Controlling access for database administrators (DBAs) 19

Last Updated: 2024-01-12

You may want to monitor, control, or prevent access to data by database administrators (users holding DBADM authority). 19

Monitoring access to data

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. 19

Preventing access to data

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

- To prevent access to data in all tables, revoke DATAACCESS from your DBADM user, role or group. Alternatively, you could grant DBADM to the user, role or group of interest without the DATAACCESS option
- To prevent access to data in one particular table, follow these steps:
  - Assign a security label to every column in the table.
  - Grant that security label to a role.
  - Grant that role to all users (or roles) that have a legitimate need to access the table.

  No user, regardless of their authority, will be able to access data in that table unless they are a member in that role.

19

Parent topic:

→ Authorization, privileges, and object ownership

Related concepts

→ Audit policies

→ Data access administration authority (DATAACCESS)

→ Database administration authority (DBADM)

→ Label-based access control (LBAC) overview

→ The EXECUTE category for auditing SQL statements

Related tasks

→ Establishing an explicit trusted connection and switching the user ID