

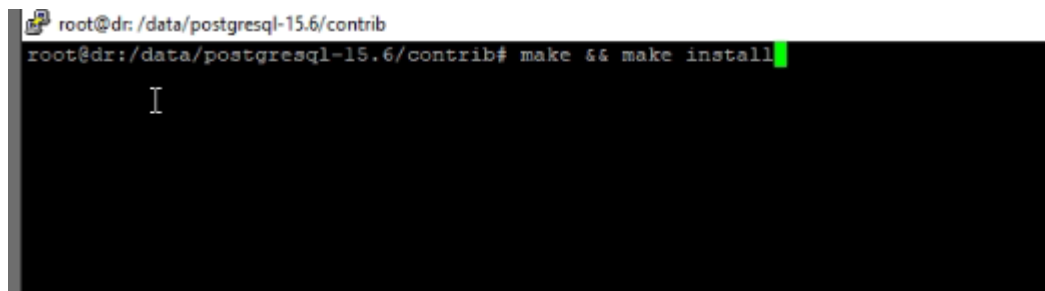
# Pg\_audit installation

## 1. check contrib package and make file are present or not:-

if not then configure bin path with the help of source code.

- wget <https://ftp.postgresql.org/pub/source/v15.6/postgresql-15.6.tar.gz>
- ./configure --prefix=/usr/lib/pgsql-15.6
- make && make install

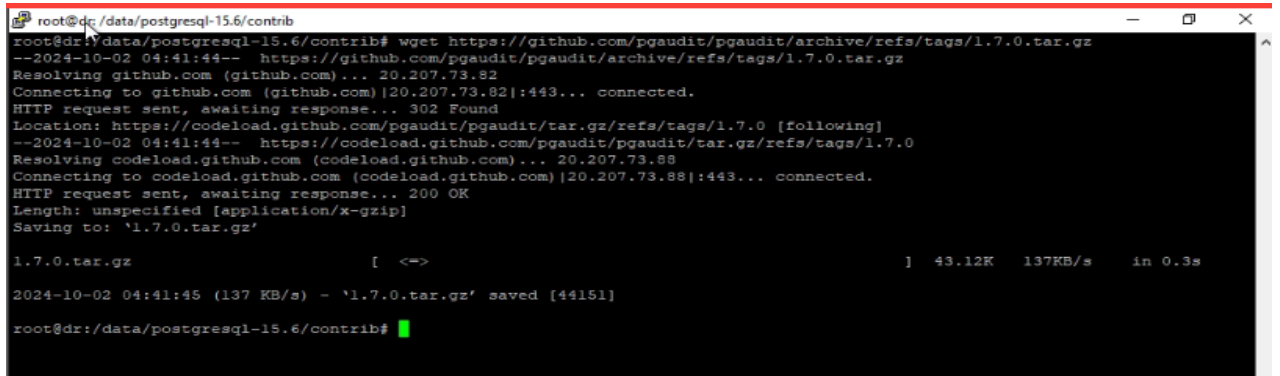
cd contrib



```
root@dr:/data/postgresql-15.6/contrib
root@dr:/data/postgresql-15.6/contrib# make && make install
```

## 2. Download pgaudit in contrib package:-

Github site:- <https://github.com/pgaudit/pgaudit/releases>



```
root@dr:/data/postgresql-15.6/contrib
root@dr:/data/postgresql-15.6/contrib# wget https://github.com/pgaudit/pgaudit/archive/refs/tags/1.7.0.tar.gz
--2024-10-02 04:41:44-- https://github.com/pgaudit/pgaudit/archive/refs/tags/1.7.0.tar.gz
Resolving github.com (github.com)... 20.207.73.82
Connecting to github.com (github.com)|20.207.73.82|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://codeload.github.com/pgaudit/pgaudit/tar.gz/refs/tags/1.7.0 [following]
--2024-10-02 04:41:44-- https://codeload.github.com/pgaudit/pgaudit/tar.gz/refs/tags/1.7.0
Resolving codeload.github.com (codeload.github.com)... 20.207.73.88
Connecting to codeload.github.com (codeload.github.com)|20.207.73.88|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [application/x-gzip]
Saving to: '1.7.0.tar.gz'

1.7.0.tar.gz           [ <=> ] 43.12K  137KB/s  in 0.3s

2024-10-02 04:41:45 (137 KB/s) - '1.7.0.tar.gz' saved [44151]

root@dr:/data/postgresql-15.6/contrib#
```

wget <https://github.com/pgaudit/pgaudit/archive/refs/tags/1.7.0.tar.gz>

- tar -xvf 1.7.0.tar.gz

```

root@dr:/data/postgresql-15.6/contrib#
root@dr:/data/postgresql-15.6/contrib#
root@dr:/data/postgresql-15.6/contrib# tar -xvf 1.7.0.tar.gz
pgaudit-1.7.0/
pgaudit-1.7.0/.editorconfig
pgaudit-1.7.0/.github/
pgaudit-1.7.0/.github/workflows/
pgaudit-1.7.0/.github/workflows/test.yml
pgaudit-1.7.0/.gitignore
pgaudit-1.7.0/LICENSE
pgaudit-1.7.0/Makefile
pgaudit-1.7.0/README.md
pgaudit-1.7.0/expected/
pgaudit-1.7.0/expected/pgaudit.out
pgaudit-1.7.0/pgaudit--1.7.sql
pgaudit-1.7.0/pgaudit.c
pgaudit-1.7.0/pgaudit.conf
pgaudit-1.7.0/pgaudit.control
pgaudit-1.7.0/sql/
pgaudit-1.7.0/sql/pgaudit.sql
pgaudit-1.7.0/test/
pgaudit-1.7.0/test/Dockerfile.debian
pgaudit-1.7.0/test/Dockerfile.rhel
pgaudit-1.7.0/test/README.md
pgaudit-1.7.0/test/test.sh
root@dr:/data/postgresql-15.6/contrib# chown postgres:postgres pgaudit-1.7.0/ -R
root@dr:/data/postgresql-15.6/contrib#

```

- cd pgaudit-1.7.0 & execute make && make install command

```

root@dr:/data/postgresql-15.6/contrib/pgaudit-1.7.0#
root@dr:/data/postgresql-15.6/contrib/pgaudit-1.7.0#
root@dr:/data/postgresql-15.6/contrib/pgaudit-1.7.0# cd pg
pgaudit-1.7.0/      pgcrypto/      pg_prewarm/      pg_stat_statements/  pg_surgery/      pg_visibility/
pg_buffercache/    pg_freespacemap/  pg_growlocks/    pgstattuple/        pg_trgm/         pg_walinspect/
root@dr:/data/postgresql-15.6/contrib/pgaudit-1.7.0# make
make -C ../../src/backend generated-headers
make[1]: Entering directory '/data/postgresql-15.6/src/backend'
make -C catalog distprep generated-header-symlinks
make[2]: Entering directory '/data/postgresql-15.6/src/backend/catalog'
make[2]: Nothing to be done for 'distprep'.
make[2]: Nothing to be done for 'generated-header-symlinks'.
make[2]: Leaving directory '/data/postgresql-15.6/src/backend/catalog'
make -C utils distprep generated-header-symlinks
make[2]: Entering directory '/data/postgresql-15.6/src/backend/utils'
make[2]: Nothing to be done for 'distprep'.
make[2]: Nothing to be done for 'generated-header-symlinks'.
make[2]: Leaving directory '/data/postgresql-15.6/src/backend/utils'
make[1]: Leaving directory '/data/postgresql-15.6/src/backend'
gcc -Wall -Wmissing-prototypes -Wpointer-arith -Wdeclaration-after-statement -Werror=vla -Wendif-labels -Wmissing-format-attribute -Wimplicit-fallthrough=3 -Wcast-function-type -Wformat-security -fno-strict-aliasing -fwrapv -fexcess-precision=standard -Wno-format-truncation -Wno-stringop-truncation -O2 -fPIC -I. -I. -I../src/include -D_GNU_SOURCE -I/usr/include/libxml2 -c -o pgaudit.o pgaudit.c
gcc -Wall -Wmissing-prototypes -Wpointer-arith -Wdeclaration-after-statement -Werror=vla -Wendif-labels -Wmissing-format-attribute -Wimplicit-fallthrough=3 -Wcast-function-type -Wformat-security -fno-strict-aliasing -fwrapv -fexcess-precision=standard -Wno-format-truncation -Wno-stringop-truncation -O2 -fPIC -shared -o pgaudit.so pgaudit.o -L../src/port -L../src/common -Wl,--as-needed -Wl,-rpath,'/usr/lib/pgsql-15.6/lib',--enable-new-dtags
root@dr:/data/postgresql-15.6/contrib/pgaudit-1.7.0#

```

- If you got error then you have to change permission of file to postgres. Then switch to postgres user &
- Execute make && make install command

### 3. Make changes in postgresql.conf:-

```

pgaudit.log = 'READ,WRITE'
pgaudit.log_level = 'log'
pgaudit.log_parameter = on

shared_preload_libraries = 'pgaudit'

```

### 4. Restart postgresql.service

## 5. Create extension:-

Create extension pgaudit;

```
=====
```

## pgaudit parameter:-

- **pgaudit.log:-**

Specifies which classes of statements will be logged by session audit logging. Possible values are:

1. **READ:** SELECT and COPY when the source is a relation or a query.
2. **WRITE:** INSERT, UPDATE, DELETE, TRUNCATE, and COPY when the destination is a relation.
3. **FUNCTION:** Function calls and DO blocks.
4. **ROLE:** Statements related to roles and privileges: GRANT, REVOKE, CREATE/ALTER/DROP ROLE.
5. **DDL:** All DDL that is not included in the ROLE class.
6. **MISC:** Miscellaneous commands, e.g. DISCARD, FETCH, CHECKPOINT, VACUUM, SET.
7. **MISC\_SET:** Miscellaneous SET commands, e.g. SET ROLE.
8. **ALL:** Include all of the above.

```
=====
```

## pgaudit.log\_level

- Specifies the log level that will be used for log entries (see Message Severity Levels for valid levels) but note that ERROR, FATAL, and PANIC are not allowed). This setting is used for regression testing and may also be useful to end users for testing or other purposes.
- Note that pgaudit.log\_level is only enabled when pgaudit.log\_client is on; otherwise the default will be used.
- The default is log.

```
=====
```

## pgaudit.log\_parameter

- Specifies that audit logging should include the parameters that were passed with the statement. When parameters are present they will be included in CSV format after the statement text.

- The default is off.