

• DB구현 •

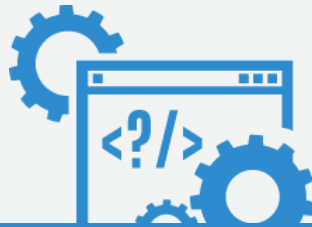
로깅과 보완



학습내용

❖ 로깅

❖ 보안



학습목표

❖ 로그와 보안의 정의 및 필요성을 설명할 수 있다.

❖ MySQL의 로그 정책을 수립할 수 있다.

❖ MySQL의 보안요소를 설정할 수 있다.

로깅

로그의 이해

➤ 로그의 정의

로그

- 로그 레코드의 연속
- 로그 레코드는 데이터베이스와 사용자의 모든 활동 작업을 기록한 데이터
- 문제 발생 시 문제의 원인 및 에러 메시지를 기록하고, 사용자의 모든 질의 요청에 대한 이전 데이터 값과 새로운 데이터 값을 저장
- 데이터 파일이 저장된 저장장치 이외의 별도의 안정적 저장장치에 기록

➤ 로그의 사용 목적

- 다양한 종류의 로그를 사용하여 DBMS 서버의 문제를 진단하고, 문제로부터 복구
- 문제 발생 시점을 파악하고 문제 발생 이전의 시점으로 데이터를 복원하는데 이용
- 서버의 성능을 향상

로깅

로그의 이해

➤ 로그의 종류

에러 로그	서버의 문제 발생 시 원인 파악에 사용
일반 쿼리 로그	사용자의 활동 사항을 모니터링하는 목적으로 사용
느린 쿼리 로그	느리게 실행되는 질의의 원인을 파악하는 목적으로 사용
이진 로그	서버의 오류(크래시) 발생 후, 테이블 복구 목적으로 사용
릴레이 로그	복제 서버(리플리케이션)가 구성되어 있는 시스템에서 마스터 서버로부터 요청된 이벤트를 파악하는 목적

➤ 에러 로그

- 서버의 시작 및 종료 기록
- 문제나 예외적인 조건에 대한 메시지 기록
- 서버의 성능을 향상

➤ 일반 쿼리 로그

- 클라이언트 연결, 클라이언트로 부터의 실행되는 질의 기록
- 서버의 활동 상황 등이 이벤트를 기록

로깅

로그의 이해

➤ 느린 쿼리 로그

- 실행 속도가 현저하게 느린 질의를 선별하고 재작성하기 위한 정보를 제공
- 시스템 변수 long_query_time(기본값 10초)의 값으로 느린 질의를 결정
- 실시간으로 long_query_time에서 결정한 값보다 처리시간이 오래 걸리면 느린 질의 로그에 기록되고, 인덱스를 사용하지 않는 질의 또한 로그에 기록

➤ 이진 로그

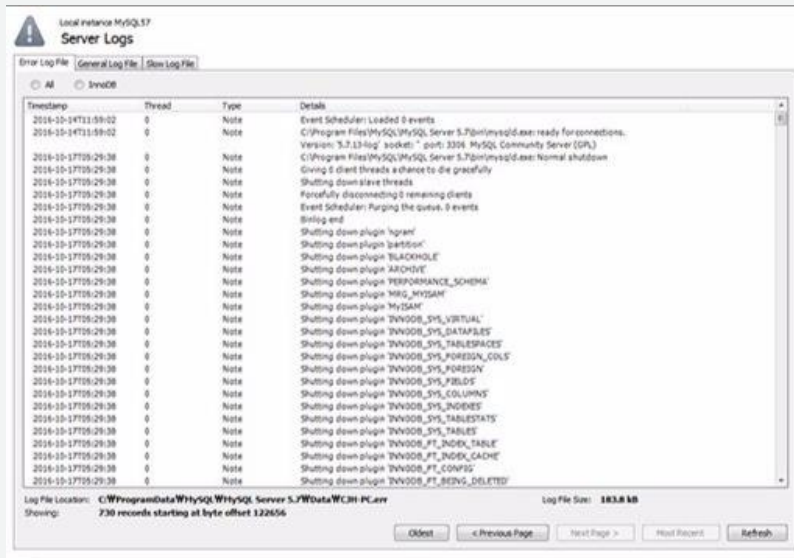
- INSERT, UPDATE, DELETE, CREATE TABLE, DROP TABLE, GRANT 등에 의해서 수행된 수정 기록 포함
- 로그 데이터는 이진 포맷으로 부호화된 데이터 수정 이벤트가 기록
- 크래시 발생 이후, 테이블 복구에 백업 데이터 파일을 이용하여 사용

➤ 릴레이 로그

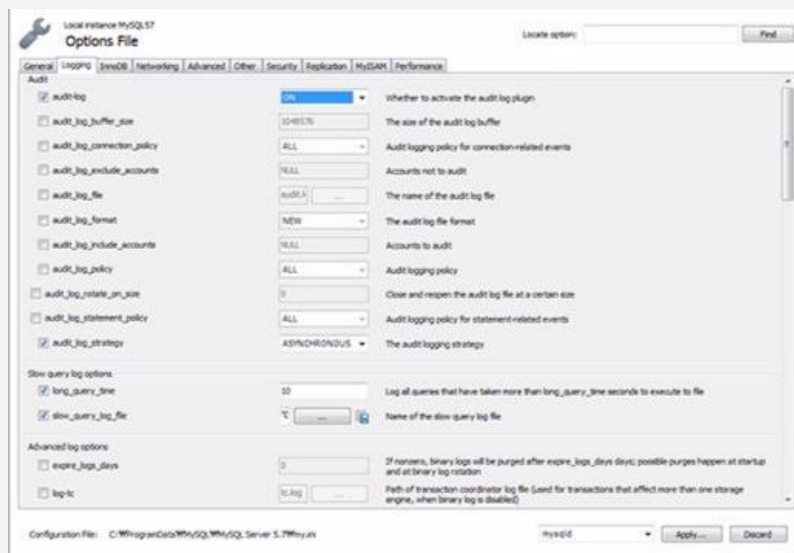
- DDL 문 요청으로 발생하는 메타데이터(테이블 구조 변경) 수정 시 발생할 수 있는 크래시로부터 복구
- 요청된 DDL 문이 정상적으로 수정되었는 확인하고 미반영 시 DDL 로그로부터 메타데이터를 재수정

MySQL의 로그 설정

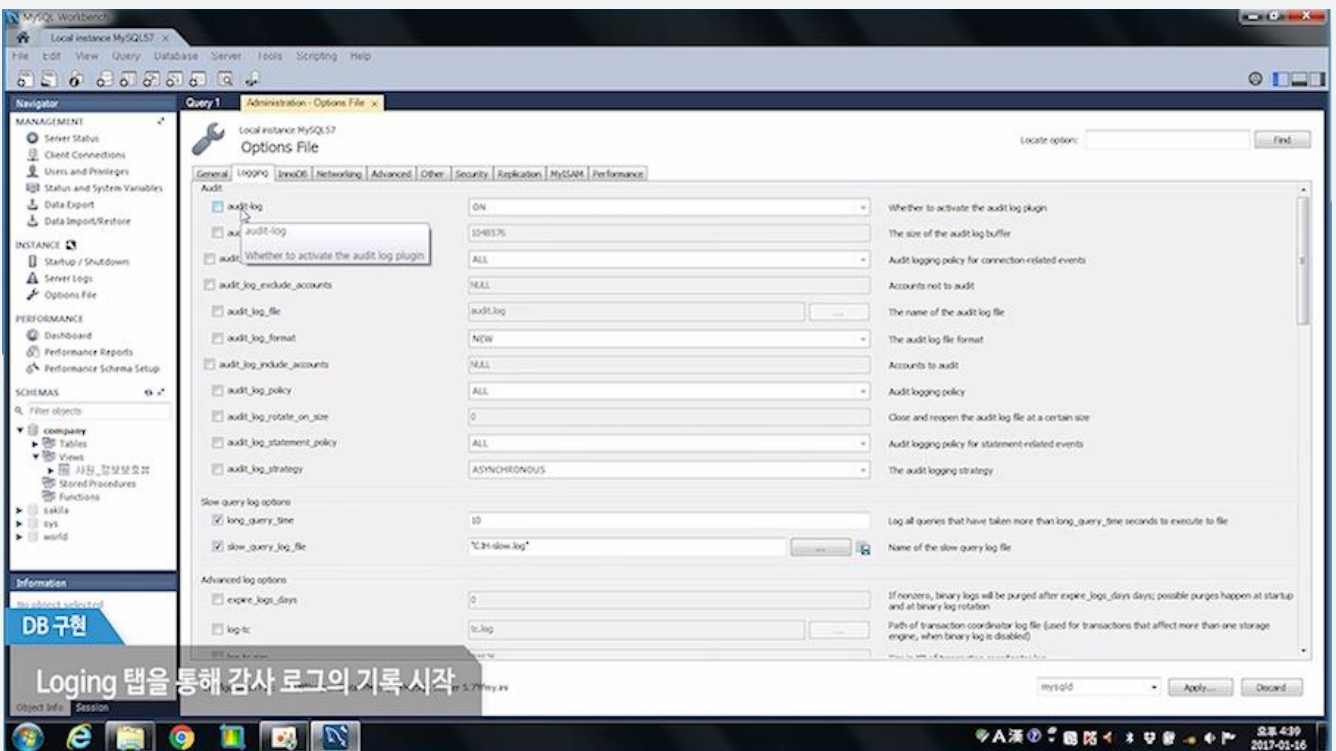
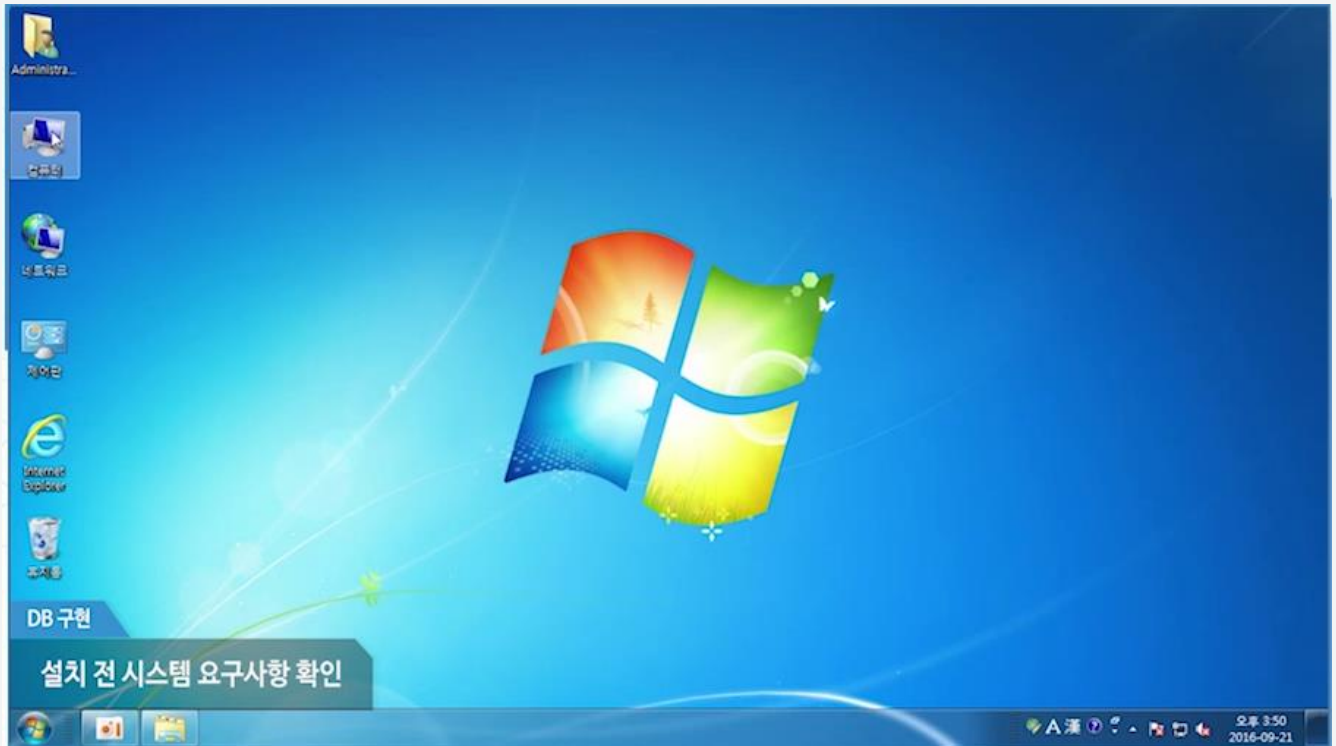
MySQL Workbench의 Server Logs 메뉴



- Server Logs 메뉴에서 로그 파일들을 확인할 수 있습니다.



- MySQL Workbench의 Option File 메뉴의 Logging 탭에서 다양한 옵션들을 확인할 수 있습니다.



보안

보안의 이해

➤ 보안의 개념

보안

- 정보 시스템과 시스템 내부의 보안을 위해 데이터의 기밀성, 무결성, 가용성을 확인하고 측정
- 중앙 집중식의 데이터 관리 장치인 DBMS에서 완전한 데이터를 유지하기 위해 필요한 과정

➤ 데이터의 기밀성

- 데이터에 인가자가 접근 할 경우 보호를 보증
- 인가된 데이터에 사용자가 접근하는 경우, 인가된 목적으로만 사용하도록 제한

➤ 데이터의 무결성

- 데이터베이스 시스템의 보안 구조 내부에서 데이터의 일관성을 보장
- 오류나 이상(Anomaly)이 발생하더라도 일관성을 유지

➤ 데이터의 가용성

- 권한이 부여된 사용자가 필요할 때마다 불필요한 방해 없이 데이터에 접근할 수 있는 특성

보안 설정

➤ 사용자 암호 정책 설정

- 접근 권한을 설정하고 강제적 암호에 대한 암호화 및 교체 정책 설정

➤ SET PASSWORD 구문형식

SET PASSWORD FOR <사용자명> = PASSWORD('패스워드')

➤ 뷰 정의

- 허가된 사용자가 접근할 수 있는 데이터 범위를 보호하고 제어하기 위해서 데이터 뷰를 정의

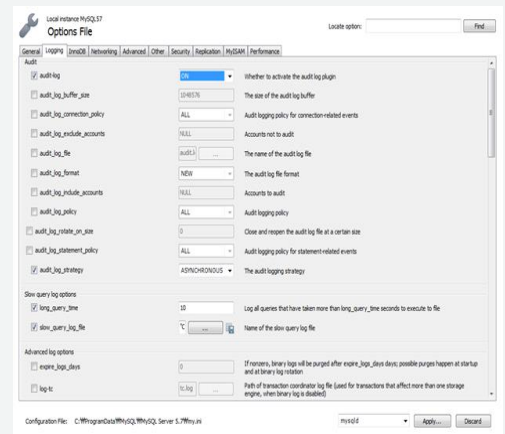
➤ 뷰 정의 구문형식

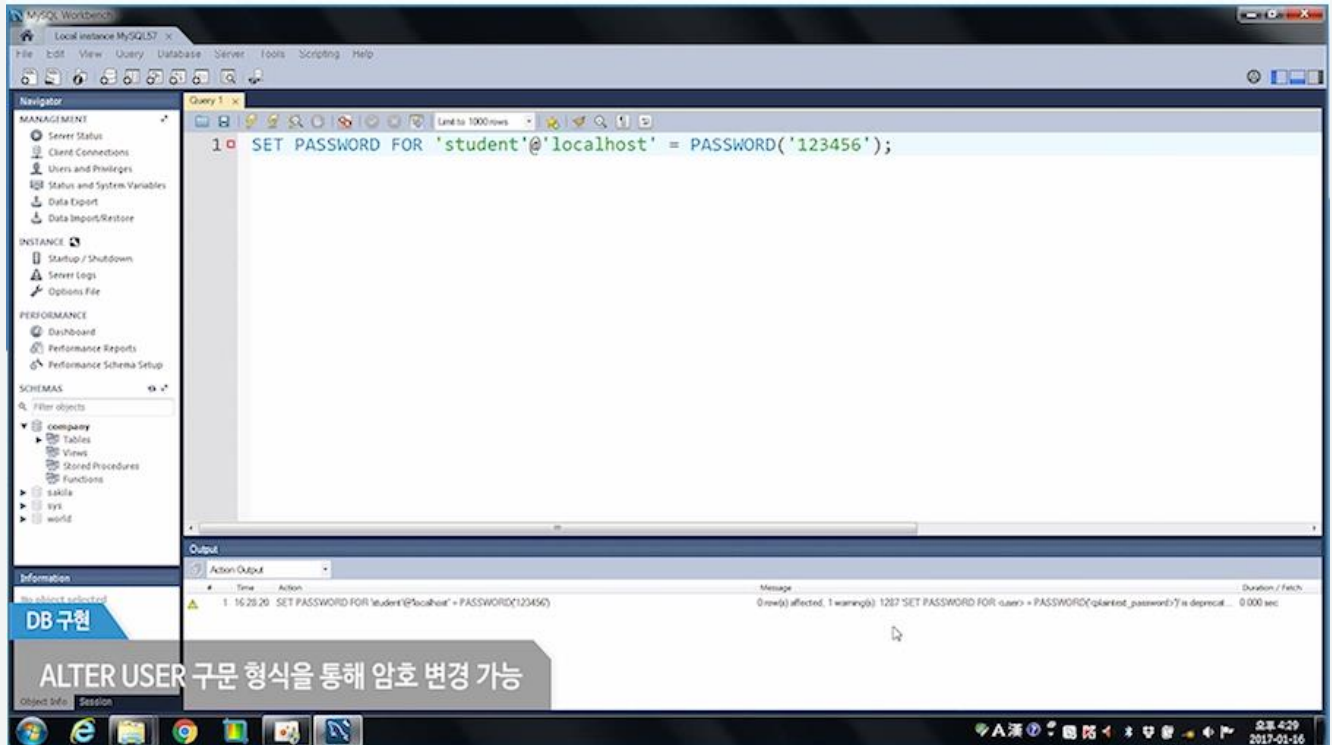
CREATE VIEW 뷰이름 AS
SELECT 컬럼명 1, 컬럼명2, ..., 컬럼명n
FROM 테이블명
[WHERE 조건]
[WITH CHECK OPTION]

➤ DBMS 사용 감시

- DBMS 내부에서 사용자의 데이터 사용을 감시, 감사 로그(audit log)를 생성

➤ MySQL에서의 감시 로그 설정





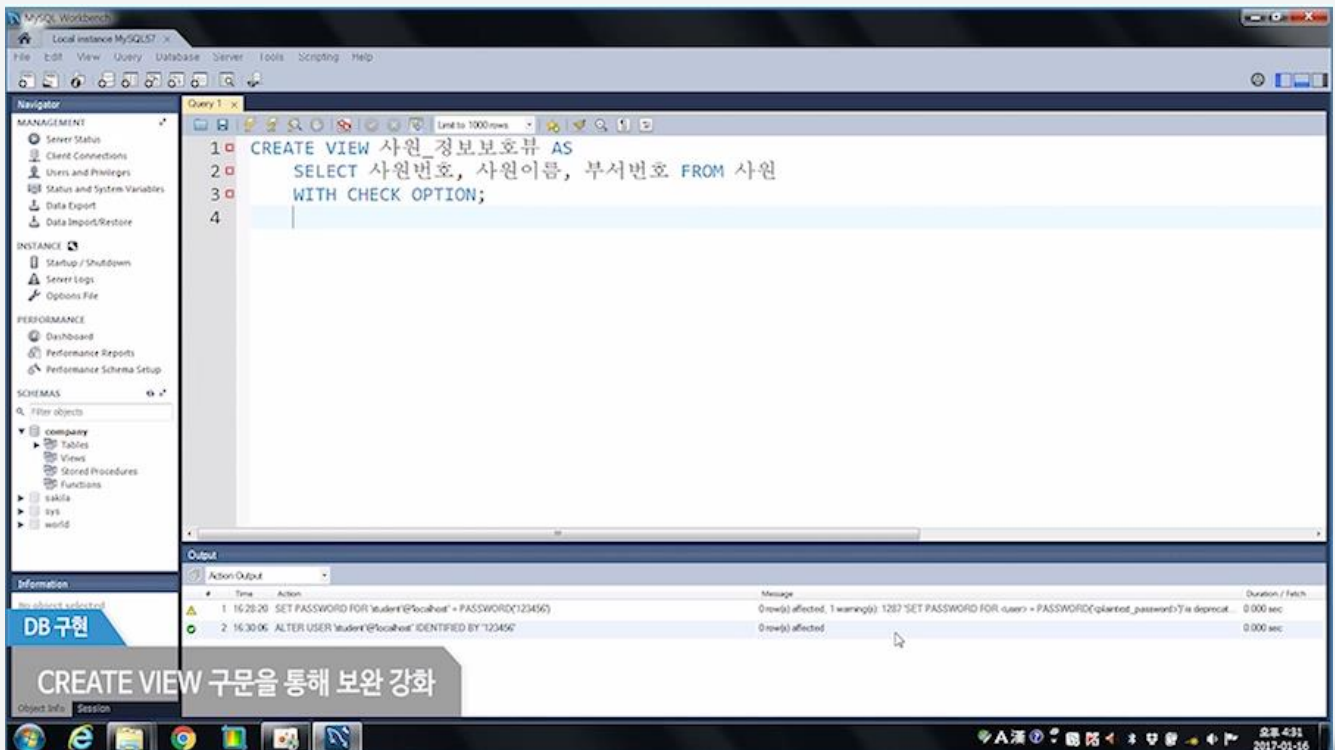
The screenshot shows the MySQL Workbench interface. The query editor contains the following SQL statement:

```
1 SET PASSWORD FOR 'student'@'localhost' = PASSWORD('123456');
```

The Output pane at the bottom shows the execution results:

Time	Action	Message	Duration / Fetch
1 16:29:20	SET PASSWORD FOR 'student'@'localhost' = PASSWORD('123456')	0 row(s) affected, 1 warning(s): 1287 SET PASSWORD FOR user = PASSWORD() is deprecated	0.000 sec

ALTER USER 구문 형식을 통해 암호 변경 가능



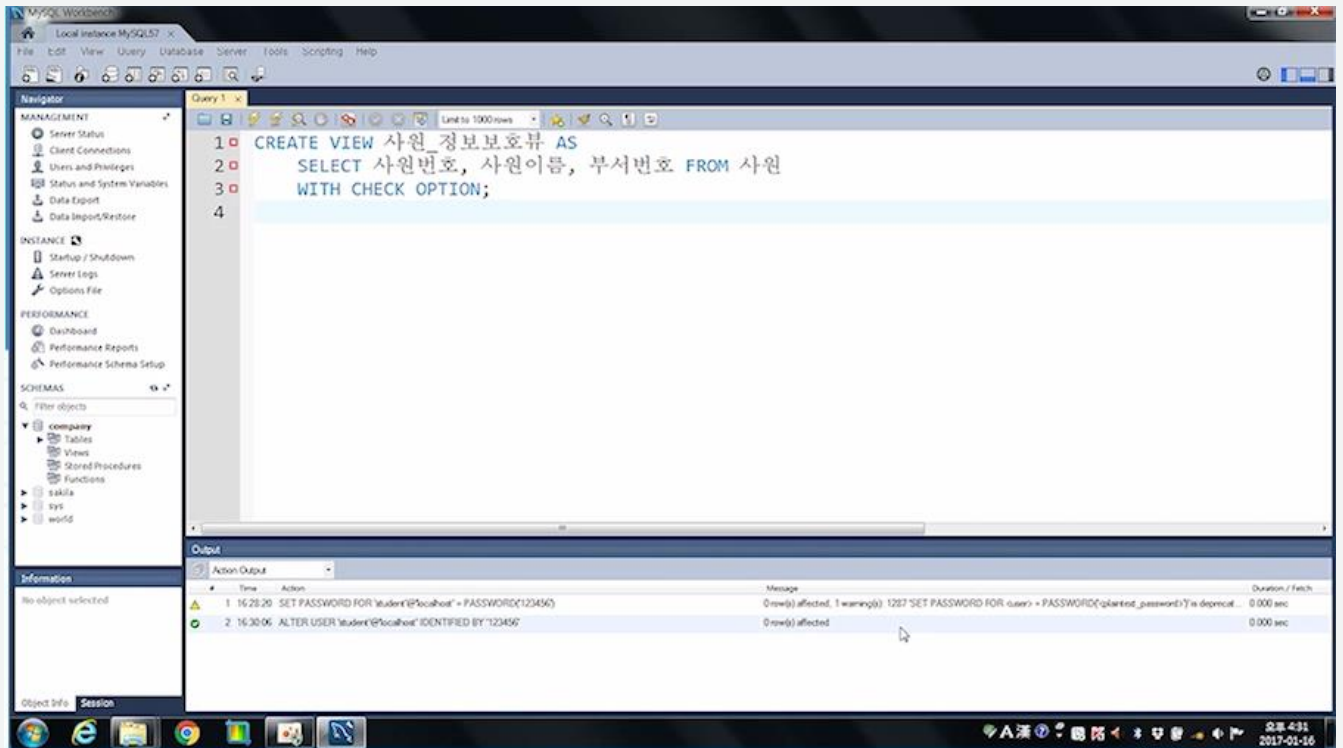
The screenshot shows the MySQL Workbench interface. The query editor contains the following SQL statements:

```
1 CREATE VIEW 사원_정보보호부 AS
2 SELECT 사원번호, 사원이름, 부서번호 FROM 사원
3 WITH CHECK OPTION;
4
```

The Output pane at the bottom shows the execution results for the second statement:

Time	Action	Message	Duration / Fetch
2 16:30:06	ALTER USER 'student'@'localhost' IDENTIFIED BY '123456'	0 row(s) affected	0.000 sec

CREATE VIEW 구문을 통해 보안 강화





핵심요약

로그

❖ 로그의 정의

- 로그 레코드는 데이터베이스와 사용자의 모든 활동 작업을 기록한 데이터
- 문제 발생 시 문제의 원인 및 에러 메시지를 기록하고, 사용자의 모든 질의 요청에 대한 이전 데이터 값과 새로운 데이터 값을 저장
- 데이터 파일 저장된 저장장치 이외의 별도의 안정적 저장장치에 기록

❖ 로그의 사용 목적

- 다양한 종류의 로그를 사용하여 DBMS 서버의 문제를 진단하고, 문제로부터 복구
- 문제 발생 시점을 파악하고 문제 발생 이전의 시점으로 데이터를 복원하는데 이용

❖ 서버의 성능을 향상 로그의 종류

종류	사용 목적
에러 로그	서버의 문제 발생 시 원인 파악에 사용
일반 쿼리 로그	사용자의 활동 사항을 모니터링하는 목적으로 사용
느린 쿼리 로그	느리게 실행되는 질의의 원인을 파악하는 목적으로 사용
이진 로그	서버의 오류(크래시) 발생 후, 테이블 복구 목적으로 사용
릴레이 로그	복제 서버(리플리케이션)가 구성되어 있는 시스템에서 마스터 서버로부터 요청된 이벤트를 파악하는 목적



핵심요약

보안

❖ 보안의 개념

- 정보 시스템과 시스템 내부의 보안을 위해 데이터의 기밀성, 무결성, 가용성을 확인하고 측정
- 중앙 집중식의 데이터 관리 장치인 DBMS에서 완전한 데이터를 유지하기 위해 필요한 과정

보안 데이터의 특성	내용
데이터의 기밀성	<ul style="list-style-type: none">▪ 통합된 데이터의 집합 - 스키마 생성 및 관리, 제약사항 추가/삭제, 뷰 및 저장 프로시저 관리 등▪ 저장된 데이터의 집합 - 저장 장치 및 메모리 관리, 백업 및 복원 설정 등▪ 공용 데이터의 집합 - 사용자 추가/삭제, 사용자 권한 관리, 보안 설정 등
데이터의 무결성	<ul style="list-style-type: none">▪ 데이터베이스 시스템의 보안 구조 내부에서 데이터의 일관성을 보장▪ 오류나 이상(Anomaly)이 발생하더라도 일관성을 유지
데이터의 가용성	권한이 부여된 사용자가 필요할 때마다 불필요한 방해 없이 데이터에 접근할 수 있는 특성



핵심요약

보안

❖ 보안 설정

- 사용자 암호 정책 설정: 접근 권한을 설정하고 강제적 암호에 대한 암호화 및 교체 정책 설정 (SET PASSWORD 구문형식)

뷰 정의

- 허가된 사용자가 접근할 수 있는 데이터 범위를 보호하고 제어하기 위한 목적으로 사용 (뷰 정의 구문형식)

❖ DBMS 사용 감시

- DBMS 내부에서 사용자의 데이터 사용을 감시, 감사 로그(audit log)를 생성