

# Transparent Data Encryption (TDE)

## Steps for creating deb packages for Cybertec-postgresql - version 15.3

Step1:

```
wget -c  
https://github.com/cybertec-postgresql/postgres/archive/refs/tags/PG_15_3_TDE_1_1_5.tar.gz
```

Step2:

```
tar -zxvf PG_15_3_TDE_1_1_5.tar.gz
```

Step3:

```
cd postgres-PG_15_3_TDE_1_1_5/
```

Step4:

```
git clone https://salsa.debian.org/postgresql/postgresql.git
```

Step5:

```
cd postgresql/
```

```
git branch
```

```
cd ..
```

```
cd postgres-PG_15_3_TDE_1_1_5/  
rsync -avz ./postgresql/debian .
```

```
sudo apt install dpkg-dev  
sudo apt install autoconf bison clang
```

```
sudo apt install flex gdb gettext libio-pty-perl libipc-run-perl  
libkrb5-dev libldap2-dev liblz4-dev libpam0g-dev
```

```
sudo apt install libperl-dev libreadline-dev libsasl2-dev libssl-dev  
libsystemd-dev libxml2-utils libxslt1-dev
```

```
sudo apt install python3-dev systemtap-sdt-dev tcl-dev uuid-dev xsltproc  
zlib1g-dev  
sudo apt install llvm-dev lz4  
sudo apt install pkg-config  
sudo apt install debhelper-compat  
sudo apt install dh-exec  
sudo apt install docbook-xsl  
sudo apt install libzstd-dev  
sudo apt install postgresql-common
```

```
vim postgresql-15.install (in the debian folder. Add pg_keytool binary  
as well as pg_keytool manpage)
```

```
cp debian/libpq5/DEBIAN/symbols debian/libpq5.symbols (file attached)  
dpkg-buildpackage -rfakeroot -b -uc -us
```

```
cd ..  
ls  
mkdir packages  
ls *.deb  
mv *.deb packages/
```

```
# create a container of postgres
```

```
ravi@VALHALLA:~/tomtest$ podman run -dt --name poscon -e  
POSTGRES_USER=demo -e POSTGRES_PASSWORD=demo -e POSTGRES_DB=demo  
-p 5432:5432 -d docker.io/postgres:12
```

```
Ab718422acdd748e3e632357547fc2083bc83b19fd4aaa020c6a27b106e60f83
```

```
ravi@VALHALLA:~/tomtest$ podman ps
```

CONTAINER ID	IMAGE	COMMAND	CREATED
STATUS	PORTS	NAMES	
ab718422acdd	docker.io/library/postgres:12	postgres	5 seconds ago
Up 6 seconds ago	0.0.0.0:5432->5432/tcp	poscon	

```
# go inside container
```

```
ravi@VALHALLA:~/tomtest$ podman exec -it poscon bash
```

```
root@ab718422acdd:/# psql -U demo
psql (12.16 (Debian 12.16-1.pgdg120+1))
Type "help" for help.
```

```
demo=#
```

```
demo=# CREATE TABLE tbl_demo (
    id serial PRIMARY KEY,
    name VARCHAR,
    email VARCHAR,
    mobile CHARACTER(10)
);
```

```
CREATE TABLE
```

```
demo=# INSERT INTO tbl_demo (name, email, mobile) VALUES ('demo1',
'demo1@demo.com', '1234567890');
```

```
INSERT 0 1
```

```
demo=# SELECT * FROM tbl_demo;
```

id	name	email	mobile
1	demo1	demo1@demo.com	1234567890

(1 row)

```
demo=# SELECT pg_relation_filepath('tbl_demo');  
pg_relation_filepath
```

```
-----  
base/16384/16387  
(1 row)
```

```
demo=# \q
```

```
ravi@VALHALLA:~/tomtest$ podman exec -it poscon bash  
root@ab718422acdd:/var/lib/postgresql/data/base/16384# cat 16387  
demo1demo1@demo.com1234567890
```

## Transparent Data Encryption (TDE) enabled in PostgreSQL

*In the TDE-enabled PostgreSQL setup, you've shown that the data in the physical database files appears to be encrypted and not readable. This is the expected behavior of TDE, where the data is encrypted at the storage level, and even if someone gains access to the physical database files, they wouldn't be able to read the actual data without proper decryption keys.*

*TDE provides an extra layer of security for data stored on disk, making it more difficult for unauthorized individuals to access sensitive information in case they gain access to the physical storage.*

FOLLOW THIS LINK FOR FURTHER STEP ;

<https://www.cybertec-postgresql.com/en/transparent-data-encryption-installation-guide/>

```
wget https://download.cybertec-postgresql.com/postgresql-12.3_TDE_1.0.tar.gz
```

```
tar xvfz postgresql-12.3_TDE_1.0.tar.gz
```

```
ravi@clientldp:~/postde$ Wget  
https://download.cybertec-postgresql.com/postgresql-12.3_TDE_1.0.tar.gz
```

```
tar xvfz postgresql-12.3_TDE_1.0.tar.gz
```

```
ravi@clientldp:~$ ls  
' ''\004' Desktop Downloads Music postde snap Videos  
389ds Documents ldaptest.sh Pictures Public Templates  
ravi@clientldp:~$ cd postde/  
ravi@clientldp:~/postde$ ls  
postgresql-12.3_TDE_1.0 postgresql-12.3_TDE_1.0.tar.gz  
ravi@clientldp:~/postde$ cd postgresql-12.3_TDE_1.0/  
ravi@clientldp:~/postde/postgresql-12.3_TDE_1.0$
```

```
cd postgresql-12.3_TDE_1.0.tar.gz
```

```
sudo apt update
```

```
ravi@clientldp:~$ sudo apt-get update  
[sudo] password for ravi:  
Sorry, try again.  
[sudo] password for ravi:  
Hit:1 http://in.archive.ubuntu.com/ubuntu focal InRelease  
Get:2 http://security.ubuntu.com/ubuntu focal-security InRelease [114 kB]
```

```
sudo apt-get install build-essential checkinstall zlib1g-dev  
postgresql-client-common libreadline-dev libpq-dev
```

```
ravi@clientldp:~/postde/postgresql-12.3_TDE_1.0$ sudo apt-get install build-essential checkinstall zlib1g-dev postgresql-client-common  
libreadline-dev libpq-dev  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
libreadline-dev is already the newest version (8.0-4).  
checkinstall is already the newest version (1.6.2+git20170426.d24a630-2ubuntu1).  
build-essential is already the newest version (12.8ubuntu1.1).  
libpq-dev is already the newest version (12.10-0ubuntu0.20.04.1).  
postgresql-client-common is already the newest version (214ubuntu0.1).  
zlib1g-dev is already the newest version (1:1.2.11.dfsg-2ubuntu1.5).  
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.  
ravi@clientldp:~/postde/postgresql-12.3_TDE_1.0$
```

```
sudo apt-get install libldap2-dev libperl-dev python-dev
```

```
ravi@clientldp:~/postde/postgresql-12.3_TDE_1.0$ sudo apt-get install libldap2-dev libperl-dev python-dev  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
Note, selecting 'python-dev-is-python2' instead of 'python-dev'  
python-dev-is-python2 is already the newest version (2.7.17-4).  
libldap2-dev is already the newest version (2.4.49+dfsg-2ubuntu1.9).  
libperl-dev is already the newest version (5.30.0-9ubuntu0.4).  
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.  
ravi@clientldp:~/postde/postgresql-12.3_TDE_1.0$
```

```
./configure --prefix=/usr/local/pg12tde --with-openssl --with-perl \  
--with-python --with-ldap
```

```
ravi@clientldp:~/postde/postgresql-12.3_TDE_1.0$ ./configure --prefix=/usr/local/pg12tde --with-openssl --with-perl --with-python --wi  
th-ldap  
checking build system type... x86_64-pc-linux-gnu  
checking host system type... x86_64-pc-linux-gnu  
checking which template to use... linux  
checking whether NLS is wanted... no  
checking for default port number... 5432  
checking for block size... 8kB  
checking for segment size... 1GB  
checking for WAL block size... 8kB  
checking for gcc... gcc  
checking whether the C compiler works... yes  
checking for C compiler default output file name... a.out  
checking for suffix of executables...  
checking whether we are cross compiling... no  
checking for suffix of object files... o  
checking whether we are using the GNU C compiler... yes  
checking whether gcc accepts -g... yes  
checking for gcc option to accept ISO C89... none needed  
checking for gcc option to accept ISO C99... none needed  
ravi@clientldp:~/postde/postgresql-12.3_TDE_1.0$
```

```
Sudo make install
```

```
ravi@clientldp:~/postde/postgresql-12.3_TDE_1.0$ sudo make install
make -C ./src/backend generated-headers
make[1]: Entering directory '/home/ravi/postde/postgresql-12.3_TDE_1.0/src/backend'
make -C catalog distprep generated-header-symlinks
make[2]: Entering directory '/home/ravi/postde/postgresql-12.3_TDE_1.0/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 '/home/ravi/postde/postgresql-12.3_TDE_1.0/src/backend/catalog'
make -C utils distprep generated-header-symlinks
make[2]: Entering directory '/home/ravi/postde/postgresql-12.3_TDE_1.0/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 '/home/ravi/postde/postgresql-12.3_TDE_1.0/src/backend/utils'
make[1]: Leaving directory '/home/ravi/postde/postgresql-12.3_TDE_1.0/src/backend'
make -C src install
```

```
cd contrib
```

```
make install
```

```
ravi@clientldp:~/postde/postgresql-12.3_TDE_1.0$ cd contrib
ravi@clientldp:~/postde/postgresql-12.3_TDE_1.0/contrib$ make install
make -C ../src/backend generated-headers
make[1]: Entering directory '/home/ravi/postde/postgresql-12.3_TDE_1.0/src/backend'
make[1]: Nothing to be done for 'generated-headers'.
make[1]: Leaving directory '/home/ravi/postde/postgresql-12.3_TDE_1.0/src/backend'
make[1]: Entering directory '/home/ravi/postde/postgresql-12.3_TDE_1.0/src/backend/catalog'
make[2]: Nothing to be done for 'distprep'.
```

```
vim /somewhere/provide_key.sh
```

```
#!/bin/sh
echo 882fb7c12e80280fd664c69d2d636913
```

```
chmod +x /somewhere/provide_key.sh
```

```
ravi@clientldp:~$ sudo mkdir /usr/local/pg12tde/data
ravi@clientldp:~$ sudo chmod 775 /usr/local/pg12tde/data
ravi@clientldp:~$ sudo chown ravi /usr/local/pg12tde/data/
```

```
ravi@clientldp:~$ sudo mkdir /usr/local/pg12tde/data
ravi@clientldp:~$ sudo chown ravi /usr/local/pg12tde/data/
ravi@clientldp:~$
```

```
export PATH=$PATH:/usr/local/pg12tde/bin
```

```
ravi@clientldp:/usr/local/pg12tde$ /usr/local/pg12tde/bin/initdb -D /usr/local/pg12tde/data/ -K /home/ravi/provide_key.sh
```

```
ravi@clientldp:/usr/local/pg12tde/data$ /usr/local/pg12tde/bin/initdb -D /usr/local/pg12tde/data/ -K /home/ravi/provide_key.sh
The files belonging to this database system will be owned by user "ravi".
This user must also own the server process.

The database cluster will be initialized with locale "en_IN".
The default database encoding has accordingly been set to "UTF8".
The default text search configuration will be set to "english".

Data page checksums are disabled.
Data encryption is enabled.

fixing permissions on existing directory /usr/local/pg12tde/data ... ok
creating subdirectories ... ok
selecting dynamic shared memory implementation ... posix
selecting default max_connections ... 100
selecting default shared_buffers ... 128MB
selecting default time zone ... Asia/Kolkata
creating configuration files ... ok
running bootstrap script ... ok
performing post-bootstrap initialization ... ok
syncing data to disk ... ok
```

```
initdb: warning: enabling "trust" authentication for local connections
You can change this by editing pg_hba.conf or using the option -A, or
--auth-local and --auth-host, the next time you run initdb.
```

```
Success. You can now start the database server using:
```

```
/usr/local/pg12tde/bin/pg_ctl -D /usr/local/pg12tde/data/ -l logfile start
```

```
ravi@clientldp:/usr/local/postgres$ pg_ctl -D /usr/local/pg12tde/data start
```

```
ravi@clientldp:/usr/local/postgres$ pg_ctl -D /usr/local/pg12tde/data start
2023-10-14 12:08:08.892 IST [24065] LOG:  starting PostgreSQL 12.3_TDE_1.0 on x86_64-pc-linux-gnu, compiled by gcc (Ubuntu 9.4.0
-lubuntu1-20.04.2) 9.4.0, 64-bit
2023-10-14 12:08:08.893 IST [24065] LOG:  listening on IPv4 address "127.0.0.1", port 5432
2023-10-14 12:08:08.899 IST [24065] LOG:  listening on Unix socket "/tmp/.PGSQL.5432"
waiting for server to start....2023-10-14 12:08:08.937 IST [24072] LOG:  database system was shut down at 2023-10-14 11:28:40 IS
T
2023-10-14 12:08:08.949 IST [24065] LOG:  database system is ready to accept connections
done
server started
```

```
ravi@clientldp:/usr/local/postgres$ pg_controldata //usr/local/pg12tde/data  
| grep -i encryp
```

```
ravi@clientldp:/usr/local/postgres$ pg_controldata //usr/local/pg12tde/data | grep -i encryp  
Data encryption:          on  
Data encryption fingerprint: 740A905130FE614CE0BE36B612157A09
```

```
ravi@clientldp:/usr/local/postgres$ /usr/local/pg12tde/bin/psql postgres
```

```
postgres=# SHOW data_encryption;  
data_encryption ----- on (1 row)
```

```
postgres=# CREATE TABLE employe (  
    employee_id serial PRIMARY KEY,  
    first_name VARCHAR (50),  
    last_name VARCHAR (50),  
    job_title VARCHAR (100),  
    hire_date DATE  
) ;
```

```
postgres=# INSERT INTO employe (first_name, last_name, job_title, hire_date)  
VALUES  
    ('John', 'Doe', 'Software Engineer', '2023-10-14'),  
    ('Jane', 'Smith', 'Product Manager', '2023-09-30'),  
    ('Bob', 'Johnson', 'Data Analyst', '2023-10-01');  
INSERT 0 3
```

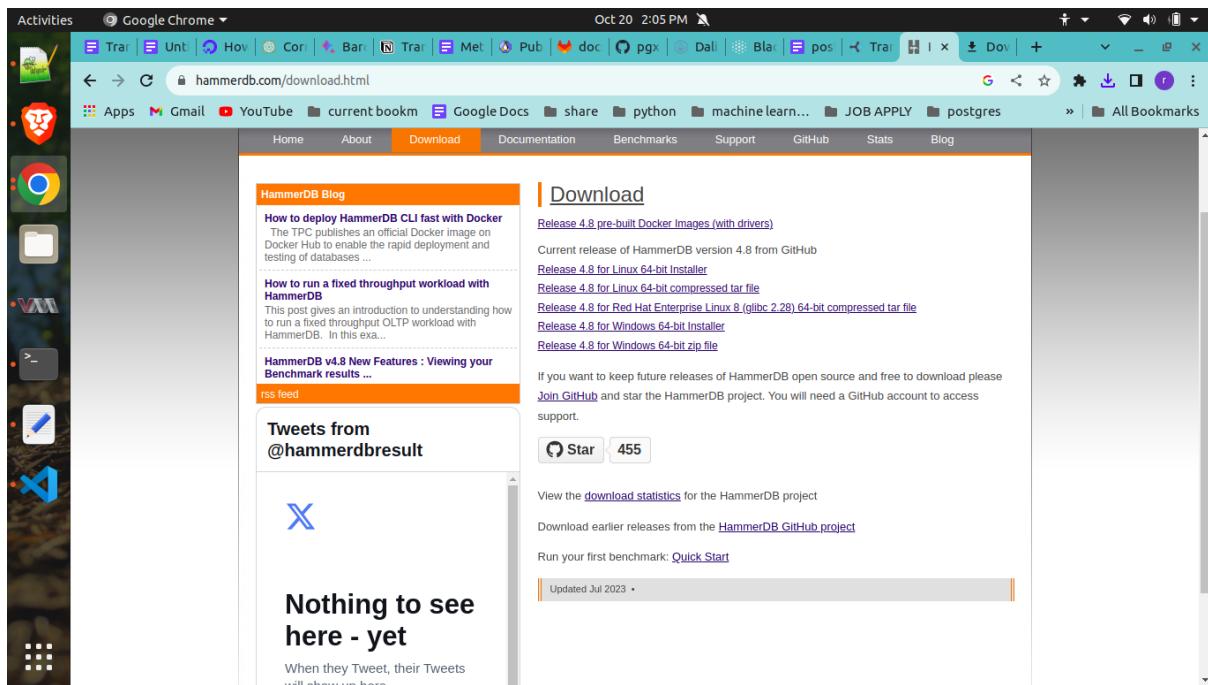
```
postgres=# select * from employe;
```



# Load Testing b/w Traditional and TDE using HammerDB

Download hammerdb tar file

<https://www.hammerdb.com/download.html>

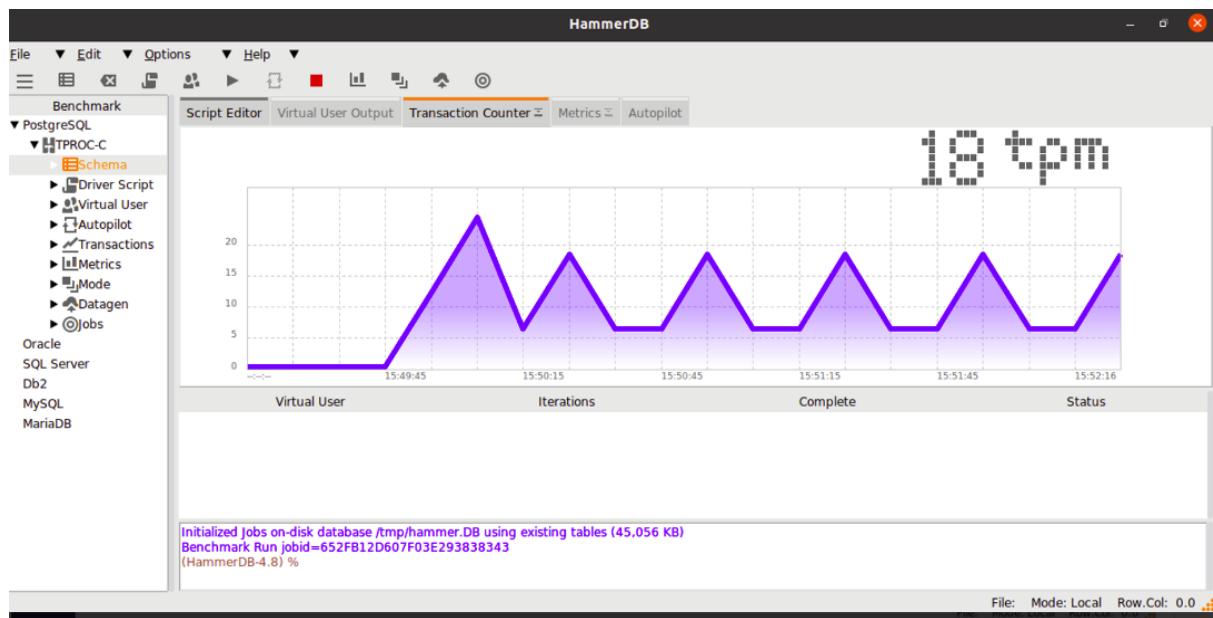
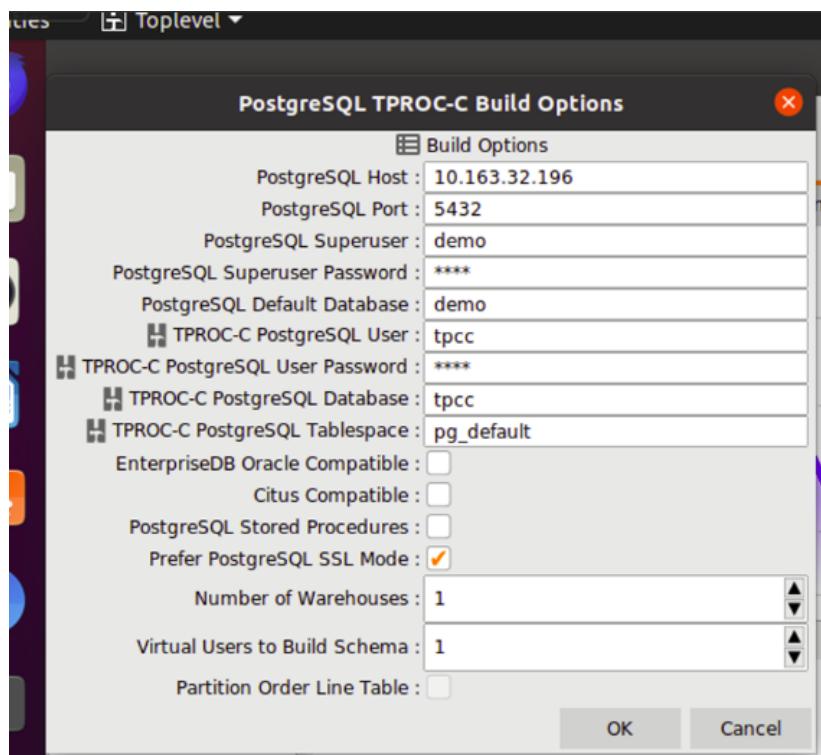


```
ravi@clientldp:~$ cd Downloads/
ravi@clientldp:~/Downloads$ ls
HammerDB-4.8-Linux.tar.gz postgresql-12.3_TDE_1.0.tar.gz
ravi@clientldp:~/Downloads$ tar -xvf HammerDB-4.8-Linux.tar.gz
```

```
ravi@clientldp:~$ cd Downloads/
ravi@clientldp:~/Downloads$ ls
HammerDB-4.8 HammerDB-4.8-Linux.tar.gz postgresql-12.3_TDE_1.0.tar.gz
ravi@clientldp:~/Downloads$ cd HammerDB-4.8/
ravi@clientldp:~/Downloads/HammerDB-4.8$ ls
agent  ChangeLog      config      hammerdb    hammerdbws  include  LICENSE  README.md  SQL
bin   CODE_OF_CONDUCT.md  CONTRIBUTING.md  hammerdbcli  Images    lib      modules  scripts
```

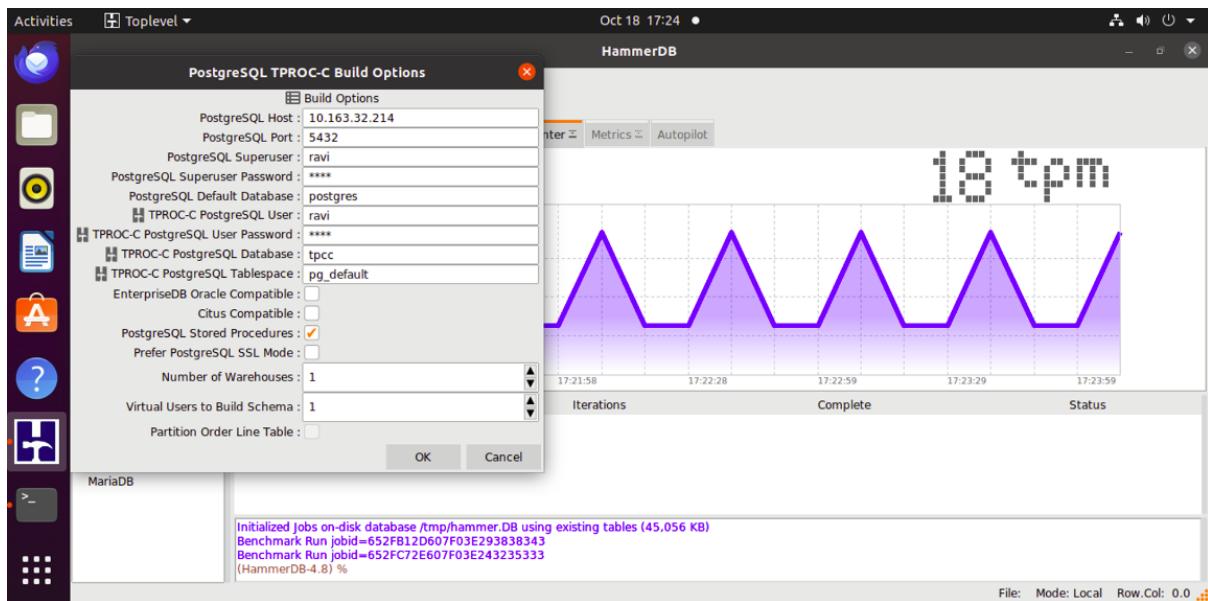
[OB]

For 1st machine 10.163.32.196



For second machine ip 10.123.32.214

## TDE LOAD TESTING



# SSL

```
ravi@clientldp:~$ openssl req -new -newkey rsa:2048 -days 365 -nodes -x509 -keyout server.key -out server.crt
```

```
pg_commit_ts pg_ident.conf pg_notify pg_snapshots pg_subtrans PG_VERSION postgresql.auto.conf postmaster.pid
ravi@clientldp:/usr/local/pgl2tde/data$ openssl req -new -newkey rsa:2048 -days 365 -nodes -x509 -keyout server.key -out server.crt
Generating a RSA private key
.....+++++
.....+++++
writing new private key to 'server.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:IN
State or Province Name (full name) [Some-State]:INDIA
Locality Name (eg, city) []:DELHI
Organization Name (eg, company) [Internet Widgits Pty Ltd]:KEENABLE
Organizational Unit Name (eg, section) []:DEVOPS
Common Name (e.g. server FQDN or YOUR name) []:RAVI
Email Address []:ravishankar.ravi@fosteringlinux.com
ravi@clientldp:/usr/local/pgl2tde/data$ ls
base          pg_hba.conf    pg_notify      pg_stat      pg_twophase  postgresql.auto.conf  server.crt
global        pg_ident.conf  pg_replslot   pg_stat_tmp  PG_VERSION  postgresql.conf       server.key
pg_commit_ts  pg_logical    pg_serial     pg_subtrans  pg_wal      postmaster.opts
pg_dynshmem   pg_multixact  pg_snapshots pg_tblspc   pg_xact    postmaster.pid
ravi@clientldp:/usr/local/pgl2tde/data$ vim postgresql.conf
ravi@clientldp:/usr/local/pgl2tde/data$
```

[OB]

```
ravi@clientldp:~$ openssl req -new -newkey rsa:2048 -days 365 -nodes -x509 -keyout server.key -out server.crt
Generating a RSA private key
.....+++++
.....+++++
writing new private key to 'server.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:india
string is too long, it needs to be no more than 2 bytes long
Country Name (2 letter code) [AU]:In
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:delhi
Organization Name (eg, company) [Internet Widgits Pty Ltd]:keenable
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:ravi
Email Address []:rshsr25@gmail.com
```

```
ravi@clientldp:/usr/local/pg12tde/data$ vim postgresql.conf
```

```
#-----  
# CONNECTIONS AND AUTHENTICATION  
#-----  
  
# - Connection Settings -  
  
listen_addresses = '*'          # what IP address(es) to listen on;  
                                # comma-separated list of addresses;  
                                # defaults to 'localhost'; use '*' for all  
                                # (change requires restart)  
port = 5432                      # (change requires restart)  
max_connections = 100           # (change requires restart)  
  
# - SSL -  
  
ssl = on  
#ssl_ca_file = ''  
ssl_cert_file = '/usr/local/pg12tde/data/server.crt'  
#ssl_crl_file = ''  
ssl_key_file = '/usr/local/pg12tde/data/server.key'  
#ssl_ciphers = 'HIGH:MEDIUM:+3DES:!aNULL' # allowed SSL ciphers  
#ssl_prefer_server_ciphers = on  
#ssl_ecdh_curve = 'prime256v1'  
#ssl_min_protocol_version = 'TLSv1'  
#ssl_max_protocol_version = ''  
#ssl_dh_params_file = ''  
#ssl_passphrase_command = ''  
#ssl_passphrase_command_reload = off  
  
# - Encryption -
```

```
ravi@clientldp:/usr/local/pg12tde/data$ vim pg_hba.conf
```

```
# That name.

# This file is read on server startup and when the server receives a
# SIGHUP signal. If you edit the file on a running system, you have to
# SIGHUP the server for the changes to take effect, run "pg_ctl reload",
# or execute "SELECT pg_reload_conf()".

# Put your actual configuration here
# -----
#
# If you want to allow non-local connections, you need to add more
# "host" records. In that case you will also need to make PostgreSQL
# listen on a non-local interface via the listen_addresses
# configuration parameter, or via the -i or -h command line switches.

# CAUTION: Configuring the system for local "trust" authentication
# allows any local user to connect as any PostgreSQL user, including
# the database superuser. If you do not trust all your local users,
# use another authentication method.

# TYPE   DATABASE     USER      ADDRESS         METHOD
#
# "local" is for Unix domain socket connections only
local  all        all            trust
# IPv4 local connections:
hostssl postgres    ravi      127.0.0.1/32  md5
hostssl all        all      0.0.0.0/0    md5
# IPv6 local connections:
host  all        all      ::1/128       trust
# Allow replication connections from localhost, by a user with the
# replication privilege.
local  replication all            trust
host  replication all      127.0.0.1/32  trust
host  replication all      ::1/128       trust
```

```
ravi@clientldp:/usr/local/pg12tde/data$ grep -i "ssl"
/usr/local/pg12tde/data/postgresql.conf
```

```
ravi@clientldp:/usr/local/pg12tde/data$ /usr/local/pg12tde/bin/pg_ctl -D
/usr/local/pg12tde/data/ restart
```

```
ravi@clientldp:/usr/local/pg12tde/data$ /usr/local/pg12tde/bin/pg_ctl -D /usr/local/pg12tde/data/ restart
waiting for server to shut down...2023-10-17 11:33:46.622 IST [4268] LOG: received fast shutdown request
2023-10-17 11:33:46.625 IST [4268] LOG: aborting any active transactions
2023-10-17 11:33:46.628 IST [4268] LOG: background worker "logical replication launcher" (PID 4280) exited with exit code 1
2023-10-17 11:33:46.631 IST [4275] LOG: shutting down
2023-10-17 11:33:46.655 IST [4268] LOG: database system is shut down
done
server stopped
2023-10-17 11:33:46.812 IST [4308] LOG: starting PostgreSQL 12.3_TDE_1.0 on x86_64-pc-linux-gnu, compiled by gcc (Ubuntu 9.4.0-1ubuntu1~20.04.2) 9.4.0, 64-bit
2023-10-17 11:33:46.813 IST [4308] LOG: listening on IPv4 address "127.0.0.1", port 5432
2023-10-17 11:33:46.821 IST [4308] LOG: listening on Unix socket "/tmp/.s.PGSQL.5432"
waiting for server to start...2023-10-17 11:33:46.859 IST [4313] LOG: database system was shut down at 2023-10-17 11:33:46 IST
2023-10-17 11:33:46.868 IST [4308] LOG: database system is ready to accept connections
done
server started
```

If ask password for user then

```
ravi@clientldp:/usr/local/pg12tde/data$ psql -U ravi -d postgres -h 127.0.0.1
psql (16.0 (Ubuntu 16.0-1.pgdg20.04+1), server 12.3_TDE_1.0)
SSL connection (protocol: TLSv1.3, cipher: TLS_AES_256_GCM_SHA384, compression: off)
Type "help" for help.

postgres=# ALTER USER ravi PASSWORD 'your_password';
ALTER ROLE
postgres=# ALTER USER ravi PASSWORD 'ravi';
ALTER ROLE
postgres=# \q
```

```
ravi@client1dp:/usr/local/pg12tde/data$ /usr/local/pg12tde/bin/pg_ctl -D /usr/local/pg12tde/data/ restart
waiting for server to shut down...2023-10-17 11:34:59.108 IST [4308] LOG: received fast shutdown request
.2023-10-17 11:34:59.111 IST [4308] LOG: aborting any active transactions
2023-10-17 11:34:59.114 IST [4308] LOG: background worker "logical replication launcher" (PID 4320) exited with exit code 1
2023-10-17 11:34:59.117 IST [4315] LOG: shutting down
2023-10-17 11:34:59.143 IST [4308] LOG: database system is shut down
done
server stopped
2023-10-17 11:34:59.231 IST [4339] LOG: starting PostgreSQL 12.3_TDE_1.0 on x86_64-pc-linux-gnu, compiled by gcc (Ubuntu 9.4.0-lubuntu1~20.04
.2) 9.4.0, 64-bit
2023-10-17 11:34:59.232 IST [4339] LOG: listening on IPv4 address "127.0.0.1", port 5432
2023-10-17 11:34:59.237 IST [4339] LOG: listening on Unix socket "/tmp/.s.PGSQL.5432"
waiting for server to start....2023-10-17 11:34:59.276 IST [4344] LOG: database system was shut down at 2023-10-17 11:34:59 IST
2023-10-17 11:34:59.288 IST [4339] LOG: database system is ready to accept connections
done
server started

postgres=# select * from pg_stat_ssl;
 pid | ssl | version | cipher | bits | compression | client_dn | client_serial | issuer_dn
----+---+-----+-----+-----+-----+-----+-----+-----+
 4349 | f |          |        |      |          |          |          |          |
 4351 | f |          |        |      |          |          |          |          |
 4354 | t | TLSv1.3 | TLS_AES_256_GCM_SHA384 | 256 |          |          |          |          |
 4347 | f |          |        |      |          |          |          |          |
 4346 | f |          |        |      |          |          |          |          |
 4348 | f |          |        |      |          |          |          |          |
(6 rows)

postgres=# \q
```

# MASKING

[https://gitlab.com/dalibo/postgresql\\_anonymizer/blob/master/docs/INSTALL.md](https://gitlab.com/dalibo/postgresql_anonymizer/blob/master/docs/INSTALL.md)

## Step1: Clone the git repository

```
[postgres@localhost ~]$ git clone https://gitlab.com/dalibo/postgresql_anonymizer.git
Cloning into 'postgresql_anonymizer'...
remote: Enumerating objects: 5748, done.
remote: Counting objects: 100% (299/299), done.
remote: Compressing objects: 100% (102/102), done.
remote: Total 5748 (delta 220), reused 246 (delta 194), pack-reused 5449
Receiving objects: 100% (5748/5748), 25.85 MiB | 9.35 MiB/s, done.
Resolving deltas: 100% (3733/3733), done.
[postgres@localhost ~]
```

```
ravi@clientldp:~/postde$ cd postde/
ravi@clientldp:~/postde$ ls

postgresql-12.3_TDE_1.0  postgresql-12.3_TDE_1.0.tar.gz
postgresql_anonymizer  provide_key.sh
ravi@clientldp:~/postde$ cd postgresql
```

## Step2: Build the source in postgres user

```
ravi@clientldp:~/postde/postgresql_anonymizer$ sudo make extension
PG_CONFIG=/usr/local/pg12tde/bin/pg_config
```

```
ravi@clientldp:~/postde/postgresql_anonymizer$ sudo make install
PG_CONFIG=/usr/local/pg12tde/bin/pg_config
```

```
ravi@clientldp:~/postde$ cd postgresql_anonymizer/
ravi@clientldp:~/postde/postgresql_anonymizer$ sudo make extension PG_CONFIG=/usr/local/pg12tde/bin/pg_config
cp anon.sql anon/anon--1.2.0.sql
cp data/*.csv anon/
ravi@clientldp:~/postde/postgresql_anonymizer$ sudo make install PG_CONFIG=/usr/local/pg12tde/bin/pg_config
cp anon.sql anon/anon--1.2.0.sql
cp data/*.csv anon/
/usr/bin/mkdir -p '/usr/local/pg12tde/share/postgresql/extension'
/usr/bin/mkdir -p '/usr/local/pg12tde/share/postgresql/extension/anon'
/usr/bin/mkdir -p '/usr/local/pg12tde/lib/postgresql'
install -d /usr/local/pg12tde/bin
install -m 0755 bin/pg_dump_anon.sh /usr/local/pg12tde/bin
/usr/bin/install -c -m 644 ./anon.control '/usr/local/pg12tde/share/postgresql/extension/'
/usr/bin/install -c -m 644 ./anon/* '/usr/local/pg12tde/share/postgresql/extension/anon/'
/usr/bin/install -c -m 755 anon.so '/usr/local/pg12tde/lib/postgresql/'
ravi@clientldp:~/postde/postgresql_anonymizer$ /usr/local/pg12tde/bin/pg_ctl -D /usr/local/pg12tde/data/ stop
waiting for server to shut down.... done
server stopped
```

```
ravi@clientldp:~/postde/postgresql_anonymizer$ sudo apt install
pgxnclient postgresql-server-dev-12
```

```
ravi@clientldp:~/postde/postgresql_anonymizer$ sudo apt install pgxnclient postgresql-server-dev-12
Reading package lists... Done
E Virtual Machine Manager tree
Reading state information... Done
pgxnclient is already the newest version (1.3.2-2.pgdg20.04+2).
postgresql-server-dev-12 is already the newest version (12.16-1.pgdg20.04+1).
postgresql-server-dev-12 set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

```
ravi@clientldp:~/postde/postgresql_anonymizer$ sudo pgxn install
postgresql_anonymizer
```

```
ravi@clientldp:~/postde/postgresql_anonymizer$ sudo pgxn install postgresql_anonymizer
INFO: best version: postgresql_anonymizer 1.1.0
INFO: saving /tmp/tmpuxzdi_u6/postgresql_anonymizer-1.1.0.zip
INFO: unpacking: /tmp/tmpuxzdi_u6/postgresql_anonymizer-1.1.0.zip
INFO: building extension
cp anon.sql anon/anon--1.1.0.sql
cp data/*.csv anon/
cp python/populate.py anon/
gcc -Wall -Wmissing-prototypes -Wpointer-arith -Wdeclaration-after-statement -Werror=vla -Wendif-labels -Wmissing-format-attribute
-Wimplicit-fallthrough=3 -Wcast-function-type -Wshadow=compatible-local -Wformat-security -fno-strict-aliasing -fwrapv -fexec
ss-precision=standard -Wno-format-truncation -Wno-string-truncation -g -O2 -fstack-protector-strong -Wformat -Wformat=
```

Start database

Step3: Restart the DB services

```
ravi@clientldp:~/postde/postgresql_anonymizer$
/usr/local/pg12tde/bin/pg_ctl -D /usr/local/pg12tde/data/ stop
```

```
ravi@clientldp:~/postde/postgresql_anonymizer$
/usr/local/pg12tde/bin/pg_ctl -D /usr/local/pg12tde/data/ start
```

```
ravi@clientldp:~/postde/postgresql_anonymizer$  
/usr/local/pg12tde/bin/pg_ctl -D /usr/local/pg12tde/data/ stop  
  
waiting for server to shut down.... done  
server stopped  
  
=====  
===  
  
ravi@clientldp:~/postde/postgresql_anonymizer$  
/usr/local/pg12tde/bin/pg_ctl -D /usr/local/pg12tde/data/ start  
  
2023-10-16 16:42:04.268 IST [1975] LOG:  starting PostgreSQL  
12.3_TDE_1.0 on x86_64-pc-linux-gnu, compiled by gcc (Ubuntu  
9.4.0-1ubuntu1~20.04.2) 9.4.0, 64-bit  
2023-10-16 16:42:04.268 IST [1975] LOG:  listening on IPv4 address  
"127.0.0.1", port 5432  
2023-10-16 16:42:04.275 IST [1975] LOG:  listening on Unix socket  
"/tmp/.s.PGSQL.5432"  
waiting for server to start....2023-10-16 16:42:04.317 IST [1980] LOG:  
database system was shut down at 2023-10-16 16:41:56 IST  
2023-10-16 16:42:04.328 IST [1975] LOG:  database system is ready to  
accept connections  
done  
server started
```

```
ravi@clientldp:~/postde/postgresql_anonymizer$ /usr/local/pg12tde/bin/pg_ctl -D /usr/local/pg12tde/data/ start  
2023-10-16 16:42:04.268 IST [1975] LOG:  starting PostgreSQL 12.3_TDE_1.0 on x86_64-pc-linux-gnu, compiled by gcc (Ubuntu 9.4.0-  
1ubuntu1~20.04.2) 9.4.0, 64-bit  
2023-10-16 16:42:04.268 IST [1975] LOG:  listening on IPv4 address "127.0.0.1", port 5432  
2023-10-16 16:42:04.275 IST [1975] LOG:  listening on Unix socket "/tmp/.s.PGSQL.5432"  
waiting for server to start....2023-10-16 16:42:04.317 IST [1980] LOG:  database system was shut down at 2023-10-16 16:41:56 IST  
2023-10-16 16:42:04.328 IST [1975] LOG:  database system is ready to accept connections  
done  
server started
```

#### Step 4 : Activate the dynamic masking engine

```
ravi@clientldp:~/postde/postgresql_anonymizer$ cd -  
/home/ravi/postde  
ravi@clientldp:~/postde$ /usr/local/pg12tde/bin/psql postgres  
psql (12.3_TDE_1.0)  
Type "help" for help.  
  
postgres=# CREATE EXTENSION IF NOT EXISTS anon CASCADE;  
NOTICE: installing required extension "pgcrypto"  
CREATE EXTENSION  
postgres=#
```

```
CREATE EXTENSION IF NOT EXISTS anon CASCADE;
```

```
SELECT anon.start_dynamic_masking();
```

```
postgres=# CREATE EXTENSION IF NOT EXISTS anon CASCADE;  
NOTICE: installing required extension "pgcrypto"  
CREATE EXTENSION  
postgres=# SELECT anon.start_dynamic_masking();  
 start_dynamic_masking  
-----  
 t  
(1 row)
```

```
ravi@clientldp:~$ psql -U ravi -d postgres -h localhost
```

```
postgres=# create database demo;
CREATE DATABASE

postgres=# \c demo
You are now connected to database "demo" as user "ravi".
demo=# create table tbl_demo(id serial primary key, name varchar, email
varchar, mobile character(10));
CREATE TABLE

demo=# INSERT INTO tbl_demo (name, email, mobile) VALUES
demo-#   ('demo1', 'demo1@demo.com', '1234567890'),
demo-#   ('demo2', 'demo2@demo.com', '1234567890');
INSERT 0 2
```

## STEP 5 : Declare a masked user

```
CREATE ROLE ext_user LOGIN;
```

```
postgres=# CREATE ROLE ext_user LOGIN;
CREATE ROLE
postgres=# SECURITY LABEL FOR anon ON ROLE ext_user IS 'MASKED';
SECURITY LABEL
```

```
ravi@clientldp:~$ psql -U ravi -d postgres -h localhost
psql (16.0 (Ubuntu 16.0-1.pgdg20.04+1), server 12.3_TDE_1.0)
Type "help" for help.

postgres=# \c demo
psql (16.0 (Ubuntu 16.0-1.pgdg20.04+1), server 12.3_TDE_1.0)
You are now connected to database "demo" as user "ravi".
demo=# select * from tbl_demo;
 id | name    |      email      |      mobile
----+-----+-----+-----+
  1 | demo1  | demo1@demo.com | 1234567890
  2 | demo2  | demo2@demo.com | 1234567890
(2 rows)

demo=# SECURITY LABEL FOR anon ON COLUMN tbl_demo.email IS 'MASKED WITH
FUNCTION anon.partial(email,2,$$*****$$,2)';
SECURITY LABEL
demo=# \q
ravi@clientldp:~$ psql -U ext_user -d demo -h localhost;
psql (16.0 (Ubuntu 16.0-1.pgdg20.04+1), server 12.3_TDE_1.0)
Type "help" for help.

demo=> select * from tbl_demo;
 id | name    |      email      |      mobile
----+-----+-----+-----+
  1 | demo1  | de*****om | 1234567890
  2 | demo2  | de*****om | 1234567890
(2 rows)

demo=> \q
```

```

psql (16.0 (Ubuntu 16.0-1.pgdg20.04+1), server 12.3_TDE_1.0)
You are now connected to database "demo" as user "ravi".
demo=#
demo=#
demo=# select * from tbl_demo;
 id | name      | email           | mobile
----+-----+-----+-----+
 1 | demo1    | demo1@demo.com | 1234567890
 2 | demo2    | demo2@demo.com | 1234567890
(2 rows)

demo=# SECURITY LABEL FOR anon ON COLUMN tbl_demo.mobile IS 'MASKED WITH
FUNCTION anon.partial(mobile,2,$$*****$$,2)';
SECURITY LABEL
demo=# \q
ravi@clientldp:~$ psql -U ext_user -d demo -h localhost;
psql (16.0 (Ubuntu 16.0-1.pgdg20.04+1), server 12.3_TDE_1.0)
Type "help" for help.

demo=> select * from tbl_demo;
 id | name      | email           | mobile
----+-----+-----+-----+
 1 | demo1    | de*****om     | 12*****90
 2 | demo2    | de*****om     | 12*****90
(2 rows)

```

## Uninstall

If you want to uninstall, then you can use the steps below.

**Step 1:** Remove all rules

```
SELECT anon.remove_masks_for_all_columns();
```

```
SELECT anon.remove_masks_for_all_roles();
```

THIS IS NOT MANDATORY ! It is possible to keep the masking rules inside the database schema even if the anon extension is removed !

**Step 2:** Drop the extension

```
DROP EXTENSION anon CASCADE;
```

**Step 3:** Unload the extension

```
ALTER DATABASE demo RESET session_preload_libraries;
```

# Using Vault in TOMCAT for Saving password defined in context.xml

1. Download the Tomcat of any version in which you want to configure the Vault if you have running tomcat. Please skip this step.

go to this link <https://dlcdn.apache.org/tomcat/tomcat-10/v10.1.14/bin/>

```
wget  
https://dlcdn.apache.org/tomcat/tomcat-10/v10.1.14/bin/apache-tomcat-10.  
1.14.tar.gz
```

 apache-tomcat-10.1.14.tar.gz 2023-10-09 22:15 12M

```
ravi@clientldp:~$ wget https://dlcdn.apache.org/tomcat/tomcat-10/v10.1.14/bin/apache-tomcat-10.1.14.tar.gz  
--2023-10-17 13:00:33-- https://dlcdn.apache.org/tomcat/tomcat-10/v10.1.14/bin/apache-tomcat-10.1.14.tar.gz  
Resolving dlcdn.apache.org (dlcdn.apache.org)... 151.101.2.132, 2a04:4e42:644  
Connecting to dlcdn.apache.org (dlcdn.apache.org)|151.101.2.132|:443... connected.  
HTTP request sent, awaiting response... 200 OK  
Length: 12408053 (12M) [application/x-gzip]  
Saving to: 'apache-tomcat-10.1.14.tar.gz'  
  
apache-tomcat-10.1.14.tar.gz 100%[=====] 11.83M 699KB/s in 48s  
2023-10-17 13:01:22 (251 KB/s) - 'apache-tomcat-10.1.14.tar.gz' saved [12408053/12408053]
```

```
ravi@clientldp:~$ tar -xvf apache-tomcat-10.1.14.tar.gz  
apache-tomcat-10.1.14/conf/  
apache-tomcat-10.1.14/conf/catalina.policy  
apache-tomcat-10.1.14/conf/catalina.properties  
apache-tomcat-10.1.14/conf/context.xml  
apache-tomcat-10.1.14/conf/jaspic-providers.xml  
apache-tomcat-10.1.14/conf/iaspic-providers.xsd
```

```
ravi@clientldp:~$ ls  
'$_'\004' apache-tomcat-10.1.14-src.zip Documents Music provide_key.sh server.crt Templates  
389ds apache-tomcat-10.1.14.tar.gz Downloads Pictures provide_key.sh_ server.key Videos  
apache-tomcat-10.1.14 Desktop ldaptest.sh postde Public snap  
ravi@clientldp:~$
```

```
ravi@clientldp:~/apache-tomcat-10.1.14/bin$ sh startup.sh  
Neither the JAVA_HOME nor the JRE_HOME environment variable is defined  
At least one of these environment variable is needed to run this program
```

```
sudo apt update  
sudo apt install openjdk-11-jdk
```

```
ravi@client1dp:~/apache-tomcat-10.1.14/bin$ sudo apt install openjdk-11-jdk
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  ca-certificates-java fonts-dejavu-extra java-common libatk-wrapper-java libatk-wrapper-java-jni libice-dev
  libpthread-stubs0-dev libsm-dev libx11-dev libxau-dev libxcb1-dev libxdmcp-dev libxt-dev openjdk-11-jdk-headless
  openjdk-11-jre openjdk-11-jre-headless x11proto-core-dev x11proto-dev xorg-sgml-doctools xtrans-dev
Suggested packages:
```

```
ravi@clientldp:~/apache-tomcat-10.1.14/bin$ sh startup.sh
```

```
ravi@client1dp:~/apache-tomcat-10.1.14/bin$ sh startup.sh
Using CATALINA_BASE:   /home/ravi/apache-tomcat-10.1.14
Using CATALINA_HOME:   /home/ravi/apache-tomcat-10.1.14
Using CATALINA_TMPDIR: /home/ravi/apache-tomcat-10.1.14/temp
Using JRE_HOME:        /usr
Using CLASSPATH:       /home/ravi/apache-tomcat-10.1.14/bin/bootstrap.jar:/home/ravi/apache-tomcat-10.1.14/bin/tomcat-juli.jar
Using CATALINA_OPTS:
Tomcat started.
```

## 2. Configure Vault in Tomcat.

```
git clone https://github.com/web-servers/tomcat-vault.git
```

```
ravi@clientldp:~$ git clone https://github.com/web-servers/tomcat-vault.git
Cloning into 'tomcat-vault'...
remote: Enumerating objects: 1469, done.
remote: Counting objects: 100% (109/109), done.
remote: Compressing objects: 100% (61/61), done.
remote: Total 1469 (delta 25), reused 79 (delta 14), pack-reused 1360
Receiving objects: 100% (1469/1469), 17.88 MiB | 2.76 MiB/s, done.
Resolving deltas: 100% (490/490), done.
```

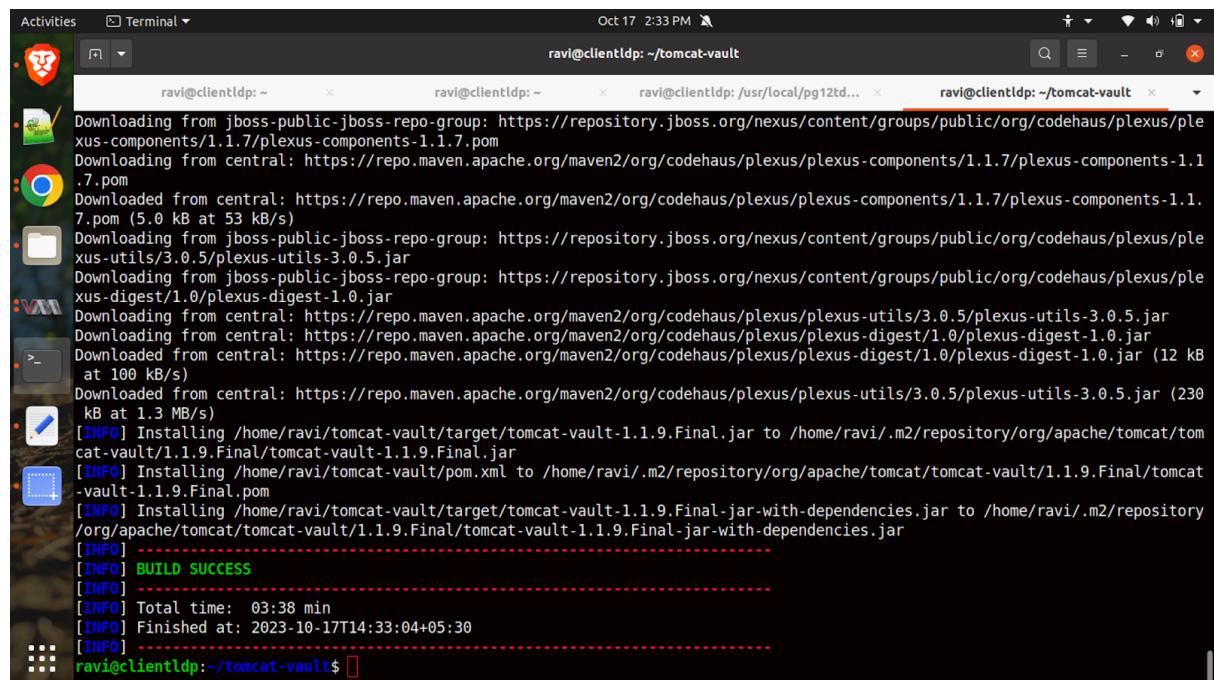
```
ravi@clientlbp:~$ ls  
'`$!004'  
389ds  
apache-tomcat-10.1.14  
apache-tomcat-10.1.14-src.zip  
apache-tomcat-10.1.14.tar.gz  
Desktop  
Documents  
Downloads  
Pictures  
provide_key.sh  
provide_key.sh_  
server.crt  
server.key  
Templates  
tomcat-vault  
daptest.sh  
postde  
Public  
snap  
Videos  
ravi@clientlbp:~$ cd
```

```
cd tomcat-vault  
ravi@clientldp:~/tomcat-vault$ ls -lrh
```

```
ravi@clientlbp:~$ ls
'..' '004' apache-tomcat-10.1.14-src.zip Documents Music provide_key.sh server.crt Templates
389ds apache-tomcat-10.1.14.tar.gz Downloads Pictures provide_key.sh_ server.key tomcat-vault
apache-tomcat-10.1.14 Desktop ldaptest.sh postde Public snap Videos
ravi@clientlbp:~$ cd tomcat-vault/
ravi@clientlbp:~/tomcat-vault$ ls
bin examples INSTALL.md LICENSE pom.xml README.md src Using_Crypt.md
ravi@clientlbp:~/tomcat-vault$ ls -lrth
total 44K
-rw-rw-r-- 1 ravi ravi 12K Oct 17 13:22 LICENSE
-rw-rw-r-- 1 ravi ravi 3.7K Oct 17 13:22 INSTALL.md
-rw-rw-r-- 1 ravi ravi 3.3K Oct 17 13:22 Using_Crypt.md
-rw-rw-r-- 1 ravi ravi 724 Oct 17 13:22 README.md
drwxrwxr-x 2 ravi ravi 4.0K Oct 17 13:22 bin
drwxrwxr-x 4 ravi ravi 4.0K Oct 17 13:22 examples
drwxrwxr-x 3 ravi ravi 4.0K Oct 17 13:22 src
-rw-rw-r-- 1 ravi ravi 5.1K Oct 17 13:22 pom.xml
ravi@clientlbp:~/tomcat-vault$
```

```
ravi@clientldp:~/tomcat-vault$ maven clean install
```

```
avi@clientdp:~/tomcat-vault$ mvn clean install
WARNING: An illegal reflective access operation has occurred
WARNING: Illegal reflective access by com.google.inject.internal.cglib.core.$ReflectUtils$1 (file:/usr/share/maven/lib/guice.jar
) to method java.lang.ClassLoader.defineClass(java.lang.String,byte[],int,int,java.security.ProtectionDomain)
WARNING: Please consider reporting this to the maintainers of com.google.inject.internal.cglib.core.$ReflectUtils$1
WARNING: Use --illegal-access=warn to enable warnings of further illegal reflective access operations
WARNING: All illegal access operations will be denied in a future release
[INFO] Scanning for projects...
[INFO]
[INFO] -----< org.apache.tomcat:tomcat-vault >-----
[INFO] Building Vault extension for Apache Tomcat 1.1.9.Final
[INFO] ----- [ jar ] -----
downloading from jboss-public-jboss-repo-group: https://repository.jboss.org/nexus/content/groups/public/org/apache/maven/plugin/maven-clean-plugin/3.0.0/maven-clean-plugin-3.0.0.pom
downloading from central: https://repo.maven.apache.org/maven2/org/apache/maven/plugins/maven-clean-plugin/3.0.0/maven-clean-plu
```



```
ravi@clientldp:~/tomcat-vault$ cd target
ravi@clientldp:~/tomcat-vault/target$ ls -lrth

ravi@clientldp:~/tomcat-vault$ ls
bin examples INSTALL.md lib LICENSE pom.xml README.md src target Using_Crypt.md
ravi@clientldp:~/tomcat-vault$ cd target/
ravi@clientldp:~/tomcat-vault/target$ ls
antrun      classes      maven-archiver  tomcat-vault-1.1.9.Final.jar
archive-tmp  generated-sources  maven-status  tomcat-vault-1.1.9.Final-jar-with-dependencies.jar
ravi@clientldp:~/tomcat-vault/target$
```

```
ravi@clientldp:~/tomcat-vault/target$ ls -lrth
total 340K
drwxrwxr-x 3 ravi ravi 4.0K Oct 17 14:30 classes
drwxrwxr-x 3 ravi ravi 4.0K Oct 17 14:31 maven-status
drwxrwxr-x 3 ravi ravi 4.0K Oct 17 14:31 generated-sources
drwxrwxr-x 2 ravi ravi 4.0K Oct 17 14:32 maven-archiver
-rw-rw-r-- 1 ravi ravi 70K Oct 17 14:32 tomcat-vault-1.1.9.Final.jar
drwxrwxr-x 2 ravi ravi 4.0K Oct 17 14:32 archive-tmp
-rw-rw-r-- 1 ravi ravi 244K Oct 17 14:32 tomcat-vault-1.1.9.Final-jar-with-dependencies.jar
drwxrwxr-x 2 ravi ravi 4.0K Oct 17 14:33 antrun
```

```
ravi@clientldp:~/tomcat-vault$ cd
ravi@clientldp:~$ cd apache-tomcat-10.1.14/
ravi@clientldp:~/apache-tomcat-10.1.14$ ls
bin      conf      lib      logs      README.md      RUNNING.txt  webapps
BUILDING.txt  CONTRIBUTING.md  LICENSE  NOTICE  RELEASE-NOTES  temp      work
ravi@clientldp:~/apache-tomcat-10.1.14$ cd lib/
ravi@clientldp:~/apache-tomcat-10.1.14/lib$ ls
annotations-api.jar      jakartaee-migration-1.0.7-shaded.jar  tomcat-i18n-cs.jar      tomcat-jdbc.jar
catalina-ant.jar          jasper-el.jar                  tomcat-i18n-de.jar      tomcat-jni.jar
catalina-ha.jar           jasper.jar                  tomcat-i18n-es.jar      tomcat-util.jar
catalina.jar              jaspic-api.jar                tomcat-i18n-fr.jar      tomcat-util-scan.jar
catalina-ssi.jar          jsp-api.jar                  tomcat-i18n-ja.jar      tomcat-websocket.jar
catalina-storeconfig.jar  servlet-api.jar              tomcat-i18n-ko.jar      websocket-api.jar
catalina-tribes.jar       tomcat-api.jar                tomcat-i18n-pt-BR.jar   websocket-client-api.jar
ecj-4.27.jar              tomcat-coyote.jar            tomcat-i18n-ru.jar
el-api.jar                tomcat-dbcp.jar              tomcat-i18n-zh-CN.jar
ravi@clientldp:~/apache-tomcat-10.1.14/lib$ cd
ravi@clientldp:~/tomcat-vault
```

```
ravi@clientldp:~/tomcat-vault$ cp lib/tomcat-vault.jar
~/apache-tomcat-10.1.14/lib
```

```
ravi@clientldp:~/apache-tomcat-10.1.14/lib$ ls -lrth
```

```
ravi@clientldp:~/apache-tomcat-10.1.14/lib$ ls -lrth
total 11M
-rw-r---- 1 ravi ravi 31K Oct 10 02:31 websocket-client-api.jar
-rw-r---- 1 ravi ravi 15K Oct 10 02:31 websocket-api.jar
-rw-r---- 1 ravi ravi 236K Oct 10 02:31 tomcat-websocket.jar
-rw-r---- 1 ravi ravi 224K Oct 10 02:31 tomcat-util-scan.jar
-rw-r---- 1 ravi ravi 206K Oct 10 02:31 tomcat-util.jar
-rw-r---- 1 ravi ravi 16K Oct 10 02:31 tomcat-jni.jar
-rw-r---- 1 ravi ravi 147K Oct 10 02:31 tomcat-jdbc.jar
-rw-r---- 1 ravi ravi 173K Oct 10 02:31 tomcat-i18n-zh-CN.jar
-rw-r---- 1 ravi ravi 62K Oct 10 02:31 tomcat-i18n-ru.jar
-rw-r---- 1 ravi ravi 51K Oct 10 02:31 tomcat-i18n-pt-BR.jar
-rw-r---- 1 ravi ravi 189K Oct 10 02:31 tomcat-i18n-ko.jar
-rw-r---- 1 ravi ravi 189K Oct 10 02:31 tomcat-i18n-ja.jar
-rw-r---- 1 ravi ravi 167K Oct 10 02:31 tomcat-i18n-fr.jar
-rw-r---- 1 ravi ravi 102K Oct 10 02:31 tomcat-i18n-es.jar
-rw-r---- 1 ravi ravi 76K Oct 10 02:31 tomcat-i18n-de.jar
-rw-r---- 1 ravi ravi 67K Oct 10 02:31 tomcat-i18n-cs.jar
-rw-r---- 1 ravi ravi 330K Oct 10 02:31 tomcat-dbcp.jar
-rw-r---- 1 ravi ravi 869K Oct 10 02:31 tomcat-coyote.jar
-rw-r---- 1 ravi ravi 12K Oct 10 02:31 tomcat-api.jar
-rw-r---- 1 ravi ravi 358K Oct 10 02:31 servlet-api.jar
-rw-r---- 1 ravi ravi 76K Oct 10 02:31 jsp-api.jar
-rw-r---- 1 ravi ravi 28K Oct 10 02:31 jaspic-api.jar
-rw-r---- 1 ravi ravi 557K Oct 10 02:31 jasper.jar
-rw-r---- 1 ravi ravi 169K Oct 10 02:31 jasper-el.jar
-rw-r---- 1 ravi ravi 776K Oct 10 02:31 jakartaee-migration-1.0.7-shaded.jar
-rw-r---- 1 ravi ravi 88K Oct 10 02:31 el-api.jar
-rw-r---- 1 ravi ravi 3.1M Oct 10 02:31 ecj-4.27.jar
-rw-r---- 1 ravi ravi 318K Oct 10 02:31 catalina-tribes.jar
-rw-r---- 1 ravi ravi 78K Oct 10 02:31 catalina-storeconfig.jar
-rw-r---- 1 ravi ravi 63K Oct 10 02:31 catalina-ssi.jar
-rw-r---- 1 ravi ravi 1.7M Oct 10 02:31 catalina.jar
-rw-r---- 1 ravi ravi 123K Oct 10 02:31 catalina-ha.jar
-rw-r---- 1 ravi ravi 55K Oct 10 02:31 catalina-ant.jar
-rw-r---- 1 ravi ravi 14K Oct 10 02:31 annotations-api.jar
-rw-rw-r-- 1 ravi ravi 244K Oct 17 14:51 tomcat-vault.jar
ravi@clientldp:~/apache-tomcat-10.1.14/lib$
```

```
ravi@clientldp:~/apache-tomcat-10.1.14$ ls
bin          conf        lib      logs      README.md      RUNNING.txt  webapps
BUILDING.txt  CONTRIBUTING.md  LICENSE  NOTICE  RELEASE-NOTES  temp        work
ravi@clientldp:~/apache-tomcat-10.1.14$ cd conf/
ravi@clientldp:~/apache-tomcat-10.1.14/conf$ ls
catalina      catalina.properties  jaspic-providers.xml  logging.properties  tomcat-users.xml  web.xml
catalina.policy  context.xml       jaspic-providers.xsd  server.xml           tomcat-users.xsd
ravi@clientldp:~/apache-tomcat-10.1.14/conf$ vim catalina.properties
ravi@clientldp:~/apache-tomcat-10.1.14/conf$ vim catalina.properties
```

```
ravi@clientldp:~/apache-tomcat-10.1.14$ cd conf/
ravi@clientldp:~/apache-tomcat-10.1.14/conf$ vim catalina.properties
```

```
Activities Terminal Oct 17 3:03 PM ravi@clientldp: ~/apache-tomcat-10.1.14/conf
ravi@clientldp: ~ ravi@clientldp: ~ ravi@clientldp: /usr/local/pg12td... ravi@clientldp: ~/apache-tomcat-...
xmlParserAPIs.jar,\xom-*.jar
# Default list of JAR files that should be scanned that overrides the default
# jarsToSkip list above. This is typically used to include a specific JAR that
# has been excluded by a broad file name pattern in the jarsToSkip list.
# The list of JARs to scan may be over-ridden at a Context level for individual
# scan types by configuring a JarScanner with a nested JarScanFilter.
tomcat.util.scan.StandardJarScanFilter.jarsToScan=
log4j-taglib*.jar,\
log4j-jakarta-web*.jar,\
log4javascrip*.jar,\
slf4j-taglib*.jar
# String cache configuration.
tomcat.util.buf.StringCache.byte.enabled=true
#tomcat.util.buf.StringCache.char.enabled=true
#tomcat.util.buf.StringCache.trainThreshold=500000
#tomcat.util.buf.StringCache.cacheSize=5000
# Disable use of some privilege blocks Tomcat doesn't need since calls to the
# code in question are always already inside a privilege block
org.apache.el.GET_CLASSLOADER_USE_PRIVILEGED=false
#org.apache.tomcat.util.digester.PROPERTY_SOURCE=org.apache.tomcat.vault.util.PropertySourceVault
#####added extra line for tomcat vault
org.apache.tomcat.util.digester.PROPERTY_SOURCE=org.apache.tomcat.vault.util.PropertySourceVault
org.apache.tomcat.util.digester.REPLACE_SYSTEM_PROPERTIES=true
"catalina.properties" 226L, 7991C
226,38 Bot
```

```
#####added extra line for tomcat vault
org.apache.tomcat.util.digester.PROPERTY_SOURCE=org.apache.tomcat.vault.util.PropertySourceVault
org.apache.tomcat.util.digester.REPLACE_SYSTEM_PROPERTIES=true
226,38 Bot
```

```
ravi@clientldp:~/apache-tomcat-10.1.14/conf$ cd
ravi@clientldp:~$ cd /tmp

ravi@clientldp:~$ cd /tmp
ravi@clientldp:/tmp$ ls
hsperfdata_ravi
hsperfdata_root
snap-private-tmp
systemd-private-dbd3b012413740f9920cefcfd32ab8741-colord.service-qqM6ah
systemd-private-dbd3b012413740f9920cefcfd32ab8741-fwupd.service-xGclxg
systemd-private-dbd3b012413740f9920cefcfd32ab8741-ModemManager.service-pUuTe
systemd-private-dbd3b012413740f9920cefcfd32ab8741-spice-vdagentd.service-67kZki
systemd-private-dbd3b012413740f9920cefcfd32ab8741-switcheroo-control.service-gRuNTh
systemd-private-dbd3b012413740f9920cefcfd32ab8741-systemd-logind.service-JRFAui
systemd-private-dbd3b012413740f9920cefcfd32ab8741-systemd-resolved.service-Cy0t6i
systemd-private-dbd3b012413740f9920cefcfd32ab8741-systemd-timesyncd.service-AI6Wbi
systemd-private-dbd3b012413740f9920cefcfd32ab8741-upower.service-uIguoj
tracker-extract-files.1000
tracker-extract-files.125

ravi@clientldp:/tmp$ mkdir vault
ravi@clientldp:/tmp$ cd vault/
```

```
ravi@clientldp:/tmp/vault$ keytool -gensecretkey -keystore
/tmp/vault/vault.keystore -alias my_vault -storetype jceks -keyalg AES
-keysiz 128 -storepass my_password123 -keypass my_password123 -validity
730
```

```
ravi@clientldp:~/tmp$ mkdir vault
ravi@clientldp:~/tmp$ cd vault/
ravi@clientldp:~/tmp/vault$ ls
ravi@clientldp:~/tmp/vault$ keytool -genkey -keystore /tmp/vault/vault.keystore -alias my_vault -storetype jceks -keyalg AES -keysize 128 -storepass my_password123 -keypass my_password123 -validity 730

Warning:
The JCEKS keystore uses a proprietary format. It is recommended to migrate to PKCS12 which is an industry standard format using "keytool -importkeystore -srckeystore /tmp/vault/vault.keystore -destkeystore /tmp/vault/vault.keystore -deststoretype pkcs12".
```

```
ravi@clientldp:~$ cd apache-tomcat-10.1.14/
ravi@clientldp:~/apache-tomcat-10.1.14$ ls
bin BUILDING.txt conf CONTRIBUTING.md lib LICENSE logs NOTICE README.md RELEASE-NOTES RUNNING.txt temp webapps work
ravi@clientldp:~/apache-tomcat-10.1.14$ cd conf
ravi@clientldp:~/apache-tomcat-10.1.14/conf$ ls
Catalina catalina.properties jaspic-providers.xml logging.properties tomcat-users.xml web.xml
catalina.policy context.xml jaspic-providers.xsd server.xml tomcat-users.xsd
ravi@clientldp:~/apache-tomcat-10.1.14/conf$ touch vault.properties

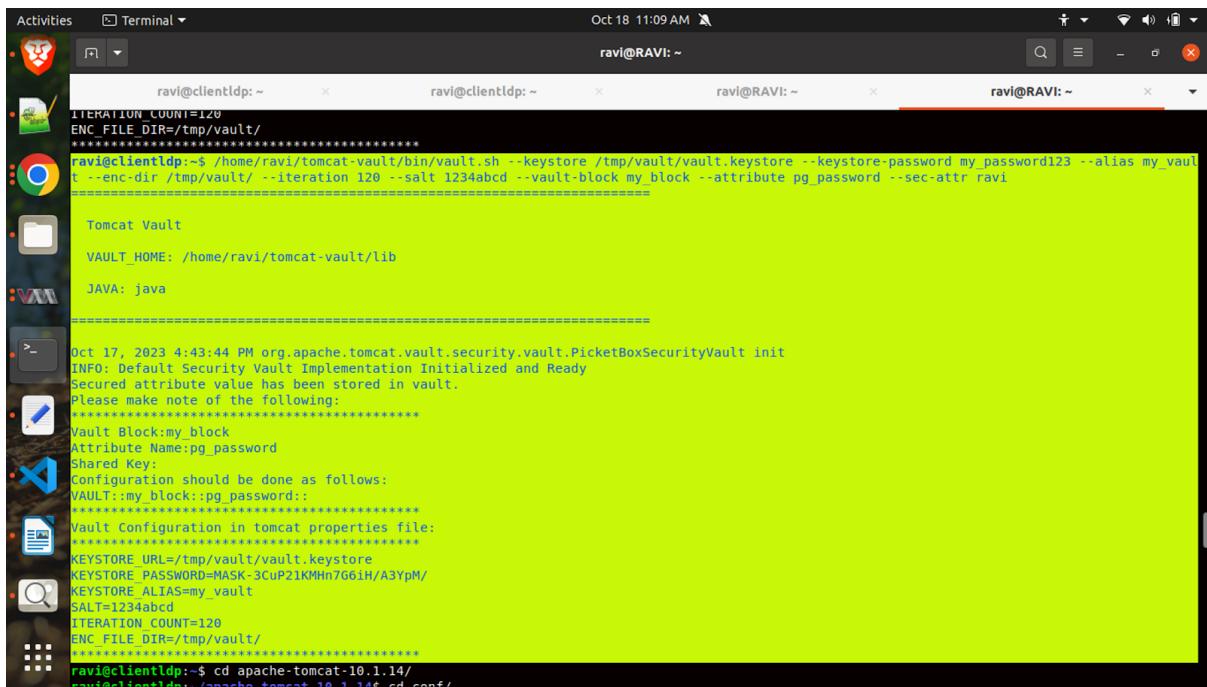
**

ravi@clientldp:~/tomcat-vault/bin$ /home/ravi/tomcat-vault/bin/vault.sh --keystore /tmp/vault/vault.keystore --keystore-password my_password123 --alias my_vault --enc-dir /tmp/vault/ --iteration 44 --salt 1234abcd -g /home/ravi/apache-tomcat-10.1.14/conf/vault.properties
=====
Tomcat Vault
VAULT_HOME: /home/ravi/tomcat-vault/lib
JAVA: java
=====

Oct 17, 2023 3:14:59 PM org.apache.tomcat.vault.security.vault.PicketBoxSecurityVault init
INFO: Default Security Vault Implementation Initialized and Ready
Vault Configuration in tomcat properties file:
*****
KEYSTORE_URL=/tmp/vault/vault.keystore
KEYSTORE_PASSWORD=MASK-3q5QEqp8X.LABR77t4LnDI
KEYSTORE_ALIAS=my_vault
SALT=1234abcd
ITERATION_COUNT=44
ENC_FILE_DIR=/tmp/vault/
*****
```

```
ravi@clientldp:~$ /home/ravi/tomcat-vault/bin/vault.sh --keystore
/tmp/vault/vault.keystore --keystore-password my_password123 --alias
my_vault --enc-dir /tmp/vault/ --iteration 120 --salt 1234abcd
--vault-block my_block --attribute pg_password --sec-attr ravi
```

# RAVI IS PASSWORD OF POSTGRES DATABASE



```
ravi@clientldp: ~          ravi@clientldp: ~          ravi@RAVI: ~          ravi@RAVI: ~
ITERATION_COUNT=120
ENC_FILE_DIR=/tmp/vault/
*****
ravi@clientldp:~$ /home/ravi/tomcat-vault/bin/vault.sh --keystore /tmp/vault/keystore --keystore-password my_password123 --alias my_vault --enc-dir /tmp/vault/ --iteration 120 --salt 1234abcd --vault-block my_block --attribute pg_password --sec-attr ravi
*****
Tomcat Vault
VAULT_HOME: /home/ravi/tomcat-vault/lib
JAVA: java
*****
Oct 17, 2023 4:43:44 PM org.apache.tomcat.vault.security.vault.PicketBoxSecurityVault init
INFO: Default Security Vault Implementation Initialized and Ready
Secured attribute value has been stored in vault.
Please make note of the following:
*****
Vault Block:my_block
Attribute Name:pg_password
Shared Key:
Configuration should be done as follows:
VAULT::my_block::pg_password:
*****
Vault Configuration in tomcat properties file:
*****
KEYSTORE_URL=/tmp/vault/vault.keystore
KEYSTORE_PASSWORD=MASK-3CuP21KMHn7G61H/A3YpM/
KEYSTORE_ALIAS=my_vault
SALT=1234abcd
ITERATION_COUNT=120
ENC_FILE_DIR=/tmp/vault/
*****
ravi@clientldp:~$ cd apache-tomcat-10.1.14/
ravi@clientldp:~/apache-tomcat-10.1.14$ cd conf/
```

code of tomcat to maven

```
ravi@clientldp:~$ mkdir tomtest
ravi@clientldp:~$ cd tomtest/
ravi@clientldp:~/tomtest$ git clone
https://github.com/IsuruX98/Basic-Java-CRUD
```

```
ravi@clientldp:~/tomtest$ ls
Basic-Java-CRUD generate.sh java-crud-webapp
ravi@clientldp:~/tomtest$ cd java-crud-webapp/
ravi@clientldp:~/tomtest/java-crud-webapp$ ls
pom.xml src
ravi@clientldp:~/tomtest/java-crud-webapp$ vim pom.xml
ravi@clientldp:~/tomtest/java-crud-webapp$ rsync -avz /home/ravi/tomtest/Basic-Java-CRUD/signup/src/ /home/keen/tomtest/java-crud-webapp/src/
sending incremental file list
rsync: mkdir "/home/keen/tomtest/java-crud-webapp/src" failed: No such file or directory (2)
rsync error: error in file IO (code 11) at main.c(679) [Receiver=3.1.3]
ravi@clientldp:~/tomtest/java-crud-webapp$ rsync -avz /home/ravi/tomtest/Basic-Java-CRUD/signup/src/ /home/ravi/tomtest/java-crud-webapp/src/
sending incremental file list
./
main/
main/java/
main/java/registration/
main/java/registration/DBConnect.java
main/java/registration/LoginServletNew.java
```

```
ravi@clientldp:~/tomtest/java-crud-webapp$ ls
pom.xml  src
ravi@clientldp:~/tomtest/java-crud-webapp$ cd src
ravi@clientldp:~/tomtest/java-crud-webapp/src$ ls
main
ravi@clientldp:~/tomtest/java-crud-webapp/src$ cd main/
ravi@clientldp:~/tomtest/java-crud-webapp/src/main$ ls
java  resources  webapp
ravi@clientldp:~/tomtest/java-crud-webapp/src/main$ cd java/
ravi@clientldp:~/tomtest/java-crud-webapp/src/main/java$ ls
registration
ravi@clientldp:~/tomtest/java-crud-webapp/src/main/java$ cd registration/
ravi@clientldp:~/tomtest/java-crud-webapp/src/main/java/registration$ ls
DBConnect.java          LoginServletNew.java  RegistrationServlet.java  User.java
deleteuserServlet.java  logoutservlet.java   UpdateUserServlet.java  UsersDBUtil.java
ravi@clientldp:~/tomtest/java-crud-webapp/src/main/java/registration$ vim DBConnect.java
```

```
ravi@clientldp:~/tomtest/java-crud-webapp/src/main/java/registration$ cat DBConnect.java
package registration;

import java.sql.Connection;
import java.sql.DriverManager;
import java.sql.SQLException;

public class DBConnect {

    public static Connection getConnection() {
        String url = "jdbc:postgresql://10.163.32.214:5432/postgres"; // PostgreSQL URL, change port if necessary
        String username = "ravi"; // Your PostgreSQL username
        String password = "ravi"; // Your PostgreSQL password
        Connection con = null;

        try {
            Class.forName("org.postgresql.Driver"); // Use PostgreSQL JDBC Driver
            con = DriverManager.getConnection(url, username, password);
            System.out.println("Connection successful"); // Print success message
        } catch (ClassNotFoundException e) {
            System.out.println("Failed to load PostgreSQL JDBC Driver!");
            e.printStackTrace();
        } catch (SQLException e) {
            System.out.println("Database connection failed!");
            e.printStackTrace();
        }

        return con;
    }
}
```

```
ravi@clientldp:~$ psql -U ravi -d postgres -h localhost
Password for user ravi:
psql (16.0 (Ubuntu 16.0-1.pgdg20.04+1), server 12.3_TDE_1.0)
SSL connection (protocol: TLSv1.3, cipher: TLS_AES_256_GCM_SHA384, compression: off)
Type "help" for help.
```

```
postgres=#  
postgres=#
```

```
postgres=# CREATE TABLE users(userid serial NOT NULL ,uname VARCHAR(50) NOT NULL,upwd VARCHAR(60) NOT NULL,uemail VARCHAR(30) NOT NULL,umobile VARCHAR(10) NOT NULL, type VARCHAR(5) NOT NULL DEFAULT 'user', PRIMARY KEY(userid));
CREATE TABLE
postgres=#
```

```
ravi@clientldp:~$ cd /usr/local/
ravi@clientldp:/usr/local$ ls
bin etc games include lib man pg12tde postgres sbin share src
ravi@clientldp:/usr/local$ cd postgres/
ravi@clientldp:/usr/local/postgres$ ls
ravi@clientldp:/usr/local/postgres$ cd ..
ravi@clientldp:/usr/local$ cd pg12tde/
ravi@clientldp:/usr/local/pg12tde$ ls
bin data include lib share
ravi@clientldp:/usr/local/pg12tde$ cd data/
ravi@clientldp:/usr/local/pg12tde/data$ ls
base pg_hba.conf pg_notify pg_stat pg_twophase postgresql.auto.conf server.crt
global pg_ident.conf pg_replslot pg_stat_tmp PG_VERSION postgresql.conf server.key
pg_commit_ts pg_logical pg_serial pg_subtrans pg_wal postmaster.opts
pg_dynshmem pg_multixact pg_snapshots pg_tblspc pg_xact postmaster.pid
ravi@clientldp:/usr/local/pg12tde/data$ vim pg_hba.conf
ravi@clientldp:/usr/local/pg12tde/data$ ^C
ravi@clientldp:/usr/local/pg12tde/data$
```

#	TYPE	DATABASE	USER	ADDRESS	METHOD
# "local" is for Unix domain socket connections only					
local	all		all		trust
# IPv4 local connections:					
host	all		all	127.0.0.1/32	trust
host	all		all	10.163.32.214/24	trust
# IPv6 local connections:					
host	all		all	::1/128	trust
# Allow replication connections from localhost, by a user with the					
# replication privilege.					
local	replication		all		trust
host	replication		all	127.0.0.1/32	trust
host	replication		all	::1/128	trust
"no_hba.conf" 941 . 4584C					

```
ravi@clientldp:/usr/local/pg12tde/data$ psql -U ravi -d postgres -h localhost
psql (16.0 (Ubuntu 16.0-1.pgdg20.04+1), server 12.3_TDE_1.0)
SSL connection (protocol: TLSv1.3, cipher: TLS_AES_256_GCM_SHA384, compression: off)
Type "help" for help.

postgres=# \q
```

```

#-----#
# CONNECTIONS AND AUTHENTICATION
#-----#

# - Connection Settings -

listen_addresses = '*'          # what IP address(es) to listen on;
                                # comma-separated list of address
                                # defaults to 'localhost'; use '*'
                                # (change requires restart)
port = 5432                      # (change requires restart)
max_connections = 100           # (change requires restart)
#superuser_reserved_connections = 3 # (change requires restart)
#unix_socket_directories = '/tmp' # comma-separated list of directo

```

```

ravi@clientldp:/usr/local/pgl2tde/data$ /usr/local/pgl2tde/bin/pg_ctl -D /usr/local/pgl2tde/data/ restart
waiting for server to shut down....2023-10-18 14:11:47.191 IST [3769] LOG:  received fast shutdown request
2023-10-18 14:11:47.194 IST [3769] LOG:  aborting any active transactions
2023-10-18 14:11:47.210 IST [3769] LOG:  background worker "logical replication launcher" (PID 3780) exited with exit code 1
2023-10-18 14:11:47.216 IST [3775] LOG:  shutting down
2023-10-18 14:11:47.240 IST [3769] LOG:  database system is shut down
done
server stopped
2023-10-18 14:11:47.355 IST [3981] LOG:  starting PostgreSQL 12.3_TDE_1.0 on x86_64-pc-linux-gnu, compiled by gcc (Ubuntu 9.4.0
.2) 9.4.0, 64-bit
2023-10-18 14:11:47.356 IST [3981] LOG:  listening on IPv4 address "0.0.0.0", port 5432
2023-10-18 14:11:47.356 IST [3981] LOG:  listening on IPv6 address "::", port 5432
2023-10-18 14:11:47.360 IST [3981] LOG:  listening on Unix socket "/tmp/.PGSQL.5432"
waiting for server to start....2023-10-18 14:11:47.399 IST [3986] LOG:  database system was shut down at 2023-10-18 14:11:47 IS
2023-10-18 14:11:47.413 IST [3981] LOG:  database system is ready to accept connections
done
server started

```

```

ravi@clientldp:/usr/local/pgl2tde/data$ psql -U ravi -d postgres -h 10.163.32.214
psql (16.0 (Ubuntu 16.0-1.pgdg20.04+1), server 12.3_TDE 1.0)
SSL connection (protocol: TLSv1.3, cipher: TLS_AES_256_GCM_SHA384, compression: off)
Type "help" for help.

postgres=# select * from users;
 userid | uname | upwd | uemail      | umobile | type
-----+-----+-----+-----+-----+
      1 | ravi | ravi | ravi@gmail.com | 1929228 | user
(1 row)

postgres=# \q

```

```

ravi@clientldp:~/apache-tomcat-10.1.14/bin$ sh shutdown.sh
ravi@clientldp:~/apache-tomcat-10.1.14/bin$ sh startup.sh

```

<http://10.163.32.214:8080/java-crud-webapp/login.jsp>

Activities Google Chrome Oct 18 2:35 PM

10.163.32.214:8080/java-crud-webapp/login.jsp

Apps Gmail YouTube current bookm Google Docs share python machine learn... JOB APPLY postgres All Bookmarks

## sign in



Your Name

Password

Remember me

**Log in**

[Create an account](#) Or login with   

Activities Google Chrome Oct 18 2:42 PM

Not secure | 10.163.32.214:8080/java-crud-webapp/registration.jsp

Apps Gmail YouTube current bookm Google Docs share python machine learn... JOB APPLY postgres All Bookmarks

## Sign up



ravil23

rsr@gmail.com

....

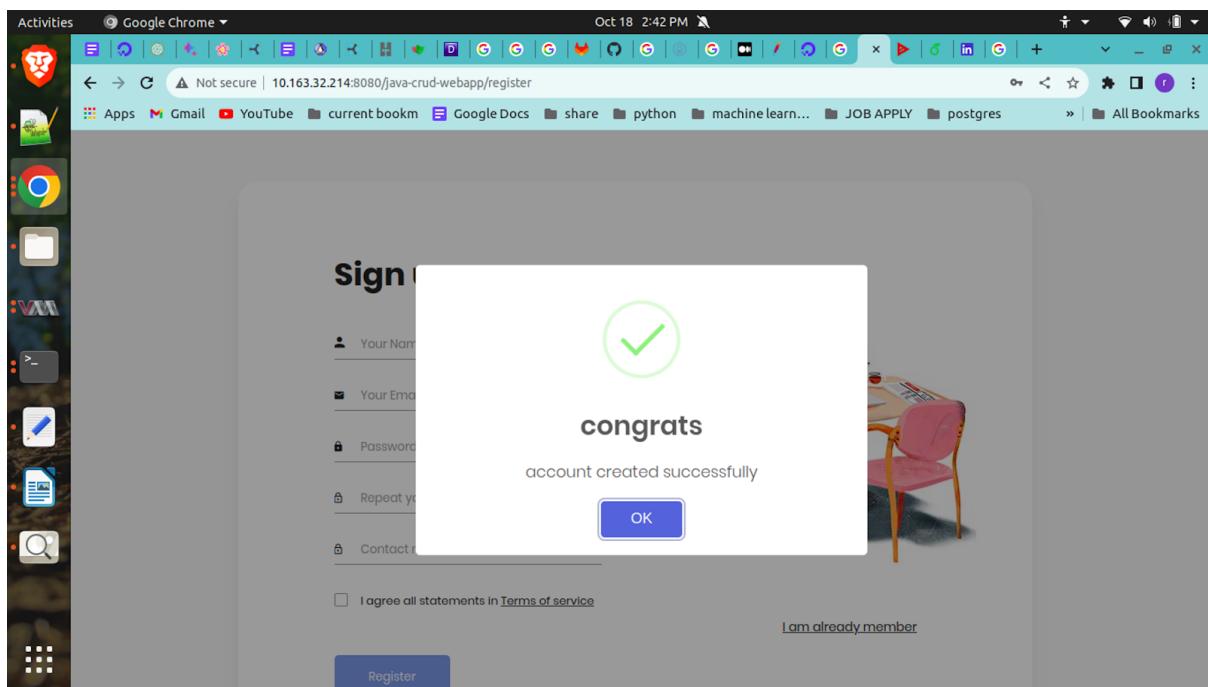
....

23456789

I agree all statements in [Terms of service](#)

[I am already member](#)

**Register**



```
ravi@clientldp:/usr/local/pg12tde/data$ psql -U ravi -d postgres -h 10.163.32.214
psql (16.0 (Ubuntu 16.0-1.pgdg20.04+1), server 12.3_TDE_1.0)
SSL connection (protocol: TLSv1.3, cipher: TLS_AES_256_GCM_SHA384, compression: off)
Type "help" for help.

postgres=# select * from users;
 userid |  uname   | upwd    |     uemail      | umobile | type
-----+-----+-----+-----+-----+-----+
      1 | ravi    | ravi   | ravi@gmail.com | 1929228 | user
      2 | ravi123 | ravi   | rsr@gmail.com  | 23456789 | user
(2 rows)

postgres=#
```