

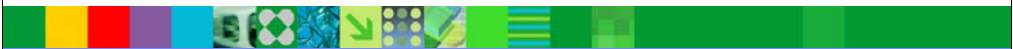


IBM Software Group

DB2 for z/OS Security: Protect Your Assets

An overview of DB2 security

DB2 Information Management Software



@business on demand software

Roger Miller
DB2 for z/OS Development
IBM Silicon Valley Lab
October 8, 2007

This is a presentation of DB2 ® for z/OS Security, starting with the objects, describing their relationships and discussing techniques for security and auditing. The first part of the session will discuss native DB2 security. This presentation starts at the DB2 V6 level and includes information about changes in DB2 Version 7 and beyond. The second part of the session will focus on the DB2 option to use RACF or the z/OS Security Server for access control. This session will begin with discussing whether to choose this option. DB2 has always relied upon operating system identification and authentication, but has separate SQL mechanisms for access control that provides integration with the database management system. It is very important to understand the relationships and the integration if you make choices about DB2 security.

IBM Software Group | DB2 Information Management Software IBM

How is Security Different on the Mainframe?

Information & Applications

Supports a variety of encryption standards to help keep **current with industry and government security regulations**

People

Manage access of critical data for users through **Multiple Level Security**

Networks

Integrates security with the network with built-in technology **resistant to hackers**


A highly secure business environment with compliance to standards helps build industry credibility and gain consumer trust

Hardware

End-to-end protection that helps keep data uncorrupted and uncompromised

Operating System

Architected for security from within to **reduce risk and not be susceptible to viruses**



"The IBM mainframe is the only computing system to earn the highest level of industry security certification, EAL5." Bob Hoey, Worldwide VP Sales for System z
"Operating systems generally called 'secure' rarely reach higher rankings than EAL4." wikipedia.org
(Evaluation Assurance Level) = International standard to define security requirements in computer systems.

*EAL

18

As we all know, security is one of the hottest topics in the industry these days. You may have heard in the news about data cartridges being lost in transit and legislation demanding higher levels of accountability. Because of unfortunate events like these, security has become a front and center topic in every IT shop. Not surprisingly, there is no better platform to handle the challenges of keeping your data secure than the System z.

System z has a history of ensuring that any and all data residing on it is safe and secure. This goes far beyond the usual measures of other platforms. System z takes a holistic approach to security and is designed so that every component works flawlessly. Each component cooperates with the system as a whole to guarantee the safety of your most important revenue generating items. Everything -- from the data coming through your network to the people allowed to access that data -- is closely monitored, thus providing end-to-end protection of your critical business information.

But how secure is it, really? System z has been certified at EAL level 5. EAL, or Evaluation Assurance Level, is an industry security certification ranging from level 1 through 7. Only 3 systems have reached EAL 5... and they're all IBM machines. That has to give you an idea of the strength of System z security. z/OS has achieved EAL4 certification and DB2 V8 is currently in evaluation at EAL3 for two profiles, CAPP and LSPP.

IBM Software Group | DB2 Information Management Software IBM



Enterprise Systems
Mainframe and High-end Server Solutions in Focus

[Home](#) | [About ES](#) | [Subscribe](#) | [Contact Us](#) | [RSS](#) | [XML](#)

News

- Enterprise
- Security
- Storage
- Mainframes
- Servers
- Data Center
- Networking
- Open Source/Linux
- Data Management
- Development
- Emerging Tech
- Case Studies/Best Practices
- IT Careers

RESOURCE CENTER

- White Papers/Case Studies
- ESG: Clustered Storage: Valuable Today - Requisite Tomorrow
- Simple Steps to IM Management
- IT Salary Survey
- Business Intelligence
- Compliance

Enterprise

Mainframe Proponents Talk Up Platform's Security Strengths

There's a growing consensus -- among IBM users, at least -- that Big Iron's biggest selling point might well be its proven security model.

by Stephen Swoyer
9/4/2007

IBM officials like to point out the [mainframe's](#) all-in-one power and refrigeration model as a great solution for rising data-center power and cooling costs. That's a given. Now there's a growing consensus among IBM users that Big Iron's biggest selling point might well be its proven security model.

"We've heard from a lot of customers who are interested in [the mainframe's all-in-one power and cooling footprint], and we've also had success with [customers attracted by] virtualization and other [mainframe] features. We're also increasingly hearing from customers interested in using the mainframe as a sort of security hub," says Mary Moore, [System z](#) security initiative leader with Big Blue.

To a degree, Moore maintains, the mainframe has comprised a kind of de facto security hub for many years. "Our customers for 40 years have been positioning their mainframes as their security hubs, and security and availability have been the two most important features that we continue to invest in and ensure that we're leading the industry."

The mainframe's role as security hub doesn't just mean it's the last line of defense against outside attacks. The Big Iron security hubs that Moore and others talk up are more than just information citadels; instead, Moore says, they're designed to function as coordination, automation, and response centers for enterprise-wide information access.

Consider the z/OS 1.9 updates Big Blue announced last month: a number of these improvements—new support for network security policy management, enhancements to z/OS' Public Key Infrastructure (PKI) services, and an update that lets the z/OS Integrated Cryptographic Facility (ICSF) support the popular PKCS #11 security standard—boost System z security and enhance Big Iron's cross-platform security credentials, too. It is—as Burt Reynolds' Jack Horner once put it in the film *Boogie Nights*—an important part of the process.

More Enterprise News

- ▶ Analysis: Lifting the Hood on Sun's New UltraSPARC T2 Chip
- ▶ Avoiding the RAMifications of Storage Retention
- ▶ How IBM's Updated z/OS Improves Security
- ▶ Big Blue Unveils Next-Gen Notes
- ▶ Reverse Network Analysis: Simple Solutions for Complex Networks

Print Email



<http://www.esj.com/news/print.aspx?editorialId=2782>

This article outlines some of the System z security advantages.

Here are some other pointers:

<http://www.ibm.com/systems/z/security/solutions/>

<http://www.ibm.com/systems/z/security/>

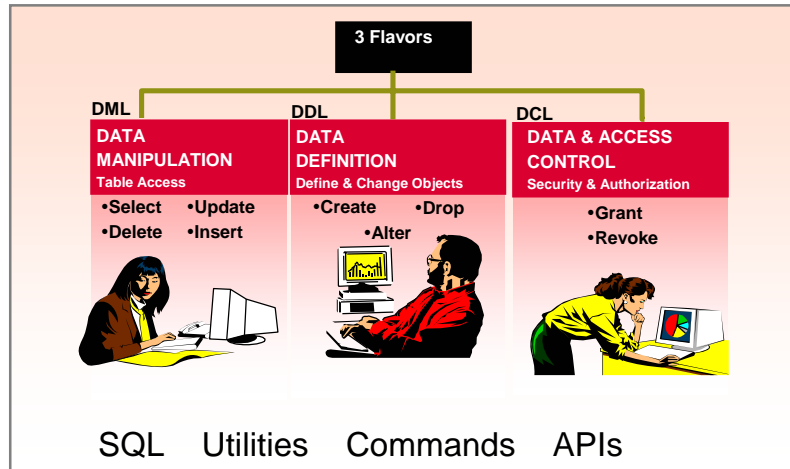
Agenda

- **Part 1 Native DB2 Authorization**
 - SQL, Objects & Relationships
 - DB2 Security Techniques
 - Version 7 and 8 Changes
- **Part 2 RACF Authorization Control**
 - Does this option fit you?
 - Implementation & Considerations
 - Version 8 Multilevel Security Row Level
- **References and backup foils**

This is the agenda, with a quick overview of the objects and the relationships between the objects. The second part discusses DB2 security mechanisms and how they are used. The third part goes over some of the other controls and auditing. Then we will talk about some of the enhancements in Version 7 and summarize.

This is an overview. As you understand the details later, you will notice that there are a few exceptions to the overview rules. These notes almost certainly have some errors. Please refer to the formal documentation for your release levels and products when you need the best accuracy.

Structured Query Language (SQL)



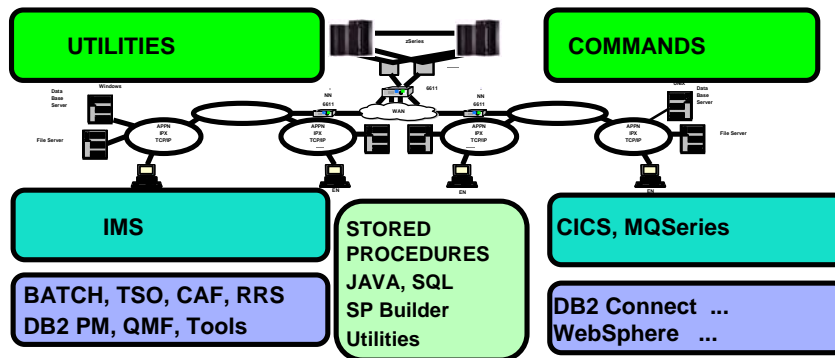
SQL or the Structured Query Language is generally separated into the ability to manipulate data: get information via SELECT or modify via INSERT, UPDATE and DELETE
 define data: CREATE new objects, ALTER them or DROP them

data access and control: GRANT and REVOKE provide the built-in security.

There are many other interfaces into DB2: utilities, commands, and other Application Programming Interfaces (API). Security and authorization are included in GRANT and REVOKE for all of the interfaces.

DB2 Operational Environment

- ➔ Users come from many environments
- ➔ Many possible sources, varieties of userids
- ➔ Many security and audit products, e.g. RACF **Tivoli** software
- ➔ Many options, exits and applications



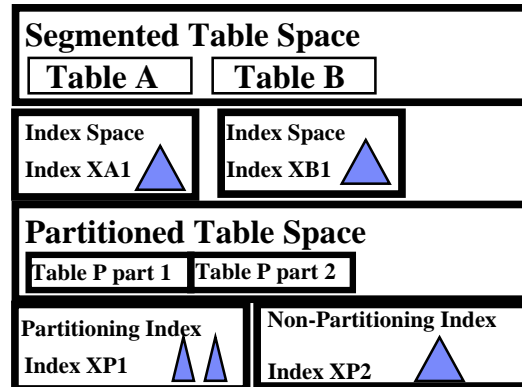
There are many different environments for DB2, with different connections and security. DB2 uses the security context when possible, so batch jobs, TSO users, IMS and CICS transactions have security that uses a consistent identification and authentication. This is true for stored procedures from these environments as well. The large number of options, exits, environments and asynchronous or parallel work provide challenges for security. Some key applications manage security at the application level.

For some work, such as distributed database serving, DB2 is the initial point on this platform. For this work (DRDA distributed access, remote stored procedures), DB2 establishes the security context and manages the work.

DB2 Database Structures

Subsystem or data sharing group

Database



These are the structures used in DB2 for z/OS. All databases are within a subsystem or data sharing group. The term database is similar to the usage in IMS, but not like the term used in most other RDBMS, including DB2 for UNIX & Windows. Database in most RDBMS is closer to subsystem than to other concepts. In DB2 for z/OS a database is a logical construct, & is the qualifier for table spaces.

Table spaces come in several varieties. Segmented table spaces are the primary version recommended for small and medium tables. They can contain one or more tables. Partitioned table spaces are for large tables, and they contain only one table. Indexes use separate spaces. Table and index spaces can be one or more data sets. A partitioned DB2 table can be up to 128 terabytes or 64,000 terabytes for LOBs.

DB2 Data Structures

Subsystems or Data Sharing Groups

Databases

Table Spaces

Partitions

Tables

Indexes

Triggers

Views, Aliases & Synonyms

Storage Groups

*See Administration Guide
Chapter 1.2 picture,
Multilevel DB2
Authorization Hierarchy*

This is a hierarchy for the DB2 data objects. I've used subsystems or data sharing groups as the top level. DB2 authorization is defined for each subsystem or data sharing group. Security can be defined for multiple subsystems using the security subsystem, RACF.

Databases are the next level. All of the table spaces are within a database. If the table space is partitioned, then the partitions are within the table space. Each table is in a single table space. Indexes are in separate spaces within a database, but each index is defined on a single table. Triggers are also defined for a table, as are constraints.

Views, aliases and synonyms can be across multiple databases. Storage groups are an indication to use System Managed Storage (*) or volumes for data set allocations.

Cascade Revoke

Referential Integrity on catalog

DELETE CASCADE

Determining revoke cascade

Save authorization copy

Revoke

Determine difference

Rollback

Avoiding cascade delete

Authid install sysadm for short period

Revoke authority

Return to normal install sysadm

This hierarchy is reflected in the DB2 catalog with referential integrity. The cascade revoke is done by the same referential integrity code that implements delete cascade, in part.

If you want to determine how much will be removed with a cascade revoke, the process is generally to save a current copy of the information, issue the revoke, to query to information again to determine the difference, and then to rollback.

If you need to avoid cascade delete, then the usual technique is to have the authid whose authority is to be revoked become an install sysadm for a short time. Revoke the authority and then set up the normal install zparms. These change currently require stopping and restarting DB2.

DB2 Application Structures

Plan: set of packages and/or SQL from programs

Collection

Package: SQL from program

Dynamic SQL or static SQL

BIND process

There are two types of application structures, plans and packages. Plans have a single short name. Plans provide the connection & controls for IMS & CICS environments. SQL statements from one or more programs are precompiled & bound into plans. Plans can have a list of packages for additional flexibility.

A package is the SQL from a single program. They are part of a plan and do not have as much authorization control as plans. They are grouped into collections & also have versions. Package authorization is at the package level, not for versions. Collections have authorization for being able to create a package in it and package administration.

Plan & package authorization for static SQL is checked at BIND or compile time. At run time, authorization to execute the plan is often the only check, improving performance substantially. If authorization is lost, then the plan or package is invalidated. Dynamic SQL is checked at run time.

Views

SQL - Data Definition Language

```
CREATE VIEW SW_CUSTOMER AS
SELECT CUST_NBR, CUST_NAME,
       CUST_CREDIT
FROM CUSTOMER
WHERE CUST_REGION='SW'
```

- Only customers in SW
- Only customer number, name & credit

■ **Views can:**

- Protect data: rows and/or columns
- Simplify access to data
- Join or union to add or remove information

Views can be used to hide data. They can provide only certain fields, as noted. Views are often used to simplify access to data by being able to define the view once and use it many times.

Table privileges DELETE, INSERT, SELECT, UPDATE, or ALL can be granted individually on a view. By creating a view and granting privileges on it, you can give someone access only to a specific combination of data. This capability is sometimes called field-level access control or field-level sensitivity.

Using a VIEW

Retrieve from CUSTOMER table
using SW_CUSTOMER view

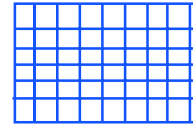
```
SELECT *  
FROM SW_CUSTOMER  
WHERE CUST_CREDIT = 'AAA'
```

or without the SW_CUSTOMER view

```
SELECT CUST_NBR, CUST_NAME,  
       CUST_REGION  
FROM CUSTOMER  
WHERE CUST_REGION = 'SW'  
       AND CUST_CREDIT = 'AAA'
```

This example shows the ability to simplify. Using the view, only the additional qualification is needed. Often a view can be used to handle more complex logic, such as a multiple table join or UNION (in Version 7). The person who uses the view does not need to be concerned with the join, UNION or authorization concerns.

DB2 Security Concepts



Database Constructs: Relationships

- Table: Data in rows and columns
- Index: Ordered set of data and pointers to rows
 - No direct access or authority check for use
- Table space: Data sets containing tables
- Database: A logical set of tables and table spaces
- View: "Virtual table" or logical view of data
 - Subset of table
 - Across multiple tables, databases, even subsystems
 - Data for view is not stored
 - Views may be built on views
 - Provides field level and content controls
- Plan or package: Set of SQL statements from program
- Authorization methods: dynamic or static SQL

The database objects are tightly connected. If you drop a database, then all of the table spaces, tables, indexes, views and authorization on the objects are also dropped. If authorization is revoked, then dependent objects and authorization are dropped or invalidated.

The index has a subset of the data in a table, but there is no authorization for indexes. Authorization for the table is used to control the index as well.

The view is a key concept for security. It provides a mechanism that is built into the DBMS that allows a wide variety of controls. Subsets of columns and rows can be defined, and joins can be used, with the USER and CURRENT SQLID to provide additional security.

DB2 Access Control

Authorization via GRANT and REVOKE

- Subsystem privileges: individual and administrative
- Table and view privileges
- Plan privileges
- Package privileges
- Collection Privileges
- Database privileges: individual and administrative
- Usage privileges: bufferpool, stogroup, table space
- Distinct types, functions, stored procedures, JARs (V7)



Delegation via GRANT ... WITH GRANT OPTION

- Cascading revoke

Access checking

- Direct: user to data
- Indirect: user to transaction, transaction to data

Grant and revoke statements provide the access control for DB2 objects. Each object has specific privileges, and some groups or administrative privileges are defined to improve productivity.

When authority is granted, there is an option to grant with the grant option. This allows the new person to grant access. If the first grantee has their authorization revoked, then the new person's authorization is also revoked. This is called cascading revoke.

The DB2 access models are both direct: check the user for authority to the data and indirect: check at bind time for the application process to the data, check at run time for user to application process.

DB2 for z/OS Security Exits and Interfaces

- Connection routines and sign-on routines
- Access control authorization exit routine
- RACF access control module
- Edit routines
- Validation routines
- Field procedures
- Log capture routines
- Instrumentation Facility Interface
- Interpreting Trace information
- Interpreting Recovery Log information

DB2 exit routines can make significant changes in identification, authentication, access control and auditing. Most of the information about these routines is in Appendix B, Writing Exit Routines, of the Administration Guide. Other appendices document tracing, instrumentation interfaces, and recovery log data used for audit.

Protecting Data

SQL - Data Control Language

```
GRANT ALL ON CUSTOMER  
TO NATIONAL_SALES, MARY, TED  
  
GRANT SELECT ON SW_CUSTOMER TO  
SW_SALES, JOHN  
  
REVOKE SELECT ON SW_CUSTOMER  
FROM NE_SALES, JANE
```

Ownership concept for data, plans, packages, ...

If you don't "own" a table or view, you must be "GRANTED" access to use a table or view or have administrative authority.

Default access is none. Until access is granted, nothing can be accessed. To provide a facility like RACF UACC, the SQL syntax is GRANT ... TO PUBLIC.

The SQL Reference documents SQL authorization, showing that the authorization ID must have at least one of the following to be able to SELECT:

Ownership of the table or view

SELECT privilege on the table or view

DBADM authority for the database

SYSCTRL authority (catalog tables only)

SYSADM authority

Ownership is a concept that provides access which can't be controlled via authorization. Authorization in plans and packages comes from only the owner, not from the full list of authorization ids. While most authorization works like a list of groups, these persistent authorities come only from one source.

Protecting Data

- Integral part of SQL language: GRANT & REVOKE
- Access and execution authorization
- Query language is security language also
 - ▶ Any possible SQL qualification can be used to limit access including restricting on field value, only aggregated data, etc.
- Administrative authorities - SYSADM, DBADM, ...
- z/OS Security Server or RACF can be used
 - ▶ To control access to DB2 subsystem
 - ▶ To control non-DB2 access to DB2 data
 - ▶ To define groups of users
 - ▶ Alternative for access control security (grant & revoke)

The GRANT and REVOKE SQL statements are an integral part of the SQL language and SQL standards. Both direct data access and indirect or plan execution are included in the controls.

Views provide the ability to include a wide range of restrictions that are enforced by the DBMS.

The administrative authorities were modeled upon DBAs and system administrators, but variations in job responsibilities are common.

There is an option to use RACF or the Security Server for access control.

Controls for Data Integrity → redbook SG24-7111

- **Atomicity, Consistency, Isolation & Durability**
- **Entity Integrity**
- **Referential Integrity**
- **Views & check option**
- **Stored procedures**
- **Table check constraints**
- **Triggers**
- **Distinct data types & User-Defined Functions**
- **Database procedures (exits for validation, conversions, encryption, ordering)**



Database constructs for data integrity are one of the most important facets of DBMS. The defining attributes for DBMS are called ACID properties (Atomicity, Consistency, Isolation & Durability). Primary keys must be unique, so that each entity is identified uniquely. This is called entity integrity. Parent and child integrity is called referential integrity. The rule can be described as no orphans.

Views provide a wide range of possible constraints, as noted on earlier pages. Specify `WITH CHECK OPTION` when views are used for `INSERTs` or `UPDATEs`.

A wide range of additional checking can be provided with table check constraints, stored procedures, triggers, distinct types and database procedures. Triggers, stored procedures and distinct or user-defined types allow some processes to be managed with the data, so the database is often called active or object-relational.

DB2 Audit Summary

DB2 catalog data

- Tables, Table Spaces, Databases, Views, ...
- Authorization data from GRANT, REVOKE

Audit Trace sent to SMF, GTF, programs

- Selective tracing with 9 classes of information
- Access denials
- Authorization changes
- Audit changes, multilevel security
- Update of audited tables
- Access to read audit tables

DB2 Recovery Log, Image Copies, Data Replication, ...

There are many kinds of audit information available in DB2. The DB2 catalog stores the definitions of all the objects and the authorization. Users who are allowed to access these tables can use the power of SQL to audit and manage security. RACF has an unload facility that allows its security definitions to be loaded into DB2, so that broader auditing can be performed.

One of the primary audit sources is an audit trace that can provide very selective information. Other trace information can also be used in auditing.

The DB2 recovery log and utilities are also helpful in finding out how and when some data was modified.

Please read the Audit section of the Security and Auditing chapter of the DB2 Administration Guide.

DB2 Instrumentation Facility

- DB2 uses SMF and/or GTF and/or monitor program for trace data
 - ▶ Statistics, Accounting, Performance & Audit
 - ▶ Allows integrated reporting with other SMF/GTF data
 - ▶ Fully supported interface
 - ▶ Extensive DB2 information
 - Audit information
 - SQL statements
 - See DSNWMSGs for details of trace records

The audit trace and other traces can be sent to SMF, so that they can be processed with other audit data. Other destinations for the trace data include GTF and being sent directly to a program. A program could be an online audit monitor, for example.

The instrumentation can include information about the performance, resources, and processes. If detailed information is required, you can also examine the individual SQL statements, record accesses and locking. The data allows full accounting by user/transaction, with detailed data written every plan deallocation or change of user and fully detailed tracing down to individual call / IO / component level.

DB2 Version 7 Improvements

- Views: Option for DBADM create views & aliases for others, UNION in a view
- Kerberos Authentication
 - ▶ Requires Security Server OS/390 Version 2.10 or z/OS
- Authorization for Java ARchive file (JAR) usage
- Provide database name to access control authorization exit for create / alter index
- Encrypted userid & password authentication, change password support
- CONNECT with userid and password

There is a broad range of security improvements in DB2 for z/OS and OS/390 Version 7. For more details, see the V7 Presentation Guide or the V7 library.

Views are a key security facility and they are made substantially more usable with the ability to have a database administrator who is not a SYSADM define views & aliases for others. The ability to have UNIONS in views allows more ways to use views for security.

Kerberos authentication is an important change for many customers. Authorization was added for the JAR. The exit used for Security Server access control was enhanced to add more information and allow better database authorization instead of requiring table level. Improved flexibility for encryption & connection improves DB2 use as a web server.

DBADM authority for create view for others

Most customers should set DBADM CREATE AUTH to YES

Does not provide grant, revoke, drop or use of view

```

DSNTIPP          INSTALL DB2 - PROTECTION
====>
Enter data below:

 1 ARCHIVE LOG RACF  ====> NO           RACF protect archive log data sets
 2 USE PROTECTION   ====> YES          DB2 authorization enabled. YES or NO
 3 SYSTEM ADMIN 1   ====> RHA          Authid of system administrator
 4 SYSTEM ADMIN 2   ====> ERB          Authid of system administrator
 5 SYSTEM OPERATOR 1 ====> RHA          Authid of system operator
 6 SYSTEM OPERATOR 2 ====> ERB          Authid of system operator
 7 UNKNOWN AUTHID   ====> IBMUSER       Authid of default (unknown) user
 8 RESOURCE AUTHID  ====> SYSIBM        Authid of Resource Limit Table creator
 9 BIND NEW PACKAGE ====> BINDADD       Authority required: BINDADD or BIND
10 PLAN AUTH CACHE  ====> 1024          Size in bytes per plan (0 - 4096)
11 PACKAGE AUTH CACHE====> 32768        Global - size in bytes (0-2M)
12 ROUTINE AUTH CACHE====> 32768        Global - size in bytes (0-2M)
13 DBADM CREATE AUTH ====> NO           DBA can create views/aliases for others

PRESS: ENTER to continue RETURN to exit HELP for more information

```

A new option is provided as DB2 is installed. Users who have DBADM authority may be allowed to create a view / alias for another person. This has not been permitted in the past, due to a concern for security - but there are some other customers who think this is much better security, with fewer individuals who need to have SYSADM authority.

Most customers are expected to set the DBADM CREATE AUTH parameter to YES. The ability is controlled by the panel shown above or the DSNZPARM parameter DBACRVW. Setting this value to YES makes it possible to reduce the number of people who need SYSADM authority.

The default is consistent with prior releases, that is to say no increased ability for DBADM.

UNION everywhere

- A fullselect (union and union all operations) may appear anywhere a subselect was allowed previously
 - ▶ Now UNION can appear in
 - CREATE VIEW
 - table expressions
 - predicates
 - INSERT INTO ... (subselect)
 - UPDATE ... set column = (subselect)
- Improves usability and flexibility
 - ▶ Easier to view multiple tables as one
 - ▶ More uses for views in implementing security
- Syntax change
 - ▶ V6: Create view as <subselect> ...
 - ▶ V7: Create view as <fullselect> ...

The CREATE VIEW statement was able to provide several kinds of join processing, INNER, LEFT, RIGHT and OUTER joins, but was not able to include a UNION operator until Version 7.

Removing this restriction allows views to be used in more situations for controls, simplification and security.

This change also helps provide better DB2 family consistency and compliance with national and international standards.

What is Kerberos ?

- Authentication mechanism for network security
- DB2 V7 provides server support
- DB2 Connect V7 provides client support
- OS/390 V2R10 provides Security Server
- Similar to DCE
 - Flows encrypted tickets instead of 'clear text' userids and passwords
- More information
 - Version 7 Presentation Guide, SG24-6121
 - <http://web.mit.edu/kerberos/www/>
 - <http://web.mit.edu/kerberos/www/dialogue.html>



Kerberos security is an option for network security with DB2 Version 7, DB2 Connect Version 7 and OS/390 Version 2 Release 10 Security Server.

Kerberos is an industry accepted standard that provides better integration with other platforms and a single signon capability.

This function is for DB2 as a server, not as a requester.

This third party authentication flows encrypted tickets, rather than userids and passwords.

Encrypted userid & password

- Encrypted password support introduced in V5 and V6 via APAR PQ21525
- Support now extended to encrypt userid and password
- Server support only
- Function currently only used by DB2 Connect V7 clients

Password encryption has been provided for some time, and this support has been extended to encrypt both the userid and the password.

These changes are only the server support, not the requester, and the requester changes are in DB2 Connect V7.

Encrypted change password

- Encrypted support extended to change password function
- Server support only
- Function currently only used by DB2 Connect V7 clients

The ability to change a password was added in V5 as well, and the encryption support is extended here too, with similar function and support to the prior foil.

CONNECT with userid & password

New option on CONNECT

```
CONNECT USER :userid USING :password
```

(connect to local DB2 with userid and password)

```
CONNECT TO location USER :userid USING :password
```

```
CONNECT TO :location USER :userid USING :password
```

(location or :location may specify the local DB2 or a DRDA server)

You can specify a userid and password when connecting to a server from an application running on z/OS or OS/390. While this technique is not recommended for the best security, it is required for interoperability with many of the world wide web applications.

Note that the userid and password must be in host variables, so they are not in the SQL, the DBRM, the DB2 catalog, ...

Return Authid Information

- APAR PQ47973 in V6 & V7
- READS IFI Call to retrieve
 - Primary AUTHID USER
 - SQL AUTHID CURRENT SQLID
 - SECONDARY AUTHIDS
- IFCID 234 maps the information
- QMF V7.2 LIST TABLES
 - works with authority groups defined by DB2 secondary authorization IDs.

A function was added to DB2 V6 & V7 via APAR PQ47973 in late 2001. Customers have been asking for a technique that will return the list of secondary authids to a program. Customers can use the Instrumentation Facility interface or IFI to retrieve this information with a synchronous READS call. QMF V7.2 uses this function in the LIST TABLES command and provides a table UDF which makes the secondary ids available in SQL.

DB2 for z/OS Version 8 Security Outline

- Multilevel Security with Row Level Granularity
- Multilevel Security for Access Control
- Special Registers and Session Variables
- Encryption
- Other authorization changes
 - ▶ Materialized Query Tables
 - ▶ Sequences

This is the outline of security in DB2 for z/OS Version 8, with most of the information on multilevel security with row level granularity (second half of presentation).

Customers who use RACF access control can also use multilevel security with their access control.

Customers who need more flexible security can use the new special registers and session variables to provide secure information to views, triggers, stored procedures and UDFs.

Encryption has been used with DB2 for some time, but V8 adds some new encryption options. New objects in DB2 V8 materialized query tables (MQTs) and sequences have new authorization.

Session Variables

- Variables set by DB2, connection or signon exit
- Built in function to retrieve value for a variable
 - Use function in views, triggers, stored procedures & constraints to enforce security policy
- Can have more general, flexible access checks
 - Multiple columns, AND/OR logic, ...
- Complements other security mechanisms

```
CREATE VIEW V1 AS SELECT * FROM T1 WHERE  
COL5 = GETVARIABLE('SYSIBM.SECLABEL');
```

Session Variables provide another way to provide information to applications. Some variables will be set by DB2. Others can be set in the connection and signon exits to set these session variables

A new built-in function **GETVARIABLE** is added to retrieve the values of a session variable. This function can be used in views, triggers, stored procedures and constraints to help enforce a security policy. If your primary security need is more general, flexible controls, this information complements other security mechanisms.

For example, you can have a view which provides data that is at the user's current security label.

Session Variables ...

Set by DB2 SYSIBM.varname

- PLAN_NAME
- PACKAGE_NAME
- PACKAGE_SCHEMA
- PACKAGE_VERSION
- SECLABEL
- SYSTEM_NAME
- VERSION
- DATA_SHARING_GROUP_NAME
- SYSTEM_ASCII_CCSID
- EBCDIC
- UNICODE

Set by connection & signon exits

- Up to 10 variables SESSION.varname

The session variables set by DB2 are qualified by SYSIBM. You can get the plan name, package name, the user's seclabel, DB2 subsystem version and CCSID information. This information is useful for security controls, but programmers have other needs for this information as well. Customers can add up to ten variables, with the qualifier SESSION, by setting the name and value in the connection and signon exits. Both the name and the value allow up to 128 characters. Session variables can be accessed, but not changed, in applications.

New Special Registers

Client information for this connection

Provided by sqlseti, Java methods, RRS SIGNON & SET_CLIENT_ID

- CLIENT_ACCTNG accounting string
- CLIENT_APPLNAME value of application name
- CLIENT_USERID client user ID
- CLIENT_WRKSTNNAME workstation name

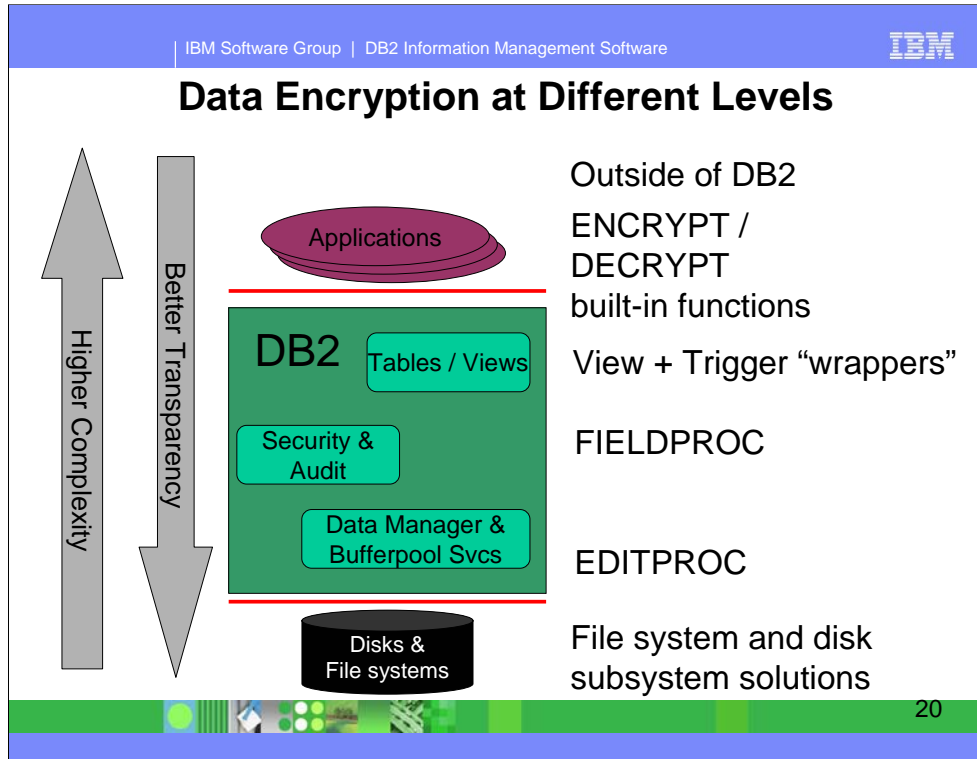
Four new SPECIAL REGISTERS are added to the product. These special registers are CLIENT_ACCTNG, CLIENT_APPLNAME, CLIENT_USERID, and CLIENT_WRKSTNNAME. The information is provided through a number of application programming interfaces. Similar special registers (without the underscore) were added to DB2 for Linux, UNIX & Windows, V8. Since applications can change the information, it is not as secure.

Cryptography and DB2: options

What do you want to protect? From whom? Effort?
Techniques, where to encrypt / decrypt

Outside of DB2 (ICSF, IBM Encryption for z/OS)	General, flexible, no relational range comparisons FOR BIT DATA
DB2 FIELDPROC	No relational range comparisons, FIELDPROC restrictions, FOR BIT DATA
DB2 EDITPROC (IBM tool)	indexes are not encrypted, EDITPROC restrictions
User-defined function or stored procedure	General, flexible, invocation needed, no relational range comparisons
SQL functions (DB2 V8)	General, flexible, invocation needed, no relational range comparisons
On the wire (DRDA V8, DB2 9: SSL, IPsec)	General, flexible
Tape Backup (z/OS, TS1120)	General, flexible, IBM hardware & software

There are many ways to encrypt data in DB2. The answers to the questions, "What do you want to protect and from whom?" and "How much effort can be used?" are generally needed to determine which technique to use and where to encrypt and decrypt. Encryption does mean some tradeoffs in function, usability and performance. Either the indexes are not encrypted or encrypted data will not give correct results for comparisons other than equals or not equals. All greater than, less than and range predicates are not usable. An EDITPROC is the most used technique, and one is provided to use cryptography hardware with an IBM Tool. The CMOS Cryptographic Coprocessors feature and ICRF hardware were designed to address high volume cryptographic transaction rates and bulk security requirements on z/OS. The Integrated Cryptographic Service Facility (ICSF) and the IBM Encryption Facility for z/OS provide the interfaces to service routines supported by the hardware, such as key management.
<http://www.ibm.com/servers/eserver/zseries/security/cryptography.html>



This diagram shows the range of places where data encryption can be performed. It is complementary to the prior page, which indicates some of the specific challenges.

If the applications are already written, then there is generally a very high need for transparency. But transparency means that some kinds of protection are not provided.

Some vendors address encryption as well.

Here are the primary references for encryption in DB2.

<http://www.ibm.com/support/docview.wss?uid=swg21168217>

<http://www.ibm.com/support/docview.wss?uid=swg27007844&aid=1>

<http://www.ibm.com/support/docview.wss?uid=swg27007842&aid=1>

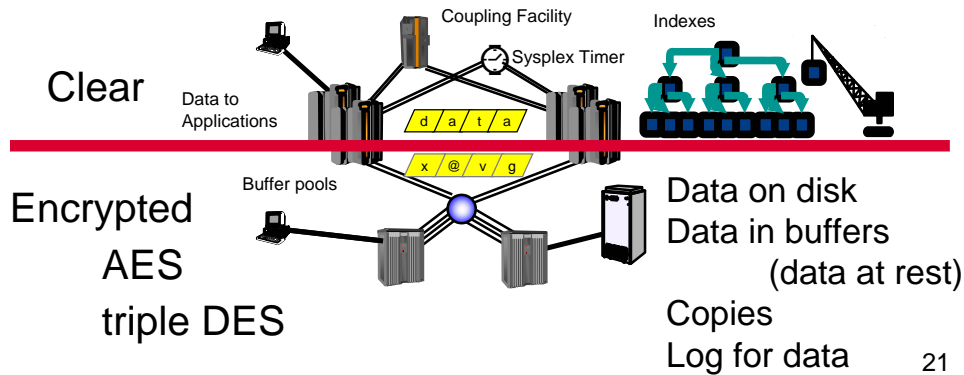
<http://www.ibm.com/developerworks/db2/library/techarticle/benfield/0108benfield.html>

<http://www.redbooks.ibm.com/redbooks/pdfs/sg247111.pdf>

sections 1.1.13 & 1.1.14

IBM Tool for DB2 EDITPROC and IMS Encryption

- Data encryption on disk, data at rest
 - Data on channel, in buffer pools are encrypted
 - Data to applications & indexes are not encrypted
- Existing authorization controls are unaffected



21

On this slide, data above the middle line is not encrypted and data below the line is encrypted.

In this example, the encryption is not providing an additional level of security for your DB2 or IMS applications. It is providing encryption of the data on the disk.

Once the data is brought, for example, into DBMS working storage, you are using the existing DB2 and IMS authorizations to secure data. As the data is written out to disk, that is once it leaves the channel and enters the network to move to the disk, the data is encrypted.

The example on this slide shows two subsystems with disks. The circle on the bottom half of the picture might be what we have known as an ESCON director in the past. The processor on the right hand side, below the line, might also be attached to that same I/O device; however, if the processor is a zSeries system that does not have the encryption key it will not be able to interpret the data.

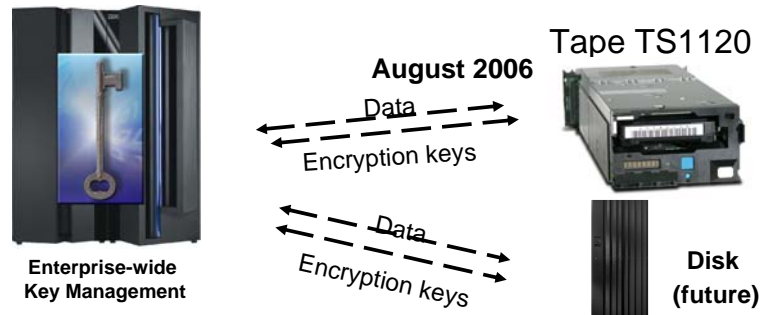
See the DB2 tools web pages for more about this.

<http://www.ibm.com/software/data/db2imstools/db2tools/ibmencrypt.html>

<http://www.ibm.com/software/os/zseries/telecon/14sep/>

Future Directions – Extending Encryption to IBM TotalStorage

- Statement of Direction: To address customers' growing concern with data security, IBM is announcing a statement of direction for the development, enhancement and support of encryption capabilities within storage environments such that the capability does not require the use of host server resources.
- This includes the intent to offer, among other things, capabilities for products within the IBM TotalStorage® portfolio to support outboard encryption and to leverage the centralized key management functions planned for z/OS ICSF.



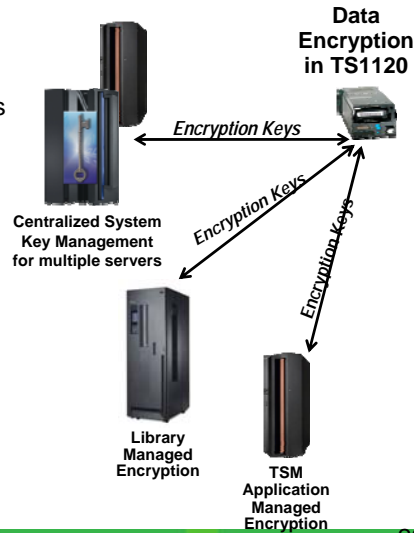
Statement of Direction: To address customers' growing concern with data security, IBM is announcing a statement of direction for the development, enhancement and support of encryption capabilities within storage environments such that the capability does not require the use of host server resources.

This includes the intent to offer, among other things, capabilities for products within the IBM TotalStorage® portfolio to support outboard encryption and to leverage the centralized key management functions planned for z/OS ICSF. The first part of this statement of direction is delivered in the TS1120 announced in August 2006.

The rest of the statement of direction is beyond currently announced products, including DB2 9.

TS1120 Tape Drive Encryption

- High performance tape drive encryption
 - Cost effectively encrypt large quantities of tape data
 - Avoid Host MIPS encryption overhead
 - Minimize impact to existing processes and applications
- Variety of implementation methods
 - System managed
 - Library managed TS3500 Tape Library
 - Application managed
 - IBM Tivoli® Storage Manager
- Supported in a wide range of environments including: z/OS™, i5/OS™, AIX®, HP, Sun, Linux and Windows



23

The IBM System Storage TS1120 Tape Drive has been enhanced to provide the customer the option of using drive based data encryption. This encryption capability is now standard on all new TS1120 Tape Drives and is a chargeable upgrade feature for existing installed TS1120 Tape Drives. The encryption capability includes drive hardware as well as microcode additions and changes. Also being introduced is a new, separate IBM Encryption Key Manager component for the Java Platform(TM) program that supports the generation and communication of encryption keys for the tape drives across the enterprise.

The TS1120 based encryption and associated Encryption Key Manager component are supported in a wide variety of operating system environments including z/OS, i5/OS, AIX, HP, Sun, Linux and Windows. In addition, three different encryption management methods are supported: Application, System, or Library Managed. This encryption capability is supported when the TS1120 Tape Drive is integrated or attaches in the IBM System Storage TS3500 Tape Library, IBM System Storage TS1120 Tape Controller Model C06, IBM TotalStorage 3592 Tape Controller Model J70, IBM TotalStorage 3494 Tape Libraries, IBM TotalStorage C20 Silo Attach frame, and standalone environments. For more information on encryption please see:

http://www.ibm.com/servers/eserver/zseries/zos/pdf/White_Paper_ESG_System_z_final.pdf

IBM Software Group | DB2 Information Management Software IBM

Don't let the next headline be you

TECH DISPENSER
Tech blogs filtered by humans, *not* bots

COMPUTERWORLD

Security

JUMP TO
SEARCH

- Home
- News
- E-mail Newsletters
- Tech Dispenser
- + Shark Bait
- Knowledge Centers
 - + Operating Systems
 - + Networking & Internet
 - + Mobile & Wireless
 - Security
 - Cybercrime & Hacking
 - Spam, Malware & Vulnerabilities
 - Security Hardware & Software
 - Standards & Legal Issues
 - Privacy
 - Intellectual Property & DRM
 - Disaster Recovery
 - + Storage
 - + Business Intelligence

Missing UK bank customer data was not encrypted

It should have been, and it shouldn't have shipped via regular mail either

Tash Shifrin [Today's Top Stories](#) or [Other Security Stories](#)

Comments (0) Recommendations: 5 — [Recommend this article](#)

June 06, 2007 (Computerworld UK) – A lost disk holding confidential data on 62,000 HBOS banking group mortgage customers was not encrypted -- although it should have been, the bank has admitted.

The bank had promised to learn lessons and overhaul its procedures after a similar loss of customer data in March, but said the second loss was "unrelated" because the data had gone missing in a different way.

This month's data breach included names, addresses, dates of birth and mortgage account numbers on a CD-ROM sent by HBOS subsidiary Bank of Scotland to a credit reference agency. It was **reported** missing when the agency did not receive the expected monthly dispatch of information.

An HBOS spokesperson confirmed: "The disk would usually be encrypted. Unfortunately, due to human error on this occasion the usual policy was not followed. We apologize to our customers for this."

The bank also confirmed that although disks were usually sent out using a secure post service, the missing disk had been sent through

IS YOUR DATA

MORE RELA'

- Ultramobiles hungry, AMF
- Parallels Det released
- Computex: Ir graphics chi

TODAY'S TO

- Microsoft s for next wi
- Beyond iPh gadget trer
- Offshore fi settle H_1R

24

You don't want the next headline to be yours. The costs are simply too high in terms of disclosure and lost customers. The costs are too low to encrypt anything which might be sent outside the secure vault.

IBM Software Group | DB2 Information Management Software IBM

Extending Mainframe Encryption to Tape *Encryption Facility for z/OS*

Centralized Key Management

Mainframe Encryption Services
 Encryption hardware
 Centralized key management
 Encryption standards (AES, TDES, SHA-256)

Compressed & Encrypted Tape

Partner, customers, branch office with z/OS mainframe

Encrypt and decrypt with Java client

Partners, customers

Archiving

Compressed & Encrypted Tape

Compressed & Encrypted Tape

MFE_120

Improvements in encryption come in our new processors and in new operating system releases, as well as in new products and new releases of software.

Here are the primary references:

<http://www.ibm.com/servers/eserver/zseries/security/>

<http://www.ibm.com/servers/eserver/zseries/security/cryptography.html>

http://www.ibm.com/servers/eserver/zseries/zos/encryption_facility/

http://www.ibm.com/servers/eserver/zseries/security/ccs_certification.html

<http://www.ibm.com/servers/eserver/zseries/zos/>

<http://www.ibm.com/servers/eserver/zseries/zos/racf/>

<http://www.ibm.com/servers/eserver/zseries/security/mls.html>

IBM Software Group | DB2 Information Management Software IBM

Further Advances in Mainframe Encryption

Data and transactions on the Internet

Heterogeneous systems ← → Heterogeneous systems

Mainframe Encryption Services		
Open Internet encryption services	Encryption hardware Centralized key management	Open tape encryption services
<p>Internet encryption advances New in z/OS 1.7</p> <ul style="list-style-type: none"> • Application Transparent TLS <ul style="list-style-type: none"> • Facilitate Internet encryption of mainframe applications and data transfers • Can enable TLS or SSL protocols without necessarily modifying applications • Can improve IPsec performance 	<p>Encryption hardware advances</p> <ul style="list-style-type: none"> • <i>Cryptographic Express2 Coprocessor</i> <ul style="list-style-type: none"> • Can improve performance and scale • Available with System z9, z990 and z890 • Enhanced CPACF performance for TDES & support for AES-128 and SHA-256 (requires z9) <p><i>Statement of Direction for z9 servers:</i> <i>Remote Key loading of ATMs</i></p> <ul style="list-style-type: none"> • Can change ATM keys without manual process 	

Statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only

MFE_130

These are the most recent improvements in encryption coming in our new processors and in operating system releases.

Here are the primary references:

<http://www.ibm.com/servers/eserver/zseries/security/>

<http://www.ibm.com/servers/eserver/zseries/security/cryptography.html>

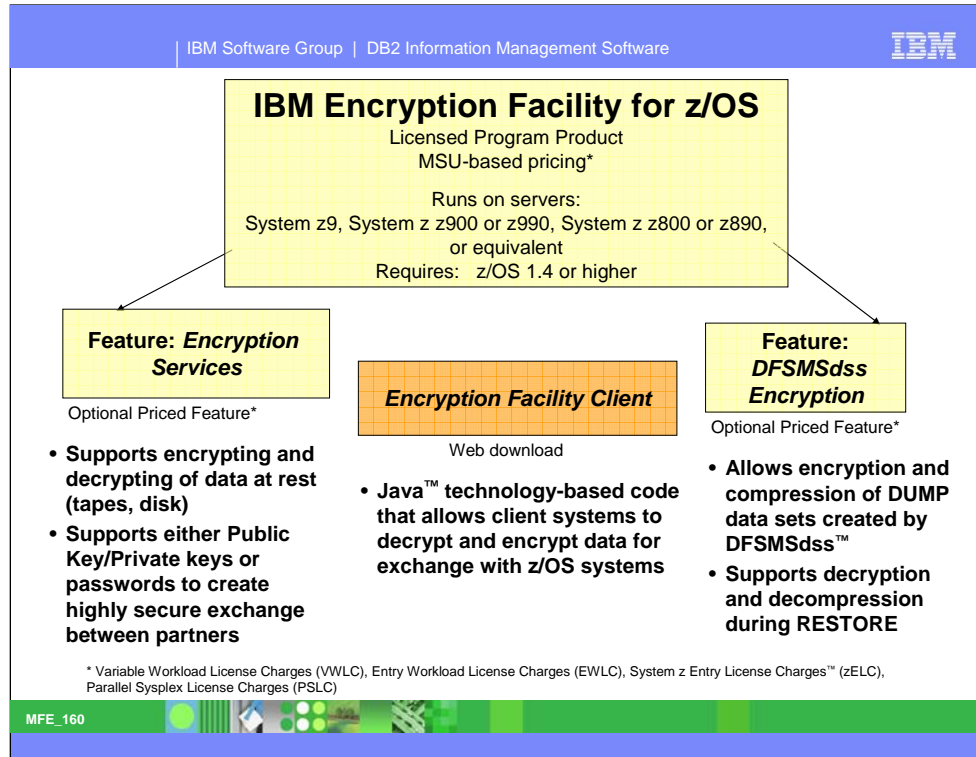
http://www.ibm.com/servers/eserver/zseries/zos/encryption_facility/

http://www.ibm.com/servers/eserver/zseries/security/ccs_certification.html

<http://www.ibm.com/servers/eserver/zseries/zos/>

<http://www.ibm.com/servers/eserver/zseries/zos/racf/>

<http://www.ibm.com/servers/eserver/zseries/security/mls.html>



See the web for this encryption facility. The Encryption Services feature supports encrypting and decrypting of data at rest (tapes, disk) and supports either Public Key/Private keys or passwords to create highly secure exchange between partners .

The Encryption Facility Client is Java™ technology-based code that allows client systems to decrypt and encrypt data for exchange with z/OS systems.

The DFSMSdss Encryption feature allows encryption and compression of DUMP data sets created by DFSMSdss™. It supports decryption and decompression during RESTORE.

* Variable Workload License Charges (VWLC), Entry Workload License Charges (EWLC), System z Entry License Charges™ (zELC), Parallel Sysplex License Charges (PSLC)

http://www.ibm.com/servers/eserver/zseries/zos/encryption_facility/

http://www.ibm.com/common/ssi/rep_ca/3/897/ENUS205-243/ENUS205-243.PDF

Materialized Query Table (MQT) Authorization V8

- Use of MQT may be implicit or explicit
 - Explicit use requires MQT authorization
 - Implicit use requires base table or view authorization.
- Creation of table requires CREATE TABLE authorization and SELECT to base table or view
 - DBADM can create MQT for another authorization ID
- REFRESH TABLE authorization
 - Ownership of MQT, DBADM, DBCTRL, SYSADM or SYSCTRL

The materialized query table is often a summary table. DB2 optimization can rewrite a query on the base tables to use the MQT. No authorization on a MQT is required for it to be used in automatic query rewrite or implicitly.

Authorization: To ALTER, the privilege set that is defined below must include at least one of the following:

The ALTER privilege on the table

Ownership of the table

DBADM authority for the database

SYSADM or SYSCTRL authority

Additional privileges might be required when FOREIGN KEY, DROP PRIMARY KEY, DROP FOREIGN KEY, or DROP CONSTANT is specified; the data type of a column that is added to the table is a distinct type; or a fullselect is specified.

Sequence Authorization V8

- **CREATE:** CREATEIN for schema, SYSADM or SYSCTRL
- **ALTER:** Ownership, ALTER for sequence, ALTERIN for schema, SYSADM or SYSCTRL
- **DROP:** Ownership, DROPIN for schema, SYSADM or SYSCTRL
- **COMMENT:** Ownership, ALTER for sequence, ALTERIN for schema, SYSADM or SYSCTRL
- **GRANT & REVOKE:** ALTER & USAGE
 - **USAGE:** NEXT VALUE or PREVIOUS VALUE expression used

The sequence is a new DB2 object, and these new SQL statements require authorization. The USAGE privilege for the sequence will be the most common privilege, I expect.

There are new authorization rules for data definition and for use of this new function.

DB2 Command Control Improved

- DB2 commands – using GRANTs
- When signed on console, jobs, TSO SDSF, ...
- Signed on id used, rather than SYSOPR
 - ▶ Not compatible
- Need to GRANT proper authorization e.g. SYSOPR, DISPLAY, ...
- Options for commands (secondary ids are new)
 - ▶ Grant access to primary or **secondary** authids
 - ▶ Grant access to public
 - ▶ Use exit or RACF authorization control for commands

Access control is improved for DB2 commands, whether or not RACF access control is used. While there is an improvement, the change is not completely compatible, and customers need to be sure that the appropriate authorization is GRANTED. Grants could only use the primary authorization id for commands before, but the ability to use secondary ids is added in V8. Some alternatives would be granting access to the individual ids, granting access to public or using the Access Control Authorization Exit or RACF control of commands (see next page).

Other authorization changes

- Schema evolution means alter, instead of drop, so we don't need to save and regrant authority.
- If the select-statement contains an INSERT statement, then INSERT & SELECT privileges on the target table or view are required.
- Access Control Authorization Exit changed substantially
 - RACF version shipped with DB2, SDSNSAMP
 - Exit for prior versions are not usable
 - long names, new objects, ...

For some database administrators, the biggest change in authorization will be the ability to avoid the cascade revoke caused by deleting a table or table space to change attributes. Being able to ALTER is faster, more available and safer.

The RACF access controls are changed very substantially. The exit has additional capabilities for sequences, and changes in the interface to handle long names. The exit is provided names converted from Unicode to EBCDIC. While the RACF exit has been shipped by RACF in SYS1.SAMPLIB, now it will come with DB2 in prefix.SDSNSAMP.

Summary of DB2 for z/OS V8 Security

Very significant changes for increased

- ✓ Security
- ✓ Flexibility
- ✓ Integration
- ✓ Ease of use for safe security
- ✓ Assurance



Everyone seems to be more aware of security today. Improving integration and making security more robust and easier to manage are very important. Customers asked for a wide range of enhancements for security. New options for tighter security, more granularity, and more information for additional flexibility in applications and SQL are needed. Improved integration with the hardware and software platform provide a better end-to-end solution. The design point for DB2 security is being easy to use for safe security, with solid system security and some security that is more flexible, that we'll call application security. Finally, it will be helpful to see what assurance can be provided, such as certification.

Security work DB2 9 for z/OS

Some key implementations

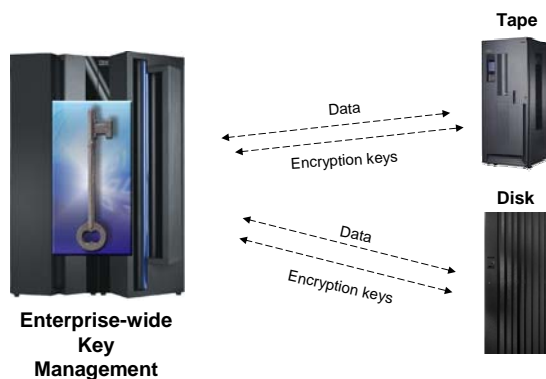
- Roles
- Network Trusted Contexts
- Instead of Triggers
- Improved auditing
- Secure Socket Layer
- Data Encryption



While DB2 for z/OS V8 provides many enhancements for security, there are still many more needs and much more work to do. While we cannot commit to a specific delivery, the work is in many different areas. Roles are used to provide a more flexible technique than users and groups in assigning and controlling authorization, while improving consistency with the industry. A network trusted context provides a technique to work with other environments more easily, improving flexibility. The instead of trigger is an SQL technique that allows a trigger to be used in place of a view. Improved audit selectivity is needed for being able to see that security is functioning. Secure Socket Layer implementation provides encryption of data on the wire. Some additional techniques for data encryption will help protect data at rest and in backups.

Protecting data on disk

- Allow encryption for key DB2 disk resources:
 - Tables
 - LOBs
 - Indexes
 - Image copies
 - Logs
 - Archive logs



Encryption is a significant technology for the System z9 and System z platform. There are new facilities that have just been provided and more work is coming. See the encryption section earlier.

Database ROLES

- ROLE is a “virtual authid”
 - Assigned via TRUSTED CONTEXT
 - Provides additional privileges only when in a trusted environment using existing primary AUTHID.
 - Can optionally be the OWNER of DB2 objects

```
CREATE ROLE PROD_DBA;  
GRANT DBADM ... TO PROD_DBA;  
  
CREATE TRUSTED CONTEXT DBA1 ...  
  DEFAULT ROLE PROD_DBA OWNER(ROLE);
```

Database role: A database role is a virtual authorization ID that is assigned to the user via the context mentioned next. DB2 privileges are assigned to the defined role.

The role exists as an object independent of its creator, so creation of the role does not produce a dependency on its creator.

This capability can allow a DBA to have privileges to create objects and manage them for a time, even though ownership is to be another id.

The role can be assigned and removed from individuals via the trusted authorization context as needed. This allows a DBA to perform object maintenance during a change control window on a Saturday night, for example. But when Monday arrives, they do not have the authority to do this same work.

Auditing trails of the work completed during the maintenance window are available for verification by a security administrator or auditor.

Database ROLES Examples

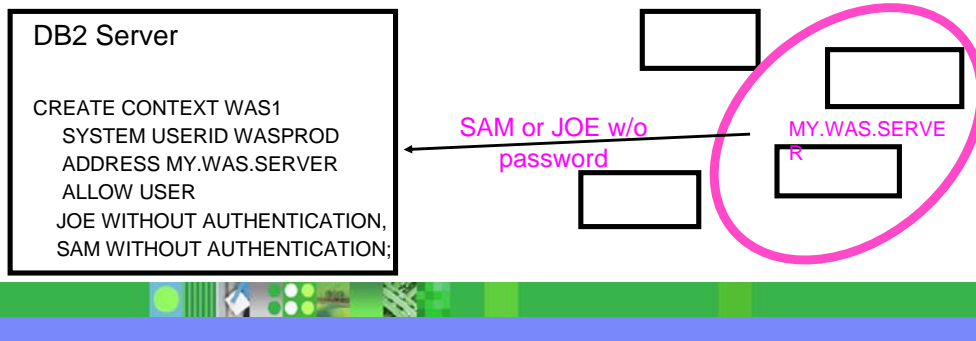
- Dynamic SQL access to DB2 tables using JDBC or CLI, but only when running on a specific server.
- DBA can be temporarily assigned a DBA ROLE for weekend production table admin work – no table access at other times.
- DBA uses a ROLE for CREATE statements, so that the ROLE owns the objects he or she creates.
- Project librarian assigned a BIND ROLE only when running on the production code library server – can't BIND from any other server.

The Trusted Context and ROLE support can be used to implement DBA privileges that can easily be disconnected and reconnected to individual employees. This provides function similar to shared SYSADM or DBADM userids, but avoids the audit compliance problems associated with shared userids. The ROLES have the ability to “own” DB2 objects, so that revoking a person’s ROLE does not cause the objects to be cascade deleted.

With these capabilities, customers are able to create DBA procedures that can be audited and protected so that one individual cannot violate the established rules without being detected during the audit review.

Trusted Security Context

- Identifies “trusted” DDF, RRS Attach, or DSN application servers
- Allows selected DB2 authids on connections without passwords
 - reduces complexity of password management
 - reduces need for an all-inclusive “system authid” in app servers
 - more visibility/auditability of which user is current running
 - enables mixed security capabilities from a single app server

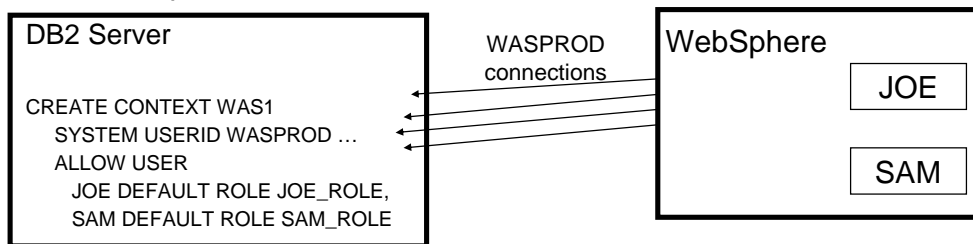


Trusted security context: Today, you have the option to set a system parameter which indicates to DB2 that all connections are to be trusted. It is unlikely that all connection types, such as DRDA, RRS, TSO, and batch, from all sources will fit into this category. It is likely that only a subset of connection requests for any type and source may be trusted or that you want to restrict trusted connections to a specific server. More granular flexibility will allow for the definition of *trusted connection objects*.

Once defined, connections from specific users via defined attachments and source servers will allow trusted connections to DB2. The users defined in this context can also be defined to obtain a *database role*.

Trusted Security Context / ROLE WebSphere example

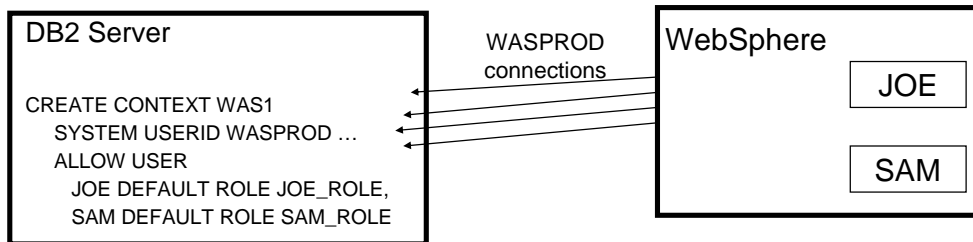
- WebSphere connection pool can be created with one DB2 AUTHID
- WebSphere can reuse pooled connections to DB2 with different AUTHIDs
- DB2 AUTHIDs can be given privileges that are only available when executing in WebSphere:
 - ✓ e.g. dynamic SQL access for JDBC only when using WebSphere



ROLES and Trusted Context can be used to provide added security for your network-attached application servers. These new capabilities allow the DBA to make GRANT statements conditional, so that they can only be used from a specified list of IP addresses. If someone steals the application server's userid/password, they won't be able to access the database unless they are also able to execute the SQL statement on one of the approved application servers.

Trusted Security Context / ROLE WebSphere example

- WebSphere connection pool can be created with one DB2 AUTHID
- WebSphere can reuse pooled connections to DB2 with different AUTHIDs
- DB2 AUTHIDs can be given privileges that are only available when executing in WebSphere:
 - ✓ e.g. dynamic SQL access for JDBC only when using WebSphere



ROLES and Trusted Context can be used to provide added security for your network-attached application servers. These new capabilities allow the DBA to make GRANT statements conditional, so that they can only be used from a specified list of IP addresses. If someone steals the application server's userid/password, they won't be able to access the database unless they are also able to execute the SQL statement on one of the approved application servers.

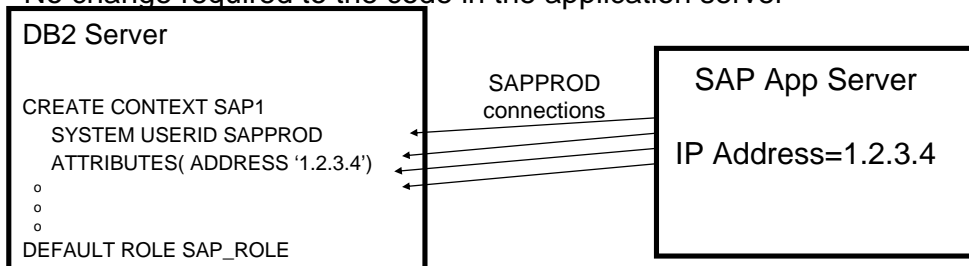
Improved audit: DB2 Trace Filtering

- New filtering capabilities for `–START TRACE` that `INCLUDE` or `EXCLUDE` based on these keywords:
 - USERID -- client userid
 - WRKSTN -- client workstation name
 - APPNAME -- client application name
 - PKGLOC -- package LOCATION name
 - PKGCOL -- package COLLECTION name
 - PKGPROG -- PACKAGE name
 - CONNID -- connection ID
 - CORRID -- correlation ID
 - ROLE – end user's database ROLE

Improved trace filtering makes the job of auditing and of performance management easier.

Example 1: ROLES and Trusted Context used to Secure App Servers

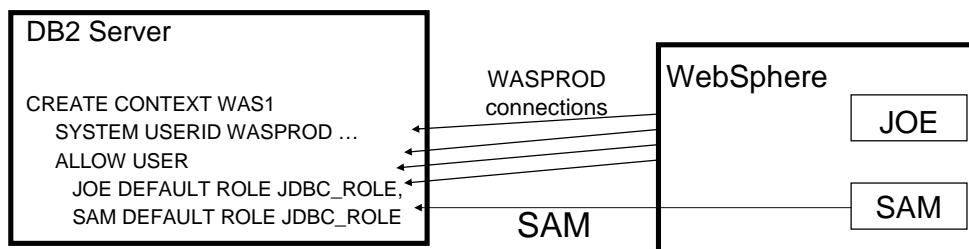
- Most existing application servers connect to DB2 using userid/password pairs:
 - Significant exposure if someone steals the userid/password!!!
- Trusted Context and ROLES can be used to limit exposure:
 - GRANTs to SAP_ROLE can be restricted so that they are only valid when used by a valid SAP app server IP address
- No change required to the code in the application server



ROLES and Trusted Context can be used to provide added security for your network-attached application servers. These new capabilities allow the DBA to make GRANT statements conditional, so that they can only be used from a specified list of IP addresses. If someone steals the application server's userid/password, they won't be able to access the database unless they are also able to execute the SQL statement on one of the approved application servers.

Example 2: ROLES and Trusted Context for Dynamic SQL Auditing

- Better auditing controls:
 - GRANT dynamic SQL privileges to a ROLE
 - End user identity can be delegated directly to DB2 without granting dynamic SQL privileges directly to the end user
 - End user passwords can be optional.
 - No added complexity for administration of GRANTS, while retaining the ability to audit the end user's identity!!!



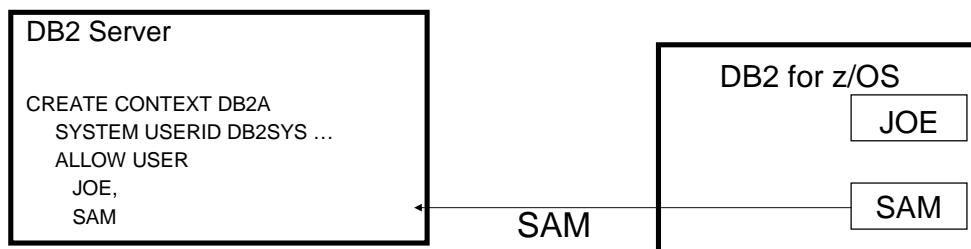
ROLES and Trusted Context also enable customers to improve DB2 system auditing. Today, many customers use a “system” userid to access DB2 so that they don’t have to grant dynamic SQL privileges to their end users. A second benefit to the system userid is connection pooling in the application server.

With DB2 9, customers will be able to grant dynamic SQL table privileges to a ROLE, and specify that the end user can only use that ROLE when the end user is running on an approved application server. This has several benefits:

- A ROLE can be used as a single database authid that can be used to simplify administration of dynamic SQL privileges.
- The end user’s authid can be used to run database transactions, so that the DB2 audit is able to identify the end users individually (important capability for meeting some regulatory compliance requirements).
- The Trusted Context retains many of the performance benefits of connection pooling, while eliminating the restriction that a single authid (the system authid) must be used for all the uses of the connections in the pool.

Example 3: ROLES and Trusted Context for Already-Verified DRDA

- Can be used to establish already-verified TCP/IP connections:
 - Improves ability to replace SNA connections with TCP/IP
 - Communication Database is used to identify trusted connections and specify “system userid” for the Trusted Context
 - End user identity is automatically propagated from one DB2 system to the other.



Many customers would like to migrate from SNA and PRIVATE protocol to a solution based on TCP/IP and DRDA protocol. Prior to DB2 9, lack of already-verified support in TCP/IP prevented many customers from migrating to DRDA. With Trusted Context and changes to the Communication Database (CDB) in DB2 9, customers will now be able to identify DB2 servers that are trusted to send already-verified connection requests.

Example 4: ROLES and Trusted Context to Secure DBA Activities

- Many customers are concerned about DBA access to sensitive customer data. DB2 9 can help by enabling an auditable DBA process:
 1. Grant DBA privileges to a ROLE, Audit role
 2. When a DBA needs to perform a system change:
 - Use Trusted Context to assign DBA ROLE to person
 - DBA is given request and performs activity
 - Revoke Trusted Context
- Have another person review the audit trace

The Trusted Context and ROLE support can be used to implement DBA privileges that can easily be disconnected and reconnected to individual employees. This provides function similar to shared SYSADM or DBADM userids, but avoids the audit compliance problems associated with shared userids. The ROLES have the ability to “own” DB2 objects, so that revoking a person’s ROLE does not cause the objects to be cascade deleted.

With these capabilities, customers are able to create DBA procedures that can be audited and protected so that one individual cannot violate the established rules without being detected during the audit review.

DB2 Security Summary

Extensive controls

- Constructs: database, table, view, plan, package, ...
 - Constructs are related. Dropping database includes tables, authorization ...
- Dynamic: User to data or Static: User to plan and plan to data
- Groups and administrative authorities
- Discretionary and mandatory access controls

Integrated with database management system

- GRANT, REVOKE, VIEWS in SQL
- Views can limit access to field, content level
- System catalog tables can be queried, construct dependencies managed
- Encryption supported for data at rest, on wire, in functions

Extensive audit for security and table access

Connections to many environments

- Web, Batch, TSO, IMS-TM, CICS, ...
- Use RACF for ids, connect, data set protection
- Option to use RACF for access control

DB2 has extensive, granular controls for DB2 security. DB2 security covers the database objects and access. The data and application objects are related and dependencies are managed. Discretionary and mandatory access controls are provided.

DB2 access controls include both users direct to the data and indirect with user to plan or package to data checking. Plans and packages provide a cache of authority.

DB2 security is very tightly integrated with the DBMS in the language, views, catalog tables, data integrity and monitoring. DB2 audit controls are strong.

Connections to many environments does add complexity, but using RACF or the Security Server for ids, connection controls, and protection of the underlying data sets helps. Customers have the option of using RACF for access control as well.

Z39 - PART 2

IBM

IBM Software Group

DB2® for z/OS Security: Protect Your Assets Using RACF for Security

DB2 Information Management Software

Roger Miller
DB2 for z/OS Development
IBM Silicon Valley Lab

@business on demand software

This is a presentation of DB2 for z/OS Security, starting with the objects, describing their relationships and discussing techniques for security and auditing. The first part of the session will discuss native DB2 security. This presentation starts at the DB2 V6 level and includes information about changes in DB2 Version 7 and beyond.

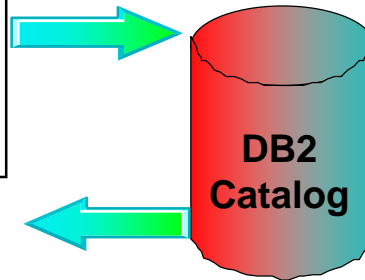
The second part of the session will focus on the DB2 option to use RACF or the z/OS Security Server for access control. This session will begin with discussing whether to choose this option. DB2 has always relied upon operating system identification and authentication, but has separate SQL mechanisms for access control that provides integration with the database management system. It is very important to understand the relationships and the integration if you make choices about DB2 security.

Native DB2 Authorization

SQL - Data Control Language

```
GRANT ALL ON CUSTOMER  
TO NATIONAL_SALES, MARY, TED  
  
GRANT SELECT ON SW_CUSTOMER  
TO SW_SALES, JOHN  
  
REVOKE SELECT ON SW_CUSTOMER  
FROM NE_SALES, JANE
```

Access controls check for granted authority.



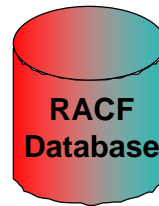
Native DB2 authorization uses the grant and revoke statements to keep the information in the DB2 catalog. Checking access means checking the DB2 catalog.

DB2 access control uses tight integration with DB2 and database integrity techniques to provide robust security. There will not be a security rule granted without a related object in most situations. For some customers and security needs, these techniques do not fit.

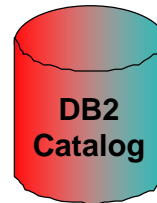
In 2007, we estimate that more than 95% of customers use native DB2 authorization.

DB2 Authorization with RACF

RACF Permits
27 new classes



SQL - Grants & Revokes



Access controls check both RACF and DB2 for authority. So you can migrate to RACF access control selectively.

Administrators must understand DB2 objects and privileges. This technique has less integration with DB2.

There are significant policy and people implications when using RACF access control. If you want the database administrators to manage security, then integration with DB2 is very important. If you want security administrators to manage security, then integration with the security server and the ability to have separate security and database administration are more important. The change to RACF access control, causes roles to change and authorities to change. Converting to RACF from DB2 security is not a completely compatible change. Authority based on secondary IDs, such as BINDAGENT, requires a new technique under RACF. There are some situations where DB2 access control must be used. V8 removed one situation where DB2 GRANT was needed, for DB2 commands. If you want a security group to define authorization and a centralized security control point, then RACF access control is a match.

Plan to use RACF facilities in a similar manner to groups and patterns. The implementation team requires both DB2 and RACF knowledge for implementation. If you want a security group to define authorization and provide a centralized security control point, then RACF access control is a match. As you implement RACF, plan to use security access patterns instead of access authorities on individual items. The implementation team needs both DB2 and RACF skills.

The DB2 Administration Guide appendix Writing Exit Routines has a section, **Access control authorization exit routine** with more detail on this exit, titled "**Is this exit routine right for you?**" The Protect Your Assets presentation discusses use of RACF. The RACF Access Control Module Guide has guidance on the implementation which can affect your choice.

RACF Authorization Agenda

- **Requirements**

- ▶ Which customers does this method fit?

- **Mapping DB2's controls to RACF**

- ▶ DB2 object types to RACF classes
- ▶ DB2 privileges (e.g. database, system, table)
- ▶ DB2 administrative authorities (e.g. SYSADM)
- ▶ DB2 Version 7 and 8 Improvements

- **Installation, Customization & Migration**

- **Considerations, Concerns, & Requirements**

This is the agenda for discussing use of RACF access control with DB2. We'll discuss which customer requirements match well with RACF and which match with DB2 native authorization.

The RACF controls are similar to those in DB2, but there are some differences. There are separate sections for the changes in V6 and V7.

There are many options and choices to consider in implementing access control via the Security Server.

Requirements

- **Provide the ability to control DB2 resources from RACF, specifically the ability to:**
 - Define pattern to define authorization rules
 - Define security rules before object is created
 - Preserve security rules for dropped objects
 - Control and audit resources for multiple DB2 subsystems from single point
 - Administer DB2 security with minimum DB2 skill
 - Eliminate DB2 cascading revoke
 - Use RACF userids and groups directly
- **Provide an exit point which can control access to DB2 resources**

This is a list of some requirements that can be satisfied using RACF access control for DB2.

Here are some additional ones.

Eliminate the ability to define duplicate security rules

Separate Control rights from Access rights

Validate authIDs before granting DB2 authorities

Notes: What Does This do for me?

- Using RACF for access control provides several advantages over native DB2 controls, including:
 - ▶ Reducing the number of authorization rules that are required to implement your installation's security policy, which reduces administrative complexity and reduces the work required to create and maintain your access control policy.
 - ▶ Providing a more flexible access control mechanism.
 - ▶ Cascading revocations are eliminated.
 - ▶ Access rules can be defined before a DB2 object is created.
 - ▶ Access rules are preserved when a DB2 object is dropped.
 - ▶ RACF's groups can be used for access control, eliminating one of the common reasons for a secondary auth ID exit.
 - ▶ Consolidated security administration and audit for multiple DB2 subsystems or data sharing groups.
 - ▶ Consolidation of security administration within the security administration organization.
 - ▶ Consolidation of DB2 audit data with RACF audit data.
 - ▶ Access control can be made the responsibility of the external security manager, without having to make modifications to DB2 code.

There are many advantages to using RACF directly for access control, but there are also some disadvantages, as we will see on the next pages.

When to look at this change

- **Policy and people implications**

- Roles will change
- Authorities will change
 - ▶ Use RACF facilities more, e.g. groups & patterns
 - ▶ Not a completely compatible change
- Need both DB2 & RACF knowledge for implementation and for administration
- Mix of RACF and DB2 Authorization

- **Security group should define authorization**

- **Centralized Security Control Point**

- **Use patterns instead of individual item access authorities**

The choice of using RACF for access control is not for everyone. There are significant policy and people implications. If you want the database administrators to manage security, then integration with DB2 is very important. If you want security administrators to manage security, then integration with the security server and ability to separate security administration from database administration are more important. As you make this change, note that roles will change and authorities will change.

You should plan to use RACF facilities more, like groups and patterns. The implementation team needs both DB2 and RACF knowledge and skills.

If you want a security group to define authorization and a centralized security control point, then RACF Access Control is a good match. As you implement, plan to use patterns instead of individual item access authorities.

RACF and DB2 Solution

● DB2 - Access Control Authorization Exit Point

- A new exit point documented by DB2
- Exit point is driven:
 - ▶ Once at subsystem startup
 - ▶ For each DB2 authorization request
 - ▶ Once at subsystem Termination
- Exit CSECT Name - DSNX@XAC
- Exit parameter list - DSNDXAPL
- DB2 Provides dummy DSNX@XAC routine

● RACF - The RACF/DB2 External Security Module

- Fully supported exit module designed to receive control from the DB2 Access Control Authorization Exit Point

The solution to the problem of interfacing multiple subsystems was addressed by using an exit in DB2, with the exit code provided by the RACF or Security Server.

The resulting interface provides function that is similar to DB2 security, while using the Security Server or RACF function of z/OS or OS/390, rather than DB2 tables.

Mapping DB2 Authorization Checks

- **DB2 security mechanisms consist of several constructs:**
 - Objects, e.g. tables, databases
 - Privileges, e.g. insert, update, select
 - Administrative authorities, e.g. DBADM, SYSADM
- **Authorization will be mixture of RACF & DB2**
 - If RACF identifies the user and object, RACF authorization is used.
 - If RACF does not identify the user or object, DB2 authorization is used.
 - If RACF is not functional, DB2 authorization is used or DB2 V7 option to stop DB2.

The DB2 security mechanisms include specific objects, privileges on those objects and some privileges which provide broader authority.

Objects, such as tables, views, table spaces, databases, etc.

Privileges, such as insert, update, select, etc.

Administrative authorities, such as DBADM, SYSADM, etc.

When you use RACF authority, you also use DB2 authorities in some cases. If RACF can identify the user and has a profile for the object, then RACF authority is used. If RACF cannot identify the user (no ACEE is passed) or if RACF has no profile for the object, then DB2 access control is used. DB2 administrative authorities are also checked.

If RACF is not functional, DB2 authorization is used, or in DB2 V7, an option is provided to stop DB2.

Mapping DB2 Checks...

- **How are DB2 authorization checks mapped to RACF?**
 - DB2 objects (table, database, view) correspond to RACF general resource classes
 - DB2 privileges are a part of RACF profile names
 - DB2 administrative authorities are profiles within RACF general resource classes

The DB2 authorization checks use RACF general resource classes that correspond to the DB2 objects.

The DB2 privileges are more specialized than the RACF ones, so they are included as part of the resource name.

The DB2 administrative authorities also have profiles within other RACF resource classes.

DB2 Object Types

DB2 Object Types

Table, Index, View, Trigger

Database

Subsystem or data sharing group

Plan, Package, Collection

Stored Procedure, User-Defined Function

Java ARchive (JAR) (V7)

Distinct Type

Storage Group

Bufferpool

Table Space

Schema

These are the primary object types in DB2. SQL statements and commands can create and alter the objects.

Most security definitions are for the key data and application structures. We'll be explaining them more in the next set of slides.

Tables and views are the primary objects for authorization. They are the basic building block for relational database.

Database level authorization is used for utilities and for creation of objects. This is generally the need for a DBA.

Plans and packages are the application structures. Static SQL is checked when it is compiled or bound.

Subsystem level authorization is required for administrative tasks and for work that can affect other users.

RACF / DB2 Class Names

<u>DB2 Object Type</u>	<u>RACF Class Name</u>
Bufferpool	MDSNBP
Collection	MDSNCL
Database	MDSNDB
Package	MDSNPK
Plan	MDSNPN
Storage Group	MDSNSG
System	MDSNSM
Table / Index / View	MDSNTB
Table Space	MDSNTS

The RACF class names map to the DB2 objects in a fairly straightforward way.

The MDSN indicates use for DB2, while the last two characters indicate the specific resource or object type.

The above classes are defined in the IBM supplied Class Descriptor Table. In addition, for each member class, there is also a grouping class profile defined. The first character is M for a member class and G for a grouping class.

Scope of RACF Classes

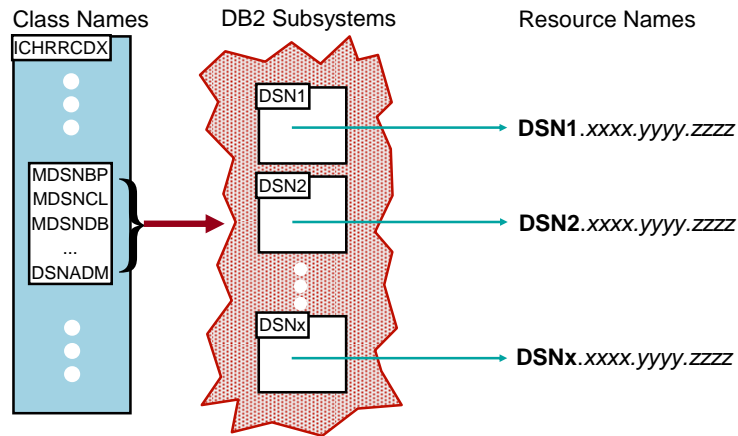


- Multi-Subsystem Scope (default)
 - ▶ One set of general resource classes for multiple subsystems
 - ▶ Names prefixed with DB2 data sharing group or subsystem name
 - ▶ Classes provided
 - ▶ Why? Protect multiple subsystems with single set of resource profiles, Fewer classes overall
- Single Subsystem Scope (an option)
 - ▶ One set of general resources classes per subsystem or data sharing group
 - ▶ Names not prefixed
 - ▶ Classes must be defined by the installation
 - ▶ Why? Segregates resources by subsystem, Fewer profiles per class

Multi-Subsystem Scope (default). Most customers choose this option. One set of general resources classes can protect multiple subsystems. General resource names are prefixed with the specific DB2 data sharing group or subsystem name. Classes provided in the IBM supplied CDT are multi-system scope. The primary reason for this choice is to protect multiple subsystems with a single set of resource profiles and to have fewer classes overall.

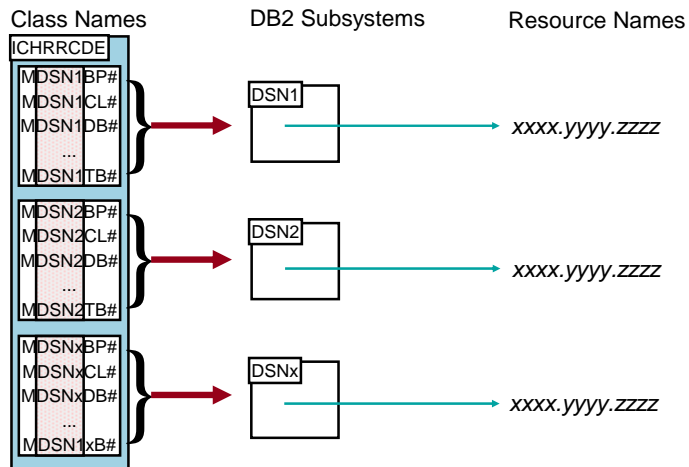
Single Subsystem Scope (an option). This is more like current DB2 authorizations, where authorization is defined for a data sharing group or subsystem. One set of general resources classes is dedicated to one subsystem or group. General resource names are not prefixed with DB2 subsystem name. The RACF classes must be defined by the installation. The primary reason for this choice is that it segregates resources by subsystem and permits fewer profiles per class. This may be easier for migration.

Multi-Subsystem Scope Classes



This diagram illustrates the names, with the data sharing group name or subsystem name as a prefix to the resource name. If you are data sharing, use the group name.

Single Subsystem Scope Classes



This diagram illustrates the single subsystem or single data sharing group scope classes. Since the class name includes the group or subsystem name, the prefix is not required in resource names.

DB2 Privileges

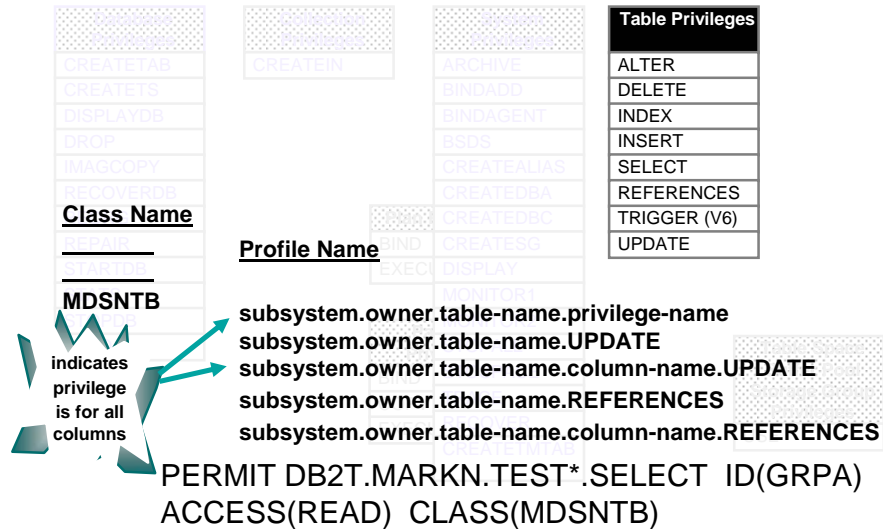
Database Privileges	Collection Privileges	System Privileges	Table Privileges
CREATETAB	CREATEIN	ARCHIVE	ALTER
CREATETS		BINDADD	DELETE
DISPLAYDB	Plan Privileges	BINDAGENT	INDEX
DROP	BIND	BSDS	INSERT
IMAGCOPY	EXECUTE	CREATEALIAS	SELECT
RECOVERDB		CREATEDBA	REFERENCES
REORG	Package Privileges	CREATEDBC	TRIGGER (V6)
REPAIR	BIND	CREATESG	UPDATE
STARTDB	COPY	DISPLAY	
STATS	EXECUTE	MONITOR1	Table Space Buffer Pool Storage Group Privileges
STOPDB		MONITOR2	USE
LOAD		STOPALL	
		STOSPACE	
		TRACE	
		RECOVER	
		CREATETMTAB	

These privileges and structures are similar to those in the authorization tables for DB2.

A privilege allows a specific function to be performed, often on a specific object. With RACF controls, the profiles generally are for many objects, using generic names.

Not all DB2 privileges are explicitly able to be delegated via GRANT or PERMIT, but all privileges listed on this page are explicitly able to use GRANT or PERMIT. Concepts of ownership will be noted later.

Profiles for Tables



This is how the profiles are defined for a specific authority. The names use multi-subsystem scope, so they are prefixed by the subsystem or group and suffixed by the privilege.

For the example, we are permitting all of the tables (MDSNTB) in subsystem DB2T owned by MARKN and starting with TEST to be SELECTed by anyone in GRPA.

DB2 Administrative Authorities

Database Authorities
DMAINT
DBCTRL
DBADM

Package Authorities
PACKADM

System Authorities
SYSOPR
SYSCTRL
SYSADM

■ **Administrative authority**

- **Set of privileges**
- **Are hierarchical**
- **Class name is DSNADM**
- **Can not be used to deny access**

An administrative authority is a set of privileges, often covering a related set of objects. Authorities often include privileges that are not explicit, have no name and can not be specifically granted.

Administrative authorities for a given object type are hierarchical. (For example, DBADM authority includes all DBCTRL privileges.)

The class name for the administrative authorities is DSNADM.

Administrative authorities can not be used to deny access to explicitly GRANTable privileges.

New Privileges for DB2 V6

Schema Privileges	Stored Procedure Privileges	User Defined Function Privileges	User Defined Distinct Type Privileges	Table Privileges
ALTER	EXECUTE	EXECUTE	USAGE	TRIGGER
COMMENT ON &&	DISPLAY **	DISPLAY **		
CREATEIN	START **	START **		
DROP	STOP **	STOP **		
QUALIFIER CHANGE &&				

- **Privilege allows a specific function**
- **Some DB2 privileges not explicitly grantable**
Privileges marked with && are not grantable
- **Privileges marked with ** are DB2 Operator commands, will defer to DB2**
- **START & STOP are not grantable.**

A privilege allows a specific function to be performed, often on a specific object or on a group.

Not all DB2 privileges are explicitly grantable. Some are controlled by ownership defined when the object was created.

Privileges marked with && are not grantable

Privileges marked with ** are DB2 Operator commands, will always defer to DB2, and START & STOP are not grantable as well.

Ownership in DB2

- Ownership is checked for User Defined Functions, User Defined Types and Stored Procedures.
- A check for MATCH is also done for the above objects.
- Ownership check for BIND privilege (for PLANS and PACKAGES).
- Ownership check for COPY privilege (PACKAGES)

New objects (UDTs, UDFs, SPROC, and TRIGGERS) have an owner and a qualifier (for TABLES, the qualifier is always the owner).

The qualifier is referred to as the SCHEMA to which the object is associated. The SCHEMA and OWNER need not be the same.

For example, if USERA created a UDF called USERB.FUNC1, USERA would pass the ownership check, USERB would pass the MATCH check.

The addition of ownership checks to certain PLAN and PACKAGE privileges was done to satisfy a customer request, not for DB2 V6 function.

RACF with DB2 Version 7

- Java ARchive (JAR) object & privilege
- Database name(s) passed on DBADM check
 - ▶ CREATE VIEW, ALTER INDEX, & DROP INDEX if chosen
 - ▶ CREATE ALIAS

Java ARchive (JAR): The JAR object and the USAGEAUTJ privilege are added to DB2 objects with security.

Database name(s) are passed on the DBADM privilege check for CREATE VIEW, ALTER INDEX, and DROP INDEX if the DB2 DBADM CREATE AUTH is on.

Multiple database names may be passed on a CREATE VIEW request

Database name is passed on DBADM privilege check for CREATE ALIAS request (but the Security Server does not use this yet).

RACF with DB2 Version 7 ...

- ▶ New reason code: DB2 subsystem to terminate if:
 - Abend in access control exit
 - Exit instructs DB2 to no longer call it
 - Unexpected return code from exit
- ▶ Security Server APAR OW45152

DB2 DSNX@XAC supports a reason code of x'10' (16) on initialization. This new reason code instructs the DB2 subsystem to terminate if:

An abend occurs in the DSNX@XAC exit

The DSNX@XAC exit instructs DB2 to no longer call it

An unexpected return code is returned to DB2 from the DSNX@XAC exit

See Security Server APAR OW45152

Also see DB2 APAR PQ53994.

Installation

- Source code provided in SYS1.SAMPLIB(IRR@XACS)
- Version 8 source SDSNSAMP(DSNSXACS)
- Installation Steps:
 - ▶ Copy exit to a private library with member name of DSNX@XAC
 - ▶ Set exit options (if not using the defaults)
 - ▶ Define classes (if not using the defaults)
 - ▶ Define profiles
 - ▶ Activate desired classes
 - ▶ Run DB2 install job DSNTIJEX Step 3

When DB2 Subsystem starts, RACF / DB2 External Security Module will be active

Source code provided in: SYS1.SAMPLIB(IRR@XACS) prior to V8, and in SDSNSAMP with V8.

Installation Steps:

Copy exit to a private library with a member name of DSNX@XAC

Set exit options (required only if not using the defaults)

Define classes (required only if not using the defaults)

Define profiles

Activate classes (may be a subset of the classes)

Run Step 3 (JEX0003) of DB2 install job DSNTIJEX specifying private library as input

Exit should now be in DB2 exit load library (SDSNEXIT)

The next time the DB2 Subsystem starts, the RACF / DB2 External Security Module will be active.

Migration

- ▶ Can migrate one DB2 object at a time
 - If the object class is not active or an object profile is not defined, DB2 authority checked
 - When classes activated, restart DB2
 - Generally migration is staged
 - One subsystem or group of subsystems
 - One application or application area

Migration can be implemented with a granularity as fine as one DB2 object at a time.

If the RACF / DB2 External Security Module detects that an object class is not active or an object profile is not defined it will defer to DB2 authority checking.

When additional classes have been setup and activated, restart DB2.

Generally migration is staged

One subsystem or group of subsystems

One application or application area

Migration: RACF / DB2 Conversion Utility

- Convert SYSIBM.SYSxxxAUTH tables into RACF profiles and many GRANTs into each PERMIT
- As is, download from web (see notes)
- Requires RXSQL or DB2 REXX function
 - Versions for RXSQL, Pipes, DB2 REXX
- Queries provided in redbooks
- You should customize queries to use patterns, generic authorization
 - More work for implementation required to yield benefits and performance in operation

Convert SYSIBM.SYSxxxAUTH tables into RACF profiles and many GRANT statements into each PERMIT. The most successful customers with this technique have strong naming standards that reflect the security policy, so the number of PERMIT statements is in the hundreds, rather than in the hundreds of thousands. The authorization and ownership should be to groups and roles to the greatest extent possible. Where resources are for an individual, then individual ownership may make sense.

Tool provided on as is basis, Download from

<http://www.ibm.com/servers/eserver/zseries/zos/racf/>

<http://www.ibm.com/servers/eserver/zseries/zos/racf/goodies.html>

Requires RXSQL or DB2 REXX function

See Rexx to SQL interface on DB2 for z/OS home page:

ibm.com/software/db2os390

Three versions:

RACFDB2/ RXSQL - Requires RXSQL

RACFDB2/ BatchPipes - Requires BatchPipes or MVS Pipes

Considerations

- Use a mix of DB2 and RACF authorization
 - ▶ Situations with no ACEE examples: IMS
 - DB2 operator commands (before V8)
- Some authorization techniques must be changed to use RACF techniques
 - Secondary ids are not in RACF, use groups
 - BINDAGENT (based on secondary ids)
 - SET CURRENT SQLID
 - OWNER(secondary id)
- Less integration with DB2: cache, invalidation, cleanup

You may need to use a mix of DB2 & RACF authorization. There are some situations & options where there is no ACEE provided, such as DB2 operator commands (e.g. -display) unless the console is signed on or prior to V8, IMS or SRB usage. Use current service levels for CICS: See APARs PQ23197, PQ23492, PQ28029. Some authorization techniques must be changed to use RACF techniques instead of DB2 ones. Secondary ids are not implemented with RACF. Use groups instead. BINDAGENT is based on secondary authorization ids & is not implemented in RACF. SET CURRENT SQLID can set a qualifier, but not change authorization. OWNER(secondary id) will generally need to be a valid RACF group. Less integration with DB2: Caching may need to be turned off. There is no plan or package invalidation if authorization is revoked. Views are not dropped if authorization is revoked. There is no automatic cleanup for authorization if objects are dropped or renamed. You should implement checks for authorization versus existing objects.

Other considerations

- ▶ Execute authority on plans not cached
- ▶ Dynamic statement cache not invalidated, use RUNSTATS
- ▶ Situations where authorization exit not called
 - e.g. GRANT, install SYSADM, cached authority
 - See DB2 Administration Guide exit appendix
- ▶ May need DB2 authorization table data for applications, e.g. show authorized tables. Use RACF unload utility.
- ▶ Check third party software & packages

One major concern is DB2 caching of authority. The primary resolution is that execute authority on plans is not cached. Performance has not been an issue.

Dynamic statement cache not invalidated when authorization is revoked outside of DB2. Use RUNSTATS for invalidation.

The authorization exit is not called in some cases:
e.g. GRANT, install SYSADM, cached authority

See current DB2 Administration Guide exit appendix, Access control authorization exit.

May need DB2 authorization table data for applications, e.g. show authorized tables. The RACF unload utility can help. Data can be loaded into a DB2 table or Grants can be used to have DB2 authorization mirror the RACF choices.

Check third party software & packages. Some have dependencies on DB2 authorization.

Auditing with RACF

- Auditing needed for implementation
 - ▶ Check for failures
 - ▶ Ensure access is intended
- Failure SMF records after entire list of profiles is exhausted
- SMF records have correlation information
- Both RACF and DB2 audit records needed
- DB2 trace record IFCID 314

Security without auditing is not secure unless the implementation is perfect. Check for failures, especially for repeated attempts. Ensure that the access being permitted is within your security policy for a sample set of accesses and your most critical information.

Failure SMF records are produced only after entire list of profiles is exhausted.

The SMF records have information needed for correlation. SMF records for a single invocation of the exit will have LOGSTR data which contains:

Time Stamp, Subset of exit input parameters

Class Name & Profile Name for first profile in list

There is a DB2 trace record IFCID 314. The DB2 trace record and RACF SMF records have data needed to join them. Check to see if RACF is controlling as expected.

DB2 Security Needs

Very significant need for increased

✓ **Security**

Mandatory security

Row level granularity

✓ **Flexibility** 

✓ **Integration**

✓ **Ease of use for safe security**

✓ **Assurance**



Everyone seems to be more aware of security today. Improving integration and making security more robust and easier to manage are very important. Customers asked for a wide range of enhancements for security. New options for tighter security, more granularity, and more information for additional flexibility in applications and SQL are needed. Improved integration with the hardware and software platform provide a better end-to-end solution. The design point for DB2 security is being easy to use for safe security, with solid system security and some security that is more flexible, that we'll call application security. Finally, it will be helpful to see what assurance can be provided, such as certification.

DB2 Security Needs ... Data Security

- Data security is a top issue in today's world due to:
 - Need for compliance with security legislation
 - Examples
 - Health Insurance Portability and Accountability Act of 1996 (HIPAA); Health care
 - Gramm-Leach-Bliley Act of 1999 (GLBA); Financial services
 - Emergence of Storage Area Networks (SANs)
 - The need for safely storing data in a widely accessible device has increased

Data security is a top issue for many people. There are a couple reasons for this. One reason is that current world events have increased our need for security. Another reason is that security legislation has been enacted requiring increased security.

Here are two U.S. examples of security legislation. The first one is the Health Insurance Portability and Accountability Act (HIPAA) of 1996, which affects health care. The second, which has existed for a while, relates to the finance industry and is known as the Graham-Leach-Bliley Act of 1999. The HIPAA Act has a deadline of April 15, 2003. This act requires health care companies to protect what is called personally identifiable information (PII).

Data Encryption for IMS and DB2 databases helps provide the security protection that the customer needs.

Another reason why data security has become a top issue concerns storage area networks (SANs). The model for a storage area network is one in which a pool of disk space is used by many different systems and is on the network. The network could be a company's intranet, or it could even be the internet. By having such modularity (much like grid computing) and plugging more storage into the network, a possible security exposure is presented; this is because now different systems, different applications, and different platforms are all accessing the same hardware devices that have data on them. Some of that data may be highly sensitive.

Database security & granularity

- Low level access control is increasingly critical
 - ▶ Web hosting
 - ▶ Privacy
- Need row level granularity
 - ▶ Individual user restricted to a specific rows
- Views can limit access
 - ▶ May be cumbersome
 - ▶ Not as effective for update, insert, delete & utilities

Low level access control is increasingly critical.

Examples:

Web hosting company to store multiple customers' data into a single subsystem, database or table

Security & laws on privacy demand row level security

Many customers need to extend the granularity from table level to row level, so that an individual user is restricted to a specific set of rows.

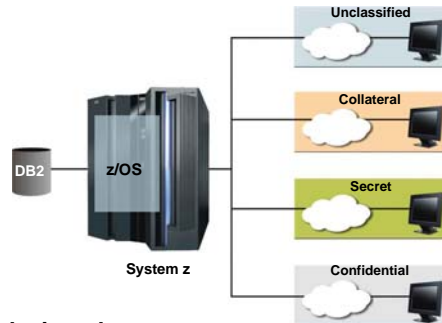
Views can limit access to selected rows & columns, but they may be cumbersome to construct with desired level of granularity.

Not very effective for update, insert, delete & utilities

Database constraints, triggers & UDFs, and stored procedures are often needed for update control.

Multilevel security helps prevent declassifying of data

Multilevel Security (MLS) helps prevent unauthorized users from accessing information at a classification level for which they are not authorized, or changing the classification of information they do have access to.



MLS support with z/OS and DB2 is designed to:

- Protect confidentiality within a single database
- Security labels at DB2 row-level
- A common security manager, RACF®
- System z scale, availability and resiliency

Multilevel security addresses government requirements for highly secure data which can be shared between agencies on demand.

Not just for governments

While multilevel security began as a US Federal government requirement, this new technology has applications elsewhere as well, as security controls become more critical in the on demand, virtual environments that are emerging. The ability to isolate data within the database may allow banks to host other banks, and distributors to host other distributors, sharing the same assets, procedures and skills.

A multilevel security system has two primary goals: first, the controls are intended to prevent unauthorized individuals from accessing information at a higher classification than their authorization. Second, the controls are intended to prevent individuals from declassifying information. Multilevel security function will allow customers more stringent access control to resources than is provided by user permissions.

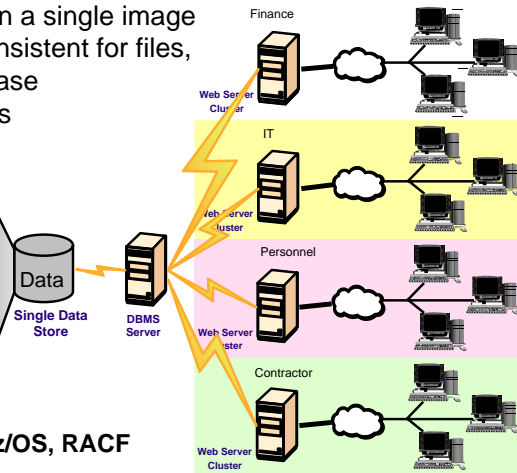
Security features in DB2 V8 and z/OS 1.5 and later enable customers to have a secure single repository of data which can be accessed by different agencies, by people with different need-to-know authority. This secure access is managed at the row level in DB2 to provide the required granularity.

NEW: RedHat support for Security Enhanced Linux for System z (SELinux)

Multilevel Security and DB2 for z/OS V8

- Labeled security allows sharing of resources with mixed levels of security in a single image
- Integrated access control, consistent for files, communications, print, database
- Control SQL and utility access

SECURITY LABEL	Col 1	Col 2	Col 3
Personnel	234	USA	50%
Finance	198	France	23%
Personnel	2	UK	9%
Finance	234	USA	11%
Personnel	22	Germany	9%
IT	87	USA	14%
Contractor	23	UK	20%
Personnel	34	Germany	43%
Finance	981	USA	12%
IT	223	USA	10%
Contractor	45	Canada	29%



Multilevel Security on System z, z/OS, RACF

Architecture

z/OS 1.5 and RACF 1.5 or Security Server added another type of security, called multilevel security, labeled security or mandatory access control (MAC) to our capabilities. The only option in the past with a high degree of separation has been physical separation. In the database world that might mean another machine or LPAR or perhaps another subsystem, another database or another table. With multilevel security, we still have a high degree of security even with data in the same table.

Access control is consistent across many types of resources using RACF, so that multilevel controls apply for data sets, for communications, for print and for database access – both objects and now with row level granularity. The DB2 controls are for both SQL access and for utility access.

For an more on multilevel security, see **Planning for Multilevel Security and Common Criteria (GA22-7509)**

<http://publibz.boulder.ibm.com/epubs/pdf/e0z2e130.pdf>

Securing DB2 and Implementing MLS on z/OS, SG24-6480-01

<http://www.redbooks.ibm.com/redpieces/pdfs/sg246480.pdf>

New concepts for DB2 people

- Multilevel security (MLS)
- Discretionary access control (DAC)
- Mandatory access control (MAC)
- Security label or seclabel
- No Read up
- Controlled Write down

Two central concepts of security are security policy and accountability. A security policy is a set of laws, rules and practices that regulate how an organization manages, protects and distributes its sensitive data. It is the set of rules that the system uses to decide whether a particular subject can access a particular object.

Accountability requires that each security- relevant event must be able to be associated with a subject. Accountability ensures that every action can be traced to the user who caused the action.

Multilevel security (MLS) is a security policy that allows the classification of data and users based on a system of hierarchical security levels combined with a system of non-hierarchical security categories. A multilevel-secure security policy has two primary goals. 1. Controls must prevent unauthorized individuals from accessing information at a higher classification than their authorization (read up). 2. Controls must prevent individuals from declassifying information (write down).

New concepts for DB2 people ...

- Seclabel comparisons
 - Dominance
 - Reverse dominance
 - Equivalence
 - Disjoint

Terms for comparing seclabels differ from relational algebra. The combination of hierarchies and non-hierarchical categories means that the result of a comparison for valid seclabels has four possible values.

Dominance: "greater than or equal to"

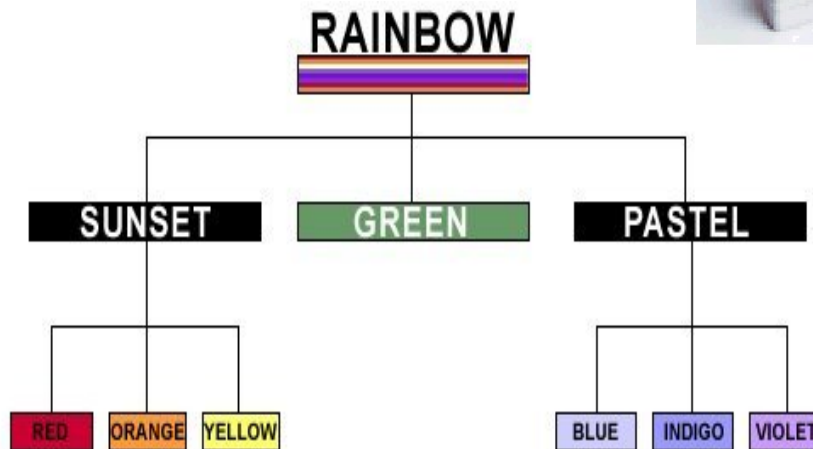
Reverse dominance: "less than or equal to"

Equivalence: "equal to" Equivalent means the seclabels are the same or have the same level and set of categories. One way to check is if both dominance and reverse dominance are true.

Disjoint: None of the above, what we might call null in database terminology. Disjoint access is not allowed, even when a user is allowed to write down. Two security labels are said to be disjoint or incompatible if incompatible security categories cause neither security label to dominate the other security label. Two security labels are disjoint when each of them has at least one category that the other does not have. Neither of the labels dominates the other. Disjoint is an error.

The new concepts are described in the book *Planning for Multilevel Security*, available in the general books on the z/OS Library web pages and also in Chapter 9, *Controlling access to DB2 objects* in the *DB2 V8 Administration Guide*.

Multilevel Security by Row ...



With the hierarchy established in the security server, the system would understand that users with authority to access RAINBOW can access anything. Someone with authority to access PASTEL information can access any row associated with BLUE, INDIGO, VIOLET, or PASTEL. Someone with SUNSET can access SUNSET, RED, ORANGE, YELLOW. This is a lot more powerful than just having an exact match on security label (i.e., user's label must exactly match the data's label), since it has the notion of "groups" that make security administration easier to manage.

With this additional capability, we'll be able to implement that type of security scheme without requiring the application to access the data using special views or predicates.

<http://www7b.boulder.ibm.com/dmdd/library/techarticle/0209cotner/0209cotner.html>

Security Labels in RACF



Key advantage: security integration

Users have default SECLABEL

Users (TSO/E, batch jobs) can request specific SECLABEL

Port of entry (e.g. terminal) has SECLABEL

Print labeled with SECLABEL

Datasets, other objects have a SECLABEL

Each SECLABEL has a RACF profile:

Access list, Universal access, Audit information

System and user controls for write-down

The SECLABELS and their relationships are defined within RACF. The key advantage is that security is integrated across the platform, with the same security for files, print, and DB2. SECLABEL can be assigned to users, ports of entry, systems, data sets and other objects. There are controls to require users and objects to have SECLABELS, and to ensure consistency. Printer support will label the output with the SECLABEL.

RACF also has controls for the ability to write down at both the system and the user level. Users who have the ability to write down can enable, disable and reset the ability to write down.

Customers who are interested in this topic will need to read Planning for Multilevel Security.

Built-in Security Labels in RACF



SYSHIGH highest security level and all categories. Dominates all other security labels

SYSLOW lowest security level and no categories (users)

SYSNONE lowest security level and no categories (catalogs, not users)

SYSMULTI equivalent to any security label

Can contain data with different security classifications, e.g. subsystem, row-level tables

SYSHIGH: This label is equivalent to the highest security level defined by the security administrator, and all categories defined by the security administrator. It dominates all other security labels in the system. **SYSHIGH** should be restricted to special system-level address spaces such as consoles, and to system programmers, system operators, and system administrators.

SYSLOW: This label is equivalent to the lowest security level defined by the security administrator, and no categories. It is dominated by all other security labels.

SYSNONE is treated as equivalent to any security label to which it is compared. **SYSNONE**, like **SYSLOW**, should be used only for resources that have no classified data content.

SYSMULTI: This label is considered to be equivalent to any defined security label. It is intended for use by multilevel security servers and tables that have multilevel data. See *Planning for Multilevel Security* for more.

Row Granularity Multilevel Security

	DB2 SECURITY LABEL_EXT	COL1	COL2	COL2
Sally SECLABEL='RAINBOW'	RAINBOW	56	7	76
	RAINBOW	24	56	65
	RAINBOW	42	6	45
Joe SECLABEL='PASTEL'	BLUE	3	456	7
	INDIGO	113	456	56
	VIOLET	3	456	4
Sam SECLABEL='SUNSET'	BLUE	4	4566	7
	RED	4	76	567
	ORANGE	33	7	567
	RED	5455	76	567
	YELLOW	999	65	45

- Table column defined AS SECURITY LABEL
- Check for each new seclabel value accessed
- Mandatory access control: run time user to data
- Works with native DB2 access control or RACF

Customers asked for row-level security for applications that need more granular security or mandatory access control. For example, an organization may want a hierarchy in which employees can see their own payroll data, a first line manager can see his or her payroll information and all of the employees reporting to that manager, and so on. Security schemes often include a security hierarchy and non-hierarchical categories.

You can add a column that acts as the security label (seclabel), with a column defined AS SECURITY LABEL: Each row value has a specific seclabel. The seclabels are defined and provided by RACF for a user, then saved in rows for INSERT, UPDATE, LOAD, ... When rows are accessed, we check for each new seclabel value accessed. If access is allowed, then normal access. If access is not allowed, data is not returned. This is runtime user seclabel to data checking, in addition to grant and permit controls. Multilevel security (MLS) requires z/OS V1R5 & Security Server (RACF).

CREATE TABLE / ALTER TABLE statements

- To enable the row level security
 - Table must have a column with char(8) to store the seclabel
- To define the security label column
 - Specify "AS SECURITY LABEL" in the column-options in the "create table / alter table" column-definition
- Table once created with seclabel cannot be disabled
- Audit record produced if the table with security label is created, altered or dropped

When you CREATE a table or ALTER it, you can decide to implement row-level security by including or adding a column that is specified AS SECURITY LABEL. The audit record is IFCID 0142.

The only technique to disable this security is to drop the table, table space or database.

Column-Definition

- Any column name
- Data-type must be CHAR(8)
 - Subtype associated with the column must be single byte
 - NOT NULL WITH DEFAULT required
- Column-option AS SECURITY LABEL
 - Indicates that the table is defined with Multilevel security with row level granularity, and that the column will contain the security label values
- Cannot specify for the column: Field procedures, Edit procedures, Check constraints

Any column name can be the security label, but the same column name cannot be used more than once in the a table. Only one security label column is allowed in a table.

The security label column must be data type single byte character, char(8), NOT NULL WITH DEFAULT. This column cannot have field procedures, edit procedures or check constraints.

MLS SELECT

- User's seclabel compared to seclabel of the row
 - If user seclabel dominates the data seclabel
 - Row is returned
 - If user seclabel does not dominate the data seclabel
 - Row is not returned, but no error is reported

The security rule for select is that your current security label must dominate the security label of all the rows read. If your security label does not dominate the label of the data row, then that row is not returned.

The user's seclabel is compared to the data seclabel of the row to be selected.

If user seclabel dominates the data seclabel then the row is returned

If user seclabel does not dominate the data seclabel, then the row is not included in data returned, but no error is reported

User must be identified to Security Server with a valid seclabel. If not, authorization error and audit record produced (IFCID 0140).

MLS INSERT

- Value of the seclabel column for inserted row set to the value of the user's seclabel
 - If user has authority for write-down, then user is allowed to set the seclabel field

The access rules for INSERT do not require checking, since there is no current row, but we will save the user's current seclabel as we insert a row.

If a user does not have the write-down privilege, then the seclabel of inserted rows will be exactly the current seclabel. If the user does have the write-down privilege, then he or she can set the value of the seclabel column to a seclabel to allow dominance or reverse dominance (writing up or down level), but not disjoint labels.

MLS UPDATE

- User's seclabel compared with the seclabel of the row to be updated
 - If the seclabels are equivalent
 - Row is updated.
 - Value of the seclabel in updated row is set to the value of the user seclabel.
- If user has write-down authority, then down level rows can be accessed and updated

The rules for update are similar, with the SELECT rules for access to the data and setting the seclabel like INSERT. Update requires equivalence for users who are not allowed to write down. User's seclabel is compared with the seclabel of the row to be updated

If the seclabels are equivalent then the row is updated. The value of the original data seclabel in the updated row is set to the value of the user seclabel.

If the user has write-down authority, then down level rows can be accessed and updated to a seclabel that has dominance or reverse dominance. Updating through a view with check option and a predicate specifying the seclabel is an exception, which can be used to force the seclabel to the user's current seclabel.

User must be identified to Security Server with a valid seclabel. If not, an authorization error and audit record are produced.

MLS DELETE

- User seclabel compared to seclabel of the row to be deleted
 - If the seclabels are equivalent
 - Row is deleted
- If user has write-down authority, then down level rows can be accessed and deleted

For DELETE, the seclabels must be equivalent, but we will not be recording the seclabel in the row, since the row is being deleted.

Again, a user who has write down authority can access and delete down-level (dominance) rows, but not up-level (reverse dominance) rows.

Utilities Changes

- UNLOAD and REORG UNLOAD EXTERNAL
 - Similar to SELECT rules
 - Rows unloaded if the user seclabel dominates the row seclabel

UNLOAD and REORG UNLOAD EXTERNAL use rules similar to SELECT. These utilities read information, like the SELECT statement, so the authorization is similar to SELECT rules. Users must be identified to RACF and have a valid seclabel.

Rows can only be unloaded if the user seclabel dominates the data seclabel. No error returns if this is not true, but the row is not unloaded.

Utilities Changes (cont)

- LOAD RESUME of table space containing tables with MLS
 - Similar to INSERT rules
 - Without write down, seclabel set to current seclabel
 - With write down permission, permitted to specify seclabel
- LOAD REPLACE on MLS requires write down authority plus INSERT rules

LOAD RESUME is like INSERT for MLS rules. LOAD RESUME of a table space containing tables with MLS with row granularity is very similar to the rules for INSERT: Without write down, the row seclabel is set to user's current seclabel.

With write down permission, the user is permitted to specify a valid seclabel (dominance or reverse dominance), but not a disjoint one.

LOAD REPLACE on MLS row table requires write down authority.

LOAD REPLACE deletes all rows, so write down authority is required, but the user seclabel does not need to dominate all rows in the table. Then the insert does allow the user to set seclabel to dominance or reverse dominance.

Utilities Changes (cont)

- REORG DISCARD of tables
 - For each row discarded, user seclabel is compared to row seclabel.
 - If they are equivalent
 - Row discarded
 - Otherwise, row is not discarded
- If user has write-down authority, then down level rows can be accessed and discarded

REORG DISCARD is similar to DELETE in function as well as in authorization rules. For each row to be discarded from those tables, if the row qualifies to be discarded, the user seclabel is compared to the data seclabel.

If the seclabels are equivalent, then the row is discarded.

Otherwise, row is not discarded

User must be identified to RACF and have a valid seclabel.

If the user has write-down authority, then the seclabel comparison is different. Rows that are dominated by the current user can be accessed and discarded.

Utilities Changes (cont)

- Access control not changed for other utilities, which don't change rows or ...
 - REORG without discard or unload
 - COPY, RECOVER
 - DSN1* - data set access – MLS on files?
 - REPAIR
 - ...
- Need to have administrative controls
 - RACF and DB2

The utilities which insert and delete data have the new multilevel security access controls, but other utilities are not changed. An administrator will generally be running these who has access to all of the data. Data sets for copies and work files need to be protected. DSN1* utilities require access control for the data sets.

Use RACF controls for the data sets at the highest level of data within the data set. For better control of the other utilities, use RACF access control.

Row level MLS

- Checks using RACF for seclabel
 - RACF defines seclabels for users
 - DB2 implements seclabel checking
- Works with native DB2 GRANT & REVOKE or with RACF Access Control
- Implementation with RACF access control
 - Consolidated access control
 - Ability to have MLS access control for larger objects e.g. table, database

While row level MLS will use RACF to access the seclabels and to compare them, it does not depend upon using RACF access control (PERMIT). You can use row level MLS with native DB2 GRANT and REVOKE or with RACF PERMITs. Still, the integration is better with RACF access control, since that allows you to have a single consolidated source for the access control and to have MLS for objects like tables and databases. Row-level access controls can be used with native DB2 access controls or with RACF access controls. Use RACF access control for the data sets in any case.

Performance Considerations

Caching used to avoid performance impact

- Initial measurements made, generally small

- Works best with small number of seclabels retrieved per commit

Index concerns

- If current access is index only, need to access data for seclabel column

- Add seclabel column to the index

- Changed design for unique indexes

Caching is used to avoid extra calls to RACF. The caching works best if there is a relatively small number of seclabels to be checked compared with the number of rows accessed.

The seclabel column will need to be accessed always. If the current access is index-only, then adding this column would change to access the data as well. If index-only access is needed, then you should add the seclabel column to the index. This would affect uniqueness, but this change may be useful to avoid inference issues.

See section 4.9 in the V8 Performance Topics redbook, SG24-6465 for more on multilevel security performance.

<http://www.redbooks.ibm.com/abstracts/SG246465.html?Open>

Some Requirements and Restrictions

- Requires z/OS V1R5 & Security Server (RACF) V1R5
- Row level security not enforced for referential constraints
- Referential constraints cannot be defined on a seclabel column
- Sysplex parallelism not used for queries on table with seclabel
- Not allowed on seclabel column: Field procedures, Edit procedures, Check constraints
- Trigger transition tables do not have security labels
- Some additional restrictions for MQTs

Note that there are requirements for z/OS V1R5 and the Security Server (RACF) V1R5 (or equivalent function). There are some additional restrictions: Row level security is not enforced for referential constraint checking.

Referential constraints cannot be defined on a security label column. Sysplex parallelism is not used for queries that access a table with a security label column. Field procedures and edit procedures are not allowed on a security label column. Trigger transition tables do not have security labels.

RACF Access Control Improved

- DB2 commands – using RACF access control
 - ▶ When signed on console, jobs, TSO, ...
 - ▶ Signed on id used, rather than SYSOPR
 - ▶ Not compatible
 - ▶ Need to provide proper authorization, using PERMIT or GRANT, users, groups, ...
- WebSphere environment
- Multilevel security for object access control

RACF access control has been improved in several ways. DB2 operator commands are able to use RACF access control for the first time. If the DB2 command is issued in an environment that has an ACEE, then RACF access control can be used. Signed on consoles do have an ACEE, but others do not. Jobs and TSO environments generally have an ACEE.

Access control is improved for DB2 commands, whether or not RACF access control is used. RACF has not been able to control access for DB2 commands in the past. While there is an improvement, the change is not completely compatible, and customers need to be sure that the appropriate authorization is GRANTED or PERMITTED. Authorization with RACF is improved for the WebSphere environment and for use of multilevel security.

The WebSphere environment is better-managed, with more robust handling of the ACEE in that environment.

RACF access control is enhanced with the ability to have multilevel security. Having MLS at a table level and a database level provides complementary function to the new row level MLS.

Multilevel security for RACF Access Control

- Ability to use multilevel security with RACF access control for objects: views, tables, databases, ...
- Use security profile definitions, not PERMITs
- Ship access control authorization exit with DB2
 - prefix.SDSNSAMP instead of SYS1.SAMPLIB
- Requires z/OS V1R5 & Security Server V1R5

If you use RACF access controls, then you can define multilevel security for other objects. Then, access will require both the discretionary access control (PERMIT) and the mandatory access control (seclabel comparison).

While earlier exits came with RACF in SYS1.SAMPLIB, the new exit comes with DB2 in prefix.SDSNSAMP.

The RACF Access Control Module Guide book is available with other DB2 books on the DB2 for z/OS Library web pages.

Multilevel DB2 Authorization Hierarchy

Hierarchy for DB2 objects

- Subsystem or data sharing group
 - Database
 - Table Space
 - Table
 - Column
 - Row
- View
- Storage Group
- Bufferpool
- ...

MLS security can be defined for the DB2 objects, but in general, you will want the seclabel of an object higher in the object hierarchy to dominate all objects within it. There will be some exceptions, similar to a write-down capability. Managing the relationships among DB2 objects is still a manual process. Using RACF should allow the number of seclabels and permits to be small enough to manage this way, because of groups and generic authority.

Multilevel Authorization Hierarchy ...

- Subsystem or data sharing group
 - Plan
 - Collection
 - Package
 - Schema
 - Stored Procedure, User-Defined Function
 - Java ARchive (JAR)
 - Distinct Type
 - Sequence

This is the second half of the hierarchy. While this hierarchy is not enforced, meaningful authorization rules will generally require that the higher level in this hierarchy have a seclabel which dominates the objects lower in the hierarchy.

In some cases, you may need to use some of the system built-in seclabels, such as SYSMULTI.

Views with Multilevel Security, Session Variables, ...

```
CREATE VIEW SW_CUSTOMER AS  
SELECT CUST_NBR, CUST_NAME,  
CUST_CREDIT  
FROM CUSTOMER  
WHERE CUST_REGION='SW'
```

- Only customers in SW
- Only customer number, name & credit

- **Views can provide only equivalent seclabel data**
- **Views can have lower seclabel than tables**
 - Eliminate protected data: rows and/or columns
 - Join or union with other tables to add or remove information
 - Use triggers, stored procedures, constraints and with check option for update control at row level
- **Views can use plan or package, seclabel, site-defined comparisons with special registers & session variables**

Views can be used to hide data. They can subset to provide only certain columns or fields. Views are often used to simplify access to data by being able to define the view once and use it many times.

Table privileges DELETE, INSERT, SELECT, UPDATE, or ALL can be granted individually on a view. By creating a view and granting privileges on it, you can give someone access only to a specific combination of data. This capability is sometimes called field-level access control or field-level sensitivity.

Materialized Query Table (MQT) Authorization

- Use of MQT may be implicit or explicit
 - Explicit use requires MQT authorization
 - Implicit use requires base table or view authorization.
- Creation of table requires CREATE TABLE authorization and SELECT to base table or view
 - DBADM can create MQT for another authorization ID
 - Some restrictions for MQT and MLS
- REFRESH TABLE authorization
 - Ownership of MQT, DBADM, DBCTRL, SYSADM or SYSCTRL

The materialized query table is often a summary table. DB2 optimization can rewrite a query on the base tables to use the MQT. No authorization on a MQT is required for it to be used in automatic query rewrite or implicitly.

Authorization: To ALTER, the privilege set that is defined below must include at least one of the following:

The ALTER privilege on the table, Ownership of the table, DBADM authority for the database, or SYSADM or SYSCTRL authority

Additional privileges might be required when: FOREIGN KEY, DROP PRIMARY KEY, DROP FOREIGN KEY, or DROP CONSTANT is specified; The data type of a column that is added to the table is a distinct type; or a fullselect is specified.

Materialized Query Table and Multilevel Security

- DEFINITION only: AS SECURITY LABEL attribute not inherited
- Only one source table can have security label
- Security label column must be included in MQT
- AS SECURITY LABEL attribute is inherited
- ALTER TABLE to add seclabel will fail if table is source of MQT

If any table in the fullselect of the materialized query definition contains a security label column,

1. If for DEFINITION ONLY: The column attribute AS SECURITY LABEL is not inherited from table.
2. If only one table contains the security label column, the security label column must be included in the MQT. The MQT will inherit the column attribute AS SECURITY LABEL. The MAINTAINED BY USER option is allowed.
3. If more than one source table contains a security label column, an error is returned.

ALTER MQT source TABLE by adding security label column: An ALTER TABLE to add a security label column will fail if the table is a source table of an MQT.

REFRESH TABLE for MQT: The REFRESH TABLE SQL statement, used to delete the data currently in the materialized query table and then to repopulate the materialized query table by executing the fullselect, does not check for MLS with row level granularity. The MLS row level granularity check is enforced when using the MQT, either by exploiting the MQT or by using the MQT directly.

Sequence Authorization

- CREATE: CREATEIN for schema, SYSADM or SYSCTRL
- ALTER: Ownership, ALTER for sequence, ALTERIN for schema, SYSADM or SYSCTRL
- DROP: Ownership, DROPIN for schema, SYSADM or SYSCTRL
- COMMENT: Ownership, ALTER for sequence, ALTERIN for schema, SYSADM or SYSCTRL
- GRANT & REVOKE: ALTER & USAGE
 - USAGE: NEXT VALUE or PREVIOUS VALUE expression used

The sequence is a new DB2 object, and these new SQL statements require authorization. The USAGE privilege for the sequence will be the most common privilege, I expect. There are new authorization rules for data definition and for use of this new function.

Other authorization changes

- Schema evolution means alter, instead of drop, so we don't need to save and regrant authority.
- If the select-statement contains an INSERT statement, then INSERT and SELECT privileges on the target table or view are required.
- Access Control Authorization Exit changed
 - RACF version shipped with DB2: code and book
 - Exit for prior versions are not usable
 - long names, new objects, ...
- Maximum secondary ids increased from 245 to 1012
- EXPLAIN authorization without table access sample

For many database administrators, the biggest change in authorization will be the ability to avoid the cascade revoke caused by deleting a table or table space to change attributes. Being able to ALTER is faster, more available and safer.

The RACF access controls are changed very substantially. The exit has additional capabilities for sequences, and changes in the interface to handle long names. The exit is provided names converted from Unicode to EBCDIC. While the RACF exit has been shipped by RACF in SYS1.SAMPLIB, now it will come with DB2 in prefix.SDSNSAMP. The maximum number of secondary authorization ids has increased from 245 to 1012 with APAR PQ90147.

An example showing how to have EXPLAIN authorization without direct access to the tables is provided with the V8 Visual Explain.

<http://www.ibm.com/software/data/db2/zos/osc/ve/index.html>

Summary of DB2 for z/OS V8 Security

Very significant changes for increased

- ✓ Security
- ✓ Flexibility
- ✓ Integration
- ✓ Ease of use for safe security
- ✓ Assurance



Everyone seems to be more aware of security today. Improving integration and making security more robust and easier to manage are very important. Customers asked for a wide range of enhancements for security. New options for tighter security, more granularity, and more information for additional flexibility in applications and SQL are needed. Improved integration with the hardware and software platform provide a better end-to-end solution.

The design point for DB2 security is being easy to use for safe security, with solid system security and some security that is more flexible, that we'll call application security. It will be helpful to see what assurance can be provided, such as certification.

DB2 for z/OS provides many enhancements for security. There are new options for tighter security, more granularity, and more information for additional flexibility in applications and SQL. Integration has been improved with other platforms and with z/OS and the Security Server (RACF). The changes are intended to improve your ability to implement and use security safely. Let's be safe out there.

Concerns & Requirements

- ☑ ▶ DB2 operator command support for RACF
 - ▶ IMS and other environments for RACF
 - ▶ More portable, controllable identification
 - ▶ Avoid cascade revoke
- ☑ ▶ Row level security (many possible interpretations)
- ☑ ▶ Security classifications or Mandatory Access Control or multi-level security
- ☑ ▶ Improved ability to protect with encryption, ...
 - ▶ Please discuss and help us prioritize
 - Explain the problems and justification
 - What do you want to protect? from whom?
 - What alternatives are possible?

There are many different requirements for improvements, and the ones above are some that I hear the most.

Some of the changes will require changes in the Security Server and DB2. Others will require architecture changes in z/OS and major subsystems like IMS, CICS, MQSeries, and WebSphere as well. I expect almost every new release of DB2 to require a small corresponding change in the Security Server.

If you are submitting a requirement, one of the most effective techniques you can use is to specify the problem and justification carefully.

RACF Authorization Summary

- Control Access to DB2 Objects Using RACF
 - ▶ Single point of control for administration & audit
 - ▶ Define security before DB2 object exists
 - ▶ Allow security to persist when a DB2 object dropped
 - ▶ Eliminate DB2 cascade revoke
 - ▶ Protect multiple DB2 objects with a single security rule
 - ▶ Flexibility for multiple DB2 Subsystems
 - One set of RACF classes for multiple DB2 subsystems
 - One set of RACF classes for each DB2 subsystem

These are the key benefits for controlling access to DB2 objects Using RACF.

Single point of control for administration and auditing

Define security rules before a DB2 object is created

Allow security rules to persist when a DB2 object is dropped

Ability to protect multiple DB2 objects with a single security rule using generic profiles and/or member/grouping profiles

Eliminate DB2 cascading revoke

Preserve DB2 privileges and administrative authorities

Flexibility for multiple DB2 Subsystems

One set of RACF classes for multiple DB2 subsystems

One set of RACF classes for each DB2 subsystem

Selectable on an object-by-object basis

DB2 Security Bibliography

- **Introduction to DB2 for z/OS**
 - ✓ Focus on user new to DB2 for z/OS
- **What's New?** overview of new version
- **Administration Guide**
 - ✓ Security & Audit section
 - ✓ Appendices for Exits, Audit, IFI
- **SQL Reference**
 - ✓ Grant & Revoke
 - ✓ Authorization for SQL
- **Command Reference** authorization for commands, BIND
- **Utility Guide & Reference** authorization for utilities
- **Installation Guide** choices for security
- **Version 8 Everything ..., SG24-6079**
- **RACF Access Control Module Guide, SC28-7433**
- **Planning for Multilevel Security, GA22-7509**



Here is the recommended reading list for security.

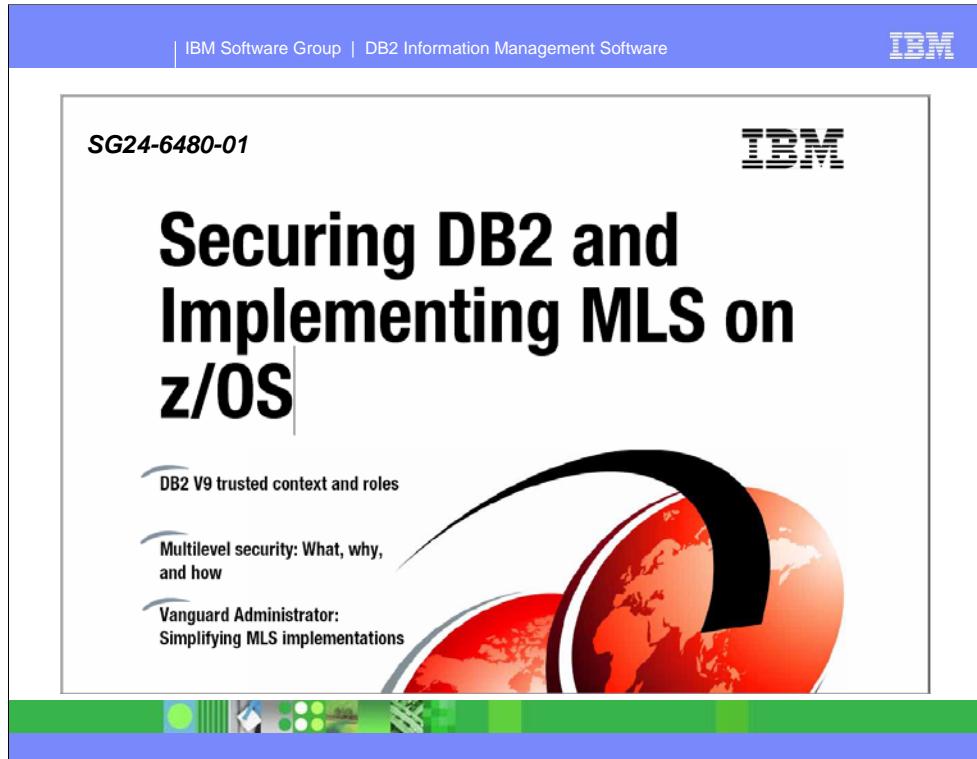
<http://www.ibm.com/software/data/db2/zos/v8books.html>

If you just want an overview of what is in a new version, such as V8 or V7, the What's New? book is the best, with details in the Release Guide.

If you are new to DB2, the Introduction is designed to help you understand the differences from other RDBMS. The primary information for Security and Audit is in the Administration Guide.

If you want to know the authorization for an SQL statement, see the SQL Reference; for a command, see the Command Reference; for a utility, see the Utility Guide and Reference. The Installation Guide includes choices that affect security.

The red book, V8 Everything you wanted ..., includes more detail on the security changes for V8. The RACF access control module guide discusses specifics for using RACF access control. Planning for Multilevel Security is a z/OS document that includes DB2 and other products. <http://publibz.boulder.ibm.com/epubs/pdf/e0z2e120.pdf>



This is the recently updated redbook, SG24-6480-01. It discusses use of DB2 for z/OS Version 8 multi-level security and the new DB2 9 security enhancements.

The DB2 9 for z/OS Technical Overview, SG24-7330, chapter on security, chapter 10, also provides a brief description of the DB2 9 improvements in security.

Data Integrity with DB2 for z/OS, SG24-7111 provides some discussion of audit for security and for application controls. Also see the best practices presentation for audit suggestions as well as the audit chapter of the Administration Guide.

Reading suggestions: Using RACF access control

- ✓ DB2 Administration Guide appendix Access Control Authorization Exit
- ✓ Presentations on the web: (next page)
- ✓ Security Server or RACF books
 - RACF Access Control Module Guide, SC18-7433
- ✓ CICS RACF Security Guide, SC34-6011
- ✓ RACF APARs and associated information

Read DB2 Administration Guide appendix on Access Control Authorization Exit for your version. Get the latest from the web. V7 books updated July 2003.

<http://www.ibm.com/software/data/db2/os390/library.html>

There are very good presentations on the web.

<http://www.ibm.com/servers/eserver/zseries/zos/racf/presentations.html>

<http://ibm.com/software/db2zos> Click Support, then Technical Presentations. Qualify by security.

<ftp://ftp.software.ibm.com/software/db2storedprocedure/db2zos390/techdocs/Z15.pdf>
RACF Access Control Module Guide

Audit and security: other presentations

Protect & Comply – spectrum of solutions

Best practices for security

DB2 9 for z/OS security enhancements

DB2 for z/OS Version 8 security enhancements

Protect Your Assets with DB2 security

DB2 for z/OS Auditing

Other presentations on DB2 Events web page

Click on Presentations from previous conferences



DB2 security and auditing presentations:

<ftp://ftp.software.ibm.com/software/data/db2/zos/presentations/security/>

Protect & Comply – spectrum of solutions

<ftp://ftp.software.ibm.com/software/data/db2/zos/presentations/security/protect-comply-imtc-2007-miller.pdf>

Best practices for security

<ftp://ftp.software.ibm.com/software/data/db2/zos/presentations/security/best-practice-security-idug-eu-2007-miller.pdf>

DB2 9 security enhancements

<ftp://ftp.software.ibm.com/software/data/db2/zos/presentations/security/db2-9-security-enhancements-iod-2007-chandran.pdf>

Protect your assets with DB2 security (this long presentation)

<ftp://ftp.software.ibm.com/software/data/db2/zos/presentations/security/>

Other presentations on DB2 Events web page. Start here, then Click on Presentations from previous conferences

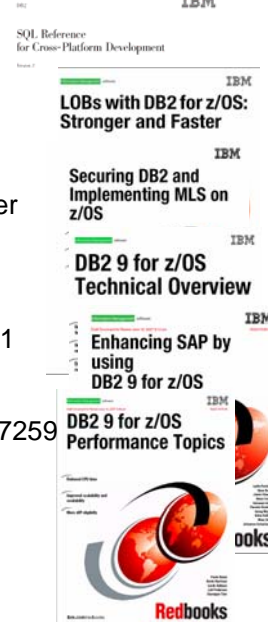
<http://www.ibm.com/software/data/db2/zos/events.html>

Securing DB2 and Implementing MLS on z/OS, SG24-6480-01

<http://www.redbooks.ibm.com/redpieces/pdfs/sg246480.pdf>

Other books: DB2 9 in **IBM Redbooks**

- DB2 9 Technical Overview SG24-7330
- DB2 9 Performance Topics SG24-7473
- DB2 9 Stored Procedures SG24-7604
- Index Compression with DB2 9 for z/OS paper
- SQL Reference for Cross-Platform Development
- DB2 9 Optimization Service Center SG24-7421
- LOBs with DB2 for z/OS SG24-7270
- Powering SOA with IBM Data Servers SG24-7259
- Enhancing SAP - DB2 9 SG24-7239
- Best practices SAP BI - DB2 9 SG24-6489-01
- Data Sharing in a Nutshell, SG24-7322
- Securing DB2 & MLS z/OS SG24-6480-01



DB2 library more information <http://www.ibm.com/software/data/db2/zos/library.html>

Ten IBM Redbooks publications, one Redpaper and one cross-platform book on DB2 9 are published, in addition to the standard library, with more in the works. Check for updates.

- DB2 9 Technical Overview, SG24-7330 <http://www.redbooks.ibm.com/abstracts/SG247330.html>
- DB2 9 Performance Topics, SG24-7473, <http://www.redbooks.ibm.com/abstracts/SG247473.html>
- DB2 for z/OS Stored Procedures: CALL & Beyond SG24-7604, <http://www.redbooks.ibm.com/abstracts/SG247604.html>
- Index Compression with DB2 9 for z/OS, redpaper REDP4345 <http://www.redbooks.ibm.com/abstracts/redp4345.html>
- Cross-Platform Development Version 3, <http://www.ibm.com/developerworks/db2/library/techarticle/0206sqlref/0206sqlref.html>
ftp://ftp.software.ibm.com/ps/products/db2/info/xplatsql/pdf/en_US/cpsqlrv3.pdf
- Powering SOA with IBM Data Servers, SG24-7259 <http://www.redbooks.ibm.com/abstracts/SG247259.html>
- LOBs with DB2 for z/OS: Stronger & Faster SG24-7270, <http://www.redbooks.ibm.com/abstracts/SG247270.html>
- Securing DB2 & MLS z/OS, SG24-6480-01, <http://www.redbooks.ibm.com/abstracts/sg246480.html>
- Enhancing SAP - DB2 9, SG24-7239, <http://www.redbooks.ibm.com/abstracts/SG247239.html>
- Best practices SAP BI - DB2 9, SG24-6489-01, <http://www.redbooks.ibm.com/abstracts/sg246489.html>
- DB2 9 Optimization Service Center, SG24-7421, <http://www.redbooks.ibm.com/abstracts/sg247421.html>
- Data Sharing in a Nutshell, SG24-7322, <http://www.redbooks.ibm.com/abstracts/sg247421.html>

Audit: DB2 library, redbook, and other references:

DB2 for z/OS Administration Guide, SC18-9840

Part 3: Security and Auditing

Chapter 10 Auditing access to DB2

Securing DB2 and Implementing MLS on z/OS, SG24-6480-01

Audit reporting tools from IBM

Consul

Audit Management Expert

Tivoli Omegamon for DB2

Log Analysis tool

Older books

DB2 Audit Guideline

Security and Authorization Extensions Guide, GG24-3299

Audit Usage Guide, GG24-3300

IBM DATABASE 2 Security and Authorization Guide GG24-1599

Audit and Control in the DATABASE 2 environment, GE20-0783

DB2 library, redbook, and other references: (most current at top)

DB2 library: <http://www.ibm.com/software/data/db2/zos/library.html>

DB2 for z/OS Administration Guide, SC18-9840 Part 3: Security & Auditing
Chapter 10 Auditing access to DB2 <http://publib.boulder.ibm.com/epubs/pdf/dsnagk10.pdf>

Securing DB2 and Implementing MLS on z/OS SG24-6480-01

<http://www.redbooks.ibm.com/redbooks/pdfs/sg246480.pdf> Consul press release

<http://www.consul.com/PressReleaseDetail.asp?prid=102&pid=23>

Audit Management Expert

<http://www.ibm.com/software/data/db2imstools/db2tools/db2ame-zos/>

Tivoli Omegamon for DB2

<http://www.ibm.com/software/tivoli/products/omegamon-xe-db2-peex-zos/>

Log Analysis tool

<http://www.ibm.com/software/data/db2imstools/db2tools/db2lat.html>

DB2 Audit Guideline book, non IBM

<http://www.isaca.org/Template.cfm?Section=Home&CONTENTID=10762&TEMPLATE=/ContentManagement/ContentDisplay.cfm>

Security and Authorization Extensions Guide, GG24-3299

Audit Usage Guide, GG24-3300

IBM DATABASE 2 Security and Authorization Guide, GG24-1599

Audit and Control in the DATABASE 2 environment, GE20-0783

Secondary Authids

Environment is complex and heterogeneous

May be a userid or a group or whatever the exit code decides ...

SET CURRENT SQLID

Name qualification, not authorization

Must be a secondary id unless the user has SYSADM authority

Secondary ids in DB2 reflect the heterogeneous environment. Authorization ids have included transaction names, terminal ids, and various other strings. For processes managed by RACF and the provided exit, the primary authorization id is the userid and the secondary ids are the list of groups.

SET CURRENT SQLID can set a qualifier to a primary authorization id or to one of the secondary ids, except when the user has SYSADM authority. With SYSADM authority, the user can set any CURRENT SQLID.

There is a specific authority called BINDAGENT that is somewhat like a surrogate privilege and based upon secondary authids. BINDAGENT provides weaker security, but not strong security like almost every other authority. SYSCTRL also has a weaker security.

BIND Process

Security controls for BIND

BINDADD for new, BIND for existing

CREATEIN, PACKADM for package collections

BIND ENABLE & DISABLE environment control

OWNER

QUALIFIER

DYNAMICRULES (RUN | BIND)

BINDAGENT

The BIND process for static SQL provides some specific authorization, by "compiling" the SQL statements and checking authorization of the BIND owner. If the BIND owner authority is revoked, then the plan or package is invalidated, so it must be rebound. There are many BIND parameters and security choices.

To BIND a plan or package, the BIND owner needs to have BINDADD authority for a new plan or package or BIND for existing ones and authority for all of the SQL in the plan or package. If you BIND a package, then you need to have authority to BIND into a specific collection. The BIND command also has the ability to limit the environments in which the plan or package is run to specific IMS or CICS environments, for example.

The qualifier is the default authorization-id qualifier of a table name, when only one name is specified. DYNAMICRULES provide a choice of using the current user for access checking or checking access for the BIND OWNER.

Bind control

- BIND OWNER has access to data
- BIND plan and package with selects, updates
ENABLE(CICSPROD)
- RACF profile which includes table
UACC(NONE), no PERMITS
- PERMIT on plan and package to JoG
- JoG can run plan and package
- JoG cannot run SQL directly
- JoG cannot BIND SQL to use table
- PLAN can only be run within CICSPROD

This is an example, showing the difference between the ability to BIND and have direct table access and the ability to run the plan(JoG). Additional controls could be implemented within the CICS subsystem.

Example: SELECTing from a Table

▶ SELECT

The SQL Reference shows that the authorization ID must have at least one of the following:

- Ownership of the table or view
- SELECT privilege on the table or view
- DBADM authority for the database
- SYSCTRL authority (catalog tables only)
- SYSADM authority

This is an example of authorization checking for an SQL SELECT statement. For SQL statements, the authorization is in the SQL Reference, and these are the checks.

Example: SELECTing from a Table...

▪ SELECT

- The user must have:

Ownership of the table or view (DB2 owner compared to requester id)

- Or access to any one of the following profiles:

Class	Profile	Access
MDSNTB	<i>subsystem.table-name</i> .SELECT	READ
DSNADM	<i>subsystem.database-name</i> .DBADM	READ
DSNADM	<i>subsystem</i> .SYSCTRL*	READ
DSNADM	<i>subsystem</i> .SYSADM	READ



This is the diagram which corresponds to the example of selecting from a table.

References

- ❑ **Security Server (RACF) publications:**
 - **RACF Command Language Reference (SC28-1919)**
 - **RACF Security Administrator's Guide (SC28-1915)**
 - **RACF Callable Services Guide (SC28-1921)**
- ❑ **z/OS publications:**
 - **Planning for Multilevel Security (GA22-7509)**
<http://publibz.boulder.ibm.com/epubs/pdf/e0z2e100.pdf>
- ❑ **RACF MLS implementation presentation**
- ❑ **RACF web site:**
<http://www.ibm.com/servers/eserver/zseries/zos/racf>

Here are some additional pointers for information about RACF. z/OS V1R5 is available. Check for the additional information and see one DB2 & RACF book shipped as a pdf file with DB2, RACF Access Control Module Guide and Reference Version 8 on the next page.

Planning for Multilevel Security is on the web under z/OS library, System level books, or

<http://www.ibm.com/servers/eserver/zseries/zos/bkserv/r5pdf/zsys.html>

DB2 V8 books including the RACF Access Control Module Guide are located at

<http://www.ibm.com/software/data/db2/os390/v8books.html>

More information on DB2 for z/OS web site

ibm.com/software/db2zos

- primary home page

ibm.com/software/db2zos/support.html

- Click on Support for much more information
- Technotes, presentations, Redbooks, ...

ibm.com/software/data/db2imstools

- Encryption tool EDITPROC

ibm.com/developerworks/db2

- programmer information

ibm.com/servers/eserver/zseries/security/

Here are the primary places to look for additional information. Check the primary home page to see what's new in the product.

The Support page has hundreds of items ranging from answers to frequently asked questions to redbooks and technical presentations. There is a new redbook, DB2 for z/OS Version 8 Technical Preview, SG24-6871 on the web.

The presentations page has many presentations from conferences, so that customers can get the latest information even if they can't come to every conference.

For the latest on DB2 for z/OS V8, check the V8 page.

Encryption References

- IBM Data Encryption Tool for IMS and DB2 Databases Version 1.1
 - <http://www.ibm.com/software/data/db2imstools/db2tools/ibmencrypt.html>
- System z9 and System z cryptography
 - <http://www.ibm.com/servers/eserver/zseries/security/cryptography.html>
- Encryption Facility for z/OS
 - http://www.ibm.com/servers/eserver/zseries/zos/encryption_facility/
- Hardware Crypto Benefits (SecureWorld Session I04)
 - ftp://ftp.software.ibm.com/software/mktsupport/techdocs/crypto_hdw_benefits_i04.pdf
- Understanding the Crypto Hardware Available for System z and S/390
 - ftp://ftp.software.ibm.com/software/mktsupport/techdocs/cryhw_descriptions.pdf
- Enabling the Crypto Environment - A User's Experience
 - <http://www.share.org/proceedings/sh99/SHARE/data/S1722.pdf>
- System z Crypto Guide Update, an IBM Redbook to understand and implement the z/OS Cryptographic PCICC and PCICA cards
 - <http://publib-b.boulder.ibm.com/redbooks.nsf/RedbookAbstracts/sq246870.html?Open>

These references provide much more information about encryption.


Disclaimers: This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice. Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

Disclaimer and Trademarks

Information contained in this material has not been submitted to any formal IBM review and is distributed on "as is" basis without any warranty either expressed or implied. Measurements data have been obtained in laboratory environment. Information in this presentation about IBM's future plans reflect current thinking and is subject to change at IBM's business discretion. You should not rely on such information to make business plans. The use of this information is a customer responsibility.

IBM MAY HAVE PATENTS OR PENDING PATENT APPLICATIONS COVERING SUBJECT MATTER IN THIS DOCUMENT. THE FURNISHING OF THIS DOCUMENT DOES NOT IMPLY GIVING LICENSE TO THESE PATENTS.

TRADEMARKS: THE FOLLOWING TERMS ARE TRADEMARKS OR ® REGISTERED TRADEMARKS OF THE IBM CORPORATION IN THE UNITED STATES AND/OR OTHER COUNTRIES: AIX, AS/400, DATABASE 2, DB2, e-business logo, Enterprise Storage Server, ESCON, FICON, OS/390, OS/400, ES/9000, MVS/ESA, Netfinity, RISC, RISC SYSTEM/6000, iSeries, pSeries, xSeries, SYSTEM/390, IBM, Lotus, NOTES, WebSphere, z/Architecture, z/OS, System z 

The FOLLOWING TERMS ARE TRADEMARKS OR REGISTERED TRADEMARKS OF THE MICROSOFT CORPORATION IN THE UNITED STATES AND/OR OTHER COUNTRIES: MICROSOFT, WINDOWS, WINDOWS NT, ODBC, WINDOWS 95

For additional information see ibm.com/legal/copytrade.phtml

1

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in the operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

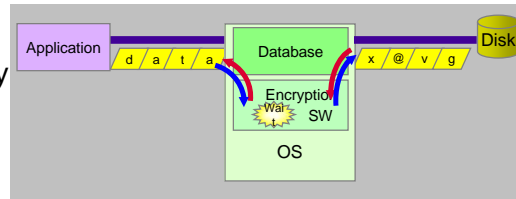
Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only. This information may contain examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

Encryption Techniques

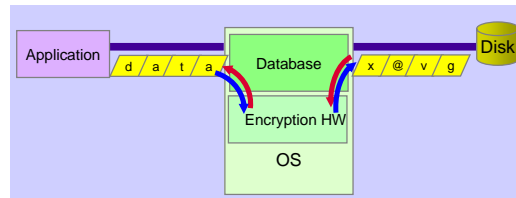
Software

Advantage: Portability



Hardware

Advantage: Speed



Now we will look at encryption itself and how encryption techniques and issues apply to the tool. In general, there are two encryption techniques, encryption using software and encryption using hardware.

If you do your encryption in software, the data on the disk is encrypted as shown in the top picture. As data comes in, it goes through some encryption software to get the data decrypted out to an application. Encryption using software is inherently slower than encryption using hardware.

The bottom picture shows the same flow, but here some type of hardware assist is used to do encryption and decryption. This is very similar to the concept of compression and decompression. We use a hardware assist to do encryption in the same way that we used a hardware assist to do compression.

The advantage of software encryption is that you have portability. You can take the encryption software and put it on any platform as long as you have it coded in some language that lets you compile it on the different operating systems.

The advantage of hardware encryption is speed.

Row-level versus Column-level encryption

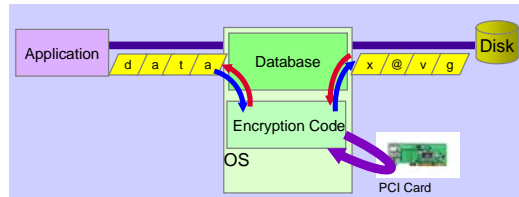
- This offering provides row-level encryption
- Column-level encryption was considered, however,
 - The cost to encrypt one column is roughly equivalent to the cost to encrypt the entire row
 - If this offering supported column level encryption, then two calls to the crypto hardware would be needed, thus doubling the performance overhead when compared to row-level encryption
- The size of the row has very little impact on the performance overhead
- Therefore, encryption of the entire row provides the lowest performance overhead possible

If you want column-level encryption, rather than row-level encryption, there are some tradeoffs. The real difference is what you are trying to protect and from whom. If your objective is to protect the data at rest, this offering does the job, ensuring that access is through the primary interfaces and uses the security checking. If you want column-level encryption or field-by-field encryption, then V8 provides functions for the encryption and decryption. This is application level or user level encryption, and your applications or users must do the key management.

Hardware Encryption Techniques

Brand X PCI Card

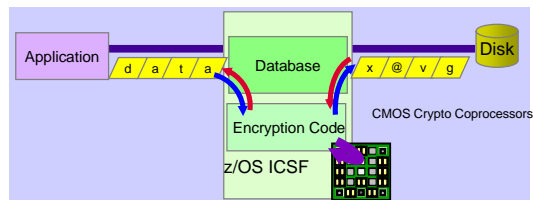
Advantage: Portability



System z CCF

Advantage: Speed

Crypto requests managed by z/OS Integrated Cryptographic Services Facility (ICSF), which utilize on-board processors



There are many PCI cards available that do encryption. A PCI card is a standard hardware card that you can plug into almost any architecture. You plug in the PCI card, and you have hardware encryption. And since it is hardware encryption, you get much better speed than you would with software encryption.

One advantage that we have with the System z is that the cryptographic co-processor facility (CCF) gives us even more speed than a PCI card. Instead of going from a general purpose processor onto a PCI bus and into a PCI card to do the encryption and then back to the processor across the various buses, we use the crypto chips that are on the same MCM board as the rest of the general purpose processor. This is an exclusive for System z.

A software component in z/OS called the Integrated Cryptographic Services Facility (ICSF) is used. ICSF is invoked from the product exits, and it is ICSF that utilizes and accesses the cryptographic co-processor hardware.

With the on-board processors, we get faster speeds than we can on PCI cards.

How Does Data Encryption for IMS and DB2 Databases Address These Challenges?

- Performance overhead
 - Lowest encryption overhead possible
 - Uses on-board processor hardware encryption
 - Infinitely faster than software encryption
 - Faster than off-board (PCI card) hardware encryption
 - Worst case laboratory measurements show 400% CPU path length increase for DB2 workloads (tablespace scan) -- this overhead is much less than the overhead for other encryption processes
- Key management
 - No new key management facility learning curve
 - Uses existing ICSF facility to manage encryption keys in one central repository
- Application changes
 - No application changes required - no passwords passed
 - System administration changes necessary only to the segment or table definition

The challenge for data encryption is in the areas of performance overhead, key management, and application changes. How do we address these challenges with the IBM Data Encryption for IMS and DB2 Databases tool?

Performance overhead. This tool has very low encryption overhead. Performance is better than any software encryption that can be performed. And it is faster than outboard or PCI-based compression; this is because of the location of the processors and because all processors share the same I/O bus. There are no calls to other pieces of hardware. Worst case laboratory measurements show about a 400 percent CP path link increase for a DB2 workload. In this case, the workload was a table space scan. A table space scan should be the worst case performer, because every row has to be decrypted while it is being accessed. This is not the case when you are going through an index. Indexes are not encrypted in DB2. The overhead to access an index is going to be much less. In some cases, the overhead may even be unnoticeable.

Key management. There is no new key management facility to learn. Existing ICSF services are used. **Application changes.** There are no application changes required. There are no passwords that need to be stored in applications. Passwords are passed at an exit level, and passwords are all managed. Note, however, that in order to implement data encryption in DB2 the table must be redefined. For example, if you want to add an EDITPROC into a DB2 table you cannot alter the table and add the EDITPROC. Instead, you have to UNLOAD the data, DROP and RECREATE the table and all of its dependent objects, RELOAD the data, and REDEFINE your applications. If you have the IBM DB2 Administration Tool installed, that tool will do these steps for you (the UNLOAD, DROP and RECREATE, and RELOAD of the encrypted data by way of the exit).

Prerequisite Requirements

- Hardware Requirements
 - Any processor capable of operating IMS Version 6 and later, and/or DB2 for OS/390 Version 6 and later
 - Any processor that supports the IBM Cryptographic Coprocessor Feature (CCF)
 - The hardware CCF modules must be enabled with configuration data (a separately orderable feature) and require a processor power-on-reset to complete the loading of the data into the crypto modules
 - Before use of the hardware encryption can occur, the hardware modules must be loaded with at least host DES master keys
- Software Requirements
 - IMS Version 6 or higher, and/or DB2 for OS/390 Version 6 or higher
 - OS/390 or z/OS Integrated Cryptographic Service Facility (ICSF)

Hardware requirements - any hardware that supports IMS version 6 or later or DB2 Version 6 or later is supported. This means that all the processors that DB2 V6 and IMS V6 run on have the crypto hardware. The crypto hardware must be enabled, and you must do a power-on-reset to enable the CCF modules.

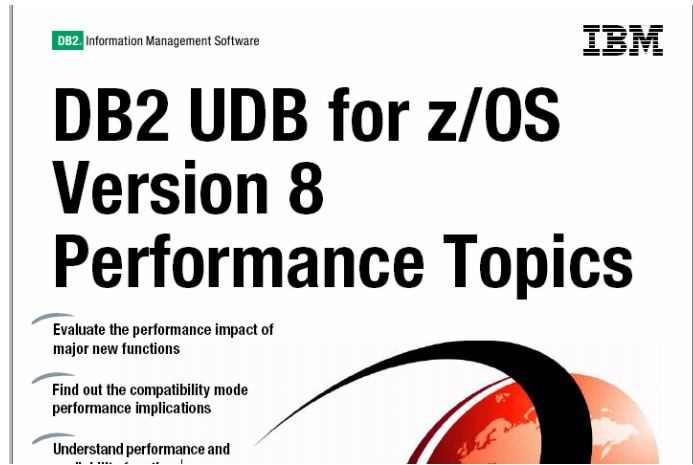
Software requirements - IMS Version 6 or higher and/or DB2 Version 6 or higher. ICSF, which is a part of the z/OS operating system, is also required. ICSF is not an add-on price feature. It is a base element of z/OS and OS/390.

What about built-in encryption functions in DB2 for z/OS?

- Different solution to a different problem
 - Column/cell based encryption
 - Application passes password in SQL statements for each cell
 - Application must manage keys (very difficult to do correctly)
 - Uses the same crypto hardware (fast)
 - No password/key management provided
- Could be used in conjunction with the Data Encryption for IMS and DB2 Databases product

Comparisons of encryption functions in DB2 V8 versus encryption of the data on disk versus encryption of data on the wire: All use encryption, but the techniques and objectives are very different. See the discussion comparing performance of the encryption tool versus BIFs in the V8 Performance Topics redbook, SG24-6465, section 4.8.

What about encryption performance?



See section 4.8

See the discussion comparing performance of the encryption tool versus BIFs in the V8 Performance Topics redbook, SG24-6465, section 4.8. The performance implications for encryption are roughly similar to data compression when only considering CPU overhead. In this section, we introduce both DB2 encryption and the IBM Data Encryption Tool and discuss recent hardware enhancements that improve encryption performance.

IBM Software Group | DB2 Information Management Software IBM

VIEW NOW **COMPUTERWORLD** **Security**

SEARCH Google™ Custom

Expert finds 'stupid' vulnerabilities in Oracle 11g

Summer Lemon [Today's Top Stories](#) or [Other Security Stories](#)

Comments (0) Recommendations: 7 — [Recommend this article](#)

September 03, 2007 (IDG News Service) — The latest version of Oracle Corp.'s flagship database offers better security than earlier versions, but development errors have left vulnerabilities that attackers can use to steal data, an expert warned Monday.

"Oracle made big progress with 11g, but some of the vulnerabilities I've found so far in 11g are stupid programming errors," said Alexander Kornbrust, managing director of Red Database Security GmbH, during an interview at the Hack In The Box (HITB) Security Conference 2007 in Kuala Lumpur, Malaysia.

"Oracle must educate their own development team because they should normally avoid these simple security vulnerabilities," Kornbrust said.

Oracle executives were not immediately available for comment.

Kornbrust, who helps large companies audit the security of their Oracle databases, examined the software and found SQL injection vulnerabilities, which allow attackers to run malicious code. He also uncovered a way to circumvent the auditing capability in 11g and other versions of the database, which could undermine a company's

SONICWALL EMAIL SECURITY

TAKE A DEEPER LOOK.

MORE RELATE

- HITB - Expert 1 vulnerabilities
- Corporate Exp data warehou
- Oracle to char key 11g datab

TODAY'S TOP

- Custom-built eBay account
- ISO votes to Microsoft's O standard
- Cisco jumps i wireless mar switch

Here is a September 3, 2007 headline in ComputerWorld security. The article speaks for itself. On the one hand, we see security as a significant part of the value in DB2, so we are not very likely to see this headline. Thorough testing for security and working through a Common Criteria ISO standard is helping to avoid such vulnerabilities.

There are challenges in implementations and understanding for security administrators.

IBM Software Group | DB2 Information Management Software IBM

TECH DISPENSER
Tech blogs filtered by humans, not bots

COMPUTERWORLD
Security IDG

JUMP TO More Resources SEARCH Google Custom Search GO

- Home
- News
- E-mail Newsletters
- Tech Dispenser
- + Shark Bait
- Knowledge Centers
 - + Operating Systems
 - + Networking & Internet
 - + Mobile & Wireless
- Security
 - + Cybercrime & Hacking
 - + Spam, Malware & Vulnerabilities
 - + Security Hardware & Software
 - + Standards & Legal Issues
 - + Privacy
 - + Intellectual Property & DRM
 - + Disaster Recovery
 - + Storage
 - + Business Intelligence
 - + Servers & Data Center
 - + Hardware
 - + Software
 - + Development
 - + Careers
 - + Management
 - + Government
- Opinion/Blogs
 - + Columnists
 - + Blogs
 - + SharkTank

Update: Two-thirds of Oracle DBAs don't apply security patches

Complexity of task makes admins not want to bother

Jaikumar Vijayan [Today's Top Stories](#) or [Other Security Stories](#)

Comments (7) Recommendations: 28 — [Recommend this article](#)

January 14, 2008 (Computerworld) -- Oracle Corp. issues dozens of security patches every quarter, but that doesn't mean database administrators are necessarily implementing them.

In fact, a good two-thirds of all Oracle DBAs appear not to be installing Oracle's security patches at all, no matter how critical the vulnerabilities may be, according to survey results from Sentrigo Inc., a Woburn, Mass.-based vendor of database security products.

The results are "surprising, and to be candid, quite frightening," said Mike Rothman, president of consulting firm Security Incite in Atlanta.

Sentrigo polled 305 Oracle database administrators from 14 Oracle user groups between August 2007 and January 2008. The company basically asked the administrators two questions: whether they had installed the latest Oracle patches, and whether they had ever installed any of Oracle's security updates.

The results, which come even as Oracle is scheduled to release its **next batch** of quarterly Critical Patch Updates tomorrow, showed that 206 out of the 305 surveyed said they had never applied any Oracle CPUs. Just 31 said they had installed the most recent security update from the company. In total, only one-third said they had ever installed an Oracle CPU.

In an e-mailed statement, Oracle said the company encourages administrators to apply



Get enterprise IT news headlines in your inbox

[FREE Newsletters](#)

MORE RELATED CONTENT

- Oracle preps critical security patches for next week
- Outlasting the Competition: Why High Availability is Critical to Midsize Businesses
- Oracle Virtual Server Unlikely to Blunt VMware

TODAY'S TOP STORIES

- Michigan voting officials confident of e-voting systems
- IBM warns of flaw in Tivoli Storage Manager Express
- The R Word: Are you prepared for a recession?

[More top stories](#)

IDG RELATED CONTENT

- Mac security program tries to

January 14, 2008 ([Computerworld](#)) -- [Oracle Corp.](#) issues dozens of security patches every quarter, but that doesn't mean database administrators are necessarily implementing them.

In fact, a good two-thirds of all Oracle DBAs appear not to be installing Oracle's security patches at all, no matter how critical the vulnerabilities may be, according to survey results from Sentrigo Inc., a Woburn, Mass.-based vendor of database security products.

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9057226&source=NLT_SEC&nId=38

Top Security Requirements beyond DB2 9

1. Fine grained access control
2. SYSADM & DBADM privilege finer granularity
3. SYSADM, DBADM without read
4. FIPS 140-2 compliance (encryption)
5. Generic wild cards for authorization
6. Cascade revoke control
7. Allow multiple authorities for DDL and BIND
8. Audits for read, completeness, data, any alter
9. ACEE accessibility, doc
10. RACF access control usability
11. Exit cached id, owner passed always, clear caches
12. Low level access control
13. Kerberos client support
14. Improve security, integrity, encryption capabilities

1. Fine Grained Access Control (FGAC) - Ability to restrict end user access to individual cells in the table. Allows user to specify the value that should be returned when access is denied. For example, credit card account number might be returned as 'xxxx xxxxxxxx1234' - showing only the last 4 digits to unauthorized query users. We need to compare and contrast with tools like Test Database Generator and Entity Analytic Solutions.
2. New SYSADM & DBADM privileges with finer granularity - SYSADM and DBADM are too coarse-grained. Introduce new privileges (SECADM, EXPLAIN, DDLADM, DBMAINT, DB2ADM) that have granularity that resembles how customers divide their job tasks. We want customers to be able to perform DBA work without having access to read the data. Some customers have also requested a SECADM whose actions don't take effect until another SECADM approves them. We do have DBMAINT and DBCTRL authorities today, with almost no usage.
3. SYSADM & DBADM without the ability to read or access data is one specific option for 2.
4. FIPS FIPS 140-2 compliance which is required for a vendor to qualify for selection by a US government agency for IT product bids. SWG offerings with cryptographic function must meet this compliance requirement so that they can be marketed to the Federal Sector. DB2 has a number of changes that must be made to allow compliance.
5. Generic wild cards are needed in many places for authorization. It may not coexist with cascade delete.
6. Cascade revoke is the relational standard, but it's often more of a problem when an administrator changes jobs. Roles and groups are crucial for administration, but individual authority has been used for a long time, and the process of revoking without cascade is too difficult.
7. Allow multiple authority for DDL, BIND too after taking out cascade revoke. This also would take quite a bit of work, but would deliver a lot of value. Currently there is a situation for install sysadm that does not provide a cascade revoke, so perhaps that case can be broadened without a high cost.
8. 3. Audit trace for RENAME statement, all DDL, access success, ... These changes are needed to make our security story more complete.
9. 4. Many different problems, but need clean description (probably from RACF about conditions for having an ACEE. Missing ACEE for outbind, other DB2 issues?

V8 Built-in Functions for Encryption

- ENCRYPT_TDES encrypt a column in a table with a user-provided encryption password
- ENCRYPTION PASSWORD special register
- DECRYPT_BIT, DECRYPT_CHAR, DECRYPT_DB
- GET_HINT obtain hint to help remember ENCRYPTION PASSWORD
- GENERATE_UNIQUE creates CHAR(13) FOR BIT DATA value that is unique across Sysplex
- DRDA encryption on the wire

Functions ENCRYPT_TDES (triple DES), DECRYPT_BIN, DECRYPT_CHAR, and GETHINT are added. The SET ENCRYPTION PASSWORD statement allows the application to specify a password

The ability to generate a unique value is also included. These changes came in DB2 for Linux, UNIX and Windows V8, so this change improves DB2 family consistency.

DRDA is extended to allow encryption of the data being sent. The DB2 Connect change is provided V8.2.