Authorization, privileges, and object ownership

Last Updated: 2024-01-12

Users (identified by an authorization ID) can successfully execute operations only if they have the authority to perform the specified function. To create a table, a user must be authorized to create tables; to alter a table, a user must be authorized to alter the table; and so forth.

The database manager requires that each user be specifically authorized to use each database function needed to perform a specific task. A user can acquire the necessary authorization through a grant of that authorization to their user ID or through membership in a role or a group that holds that authorization.

There are three forms of authorization, *administrative authority*, *privileges*, and *LBAC credentials*. In addition, ownership of objects brings with it a degree of authorization on the objects created. These forms of authorization are discussed in the following section.

Administrative authority

The person or persons holding administrative authority are charged with the task of controlling the database manager and are responsible for the safety and integrity of the data.

System-level authorization

The system-level authorities provide varying degrees of control over instance-level functions:

- SYSADM (system administrator) authority
  The SYSADM (system administrator) authority provides control over all the resources created and maintained by the database manager. The system administrator possesses all the authorities of SYSCTRL, SYSMAINT, and SYSMON authority. The user who has SYSADM authority is responsible both for controlling the database manager, and for ensuring the safety and integrity of the data.

- SYSCTRL authority
  The SYSCTRL authority provides control over operations that affect system resources. For example, a user with SYSCTRL authority can create, update, start, stop, or drop a database. This user can also start or stop an instance, but cannot access table data. Users with SYSCTRL authority also have the SYSMAINT and SYSMON authorities.

- SYSMAINT authority
  The SYSMAINT authority provides the authority required to perform maintenance operations on all databases associated with an instance. A user with SYSMAINT authority can update the
  22 database configuration, backup a database or table space, restore an existing database, and
  monitor a database. Like SYSCTRL, SYSMAINT does not provide access to table data. Users with SYSMAINT authority also have SYSMON authority.

- SYSMON (system monitor) authority
  The SYSMON (system monitor) authority provides the authority required to use the database system monitor.

22

Database-level authorization

The database level authorities provide control within the database:

- DBADM (database administrator)
  The DBADM authority level provides administrative authority over a single database. This database administrator possesses the privileges required to create objects and issue database commands.

  The DBADM authority can be granted only by a user with SECADM authority. The DBADM authority cannot be granted to PUBLIC.

- SECADM (security administrator)
  The SECADM authority level provides administrative authority for security over a single database. The security administrator authority possesses the ability to manage database security objects (database roles, audit policies, trusted contexts, security label components, and security labels) and grant and revoke all database privileges and authorities. A user with SECADM authority can transfer the ownership of objects that they do not own. They can also use the AUDIT statement to associate an audit policy with a particular database or database object at the server.

  The SECADM authority has no inherent privilege to access data stored in tables. It can only be granted by a user with SECADM authority. The SECADM authority cannot be granted to PUBLIC.

- SQLADM (SQL administrator)
  The SQLADM authority level provides administrative authority to monitor and tune SQL statements within a single database. It can be granted by a user with ACCESSCTRL or SECADM authority.

- WLMADM (workload management administrator)
  The WLMADM authority provides administrative authority to manage workload management objects, such as service classes, work action sets, work class sets, and workloads. It can be granted by a user with ACCESSCTRL or SECADM authority.

- EXPLAIN (explain authority)
  The EXPLAIN authority level provides administrative authority to explain query plans without gaining access to data. It can only be granted by a user with ACCESSCTRL or SECADM authority.

- ACCESSCTRL (database access control authority)
  The ACCESSCTRL authority level provides administrative authority to issue the following GRANT (and REVOKE) statements.
  - GRANT (Database Authorities)
    ACCESSCTRL authority does not give the holder the ability to grant ACCESSCTRL, DATAACCESS, DBADM, or SECADM authority. Only a user who has SECADM authority can grant these authorities.

Controlling access for database administrators (DBAs)

Last Updated: 2024-01-12

You may want to monitor, control, or prevent access to data by database administrators (users holding DBADM authority).

Monitoring access to data

22

You can use the Db2® audit facility to monitor access by database administrators. To do so, follow these steps:

1. Create an audit policy that monitors the events you want to capture for users who hold DBADM authority.
2. Associate this audit policy with the DBADM authority.

Controlling access to data

You can use trusted contexts in conjunction with a role to control access by database administrators. To do so, follow these steps:

1. Create a role and grant DBADM authority to that role.
2. Define a trusted context and make the role the default role for this trusted context.
   Do not grant membership in the role to any authorization ID explicitly. This way, the role is available only through this trusted context and a user acquires DBADM capability only when they are within the confines of the trusted context.

3. There are two ways you can control how users access the trusted context:
   - Implicit access: Create a unique trusted context for each user. When the user establishes a regular connection that matches the attributes of the trusted context, they are implicitly trusted and gain access to the role.
   - Explicit access: Create a trusted context using the WITH USE FOR clause to define all users who can access it. Create an application through which those users can make database requests. The application establishes an explicit trusted connection, and when a user issues a request, the application switches to that user ID and executes the request as that user on the database.

If you want to monitor the use of this trusted context, you can create an audit policy that captures the events you are interested in for users of this trusted context. Associate this audit policy with the trusted context.

Preventing access to data

To prevent access to data in tables, choose one of these options:

ORACLE View Accounts Contact Sales

Products Industries Resources Customers Partners Developers Company

Plug-in for IBM DB2 Database

22

Oracle Enterprise Manager Plug-in for IBM DB2 Database

Description

The Oracle System Monitoring Plug-in for IBM DB2 Database extends Oracle Enterprise Manager to add support for managing IBM DB2 Database instances. By deploying the plug-in in your Grid Control environment, you gain the following management features:

- Monitor DB2 Database instances.
- Gather configuration data and track configuration changes for DB2 Database instances.
- Raise alerts based on thresholds set on monitoring data*.
- Provide rich out-of-box reports*.
- Support monitoring of the DB2 Database by a remote Agent. For remote monitoring, the Agent does not need to be on the same computer as the DB2 Database.

Installation Instructions

1. Download the Installation Guide

2. Click on the "Download Connector Bundle" link, and save the archive on your machine

3. Follow the instructions mentioned in the installation guide

4. If multiple versions of a plug-in are available, Oracle recommends you to use the latest version of the plug-in, as long as its pre-requisites as mentioned in the documentation are met by your environment.

5. Still not sure which version to download? Review the certification matrix to see plug-in version compatibilities.

* Review the reference manual (html , pdf) for a list of metrics monitored as well as out-of-box reports for this plug-in.

IBM DB2 Database Plug-in

Talk to sales

Enterprise Manager Release