DBMS(My-SQL) 감사

1. 목적

* 작업자의 Login, DML, DDL Log 기록 및 접근 제어

1. 설계

* Audit 정책 수립
* 사용자 및 사용자별 권한 수립
* Log 저장 및 소산 방법 논의

1. 구현

* DBMS user 생성 및 권한 구분

root: all privileges(DCL(Data Control Language) – GRANT, REVOKE)

1. **접속 제한**

로컬에서만 접속 - GRANT ALL privileges ON DB.\* TO user@locahost IDENTIFIED BY ‘pw’;

모든 원격지에서 접속 - GRANT ALL privileges ON DB.\* TO user@'%' IDENTIFIED BY ‘pw’;

예) 119.192.X.X 의 IP에서 원격 접속 허용: GRANT ALL privileges ON DB.\* TO user@’119.192.%' IDENTIFIED BY ‘pw’;

예) 119.192.146.202 의 IP에서 원격 접속 허용: GRANT ALL privileges ON DB.\* TO user@’ 119.192.146.202' IDENTIFIED BY ‘pw’;

1. **DML 제한**

user(사용자)에게 test DB 내 모든 TABLE의 모든 권한 부여: grant all privileges on test.\* to user@localhost identified by 'pw';

user(사용자) 에게 test DB 내 모든 table에 권한(select, insert, update) 부여: grant select, insert, update on test.\* to user@localhost identified by 'pw';

* Audit Plugin을 이용한 Database 접근 시 사용자 별 권한 제한

1. 계정별 Filtering(Ver. 5.6.20 이상): user\_name@host\_name format으로 명시

Audit 계정 추가: audit\_log\_include\_accounts

예) SET GLOBAL audit\_log\_include\_accounts = ‘user1@localhost,user2@localhost’;

Audit 예외 계정 추가: audit\_log\_exclude\_accounts

예) SET GLOBAL audit\_log\_exclude\_accounts = ‘root@localhost’;

\* Ver. 5.6.23이하는 모든 사용자의 connect 및 disconnect 로그가 남으며 Ver. 5.6.24이상은 설정된 사용자만 Audit

지속적인 적용을 위해 my.cnf에 해당 옵션 명시

1. command 별 Filtering

audit\_log\_policy : ALL | LOGINS | QUERIES | NONE

•ALL - all events will be logged

•LOGINS - only logins will be logged

•QUERIES - only queries will be logged

•NONE - no events will be logged

* Audit file rotate

1. audit\_log\_rotate\_on\_size 설정

지정된 사이즈만큼 커지고 넘어가게 되면 timestamp의 값을 추가하여 archiving

(default: 0 (don’t rotate the log file))

1. 수동 설정
2. 수동으로 해당 파일 분리: mv /data1/5.6/data/audit.log /data1/5.6/data/audit.log.bak

\* MySQL 의 Data Home Directory는 /data1/5.6/data

\* mv로 옮겨도 file descriptor를 mysql이 가지고 있기 때문에 지속적으로 변경된 파일에 쓰게 된다.

1. audit log를 flush: SET GLOBAL audit\_log\_flush = 1;

기존의 /data1/5.6/data/audit.log.bak을 닫고 새로운 /data1/5.6/data/audit.log 생성

* Audit 파일 테이블로 저장: table을 만들고, XML을 LOAD

Audit\_backup\_Plan.sql

\* 해당 /data1/5.6/data/audit.log.bak 을 테이블로 Load. mv로 해당 파일을 바꾸지 않고 쓰고 있는 파일에 대하여 넣어도 상관없다.

\* 중복을 방지용 UNIQUE U\_RECORD\_ID 추가

\* 필요한 business logic에 맞춰 테이블의 인덱스를 추가 가능

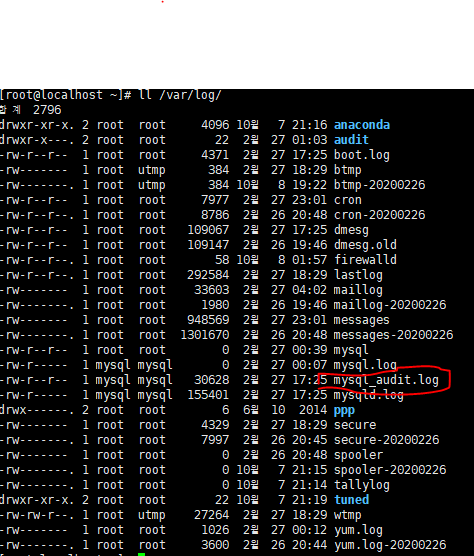
* Audit\_log 파일 저장 경로 및 형식

1. My.cnf 에 아래와 같이 저장 경로 설정

audit\_json\_file=1

audit\_json\_log\_file=/var/log/mysql\_audit.log

1. Log 파일 형식



1. Log 파일 내용

JSON 형식으로 저장되며 Notepad에서 바로 확인가능

날짜, User, 접속 IP, Host IP, 사용자 OS, 사용된 Client 종류 및 버전, 행해진 질의 내용(Query), Query로 산출된 결과의 ROW 수

