DATABASE SECURITY OF HUMAN RESOURCE MANAGEMENT SYSTEM IN CLOUD

[1]Mr. Navendu Mishra, [2]Mr. Jayant Sawarkar, [3] Mr. Suraj Dubey
[1]Team Leader, [2]Assistant Professor, [3]COO
[1]Osource Global Private Limited, [2]Datta Meghe College of Engineering, [3]Osource Global Private Limited,
[1]Mumbai, India, [2]Navi Mumbai, India., [3]Mumbai, India.

Abstract: Database security is a very significant aspect for the overall management of the DB services and which pertains to core areas of large applications .Human Resource Management System, which includes areas such as Soft Joining, Promotion, Confirmation, Attendance and Exit, etc. Payroll Information Portal, wherein employees can view their individual Salary details, submit investment declaration, Reimbursement claim etc. Management of Large Database in Cloud involves continuous monitoring with regards to the critical areas of security of the data by Encryption & Decryption mechanism, which uses user-defined functions (key and algorithms).Auditing provides a detailed control of the user's action on the database, which enhances the database security to the larger extent, and at any point of time all those actions of the users can be traced, and the information of which can be maintained both at the database level and also at the operating system level . All the basic user's privileges and profiles are well defined under the database security mechanism, and thus it provides many layers of security of the data, so that the unauthorized access is completely eradicated, and data confidentiality is maintained all the time, and which helps in providing the enhanced database security.

Broad Academic Area of Work: CLOUD COMPUTING

Key words: AWS Cloud, Database, ERP, Hotels, PL/SQL, S3 bucket and Query.

INTRODUCTION

Oracle Database works by utilizing the various components of the Hardware resources. The performance of the database depends upon the resource usages. Queries in a database is written to fetch or get the results, wherein all the resources are utilized. Security a very important aspect in the database, which needs to be looked into a great extent, for the betterment of the database services.

Most of the organizations prefer to use Oracle database on the Linux flavors world-wide, however, Oracle also provides database services for the Windows Operating System users as well. Linux is more robust, and from the security point of view is more desirable as compared to the Windows O/S.

The latest version of 19c provides the database in the form of CDB & PDB's on ASM & LVM.

One of the best feature called **LVM**, which stands for **Logical Volume Manager**, is a highly efficient used framework in the Linux distributions, owing to the facility of providing logical volume management for the Linux kernel. The basic function of LVM, is to provide allocation of disks, mirroring and stripping, and re-sizing the logical volumes.

Also, keeping the data files on the SAN box is mandatory not only for performance (I/O), but also in case any damage happens to any of the disks due to block corruption, the other mirrored disks can be used , and hence, there will not be any data loss or any DB outage.

Oracle Golden Gate is used for the data migration services to replicate data from one database to the other database across different geographic regions world-wide. Oracle Golden Gate allows to migrate the committed transactions in the database across multiple heterogeneous systems. Oracle Golden Gate comes as a separate software product, which needs installation & configurations.

As I being a DBA (Database Administrator), my core responsibility is to manage all the company's database pertaining to the very important and critical areas such as database security (apart from other area as well such as performance, backup & recovery) through the encryption and decryption mechanisms, as per the industry standards. The solutions implemented in the database focuses in the core areas of security, keeping in view the wide variety of clients world-wide. Before the implementation of any security solutions on the production, the same is first tested on the UAT environment by our Team and in consultation with the IT Team.

Now I am working on the fore-front of the implementation of solutions in the OCI (Oracle Cloud Infrastructure) in conjunction with the AWS cloud. Also working for the migration of databases to a higher version which presents various enhanced database security features, which helps the company's growth immensely. Another solution which needs to be implemented for the database is the migration of the current database from Non-Container database to **container database (CDB / PDB's)**, and also to utilize the **ATP (Autonomous Transaction Processing)** of **Oracle** database. **OCI (Oracle Cloud Infrastructure)**

provides the **Real Application Clustering (RAC)** environments, wherein the automatic storage management is done by using ASM disks, wherein the High Availability (HA) is provided continuously, without any database outage (downtime).This is a very important feature of Oracle which helps the business to the maximum possible extent.

As a DBA it's my and my team's responsibility to provide the 24x7 database availability to all of the client's, by following all the DB standards as set in the industry, and as per the organization policy's.

LITERATURE REVIEW

ENCRYPTION AND DECRYPTION & ORACLE SECURITY

Encryption and **Decryption**

Is a mechanism which has been implemented successfully with the use of user defined functions, and calling those function in various objects like views, procedures, to protect the PI (Personal Information) data of the clients and for password authentication.

Below are the steps which needs to be followed for the implementation of the Encryption and Decryption at the schema level:

- *Inform client for the downtime. This will be done by the company's Business Analyst team head.*
- *Disable all the schedulers in the schema for which the Encryption & Decryption implementation to protect client's PI data is being carried out, for that much time for which the activity would be going on. It was approximately for 12 hours on weekday (Sunday).*
- *Obtain the list of view, procedures in which the said Encryption & decryption mechanism needs to be implemented at the code level.*
- *Create the table lists which will store the encryption & decryption values for every user, so that the DB load can be maintained, and DB performance is not hampered.*
- *Verify the Encryption & Decryption function before it's created in the production.*
- *Create both the Encryption & Decryption function, by using the appropriate algorithms.*
- *Amend all the VIEWS with regards to Encryption & decryption functionality, where-ever the PI data is being called for.*
- *Amend all the PROCEDURE with regards to Encryption & decryption functionality, where-ever the PI data is being called for.*

Encryption & Decryption functions can be used in the database objects like Views, procedures, packages etc., to restrict the users from accessing the PI (Personal Information) Data in an unauthorized manner. Both the Encryption & Decryption functions enhances the data security area to a largest extent successfully.

Oracle Security

Oracle 19c Database is a new brand in the database technology, and have new security features that have been implemented in Oracle Database 19c

Oracle Database 19c provides a long term support release of Oracle Database 12c Family, which includes Oracle database 18c as well. Oracle database 19c provides new features for DBA & developers.

Oracle Database **19c** has new **Oracle Security** features and are described as below.

- Oracle database 19c supports **Oracle Native Encryption** and **SSL Authentication** for Different Users Concurrently.
- Oracle database 19c has the ability to Audit Only Top-Level **SQL** Statements.
- Oracle database 19c provides improved Read Performance for the Unified Audit Trial. The system table, stores the unified audit trail records, and, which has been redesigned to use partition pruning to improve read performance.
- Oracle Database 19c has the ability to **Grant** or **Revoke Administrative Privileges** to and from Schema-Only Accounts.
- Performance - SQL Quarantine: SQL statements that are terminated by Oracle Database Resource Manager due to their excessive consumption of CPU and I/O resources can be automatically quarantined.
- Availability - Dynamically change Fast-Start Failover (FSFO) target: This new command allows the user to dynamically change the FSFO Target standby to another standby in the target list without disabling the FSFO.

- Application Development - REST Enabled SQL Support: Developers can easily create REST Enabled SQL references by defining a name, the endpoint URL, and authentication information.
- Flashback Standby database when Primary database is flashed back: Flashback Database moves the entire database to an older point in time and opens the database with RESETLOGS.
- RAC & Grid infrastructure: It enables patching of Oracle Grid Infrastructure without interrupting database operations. Patches are applied out-of-place and in a rolling fashion, with one node being patched at a time, while the database instances on the node remain operational all the time.
- Other new features in Oracle database 19c includes such as Automatic Indexing, Trace File Analyzer, Cluster health checks, Machine learning user interface (Data Miner), Security, Big data & Data warehousing and more.

Database Profiles

Profile refers to a database object, which is a named set of resource limits, which a user can use. It sets up the threshold limit for the amount of resources, which a database user can use. A default profile is created when the database is created for the first time, and is assigned to all the users created by default. The most important advantage of a database profile is that, once a profile has been assigned to a user in the database, then that user in the database will not be able to exceed the threshold limit of database resources and password limits

A DBA can create his own profile, as per the DBA policy and assign that profile to the concerned users to limit the resource usages in the database. There are various resources on which the limits can be imposed through the profiles, and the same can be assigned to the user. The named set of resource limits are SAN storage space,I/O to run the queries,CPU power, connect time,CPU time, Enforce passwords, number of sessions per user, etc.

A database profiles can also be used to set limits to the user password also. Generally, all the available password rules will not be used, but it depends upon the level of password verification that the organization is willing to accept in case of setting up the password verification function. For instance, once the account gets locked after five successive failed attempts to log in, then in that case the account would remain in the locked state till the next 24 hours, until and less it's unlocked by the DBA.

Also another criteria for the password verification function is that the password expiration days can be set, and the existing password verification is validated by using a user defined verification function which is created by the user who has the full database privileges.

LITERATURE REVIEW

Mostly, I have used my knowledge and working experience to present the details in the paper, however, there were instance, wherein I do have taken the reference of some of the websites pertaining to the database such as the Oracle Base repositories **(https://oracle-base.com/**), and, AWS repositories, (**https://aws.amazon.com/**) which in itself is very huge for the database knowledge know-how, and have presented all the details in my own words after understanding the concept of the said area (Performance) which refers to in this paper.. Also checked and verified the database blogs, and then used some information from the blogs to present the same in my own words for this paper.

Also I have taken the references from my own prepared notes during the day-today working in the database fields, as the challenges which comes into the DB area, and post, the resolution (errors) of the same it brings the solution which is required for the database to work efficiently.

LEARNINGS FROM THIS PAPER

This paper covers the aspects of database security, in **AWS** cloud & Oracle Cloud Infrastructure (**OCI**), which is an important factor in the database management area. The work which has been done to prepare this paper has helped me to a large extent to enhanced my database knowledge not only to the previous versions of database but also to the latest version of Oracle DB 19c, which has many newly added database features (CDB /PDB's)which will definitely help me (DBA) and also the developers.

The implementations of the security features such as encryption and decryption mechanism, database auditing has helped me a lot to monitor the DB server performance with great ease, and which has resulted in the database server performance and health not getting hampered under any circumstances. It is a very good working experience through this paper as it involved live implementations, including development and UAT, on the various security features available in Oracle database technology.

For the preparation of this paper, I have gone into details of each and every components of database aspects pertaining to the overall performance of the DB server, as performance is the most vital part in the database functioning.

IMPLEMENTATIONS

Encryption and Decryption

The encryption & decryption keys are used to encrypt and decrypt data, which are typically, a random strings of bits, and which are generated to scramble and unscramble data. The Encryption & Decryption keys are created with algorithms which are designed to ensure that each key is unique and unpredictable. The longer the keys constructed in this way, the harder it is to break the encryption & decryption code.

The Encryption and Decryption function uses DBMS_CRYPTO which is an inbuilt functionality of Oracle, and which is used to enable encryption and decryption for common Oracle data types like LOBS, BLOBS, RAW, etc. It provides support for encryption and decryption of data across different character sets.DBMS_CRYPTO here uses the "Advanced Encryption Standard (AES)" cryptographic algorithms.

The encryption and decryption mechanism uses a combination of enumerated constants such as Block Cipher Algorithms (ENCRYPT_AES256) plus Block Cipher Chaining Modifiers (CHAIN_CBC) and Block Cipher Padding Modifiers (PAD_PKCS5).

For all the ASCII-based platforms, the AL32UTF8 character set is used, which is used as the Oracle database character set which is accurate for the XML data types. It supports the current version of the Unicode standard, which encodes characters in one, two, or three bytes.

The DBMS_CRYPTO package needs to be used carefully, as if one loses a key or implemented improperly, then the data in this case would be almost unrecoverable.

The Encrypt and decrypt parameters are used in the DBMS_CRYPTO in the Oracle database. Encrypt is an overloaded procedure for encrypting the data, and the details of which is shown below.

Argument	Type	In / Out	Default Value
DST	BLOB | CLOB	IN | OUT	
SRC	BLOB	IN	
TYP	PLS_INTEGER	IN	
KEY	RAW	IN	
IV	RAW	IN	NULL

Figure 1.1 Encrypt Parameters

Decrypt is an overloaded procedure for decrypting the data, and the details of which is shown below.

Argument	Type	In / Out	Default Value
DS	BLOB | CLOB	IN | OUT	
SRC	BLOB	IN	
TYP	PLS_INTEGER	IN	
KEY	RAW	IN	
IV	RAW	IN	NULL

Figure 1.2 Decrypt Parameters

Auditing

Auditing refers to the mechanism in which the monitoring and recording of database actions of the selected user are done. The actions which are recorded in the auditing could be type of SQL statement executed and other factors such as the combination of user name, time, and so on. There are auditing parameters which can be configured to impose the administering of the auditing actions from the database users. In-short auditing helps in tracking all the Database changes in the production environment.

Auditing helps in obtaining the current actions that has been taken place in a particular schema, table, or a record in a table, or affecting specific contents. Auditing is very much helpful in the investigation of the suspicious activity by users in the database. For instance, if some user is deleting data from tables, then in this case the security administrator (DBA), can decide to audit all connections to the database.

Auditing notifies, an auditor that an unauthorized user is manipulating data, and the privilege that the user has is more than expected and can lead to reassessing user authorizations (access given to a particular user).

The use of auditing is such that it is very much helpful in monitoring and gathering data about specific database activities. The various types of auditing that can be performed in a database could be Auditing types and records, SQL statement auditing, schema object auditing, privilege auditing, etc.

Audit records are referred to as the information about the operation that was audited, the specific user performing the operation, and the date and time at which the operation was performed. Audit records can be stored either in the database in a data dictionary table, which is known as database audit trail, or in an Operating System files, which is called as Operating System audit trail.

There are various enhancements that has been done in the Auditing in the latest releases of Oracle wherein the database audit trail can now be moved to a different table space, and this will be helpful in limiting the size of the audit trail. Also the Audit trail records can be purposed as per the DBA policy to keep a track on the growth of the audit trail files. The purging of the audit trail records could be manual or automated purging.

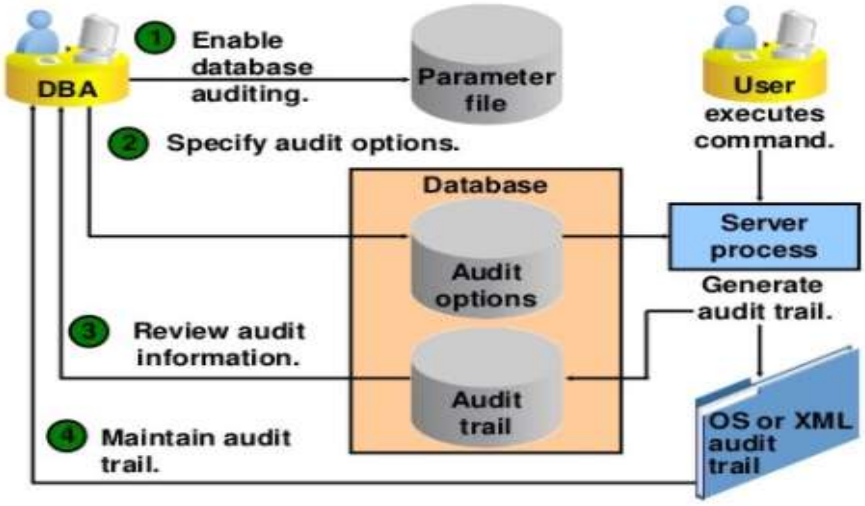

Figure 1.3 Standard Database Auditing

Auditing in the Oracle happens at the database, schema, table level through which it can be tracked the changes which were done by whom in which all objects, relating to DML (Insert, Update, Delete, Merge, Select), etc. as per the standards of auditing

.The information which is required for auditing is stored in the data dictionary. If auditing is enabled, then each time an audit record is created. Database auditing is enabled for some system level privileges. Auditing can also be done at the statement and object level as well.

Audit actions of the users are recorded in the system defined tables within the database, and which can be accessed by only that person (DBA), who has got the access privileges. A normal user cannot get access to the database audit tables, as it is the most critical part for the database security.

The details of the database auditing are stored within the database files, and also at the O/S level. Oracle supports RMAN & EXPDP/IMPDP auditing as well, apart from SYS operations auditing and which needs to be used carefully, as it is at the highest level (data dictionary).

Upgrading Oracle DB Engine in AWS RDS

Amazon RDS supports the following upgrades to an Oracle DB instance:

Major version upgrades:

This requires the DB instance to be modified manually.

Minor version upgrades:

A minor version upgrade includes those changes which are backward-compatible. Minor version upgrades occurs automatically.

Upgrading of the Oracle DB engine requires outage (downtime), the time of which depends upon the DB engine version and the size of the instance.

Depending upon the backup retention period for the DB instance and if it's greater than 0, then, AWS RDS takes the following DB snapshots during the upgrade:

- *A snapshot of the DB instance before any upgrade changes have been made. If the upgrade doesn't work for your databases, you can restore this snapshot to create a DB instance running the old version.*

- *A snapshot of the DB instance after the upgrade completes.*

Very important is to know that, after the completion of the upgrade, you can't revert to the previous version of the DB engine. However, a new DB instance can be created by restoring the DB snapshot taken before the upgrade.

Current Version	Upgrade Supported
12.2.0.1	19.0.0.0 / 12.2.0.1
12.2.0.1	19.0.0.0 / 18.0.0.0
12.1.0.2	19.0.0.0 / 18.0.0.0 /12.2.0.1
11.2.0.4	19.0.0.0 / 18.0.0.0 /12.2.0.1 /12.1.0.2.v5 and higher 12.1 versions

Figure 1.4 AWS RDS Major Version Upgrades

Statistics gathering is mandatory before any major upgrades is accomplished by using the below code:

EXEC DBMS_STATS.GATHER_DICTIONARY_STATS;

Oracle Minor Version Upgrades

An Oracle DB instance in AWS RDS is scheduled to be upgraded automatically during its next maintenance window. One of the most important point is minor version downgrades aren't supported.

Current Version	Upgrade Not Supported
12.1.0.2.v6	12.1.0.2.v7
12.1.0.2.v5	12.1.0.2.v7
12.1.0.2.v5	12.1.0.2.v6

Figure 1.5 Minor Version upgrades not supported

Oracle SE2 Upgrade Paths

Your Existing Configuration	Supported SE2 Configuration
12.2.0.1 SE2, BYOL	12.2.0.1 SE2, BYOL or License Included
12.1.0.2 SE2, BYOL	12.2.0.1 SE2, BYOL or License Included, 12.1.0.2 SE2, BYOL or License Included
11.2.0.4 SE1, BYOL or License Included	12.2.0.1 SE2, BYOL or License Included
11.2.0.4 SE, BYOL	12.1.0.2 SE2, BYOL or License Included

Figure 1.6 Oracle SE2 Upgrade Paths

The DBA should analyze the implications for option groups, parameter groups, and time zones, needs to be reviewed, before performing Oracle DB upgrades.

Data migrations can be performed by using several techniques, like:

- *Oracle Golden Gate.*
- *AWS Database Migration Service (DMS).*
- *Oracle Data Pump (EXPDP / IMPDP).*

Thorough testing of the database and all applications that access the database for compatibility, before performing an upgrade with the new version. This is the most important criteria for any version upgrades.

CONCLUSIONS AND RECOMMENDATIONS

This paper was immensely helpful in implementing the various Oracle database security features with regards to the management of the **large chain of hotels** & **ERP Database world-wide**. The widely regarded and mandatory aspects of the database management in AWS cloud pertains to the security of the DB server. Owing to the growing demand of the database size and taking into account the core areas of database it's very much required to migrate to **19c**.By migrating to **19c** the organizations will get the benefit of **Oracle's ATP (Autonomous Transaction Processing)** feature including **Container databases (CDB/PDB's)** and which provides the HA (High availability). This is highly appreciated and used globally. There is vast features in **Oracle 19c,** and by utilizing which will increase the overall security of the database at large.

The objective of this paper is to convey the core idea of security concerning Database services, and by going through this document, the users would definitively gain a lot of confidence in handling the day-to-day issues arising out at their workplace in their of area of Database Technology (Oracle).Also have elaborated in brief the security features of the latest version of Oracle (19C) Cloud Database, and it's very much advised for all the Organization to shift their Database into 19c Cloud. (First migrate to AWS and then in a phased manner migrate it to 19c Oracle Cloud Database).

As far as recommendations is concerned, I would like to take this opportunity to implement new security features through the use of latest version of **Oracle 19c in AWS cloud / OCI (Oracle Cloud Infrastructure)**, which also supports **Autonomous Transaction Processing (ATP)** feature which reduces the manual intervention of the DBA. Also would like to implement other available feature in **Oracle AWS cloud / OCI Container database (CDB) and pluggable databases (PDB's)**.

Implementations of setting up the **DR at the OCI (Oracle Cloud Infrastructure)** container database environment, where in the primary database is at AWS cloud is completed. Also the **Payroll services** would be migrated to **Oracle 19c OCI (Oracle Cloud Infrastructure)**, which will eventually eradicate the issue of resource management manually, and will obviously enhance the DB performance and security.

Oracle database 19c has new features as compared to **Oracle 12c**, and depending upon the current industry trend it's the right time to migrate to **Oracle Cloud Infrastructure (OCI)**, which is a great player in the database cloud environment management.

BIBLIOGRAPHY

[1] Badger, L., Grance, T., Robert, P. and Voas, J. Computer Security. DRAFT Cloud Computing Synopsis and Recommendations, NIST Special publication 800-146.

[2] Barbara, J., Jo, A., Cynthia, S. and Adam, T. (2009). Collaboration Using Cloud Computing and Traditional Systems. Western Carolina University, Vol. 10, No. 2.

[3] Dykstra, J. and Alan, T. (2012). Acquiring Evidence form Infrastructure-as-a- Service Cloud Computing: Exploring The Evaluation Tools, Trust and Techniques. Digital Investigation S90-S98.

[4] Hofer, C., Karagiannis, G. (2011). Cloud Computing Services: Taxonomy and Comparison. Received: 1 February 2011 / Accepted: 18 May 2011 / Published online: 19 June 2011 © The Author(s) 2011. Retrieved from http://link.springer.com/article/10.1007%2Fs13174-011-0027-x

[5] Lazewski, V., Javier, D., Fugang, W. and Geoffrey, C. (2012). Comparison of Multiple Cloud Frame Works. Retrieved from http://www.academia.edu/2929921/Qualitative_Comparison_of_Multiple_Cloud_Frameworks.

[6] Moghe U, L. P. (2012). Cloud Computing: Survey of Different Utilization Techniques. Sixth International Conference on Software Engineering (CONSEG), (pp. 1-4).

[7]Retrieved from https://securosis.com/blog/data-security-lifecycle-2.0.

[8] Rodriguez-Martinez M. R. (2012). MedBook: A Cloud-Based Healthcare Billing and Record Management System. 5th IEEE International Conference on Cloud Computing (CLOUD), (pp. 899-905).

[9] Tsai, H. F., Lin, Z.-Y., & Chen, C.-M. (2011). Access Security on Cloud Computing Implemented in Hadoop System. Genetic and Evolutionary Computing (ICGEC), Fifth International Conference (pp. 77-80). Xiamen: IEEE.

[10] Flavio, L. (2010). Transparent Security for Cloud. In SAC '10: Proceedings of the 2010 ACM Symposium on Applied Computing.