PostgreSQL Installation Worksheet

IT 120 - Databases

Kit Transue

Contents

Installation Worksheet

pgAdmin

pgAdmin uses a password to protect the passwords it manages in its keychain. You will need these each time you use pgAdmin.

keychain password:

pgAdmin host (localhost):

pgAdmin user (defaults to you):

When you first use pgAdmin to connect to a database server or database, it will ask for some of the server/database information that follows. It will keep this in its keychain so you can connect more quickly in the future.

PostgreSQL server

Each server instance has:

Host: (default: localhost)

Port (default: 5432):

OS username for server

Each server runs as an OS user:

User that runs server (usually "postgres"):
Operating system password for user (on *NIX, this is usually unknown; use sudo):

Database users

Each server maintains its own “database users” table. All connections to the database need to be authorized by this table. These “users” are independent of the user accounts managed by the OS.

Superuser The database superuser bypasses all permissions checks. When the installation sets up the OS user to run the server, it creates a database user with a matching name and password. (Note the OS password and database password could diverge.)

Avoid using the superuser account. If it is the only account, it must be used to create the first non-superuser, but otherwise it should not be needed. And because it operates without restrictions, it is permitted to alter tables that would corrupt the database.

Trust

The database may be configured so that logged-in users on the OS may be automatically authenticated as database users without needing a password. This is called “trust.”

Trust can simplify development. It also can make scripting safer, because the operating system manages authentication (and supports secure, passwordless authentication like ssh keys) and there is no need to expose passwords in scripts.

There are two kinds of trust:

- ident: the OS user may act as a database user with the same usernames
- trust: the OS user may act as any database user (useful for an administrator, or for a developer setting up or testing users/roles)

There is not an admin command to change trust. The server must be stopped, its pg_hba.conf file changed, and the server restarted.

“Trust” recommended for non-critical development servers.

- Modified conf to allow local ident
- Modified conf to allow local trust

Users

Regular users are prevented from doing damage to database internals. They may be given administrative privileges to create/remove databases, users, and roles. All work should be done as a regular user.

The database tools default to trying the user's login name as the default for the database user. For development work, creating a database user with the same name as the developer's system account is strongly recommended:

createuser -d with username that matches the developer's system login

Non-superuser database user:

The user should have the "CREATEDB" role.

If trust is not configured, this user will need a password.

Database User password:

(Note that database passwords are not as well-protected as system passwords, and should be different from the user's OS account password. This password protects database data, which during development should not be critical or sensitive.)

Databases

Each database hosted on the server will have the following

Hosting server:

Database name:
Owner:

If you are managing the connection in pgAdmin, it will want to know how you connect to it:

User for connecting:

The password will be stored per user (not per database) in the pgAdmin keychain.