International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Database Privilege Management and Data Dictionary: Security Issues and Avoidance

M. Rajesh

Visiting Faculty, Dept. of Information Technology, SRM University, Chennai, India.

Abstract: ***Oracle is a relational database utilized by large number of organizations. Within a database management system every user will have certain privilege limitations, but Database Administrator (DBA) will have all the access permissions (privileges) of the database. Privilege management plays a key role in the database security. So whenever a DBA grants privileges to other users, they must identify the category of privilege and the access level of the privilege. This proposed paper will lead to know about critical privileges that create security issues to data dictionary and sys users, furthermore it provide guidelines to avoid security issues.***

Keywords: Privileges, Data dictionary, accessibility, Database Administrator

1. Introduction

Oracle is one of the finest relational database to protect organizational data and also organizations will have more database users to manage their database including DBAs. Each database user needs certain privileges to do their job. Granting appropriate privileges to appropriate users is the major job in privilege management. Privileges is the key to unlock database access, so managing privileges and roles are vital responsibilities of Database administrators. Managing privilege is not only a job in the privilege management but also the administrator needs to manage user role's privileges. Role is a named groups of related privileges that granted to users or other roles. For databases with multiple users, where many users require a similar set of access level, it is beneficial to use roles. The security admin must consider problems related to privilege management for example, there are lots of sensitive and complex privileges available in oracle database. Each privilege's have their own access permissions and limitations but most of the administrators don't have 100% knowledge on all the privileges.

Assume, by mistake DBA granted high level privileges to some normal user, in this case user will be unreasonably permitted to access entire database and also user will be capable of misusing DBA data dictionary tables and auditing tables. In another case, when functionality is not operating as expected, an administrator might issue a command like “grant all privileges to user” to allow temporary access, but then forget to revert the privileges back to the original settings. With this level of access, users receive over 100 privileges, many of which they don't require, and some of which may be in violation of regulatory compliance statutes.

2. Characteristics of Oracle SYS User

When you create oracle database the SYS and SYSTEM users are created automatically and granted with DBA role. SYS user is the highest privileged user in the oracle database . All of the base tables and views for the database and data dictionary are stored in the schema SYS. SYSDBA is a system privilege that is assigned only to user SYS. It enables SYS to perform high-level administrative tasks such as starting up and shutting down the database. Similar to SYS user, the SYSTEM user is the user account that you log in with to perform all administrative functions other than starting up and shutting down the database.

3. Data Dictionary

The Most valuable part in the oracle database is data dictionary and it is owned by SYS user. Data Dictionary includes all the schema objects in the database (tables, indexes, views, Clusters, procedures , functions, packages and so on), other common database information, name of the oracle users and many more. The Oracle user SYS owns all base tables and user-accessible views of the data dictionary. No Oracle user should ever alter (UPDATE, DELETE, or INSERT) any rows or schema objects contained in the SYS schema, because Data are very confidential and sensitive. Altering or manipulating the data in data dictionary tables can permanently and detrimentally affect the operations of a database.

Key point is that the data dictionary is owned by SYS user, so make sure sys user is always highly secure and SYS schemas are inaccessible by ordinary users. There are lots of possibilities to hack the sys user and data dictionary tables through privileges. Like, whenever granting high level privileges to normal users, a window of opportunity is opened for hackers. Thus we must check that any privilege granting operations doesn't affect SYS user schemas.

4. Security Issues and Avoidance

The database security issues arise from various parts of the database through privilege management. Privileges and roles are the key to open the security locks. The security issues arise by granting unwanted privileges. The varieties of issues that can occur:

A. ROLE

There are lots of predefined role's available in oracle database but some of the roles contains more precious privileges that enables users to access data dictionary tables. The list of privileges that grant access to data dictionary are:
SELECT_CATALOG_ROLE: This role allows user to SELECT data dictionary views.

EXECUTE_CATALOG_ROLE: This role allows user to EXECUTE privileges for packages and procedures in the data dictionary.
DELETE_CATALOG_ROLE: The role allows users to delete record from the sys schema tables.

Guidelines to avoid:
- To avoid security issues through above roles, DBA must be aware about role limitations and grant this privileges only for short period of time.
- Furthermore don't grant roles with admin option. DBAs should grant privileges separately instant of granting roles.

B. O7_Dictionary_Accessibility

In reality whenever DBA grant SELECT ANY TABLE or DROP ANY TABLE or DELETE ANY TABLE privilege to user, the user will be able to access all the tables in database excluding SYS schema. If incase o7_dictionary_accessibility parameter is set to true, it enable access to objects in the SYS schema including data dictionary. This is one of the simplest way in which a normal user will be able to access sys schema because most users will have ANY TABLE privilege.

Guideline to avoid:
- DBA's must check the O7_DICTIONARY_ACCESSIBILITY if it is set as false. If it is not, then set the parameter to false using following SQL Query:
  SQL> ALTER SYSTEM SET O7_DICTIONARY_ACCESSIBILITY = FALSE SCOPE=spfile; The query will take effect from the next startup of the database.

C. Select any Dictionary

Granting SELECT ANY DICTIONARY privilege to ordinary user will allow query access to any object in the SYS schema, including tables created in that schema. It must be granted individually to each user requiring the privilege. It is not included in GRANT ALL PRIVILEGES, nor can it be granted through a role. Even if O7_DICTIONARY_ACCESIBILITY parameter is set to true/false, it won't affect SELECT ANY DICTIONARY privilege limitations.

Guideline to avoid:
- DBA should grant these roles and the SELECT ANY DICTIONARY system privilege with extreme care, since the integrity of your system can be compromised by their misuse.

D. Secure Audit Table

There are three auditing tables in the database. Two predefined dictionary auditing table named AUD$ and FGA_LOG$, and one normal audit table. AUD$ and FGA_LOG$ are predefined table in the database and one more table created to store audit information using user defined trigger.

If a user has DELETE ANY TABLE privilege along with O7_DICTIONARY_ACCESSBILITY parameter set to true, then he/ she will be able to delete Audit information from audit table. In another way, if the user possess DELETE_CATALOG_ROLE role, then the user will be able to delete AUD$ and FGA_LOG$ table. This equips the hacker to delete the sensitive audit information.

Guidelines to avoid:
- Set O7_DECTIONARY_ACCESSIBILITY set to false
- Don't Grant DELETE_CATALOG_ROLE to user in normal situation and only grant that role in Extreme difficult situations.
- don't grant ANY TABLE privileges whenever o7_dictionary_accessibility set to true.

E. Database Link

The following link-creation command is an example of one of the worst possible security holes that one can create using links:

```
CREATE DATABASE LINK LINK_B
CONNECT TO SYSTEM IDENTIFIED BY MANAGER
USING 'ORCL';
```

The problem here is that the link is created using SYSTEM user of ORCL database. Since SYSTEM user has higher privileges, the link LINK_B would provide similar levels of privileges to any connecting databases. This will lead to other database user being able to access SYSTEM schema of ORCL.

Guidelines to avoid:
- Don't creating link with higher privileged users.
- DBA must try to create a separate user to handling or connecting database link.

5. Conclusion

Security is a center part of the Oracle database, but still the DBAs have to take certain precautions to ensure complete security. The main focus in granting privilege should be "appropriate privilege to appropriate users". When a DBA regrettably grant high level privileges to inappropriate users, then the user will get unauthorized access to critical tables in the database. The most secure part of any database is it's data dictionary that is owned by SYS user. So the DBAs must follow all guidelines mentioned in this paper to secure data dictionary and sys user schema.

References

[1] Oracle Database 10g: Administration Workshop I volume I student guide, Edition 3.1 August 2010
[2] Ron Ben-Natan, "Implementing Database Security and Auditing: A Guide for DBAs, Information Security Administrators and Auditors", Published by Elsevier, 2005.
[3] Sam R Alapati, "Expert Oracle 10g/11g Administration", Dreamtech Press, First Edition, 2009.
[4] http://docs.oracle.com/cd/B19306_01/server.102/b14237/initparams134.htm#REFRN10133 (Accessed Feb 2015)
[5] http://docs.oracle.com/cd/B19306_01/server.102/b14220/datadict.htm#i1012 (Accessed JAN 2015)
[6] http://docs.oracle.com/cd/B19306_01/network.102/b14266/policies.htm#i1007332 (Accessed JAN 2015)