DB2 Data Management Software

IBM

e business software

DB2 Version 8 Basic Security

DB2 Quickstart Education

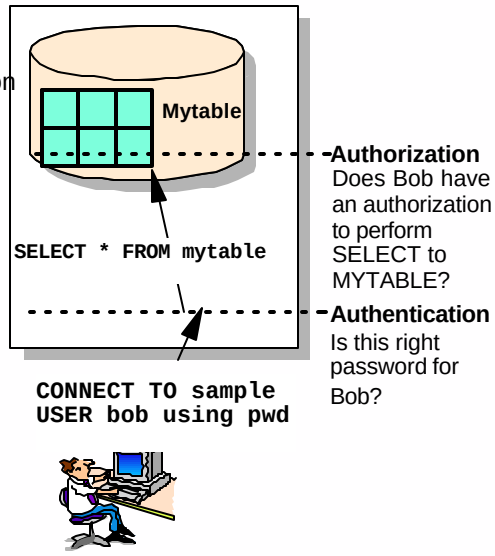
Maintained by Paul Yip (ypaul@ca.ibm.com)

February 2003

IBM Software Group

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 O/S, 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

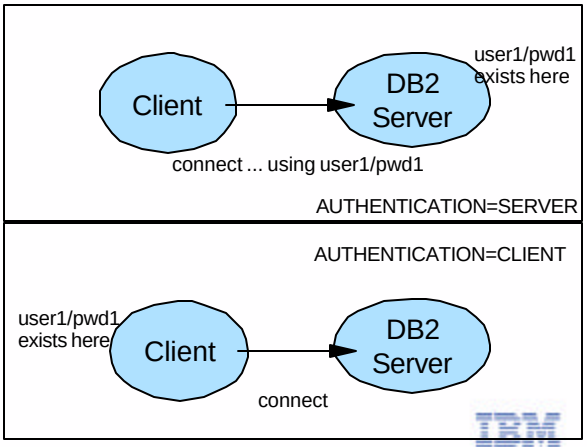


DB2 Data Management Software

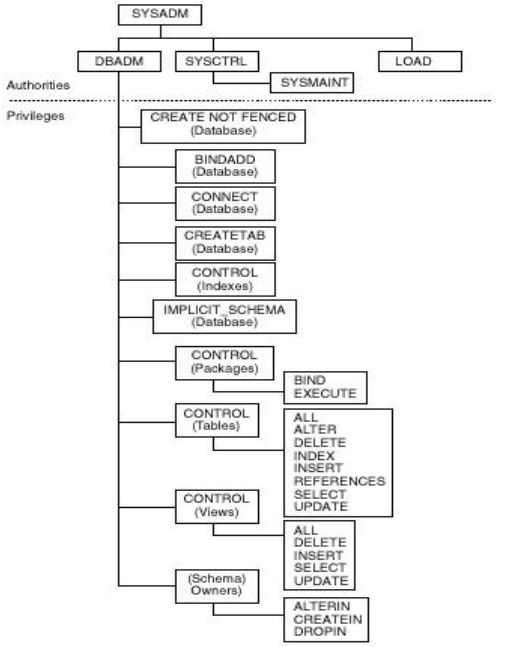
IBM

AUTHENTICATION

- When client and server are different machines, where is userid/password is checked?
- DBM CFG Parameter (at the DB2 server):
  AUTHENTICATION = SERVER (default)
- Valid values:
  - SERVER_ENCRYPT
  - CLIENT
  - CLIENT_ENCRYPT
  - KERBEROS
  - KRB_SERVER_ENCRYPT



Hierarchy of Authorities and Privileges



Authorities

Function	SYSADM	SYSCTRL	SYSMAINT	DBADM
UPDATE DBM CFG	YES			
GRANT/REVOKE DBADM	YES			
ESTABLISH/CHANGE SYSCTRL	YES			
ESTABLISH/CHANGE SYSMAINT	YES			
FORCE USERS	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	
OBTAIN MONITOR SNAPSHOTS	YES	YES	YES	
QUERY TABLE SPACE STATE	YES	YES	YES	YES*
PRUNE LOG HISTORY FILES	YES	YES	YES	YES
QUIESCE TABLE SPACE	YES	YES	YES	YES*
LOAD TABLES	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 & SYSMAIN 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>

Default Database Privileges

- 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

Object Level 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