAR):
<'E5', 2>
```

핵심요약

2. 권한 부여

■ GRANT / REVOKE 기법

- 특정 데이터와 연산을 특정 사용자만 수행할 수 있도록 권한 부여하는 DCL 문
 - GRANT문 : 자신에게 허용된 권한을 다른 사용자에게 부여하는 구문
 - REVOKE문 : 다른 사용자에게 허용한 권한을 철회하는 구문
 - DENY문 : 다른 사용자에게 특정 권한을 불허하는 구문

■ GRANT 구문

GRANT [권한ALL] ON 데이터객체 TO 사용자

- 데이터객체가 테이블 또는 뷰일 경우 : SELECT, INSERT, UPDATE, DELETE, REFERENCE 등 사용 권한
- 데이터객체가 데이터베이스일 경우 : CREATE [DB, TABLE, VIEW] 등의 권한
 - ▶ 주의점 : DROP 권한은 일반적으로 생성자(주인)만 가짐
- ALL : 모든 권한을 말함

■ REVOKE / DENY 구문

REVOEK 권한 ON 데이터객체 TO 사용자

DENY 권한 ON 데이터객체 TO 사용자

핵심요약

2. 권한 부여

■ MS-SQL에서의 권한 부여

■ 인증 모드

- MS-SQL은 인증과 권한 부여가 분리되어 있음
 - ▶ 인증을 위해서는 로그인 객체가 필요함
 - ▶ 권한 부여를 위해서는 사용자 객체가 필요함
- 윈도우 인증
 - ▶ 별도의 ID나 비밀번호 없이 Windows에 접속한 사용자로 MS-SQL에 연결할 수 있도록 하는 인증방식
- SQL-Server 인증
 - ▶ 윈도우 인증과는 무관하게 SQL-Server에 등록된 로그인 계정으로 인증
 - ▶ Windows 운영체제의 보안과는 상관없이 SQL-Server 계정으로 접속 가능
 - ▶ 보안의 취약성으로 MS사에서는 권장하지 않음
 - ▶ 실무에서는 SQL-Sever 인증을 빈번히 사용함
- 인증모드 변경 이후 컴퓨터 재시작 필수임

■ DB 사용자

- 로그인이 되었다고 MS-SQL Server가 관리하는 모든 데이터베이스들을 자동 접근할 수 있다면 심각한 보안 위협이 됨
 - ▶ MS-SQL은 인증과 권한 부여가 분리되어 있음

■ Login 객체 생성 및 사용자 등록

- SSMS를 이용하여 user1 로그인 객체를 생성하고 MagicCorp 데이터베이스에 사용자를 등록함
 - ▶ SQL-Server 인증 방식으로 만들