PostgreSQL 17 Hardening Guide

This documentprovidesa comprehensivePostgreSQL 17 hardening guidebased ontheCISBenchmark. It includes installation, configuration, security, logging, auditing, user access, and connection settings. All PostgreSQL commands and their outputs are retained for reference.

TableOfContents

1. >>Installation and Patches

1.1.1 >> Ensure packages are obtained from authorized repositories

[root@pgdbsrv~]#dnf install -y https://download.postgresql.org/pub/repos/yum/reporpms/EL-9-x86_64/pgdg-redhat-repo-latest.noarch.rpm

1.1.2>>Disable the built-in PostgreSQL module

[root@pgdbsrv~]# sudo dnf -qy module disable postgresql

1.1.3 >>PostgreSQL 17 Server and Client

[root@pgdbsrv~]# dnf install -y postgresql17-{server,contrib}

or

```
[root@pgdbsrv~]# sudo dnf install -y postgresql17-server
```

1.1.4 >> Since I have already installed PostgreSQL from the authorized repository RPM.

```
[root@pgdbsrv~]# dnf repolist all | grep -E'enabled$'
```

```
appstream           Rocky Linux 9 - AppStream                  enabled
baseos              Rocky Linux 9 - BaseOS                     enabled
crb                 Rocky Linux 9 - CRB                        enabled
droplet-agent       DigitalOcean DropletAgent                  enabled
epel               Extra Packages for EnterpriseLinux9      enabled
epel-cisco-openh264 Extra Packages for EnterpriseLinux9      enabled
extras              Rocky Linux 9 - Extras                   enabled
pgdg-common         PostgreSQL commonRPMsforRHEL/Rock        enabled
pgdg17              PostgreSQL 17 for RHEL/Rocky/AlmaL       enabled
```

```
[root@pgdbsrv~]# rpm -qa | grep postgres
```

1.1.5 >>PostgreSQL packages are installed

```
postgresql17-libs-17.5-3PGDG.rhel9.x86_64

postgresql17-17.5-3PGDG.rhel9.x86_64

postgresql17-server-17.5-3PGDG.rhel9.x86_64

postgresql17-contrib-17.5-3PGDG.rhel9.x86_64
```

1.1.6 >> To verify which repository a package or repo data came from

```
[root@pgdbsrv~]# dnf info $(rpm -qa|grep postgres) | grep -E '^Name|^Version|^From'
```

```
Name      : postgresql17

Version    : 17.5

From repo : pgdg17

Name      : postgresql17-libs

Version    : 17.5

From repo : pgdg17

Name      : postgresql17-server

Version    : 17.5

From repo : pgdg17
```

1.2 >>(Install only required packages)

```
[root@pgdbsrv~]# rpm -q $(dnf search postgresql | cut -d: -f1 | cut -d. -f1) 2>&1 | grep -Ev 'package.*is not installed'
```

```
postgresql17-17.5-3PGDG.rhel9.x86_64

postgresql17-contrib-17.5-3PGDG.rhel9.x86_64

postgresql17-libs-17.5-3PGDG.rhel9.x86_64

postgresql17-server-17.5-3PGDG.rhel9.x86_64

pg_top-4.1.2-42PGDG.rhel9.x86_64

pgaudit_17-17.1-1PGDG.rhel9.x86_64

pgdg-redhat-repo-42.0-54PGDG.noarch

set_user_17-4.1.0-1PGDG.rhel9.x86_64
```

1.3 >> Ensure systemd Service Files Are Enable

```
[root@pgdbsrv~]# systemctl status postgresql-17.service
```

```
● postgresql-17.service - PostgreSQL 17 database server
```

```
Loaded: loaded (/usr/lib/systemd/system/postgresql-17.service; enabled; preset: disabled) Drop-In:
/etc/systemd/system/postgresql-17.service.d └─security.conf, umask.conf Active: active (running) since Sat
2025-08-09 04:34:16 UTC; 24min ago Docs: https://www.postgresql.org/docs/17/static/ Process: 439067
ExecStartPre=/usr/pgsql-17/bin/postgresql-17-check-db-dir ${PGDATA} (code=exited,
status=0/SUCCESS)
Main PID: 439072 (postgres)

Tasks: 10 (limit: 22924)

Memory: 36.4M

CPU: 1.771s

CGroup: /system.slice/postgresql-17.service

├─439072 /usr/pgsql-17/bin/postgres -D /var/lib/pgsql/17/data/

├─439073 "postgres: logger "

├─439074 "postgres: checkpointer "

├─439075 "postgres: background writer "

├─439077 "postgres: walwriter " ├─439078 "postgres: autovacuum launcher " ├─439079 "postgres: logical
replication launcher " ├─439109 "postgres: postgres postgres 27.34.64.183(27100) idle" ├─439116
"postgres: postgres testdb 27.34.64.183(19050) idle" └─439129 "postgres: postgres testdb
27.34.64.183(42175) idle"
```

```
Aug 09 04:34:16 rockylinux-database systemd[1]: Starting PostgreSQL 17 database server...

Aug 09 04:34:16 rockylinux-database postgres[439072]: 2025-08-09 04:34:16.497 UTC [439072] LOG:
redirecting log output to logging collector process
```

```
Aug 09 04:34:16 rockylinux-database postgres[439072]: 2025-08-09 04:34:16.497 UTC [439072] HINT: Future log output will appear in directory "log".

Aug 09 04:34:16 rockylinux-database systemd[1]: Started PostgreSQL 17 database server.
```

```
[root@pgdbsrv~]# systemctl status postgresql-17 | grep Active
```

```
Active: active (running) since Sat 2025-08-09 04:34:16 UTC; 33min ago
```

Ensure Data Cluster Initialized Successfully (Automated)

1.4 >> Ensure Data Cluster Initialized Successfully

```
[root@pgdbsrvbin]# PGSETUP_INITDB_OPTIONS="-k" /usr/pgsql-17/bin/postgresql-17-setup initdb
Initializing database ... OK
```

1.5 >> Ensure the Latest Security Patches are Applied

```
[postgres@rockylinux-database ~]$ psql -c 'SHOW server_version'

server_version

----------------

17.5

(1 row)
```

```
[root@pgdbsrv~]# dnf update $(rpm -qa | grep '^postgresql')
```

```
Last metadata expiration check: 0:04:07 ago on Sat 09 Aug 2025 05:48:29 AM UTC.

Dependencies resolved.

Nothing to do.

Complete!
```

1.6 >> Verify That PGPASSWORD is Not Set in Users Profiles (Control >> 3.11 Encrypt Sensitive Data at Rest)

```
[root@pgdbsrv~]# grep PGPASSWORD --no-messages /home/*/.{bashrc,profile,bash_profile}

[root@pgdbsrv~]# grep PGPASSWORD --no-messages /root/.{bashrc,profile,bash_profile}

[root@pgdbsrv~]# grep PGPASSWORD --no-messages /etc/environment
```

1.7 Verify That the 'PGPASSWORD' Environment Variable is Not in Use

```
[root@pgdbsrv~]# grep PGPASSWORD /proc/*/environ */
```

2 >> Directory and File Permissions

2.1 >> Ensure the file permissions mask is correct (Manual) (Control >> 3.3 Configure Data Access Control Lists)

```
[root@pgdbsrv~]# whoami

root

[root@pgdbsrv~]# su - postgres
```

```
Last login: Sat Aug 9 05:41:12 UTC 2025 on pts/0

[postgres@rockylinux-database ~]$ whoami postgres
[postgres@rockylinux-database ~]$ umask 0022
[postgres@rockylinux-database ~]$
[postgres@rockylinux-database ~]$ ls -ld .{bash_profile,profile,bashrc}
ls: cannot access '.profile': No such file or directory
ls: cannot access '.bashrc': No such file or directory
-rwx------. 1 postgres postgres 266 Aug 3 11:05 .bash_profile
```

```
[postgres@rockylinux-database ~]$ echo "umask 077" >> .bash_profile
[postgres@rockylinux-database ~]$ source .bash_profile
[postgres@rockylinux-database ~]$ umask
0077
```

2.2 >> Ensure extension directory has appropriate ownership and permissions

```
[root@pgdbsrv~]# /usr/pgsql-17/bin/pg_config --sharedir
/usr/pgsql-17/share

[root@pgdbsrv~]# ls -ld $(/usr/pgsql-17/bin/pg_config --sharedir)/extension
drwxr-xr-x. 2 root root 53 Aug 3 11:05 /usr/pgsql-17/share/extension
```

Any differences in permissions (drwxr-xr-x. Change the ownership and poermission chown,chmod)

```
# chown -c root:root $(/usr/pgsql-17/bin/pg_config --sharedir)/extension

# chmod -c 0755 $(/usr/pgsql-17/bin/pg_config --sharedir)/extensio
```

2.3 >> Disable PostgreSQL Command History (Control >>3.5 Securely Dispose of Data)

```
[root@pgdbsrv~]# find /home -name ".psql_history" -exec ls -la {} \;

[root@pgdbsrv~]# find /root -name ".psql_history" -exec ls -la {} \;

-rw-------. 1 root root 0 Jul 29 04:07 /root/.psql_history
```

```
[root@pgdbsrv~]# rm -f ~postgres/.psql_history || true

[root@pgdbsrv~]# rm -f ~root/.psql_history || true
```

```
[root@pgdbsrv~]# sudo -u postgres sh -c 'echo "\set HISTFILE /dev/null" >> ~/.psqlrc'

# cat << EOF >> postgres/.psqlrc

\set HISTFILE /dev/null

EOF
```

```
[postgres@rockylinux-database ~]$ ln -s /dev/null ~postgres/.psql_history

[root@pgdbsrv~]# echo 'PSQL_HISTORY=/dev/null' >> /etc/environment
```

2.4 >> Ensure Passwords are Not Stored in the service file (Manual)

```
[root@pgdbsrv~]# find / -name .pg_service.conf -type f -print | xargs -I{} grep -H password {}
```

```
[root@pgdbsrv~]# grep password /root/.pg_service.conf

grep: /root/.pg_service.conf: No such file or directory

[root@pgdbsrv~]# test -z "${PGSERVICEFILE}" || grep password "${PGSERVICEFILE}"

[root@pgdbsrv~]# test -z "${PGSYSCONFDIR}" || grep password "${PGSYSCONFDIR}/pg_service.conf"
[root@pgdbsrv~]#
```

3 >> Logging And Auditing

3.1 >> Ensure the log destinations are set correctly

```
[postgres@rockylinux-database ~]$ psql

psql (17.5)

Type "help" for help.


postgres=# show log_destination;

log_destination

-----------------

stderr

(1 row)


postgres=# alter system set log_destination = 'csvlog';

ALTER SYSTEM

postgres=# show log_destination;

log_destination
```

```
-----------------
stderr
(1 row)
```

```
postgres=# show log_destination;
log_destination
-----------------
csvlog
(1 row)
```

3.2 >> Ensure the logging collector is enabled

```
postgres=# show logging_collector;
logging_collector
-------------------
on
(1 row)
postgres=# alter system set logging_collector = 'on';
ALTER SYSTEM
```

```
[root@pgdbsrv~]# systemctl restart postgresql-17
[root@pgdbsrv~]# systemctl status postgresql-17|grep 'ago$'
Active: active (running) since Sat 2025-08-09 08:34:30 UTC; 10s ago
```

3.3 >> Ensure the log file destination directory is set correctly ("/var/log/postgres" this should be set to an appropriate path as defined by your organization's logging requirements.)

```
postgres=# show log_directory;

log_directory

---------------

log

(1 row)
```

Note:it's not working (If log_destination is set to syslog, log_directory is ignored — because syslog handles the location, not PostgreSQL.)

3.4>>Ensurethefilenamepatternforlogfiles is set correctly

Ensure filename pattern for log files is set correctly

```
psql (17.5)

Type "help" for help.


postgres=# show log_filename;

log_filename

-------------------

postgresql-%a.log


postgres=# alter system set log_filename='postgresql-%Y-%m-%d_%H%M%S.log';
```

3.5 >> Ensure the log file permissions are set correctly

```
postgres=# show log_file_mode;

log_file_mode

---------------
```

```
0600

(1 row)
```

3.6 >> Ensure 'log_truncate_on_rotation' is enabled

```
postgres=# show log_truncate_on_rotation;

log_truncate_on_rotation

--------------------------

on

(1 row)
```

3.7 >> Ensure the maximum log file lifetime is set correctly

```
postgres=# show log_rotation_age;

log_rotation_age

------------------

1d

(1 row)
```

3.8 >> Ensure the maximum log file size is set correctly

```
postgres=# show log_rotation_size;

log_rotation_size

-------------------

0

(1 row)
```

```
postgres=# alter system set log_rotation_size = '100MB';

ALTER SYSTEM


postgres=# select pg_reload_conf();

pg_reload_conf

----------------

t

(1 row)


postgres=# show log_rotation_size;

log_rotation_size

-------------------

100MB

(1 row)
```

3.9 >> Ensure the correct syslog facility is selected

```
postgres=# show syslog_facility;

syslog_facility

-----------------

local0

(1 row)


postgres=# alter system set syslog_facility = 'LOCAL1';

ALTER SYSTEM

postgres=# select pg_reload_conf();
```

```
pg_reload_conf
----------------
t
(1 row)
```

3.10 >> Ensure syslog messages are not suppressed

```
postgres=# show syslog_sequence_numbers;
syslog_sequence_numbers
-------------------------
on
(1 row)
```

```
postgres=# alter system set syslog_sequence_numbers = 'on';
ALTER SYSTEM
postgres=# select pg_reload_conf();
pg_reload_conf
----------------
t
(1 row)
```

3.11 >> Ensure syslog messages are not lost due to size

```
postgres=# show syslog_split_messages;
syslog_split_messages
-----------------------
on
```

```
(1 row)

postgres=# alter system set syslog_split_messages = 'on';
ALTER SYSTEM
postgres=# select pg_reload_conf();
pg_reload_conf
----------------
t
(1 row)
```

3.12 >> Ensure the program name for PostgreSQL syslog messages are correct

```
postgres=# show syslog_ident;
syslog_ident
--------------
postgres
(1 row)

postgres=# alter system set syslog_ident = 'pglivedb';
ALTER SYSTEM
postgres=# select pg_reload_conf();
pg_reload_conf
----------------
t
(1 row)
```

```
postgres=# show syslog_ident;

syslog_ident

--------------

pglivedb

(1 row)
```

3.13 >> Ensure the correct messages are written to the server log

```
postgres=# show log_min_messages;

log_min_messages

------------------

warning

(1 row)


postgres=# alter system set log_min_messages = 'warning';

ALTER SYSTEM

postgres=# select pg_reload_conf();

pg_reload_conf

----------------

t

(1 row)


postgres=# show log_min_messages;

log_min_messages

------------------

warning
```

```
(1 row)
```

3.14 >> Ensure the correct SQL statements generating errors are recorded

```
postgres=# show log_min_error_statement;

log_min_error_statement

-------------------------

error

(1 row)



postgres=# alter system set log_min_error_statement = 'error';

ALTER SYSTEM

postgres=# select pg_reload_conf();

pg_reload_conf

----------------

t

(1 row)



postgres=# show log_min_error_statement;

log_min_error_statement

-------------------------

error

(1 row)
```

3.15 >> Ensure 'debug_print_parse' is disabled

```
postgres=# show debug_print_parse;

debug_print_parse
```

```
-------------------
off
(1 row)

postgres=# alter system set debug_print_parse='off';
ALTER SYSTEM
postgres=# select pg_reload_conf();
pg_reload_conf
----------------
t
(1 row)
```

3.16 >> Ensure 'debug_print_rewritten' is disabled

```
postgres=# show debug_print_rewritten;
debug_print_rewritten
-----------------------
off
(1 row)

postgres=# alter system set debug_print_rewritten = 'off';
ALTER SYSTEM
postgres=# select pg_reload_conf();
pg_reload_conf
----------------
t
```

```
(1 row)
```

3.17 >> Ensure 'debug_print_plan' is disabled

```
postgres=# show debug_print_plan;

debug_print_plan

------------------

off

(1 row)


postgres=# alter system set debug_print_plan = 'off';

ALTER SYSTEM

postgres=# select pg_reload_conf();

pg_reload_conf

----------------

t

(1 row)
```

3.18 >> Ensure 'debug_pretty_print' is enabled

```
postgres=# show debug_pretty_print;

debug_pretty_print

--------------------

on

(1 row)


postgres=# alter system set debug_pretty_print = 'on';

ALTER SYSTEM
```

```
postgres=# select pg_reload_conf();

pg_reload_conf

----------------

t

(1 row)
```

3.19 >> Ensure 'log_connections' is enabled

```
postgres=# show log_connections;

log_connections

-----------------

off

(1 row)


postgres=# alter system set log_connections = 'on';

ALTER SYSTEM

postgres=# select pg_reload_conf();

pg_reload_conf

----------------

t

(1 row)


postgres=# show log_connections;

log_connections

----------------

on

(1 row)
```

3.20 >> Ensure 'log_disconnections' is enabled

```
postgres=# show log_disconnections;

log_disconnections

--------------------

on

(1 row)


postgres=# alter system set log_disconnections = 'on';

ALTER SYSTEM

postgres=# select pg_reload_conf();

pg_reload_conf

----------------

t

(1 row)
```

3.21 >> Ensure 'log_error_verbosity' is set correctly

```
postgres=# show log_error_verbosity;

log_error_verbosity

---------------------

default

(1 row)


postgres=# alter system set log_error_verbosity = 'verbose';

ALTER SYSTEM
```

```
postgres=# select pg_reload_conf();

pg_reload_conf

----------------

t

(1 row)


postgres=# show log_error_verbosity;

log_error_verbosity

---------------------

verbose

(1 row)
```

3.22 >> Ensure 'log_hostname' is set correctly

```
postgres=# show log_hostname;

log_hostname

--------------

off

(1 row)


postgres=# alter system set log_hostname='off';

ALTER SYSTEM

postgres=# select pg_reload_conf();

pg_reload_conf

----------------

t

(1 row)
```

```
postgres=# show log_hostname;

log_hostname

--------------

off

(1 row
```

```
postgres=# show log_hostname;

log_hostname

--------------

off

(1 row)
```

3.23 >> Ensure 'log_line_prefix' is set correctly

```
postgres=# show log_line_prefix;

log_line_prefix

-----------------

%m [%p]

(1 row)
```

```
postgres=# alter system set log_line_prefix = '%m [%p]: [%l-1] db=%d,user=%u,app=%a,client=%h';

ALTER SYSTEM

postgres=# select pg_reload_conf();

pg_reload_conf

----------------

t
```

```
(1 row)

postgres=# show log_line_prefix;
log_line_prefix
------------------------------------------------
%m [%p]: [%l-1] db=%d,user=%u,app=%a,client=%h
(1 row)
```

3.24 >> Ensure 'log_statement' is set correctly

```
postgres=# show log_statement;
log_statement
---------------
none
(1 row)

postgres=# alter system set log_statement='ddl';
ALTER SYSTEM
postgres=# select pg_reload_conf();
pg_reload_conf
----------------
t
(1 row)

postgres=# show log_statement;
log_statement
```

```
---------------

ddl

(1 row)
```

3.25 >> Ensure 'log_timezone' is set correctly

```
postgres=# show log_timezone;

log_timezone

--------------

UTC

(1 row)


postgres=# alter system set log_timezone = ' Asia/Kathmandu';

ALTER SYSTEM

postgres=# select pg_reload_conf();

pg_reload_conf

----------------

t

(1 row)


postgres=# show log_timezone;

log_timezone

--------------

Asia/Kathmandu

(1 row)
```

3.26 >> Ensure the PostgreSQL Audit Extension (pgAudit) is enabled

```
postgres=# show shared_preload_libraries;

shared_preload_libraries

--------------------------



(1 row)
```

```
postgres=# show pgaudit.log;

ERROR: unrecognized configuration parameter "pgaudit.log"
```

```
[root@pgdbsrvdata]# dnf -y install pgaudit_17

Last metadata expiration check: 0:02:59 ago on Sat 09 Aug 2025 04:48:18 PM +0545.

Dependencies resolved.

= === == === === == === === == === === == === === == === === == === === == === === == === === == === === == =
====================================================================

Package                Architecture           Version                       Repository          Size

= === == === === == === === == === === == === === == === === == === === == === === == === === == === === == =
====================================================================
Installing:

pgaudit_17
                         x86_64               17.1-1PGDG.rhel9                   pgdg17              28 k


Transaction Summary

= === == === === == === === == === === == === === == === === == === === == === === == === === == === === == =
====================================================================
Install 1 Package



Total download size: 28 k
```

```
Installed size: 55 k

Downloading Packages:

pgaudit_17-17.1-1PGDG.rhel9.x86_64.rpm                                  136 kB/s | 28 kB
00:00
------ ----- ----- ---- ----- ----- ---- ----- ----- ---- ----- ---- ----- ----- ------ ----- ----- ---- ----- ----- ---- ----- ----- ---- ----- ---- - ---- ----
-------------------
Total
                                                         134 kB/s | 28 kB     00:00
Running transaction check

Transaction check succeeded.

Running transaction test

Transaction test succeeded.

Running transaction


Preparing       :                                                          1/1

Installing      : pgaudit_17-17.1-1PGDG.rhel9.x86_64                                  1/1

Running scriptlet: pgaudit_17-17.1-1PGDG.rhel9.x86_64                                  1/1

Verifying       : pgaudit_17-17.1-1PGDG.rhel9.x86_64                                  1/1


Installed:

pgaudit_17-17.1-1PGDG.rhel9.x86_64


Complete!
```

```
[root@rockylinux-database]#vi /var/lib/pgsql/17/data/postgresql.conf
```

add a new pgaudit-specific entry at the end of the file:

```
shared_preload_libraries = 'pgaudit'
```

```
[root@pgdbsrvdata]# systemctl restart postgresql-17
```

```
[root@pgdbsrvdata]# systemctl status postgresql-17|grep 'ago$'

Active: active (running) since Sat 2025-08-09 16:54:50 +0545; 7s ago
```

```
postgres=# show pgaudit.log;

pgaudit.log

-------------

none

(1 row)
```

```
postgres=# ALTER SYSTEM SET pgaudit.log = 'ddl,function,role,read,write';

ALTER SYSTEM

postgres=# ALTER SYSTEM SET pgaudit.log_catalog = 'off';

ALTER SYSTEM

postgres=# ALTER SYSTEM SET pgaudit.log_parameter = 'on';

ALTER SYSTEM

postgres=# ALTER SYSTEM SET pgaudit.log_statement_once = 'off';

ALTER SYSTEM

postgres=# ALTER SYSTEM SET pgaudit.log_level = 'log';

ALTER SYSTEM

postgres=# SELECT pg_reload_conf();

pg_reload_conf

----------------

t

(1 row)
```

```
postgres=# show pgaudit.log;

pgaudit.log

------------------------------

ddl,function,role,read,write

(1 row)
```

4. >> USER ACCESS AND AUTHORIZATION

4.1 >> Ensure interactive login is disabled for postgres user

```
[root@pgdbsrv~]# grep postgres /etc/shadow | cut -d: -f1-2

postgres:!!
```

4.1.1 >> Create dba group if needed

```
[root@pgdbsrv~]# groupadd dba
```

4.1.2 >> Create User and set the password testuser1,testuser2)

```
[root@pgdbsrv~]# adduser testuser1

[root@pgdbsrv~]# passwd testuser1 Changing

password for user testuser1.

New password:User@123.

Retype new password:

passwd: all authentication tokens updated successfully.

[root@pgdbsrv~]# adduser testuser2

[root@pgdbsrv~]# passwd testuser2 Changing

password for user testuser2.

New password:User@123.
```

```
Retype new password:

passwd: all authentication tokens updated successfully.
```

4.1.3 >> add user2 to dba group

```
[root@pgdbsrv~]# usermod -aG dba testuser2

[root@pgdbsrv~]# getent group dba
```

4.2 >>Ensure sudois configuredcorrectly

--(testuser1 has not been added to the /etc/sudoers file

```
[testuser1@rockylinux-database ~]$ whoami

testuser1

[testuser1@rockylinux-database ~]$ groups

testuser1

[testuser1@rockylinux-database ~]$ sudo -iu postgres



We trust you have received the usual lecture from the local System

Administrator. It usually boils down to these three things:


#1) Respect the privacy of others.

#2) Think before you type.

#3) With great power comes great responsibility.


[sudo] password for testuser1:

testuser1 is not in the sudoers file. This incident will be reported.


[root@pgdbsrv~]# echo '%dba ALL=(postgres) PASSWD: ALL' > /etc/sudoers.d/postgres
```

```
[root@pgdbsrv~]# cat /etc/sudoers.d/postgres

%dba ALL=(postgres) PASSWD: ALL

[root@pgdbsrv~]# ll /etc/sudoers.d/postgres

-rw-r--r--. 1 root root 32 Aug 9 22:05 /etc/sudoers.d/postgres

[root@pgdbsrv~]# chmod 600 /etc/sudoers.d/postgres
```

```
[postgres@rockylinux-database ~]$ psql -c "\du+ postgres"

List of roles

Role name |                  Attributes                  | Description

-----------+------------------------------------------------------------+-------------

postgres | Superuser, Create role, Create DB, Replication, Bypass RLS |
```

4.3 >> Ensure excessive administrative privileges are revoked

```
postgres=# SELECT * FROM pg_user WHERE usesuper ORDER BY usename;

usename | usesysid | usecreatedb | usesuper | userepl | usebypassrls | passwd | valuntil | useconfig

----------+----------+-------------+----------+---------+--------------+----------+----------+-----------

postgres |      10 | t         | t       | t      | t          | ******** |         |

(1 row)
```

```
[postgres@rockylinux-database ~]$ psql -c "\du+ appsadmin"

List of roles

Role name |        Attributes         | Description
```

```
-----------+----------------------------------+-------------

appsadmin | Superuser, Create role, Create DB+|

|3 connections |


[postgres@rockylinux-database ~]$ psql -c "SELECT * FROM pg_user WHERE usesuper ORDER BY usename;"
usename | usesysid | usecreatedb | usesuper | userepl | usebypassrls | passwd | valuntil |
                                                                                                     useconfig

-----------+----------+-------------+----------+---------+--------------+----------+----------+----------------------------------

appsadmin | 16426 | t           | t       | f       | f           | ******** |         | {"search_path=appschema, public"}

postgres |       10 | t          | t       | t       | t           | ******** |         |

(2 rows)
```

```
[postgres@rockylinux-database ~]$ psql -c "ALTER ROLE appsadmin NOSUPERUSER;"

ALTER ROLE

[postgres@rockylinux-database ~]$ psql -c "ALTER ROLE appsadmin NOCREATEROLE;"

ALTER ROLE

[postgres@rockylinux-database ~]$ psql -c "ALTER ROLE appsadmin NOCREATEDB;"

ALTER ROLE

[postgres@rockylinux-database ~]$ psql -c "ALTER ROLE appsadmin NOREPLICATION;"

ALTER ROLE

[postgres@rockylinux-database ~]$ psql -c "ALTER ROLE appsadmin NOBYPASSRLS;"

ALTER ROLE

[postgres@rockylinux-database ~]$ psql -c "ALTER ROLE appsadmin NOINHERIT;"

ALTER ROLE
```

```
[postgres@rockylinux-database ~]$ psql -c "\du+ appsadmin"

List of roles

Role name | Attributes | Description

-----------+----------------+-------------

appsadmin |              |
```

--For test table

```
postgres=# CREATE TABLE tbl_students(ROLL int,NAME varchar(20));

CREATE TABLE

postgres=# INSERT INTO tbl_students

SELECT 1 ROLL ,'RAM' NAME UNION ALL

SELECT 2 ROLL,'HARI' NAME UNION ALL

SELECT 3 ROLL,'GITA' NAME UNION ALL

SELECT 4 ROLL,'SITA' NAME UNION ALL

SELECT 5 ROLL,'RAMESH' NAME UNION ALL

SELECT 6 ROLL,'SANTOSH' NAME UNION ALL

SELECT 7 ROLL,'MAYA' NAME UNION ALL

SELECT 8 ROLL,'SANAM' NAME UNION ALL

SELECT 9 ROLL,'RAJAN' NAME UNION ALL

SELECT 10 ROLL,'MAHIMA';

INSERT 0 10

postgres=# select * from tbl_students ;
```

```
roll | name
------+---------
1 | RAM
2 | HARI
3 | GITA
4 | SITA
5 | RAMESH
6 | SANTOSH
7 | MAYA
8 | SANAM
9 | RAJAN
10 | MAHIMA
(10 rows)
```

```
postgres=# commit;
WARNING: there is no transaction in progress
COMMIT
```

4.4>> LockOutAccountsifNotCurrentlyinUse

```
SELECT rolname FROM pg_catalog.pg_roles WHERE rolname !~ '^pg_' AND
rolcanlogin;
rolname
-----------
admin
account
hr
```

```
postgres

appsadmin
```

```
postgres=# alter role account NOLOGIN;

ALTER ROLE
```

4.5 >> Ensure excessive function privileges are revoked

Excessive function privileges are revoked which are not required or are expressly forbidden by organizational guidance

4.6 Ensure excessive DML privileges are revoked

```
postgres=# select t.tablename, u.usename,

has_table_privilege(u.usename, t.tablename, 'select') as select,

has_table_privilege(u.usename, t.tablename, 'insert') as insert,

has_table_privilege(u.usename, t.tablename, 'update') as update,

has_table_privilege(u.usename, t.tablename, 'delete') as delete

from pg_tables t, pg_user u

where t.tablename = 'tbl_students'

and u.usename in ('postgres');


tablename | usename | select | insert | update | delete

--------------+----------+--------+--------+--------+--------

tbl_students | postgres | t     | t     | t     | t

(1 row)
```

```
postgres=# REVOKE CREATE ON SCHEMA public FROM PUBLIC;
REVOKE
```

4.7 >> Ensure Row Level Security (RLS) is configured correctly

```
postgres=# SELECT oid, relname, relrowsecurity FROM pg_class WHERE
relrowsecurity IS TRUE;
oid | relname | relrowsecurity
-----+---------+----------------
(0 rows)

postgres=# CREATE TABLE passwd (
user_name text UNIQUE NOT NULL,
pwhash text,
uid int PRIMARY KEY,
gid int NOT NULL,
real_name text NOT NULL,
home_phone text,
extra_info text,
home_dir text NOT NULL,
shell text NOT NULL
);
CREATE TABLE
postgres=# SELECT oid, relname, relrowsecurity FROM pg_class WHERE relname =
'passwd';
```

```
oid | relname | relrowsecurity
-------+---------+----------------
16401 | passwd | f
(1 row)
```

```
postgres=# CREATE USER admin;
CREATE ROLE
postgres=# CREATE USER account;
CREATE ROLE
postgres=# CREATE USER hr;
CREATE ROLE
postgres=#
INSERT INTO passwd VALUES('admin','xxx',0,0,'Admin','111-222-3333',null,'/root','/bin/dash');
INSERT 0 1
postgres=#
INSERT INTO passwd VALUES('account','xxx',1,1,'Account','123-456-7890',null,'/home/account','/bin/zsh');
INSERT 0 1
postgres=#
INSERT INTO passwd VALUES('hr','xxx',2,1,'Hr','098-765-4321',null,'/home/hr','/bin/zsh');
INSERT 0 1
```

we will enable RLS on the table:

```
postgres=# ALTER TABLE passwd ENABLE ROW LEVEL SECURITY;
ALTER TABLE
```

```
postgres=# SELECT oid, relname, relrowsecurity FROM pg_class WHERE relname =
'passwd';
oid | relname | relrowsecurity
-------+---------+----------------
16401 | passwd | t
(1 row)
```

```
postgres=# CREATE POLICY admin_all ON passwd TO admin USING (true) WITH CHECK
(true);
CREATE POLICY
postgres=# CREATE POLICY all_view ON passwd FOR SELECT USING (true);
CREATE POLICY
postgres=# SELECT current_user;
current_user
--------------
postgres
(1 row)
```

```
postgres=# GRANT SELECT, INSERT, UPDATE, DELETE ON passwd TO admin;
GRANT
postgres=# GRANT SELECT
(user_name, uid, gid, real_name, home_phone, extra_info, home_dir, shell)
ON passwd TO public;
GRANT
```

```
postgres=# GRANT UPDATE (pwhash, real_name, home_phone, extra_info, shell) ON passwd
TO public;

GRANT



postgres=# set role admin;

SET

postgres=> table passwd;

user_name | pwhash | uid | gid | real_name | home_phone | extra_info | home_dir | shell

-----------+--------+-----+-----+-----------+--------------+------------+---------------+-----------

admin     | xxx | 0 | 0 | Admin         | 111-222-3333 |            | /root         | /bin/dash

account | xxx | 1 | 1 | Account | 123-456-7890 |                  | /home/account | /bin/zsh

hr        | xxx | 2 | 1 | Hr            | 098-765-4321 |            | /home/hr      | /bin/zsh

(3 rows)


postgres=> set role account;

SET

postgres=> table passwd;

ERROR: permission denied for table passwd



postgres=> update passwd set real_name = 'Hr Dept';

UPDATE 0



postgres=> delete from passwd;

ERROR: permission denied for table passwd
```

4.8 >> Ensure the set_user extension is installed

```
appuser=# CREATE OR REPLACE VIEW appschema.roletree AS
WITH RECURSIVE
roltree AS (
SELECT u.rolname AS rolname,
u.oid AS roloid,
u.rolcanlogin,
u.rolsuper,
'{}'::name[] AS rolparents,
NULL::oid AS parent_roloid,
NULL::name AS parent_rolname
FROM pg_catalog.pg_authid u
LEFT JOIN pg_catalog.pg_auth_members m on u.oid = m.member
LEFT JOIN pg_catalog.pg_authid g on m.roleid = g.oid
WHERE g.oid IS NULL
UNION ALL
SELECT u.rolname AS rolname,
u.oid AS roloid,
u.rolcanlogin,
u.rolsuper,
t.rolparents || g.rolname AS rolparents,
g.oid AS parent_roloid,
g.rolname AS parent_rolname
FROM pg_catalog.pg_authid u

JOIN pg_catalog.pg_auth_members m on u.oid = m.member

JOIN pg_catalog.pg_authid g on m.roleid = g.oid

JOIN roltree t on t.roloid = g.oid

)

SELECT

r.rolname,

r.roloid,

r.rolcanlogin,

r.rolsuper,

r.rolparents

FROM roltree r

ORDER BY 1;
```

```
CREATE VIEW

appuser=# select * from pg_available_extensions where name = 'set_user';

name | default_version | installed_version | comment

------+-----------------+-------------------+---------

(0 rows)
```

```
appuser=# SELECT rolname FROM pg_authid WHERE rolsuper and rolcanlogin;

rolname ----------- postgres
```

```
appsadmin
(2 rows)
---- Verify there are no unexpected unprivileged roles that can login directly


appuser=# SELECT
r.rolname,
r.roloid,
r.rolcanlogin,
r.rolsuper,
r.rolparents
FROM appschema.roletree r
ORDER BY 1;
rolname          | roloid | rolcanlogin | rolsuper |      rolparents
-----------------------------+--------+-------------+----------+------------------------
account               | 16411 | t           | f        | {}
admin                 | 16410 | t           | f        | {}
appsadmin             | 16426 | t           | t        | {}
hr                    | 16412 | t           | f        | {}
pg_checkpoint         | 4544 | f            | f        | {}
pg_create_subscription   | 6304 | f            | f        | {}
pg_database_owner       | 6171 | f            | f        | {}
pg_execute_server_program | 4571 | f            | f        | {}
pg_maintain           | 6337  | f |          | f        | {}
pg_monitor            3373  |  f  |          |  f       | {pg_stat_scan_tables}
pg_monitor            3373  |  f  |          |  f       | {pg_read_all_stats}
pg_monitor            3373 | f               | f        | {pg_read_all_settings}
```

```
pg_read_all_data          | 6181|f            |f        | {}
pg_read_all_settings      | 3374|f            |f        | {}
pg_read_all_stats         | 3375|f            |f        | {}
pg_read_server_files      |  4569|f  |        |f        | {}
pg_signal_backend          4200|f             |f        | {}
pg_stat_scan_tables       | 3377|f            |f        | {}
pg_use_reserved_connections| 4550 | f         | f       |{}
pg_write_all_data         | 6182 | f          | f       | {}
pg_write_server_files     | 4570| f           | f       | {}
postgres                  |    10 | t         | t       | {}
```

```
SELECT
ro.rolname,
ro.roloid,
ro.rolcanlogin,
ro.rolsuper,
ro.rolparents
FROM appschema.roletree ro
WHERE (ro.rolcanlogin AND ro.rolsuper)
OR
(
ro.rolcanlogin AND EXISTS
(
SELECT TRUE FROM appschema.roletree ri
WHERE ri.rolname = ANY (ro.rolparents)
AND ri.rolsuper
)
);


appuser=# SELECT
ro.rolname,
ro.roloid,
ro.rolcanlogin,
ro.rolsuper,
ro.rolparents
FROM appschema.roletree ro
WHERE (ro.rolcanlogin AND ro.rolsuper)
OR
(
ro.rolcanlogin AND EXISTS
(
SELECT TRUE FROM appschema.roletree ri
WHERE ri.rolname = ANY (ro.rolparents)
AND ri.rolsuper
)
);
rolname | roloid | rolcanlogin | rolsuper | rolparents
-----------+--------+-------------+----------+------------
appsadmin | 16426 | t           | t        | {}
postgres |     10 | t           | t        | {}
```

```
(2 rows)


[root@pgdbsrv~]# dnf -y install set_user_17


DigitalOcean Droplet Agent                                         73 kB/s | 3.3 kB     00:00

Dependencies resolved.

= === == === === == === === == === === == === === == === === == === === == === === == === === == === === == =
================================================================================

Package                 Architecture           Version                  Repository           Size

= === == === === == === === == === === == === === == === === == === === == === === == === === == === === == =
================================================================================
Installing:

set_user_17
                         x86_64              4.1.0-1PGDG.rhel9              pgdg17                26 k


Transaction Summary

= === == === === == === === == === === == === === == === === == === === == === === == === === == === === == =
================================================================================
Install 1 Package



Total download size: 26 k

Installed size: 54 k

Downloading Packages:

set_user_17-4.1.0-1PGDG.rhel9.x86_64.rpm                                     114 kB/s | 26 kB
00:00
------ ----- ----- ---- ----- ----- ---- ----- ----- ---- ----- ---- ----- ----- ------ ----- ----- ---- ----- ----- ---- ----- ----- ---- ----- ---- - ---- ----
-------------------
Total
                                                              112 kB/s | 26 kB     00:00
```

```
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
Preparing       :                                                        1/1
Installing      :set_user_17-4.1.0-1PGDG.rhel9.x86_64                                1/1
Running scriptlet: set_user_17-4.1.0-1PGDG.rhel9.x86_64                              1/1
Verifying       :set_user_17-4.1.0-1PGDG.rhel9.x86_64                                1/1

Installed:
set_user_17-4.1.0-1PGDG.rhel9.x86_64


Complete!
```

```
[root@pgdbsrv~]# vi /var/lib/pgsql/17/data/postgresql.conf
shared_preload_libraries = 'set_user,pgaudit'
```

```
[root@pgdbsrv~]# systemctl restart postgresql-17
[root@pgdbsrv~]# systemctl status postgresql-17|grep 'ago$'
Active: active (running) since Sun 2025-08-10 09:43:14 +0545; 36s ago
```

```
appuser=# select * from pg_available_extensions where name = 'set_user';
name | default_version | installed_version |                 comment
----------+-----------------+-------------------+------------------------------------------
set_user | 4.1.0           |                   | similar to SET ROLE but with added logging
```

```
(1 row)

appuser=# create extension set_user;
CREATE EXTENSION
appuser=# select * from pg_available_extensions where name = 'set_user';
name | default_version | installed_version |                  comment
----------+-----------------+-------------------+------------------------------------------
set_user | 4.1.0          | 4.1.0            | similar to SET ROLE but with added logging
(1 row)

appuser=# grant execute on function set_user(text) to appsadmin ;
GRANT

appuser=# select set_user('appsadmin');
ERROR: switching to superuser not allowed
HINT: Use 'set_user_u' to escalate.
appuser=# select set_user_u('appsadmin');
set_user_u
------------
OK
(1 row)

appuser=# select current_user, session_user;
current_user | session_user
```

```
--------------+--------------
appsadmin | appsadmin
(1 row)

appuser=# select reset_user();
reset_user
------------
OK
(1 row)

appuser=# select current_user, session_user;
current_user | session_user
--------------+--------------
appsadmin | appsadmin
(1 row)
```

5 >> Connections and Login

--configure a pg_env file with the proper credentials and secure the file appropriately

5.1 >> Do Not Specify Passwords in the Command Line

[postgres@rockylinux-database ~]$ vi ~/.pg_env

```
Your server ip :5432:postgres:postgres:strongpassword
Your server ip:5432:appuser:appsadmin: strongpassword
```

```
localhost:5432:postgres:postgres: strongpassword

localhost:5432:appuser:appsadmin:Pg$A&p#S!R7*s
```

```
[postgres@rockylinux-database ~]$ ll ~/.pg_env
-rw-------. 1 postgres postgres 104 Aug 10 12:06 /var/lib/pgsql/.pg_env
[postgres@rockylinux-database ~]$ ll ~/.pg_env
-rw-------. 1 postgres postgres 104 Aug 10 12:06 /var/lib/pgsql/.pg_env
```

```
[postgres@rockylinux-database ~]$ psql -h localhost -U appsadmin -d appuser
psql: error: connection to server at "localhost" (::1), port 5432 failed: Connection refused
Is the server running on that host and accepting TCP/IP connections?
connection to server at "localhost" (127.0.0.1), port 5432 failed: Connection refused
Is the server running on that host and accepting TCP/IP connections?
[postgres@rockylinux-database ~]$ psql -h localhost or server-ip -U appsadmin -d appuser
Password for user appsadmin:
psql (17.5)
Type "help" for help.

appuser=#
```

5.2 >> Ensure PostgreSQL is Bound to an IP Address

```
[postgres@rockylinux-database ~]$ whoami
postgres
[postgres@rockylinux-database ~]$ psql -c 'SHOW listen_addresses'
```

```
listen_addresses

------------------

Your server ip

(1 row)
```

```
[root@pgdbsrv~]# vi /var/lib/pgsql/17/data/postgresql.conf

listen_addresses = 'localhost,YOUR SERVRE IP'
```

```
[postgres@rockylinux-database ~]$ psql -c 'SHOW listen_addresses'

listen_addresses

--------------------------

localhost,YOUR SERVER IP

(1 row)
```

5.3 >> Ensure login via "local" UNIX Domain Socket is configured

```
[postgres@rockylinux-database ~]$ psql 'host=localhost user=postgres sslmode=require'

Password for user postgres:

psql (17.5)
```

```
[root@rockylinux-database]# vi /var/lib/pgsql/17/data/pg_hba.conf

# "local" is for Unix domain socket connections only

local all           postgres                        peer

# Add your specific network ranges here with scram-sha-256 authentication(any address with scram-sha-256)

host all            all         0.0.0.0/0           scram-sha-256
```

5.4 >> Ensure login via "host" TCP/IP Socket is configured correctly (Manual)

```
postgres=# ALTER USER postgres WITH PASSWORD ‘strongpassword’;

ALTER ROLE
```

```
[root@pgdbsrv]# /var/lib/pgsql/17/data/pg_hba.conf

#Session encrypted

hostssl all           postgres      0.0.0.0/0          scram-sha-256

hostnossl all           postgres      0.0.0.0/0          reject
```

5.5 >> Ensure per-account connection limits are used

```
postgres=# SELECT rolname, rolconnlimit

FROM pg_roles

WHERE rolname NOT LIKE 'pg_%';

rolname | rolconnlimit

-----------+--------------

 postgres |        -1

admin      |        -1

  account |        -1

hr            |        -1

appsadmin |        -1

(5 rows)
```

```
ALTER USER postgres CONNECTION LIMIT 3;

ALTER USER appsadmin CONNECTION LIMIT 3;
```

```
postgres=# ALTER USER postgres CONNECTION LIMIT 3;

ALTER ROLE

postgres=# ALTER USER appsadmin CONNECTION LIMIT 3;

ALTER ROLE

postgres=# select pg_reload_conf();

pg_reload_conf

----------------

t

(1 row)
```

```
postgres=# SELECT rolname, rolconnlimit

FROM pg_roles

WHERE rolname NOT LIKE 'pg_%';

rolname | rolconnlimit

-----------+--------------

admin      |       -1

account    |       -1

hr         |       -1

postgres   |        3

appsadmin |         3

(5 rows)
```

5.6 >> Ensure Password Complexity is configured

```
postgres=# SHOW shared_preload_libraries;

shared_preload_libraries

--------------------------

set_user,pgaudit

(1 row)
```

```
postgres=# SHOW dynamic_library_path;

dynamic_library_path

----------------------

$libdir

(1 row)
```

```
[root@pgdbsrv]# vi /var/lib/pgsql/17/data postgresql.conf

shared_preload_libraries = 'set_user,pgaudit,$libdir/passwordcheck'
```

```
[root@pgdbsrvdata]# systemctl status postgresql-17

ines 1-27/27 (END)

[root@pgdbsrvdata]# systemctl status postgresql-17|grep 'ago$'

Active: active (running) since Sun 2025-08-10 13:38:53 +0545; 47s ago
```

```
postgres=# SELECT name, setting FROM pg_settings WHERE context IN

('backend','superuser-backend') ORDER BY 1;

name        | setting
```

```
----------------------+---------
ignore_system_indexes | off
jit_debugging_support | off
jit_profiling_support | off
log_connections       | on
log_disconnections    | on
post_auth_delay       | 0
(6 rows)
```

6. >> PostgreSQL Settings

6.1 >> Ensure 'backend' runtime parameters are configured correctly

```
[postgres@rockylinux-database ~]$ ps -few | grep -E -- '[p]ost.*-[D]'

postgres    484200            1    0 13:43 ?               00:00:00 /usr/pgsql-17/bin/postgres -D /var/lib/pgsql/17/data/
```

6.2 >> Ensure FIPS 140-2 OpenSSL Cryptography Is Used

```
[root@pgdbsrv~]#   fips-mode-setup   --check

Installation of FIPS modules is not completed.

FIPS mode is disabled.

[root@pgdbsrv~]#   fips-mode-setup   --check

Installation of FIPS modules is not completed.

FIPS mode is disabled.

[root@pgdbsrv~]# fips-mode-setup --enable
```

```
 *****************************************************************
* PRESS CONTROL-C WITHIN 15 SECONDS TO ABORT...                  *
*                                                 *
* ENABLING FIPS MODE AFTER THE INSTALLATION IS NOT RECOMMENDED. *
* THIS OPERATION CANNOT BE UNDONE.                        *
* REINSTALL WITH fips=1 INSTEAD.                        *
*****************************************************************
15... 14... 13... 12... 11... 10... 9... 8... 7... 6... 5... 4... 3... 2... 1...
Kernel initramdisks are being regenerated. This might take some time.
Setting system policy to FIPS
Note: System-wide crypto policies are applied on application start-up.
It is recommended to restart the system for the change of policies
to fully take place.
FIPS mode will be enabled.
Please reboot the system for the setting to take effect.


[root@pgdbsrv~]# fips-mode-setup --check
FIPS mode is enabled.
[root@pgdbsrv~]#
```

6.3 Ensure TLS is enabled and configured correctly

```
[postgres@rockylinux-database ~]$ psql
psql (17.5)
Type "help" for help.
```

```
postgres=# SHOW ssl;

ssl

-----

off

(1 row)
```

```
postgres=# SELECT name, setting, source FROM pg_settings WHERE name = 'ssl';

name | setting | source

------+---------+---------

ssl | off     | default
```

--we will be using a self-signed certificate

(generated via openssl) for the server, and the PostgreSQL defaults for file naming and

location in the PostgreSQL $PGDATA directory.

```
[root@pgdbsrvdata]# openssl req -new -x509 -days 365 -nodes -text \

-out "/var/lib/pgsql/17/data/server.crt" \

-keyout "/var/lib/pgsql/17/data/server.key" \

-subj "/C=US/ST=State/L=City/O=Organization/CN=localhost"

... ... .. ..+ + ++ ++ +++ +++ ++ +++ +++ ++ +++ +++ ++ +++ ++++ ++ * .+ ....+ .. ... .+ ... .. ... .. ... .. ..+ .. ..+ .. .+ .... .. ... ..+ + + ++ ++
+ +++ ++ +++ +++ ++ +++ +++ ++ +* ..... ... .. .+ ... ..+ .+ ... ... .. .+ ... ... . .+ .+ .... ... .. ..+ .+ ..+ ...+ . ... .. ...+ . ...+ . .+ .... .. .+ ... ..+ .+ ... ..
.....+.........++++++

.....+....+..++++++++++++++++++++++++++++++++++++++++*...+...++++++++++++++++++++++++++++++++++
+ +++ ++ * ...... ..+ .. ... .. ..+ .. .+ .... .. .+ ... ..+ .. ... .. ...+ . ..+ .. ... .. .+ ...+ .. ..+ .. . ... ... ..+ .. .. ...+ . ... .. ... ...+ . .+ ... ...+ . ..+ . + ...+ . ... ... .. ...
... ...+ .+ .. .. ... .+ .+ .... .. ... ..+ .+ ..+ .. .. ... .. ... .. .+ .+ .... .+ ... .+ ...+ .. .. ... .+ .+ .... .+ .... .. ... .. ... ..+ ..+ .. .. ... .. .+ ... ... . .+ .. .+ .+ ...+ .. ... .. .
... ...+ . ...+ . .+ .... .. ...+ .+ .. .. .+ ... .+ ..+ ... .. ... .. ...+ .. .. ... ..+ .. .. .+ ... ...+ . ... .. .+ ... ... .. ... .+ ... ..+ .. .. ...+ .. .. ... ..+ .. .. ..+ .. ...+ . ..+ .. .+ ....
```

```
… ..+ .. …+ . … ..+ .+ … .. .+ … ..+ .. ..+ .. …+ . ..+ .+ … …+ . … .+ … .. … ..+ .. .+ ..+ . … ..+ .. … .. …+ . … .+ …+ .. ..+ .. .. … .. . ..+ . … .. … ..+ .. .. .
+………+……+…+…..++++++
-----
```

```
[root@pgdbsrvdata]# chown -R postgres:postgres server.crt

[root@pgdbsrvdata]# chown -R postgres:postgres server.key

[root@pgdbsrvdata]# chmod -R 600 server.crt server.key
```

```
-rw-------. 1 postgres postgres 4391 Aug 10 14:21 server.crt

-rw-------. 1 postgres postgres 1704 Aug 10 14:21 server.key
```

```
# (change requires restart)

ssl = on

# force clients to use TLS v1.3 or newer

ssl_min_protocol_version = 'TLSv1.3'

# (change requires restart)

ssl_cert_file = '/var/lib/pgsql/17/data/server.crt'

# (change requires restart)

ssl_key_file = '/var/lib/pgsql/17/data/server.key'
```

```
postgres=# show ssl;

ssl

-----

on

(1 row)
```

```
postgres=# select name, setting from pg_settings where name like 'ssl%file';

name        |           setting
--------------------+----------------------------------
ssl_ca_file       |
ssl_cert_file     | /var/lib/pgsql/17/data/server.crt
ssl_crl_file      |
ssl_dh_params_file |
ssl_key_file      | /var/lib/pgsql/17/data/server.key
(5 rows)
```

6.4 >> Ensure that TLSv1.3, or later, is configured

```
postgres=# SHOW ssl_min_protocol_version;

ssl_min_protocol_version
--------------------------
TLSv1.3
(1 row)
```

6.5 >> Ensure Weak SSL/TLS Ciphers Are Disabled

```
[root@pgdbsrv~]# grep "ssl_ciphers" /var/lib/pgsql/17/data/postgresql.conf | cut -d ' ' -f 3 | sed "s/'//g" | tr ":" "\n"
HIGH
MEDIUM
+3DES
```

!aNULL

```
[postgres@rockylinux-database data]$ vi postgresql.conf
```

```
ssl_ciphers ='TLS_AES_256_GCM_SHA384,TLS_AES_128_GCM_SHA256,TLS_AES_128_CCM_SHA256,TLS_CHA
CHA20_POLY1305_SHA256,ECDHE-ECDSA-AES256-CCM,ECDHE-ECDSA-AES128-CCM,DHE-RSAAES256-
CCM,DHE-RSA-AES128-CCM,ECDHE-RSA-AES256-GCM-SHA384,ECDHE-RSA-AES128- GCM-
SHA256,ECDHE-ECDSA-AES256-GCM-SHA384,ECDHE-ECDSA-AES128-GCM-SHA256,DHEDSS-AES256-
GCM-SHA384,DHE-DSS-AES128-GCM-SHA256,DHE-RSA-AES256-GCMSHA384,DHE-RSA-AES128-GCM-
SHA256'
```

6.6 >>Ensure thepgcryptoextensionis installedandconfigured

correctly

```
postgres=# SELECT * FROM pg_available_extensions WHERE name='pgcrypto';

name | default_version | installed_version |        comment

----------+-----------------+------------------+------------------------

pgcrypto | 1.3          |                | cryptographic functions

(1 row)
```

```
postgres=# CREATE EXTENSION pgcrypto;

CREATE EXTENSION

postgres=# SELECT * FROM pg_available_extensions WHERE name='pgcrypto';

name | default_version | installed_version |        comment

----------+-----------------+------------------+------------------------

pgcrypto | 1.3          | 1.3          | cryptographic functions
```

7. >> Replication (Since this server is standalone, there is no need to configure replication settings.)

7.1 >>Ensure WAL archiving is configured and functional

```
postgres=# SELECT name, setting

FROM pg_settings

WHERE name IN ('archive_mode','archive_command','archive_library')

AND setting IS NOT NULL

AND setting <> 'off'

AND setting <> '(disabled)'

AND setting <> '';

name | setting

------+---------

(0 rows)
```

Ensure PostgreSQL subdirectory locations are outside the

data cluster

```
postgres=# SELECT name, setting FROM pg_settings WHERE (name ~ '_directory$'

OR name ~ '_tablespace');

name          |      setting

----------------------------+------------------------

allow_in_place_tablespaces | off

data_directory             | /var/lib/pgsql/17/data

default_tablespace         |

log_directory              | log

temp_tablespaces           |

(5 rows)
```

7.2 >> Ensure the backup and restore tool, 'pgBackRest', is installed and configured (Manual backup script for full, incremental, and archive (if needed).)

```
[postgres@rockylinux-database ~]$ pgbackrest

-bash: pgbackrest: command not found


[root@pgdbsrv~]# dnf install -y epel-release

DigitalOcean Droplet Agent             68 kB/s | 3.3 kB     00:00

Rocky Linux 9 - BaseOS               3.3 kB/s | 4.1 kB     00:01

Rocky Linux 9 - AppStream              4.6 kB/s | 4.5 kB     00:00

Rocky Linux 9 - CRB                 637 kB/s | 2.8 MB     00:04

Package epel-release-9-7.el9.noarch is already installed.

Dependencies resolved.

================================================================================

Package          Architecture Version          Repository    Size

================================================================================

Upgrading:

epel-release       noarch       9-10.el9         epel         19 k


Transaction Summary

================================================================================

Upgrade 1 Package


Total download size: 19 k

Downloading Packages:

epel-release-9-10.el9.noarch.rpm          64 kB/s | 19 kB     00:00

--------------------------------------------------------------------------------
```

```
Total                          14 kB/s | 19 kB     00:01

Running transaction check

Transaction check succeeded.

Running transaction test

Transaction test succeeded.

Running transaction

Preparing      :                                      1/1

Upgrading       :epel-release-9-10.el9.noarch                    1/2

Running scriptlet: epel-release-9-10.el9.noarch                    1/2

Cleanup         :epel-release-9-7.el9.noarch                     2/2

Running scriptlet: epel-release-9-7.el9.noarch                     2/2

Verifying       :epel-release-9-10.el9.noarch                    1/2

Verifying       :epel-release-9-7.el9.noarch                     2/2


Upgraded:

epel-release-9-10.el9.noarch


Complete!

[root@pgdbsrv~]# dnf -y install pgbackrest

Last metadata expiration check: 0:00:44 ago on Sun 10 Aug 2025 10:05:59 PM +0545.

Dependencies resolved.

================================================================================

Package       Arch       Version             Repository       Size

================================================================================

Installing:

pgbackrest     x86_64     2.56.0-1PGDG.rhel9     pgdg-common     546 k
```

```
Installing dependencies:

libssh2        x86_64     1.11.0-1.el9          epel           132 k


Transaction Summary

==================================================================================

Install 2 Packages


Total download size: 678 k

Installed size: 1.6 M

Downloading Packages:

(1/2): pgbackrest-2.56.0-1PGDG.rhel9.x86_64 4.7 MB/s | 546 kB    00:00

(2/2): libssh2-1.11.0-1.el9.x86_64.rpm      387 kB/s | 132 kB    00:00

-----------------------------------------------------------------------------

Total                              471 kB/s | 678 kB    00:01

Running transaction check

Transaction check succeeded.

Running transaction test

Transaction test succeeded.

Running transaction

Preparing       :                                        1/1

Installing      : libssh2-1.11.0-1.el9.x86_64                    1/2

Running scriptlet: pgbackrest-2.56.0-1PGDG.rhel9.x86_64            2/2

Installing      : pgbackrest-2.56.0-1PGDG.rhel9.x86_64            2/2

Running scriptlet: pgbackrest-2.56.0-1PGDG.rhel9.x86_64            2/2

Verifying       : libssh2-1.11.0-1.el9.x86_64                    1/2

Verifying       : pgbackrest-2.56.0-1PGDG.rhel9.x86_64            2/2
```

```
Installed:

libssh2-1.11.0-1.el9.x86_64     pgbackrest-2.56.0-1PGDG.rhel9.x86_64

Complete!
```

--Prerequisites for Base Backup of Postgres: Ensure Write-Ahead Logging (WAL) is enabled:

```
[root@pgdbsrv~]# chown -R postgres:postgres /backup/

[postgres@rockylinux-database ~]$ mkdir -p /backup/archive
```

```
postgres=# \l

List of databases

Name | Owner | Encoding | Locale Provider | Collate | Ctype | Locale | ICU Rules | Access privileges

-----------+----------+----------+-----------------+-------------+-------------+--------+-----------+----------------------

appuser   |postgres|UTF8      |libc        |en_US.UTF-8 | en_US.UTF-8 |       |         | =Tc/postgres        +

|       |       |            |         |         |      |        |postgres=CTc/postgres+

|       |       |            |         |         |      |        |appsadmin=c/postgres

postgres|postgres|UTF8       |libc        |en_US.UTF-8 | en_US.UTF-8 |       |         |

template0|postgres|UTF8      |libc        |en_US.UTF-8 | en_US.UTF-8 |       |         | =c/postgres         +

|       |       |            |         |         |      |        |postgres=CTc/postgres

template1|postgres|UTF8      |libc        |en_US.UTF-8 | en_US.UTF-8 |       |         | =c/postgres         +

|       |       |            |         |         |      |        |postgres=CTc/postgres
```

```
postgres=#ALTERSYSTEMSETwal_level='replica';

ALTER SYSTEM
```

```
postgres=# ALTER SYSTEM SET archive_mode = 'on';

ALTER SYSTEM

postgres=# ALTER SYSTEM SET archive_command = 'cp %p /backup/archive/%f';

ALTER SYSTEM

postgres=# SELECT pg_reload_conf();

pg_reload_conf

----------------

t

(1 row)



postgres=# ALTER SYSTEM SET summarize_wal = 'on';

ALTER SYSTEM

postgres=# SELECT pg_reload_conf();

pg_reload_conf

----------------

t

(1 row)



postgres=# \q

[root@pgdbsrv/]# systemctl restart postgresql-17

[root@pgdbsrv/]# systemctl status postgresql-17

● postgresql-17.service - PostgreSQL 17 database server

Loaded: loaded (/usr/lib/systemd/system/postgresql-17.service; enabled; preset: disabled)

Drop-In: /etc/systemd/system/postgresql-17.service.d

 └─security.conf, umask.conf
```

```
Active: active (running) since Sun 2025-08-10 21:05:43 +0545; 3s ago

Docs: https://www.postgresql.org/docs/17/static/

Process: 511301 ExecStartPre=/usr/pgsql-17/bin/postgresql-17-check-db-dir ${PGDATA} (code=exited, status=0/SUCCESS)
Main PID: 511307 (postgres)

Tasks: 9 (limit: 22924)

Memory: 19.6M

CPU: 119ms

CGroup: /system.slice/postgresql-17.service

 ├─511307 /usr/pgsql-17/bin/postgres -D /var/lib/pgsql/17/data/

 ├─511308 "postgres: logger "

 ├─511309 "postgres: checkpointer "

 ├─511310 "postgres: background writer "

 ├─511312 "postgres: walwriter "

 ├─511313 "postgres: walsummarizer "

 ├─511314 "postgres: autovacuum launcher "

 ├─511315 "postgres: archiver "

 └─511316 "postgres: logical replication launcher "



Aug 10 21:05:43 rockylinux-database systemd[1]: Starting PostgreSQL 17 database server...

Aug 10 21:05:43 rockylinux-database postgres[511307]: 2025-08-10 15:20:43.828 UTC [511307]: [1-1] db=,user=,app=,client=LOG: 00000: pgaudit extension init>
Aug 10 21:05:43 rockylinux-database postgres[511307]: 2025-08-10 15:20:43.828 UTC [511307]: [2-1] db=,user=,app=,client=LOCATION: _PG_init, pgaudit.c:2330
Aug 10 21:05:43 rockylinux-database postgres[511307]: 2025-08-10 15:20:43.843 UTC [511307]: [3-1] db=,user=,app=,client=LOG: 00000: redirecting log output>
Aug 10 21:05:43 rockylinux-database postgres[511307]: 2025-08-10 15:20:43.843 UTC [511307]: [4-1] db=,user=,app=,client=HINT: Future log output will appea>
Aug 10 21:05:43 rockylinux-database postgres[511307]: 2025-08-10 15:20:43.843 UTC [511307]: [5-1] db=,user=,app=,client=LOCATION: SysLogger_Start, syslogg>
Aug 10 21:05:43 rockylinux-database systemd[1]: Started PostgreSQL 17 database server.
```

(Memory Tuning of Postgresql)

-- Shared Buffers (shared_buffers = 25% of your total RAM) -- Work Mem (set this based on your available RAM and the number of concurrent connections) -- Maintenance Work Mem (This setting controls the memory available for maintenance operations such as VACUUM, CREATE INDEX, and ALTER TABLE. For a system with larger data sets, increasing this can speed up these tasks) -- Effective Cache Size (set this to around 50-75% of your total system memory)

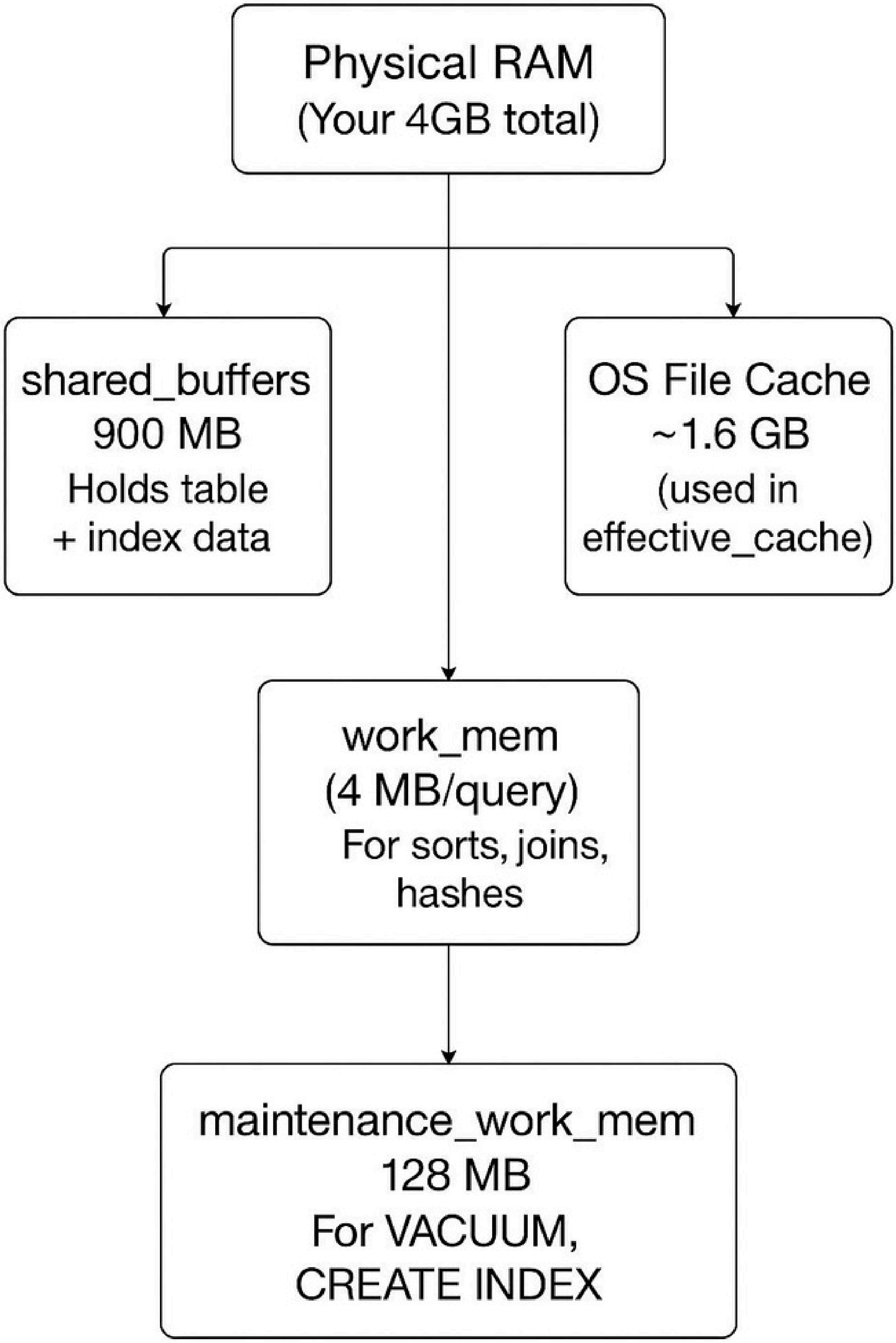
```
[root@pgdbsrvdata]# cat /var/lib/pgsql/17/data/postgresql.conf | grep -E "shared_buffers = 900MB|work_mem = 4MB|maintenance_work_mem = 128MB|effective_cache_size = 2.5GB"

shared_buffers = 900MB            # min 128kB

work_mem = 4MB                    # min 64kB

maintenance_work_mem = 128MB        # min 64kB

effective_cache_size = 2.5GB
```


Physical RAM
(Your 4GB total)
shared_buffers
900 MB
Holds table
+ index data
OS File Cache
~1.6 GB
(used in
effective_cache)
work_mem
(4 MB/query)
For sorts, joins,
hashes
maintenance_work_mem
128 MB
For VACUUM,
CREATE INDEX

--Checkpoints are moments when all data is flushed to disk. Optimizing these reduces disk I/O pressure during peak times.

--checkpoint_segments: Controls the number of log segments between checkpoints. Increasing this reduces the frequency of checkpoints.
--checkpoint_timeout: Increases the time between checkpoints.

--checkpoint_completion_target: Controls how aggressively PostgreSQL writes dirty buffers to disk between checkpoints. A higher value smooths disk I/O load.

```
[Eoot@pgdbsrvdata]# cat /var/lib/pgsql/17/data/postgresql.conf | grep "checkpoint_timeout = 15min|checkpoint_completion_target = 0.9|checkpoint_warning = 30s|max_wal_size = 1GB"

checkpoint_timeout = 15min
                                # range 30s-1d
checkpoint_completion_target = 0.9
                                   # checkpoint target duration, 0.0 - 1.0

checkpoint_warning = 30s        # 0 disables

max_wal_size = 1GB
```

```
[root@pgdbsrvdata]# cat /var/lib/pgsql/17/data/postgresql.conf | grep -E "wal_buffers = 32MB|wal_writer_delay = 500ms"

wal_buffers = 32MB              # min 32kB, -1 sets based on shared_buffers

wal_writer_delay = 500ms        # 1-10000 milliseconds
```

```
[root@pgdbsrvdata]# cat /var/lib/pgsql/17/data/postgresql.conf | grep -E "max_connections = 150"

max_connections = 150
                                # (change requires restart)
```