IBM Software Group

DB2 Express-C 9 overview course

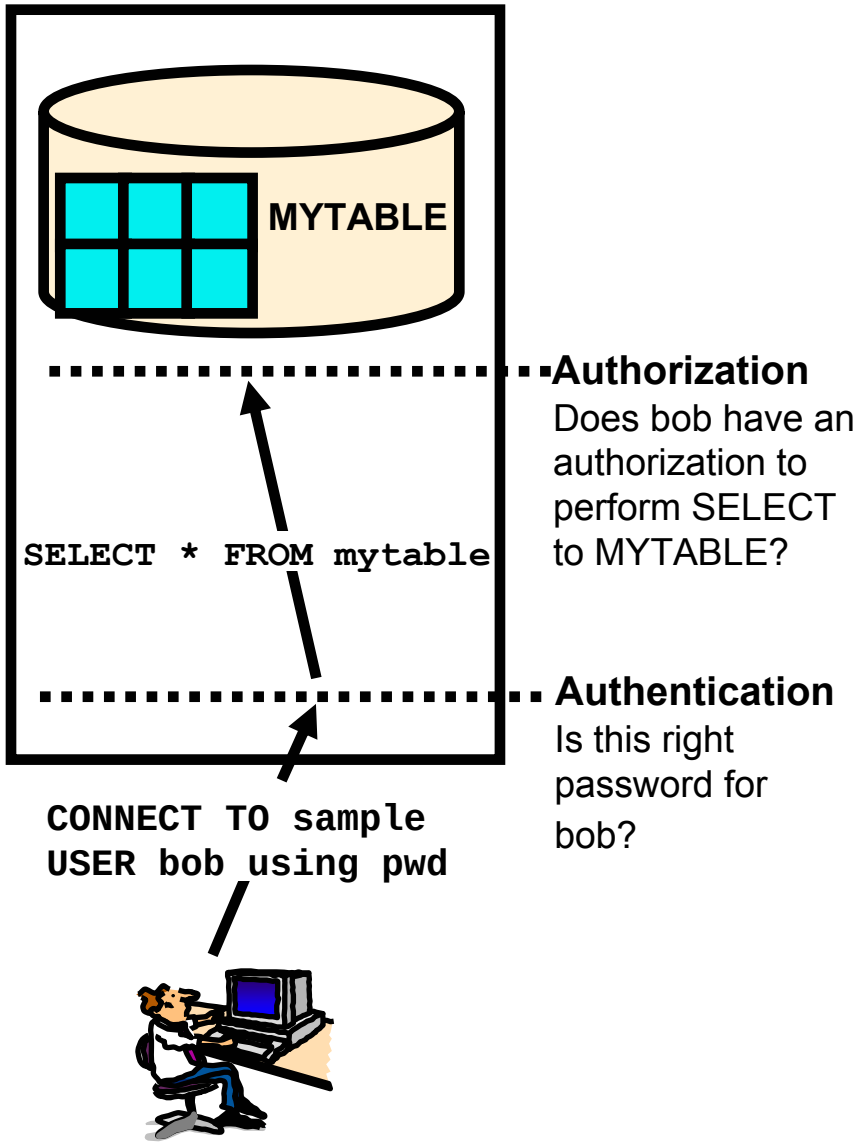
Database Security

DB2 Information Management Software

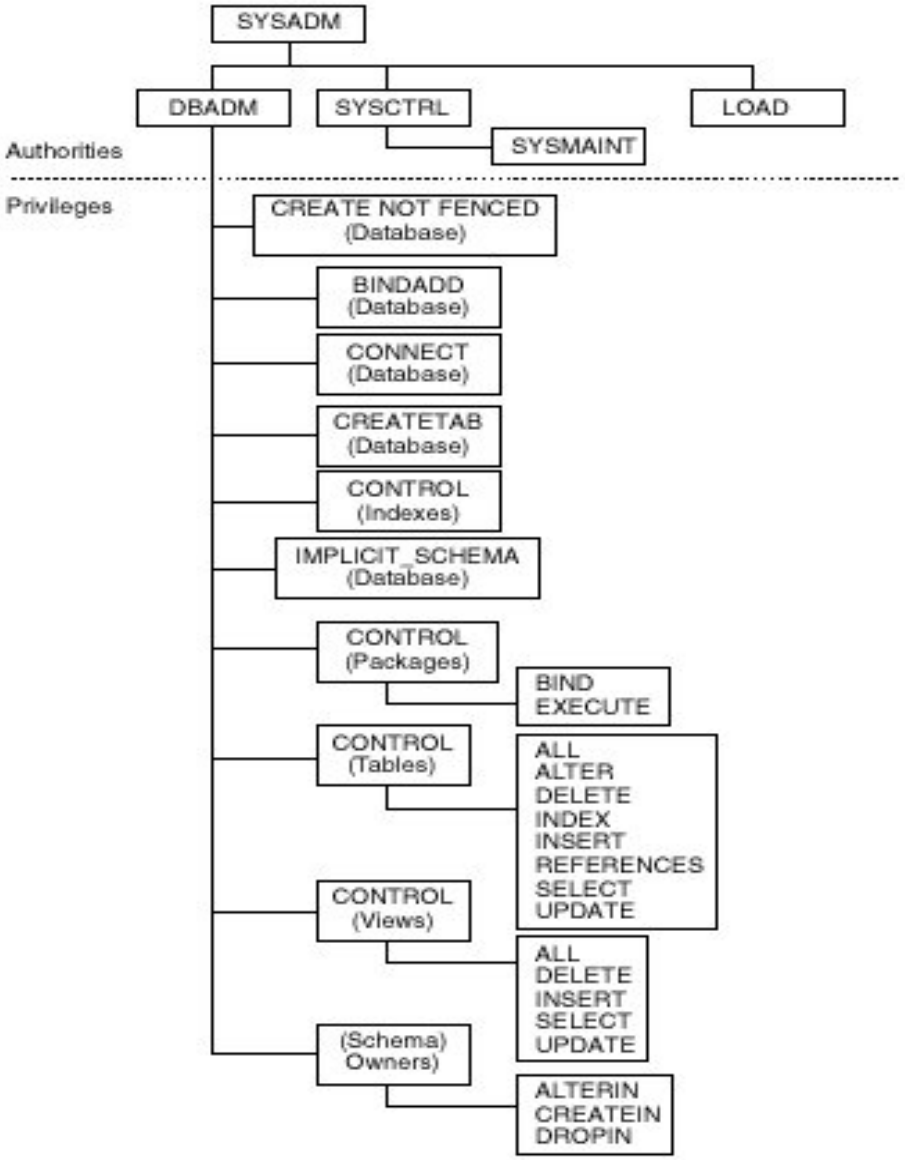
ON DEMAND BUSINESS

DB2 Security Overview

- **DB2 uses a combination of:**
  - External security service
  - Internal access control information
- **Authentication**
  - Identify the user
    - Check entered user name and password
  - Done by security facility outside of DB2 (Part of the OS, DCE, and so forth)
- **Authorization**
  - Check if authenticated user may perform requested operation
  - Done by DB2 facilities
    - Information stored in DB2 catalog, DBM configuration file



AUTHORIZATION: Authorities and Privileges



Other Authority Levels

Function	SYSADM	SYSCTRL	SYSMAINT	SYSMON	DBADM	LOAD
Update DBM CFG	YES					
Grant/Revoke DBADM	YES					
Establish/Change SYSCTRL	YES					
Establish/Change SYSMAINT	YES					
Establish/Change SYSMON	YES					
Force users off database	YES	YES				
Create/Drop database	YES	YES				
Restore to new database	YES	YES				
Update DB CFG	YES	YES	YES			
Backup database/table space	YES	YES	YES			
Restore to existing database	YES	YES	YES			
Perform roll-forward recovery	YES	YES	YES			
Start/Stop instance	YES	YES	YES			
Restore table space	YES	YES	YES			
Run trace	YES	YES	YES	YES		
Obtain monitor snapshots	YES	YES	YES			
Query table space state	YES	YES	YES			
Prune log history files	YES	YES	YES			
Quiesce table space	YES	YES	YES		YES	YES
LOAD tables	YES				YES	YES
Set/Unset check-pending status	YES				YES	
Create/Drop event monitors	YES				YES	

SYS Authorities

- Users of a DB2 database are controlled by native OS authentication services.
  - ►Free database/sysadmin/users from having to deal with multiple logins/password.

- SYSADM, SYSCTRL & SYSMAINT are defined by OS groups in DBM CFG
  - –update dbm cfg using **SYSADM_GROUP** <group>
  - –update dbm cfg using **SYSCTRL_GROUP** <group>
  - –update dbm cfg using **SYSMAINT_GROUP** <group>

- Each instance has its own authority group definitions

- On Windows, parameters are not set by default, implying local Windows Administrators group

DBADM Authority

- **DBADM** = Super user for the database. No authority at instance level

- Example:

  connect to sample

  grant DBADM on database to user <userid>

The PUBLIC group

- PUBLIC GROUP
  - ANY user id identifiable by operating system/network authentication service
- The following are granted to PUBLIC by default:
  - CONNECT
  - CREATE TAB
  - IMPLICIT_SCHEMA
  - BINDADD
- To "lock down" your system, you can revoke these privileges from PUBLIC

GRANT and REVOKE examples

- GRANT SELECT ON TABLE T1 TO USER user1
- GRANT ALL ON TABLE T1 TO GROUP group1

- REVOKE ALL ON TABLE T1 FROM GROUP group1
  - ► if user1 is part of group group1, does he/she still have SELECT privilege?

- GRANT EXECUTE ON PROCEDURE p1 TO USER user1
- REVOKE EXECUTE ON PROCEDURE p1 FROM USER user1 **RESTRICT**

- REVOKE IMPLICIT_SCHEMA ON DATABASE FROM PUBLIC
- REVOKE CONNECT ON DATABASE FROM PUBLIC

Managing Authorities and Privileges from the Control Center

DEMO