18장. 감사기능 (Audit)

18.1 개요

AgensSQL은 데이터베이스 보안 관리자 및 운영자가 감사 로깅 기능을 사용하여 데이터베이스 활동을 추적하고 분석할 수 있도록 합니다. AgensSQL 감사 로깅은 지정된 데이터베이스 이용 정보를 포함한 감사 로그 파일을 생성합니다.
postgresql.conf 또는 postgresql.auto.conf에 지정된 매개변수로 Audit 기능을 제어 할 수 있습니다.

18.1.1 특징

1) Audit 범위
    - ag_audit_statement
    - ag_audit_connect
    - ag_audit_disconnect
2) Audit Log 및 Directory
    - ag_audit_directory
    - ag_audit_filename
3) Audit Log File 관리
    - ag_audit_rotation_size
    - ag_audit_rotation_age
4) Audit Tag
    - ag_audit_tag

18.2 Parameters

postgresql.conf의 매개변수를 사용하여 데이터베이스 Audit을 구성할 수 있습니다. Audit 기능을 사용하기 위해선 기본적으로 logging_collector 설정이 on으로 설정 되어 있어야 합니다. Audit 기능의 경우 서비스 부하 및 Log Disk Full 등의 이슈가 있으므로 서비스에 모니터링이 가능한 경우에만 적용을 권고 합니다.

- **ag_audit**

  데이터베이스 감사 기능을 활성화하거나 비활성화합니다. csv 값은 데이터베이스 감사 기능을 활성화합니다. 이러한 값은 감사 정보가 저장되는 파일 형식을 나타냅니다.
  기본값은 none으로 데이터베이스 감사 기능을 비활성화합니다.

- **ag_audit_directory**

  Audit 로그 파일을 저장 디렉터리를 지정합니다. 디렉터리의 경로는 데이터 폴더에 상대적이거나 절대적일 수 있습니다. 기본값은 ag_audit으로 $PGDATA/ag_audit 디렉토리 입니다.

- **ag_audit_filename**

  감사 정보가 저장될 감사 파일의 파일 이름을 지정합니다. 기본 파일 이름은 ag-audit-%Y%m%d_%H%M%S입니다.

- **ag_audit_rotation_size**

  파일 크기에 따라 로그파일의 교체가 발생합니다. 주석 처리하거나 0으로 설정하면 파일 크기에 따른 파일 교체가 발생하지 않습니다. 단위는 Kb 이며 기본값은 0 입니다.

- **ag_audit_rotation_age**

  로그파일 교체가 발생하는 시간(분)을 지정합니다. 이 기능을 사용하지 않으려면 이 매개변수를 0으로 설정하면 됩니다. 기본값은 0 입니다.

- **ag_audit_connect**
  데이터베이스 연결 시도에 대한 감사 범위를 설정합니다. 연결 시도에 대한 감사를 사용하지 않으려면 none으로 설정합니다. 실패한 연결 시도를 감사하려면 값을 failed 값으로 설정합니다. 모든 연결 시도를 감사하려면 값을 all 값으로 설정합니다. 기본값은 failed 입니다.

- **ag_audit_disconnect**

  연결된 사용자가 데이터베이스 연결 끊김을 감사할 수 있습니다. 연결 끊김 감사를 사용하려면 값을 all 값으로 설정합니다. 사용하지 않으려면 값을 none로 설정합니다. 기본값은 none 입니다.

- **ag_audit_statement**

  세션 감사를 기록할 명령문 클래스를 지정합니다. 가능한 값은 다음과 같습니다
  - READ: SELECT, COPY
  - WRITE: INSERT, UPDATE, DELETE, TRUNCATE, COPY
  - FUNCTION : 함수 호출 및 DO 블록
  - ROLE : 역할 및 권한과 관련된 명령문 (예: GRANT, REVOKE, CREATE/ALTER/Drop ROLE)

- DDL : ROLE 클래스에 포함되지 않은 모든 DDL
- MISC : 기타 명령(예: DISCOVER, FETCH, CHECKPOINT, VACUUM, SET).
- MISC_SET : 기타 SET 명령(예: SET ROLE)
- ERROR: 모든 데이터베이스 오류
- ALL: 위의 내용을 모두 포함합니다
  쉼표로 구분된 목록을 사용하여 여러 클래스를 제공할 수 있습니다. 기본값은 DDL,ERROR입니다.

- **ag_audit_tag**

  이 구성 매개 변수를 사용하여 각 항목에 대한 감사 로그 파일에 포함될 문자열 값을 추적 태그로 지정합니다.

18.3 Audit Log File

감사 로그 파일은 ag_audit 구성 매개 변수의 설정에 따라 CSV 형식으로 생성됩니다. 다음 표에는 Audit 로그의 csv Logfile에 나타나는 순서대로 필드가 나열되어 있습니다.

(예시 Log

2023-03-02 16:17:31.859
KST,"agens","postgres",9819,"210.104.181.77:35837",64004d8b.265b,3,"SELECT",2023-03-02 16:17:31
KST,3/4,0,AUDIT,00000,"select * from test;",,,,"SESSION",,,,,,,"asql",,"READ","AgensAudit","statement")

Field	**Description**
log_time	시간 (ex. 2023-03-02 16:17:31.859 KST)
User	접속 User (ex. agens)
Database	접속 Database (ex. postgres)
process_id	OS Process_id (ex. 9819)
Host	접속 Host 정보 (ex. "210.104.181.77:35837)
session_id	접속 Session Id (ex. 64004d8b.265b)
session_line_num	세션내의 작업 순서 (ex. 3)
process_status	처리 상태 (ex. SELECT)
session_start_time	세션이 시작된 시간 (2023-03-02 16:17:31 KST)

virtual_transactio_id	가상의 트랜잭션 ID (ex. 3/4)
transaction_id	트랜잭션 ID (ex. 0)
error_severity	오류여부, Error의 경우 Error 아닐경우 AUDIT (ex. AUDIT)
sql_state_code	SQL 반환 코드 (ex. 00000)
message	감지한 SQL (ex. select * from test;)
audit_type	감사 유형 (ex. SESSION)
query	Error의 경우 Error SQL
query_pos	Error의 경우 Error 위치
application_name	접속 AP명 (ex. asql)
command_tag	작업 형태 (ex. READ)
audit_tag	설정된 Audit 태그 (ex. AgensAudit)
type	감지된 Audit 타입 (ex. statement)

18.3.1 Examples

postgresql.conf 파일에 다음과 같은 구성이 있는경우

```
logging_collector = on
ag_audit = 'csv'
ag_audit_connect = 'all'
ag_audit_disconnect = 'all'
ag_audit_statement = 'all'
ag_audit_tag = 'AgensAudit'
```

asql을 이용하여 Audit을 확인 합니다. (Audit 경로 $PGDATA/ag_audit/)

- Query

```
# asql -U agens -d postgres -h 210.104.181.77 -p 5432
asql (13.7)
Type "help" for help.
```

- Audit Log

```
2023-03-02 17:03:46.625
KST,"agens","postgres",10268,"210.104.181.77:35841",64005862.281c,1,"authentication",2023-03-02
17:03:46 KST,3/34,0,AUDIT,00000,"connection authorized: user=agens database=postgres
```

application_name=asql",,,,,,,,,,,"",,,"AgensAudit","connect"

- Query

```
postgres=# SHOW ag_audit_connect;
 ag_audit_connect
------------------
 all
(1 row)
```

- Audit Log

```
2023-03-02 17:03:46.625
KST,"agens","postgres",10268,"210.104.181.77:35841",64005862.281c,2,"SHOW",2023-03-02
17:03:46 KST,3/35,0,AUDIT,00000,"SHOW
ag_audit_connect;",,,,"SESSION",,,,,,,,"asql",,"MISC","AgensAudit","statement"
```

- Query

```
postgres=# SHOW ag_audit_statement;
 ag_audit_statement
--------------------
 all
(1 row)
```

- Audit Log

```
2023-03-02 17:03:46.625
KST,"agens","postgres",10268,"210.104.181.77:35841",64005862.281c,3,"SHOW",2023-03-02
17:03:46 KST,3/36,0,AUDIT,00000,"SHOW
ag_audit_statement;",,,,"SESSION",,,,,,,,"asql",,"MISC","AgensAudit","statement"
```

- Query

```
postgres=# CREATE ROLE adminuser;
CREATE ROLE
```

- Audit Log

```
2023-03-02 17:03:46.625
KST,"agens","postgres",10268,"210.104.181.77:35841",64005862.281c,4,"CREATE ROLE",2023-03-02
17:03:46 KST,3/38,541,AUDIT,00000,"CREATE ROLE
adminuser;",,,,"SESSION",,,,,,,,"asql",,"ROLE","AgensAudit","statement"
```

- Query

```
postgres=# ALTER ROLE adminuser WITH LOGIN, SUPERUSER, PASSWORD 'password';
ERROR:  syntax error at or near ","
LINE 1: ALTER ROLE adminuser WITH LOGIN, SUPERUSER, PASSWORD 'passwo...
```

- Audit Log

```
2023-03-02 17:03:46.625
KST,"agens","postgres",10268,"210.104.181.77:35841",64005862.281c,5,"idle",2023-03-02 17:03:46
KST,3/39,0,ERROR,42601,"syntax error at or near "","""",,,,,,,,,"ALTER ROLE adminuser WITH LOGIN,
SUPERUSER, PASSWORD 'password';",32,,"asql",,,"AgensAudit","error"
```

- Query

```
postgres=# ALTER ROLE adminuser WITH LOGIN SUPERUSER PASSWORD 'password';
```

ALTER ROLE

- Audit Log

2023-03-02 17:03:46.625
KST,"agens","postgres",10268,"210.104.181.77:35841",64005862.281c,6,"ALTER ROLE",2023-03-02 17:03:46 KST,3/40,542,AUDIT,00000,"ALTER ROLE adminuser WITH LOGIN SUPERUSER PASSWORD <REDACTED>",,,,"SESSION",,,,,,,,"asql",,"ROLE","AgensAudit","statement"

- Query

postgres=# CREATE DATABASE auditdb;
CREATE DATABASE

- Audit Log

2023-03-02 17:03:46.625
KST,"agens","postgres",10268,"210.104.181.77:35841",64005862.281c,7,"CREATE DATABASE",2023-03-02 17:03:46 KST,3/41,543,AUDIT,00000,"CREATE DATABASE auditdb;",,,,"SESSION",,,,,,,,"asql",,"DDL","AgensAudit","statement"

- Query

postgres=# ALTER DATABASE auditdb OWNER TO adminuser;
ALTER DATABASE

- Audit Log

2023-03-02 17:03:46.625
KST,"agens","postgres",10268,"210.104.181.77:35841",64005862.281c,8,"ALTER DATABASE",2023-03-02 17:03:46 KST,3/42,544,AUDIT,00000,"ALTER DATABASE auditdb OWNER TO adminuser;",,,,"SESSION",,,,,,,,"asql",,"DDL","AgensAudit","statement"

- Query

postgres=# \c auditdb adminuser
Password for user adminuser:
You are now connected to database "auditdb" as user "adminuser".

- Audit Log

2023-03-02 17:17:18.093
KST,"adminuser","auditdb",10403,"210.104.181.77:35843",64005b8e.28a3,1,"authentication",2023-03-02 17:17:18 KST,4/56,0,AUDIT,00000,"connection authorized: user=adminuser database=auditdb application_name=asql",,,,,,,,,,,"",,,"AgensAudit","connect"
2023-03-02 17:03:46.625
KST,"agens","postgres",10268,"210.104.181.77:35841",64005862.281c,9,"idle",2023-03-02 17:03:46 KST,,0,AUDIT,00000,"disconnection: session time: 0:13:31.472 user=agens database=postgres host=210.104.181.77 port=35841",,,,,,,,,,,"asql",,,"AgensAudit","disconnect"

- Query

auditdb=# CREATE SCHEMA agdb;
CREATE SCHEMA

- Audit Log

2023-03-02 17:17:18.093
KST,"adminuser","auditdb",10403,"210.104.181.77:35843",64005b8e.28a3,2,"CREATE SCHEMA",2023-03-02 17:17:18 KST,4/57,545,AUDIT,00000,"CREATE SCHEMA

agdb;",,,,"SESSION",,,,,,,,"asql",,"DDL","AgensAudit","statement"

- Query

```
auditdb=# SET search_path TO agdb;
SET
```

- Audit Log

```
2023-03-02 17:17:18.093
KST,"adminuser","auditdb",10403,"210.104.181.77:35843",64005b8e.28a3,3,"SET",2023-03-02
17:17:18 KST,4/58,0,AUDIT,00000,"SET search_path TO
agdb;",,,,"SESSION",,,,,,,,"asql",,"MISC","AgensAudit","statement"
```

- Query

```
auditdb=# CREATE TABLE department (
 deptno         INTEGER NOT NULL CONSTRAINT dept_pk PRIMARY KEY,
 dname          VARCHAR(14) CONSTRAINT dept_dname_uq UNIQUE,
 loc           VARCHAR(13)
);
CREATE TABLE
```

- Audit Log

```
2023-03-02 17:17:18.093
KST,"adminuser","auditdb",10403,"210.104.181.77:35843",64005b8e.28a3,4,"CREATE
TABLE",2023-03-02 17:17:18 KST,4/59,546,AUDIT,00000,""""CREATE TABLE department (
 deptno         INTEGER NOT NULL CONSTRAINT dept_pk PRIMARY KEY,
 dname          VARCHAR(14) CONSTRAINT dept_dname_uq UNIQUE,
 loc           VARCHAR(13)
);""",,,,"SESSION",,,,,,,,"asql",,"DDL","AgensAudit","statement"
```

- Query

```
auditdb=# \q
```

- Audit Log

```
2023-03-02 17:17:18.093
KST,"adminuser","auditdb",10403,"210.104.181.77:35843",64005b8e.28a3,5,"idle",2023-03-02
17:17:18 KST,,0,AUDIT,00000,"disconnection: session time: 0:04:33.816 user=adminuser
database=auditdb host=210.104.181.77 port=35843",,,,,,,,,,,"asql",,,"AgensAudit","disconnect"
```