Db2 for z/OS: Using RACF Training

BILGINC IT Academy
info@bilginc.com
bilginc.com

Duration: **1 Day**

Db2 for z/OS security has historically been performed using an external security product such as RACF to secure the system, while access to Db2 objects and data was controlled using Db2 internal security.
However now more and more organisations are using RACF to control all aspects of Db2 security - both at the system and data levels.
This intensive, one-day course shows exactly how this may be achieved.

This course is also available for one-company, on-site presentations and for live presentation over the Internet, via the Virtual Classroom Environment service.

Prerequisites

A working knowledge of RACF and an understanding of Db2 for z/OS at a conceptual & terminological level.

What You Will Learn

- describe Db2 security
- understand terminology used with Db2 security
- use and structure Db2 security tables
- use primary, secondary, and CURRENT SQLID authorisation IDs used by Db2
- use SQL to control security using the GRANT and REVOKE statements
- describe the meaning of explicit, implicit, composite and grouped privileges
- explain ownership considerations with regard to Db2 objects
- control Db2 address space and data set authorisation using RACF
- use RACF to control access to Db2 objects
- describe the new RACF classes for Db2 objects
- create RACF profiles for Db2 objects
- understand the additional considerations when using Db2 in a distributed environment.

Training Outline

Introduction to Db2 Security

Security overview; Sign-on security; Connection security; Db2 internal security; Other options; Security strategy (Transaction Manager or Db2); Security strategy (centralised or decentralised); Using remote applications.

Internal Db2 Security

Db2 security; Db2 security mechanism; Db2 security tables; Security terms; Authorisation ID; Privilege; Resource; Primary and Secondary Authorisation IDs; Maintaining security; Data Control Language; Grouped privileges; Explicit & implicit privileges; Ownership considerations; Static and Dynamic SQL; Static SQL considerations; Dynamic SQL considerations; Db2 security disadvantages.

Data Control Language & Privileges

SQL GRANT and REVOKE statements; Cascading REVOKE; Package, plan & collection privileges; Database, table, & view privileges; Other object privileges; System privileges; DCL examples: application

BILGINC IT Academy

info@bilginc.com

bilginc.com

development, Bind, program execution; Insufficient authority.

Db2 Security Reporting and Auditing

Db2 catalog security tables; Common table columns; Security tables 1 - 4; Auditing tables; Audit trace.

RACF Security Overview

What is RACF?; Identifying and verifying users; Checking authorisations; Recording and reporting; Terminology - users and groups; Terminology - resources and classes; Terminology - profiles; User profile; Resource Profile; Discrete and generic profiles; Creating Generic Profiles; Maintaining RACF Security.

Defining the Db2 Subsystem to RACF

Address space authorisation; Protected access profiles; RACF router table; Db2 address spaces; Permitting RACF access; Protecting Db2 datasets - create profiles; Protecting Db2 datasets - permitting access.

Defining Db2 Objects to RACF

Native DB2 security; DB2 with RACF; RACF / DB2 external security module; Installation; Mapping DB2 authorisation checks; Scope of RACF classes; Multi-subsystem scope classes; Single subsystem scope classes; Customisation; DB2 objects and RACF classes; Profiles; Privileges - buffer pools, storage groups & tablespaces; Privileges - DB2 system; Privileges - database and schema; Privileges - tables, views, indexes and user-defined functions; Privileges - collection, plan and package; Privileges - distinct types, sequences and stored procedures; Privileges - administrative authorities; Insufficient authority; Migration tools.

Further Db2 Security Techniques

Multi-level security overview; Security labels; Row level granularity; Multi-level security and SELECT; Multi-level security and INSERT; Multi-level security and UPDATE; Multi-level security and DELETE; Multi-level security and utilities; Row and column access control; row permissions; column masks.

Distributed Data Considerations

Distributed Data overview; DDF components; Communications tables; Security actions (client); Security actions (server with SNA client); Security actions (server with TCP/IP client).