Session RAA12
DB2 10 for z/OS Security Features: A New Standard in Data Protection

Gayathiri Chandran
IBM Silicon Valley Laboratory
gchandran@us.ibm.com

© 2009 IBM Corporation

DB2 for z/OS

Acknowledgments and Disclaimers:

Availability. References in this presentation to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates.

The workshops, sessions and materials have been prepared by IBM or the session speakers and reflect their own views. They are provided for informational purposes only, and are neither intended to, nor shall have the effect of being, legal or other guidance or advice to any participant. While efforts were made to verify the completeness and accuracy of the information contained in this presentation, it is provided AS-IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, this presentation or any other materials. Nothing contained in this presentation is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software.

All customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer. Nothing contained in these materials is intended to, nor shall have the effect of, stating or implying that any activities undertaken by you will result in any specific sales, revenue growth or other results.

© Copyright IBM Corporation 2012. All rights reserved.

- U.S. Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp

IBM, the IBM logo, ibm.com, DB2, RACF are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at www.ibm.com/legal/copytrade.sht

Other company, product, or service names may be trademarks or service marks of others.

Please note

IBM's statements regarding its plans, directions, and intent are subject to change or withdrawal without notice at IBM's sole discretion.

Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision.

The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Information about potential future products may not be incorporated into any contract. The development, release, and timing of any future features or functionality described for our products remains at our sole discretion.

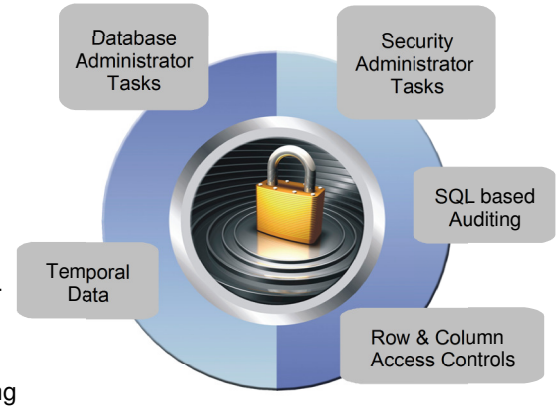
Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon many factors, including considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve results similar to those stated here.

Agenda

- DB2 10 Administrative Authorities
- Audit policies
- Security features to audit remote access
- Temporal tables
- Row and column level access controls
- Security update for DB2 10 and beyond

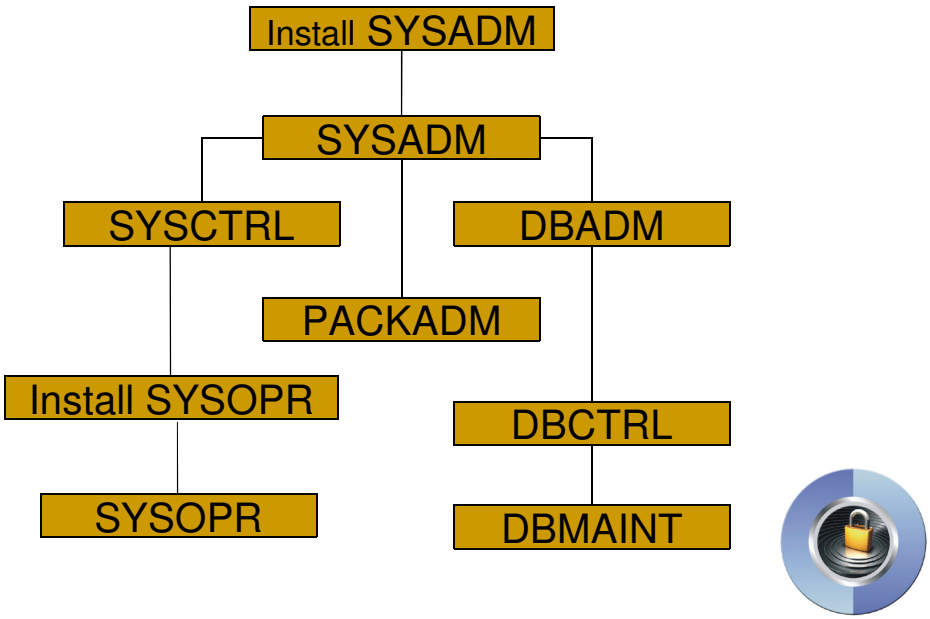
Satisfy Your Auditor: Plan, Protect and Audit

- Data Access
  - Minimize the use of a superuser authorities such as SYSADM
  - A different group should manage access to restricted data than the owner of the data
- Data Auditing
  - Any dynamic access or use of a privileged authority needs to be included in your audit trail
  - Maintain historical versions of data for years or during a business period
- Data Privacy
  - All dynamic access to tables containing restricted data needs to be protected

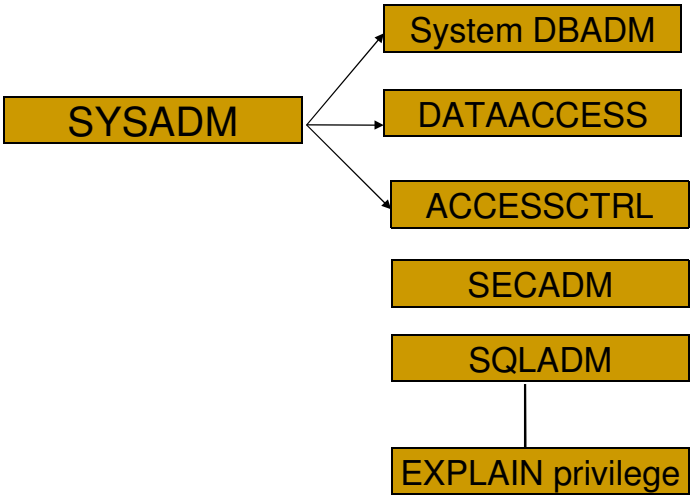


Today's Mainframe:
The power of industry-leading security,
the simplicity of centralised management

Administrative Authorities – Prior to DB2 10



DB2 10: New granular System Authorities



New authority for performing security tasks without ability to change or access data

- **SECADM authority**
  - Allows the user to
    - Issue SQL GRANT, REVOKE statements on all grantable privileges and administrative authorities
    - Manage DB2 9 roles and trusted contexts
    - Manage DB2 10 row permissions and column masks
    - Manage DB2 10 Audit policies
    - Access catalog tables
    - Issue START, STOP, and DISPLAY TRACE commands
  - Can access DB2 in ACCESS(MAINT) mode

New authority for managing objects without ability to access data or control access to data

- **System DBADM authority**
  - Allows the user to
    - Issue SQL CREATE, ALTER, DROP statements to manage most objects in the DB2 subsystem
      - Exception: Security objects, system objects
      - Additional privileges required to create objects such as views, functions, triggers
    - Issue most DB2 commands
    - Execute system defined stored procedures and functions
    - Access catalog tables

New authority for accessing data without the ability to manage data or control access to data

- **DATAACCESS authority**
  - Allows the user to
    - Issue SQL SELECT, INSERT, UPDATE, DELETE statements on all user tables, views, materialized query tables
    - Execute all plans, packages and routines
    - Run RECOVERDB, REORG, REPAIR, LOAD utilities on all user databases
    - Issue ALTER and TERM UTILITY commands
    - Access catalog tables

New authority for controlling access to data without ability to manage or access data

- **ACCESSCTRL authority**
  - Allows the user to
    - Issue SQL GRANT, REVOKE statements on most grantable privileges and administrative authorities
      - Exceptions:
      - System DBADM, DATAACCESS, ACCESSCTRL authorities
      - Security privilege, CREATE_SECURE_OBJECT
    - Access catalog tables

New authority for monitoring and tuning SQL without ability to change or access data

- **SQLADM authority**
  - Allows the user to
    - Issue SQL EXPLAIN statements
    - Issue START, STOP, and DISPLAY PROFILE commands
    - Execute system defined stored procedures and functions
    - Access catalog tables
  - Performs actions involving:
    - EXPLAIN privilege
    - STATS privilege on all user databases
    - MONITOR2 privilege
  - Cannot access data, perform DDL or execute

New privilege to validate SQL before moving application into production without risk to data

- **EXPLAIN privilege**
  - Allows the user to
    - Issue SQL EXPLAIN ALL statement without having the privileges to execute that SQL statement
    - Issue SQL PREPARE and DESCRIBE TABLE statements without requiring any privileges on the object.
    - Specify new BIND EXPLAIN(ONLY) and SQLERROR(CHECK) options
    - Explain dynamic SQL statements executing under new special register, CURRENT EXPLAIN MODE = EXPLAIN

New Install security parameters

SEPARATE_SECURITY - Prevents SYSADM and SYSCTRL from performing security functions:

- New separate security install zparm parameter
- New install SECADM authority manages subsystem security
- SYSADM and SYSCTRL can no longer implicitly grant or revoke privileges

REVOKE_DEP_PRIVILEGES - Controls cascading effect of revokes:

- New revoke dependent privileges install parameter
- New revoke dependent privileges SQL clause
  - INCLUDING DEPENDENT PRIVILEGES
  - NOT INCLUDING DEPENDENT PRIVILEGES

RACF support for the new Administrative Authorities

- RACF Access Control Module ('SYS1.SDSNSAMP (DSNXRXAC)') has been enhanced to
  - Honor the setting of SEPARATE_SECURITY
  - Implement the new DB2 administrative authorities as RACF resource checks

DB2 Authority	Resource	Class
SECADM	<subsystem>.SECADM	DSNADM
System DBADM	<subsystem>.SYSDBADM	DSNADM
DATAACCESS	<subsystem>.DATAACCESS	DSNADM
ACCESSCTRL	<subsystem>.ACCESSCTRL	DSNADM
SQLADM	<subsystem>.SQLADM	MDSNSM
EXPLAIN	<subsystem>.EXPLAIN	MDSNSM

Satisfy Your Auditor:

New Audit policies provide needed flexibility and functionality

- New auditing capability allows you to comply without the need of external data collectors
  - New audit policies managed in catalog
  - Audit privileged users
    - Records each use of an admin authority
  - Audit any access to specific tables for specific programs
    - Generates records for all read and write access for statements with unique statement qualifier
  - Audit distributed identities

How to exploit Audit policies

- Security administrator using the new SECADM authority maintains DB2 audit policies in a new catalog table
  - SYSIBM.SYSAUDITPOLICIES
- Audit policies enabled using –STA TRACE command
- Audit policies disabled using –STO TRACE command
- Up to 8 audit policies can be specified to auto start or auto start as secure during DB2 start up
- Only user with SECADM authority can stop a secure audit policy trace

Audit policy categories

Categories	Mapping IFCIDs
CHECKING	IFCID 83 (only authentication failures), IFCID 140
VALIDATE	IFCIDs 55, 83, 87, 169, 269, 319
OBJMAINT	IFCID 142
EXECUTE	IFCIDs 143, 144, 145
CONTEXT	IFCIDs 23, 24, 25
SECMAINT	IFCIDs 141, 270, 271
SYSADMIN	IFCID 361 (Audits installation SYSADM, installation SYSOPR, SYSOPR, SYSCTRL, SYSADM)
DBADMIN	IFCID 361 (Audits DBMAINT, DBCTRL, DBADM, PACKADM, SQLADM, system DBADM, DATAACCESS, ACCESSCTRL, SECADM)

Audit Policies – Dynamic auditing of tables

- Auditor audit access to specific tables for specific programs during day
  - Audit policy does not require AUDIT clause to be specified using DDL to enable auditing
  - Audit policy generate records for all read and update access not just first access
  - Audit policy includes additional records identifying the specific SQL statements
  - Audit policy provides wildcarding of based on schema and table names

Example: Dynamic auditing of tables

- Audit all the tables that start with 'PAY' in EMPLOYEE schema
  - Does not require AUDIT clause to be specified during table definition

```
INSERT INTO SYSIBM.SYSAUDITPOLICIES (AUDITPOLICYNAME,
OBJECTSCHEMA, OBJECTNAME, OBJECTTYPE, EXECUTE)
  VALUES ('TABADT1','EMPLOYEE',"'PAY%'",'T','A');

-STA TRACE (AUDIT) DEST (GTF) AUDTPLCY(TABADT1);
```

Audit Policies – Audit privileged authority

- New trace record (IFCID 361) to identify any unusual use of a privileged authority, when using DB2 native authorization
  - Records each use of a system authority
  - Audit records written only when authority is used for access
  - External collectors only report users with a system authority
- If Access Control Authorization Exit is active, then only operations performed by installation SYSADM and installation SYSOPR are audited by IFCID 361 trace
  - RACF provides similar capability with AUDIT(ALL) keyword for the profiles

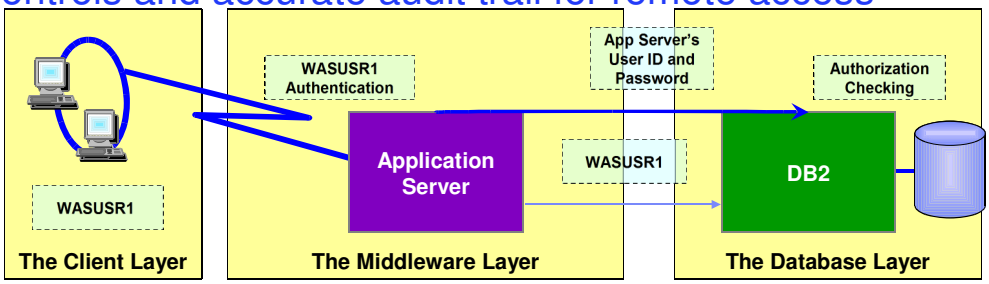
Example – Audit privileged authority

- Audit successful execution of all actions using installation SYSADM authority and system DBADM authority

```
INSERT INTO SYSIBM.SYSAUDITPOLICIES
  (AUDITPOLICYNAME, SYSADMIN, DBADMIN)
 VALUES ('AUDITADMIN','I','B');

-STA TRACE (AUDIT) DEST (GTF) AUDTPLCY(AUDITADMIN);
```

New improved security features provide more effective controls and accurate audit trail for remote access



- The application server's user ID and password are used to establish the trusted connection
- The user is switched in the trusted connection and client user ID is propagated to the server and checked for database access
- DB2 10 support for distributed identities introduced in z/OS V1R11 allows to map client user ID to RACF user ID
  - A distributed identity is a mapping between a RACF user ID and one or more distributed user identities, as they are known to application servers
  - Distributed identities are part of the DB2 audit log.

New improved security features provide more effective controls and accurate audit trail for remote access

- Support client certificate authentication in z/OS V1R10
  - AT-TLS secure handshake accomplishes identification and authentication for client certificates
  - DB2 client driver presents its certificate as identification and its *proof-of-possession* as authentication
  - DB2 server can retrieve the user ID associated with the client certificate in SAF for the AT-TLS policy rule configuration:
    HandshakeRole = ServerWithClientAuth
    ClientAuthType = SAFCheck
  - RACF certificate name filtering (RACDCERT MAP command) can map many certificates with one RACF userid

New improved security features provide more effective controls and accurate audit trail for remote access

- Support password phrases in z/OS V1R10
  - A RACF password phrase is a character string made up of mixed-case letters, numbers, special characters, and is between 9 to 100 characters long
  - Can be used instead of a traditional 8-character password
- Support connection level security enforcement using strong authentication
  - DRDA encryption is not intended to provide confidentiality and integrity of passwords or data over a network that is not secure, such as the Internet.
  - Subsystem parameter, TCPALVER value SERVER_ENCRYPT enforces connections must use strong authentication to access DB2
  - All userids and passwords encrypted using AES, or connections accepted on a port which ensures AT-TLS policy protection or protected by an IPSec encrypted tunnel

Satisfy Your Auditor:
DB2 can now manage different versions of your data

- Application programmers and database administrators have struggled for years with managing different versions of application data.
- New regulatory laws require maintaining historical versions of data for years.
- Every update and delete of data requires applications to copy data to history tables.
- Existing approaches to application level data versioning complicate table design, add complexity and are error prone for applications.

New Temporal table

- New Temporal table allows DB2 to automatically maintain different versions of your data
- Two types of time sequences of table rows are supported through the introduction of database defined time periods
  - SYSTEM_TIME is used to support data “versioning” which archives old rows into a history table
  - BUSINESS_TIME is a period that represents when a row is valid to the user or application
  - BITEMPORAL table combines SYSTEM_TIME period and BUSINESS_TIME period

Defining system period on an existing table

- System versioning is implemented by altering an existing or creating a table with two timestamps, a history table, and defining the versioning relationship between tables
- After the base and history tables are appropriately defined:
  - ALTER TABLE table-name ADD VERSIONING is specified on the base table that is to be versioned
- Auditor can query historical data through SQL
  - DB2 rewrites the user’s query to include data from the history table

Satisfy Your Auditor:

New table controls to protect against unplanned SQL access

- Define additional data controls at the row and column level
  - Security policies are defined using SQL
  - Separate security logic from application logic
- Security policies based on real time session attributes
  - Protects against SQL injection attacks
  - Determines how column values are returned
  - Determines which rows are returned
- All access via SQL including privileged users, adhoc query tools, report generation tools is protected
- Policies can be added, modified, or removed to meet current company rules without change to applications

Table controls to protect SQL access to individual row level

- Establish a row policy for a table
  - Filter rows out of answer set
  - Policy can use session information, e.g. the SQL ID is in what group or user is using what role, to control which row is returned in result set
  - Applicable to SELECT, INSERT, UPDATE, DELETE, & MERGE
  - Defined as a row permission:

```
CREATE PERMISSION policy-name ON table-name
    FOR ROWS WHERE search-condition
    ENFORCED FOR ALL ACCESS ENABLE;
```

Table controls to protect SQL access to individual column level

- Establish a column policy for a table
  - Mask column values in answer set
  - Policy can use session information, e.g. the SQL ID is in what group or user is using what role, to control what masked value is returned in result set
  - Applicable to the output of outermost subselect
  - Defined as column masks :

CREATE MASK mask-name ON table-name
FOR COLUMN column-name RETURN CASE-expression
ENABLE;

Define table policies based on who or how the table is being accessed

- SESSION_USER - Primary authorization ID of the process
- CURRENT SQLID - SQL authorization ID of the process
- VERIFY_GROUP_FOR_USER function
  - Get the authorization IDs for the value in SESSION_USER
  - Returns 1 if any of those authorization IDs is in the argument list

```
WHERE
   VERIFY_GROUP_FOR_USER (SESSION_USER, 'MGR', 'PAYROLL') = 1
```

- VERIFY_ROLE_FOR_USER function
  - Get the role for the value in SESSION_USER
  - Return 1 if the role is in the argument list

```
WHERE
   VERIFY_ROLE_FOR_USER (SESSION_USER, 'MGR', 'PAYROLL') = 1
```

Managing row and column access controls

- When activated row and column access controls:
  - All row permissions and column masks become effective in all DML
  - All row permissions are connected with 'OR' to filter out rows
  - All column masks are applied to mask output
  - All access to the table is prevented if no user-defined row permissions

```
ALTER  TABLE   table-name
   ACTIVATE ROW        ACCESS  CONTROL
   ACTIVATE COLUMN  ACCESS CONTROL;
```


Managing row and column access controls

- When deactivated row and column access controls:
  - Make row permissions and column masks become ineffective in DML
  - Opens all access to the table

```
ALTER  TABLE   table-name
   DEACTIVATE ROW       ACCESS  CONTROL
   DEACTIVATE COLUMN ACCESS CONTROL;
```

Example – A simple banking scenario

- Only allow customer service representatives to see customer data but always with masked income
- Table: CUSTOMER

Account	Name	Phone	Income	Branch
1111-2222-3333-4444	Alice	111-1111	22,000	A
2222-3333-4444-5555	Bob	222-2222	71,000	B
3333-4444-5555-6666	Louis	333-3333	123,000	B
4444-5555-6666-7777	David	444-4444	172,000	C

Define row and column access control on customer table

- **Define row and column policies for customer service representatives**
  - Allow access to all customers of the bank (a row permission)
  - Mask all INCOME values (a column mask)
    - Return value 0 for incomes of 25000 and below
    - Return value 1 for incomes between 25000 and 75000
    - Return value 2 for incomes between 75000 and 150000
    - Return value 3 for incomes above 150000
  - Customer service representatives are in the CSR group (who)

Create Row Permission

- Create a row permission for customer service representatives

```
CREATE  PERMISSION  CSR_ROW_ACCESS  ON  CUSTOMER
    FOR  ROWS  WHERE
        VERIFY_GROUP_FOR_USER (SESSION_USER, 'CSR') = 1
ENFORCED FOR ALL ACCESS ENABLE;
```


Create Column Mask

- Create a column mask on INCOME column for customer service representatives

```
CREATE  MASK  INCOME_COLUMN_MASK  ON  CUSTOMER
   FOR  COLUMN  INCOME  RETURN
     CASE WHEN (VERIFY_GROUP_FOR_USER (SESSION_USER, 'CSR') = 1)

                THEN  CASE  WHEN (INCOME > 150000) THEN  3
                            WHEN (INCOME > 75000)   THEN  2
                            WHEN (INCOME > 25000)   THEN  1
                            ELSE  0
                      END

           ELSE NULL
      END
ENABLE;
```

Start enforcing row and column access control on customer table

- Activate Row and Column Access Control

```
ALTER  TABLE  CUSTOMER
    ACTIVATE ROW       ACCESS CONTROL
    ACTIVATE COLUMN ACCESS CONTROL;
COMMIT;
```

What happens in DB2?

- A default row permission is created implicitly to prevent all access to table CUSTOMER (WHERE 1=0) except for users in the CSR group
- All packages and cached statements that reference table CUSTOMER are invalidated

Selecting from customer table … after row and column access control activated

- SELECT ACCOUNT, NAME, INCOME, PHONE FROM CUSTOMER;

ACCOUNT	NAME	INCOME	PHONE
1111-2222-3333-4444	Alice	0	111-1111
2222-3333-4444-5555	Bob	1	222-2222
3333-4444-5555-6666	Louis	2	333-3333
4444-5555-6666-7777	David	3	444-4444

INCOME automatically masked by DB2!

DB2 effectively evaluates the following revised query

```
SELECT  ACCOUNT,
          NAME,

          CASE WHEN (VERIFY_GROUP_FOR_USER (SESSION_USER, 'CSR') = 1)
                    THEN CASE  WHEN (INCOME > 150000) THEN 3
                               WHEN (INCOME > 75000)    THEN 2
                               WHEN (INCOME > 25000)    THEN 1
                               ELSE  0
                          END
               ELSE NULL
          END  INCOME,

        PHONE
FROM  CUSTOMER

WHERE  VERIFY_GROUP_FOR_USER (SESSION_USER, 'CSR') = 1   OR   1 = 0 ;
```


Security Updates for DB2 10 and beyond

- External Security (DSNX@XAC) consistency with DB2 Security
  - Support OWNER privileges for authorization
    - Allows owner to be checked for authorization on BIND and REBIND commands
    - Supports dynamic SQL authorization using DYNAMICRULES behavior
    - Allows automatic rebind
  - Refresh authorization related caches and invalidate dependent packages when external security permissions change
    - Uses z/OS event notification called ENF signals to indicate security permissions change

Security Updates for DB2 10 and beyond

- Allow the plan owner to sign a DB2 production application program
  - Owner controls the packages an application can use by defining a package list
  - Package lists are difficult to manage causing the use of wild cards
  - Owner associates a program signature with the application plan
  - DB2 verifies the signature prior to allowing the plan to execute

DB2 Security updates

- PM27835 – Provides the capability for IMS to communicate ACEE to DB2 for external authorization
- PM43292 - Allows RACF protected userids to be PASSTICKET authenticated
- PM64332 – Digital certificate authentication enhancement
- PM69429 – Trusted context support for CAF
- PM61099 – Row and Column Access control changes
  - Authorization update for TRUNCATE on row access control activated table
  - Column mask rules change:
    - INSERT or UPDATE from a subselect
    - Aggregate function with DISTINCT keyword
- PM81247 – Issue -551 if user with EXPLAIN privilege executes a statement

DB2 10 for z/OS Security Enhancements
Help Satisfy Your Auditors using new features

- ✓ New granular authorities to reduce data exposure for administrators
- ✓ New auditing features using new audit policies comply with new laws
- ✓ New temporal data to comply with regulations to maintain historical data
- ✓ New row and column access table controls to safe guard your data

References

- Security Functions of IBM DB2 10 for z/OS (SG24-7959-00)
  - **http://www.redbooks.ibm.com**

DB2 10 for z/OS Technical Overview (SG24-7892-00)
  - **http://www.redbooks.ibm.com**

DB2 10 for z/OS Managing Security (SC19-3496-01)
  - **http://publib.boulder.ibm.com/infocenter/dzichelp/v2r2/topic/com.ibm.db2z10.doc.seca/src/seca/db2z_seca.htm**

DB2 10 for z/OS Administration Guide (SC19-2968-02)
  - **http://publib.boulder.ibm.com/infocenter/dzichelp/v2r2/topic/com.ibm.db2z10.doc.admin/src/admin/db2z_admin.htm**

DB2 10 for z/OS RACF Access Control Module Guide (SC19-2982-02)
  - **http://publib.boulder.ibm.com/infocenter/dzichelp/v2r2/topic/com.ibm.db2z10.doc.racf/src/racf/db2z_racf.htm**

DB2 9 for z/OS: Configuring SSL for Secure Client-Server communications - Red paper
  - **http://www.redbooks.ibm.com/abstracts/redp4630.html?Open**

DB2 10 for z/OS: Configuring SSL for Secure Client-Server communications - Red paper
  - http://www.redbooks.ibm.com/redpieces/abstracts/redp4799.html?Open

DB2 for z/OS Information Center
  - **http://publib.boulder.ibm.com/infocenter/dzichelp/v2r2/index.jsp**


Thank
You