Access Control

PostgreSQL Version

Peter Chapin

Vermont Technical College

Overview

- These slides mostly refer to the PostgreSQL documentation.
  - They just organize the subject for purposes of presentation and review
- Some additional information is also included.

General Concepts

- “Authorization” (Access Control)
  - *What* can a principal do once they are authenticated (logged in).
- Principal
  - An entity that acts on objects in the system (user, process, etc.)
- Privilege
  - An action that can be perform
- Object
  - An entity that is acted upon

Jill reads afile.txt

Permissions

- A *permission* is a triple of (principle, privilege, object).
  - (Jill, READ, afile.txt) Allows the action on the previous slide to succeed.
- Listing all permissions is tedious so there are ways to simplify that
  - Permission Inheritance: permissions on a parent object inherit into the children
  - Groups: A set of principals are treated as a single principle
  - Roles: Similar to groups except (typically) there is a concept of "role activation" and role inheritance
- Negative permissions (Jill, **cannot** READ, afile.txt)?
  - Problematic. Not usually provided.

Owners

- In most systems objects have owners (principals that “control” the object).
- In most systems there is a special administrative user (or role or group) that can control every object without being the owner.
- Owners can create and remove permissions for others
- Owners can change ownership (thereby losing control over the object)

What About PostgreSQL?

- PostgreSQL: Documentation: 14: Chapter 21. Database Roles
- PostgreSQL: Documentation: 14: 5.7. Privileges
- PostgreSQL: Documentation: 14: CREATE FUNCTION (on writing SECURITY DEFINER functions properly)