International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No.08, March 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

Protecting Database from Administrative Perspective

Gurjit Singh

Dept. of Computer Science & IT, S.G.G.S. Khalsa College Mahilpur, Hoshiarpur, Punjab (India)

ABSTRACT

In any organization or business, information security, privacy and protection of data plays a vital role. There are various ways of providing security by DBA to manage user accounts, granting privileges and roles and auditing user activities. This paper provides us with the guidelines from database administrative point of view for protecting databases (including the data, the database applications or stored functions, the database systems, the database servers and the associated network links) against unauthorized access. It also describes how the backup administrator devises, implements, and manages a backup and recovery strategy. Generally, the purpose of a backup and recovery strategy is to protect the database against data loss and reconstruct the database after data loss. This paper mainly focuses on security issues that are associated with the database system that are often used by many firms in their operations.

Keywords: *Backup, Database threats, Roles, Recovery, RAID, Privileges.*

1. INTRODUCTION

Information or data is a valuable asset in any organization. All organizations have now automated their information systems and other operational functions. They have maintained the databases that contain the essential information of the organization. So database security is a key concern. It deals with making database secure from any form of illegal access or threat at any level. Database security deals permitting or prohibiting user actions on the database and the objects inside it. It does not allow the unauthorized access to the data/information. Organizations demand the assurance that their data is protected against any malicious or accidental modification. Moreover, as organizations increase their adoption of database systems as the key data management technology for day-to-day operations and decision making, the security of data managed by these systems becomes crucial. Damage and misuse of data affect not only a single user or application, but may have disastrous consequences on the entire organization. The recent rapid proliferation of Web-based applications and information systems have further increased the risk exposure of databases and, thus, data protection is today more crucial than ever.

Data protection is ensured by different components of a database management system (DBMS). In particular, an access control mechanism ensures data confidentiality. Whenever a user tries to access a data object, the access control mechanism checks the rights of the user against a set of authorizations, stated usually by some security administrator. An authorization states whether a user can perform a particular action on an object. Authorizations are stated according to the access control policies of the organization. Data confidentiality is further enhanced by the use of encryption techniques, applied to data when being stored on secondary storage or transmitted on a network. Recently, the use of encryption techniques has gained a lot of interest in the context of outsourced data management.

Fig. 1 below shows the properties of database security that are

Confidentiality, integrity and availability, also known as the CIA triad, is a model designed to guide policies for information security within an organization. The elements of the triad are considered the three most crucial components of security. In this context, confidentiality is a set of rules that limits access to information, integrity is the assurance that the information is trustworthy and accurate, and availability is a guarantee of reliable access to the information by authorized people.

Data/information is always a most important asset for any organization whose security cannot be compromised. With the advances in technology, the risk to these valuable assets increases. So their security is a big challenge. In different database security layers are defined shown in figure 2 below.

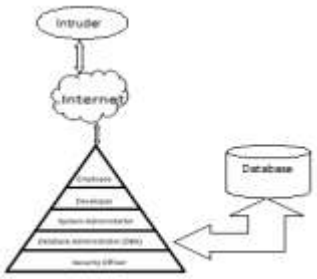

Fig. 2 security layers at organizational level

The various layers are: security officer, database administrator (DBA), system administrator, developers and employee. For each layer some well-defined security policies have been anticipated. These policies ensure the security features, privacy, confidentiality and integrity. Among all the layers, DBA layer plays a vital role in ensuring database security.

2. RELATED WORK

Early research efforts in the area of access control models and confidentiality for DBMSs focused on the development of two different classes of models, based on the discretionary access control policy and on the mandatory access control policy. This early research was cast in the framework of relational database system by the availability of declarative query languages, such as SQL. A first relevant recent research direction is motivated by the trend of considering databases as a service that can be outsourced to external companies. An important issue is the development of query processing techniques for encrypted data. Several specialized encryption techniques have been proposed, such as the order-preserving encryption technique by Agrawal et al. A second research direction deals with privacy-preserving techniques for databases, an area recently investigated to a considerable extent. Research in this direction has been motivated, on one side, by increasing concerns with respect to user privacy and, on the other, by the need to support Web-based applications across

organization boundaries. In particular privacy legislation, such as the early Federal Act of 1974 and the more recent Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Children's Online Privacy Protection Act (COPPA), require organizations to put in place adequate privacy- preserving techniques for the management of data concerning individuals. The new Web-based applications are characterized by the requirement of supporting cooperative processes while ensuring the confidentiality of data. This research direction is characterized by a number of different approaches and techniques, including privacy-preserving data mining, privacy-preserving information retrieval, and databases systems specifically tailored toward enforcing privacy.

After studying various research papers on database security, a need arises to discuss various techniques adopted by DBA to provide high level of security to organization's database by granting appropriate database access privileges, assigning roles, auditing user activities, administering backup and recovery solutions and implementing various RAID levels on database files at different levels.

3. ADMINISTERING DATABASE

As an administrator, in order to allow users to access the database, DBA must create user accounts and grant appropriate database access privileges to those accounts.

3.1 User accounts access

A user account is identified by a user name. It also defines the attributes of the user like:

- Authentication method
- Password for database authentication
- Tablespace quotas
- Default tablespaces for permanent and temporary data storage
- Account status (locked or unlocked)
- Password status (expired or not)

While creating a user account, we must not only assign a user name, a password, and default tablespaces for the account, but must also perform the following:

- Grant the appropriate system privileges, object privileges, and roles to the account.
- If the user further needs to create database objects, then allocate the user account a space usage quota on each tablespace in which the objects will be created.

When a user account is created, a schema for that user is implicitly created. A schema is a logical container for the database objects (such as tables, views, triggers, and so on) that the user creates. The schema name is same as the user name, and the objects owned by the user can be unambiguously referred by this schema name. For example, hod.teacher refers to the table named TEACHER in the HOD schema.

The basic level of database security is provided by granting the User privileges which are designed to control user access to data and to limit the kinds of SQL statements that users can execute. While creating a user, privileges are granted to enable the user to perform various activities like

- To connect to the database
- To run queries and make updates
- To create schema objects, and more.

There are two main types of user privileges:

- System privileges—A system privilege gives a user the ability to perform a particular action, or to perform an action on any schema objects of a particular type. For example, the system privilege CREATE TABLE permits a user to create tables in the schema associated with that user, and the system privilege CREATE USER permits a user to create database users.
- Object privileges-An object privilege gives a user the ability to perform a particular action on a specific schema object. Different object privileges are available for different types of schema objects. The privilege to select rows from the TEACHER table or to delete rows from the DEPARTMENT table is examples of object privileges.

3.2 Administering Roles

Roles can make easier to manage privileges. Roles are named groups of related system and object privileges. Roles are created, system and object privileges are granted to the roles, and then roles are granted to the users to other roles. Unlike schema objects, roles are not contained in any schema.

Table 1 lists three widely used roles that are predefined in Oracle Database. These roles can be granted at creation time or at any time thereafter.

Table 1 Oracle Database Predefined Roles

Roles	Description
CONNECT	Enables a user to connect to the database. Grant this role to any user or application that needs database access. If a user is created using Database Control, then this role is automatically granted to the user.
RESOURCE	Enables a user to create, modify, and delete certain types of schema objects in the schema associated with that user. Grant this role only to developers and to other users that must create schema objects.
DBA	Enables a user to perform most administrative functions, including creating users and granting privileges; creating and granting roles; creating, modifying, and deleting objects in any schema; and more. It grants all system privileges, but does not include the privileges to start or shut down the database instance. It is by default granted to users SYS and SYSTEM.

3.3. Granting and Revoking Privileges

We can GRANT and REVOKE privileges as shown in Table 2 on various database objects in Oracle like granting and revoking privileges on tables or on functions and procedures.

Table 2: Privileges and their Description

Privilege	Description
SELECT	Ability to perform SELECT statements on the table.
INSERT	Ability to perform INSERT statements on the table.
UPDATE	Ability to perform UPDATE statements on the table.
DELETE	Ability to perform DELETE statements on the table.
REFERENCES	Ability to create a constraint that refers to the table.
ALTER	Ability to perform ALTER TABLE statements to change the table definition.

INDEX	Ability to create an index on the table with the create index statement.
ALL	All privileges on table.

3.4 Auditing User Activity

Sign-On Audit feature is provided by Oracle Applications that allows to:

- Track user activities like what users are doing and when they do it.
- Select who to audit and what type of information to audit.
- View quickly online what users are doing.
- Check the security of the application.

The usernames, terminals, and the dates and times the users access applications can be recorded with Sign-On Audit feature. It can also keep track of the responsibilities and forms the users use, as well as the concurrent processes they run.

Major Features of Sign-On Audit are as follows:

- Selective Auditing

Sign-On Audit allows us to choose who to audit and what type of user information to track. It also determines what audit information we need to match the organization's needs.

- Monitor Application Users

The online, real-time information about who is using Applications and what they are doing can be checked by the Monitor Users form. It allows us to see what users are signed on, how long they have been working on forms, what responsibilities, forms, and terminals they are using and what processes they are using.

- Sign-On Audit Reports

The historical, detailed information on what users do in the application can be seen by Sign-On Audit Reports. It allows us to search criteria to narrow the search for information. Sign-On Audit information to create easy-to-read reports can also be sorted.

4. DEFINING BACKUP AND RECOVERY STRATEGY

4.1 Database backup, restoration and recovery

Database backup is the process of making copies of the data files, control file, and archived redo log files. Database restoration is the process of copying the database from a backup medium (typically disk or tape) to their original or to new locations. Database recovery means updating database files (typically using online redo log files), restored from a backup with the changes made to the database after the backup.

A backup can be of two types, either a physical backup or a logical backup. Physical backups are copies of the physical files (data files, control files, and archived redo logs) used to store and recover a database. Every physical backup is a copy of files that store database information to another location, whether on disk or on tape. Logical backups contain logical data such as tables and stored procedures. Oracle Data Pump can be used to export logical data to binary files, which can be later imported into the database. For efficient backup and recovery strategy, physical backups play a vital role.

4.2 Defining a backup and recovery strategy

Oracle Database features provides automatic management of backup and recovery files and operations. To take maximum benefit of this feature, configure the database as follows:

- Use a fast recovery area, which automates storage management for most backup-related files, and specify it as an archived redo log file destination.
- Run the database in ARCHIVELOG mode so that online backups can be performed and have data recovery options such as complete and point-in-time media recovery.

Several policies can also be set that governs which files are backed up, what format is used to store backups on disk, and when files become eligible for deletion.

5. RAID implementation

RAID is the abbreviation used to describe Redundant Arrays of Inexpensive Disks. A mechanism for load balancing and securing the data across multiple disks [13] is provided by various RAID levels. This section discusses about the most commonly used RAID levels and how they should be used with Oracle.

5.1 RAID Levels

The most commonly used RAID levels and their description are listed below in Table 3:

Table 3: RAID levels and their description

RAID Level	Description
None	Since each RAID operation involves a certain management overhead, then RAID can be avoided if the requirement is for optimum write speed and no data protection.
0	To balance the load across the disk array, this RAID level provides automatic block level striping of data across multiple disks. It doesn't provide any protection from data loss.
1	RAID level 1 is also known as disk mirroring. A complete copy of each disk on at least one other disk is kept by the RAID controller. In case of a disk failure the RAID controller switches to one of the mirrors to prevent system failure. To provide increased levels of security, double or triple mirroring can be used.
0+1	To get the benefits of block level striping across the array and the security of disk mirroring, RAID level 0+1 combines RAID 0 and RAID 1 respectively. The striping occurs across disks and the entire set is mirrored.
1+0 or 10	This is the best RAID level for Oracle as this is a combination of RAID 1 and RAID 0. It is different from RAID level 0+1 as each disk is mirrored individually and striping occurs across all the mirrored pairs.
5	This RAID level stripes data and parity information across 3 or more disks. The parity information allows the contents of lost blocks to be derived. When a disk failure occurs, the significant write overhead associated with this RAID level make it slower than the previous methods. But it is very

	cost effective as it requires far fewer disks. Earlier, RAID 5 was avoided for database applications but improvements in disk speed and controller performance makes it a viable solution for data files if performance is not a consideration.

5.2 Oracle RAID Usage

It is essential to know what the different RAID levels do and which level should be used for Oracle? Here are some suggestions as shown in Table 4, with the RAID levels listed in order of preference.

Table 4: RAID levels with their order of preference

File Type	**Preferred RAID Level**	**Comments**
Control Files	RAID1+0, RAID 0+1, RAID0, No RAID	Make sure that at least one copy of the control file is always available as the Control files are updated constantly. The quicker the files can be accessed the better would be the performance. Multiple control files should always be used whether any RAID level is used or not.
Datafiles	RAID1+0, RAID 0+1 or RAID 5	Datafiles that have more I/O requirements should use RAID 1+0 (or 0+1). This is the fastest and most secure option. RAID 5 can be used to reduce costs. Most I/O operations to datafiles are buffered, with the physical writes happening in the background.
Temporary Datafiles	NoRAID, RAID 0	The main requirement of temporary datafiles is fast access, not reliability. If the datafile is lost it can simply be recreated as there is no data to restore.
Archived Redo Logs	RAID1+0, RAID 0+1, RAID0, No RAID	These should always be multiplexed. If space is an issue, rely on RAID to provide redundancy. If archived redo logs are lost, then we have to compromise the backup and recovery.
Rollback/Undo Datafiles	RAID1+0, RAID 0+1	These files require constant I/O and must be protected. They cannot be multiplexed by Oracle but the hardware can do the multiplexing.
Online Redo Logs	RAID1+0, RAID 0+1, RAID0, No RAID	The redo Logs should always be multiplexed whether any RAID level is used or not.

An integrated suite of high availability solutions is offered by Oracle Database. It increases availability and eliminates or reduces both planned and unplanned downtime. It also increases system utilization on the primary and secondary systems. Moreover, it helps in the improvement of overall system performance, scalability, and manageability. For the primary database, all hardware resources are leveraged for performance and scalability. For secondary or disaster recovery systems, system and database resources can be used with the Active Data Guard option.

6. CONCLUSION

Data to any organization is a most valuable property. Security of sensitive data is always a big challenge for an organization at any level. In today's technological world, database is vulnerable to hosts of attacks. Organizations now are relying on data to make decisions on various businesses operations that enhance their operations. Therefore, it is prudent to keep sensitive information away from unauthorized access. This paper helps us to understand how DBA creates user accounts and grant various privileges and roles at various levels to protect the database from unauthorized access. It also described the Backup administration tasks that typically include planning and testing responses to different kinds of failures, configuring the database environment for backup and recovery, setting up a backup schedule, monitoring the backup and recovery environment, troubleshooting backup problems and recovering from data loss. It also described the various RAID levels and their appropriate uses to protect various database files.

7. REFERENCES

[1] Iqra Basharat, Farooque Azam, Abdul Wahab Muzaffar "Database Security and Encryption: A Survey Study" *International Journal of Computer Applications (0975 – 888) Volume 47–No.12*, June 2012.

[2] Elisa Bertino and Ravi Sandhu "Database Security—Concepts, Approaches, and Challenges" *IEEE Transactions on Dependable and Secure Computing, VOL. 2, NO. 1*, January-March 2005 Database Security — Concepts, Approaches, and Challenges.

[3] B. Iyer, S. Mehrotra, E. Mykletun, G. Tsudik, and Y. Wu, "A Framework for Efficient Storage Security in RDBMS," Proc.Seventh Int'l Conf. Extending Database Technology (EDBT 2004), Mar. 2004.

[4] Khaleel Ahmad; JayantShekhar; Nitesh Kumar; K.P. Yadav; Policy Levels Concerning Database Security; *International Journal of Computer Science & Emerging Technologies (E-ISSN: 2044-6004) 368 Volume 2, Issue 3*, June 2011, page(s); 368-372.

[5] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "Order-Preserving Encryption for Numeric Data, "Proc. 2004 ACM Sigmod Conf., 2004.

[6] Federal Trade Commission, "FTC Announces Settlement with Bankrupt Website, Toysmart.com, Regarding Alleged Privacy Policy Violations," July 2000, available at ww.ftc.gov/opa/2000/07/toysmart2.html.

[7] HIPAA, Health Insurance Portability and Accountability Act of 1996, available at http://www.hep-c-alert.org/links/hipaa.html, 1996.

[8] COPPA, Children's Online Privacy Protection Act of 1998, Oct. 1998, available at www.cdt.org/legislation/105th/privacy/coppa.html.

[9] J. Vaidya and C. Clifton, "Privacy Preserving Association Rule Mining in Vertically Partitioned Data, "Proc. Eighth ACM SIGKDD Int'l Conf. Knowledge Discovery and Data Mining, July 2002.

[10] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "Hippocratic Databases," Proc. 28th Int'l Conf. Very Large Databases (VLDB),2002.

[11] https://docs.oracle.com/cd/E11992_01/server.112/e25494.pdf

[12] www.oracle-dba-online.com/

[13] www.learningtree.com/courses/927/oracle-database-11g-administration/