## Authentication:

This database uses role-based authentication. All access is authenticated using username/password or API tokens, and the default access is encrypted with TLS, which means that data in transit is secure.

## Role/Privileges:

The default user is a superuser. Other users need roles and privileges explicitly granted.

## Permissions:

By default, users have no access to objects unless granted. No access is given to sensitive tables unless explicitly granted via GRANT.

## Network Security:

This database enforces secure access over HTTPS or the encrypted PostgreSQL wire protocol. Access is limited by the project connection string – other IPs cannot access your DB arbitrarily.