PostgreSQL hardening

Hardening PostgreSQL is essential for improving security and minimizing vulnerabilities.

1. File System-Level Security

Restrict PostgreSQL Data Directory Permissions

Ensure that only the PostgreSQL user (postgres) can access the data directory:

```
chown -R postgres:postgres /data/postgres_16
chmod 700 /data/postgres_16
```

Explanation:

1. chown -R postgres:postgres /data/postgres_16 → Ensures PostgreSQL owns the directory.
2. chmod 700 /data/postgres_16 → Grants read, write, and execute permissions only to PostgreSQL.

---

2. Secure PostgreSQL Configuration

Modify postgresql.conf

Edit the configuration file:

```
vi /data/postgres_16/postgresql.conf
```

Update the following settings:

```
listen_addresses = 'local-host, 192.168.1.100'          # Replace with your actual IP
ssl = on
password_encryption = scram-sha-256
log_connections = on
log_disconnections = on
log_hostname = on
```

Explanation:

- listen_addresses → Restricts connections to specific IPs.
- ssl = on → Enables SSL for secure connections.
- password_encryption = scram-sha-256 → Enforces secure password hashing.
- log_connections, log_disconnections, log_host-name → Helps in monitoring login activity.

Restart PostgreSQL for changes to take effect:

```
systemctl restart postgresql-16
```

---

3. Restrict Client Authentication (pg_hba.conf)

Edit the authentication configuration file:

```
vi /data/postgres_16/pg_hba.conf
```

Set secure authentication methods:

```
# TYPE  DATABASE   USER   ADDRESS        METHOD
host    all        all    127.0.0.1/32    scram-sha-256
host    all        all    192.168.1.0/24  scram-sha-256
```

Explanation:

- scram-sha-256 → More secure than MD5 or trust-based authentication.
- Limits access to only trusted networks.

Reload PostgreSQL configuration:

```
systemctl reload postgresql-16
```

---

4. Secure PostgreSQL Users and Roles

Enforce Strong Password Policy

Run the following SQL commands inside psql:

```
ALTER USER postgres WITH PASSWORD 'Strong@P@ssword';
```

Explanation:

Use strong passwords with uppercase, lowercase, numbers, and special characters.

Restrict Superuser Access

List all superusers:

```
SELECT usename FROM pg_user WHERE usesuper = true;
```

Revoke unnecessary superuser privileges:

```
ALTER USER user_name NOSUPERUSER;
```

---

5. Enable Logging and Auditing

Modify postgresql.conf to enable logging:

```
logging_collector = on
log_directory = '/var/log/postgresql'
log_filename = 'postgresql-%Y-%m-%d.log'
log_statement = 'all'
```

Explanation:

- logging_collector = on → Enables log collection.
- log_statement = 'all' → Logs all queries executed.

Reload PostgreSQL:

```
systemctl reload postgresql-16
```

---

6. Secure Network Connections

Enable SSL/TLS

Generate SSL certificates:

```
openssl req -new -x509 -days 365 -nodes -out /var/lib/pgsql/server.crt -keyout
/var/lib/pgsql/server.key
chmod 600 /var/lib/pgsql/server.key
chown postgres:postgres /var/lib/pgsql/server.*
```

Modify postgresql.conf:

```
ssl_cert_file = '/var/lib/pgsql/server.crt'
ssl_key_file = '/var/lib/pgsql/server.key'
```

Restart PostgreSQL:

```
systemctl restart postgresql-16
```

---

7. Disable Remote Superuser Login

Edit postgresql.conf:

```
superuser_reserved_connections = 0
```

- To enhance security, especially in production environments, **set it to** 0 to prevent remote superusers from connecting unless absolutely necessary:

Restart PostgreSQL:

```
systemctl restart postgresql-16
```

---

8. Keep PostgreSQL Updated

Check for available updates:

```
dnf check-update postgresql16-server
```

Upgrade if necessary:

```
dnf update postgresql16-server -y
```

---

9. Backup and Disaster Recovery

Enable automatic backups using pg_basebackup:

```
pg_basebackup -D /backup -Ft -z -P -U postgres
```

Schedule backups with cron:

```
crontab -e
```

Add the following entry (runs every midnight):

```
0 0 * * * /usr/bin/pg_basebackup -D /backup -Ft -z -P -U postgres
```

Explanation:

- pg_basebackup -D /backup -Ft -z -P -U postgres → Takes a compressed full backup.
- Cron job ensures daily automated backups.