Separation of Duties

User, Schema, and Service Account Definitions and How PostgreSQL Solves the Problem

Richard Stephan

Senior Database Administrator

NYISO

Database Accounts

- Users
  - Database Administrators
  - Configuration Management
  - Developers
  - Quality Assurance
  - Power Users or Report Writers
- System – Application Components
  - Schema Owner
  - Application Accounts
  - Database owner (i.e., postgres)

Account Management

- Account Profiles
  - Password complexity
  - Account expiration
  - Failed attempt lock outs
- Database Privileges
  - DBA, CM, QA, Dev, App
- Auditing Activity
- Limiting or Eliminating Shared Accounts

Application Example

- DBA User – pstewart
- CM User – lburton
- QA User – msirtis
- Dev User – wwheaton
- Schema – ncc1701d
- Object Owner Role – ncc1701d
- Application Pooled User - ltcdrdata

pg_hba.conf

```
# TYPE       DATABASE       USER         CIDR-ADDRESS       METHOD
local        all            postgres                        trust
hostssl      enterprod      all          10.50.0.0/16       ldap "ldap://corp-
   ad.company.com/OU=Standard Users,DC=corp-
   ad,DC=company,DC=com;CN=;,OU=Standard Users,DC=corp-
   ad,DC=company,DC=com"
hostssl      enterprod      all          10.10.1.0/24    md5
hostssl      enterprod      all          10.20.1.0/24    md5
```