Esri International User Conference | San Diego, CA

Technical Workshops | 14.07.11

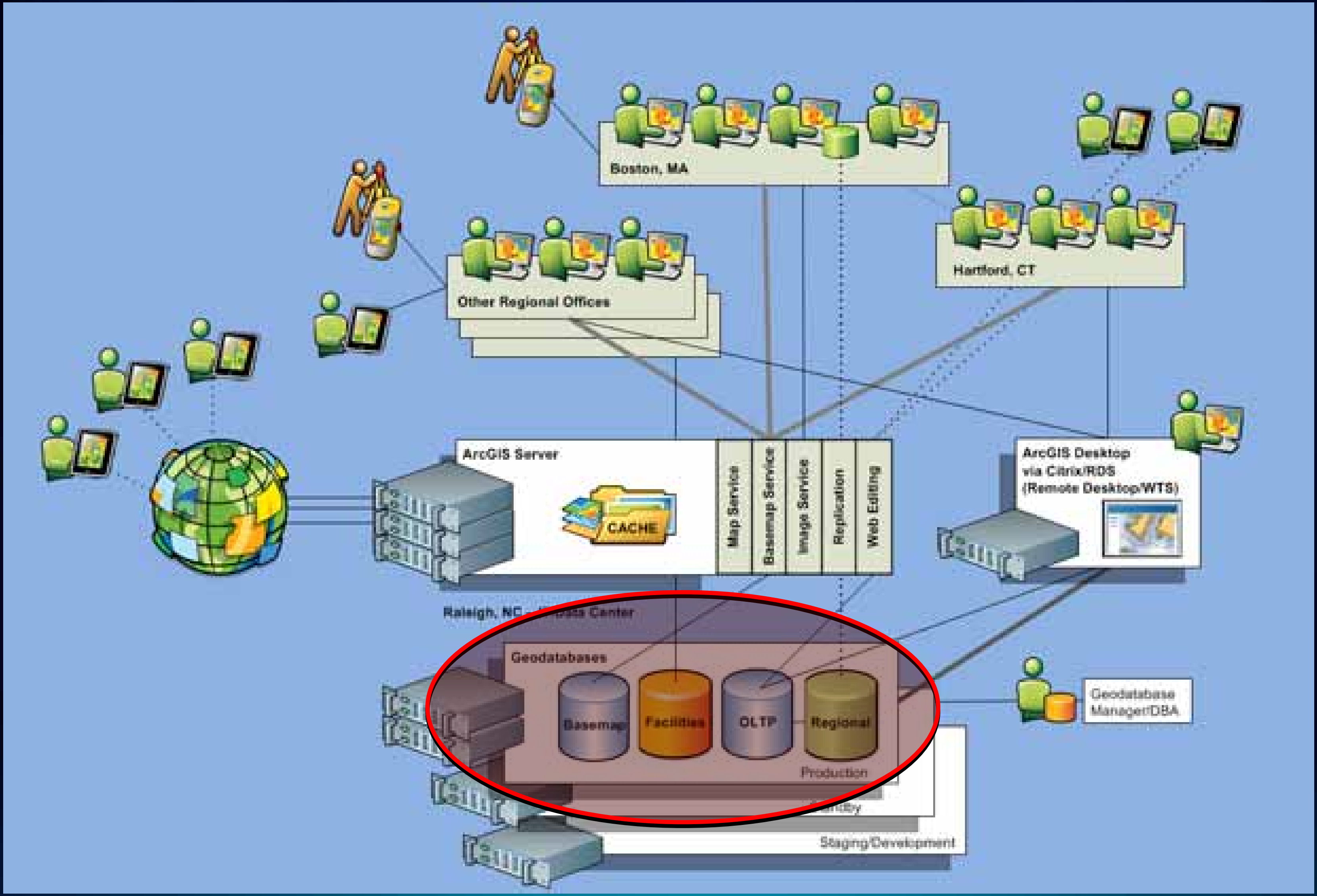
# Implementing Database Roles in the Enterprise Geodatababse

Jim McAbee

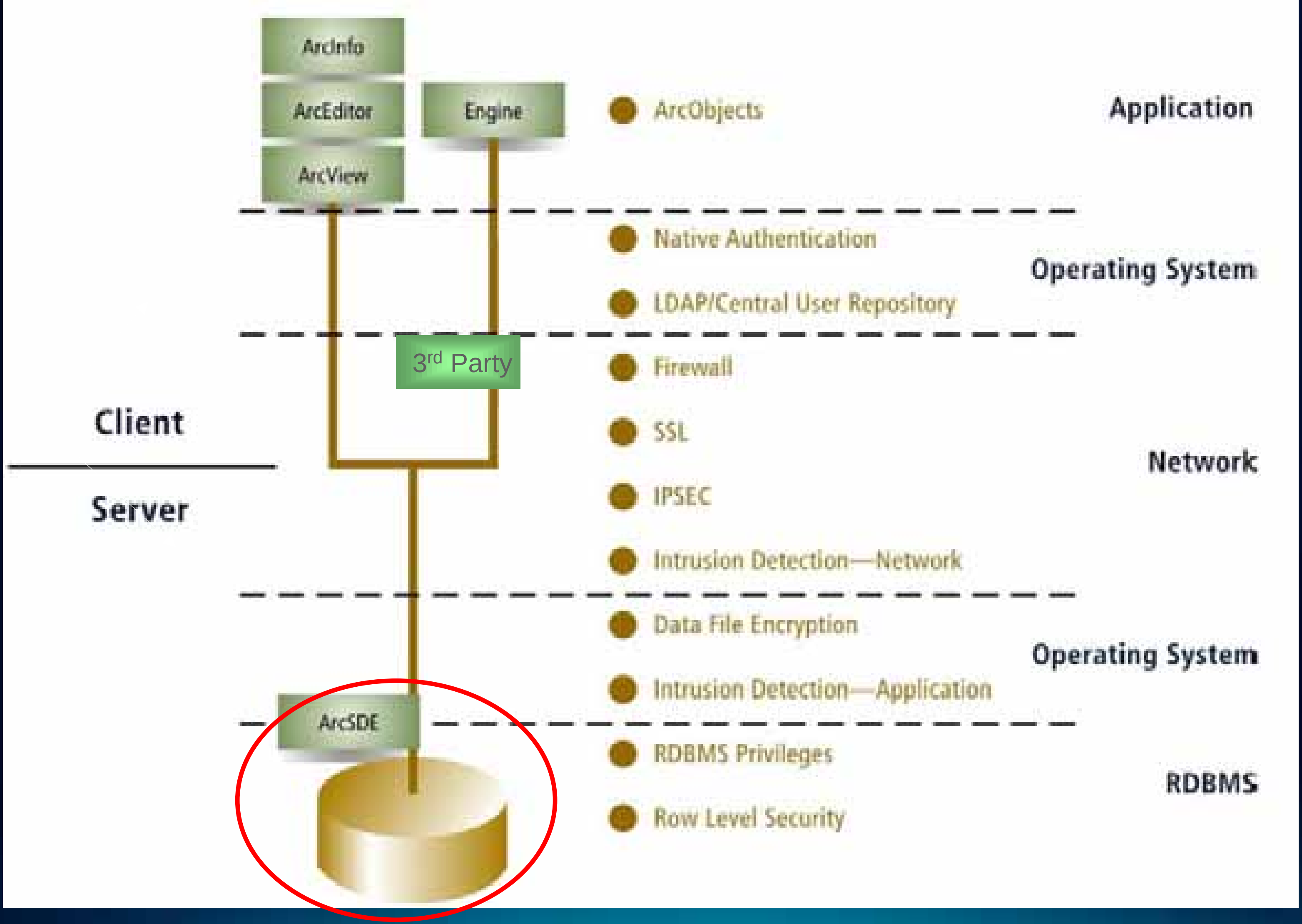
# Agenda

- Roles Overview
- Roles and OS Groups
- RDBMS Differences
- Privilege Assignment Hiearchy

# Geodatabase Security



# IT Security – Many Levels



# Authentication Methods and Authorization

- Authentication vs. Authorization
  - Authentication – “who is allowed in”
    *“Authentication is the process by which a system verifies a user's identity”*
  - Authorization or Privileges – “what they can do”
    *“Authorization indicates which database operations that user can perform, and which data objects that user can access and/or manipulate.”*

- Authentication Methods
  - Database
  - External – Local OS, Domain, other (e.g. LDAP, etc..)
    - Cross-OS possible typically but complex

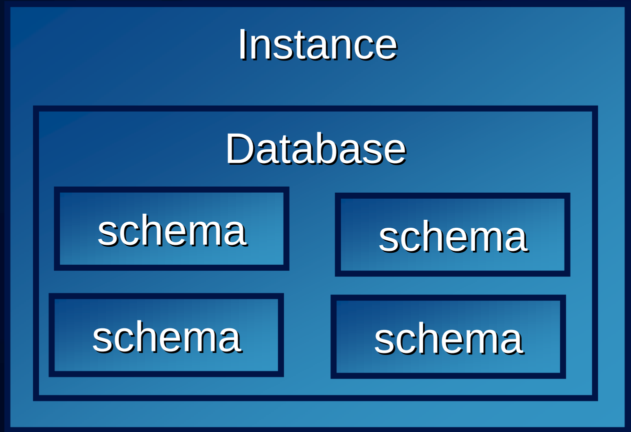
- Authorization or Privileges
  - Object Creation (DDL – Data Definition)
  - Object Manipulation (DML – Data Manipulation)

# Users - Considerations

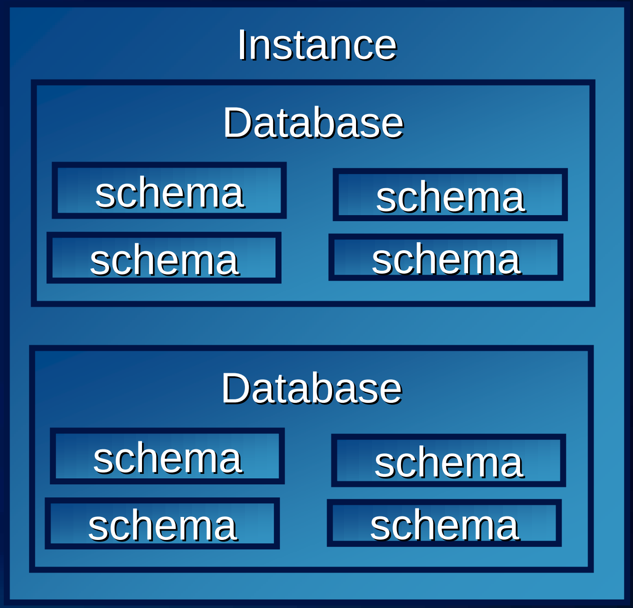
- User Types
  - System
  - General vs. Specific (“head-less” vs. employee)
    - Editor, Viewer (service specific?), Departmental, Operations, etc.…
- System Roles
  - Public
  - other
- Locked/Unlocked accounts
  - inactivity
- Password Timeout
  - automatic
  - organization policy
- User or Role based resource management
  - space, cpu, etc…

# Database Architecture and Authorization Differences

- Single vs. Multiple Database per Instance Architectures
- Instance vs. Database level privileges and roles



Oracle



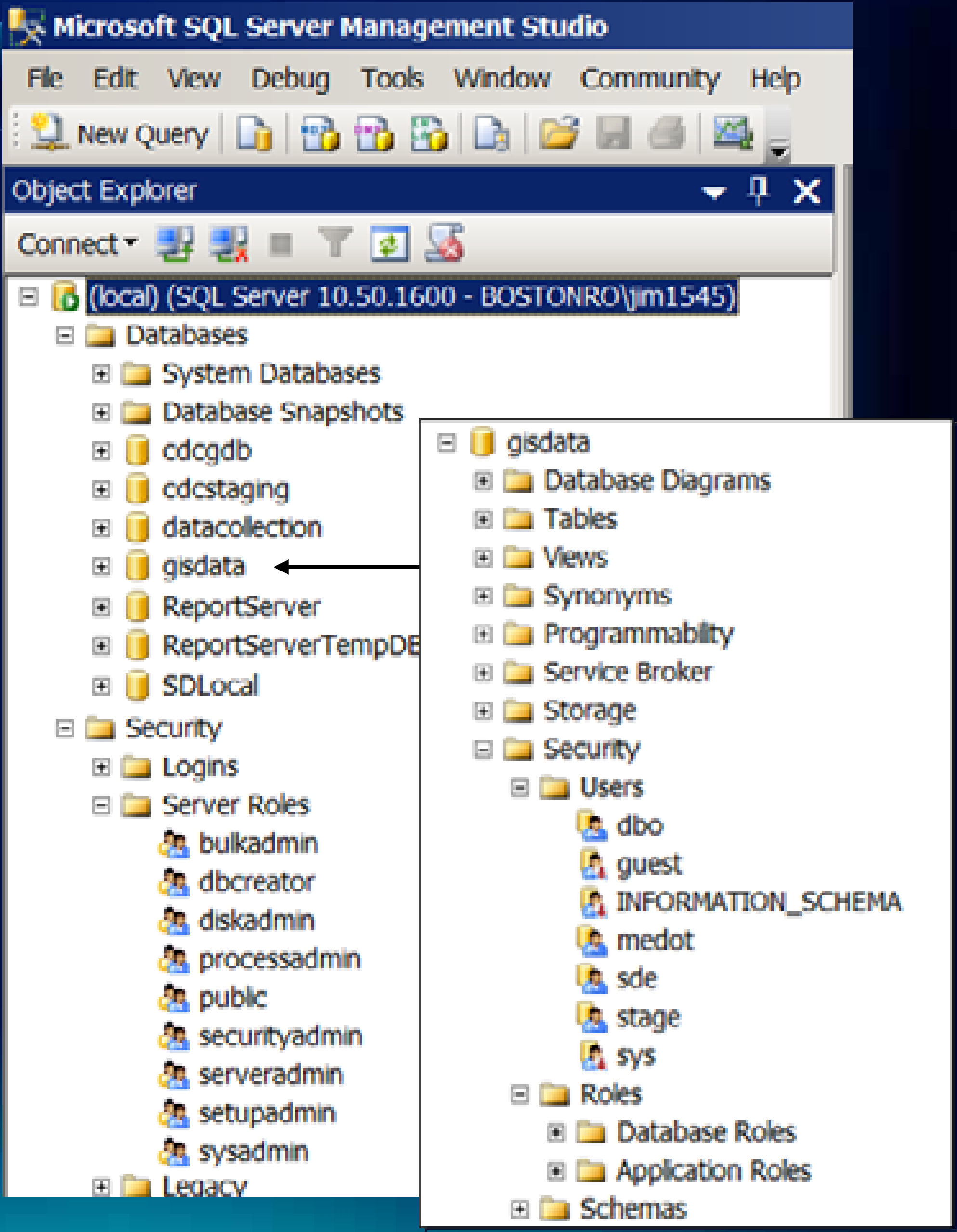
SQL Server, DB2, Postgres

# Roles Overview

- Managing and controlling privileges is easier when you use roles, which are named groups of related privileges that you grant as a group to users or other roles.
- Roles facilitate the granting of multiple privilges or roles to users.
- Similar to groups in the operating system.
- Privileges can be granted explicitely to a user or via a role

# Types of Roles

- Instance vs. Database level

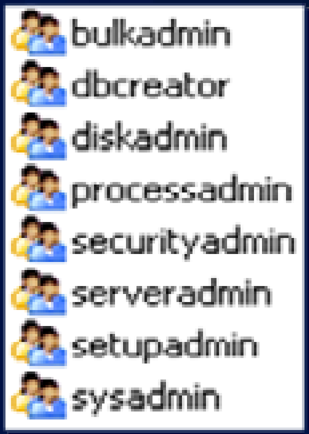


# Various types of Roles

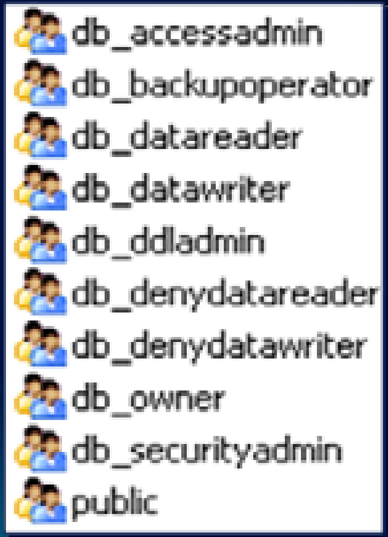
- Application
  - type of application
  - application resource usage – load
- Functional
  - editors vs. viewers
- Departmental
  - water vs. planning, new york vs. california

# SQL Server example: Fixed roles

- Many RDBMS have predefined roles used to simplify administration
- SQL Server Fixed server roles
  - Used to manage instance level permissions
  - sysadmin has full administrative privileges
- SQL Server Fixed database roles
  - Used to manage database level permissions
  - Create user-defined roles for more flexibility

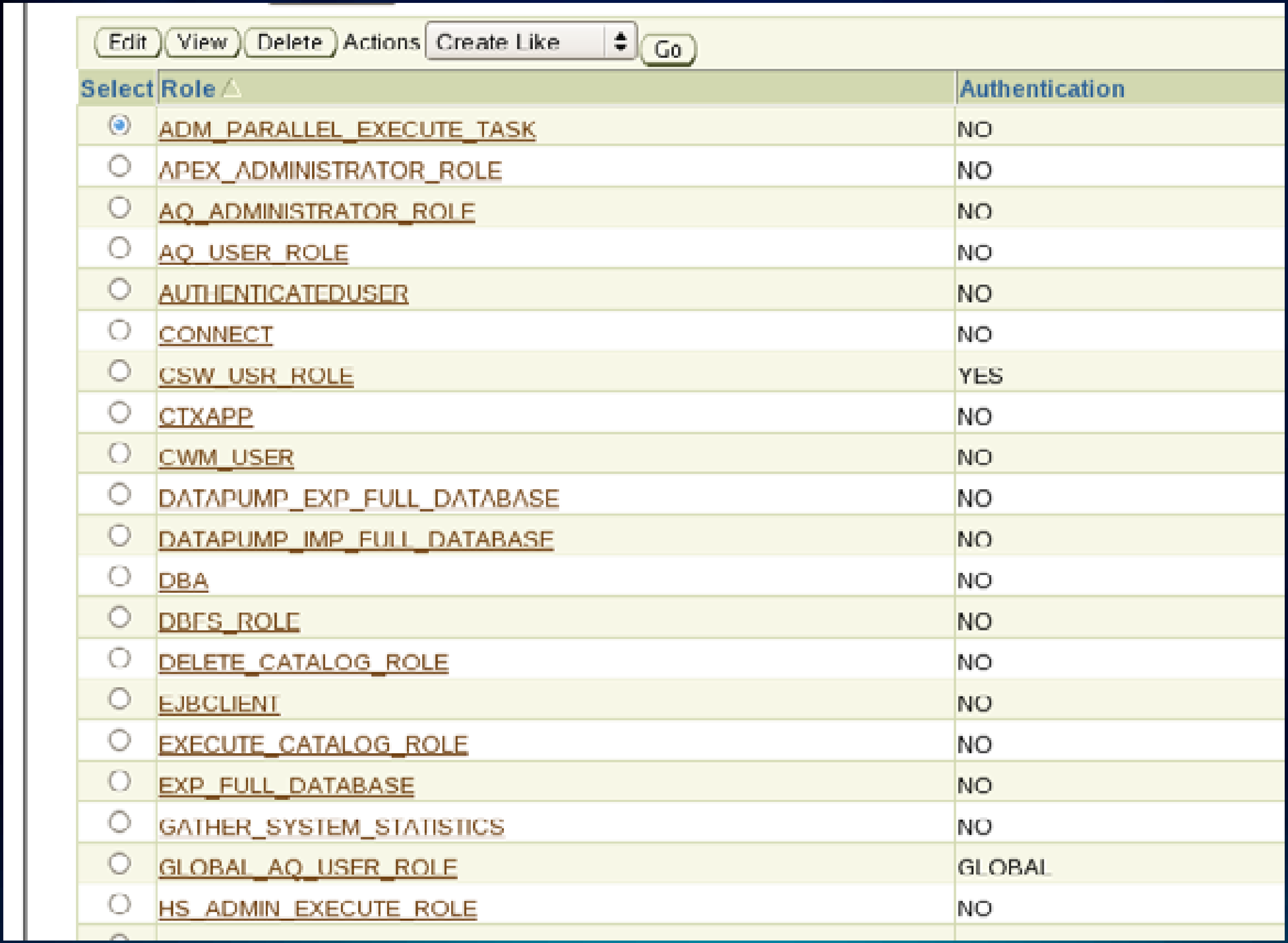


bulkadmin
dbcreator
diskadmin
processadmin
securityadmin
serveradmin
setupadmin
sysadmin



db_accessadmin
db_backupoperator
db_datareader
db_datawriter
db_ddladmin
db_denydatareader
db_denydatawriter
db_owner
db_securityadmin
public

# Oracle Fixed Roles Example



| Select | Role △ | Authentication |
|---|---|---|
| ● | ADM_PARALLEL_EXECUTE_TASK | NO |
| ○ | APEX_ADMINISTRATOR_ROLE | NO |
| ○ | AQ_ADMINISTRATOR_ROLE | NO |
| ○ | AQ_USER_ROLE | NO |
| ○ | AUTHENTICATEDUSER | NO |
| ○ | CONNECT | NO |
| ○ | CSW_USR_ROLE | YES |
| ○ | CTXAPP | NO |
| ○ | CWM_USER | NO |
| ○ | DATAPUMP_EXP_FULL_DATABASE | NO |
| ○ | DATAPUMP_IMP_FULL_DATABASE | NO |
| ○ | DBA | NO |
| ○ | DBFS_ROLE | NO |
| ○ | DELETE_CATALOG_ROLE | NO |
| ○ | EJBCLIENT | NO |
| ○ | EXECUTE_CATALOG_ROLE | NO |
| ○ | EXP_FULL_DATABASE | NO |
| ○ | GATHER_SYSTEM_STATISTICS | NO |
| ○ | GLOBAL_AQ_USER_ROLE | GLOBAL |
| ○ | HS_ADMIN_EXECUTE_ROLE | NO |

# Tips for Grouping Users

- Create separate groups (roles) for system and object privileges.
  (Provides better control of privileges for the system roles and data owners to grant privileges to the object roles exclusively.)

- Choose a naming convention that reflects each type of group/role (e.g. LANDBASE_EDITORS, PUBLIC_ACCESS, etc..)

- Grant privileges directly to the ArcSDE administrator user and grant privileges via groups (roles) for all other users.

- Avoid mixing roles with directly granted privileges for end user accounts.
  (When end user accounts receive privileges through both roles and direct grants, a well-planned security model can quickly devolve into an unmanageable mess.)

# Roles and OS Groups

- Support, use and configuration varies between RDBMS
- SQL Server
  - connect, read and edit data supported in 9.x and later
  - use of groups that contain members who can own data in 9.2 and later releases
  - But, the schema of the user must have the same name as the login of the individual user. You cannot create one schema to store the data created by all the group members.
  - permissions on the server and in individual databases is inherited from their group membership.

# Thank You

http://www.esri.com/sessionevals