Torsten Roeber – DB2 Support Specialist
October 2012

DB2 Security with DB2/VSE and DB2/LUW

DB2 Security with DB2/VSE and DB2/LUW

- DB2/VM&VSE Security with local or remote applications and database-server
- DB2/LUW Security with remote clients, application- and database-server
- Security in a combined environment (VSE and remote applications with DB2/LUW server)
- Security Hints & Tips
- Actual levels of DB2 Servers on VM/VSE and LUW
- Questions?

Source If Applicable

DB2/VM&VSE Security with local or remote applications and database server

- DB2/VM & DB2/VSE allows internal and external authentication
  - passwords stored and maintained in the database
  - external security manager to authenticate users
  - external security manager could use LDAP
- Database access rights are controlled per USER within the database using GRANT
  - Database access:SCHEDULE, CONNECT, DBA
  - Data access: SELECT, UPDATE, DELETE etc.
- DB2 Servers treat users differently if their using DRDA or SQLDS protocol
  - 'local' (CICS or BATCH) applications using SQLDS protocol can't use encrypted passwords.
  - 'remote' (DRDA) applications can use password encryption but no encrypted userid

Source If Applicable

DB2/LUW Security with remote clients, application- and database-server

- DB2/LUW uses external authentication via the operating system only!
  - users can be defined locally or in a domain
  - authentication can use various methods using plugins or OS definitions
  - LDAP can be used transparently
- Database access rights are controlled per USER, GROUP or ROLE within the database using GRANT
  - Database access:CONNECT, DBADM, SECADM, SYSADM, etc.
  - Data access: SELECT, UPDATE, DELETE etc.
- DB2/LUW Servers accept DRDA protocol only!
  - no difference between local or remote users concerning authentication
  - userid and password encryption could be used as well as data encryption
- Roles can be inherited from a trusted connection (context)
  - a trusted context definition includes a userid and a client system hostname or ip address
  - If the same user is connected from a different system it can get a different or no role
  - explicit trusted connection allows to switch userid with or w/o authentication

Source If Applicable

Security in a combined environment (VSE and remote applications with DB2/LUW server) 1/2

- DB2/LUW offers the same functionality to VSE an other applications
  - some functions might not be usable from VSE side
  - LUW system are case sensitive, which allows lower case or mixed case passwords
  - for host clients user authentication is retried with lower case folded password if the first attempt failed.
- Security issues moving from DB2/VM or DB2/VSE server to DB2/LUW server
  - applications connect to the DB2/LUW server using userid and password (if needed)
  - userid and password might be hard coded within the application source
  - these user credentials might be well known within application development or the whole company
  - DB2/LUW server could be easily accessed from any system within the company network
  - the user credentials thought to be used by VSE applications only, could be used from any client.

Source If Applicable

Security in a combined environment (VSE and remote applications with DB2/LUW server) 2/2

- Issues can be solved using trusted context and roles
  - define a ROLE corresponding to each VSE application user and revoke all access rights except CONNECT from these users.
  - define a trusted context for each VSE application user with the corresponding VSE systems IP address or hostname
  - connecting to the DB2/LUW server, the user will inherit the ROLE giving the needed data access rights for the application from the trusted context, if the application connects from the VSE system only!
  - using the same user and password to connect from another client system will still work, but the client won't get access to the data!

Source If Applicable

Security Hints & Tips

- Think about the security concept before creating the first production database
  - be very careful using a former 'test' database in production
  - never use the DB2/LUW instance owner for applications to connect to the database
- Think about auditing needs before coding applications using the same (technical) user to connect to the database server.
  - Reliable auditing needs personalized users
  - Even for administrative tasks personalized user should be used
- In a production environment all users should have the access rights needed for that users role only!

Source If Applicable

Actual levels of DB2 Servers on VM/VSE and LUW

- DB2 Server for VM & VSE 7.5.0 is the actual release
  - Server & Client edition available on zVM and zVSE
- Some features of DB2 VM & VSE are still on 7.3 or 7.4
- DB2 for Linux, Unix and Windows has following actual releases:
  - 10.1 available since April 30 2012
    - FP1 available since September 14 2012
    - FP2 planned for December 2012
  - 9.7 EOS planned for September 30 2014
    - FP7 available since October 19 2012
  - 9.5 EOS planned for April 30 2014 (extended from April 2013)
    - FP10 available since August 15 2012
  - 9.1 EOS since April 30 2012
    - service extension available until April 30 2015
    - FP 12 (July 11 2012)

Source If Applicable

Questions?

- Do you have any questions?
- Thank you!
- Email address: torsten.roeber@de.ibm.com

Source If Applicable