Sql server authorisation policies information technology essay

Technology, Information Technology

\n[toc title="Table of Contents"]\n

\n \t

1. Authorisation policies / rules \n \t
2. Oracle Authorisation Policies \n \t
3. DB2 Authorisation Policies \n \t
4. SQL Server Authorisation Policies \n \t
5. LDAP (Lightweight Directory Access Protocol) \n \t
6. RFAC (Resource Access Control Facility) \n

\n[/toc]\n \nAuthorisation is the process where the user is given permissions to access a particular data store. Once a request is placed by a user for the access to a data store, the request is validated with the access rights assigned to that user id from the database. If the requested resource is assigned to the user id, the user request is allowed to execute or else, the query will either be terminated or has to be altered based on the set of flexible transformation rules (Eavis and Altamimi, 2012).

Authorisation policies / rules

Authorisation Rules allow or reject access to certain objects (requests) by describing the subject (user) to which the rules apply to, the object (request) which the authorisation refers to, the action which the rules refer to and the warning explaining whether the rule allows or rejects subject (user) access. Authorisation rules generally include details of subjects, objects, privileges, security information, log types, conditions, etc (Blanco et. al, 2009).

Oracle Authorisation Policies

Oracle Identity Manager is in charge of the user access to different procedures in the application. An authorisation engine is embedded in the Identity Manager and it manages the user access with the help of pre-defined authorisation policies. The authorisation policies decide during runtime whether a particular action should be allowed or not. The authorisation policies are defined such that they satisfy the authorisation requirements specified by Identity Manager (Oracle, 2011). The components of Oracle Identity manager are: Role managementUser managementAuthenticated self-service user managementThe important components of Oracle authorisation policy areIdentifying details – name and description must be definedOracle identity manager feature – these are components of Identity manager like user management and role management. Each feature has its own authorisation policy. Assignee – is the role to which the privileges are granted by the authorisation policy. Privileges – are assigned to the assignee. They are identified by the feature for which this authorisation policy is defined. Data security – defined in terms of entities selection criteria which are used to establish entities for which privilege has to be granted.

DB2 Authorisation Policies

The factors to be decided before creating an authorisation policy are (IBM, n. d.), Services – are the resources protected by Security manager. The services have to be attached to an authorisation policy in order to be secured by Tivoli Security policy manager. The three methods of attaching a

policy are direct attachment through nodes, through inheritance, and through classification. Application roles – are the categories of user as a general user and authenticated user. Based on these categories, application role identifies the user groups to apply the policies. Rules – are the conditions applied on the access rights for a specific user. The components of DB2 authorisation policy arePolicy decision point – evaluates a user request and decides as to accept or reject the request. Policy enforcement point – receives the decision from above and enforces the same, i. e., either allows the access or denies the access. Policy distribution target – is the place from where the policy decision points receive the authorised policies from the security policy manager.

SQL Server Authorisation Policies

SQL Server uses the role-based access control. To regulate the access control, authorisation policies are built and stored in the Active directory in the form of authorisation stores. They are applied during run-time and validate with the policy information in the authorisation stores. The components of authorisation policy are (Microsoft, 2012), Policy stores, Applications and stores – Policy stores contain definition and is initialised by an application before using it for access control. Users and groups – include users and user groupsOperations and tasks – task contains one or more operations which are activated at run-time. The task contains the role definition also. Roles – is a group of operations or tasks depending on the category of user’s requests. Business rules – when an application validates

the access control at run-time, it refers to the business rules script.

Collections

LDAP (Lightweight Directory Access Protocol)

Lightweight Directory Access Protocol (LDAP) is a client-server protocol which works on TCP/IP for the purpose of data access and data management on the directory. LDAP stores the user information such as the user login id, roles, privileges and user groups. LDAP ensures the easy availability and efficient management of the user data (Li, Wang and Deng, 2010). LDAP directory is a hierarchical tree structure depicting the network of users based on the roles and privileges. The components of the directory are (Salim et. al, 2009), Servers – facilitates the direct data storage locally. It allows the access to the external sources. SLAPD (Stand-Alone LDAP Daemon) is the server in LDAP suite. The server supports changes to the directory data (adding, deleting or altering). Clients – access servers over LDAP network protocol. They perform by prompting that the server executes requests on behalf of the clients. Firstly, a client connects to the directory server, the next step being authentication. Finally they execute zero or more requests before disconnecting. Utilities – control data at a lower level and do not require the intervention of server. They are mainly used as additional features to maintain the server. Libraries – LDAP applications are able to access the LDAP functions through the libraries. The rest of the directory components share access to such libraries.

RFAC (Resource Access Control Facility)

Row-level security with Virtual Private Database (VPD) and Label Security

(OLS)Access control Models – 3 typesDiscretionary access control

(DAC)Mandatory access control (MAC)Role-based access control (RBAC)