DB2 Exam 610 Summary

Zeyuan Hu

January 3, 2016

Contents

1 Planning

1.1 Objectives

- Knowledge of DB2 products (z/OS vs LUW vs pureScale - at a high-level; different products and what they do)
- Knowledge of database workloads (appropriate DB2 product to use - OLTP vs warehousing)
- Knowledge of non-relational data concepts (XML data, LOB data)

1.2 Database workloads

Two main types of database application workloads:

- online transactional processing (OLTP)
- data warehousing
  - reporting
  - online analytical processing (OLAP)
  - data mining applications
  - decision support

1.3 OLTP vs. Data Warehousing

An OLTP system is typical of a web order system, where you perform transactions over the web (such as ordering a product). Online transaction processing (OLTP) systems features:

- Support day-to-day, mission-critical business activities (ie. web-based order entry, stock trading) [*current data*]
- Support hundreds to thousands of users issuing millions of transactions per day against databases that vary in size [*Frequent updates, Granular transactions*]
- Response time requirements tend to be subsecond [*Sub-second response time*]
- Queries:
  - tend to be a mix of real-time insert, update, and delete operations against current-as opposed to historical-data
  - single-row lookups with logic that likely updates a small number of records

Data warehousing system typically consist of:

- Store and manage large volumes of data that is often historical in nature and is used primarily for analysis [*Voluminous historical data*]
- Optimized for queries

- Heterogeneous data sources
- Queries: (ie. [*Summarized queries that perform aggregations and joins*])
  - bulk load operations
  - short-running queries
  - long-running complex queries
  - random queries
  - occasional updates to data
  - execution of online utilities

Example 1. *A database will be used primarily to identify sales patterns for products sold within the last three years and to summarize sales by region, on a quarterly basis. In case, a Data warehouse system is needed.*

Remark. *Different by queries that are typically used to access the data (aka workloads).*

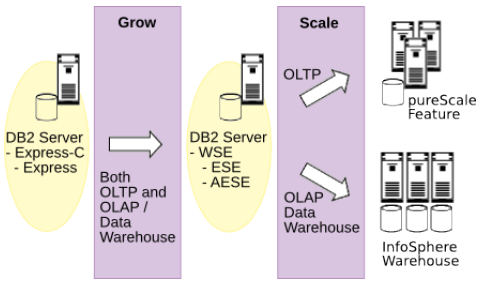

Figure 1: DB2 products, OLTP, Data Warehouse

1.4 DB2 pureScale - IBM solution for OLTP

System highlights:

- Best suited for OLTP workloads
- Enables a `DB2 for LUW` database to continously process incoming requests, even if multiple system components fail simultaneously, which makes it ideal for OLTP workloads where high availability is crucial
- Provides a database cluster solution for nonmainframe platforms
- Can **ONLY** work with the General Parallel File System (GFPS) file system

Usage:

- Can be used with `DB2 Workgroup Server Edition (WSE)`, `DB2 Enterprise Server Edition (ESE)`, `DB2 Advanced Enterprise Server Edition(AESE)`

- Can **ONLY** be installed on IBM p Series or x Series servers that are running either the AIX (p Series) or the Linux (x Series) operating system
- **CANNOT** be installed on IBM mainframes running z/OS, IBM p Series server running Linux, or IBM x Series servers running Windows

1.5 InfoSphere Warehouse - IBM solution for Data warehousing

System highlights:

- is a complete data warehousing solution that contains components that facilitate data warehouse construction and administration, as well as tools that enable embedded data mining and multidimensional online analytical processing (OLAP)

1.6 Notable DB2 features & products

IBM Data Studio

- is an Eclipse-based, integrated development environment (IDE) that can be used to perform instance and database administration, routine (SQL procedure, SQL functions, etc.) and application development, and performance-tuning tasks.
- replaces the `DB2 Control Center` as the standard GUI tool for DB2 database administration and application development.
- allows users to connect to a DB2 database using a wizard; however, users are required to provide login credentials before a connection will be established.
- components:
  - `IBM Data Studio administration client`
    - can be installed on servers running Red Hat Linux, SUSE Linux, and Windows
    - **CANNOT** be installed on AIX servers
  - `IBM Data Studio full client`
    - can be installed on servers running Red Hat Linux, SUSE Linux, and Windows
  - `IBM Data Studio web console`
    - can be installed on servers running Red Hat Linux, SUSE Linux, and Windows
    - can be installed on servers running the AIX operating system as well

IBM Workload Manager (WLM)

- is a comprehensive workload management feature that can help identify, manage, and control database workloads to maximize database server throughput and resource utilization
- cutomize execution environments for the purpose of controlling system resources so that no single workload can control and consume all of the system resources available. (This prevents any one department or service class from overwhelming the system.)

IBM InfoSphere Optim Performance Manager Extended Edition

- can be used to identify, diagnose, solve, and prevent performance problems in DB2 products and associated applications including Java and DB2 Call Level Interface (CLI) applications.

Self-Tuning Memory Manager (STMM)

- responds to significant changes in a database's workload by dynamically distributing available memory resources among several different database memory consumers

Connection Concentrator

- improves the performance of applications that require frequent, but relatively transient, simultaneous user connections by allocating host database resources only for the duration of an SQL transaction,

IBM InfoSphere Data Architect

- A complete solution for designing, modeling, discovering, relating, and standardizing data assets.
- You can use it for data modeling, transformation, and DDL generation, and to build, debug, and manage database objects such as SQL stored procedures and functions.

IBM InfoSphere Optim Query Tuner (Query Tuner)

- can analyze and make recommendations on ways to tune existing queries, as well as provide expert advice on writing new queries.

IBM InfoSphere Optim pureQuery Runtime

- Lets you deploy advanced pureQuery applications that use static SQL for a wide range of benefits.
- Briges the gap between data and Java technology by harnessing the power of SQL within an easy-to-use Java data access platform.
- Increases security of Java applications helping to prevent threats like SQL injection.

DB2 for i

- combines with `IBM BLU Acceleration` to handle Analytical workloads
- formerly known as DB2 for i5/OS, is an advanced, 64-bit Relational Database Management System that leverages the high performance, virtualization, and energy efficiency features of IBM's Power Systems
- its self-managing attributes, security, and built-in analytical processing functions make `DB2 for i` an ideal database server for applications that are analytical in nature

DB2 pureXML

- offers a simple and efficient way to create a "hybrid" DB2 database that allows XML data to be storded in its native, hierarchical format.

Data Partitioning Feature (DPF)

- provides the ability to divide very large databases into multiple parts (known as partitions) and store them across a cluster of inexpensive servers.

1.7 DB2 offering

DB2 for z/OS

- full-function database management system that has been designed specifically for z/OS, IBM's flagship mainframe operating system.
- Tightly integrated with the IBM mainframe, `DB2 for z/OS` leverages the strengths of System z 64-bit architecture to provide, among other things, the ability to support complex data warehouse.

1.8 Large Objects (LOB)

LOB data types-**not LOB locators**-are used to store binary data values in a DB2 database.

- By default, LOB data is stored in separate LOB storage objects.
- Changes to LOB data are not recorded in transaction log files.

Inline LOBs

- improve query performance by storing LOB data in the same data pages as the rest of a table's rows, rather than in a separate LOB storage object.Thus, no additional I/O is needed to store and access this type of data.
- is eligible for compression.
- When a table contains columns with inline LOBs, fewer rows can fit on a page.
- transactions that modify inline LOB data are always logged. Consequently, the use of inline LOBs can **increase** logging overhead.
- are created by appending the `INLINE LENGTH` clause to a LOB column's definition.

LOB locator

- represents a value for a LOB resource that is stored in a database
- is a simple token value that is used to refer to a much bigger LOB value
- is a mechanism that refers to a LOB value from within a transaction
- is **NOT** a data type, nor is it a database object
- **do NOT** store copies of LOB data-they store a description of a base LOB value, and the actual data that a LOB locator refers to is only materialized when it is assigned to a specific location, such as an application host variable or another table record
- they behave as a snapshot of a piece of an LOB value, and not as a pointer to a row or a location in the database

1.9 XML data

- with `pureXML`, XML documents are stored in tables that contain one or more columns that have been defined with the XML data type.
- `CREATE TABLE employee (empid INT, resume XML)`

2 Security

2.1 Objectives

- Knowledge of restricting data access
- Knowledge of different privileges and authorities
- Given a DCL SQL statement, knowledge to identify results (grant/revoke/connect statements)
- Knowledge of Row and Column Access Control (RCAC)
- Knowledge of Roles and Trusted Contexts

Three levels of security:

- level 1: control access to the instance under which a database was created
- level 2: control access to the database itself
- level 3: control access to the data and data objects reside within the database

2.2 Authentication

- is the process by which a system verifies a user's identity.
- normally, an external facility (ie. OS, DCE) that is not pat of DB2 performs the authentication.
- *authentication type* for a server is a database manager configuration parameter to decide how and where users are authenticated.

Type	Description
SERVER	➔ Authentication occurs on the server
SERVER_ENCRYPT	➔ Authentication occurs on the server ➔ Passwords are encrypted at the client machine before being sent to the server
CLIENT	➔ Authentication occurs at the client workstation, with no further checks on the server
KERBEROS	➔ Authentication is performed by the Kerberos security software
KRB_SERVER_ENCRYPT	➔ Authentication is performed by Kerberos security software if the client's authentication type is set to KERBEROS. Otherwise, SERVER_ENCRYPT is used
DATA_ENCRYPT	➔ SERVER_ENCRYPT ➔ user data are encrypted
DATA_ENCRYPT_CMP	➔ DATA_ENCRYPT ➔ Use SERVER_ENCRYPT if DATA_ENCRYPT not supported
GSSPLUGIN	➔ Authentication is controlled by an external GSS-API plugin
GSS_SERVER_ENCRYPT	➔ GSSPLUGININ ➔ Use SERVER_ENCRYPT if GSSPLUGIN not supported

2.3 Authorities

- convey the right to perform high-level administrative and maintenance/utility operations on an instance or a database
- instance-level authorities:
  - System Administrator (**SYSADM**) authority:
    - Highest level of administrative authority at the instance level
    - Only a user with SYSADM authority can perform the following:
      - Upgrade a database
      - Restore a database
      - Change the database manager configuration file (including specifying the groups having SYSADM, SYSCTRL, SYSMAINT, or SYSMON authority)
      - Grant and revoke table space privileges and also use any table space
      - Perform any SQL or XQuery operation that does not attempt to access data that is protected by RCAC or LBAC.
    - When a user with SYSADM authority creates a database, that user is automatically granted ACCESSCTRL, DATAACCESS, DBADM, SECADM authority on the database.
  - Installation System Administrator (Installation SYSADM) authority:
    - Conveys the same set of abilities that SYSADM authority provides.
    - Can perform recovery operations when the system catalog for a database is inaccessible or unavailable.
  - System Control (**SYSCTRL**) authority:
    - Highest level of system and instance control authority
    - Intended to provide select users with nearly complete control of a DB2 system without letting them access sensitive data
    - Similar to SYSADM but cannot access any data within the databases unless they are granted the privileges required to do so.
    - Commands a SYSCTRL user can perform against any database in the instance are:
      - `db2start/db2stop`
      - `db2 create/drop database`
      - `db2 create/drop tablespace`
      - `db2 backup/restore/rollforward database`
      - `db2 runstats` (against any table)
      - `db2 update db cfg for database` dbname
  - System Operator (SYSOPER) authority:
    - the ability to execute all DB2 commands available *except* ARCHIVE LOG, START DATABASE, STOP DATABASE, and RECOVER BSDS.
    - run the DSN1SDMP utility, and terminate any running utility job.
  - Installation System Operator (Installation SYSOPER) authority:

    * SYSOPER authority
    * Perform select operations when the system catalog for a database is unavailable.
- System Maintenance (**SYSMAINT**) authority:
    * SYSMAINT users can only perform tasks related to mainenance (subset of SYSCTRL authority):
        · `db2start/db2stop`
        · `db2 backup/restore/rollforward database`
        · `db2 runstats` (against any table)
        · `db2 update db cfg for database` dbname
    * users with SYSMAINT **CANNOT** create or drop databases or tablespaces.
    * They cannot access any data within the databases unless they are granted the explicit privileges required to do so.
- System Monitor (**SYSMON**) authority:
    * Provides the ability to take database system monitor snapshots of an instance and its databases.
    * SYSMON authority enables the user to run the following commands:
        · `GET DATABASE MANAGER MONITOR SWITCHES`
        · `GET MONITOR SWITCHES`
        · `GET SNAPSHOT`
        · `LIST ACTIVE DATABASES`
        · `LIST APPLICATIONS`
        · `LIST DATABASE PARTITION GROUPS`
        · `LIST DCS APPLICATIONS`
        · `LIST PACKAGES`
        · `LIST TABLES`
        · `LIST TABLESPACE CONTAINERS`
        · `LIST TABLESPACE`
        · `LIST UTILITIES`
        · `RESET MONITOR`
        · `UPDATE MONITOR SWITCHES`
    * following APIs:
        · `db2GetSnapshot` - Get snapshot
        · `db2GetSnapshotSize` - Estimate size required for `db2GetSnapshot` output buffer
        · `db2MonitorSwitches` - Get/update monitor switches
        · `db2ResetMonitor` - Reset monitor
        · `db2mtrk` - Memory tracker
    * Users with the SYSADM, SYSCTRL or SYSMAINT authority level also possess SYSMON

- Database-level authorities:
  - Database Administrator (**DBADM**) authority:
    - DBADM users **CANNOT** perform such maintenance or administrative tasks as:
      - `db2 drop database`
      - `db2 drop/create tablespace`
      - `db2 backup/restore database`
      - `db2 update db cfg for database` dbname
    - DBADM users can perform the following tasks:
      - `db2 drop/create table` (index, views)
      - `db2 grant/revoke` (any privilege)
      - `db2 runstats` (any table)
    - access data stored in tables, views, including system catalog tables and views-provided that data is not protected by RCAC or LBAC
  - Database Control (DBCTRL) authority:
    - create database objects
    - issue database-specific DB2 commands
    - run DB2 utilities (*including those that change data*)
    - terminate any running utility *except* DIAGNOSE, REPORT, and STOSPACE
  - Database Maintenance (DBMAINT) authority:
    - create database objects
    - issue database-specific DB2 commands
    - run DB2 utilities that do not change data
    - terminate any running utility *except* DIAGNOSE, REPORT, and STOSPACE
  - Package Administrator (PACKADM) authority:
    - BIND, COPY, and EXECUTE privileges on all packages in one or more specific collections
    - BIND subcommand to create new packages in certain collections
  - System Database Administrator (System DBADM) authority:
    - create, alter and drop database objects
    - issue database-specific DB2 commands
    - run the following DB2 utilities:
      `CHECK INDEX, CHECK LOB, COPY, COPYTOCOPY, DIAGNOSE, MODIFY RECOVERY, MODIFY STATISTICS, QUIESCE, REBUILD INDEX, RECOVER, REPORT, RUNSTATS`
    - access and modified data stored in system catalog tables and views
    - **cannot** access user data
    - **cannot** grant and revoke authorities and privileges
  - Security Administrator (**SECADM**) authority:
    - can only be granted by a SYSADM user
    - CANNOT access user data and create databases

    * can perform the following:
        - Create and drop security label components
        - Create and drop security policies
        - Create and drop security labels
        - Grant and revoke security labels
        - Grant and revoke LBAC rule exemptions
        - Grant and revoke setsessionuser privileges
        - Grant and revoke database privileges and authorities
        - Execute the SQL statement `TRANSFER OWNERSHIP` on objects that you do not own
        - Execute the following audit routines:
            1. `SYSPROC.AUDIT_ARCHIVE` used to archive audit logs
            2. `SYSPROC.AUDIT_LIST_LOGS` used to locate audit files present in a specific directory
            3. `SYSPROC.AUDIT_DELIM_EXTRACT` used to extract audit data to delimited files format
    * No other user can perform these functions, not even the SYSADM, unless SECADM was explicitly granted to that SYSADM user
- Access Control (ACCESSCTRL) authority:
    * can only be granted by SECADM
    * cannot grant to PUBLIC group
    * can access and modify data stored in system catalog tables and views
    * cannot access or modify user data
    * issue following GRANT (and REVOKE) statements:
        - GRANT (Database Authorities). Does not give the holder the ability to grant ACCESSCTRL, DATAACCESS, DBADM, or SECADM authority. Only SECADM can grant these authorities.
        - GRANT (Global Variable Privileges)
        - GRANT (Index Privileges)
        - GRANT (Module Privileges)
        - GRANT (Package Privileges)
        - GRANT (Routine Privileges)
        - GRANT (Schema Privileges)
        - GRANT (Sequence Privileges)
        - GRANT (Server Privileges)
        - GRANT (Table, View or Nickname Privileges)
        - GRANT (Table Space Privileges)
        - GRANT (Workload Privileges)
        - GRANT (XSR Object Privileges)
- Data Access (DATAACCESS) authority:

    - can be granted only by SECADM
    - cannot be granted to PUBLIC
    - provides the following privilege and authorities:
        - LOAD authority
        - SELECT, INSERT, UPDATE, DELETE privilege on tables, views, nicknames, and materialized query tables
        - EXECUTE privilege on packages
        - EXECUTE privilege on modules
        - EXECUTE privilege on routines *except* AUDIT_ARCHIVE, AUDIT_LIST_LOGS, AUDIT_DELIM_EXTRACT
        - READ privilege on all global variables and WRITE privilege on all global variables except variables that are read-only
        - USAGE privilege on all XSR objects
        - USAGE privilege on all sequences
- SQL Administrator (SQLADM) authority:
    - Monitor and tune SQL statements
    - granted by ACCESSCTRL and SECADM authority
    - can perform the following:
        - EXPLAIN SQL statements and PROFILE commands
        - run the RUNSTATS and MODIFY STATISTICS utilities
        - execute system-defined stored procedures, functions, and packages
        - DB2 for LUW can also run the following:

          ```
          CREATE EVENT MONITOR, DROP EVENT MONITOR, FLUSH EVENT MONITOR
          FLUSH OPTIMIZATION PROFILE CACHE, FLUSH PACKAGE CACHE,
          PREPARE, REORG, SET EVENT MONITOR STATE
          ```
- Workload Management Administrator (WLMADM) authority:
    - manage workload management objects (service classes, work action sets, work class sets, workloads)
    - granted by ACCESSCTRL or SECADM authority

Remark. *DB2 for LUW only:*

```
SYSMAINT, SYSMON, WLMADM
```

DB2 for z/OS:

```
Installation SYSADM, SYSOPER, INSTALLATION SYSOPER, DBCTRL,
DBMAINT, PACKADM, System DBADM
```

2.4 Privileges

- database-level privileges, which span all objects within the database
  - DB2 for LUW
    - BINDADD: create packages in the database using the BIND command
    - CONNECT: connect to the database
    - CREATETAB: create tables within the database
    - CREATE_EXTERNAL_ROUTINE: create a procedure for use by applications and other users of the database
    - CREATE_NOT_FENCED_ROUTINE: create unfenced user-defined functions (UDFs)
    - EXPLAIN: generate Explain query plans
    - IMPLICIT_SCHEMA: implicitly create schemas within the database without using the CREATE SCHEMA command
    - LOAD: load data into a table
    - QUIESCE_CONNECT: access a database while it is in a quiesced state
  - DB2 for z/OS
    - CREATETAB: create tables within the database
    - CREATETS: create table spaces for database
    - DISPLAYDB: display the status of a database
    - DROP: drop or alter a database
    - IMAGCOPY: prepare for, make, and merge copies of table spaces in a database; remove records of any table space copies made
    - LOAD: load data into a database
    - RECOVERDB: recover objects in a database and report recovery status
    - REORG: reorganize objects in a database (run REORG utility)
    - REPAIR: generate diagnostic information about and repair data stored in a database's objects
    - STARTDB: start database
    - STATS: gather statistics; check index and referential constraints for associated objects; delete unwanted statistics history records from the system catalog tables
    - STOPDB: stop database
- object privilege, apply to specific database objects: DB2 z/OS only; DB2 LUW only; Both

Privilege name	Relevant objects	Description
CONTROL	table, view, index, package,nickname	Provides full authority on the object. Users with this privilege can also grant or revoke privileges on the object to other users
DELETE	table, view, nickname	allows a user to remove data from object
INSERT	table, view, nickname	allows a user to add data into object
SELECT	table, view, nickname	allows a user to retrieve data from the object

UPDATE	table, view, nickname	allows a user to modify data within the object
ALTER	table, sequence, nickname	allows a user to alter the object definition, comment associated with
INDEX	table, nickname	allows a user to create an index on object
REFERENCES	table, nickname	provides the ability to create or drop foreign key constraints on the object
BIND	package, plan	allows a user to rebind(recreate) existing packages
COPY	package	allows a user to copy a certain package
EXECUTE	function, stored procedure, routine, package, plan	allows a user to invoke object
USAGE	sequence, jar, XSR, workload	allows a user to use PREVIOUS VALUE and NEXT VALUE associated with sequence/use a jar file/use a XSR object /use a workload
USAGE OF	TYPE, DISTINCT TYPE	allows a user to use object
TRIGGER	table	allows a user to create triggers for object
ALTERIN	schema	allows a user to change the comment associated with any object in a schema or modify definitions of objects in a schema
CREATEIN	schema	allows a user to create objects within a schema
CREATE IN	collection	allows a user to name a collection, execute the BIND PACKAGE subcommand
DROPIN	schema	allows user to drop objects within a schema
SETSESSIONUSER		set the session authorization ID to one of a set of specified authorization IDs available
USE OF	BUFFERPOOL, ALL BUFFERPOOLS, TABLESPACE, STORAGEGROUP	allows user to use the object
ARCHIVE		allows a user to archive active log
BINDADD		allows a user to create new plans and packages
BINDAGENT	plan, package	allows a user to bind, rebind, or free object
BSDS		recover the bootstrap data set
CREATEALIAS	table, view	allows a user to create alias for object
CREATEDBA		allows a user to create a new database and have DBADM authority over it
CREATEDBC		allows a user to create a new database and have DBCTRL authority over it
CREATESG		allows a user to create a storage group
CREATE_SECURE_OBJECT		allows a user to create secure triggers or UDFs
CREATETMTAB		allows a user to define a created temporary table
DEBUGSESSION		allows a user to control debug session activity for stored procedures, functions

DISPLAY		allows a user to display system information
EXPLAIN		allows a user to generate Explain query plans
MONITOR1		allows a user to receive trace data
MONITOR2		allows a user to receive trace data regardless of its sensitivity
RECOVER		allows a user to recover threads
STOPALL		allows a user to stop DB2
STOSPACE		allows a user to obtain information about storage space usage
TRACE		allows a user to control tracing
PASSTHRU		allows a user to issue DDL and DML directly to a data source via a federated database server
READ		allows a user to read the value of a certain global variable
WRITE		allows a user to assign a value to a certain global variable

Remark. • *Objects that can be manipulated within a schema:*

- *DB2 for LUW: tables, views, index, packages, data types, functions, triggers, procedures, alias*
- *DB2 for z/OS: distinct data types, UDFs, triggers, procedures*

2.5 Granting/Revoking Authorities and Privileges

- Implicitly:
  - DB2 may grant privileges automatically when certain commands are issued without the need for an explicit GRANT statement being issued.
- Indirectly:
  - When a user executes a package that performs operations that require certain privileges (ie. a package that deletes a row of data from a table will require DELETE privilege on the table), he or she is indirectly given those privileges for the express purpose of executing the package.
- Explicit:
  - To explicitly grant authorities and privileges, a user must possess SECADM, ACCESSCTRL, or CONTROL privilege on the object that privileges are to be granted for
- GRANT statement:

  - if the `ALL PRIVILEGES` clause is specified with the `GRANT` statement used, all authorities and privileges for the designated object- *except* the CONTROL privilege- will be granted to each recipient indicated.
  - CONTROL privilege must be granted separately.
  - if the `GRANT OPTION` clause is specified with the `GRANT` statement used, the individual receiving the designated authorities and privileges will receive the ability to grant those authorities and privileges to others.
  - if the `WITH ADMIN OPTION` clause is specified with the `GRANT` statement used, the individual being granted will receive the ability to grant that role to others.

- REVOKE statement:
- Roles:
  - is a database object that groups together one or more privileges and can be assigned to users, groups, PUBLIC, or other roles by using a GRANT statement.

2.6 Row and Column Access Control (RCAC)

- RCAC controls access to a table at the row level, column level or both.
- can use RCAC to ensure that your users have access to only the data that is required for their work.
- Regular SQL privileges cannot restrict access to portions of a table. This was usually done through views or application logic. However, users with direct access to the database can bypass these layers.
- With RCAC, even higher level authorities such as users with DATAACCESS authority are not exempt from RCAC rules. Only users with SECADM authority can manage RCAC within a database. Thus, you can use RCAC to prevent users with DATAACCESS from freely accessing all data in a database.
- RCAC rules: RCAC is compromised of SQL rules that place access control at the table level around the data itself. RCAC permits all users to access the same table. But, RCAC restricts access to the table based upon individual user permissions or roles as specified by a policy associated with the table
  - Row permissions
    * Row permission is a database object that expresses a row access control rule for a specific table. A row access control rule is an **SQL search condition** that describes what set of rows a user has access to.
  - Column masks
    * Column mask is a database object that expresses a column access control rule for a specific column in a table. A column access control rule is an **SQL CASE expression** that describes what column values a user is permitted to see and under what conditions

2.7 Trusted contexts

- is a database object that defines a trust relationship for a connection between database and an external entity such as an application server.
- the following information is used to define a trusted context:
  - **System authorization ID** - Represents the user that establishes a database connection
  - **IP address (or domain name)** - Represents the host from which a database connection is established
  - **Data stream encryption** - Represents the encryption setting (if any) for the data communication between the database server and the database client
- When a user establishes a database connection, the DB2 database system checks whether the connection matches the definition of a trusted context object in the database. When a match occurs, the database connection is said to be trusted.
- trusted context objects can only be defined by SECADM
- implicit trusted connection
  - results from a normal connection request and allows users to inherit a role that is unavailable to them outside the scope of the trusted connection
- explicit trusted connection
  - is established by making a connection request within an application.
  - can switch the connection's user to a different authorization ID

2.8 Label-Based Access Control (LBAC)