21. auditing in postgresql

Tracking any changes made at the database level is crucial for holding accountable any users with access to PostgreSQL.

During my experience as a database administrator, I encountered two situations where applications reported data loss. Upon investigation, we discovered that a table had been truncated. Unfortunately, we couldn't confirm the source of the issue because auditing was not enabled on the database. This highlights the importance of tracking all activities at the database level.

PostgreSQL supports auditing, and enabling it is relatively straightforward compared to other RDBMS systems.

Installing and configuring pgaudit

1. check if pgaudit is available in your repository

```
sudo apt list | grep -i pgaudit
```

```
dba@postgresql-stg-15:/$ sudo apt list | grep -i pgaudit

WARNING: apt does not have a stable CLI interface. Use with caution in scripts.

postgresql-10-pgaudit-dbgsym/jammy-pgdg 1:1.2.4-1.pgdg22.04+1 amd64
postgresql-10-pgaudit/jammy-pgdg 1:1.2.4-1.pgdg22.04+1 amd64
postgresql-10-pgauditlogtofile-dbgsym/jammy-pgdg 1.5.12-2.pgdg22.04+1 amd64
postgresql-10-pgauditlogtofile/jammy-pgdg 1.5.12-2.pgdg22.04+1 amd64
postgresql-11-pgaudit-dbgsym/jammy-pgdg 1:1.3.4-1.pgdg22.04+1 amd64
postgresql-11-pgaudit/jammy-pgdg 1:1.3.4-1.pgdg22.04+1 amd64
postgresql-11-pgauditlogtofile-dbgsym/jammy-pgdg 1.6.2-1.pgdg22.04+1 amd64
postgresql-11-pgauditlogtofile/jammy-pgdg 1.6.2-1.pgdg22.04+1 amd64
postgresql-12-pgaudit-dbgsym/jammy-pgdg 1.4.3-1.pgdg22.04+1 amd64
postgresql-12-pgaudit/jammy-pgdg 1.4.3-1.pgdg22.04+1 amd64
postgresql-12-pgauditlogtofile-dbgsym/jammy-pgdg 1.6.2-1.pgdg22.04+1 amd64
postgresql-12-pgauditlogtofile/jammy-pgdg 1.6.2-1.pgdg22.04+1 amd64
postgresql-13-pgaudit-dbgsym/jammy-pgdg 1.5.2-1.pgdg22.04+1 amd64
postgresql-13-pgaudit/jammy-pgdg 1.5.2-1.pgdg22.04+1 amd64
postgresql-13-pgauditlogtofile-dbgsym/jammy-pgdg 1.6.2-1.pgdg22.04+1 amd64
postgresql-13-pgauditlogtofile/jammy-pgdg 1.6.2-1.pgdg22.04+1 amd64
postgresql-14-pgaudit-dbgsym/jammy-pgdg 1.6.2-1.pgdg22.04+1 amd64
postgresql-14-pgaudit/jammy-pgdg 1.6.2-1.pgdg22.04+1 amd64
postgresql-14-pgauditlogtofile-dbgsym/jammy-pgdg 1.6.2-1.pgdg22.04+1 amd64
postgresql-14-pgauditlogtofile/jammy-pgdg 1.6.2-1.pgdg22.04+1 amd64
postgresql-15-pgaudit-dbgsym/jammy-pgdg 1.7.0-2.pgdg22.04+1 amd64
postgresql-15-pgaudit/jammy-pgdg 1.7.0-2.pgdg22.04+1 amd64
postgresql-15-pgauditlogtofile-dbgsym/jammy-pgdg 1.6.2-1.pgdg22.04+1 amd64
postgresql-15-pgauditlogtofile/jammy-pgdg 1.6.2-1.pgdg22.04+1 amd64
postgresql-16-pgaudit-dbgsym/jammy-pgdg 16.0-1.pgdg22.04+1 amd64
postgresql-16-pgaudit/jammy-pgdg 16.0-1.pgdg22.04+1 amd64
postgresql-16-pgauditlogtofile-dbgsym/jammy-pgdg 1.6.2-1.pgdg22.04+1 amd64
postgresql-16-pgauditlogtofile/jammy-pgdg 1.6.2-1.pgdg22.04+1 amd64
postgresql-17-pgaudit-dbgsym/jammy-pgdg 17~beta1-1.pgdg22.04+1 amd64
postgresql-17-pgaudit/jammy-pgdg 17~beta1-1.pgdg22.04+1 amd64
postgresql-17-pgauditlogtofile-dbgsym/jammy-pgdg 1.6.2-1.pgdg22.04+1 amd64
postgresql-17-pgauditlogtofile/jammy-pgdg 1.6.2-1.pgdg22.04+1 amd64
postgresql-9.5-pgaudit-dbgsym/jammy-pgdg 1:1.0.8-1.pgdg20.04+1 amd64
postgresql-9.5-pgaudit/jammy-pgdg 1:1.0.8-1.pgdg20.04+1 amd64
postgresql-9.6-pgaudit-dbgsym/jammy-pgdg 1:1.1.4-1.pgdg22.04+1 amd64
```

```
15  main    5432 online postgres /var/lib/postgresql/15/main /var/log/postgresql/
dba@postgresql-stg-15:/$ sudo apt list  --installed | grep -i pgaudit

WARNING: apt does not have a stable CLI interface. Use with caution in scripts.

dba@postgresql-stg-15:/
```

Since `pgaudit` is not installed on our server, we will proceed with the installation. As we are using PostgreSQL 15, I will install the appropriate version of `pgaudit` for PostgreSQL 15. `postgresql-15-pgaudit`

```
sudo apt install postgresql-15-pgaudit
```

2. Update shared library to include pgaudit
   open `postgresql.conf` located in `etc/postgresql/15/main`

```
sudo nano /etc/postgresql/15/main/postgresql.conf
```

update the parameter `shared_preload_libraries` to include `pgaudit`

```
# - Shared Library Preloading -

#local_preload_libraries = ''
#session_preload_libraries = ''
shared_preload_libraries = 'pgaudit'    # (change requires restart)
#jit_provider = 'llvmjit'               # JIT library to use

# - Other Defaults -

#dynamic_library_path = '$libdir'
#extension_destdir = ''                 # prepend path when loading extensions
                                        # and shared objects (added by Debian)
#gin_fuzzy_search_limit = 0
```

3. Restart postgresql to get changes applied

```
sudo systemctl restart postgresql@15-main.service
```

4. login to `psql` and Create the pgaudit extension

```
sudo -u postgres psql
```

```
create extension pgaudit;

\dx
```

```
postgres=# create extension pgaudit;
CREATE EXTENSION
postgres=# \dx+
    Objects in extension "pgaudit"
          Object description
--------------------------------------
 event trigger pgaudit_ddl_command_end
 event trigger pgaudit_sql_drop
 function pgaudit_ddl_command_end()
 function pgaudit_sql_drop()
(4 rows)

     Objects in extension "plpgsql"
           Object description
------------------------------------------
 function plpgsql_call_handler()
 function plpgsql_inline_handler(internal)
 function plpgsql_validator(oid)
 language plpgsql
(4 rows)

postgres=# \dx
                  List of installed extensions
  Name   | Version |   Schema   |                Description
---------+---------+------------+---------------------------------
 pgaudit | 1.7     | public     | provides auditing functionality
 plpgsql | 1.0     | pg_catalog | PL/pgSQL procedural language
(2 rows)

postgres=#
```

5. Verify the pgaudit parameters.

```
show pgaudit.log
```

```
postgres=# show pgaudit.log;
 pgaudit.log
-------------
 none
(1 row)

postgres=# ;
```

the output command show that pgaudit.log `none` meaning pgaudit is not tracking anything

6. configure pgaudit to track activity as follow

- `READ` : SELECT and COPY when the source is a relation or a query.
- `WRITE` : INSERT, UPDATE, DELETE, TRUNCATE, and COPY when the destination is a relation.
- `FUNCTION` : Function calls and DO blocks.
- `ROLE` : Statements related to roles and privileges: GRANT, REVOKE, CREATE/ALTER/DROP ROLE.
- `DDL` : All DDL that is not included in the ROLE class.
- `MISC` : Miscellaneous commands, e.g., DISCARD, FETCH, CHECKPOINT, VACUUM, SET.
- `MISC_SET` : Miscellaneous SET commands, e.g., SET ROLE.
- `ALL` : Include all of the above.
  for our case we will enable `read` , `write` , `DDL`

```
alter system set pgaudit.log to read,write,DDL;
```

```
postgres=# alter system set pgaudit.log to read,write,DDL;
ALTER SYSTEM
postgres=#
```

7. Restart postgresql services

```
sudo systemctl restart postgresql@15-main.service
```

8. verify that configuration applied on pgaudti

```
show pgaudit.log;
```

```
dba@postgresql-stg-15:~$ sudo -u postgres psql
could not change directory to "/home/dba": Permission denied
psql (15.7 (Ubuntu 15.7-1.pgdg22.04+1))
Type "help" for help.

postgres=# show pgaudit.log;
   pgaudit.log
-----------------
 read, write, ddl
(1 row)

postgres=# k
```

9. Test auditing by performing DDL commands or select command

```
postgres=# \c production;
You are now connected to database "production" as user "postgres".
production=# \dt
              List of relations
 Schema |       Name       | Type  |  Owner
--------+------------------+-------+----------
 public | pgbench_accounts | table | postgres
 public | pgbench_branches | table | postgres
 public | pgbench_history  | table | postgres
 public | pgbench_tellers  | table | postgres
(4 rows)

production=# truncate table pgbench_accounts ;
TRUNCATE TABLE
production=#
```

check log in postgresql located in `cat /var/log/postgresql/postgresql-15-main.log`

```
2024-09-24 09:40:10.750 UTC [50479] LOG:  database system is ready to accept connections
2024-09-24 09:42:13.135 UTC [50500] postgres@postgres LOG:  AUDIT: SESSION,1,1,READ,SELECT,,,"SELECT d.datname as ""Name"",
             pg_catalog.pg_get_userbyid(d.datdba) as ""Owner"",
             pg_catalog.pg_encoding_to_char(d.encoding) as ""Encoding"",
             d.datcollate as ""Collate"",
             d.datctype as ""Ctype"",
             d.daticulocale as ""ICU Locale"",
             CASE d.datlocprovider WHEN 'c' THEN 'libc' WHEN 'i' THEN 'icu' END AS ""Locale Provider"",
             pg_catalog.array_to_string(d.datacl, E'\n') AS ""Access privileges""
       FROM pg_catalog.pg_database d
       ORDER BY 1;",<not logged>
2024-09-24 09:42:25.516 UTC [50506] postgres@production LOG:  AUDIT: SESSION,1,1,READ,SELECT,,,"SELECT n.nspname as ""Schema"",
         c.relname as ""Name"",
         CASE c.relkind WHEN 'r' THEN 'table' WHEN 'v' THEN 'view' WHEN 'm' THEN 'materialized view' WHEN 'i' THEN 'index' WHEN 'S' THEN 'sequence' W
HEN 't' THEN 'TOAST table' WHEN 'f' THEN 'foreign table' WHEN 'p' THEN 'partitioned table' WHEN 'I' THEN 'partitioned index' END as ""Type"",
         pg_catalog.pg_get_userbyid(c.relowner) as ""Owner""
       FROM pg_catalog.pg_class c
           LEFT JOIN pg_catalog.pg_namespace n ON n.oid = c.relnamespace
           LEFT JOIN pg_catalog.pg_am am ON am.oid = c.relam
       WHERE c.relkind IN ('r','p','')
             AND n.nspname <> 'pg_catalog'
             AND n.nspname !~ '^pg_toast'
             AND n.nspname <> 'information_schema'
         AND pg_catalog.pg_table_is_visible(c.oid)
       ORDER BY 1,2,",<not logged>
2024-09-24 09:42:37.555 UTC [50506] postgres@production LOG:  AUDIT: SESSION,2,1,WRITE,TRUNCATE TABLE,,,truncate table pgbench_accounts ;,<not logged>
dba@postgresql-stg-15:/var/log/postgresql$
```