DATABASE SECURITY AND AUDITING

BY AMINA ABDUL

IA 315: INFORMATION SECURITY AUDITING AND ASSURANCE

AREA TO BE COVERED

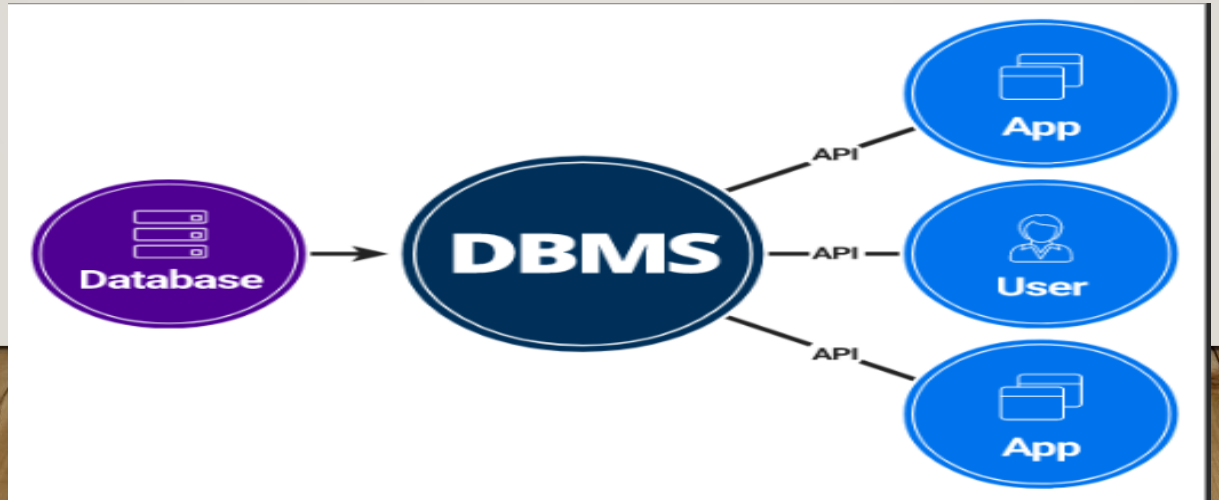
- Introduction to database
- Database security
- Methods to secure a database
- Database Access Control
- Database Auditing
- Data Encryption
- Backups and Restoration of Data

INTRODUCTION TO DATABASE

A database is an organized collection of structured information, or data, typically stored electronically in a computer system.

A database is usually controlled by a database management system (DBMS). Together, the data and the DBMS, along with the applications that are associated with them, are referred to as a database system, often shortened to just database.

Sample Diagram of database system.

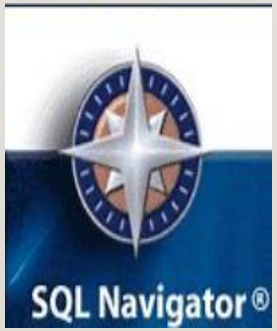


SOME OF DBMS TOOLS

- Toad by Quest
- SQL Developer
- SQL Navigator
- DBVisualizer
- Solarwinds Database Performance Analyzer











INTRODUCTION TO DATABASE Cont..

We have two main types of databases, which are Relational database(SQL) and Non Relational database (NoSQL).

Relational Database(SQL)

- In a relational database management system (RDBMS), the relationship between data is relational and data is stored in tabular form of columns and rows. Each column of a table represents an attribute and each row in a table represents a record. Each field in a table represents a data value.
- Structured Query Language (SQL) is the language used to query RDBMS, including inserting, updating, deleting, and searching records. Relational databases work on each table that has a key field that uniquely indicates each row.

Relational databases are the most popular and widely used databases. Some of the popular RDBMS are **Oracle, SQL Server, MySQL, SQLite, and IBM DB2**.

INTRODUCTION TO DATABASE Cont..

NoSQL Databases

- NoSQL databases are databases that do not use SQL as their primary data access language. Graph database, network database, object database, and document databases are common NoSQL databases.
- NoSQL database does not have predefined schemas, which makes NoSQL databases a perfect candidate for rapidly changing development environments. It also allows developers to make changes without affecting applications. Can be categorized into Column, Document, Graph, Key-value, and Object databases.

Popular NoSQL database are **Cosmos DB**, **ArangoDB, Couchbase Server, CouchDB, Amazon DocumentDB, MongoDB, CouchBase, Elasticsearch, Informix, SAP HANA.**

CAN YOU LIST 3 DATABASE VENDORS WORLDWIDE??

DIFFERENT DATABASE VENDORS



INSTALLATION OF DATABASE

In order to install database, you have to install the OS for your database. You can install database on Linux servers, or windows servers.

After installing OS of your choice successful, you can download the database software from the official websites such as oracle website for oracle database, Microsoft for MS SQL database, MySQL for MySQL database, PostgreSQL and others.

Note: The database software will be downloaded as per OS of your choice. Ie oracle database software for Linux.

Oracle Database 19c Download for Linux x86-64 link for oracle database software

Oracle Database 19c (19.3)

Oracle Database 19c (19.3) for Linux x86-64 (RPM)

Download	Description
oracle-database-ee-19c-1.0-1.x86_64.rpm	(2,694,664,264 bytes) (sha256sum - c519397aea7af9f097cbde6597783f17964e5d53ea3fd90da042d4b65d379652)

Oracle Database 19c (19.3) for Linux x86-64

USEFUL LINKS FOR STEP BY STEP INSTALLATION OF ORACLE DATABASE ON LINUX AND WINDOWS SERVER

- ORACLE-BASE - Oracle Database 19c Installation On Oracle Linux 7 (OL7)
- Installation of Oracle Database 19c On Windows – KTEXPERTS

- By following this two link you will be able to install oracle 19c successful on Linux machine and Windows Server Machine.

For student, I encourage you to install virtual Machines such as OVM or VMware as your own lab and practice this!!!

DATABASE SECURITY

WHAT IS DATABASE SECURITY

Database Security refers to the collective measures used to protect and secure a database or database management software from illegitimate use and malicious threats and attacks.

Database security, protects the confidentiality, integrity and availability (CIA) of an organization databases.

The security Information typically follows the CIA model. **Confidentiality** requires that only authorized users have access to information in order to preserve the privacy of individuals, business intellectual property, and national security efforts.

With the growth of social media and online business due to the Internet, maintaining confidentiality involves using appropriate encryption techniques as well as user authorization, identification, and authentication procedures.

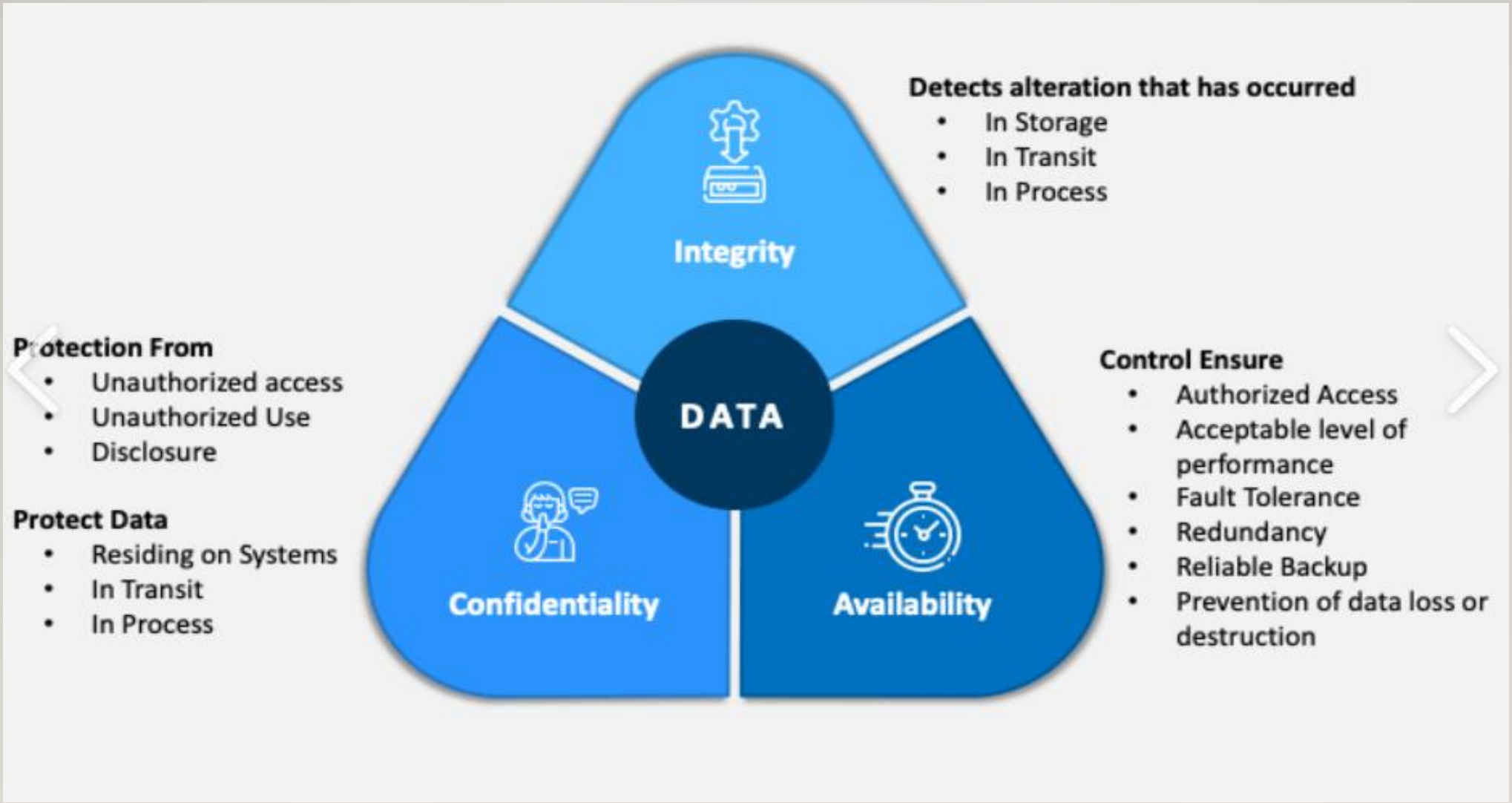
DATABASE SECURITY CONT..

Integrity

its requires that only authorized users be allowed to modify data, thus maintaining data **consistency** and **trustworthiness**. If data is incorrect, it is no longer useful. Incorrect data can also be harmful to individuals (such as wrong data on a credit report) and organizations (such as invalid financial reports).

Availability

its requires that information be accessible by authorized users when needed. Security attacks against an organization can cause business services to become unavailable, leading to violations of service level agreements that are critical to business operations.


Integrity
DATA
Confidentiality
Availability
Detects alteration that has occurred
• In Storage
• In Transit
• In Process
Protection From
• Unauthorized access
• Unauthorized Use
• Disclosure
Protect Data
• Residing on Systems
• In Transit
• In Process
Control Ensure
• Authorized Access
• Acceptable level of performance
• Fault Tolerance
• Redundancy
• Reliable Backup
• Prevention of data loss or destruction

MOST COMMON DATABASE VULNERABILITY

- Poor Encryption and Data Breach.
- SQL Injection.
- Audit Trail Tracking.
- Database Backups.
- Denial of service.
- Missing Security patches.
- Poor users and group privileges management.
- Poor Passwords resources.

METHODS TO SECURE A DATABASE

- Avoid using default ports.
- Using Firewalls.
- Using separate servers.
- **Users Authentication**
- **Database Access control**
- **Database Auditing**
- **Encryption**
- **Backups**
- Apps and database up to date

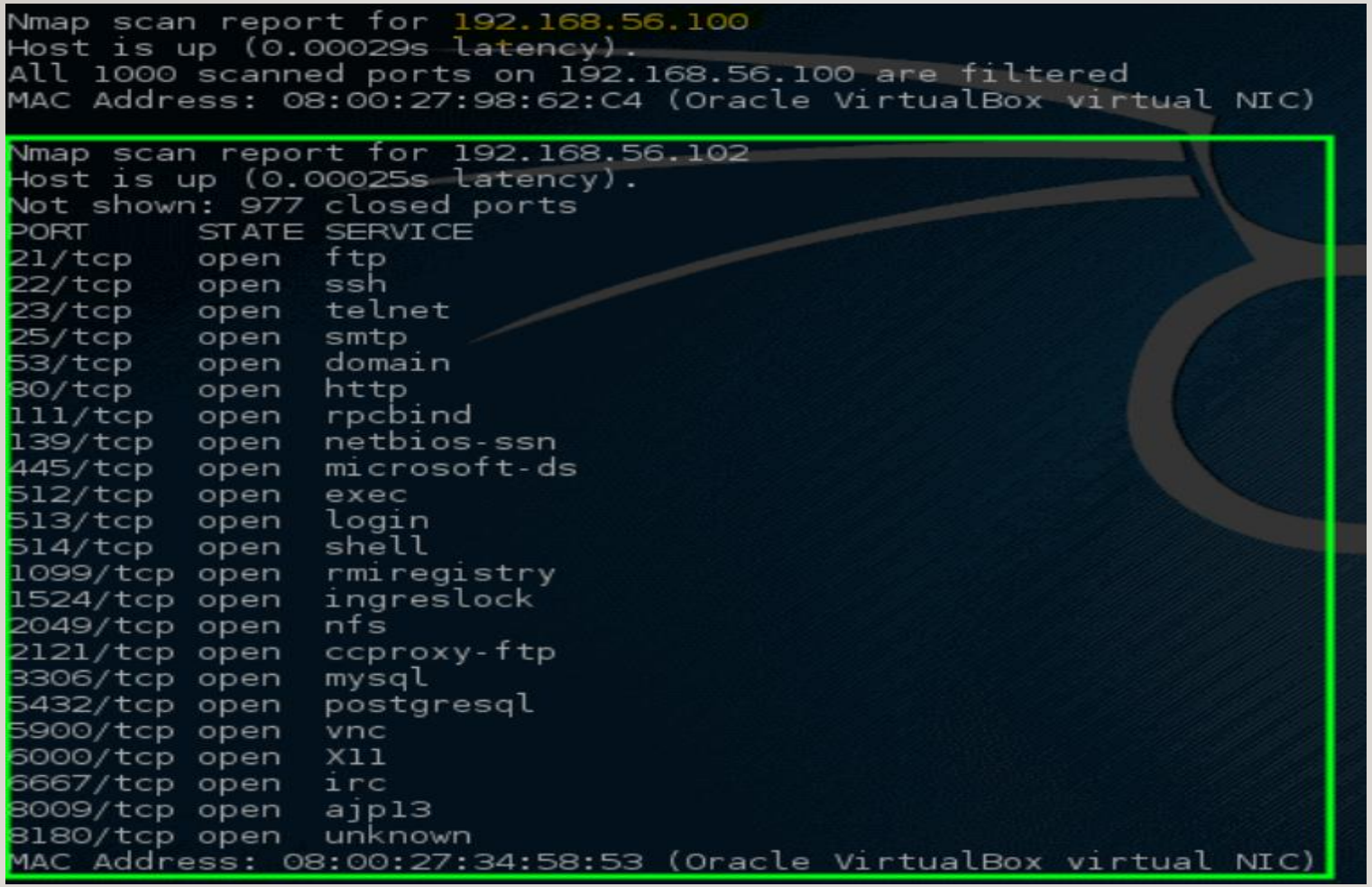
DEFAULT DATABASE PORTS

Each Database has its own default port. If a DBA install database using defaults port made an attacker task easy, because once the attacker scan the network will identify the database running on that machine.

As one of the methods to secure a database, a DBA should avoid using defaults ports.

Default ports for MS SQL, Oracle, MySQL, PostgreSQL and MongoDB database are (1433,4022,135,1434), 1521, 3306, 5432 and 27017 respectively.

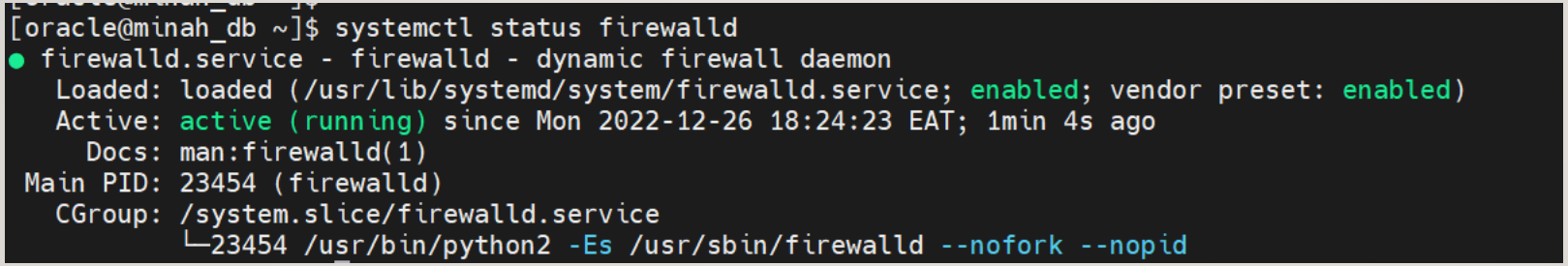
SAMPLE OF NMAP OUTPUT



USING FIREWALL

- Firewall can be used in order to allow only allowed range of IP address to connect to the database servers. Eg in Linux server, server firewall can be enables and use IP table to allow only few IP range to connect.

The following snapshot shows the status of firewall on Linux server



USING SEPARATE SERVERS

For secure database system, its better to separate database servers with application servers. This will increase data security and improve performance. Once an attacker get access to application servers wont be able to harm database server.

But on single node application and database, both database and application could be harmed/destroyed by an attacker.

Also on high availability of service multiple node are installed on different server and application is configured only to point the virtual IP , Once attacker get access to one node DBA could easy disconnect the server but application and business wont notice any changes.

UP TO DATE DATABASE AND APPLICATION

- Each database has many versions. In oracle we have oracle 11g, 12c, 18c, 19c and 21c. But starting 12c and below version are already out dated and are no longer supported by oracle. This means no any security patches which will be released by the vendor. For organizations which are still using those oracle versions are in high risk of being attacked.
- Security Patches most are released in January, April, July and October for Oracle databases and MySQL database, while in MS SQL are release after every two months (60 days).

As DBA you have to make sure all security patches are applied once are stable in order to secure the databases.

USER AUTHENTICATION

- Users can be authenticated in a number of different ways before they are allowed to create a database session.
- In database authentication, you can define users such that the database performs both identification and authentication of users.
- In external authentication, you can define users such that authentication is performed by the operating system or network service. Alternatively, you can define users such that they are authenticated by the Secure Sockets Layer (SSL).

USER AUTHENTICATION CONT..

- Passwords are one of the basic forms of authentication. A user must provide the correct password when establishing a connection to prevent unauthorized use of the database.
- In this way, users attempting to connect to a database can be authenticated by using information stored in that database.
- Passwords are assigned when users are created, a database can store a user's password in the data dictionary in an encrypted format.

Useful link: https://docs.oracle.com/cd/B14117_01/network.101/b10777/authuser.html

USER AUTHENTICATION CONT..

A number of steps can strengthen the basic password feature and provide greater control over database security:

- Password management policy can be controlled by DBAs through user profiles.
- The DBA can establish standards for password complexity, such as minimum password length.
- Passwords should be words that cannot be found in the dictionary. They should not consist of people's names or birthdates.
- Passwords can be timed out, expiring after a certain amount of time. This requires users to change the value periodically.
- Reuse of passwords can be prohibited for a certain amount of time.
- When a particular user exceeds a designated number of failed login attempts, the server can automatically lock that user's account.

USER PROFILE SNAPSHOT ON PASSWORD RESOURCES

	PROFILE	RESOURCE_NAME	RESOURCE_TYPE	LIMIT	COMMON	INHERITED	IMPLICIT
1	DEFAULT	COMPOSITE_LIMIT	KERNEL	UNLIMITED	NO	NO	NO
2	DEFAULT	SESSIONS_PER_USER	KERNEL	UNLIMITED	NO	NO	NO
3	DEFAULT	CPU_PER_SESSION	KERNEL	UNLIMITED	NO	NO	NO
4	DEFAULT	CPU_PER_CALL	KERNEL	UNLIMITED	NO	NO	NO
5	DEFAULT	LOGICAL_READS_PER_SESSION	KERNEL	UNLIMITED	NO	NO	NO
6	DEFAULT	LOGICAL_READS_PER_CALL	KERNEL	UNLIMITED	NO	NO	NO
7	DEFAULT	IDLE_TIME	KERNEL	UNLIMITED	NO	NO	NO
8	DEFAULT	CONNECT_TIME	KERNEL	UNLIMITED	NO	NO	NO
9	DEFAULT	PRIVATE_SGA	KERNEL	UNLIMITED	NO	NO	NO
10	DEFAULT	FAILED_LOGIN_ATTEMPTS	PASSWORD	10	NO	NO	NO
11	DEFAULT	PASSWORD_LIFE_TIME	PASSWORD	180	NO	NO	NO
12	DEFAULT	PASSWORD_REUSE_TIME	PASSWORD	UNLIMITED	NO	NO	NO
13	DEFAULT	PASSWORD_REUSE_MAX	PASSWORD	UNLIMITED	NO	NO	NO
14	DEFAULT	PASSWORD_VERIFY_FUNCTION	PASSWORD	NULL	NO	NO	NO
15	DEFAULT	PASSWORD_LOCK_TIME	PASSWORD	1	NO	NO	NO
16	DEFAULT	PASSWORD_GRACE_TIME	PASSWORD	7	NO	NO	NO
17	DEFAULT	INACTIVE_ACCOUNT_TIME	PASSWORD	UNLIMITED	NO	NO	NO
18	ORA_STIG_PROFILE	COMPOSITE_LIMIT	KERNEL	DEFAULT	NO	NO	NO
19	ORA_STIG_PROFILE	SESSIONS_PER_USER	KERNEL	DEFAULT	NO	NO	NO
20	ORA_STIG_PROFILE	CPU_PER_SESSION	KERNEL	DEFAULT	NO	NO	NO

DATABASE AUDITING

- Audit Trails records all access to the database, keeping information about the user who requested the access, the operation performed, the workstation used, the exact time of occurrence, the data item, its old value, and its new value, if any.
- The audit trail can therefore uncover the sources of suspicious operations on the database, even if they are performed by authorized users, such as disgruntled employees. Triggers can also be used to set up an audit trail for a table, recording all changes, the time they were made, and the identity of the user who made them.

Tools for database auditing are Oracle vault, Audit trails, Profiler (Microsoft)

https://docs.oracle.com/cd/E14472_01/doc.102/e14460/toc.html

AuditTrail Report

Sunday, November 15, 20
4:10:45 P

AuditTrailID	DateTime	UserName	FormName	Action	RecordID	FieldName
1	11/8/2015 11:17:07 AM	Tewan	Customer	New	19	
2	11/8/2015 11:18:39 AM	Tewan	Customer	New	20	
3	11/8/2015 11:19:32 AM	Tewan	Customer	Edit	19	CustomerNan
4	11/8/2015 11:19:32 AM	Tewan	Customer	Edit	19	Address
6	11/8/2015 11:23:24 AM	Tewan	Customer	Delete	20	
7	11/8/2015 11:36:11 AM	Tewan	Customer	Delete	19	
8	11/9/2015 7:46:52 PM	Tewan	Employees	New	11	
9	11/9/2015 7:48:09 PM	Tewan	Employees	New	12	
10	11/9/2015 7:49:14 PM	Tewan	Employees	Edit	12	FullName
11	11/9/2015 7:49:14 PM	Tewan	Employees	Edit		
12	11/14/2015 3:55:39 PM	nancyf	Customer	Delete		

Deleted Customer

Customer_ID	CustomerName	Address	City	S
20	James Bond	007		
19	Test Edit	9999	New York	
20	James Bond	007		
22	test preview	555	co	

Activity Overview

Rows 15 Go

Create PDF

Event Time is in the last 24 hours

Tip: The current settings would result in more than 20,000 rows. Please add more filters to ensure complete and correct results.

Source	Category	Event	User	Target	Host	Event Time
oracle1	USER SESSION	LOGOFF	MALOEUF		binks241	10/16/2009 05:11:12 PM
oracle1	USER SESSION	LOGOFF	MALOEUF		binks241	10/16/2009 05:11:8 PM
oracle1	USER SESSION	LOGOFF	MALOEUF		binks241	10/16/2009 05:9:35 PM
oracle1	USER SESSION	LOGOFF	MALOEUF		binks241	10/16/2009 08:30:55 AM
oracle1	USER SESSION	LOGOFF	MALOEUF		binks241	10/15/2009 09:28:6 PM
oracle1	USER SESSION	LOGOFF	MALOEUF		binks241	10/15/2009 11:23:33 AM
oracle1	USER SESSION	LOGOFF	MALOEUF		binks241	10/15/2009 11:19:53 AM
oracle1	SYSTEM MANAGEMENT	SUPER USER DML	/			10/13/2009 03:58:21 PM
oracle1	USER SESSION	SUPER USER LOGON	/			10/13/2009 03:57:49 PM
oracle1	USER SESSION	LOGOFF	MALOEUF		binks241	10/8/2009 08:16:50 PM
oracle1	USER SESSION	LOGOFF	MALOEUF		binks241	10/7/2009 07:40:49 AM
oracle1	USER SESSION	LOGOFF	MALOEUF		binks241	10/6/2009 04:13:51 PM
oracle1	USER SESSION	LOGOFF	MALOEUF		binks241	10/6/2009 01:9:55 PM
oracle1	USER SESSION	LOGOFF	MALOEUF		binks241	10/6/2009 12:12:24 PM
oracle1	SYSTEM MANAGEMENT	SUPER USER DDL	/			10/6/2009 10:59:52 AM

DATA ENCRYPTION

Data can be stored in the database in encrypted form. Only the database management system can unscramble the data, so that anyone who obtains data by any other means will receive jumbled data. When authorized users access the information properly, the DBMS retrieves the data and decodes it automatically.

Encryption should also be used whenever data is communicated to other sites, so that wire tappers will also receive scrambled data. Encryption requires a cipher system , which consists of the following components:

- An encrypting algorithm , which takes the normal text (plaintext) as input, performs some operations on it, and produces the encrypted text (ciphertext) as output
- An encryption key , which is part of the input for the encrypting algorithm and is chosen from a very large set of possible keys
- A decrypting algorithm , which operates on the ciphertext as input and produces the plaintext as output
- A decryption key , which is part of the input for the decrypting algorithm and is chosen from a very large set of possible keys

DATABASE ACCESS CONTROL

Database access control is the process of making sure that data or other resources are accessed only in authorized ways. In planning access, the DBA might use an access control matrix for the database.

	OBJECT					
SUBJECT	Student table	StuView1	WrapUp Procedure	Faculty table	Enroll table	CREATE TABLE
User U101	READ, UPDATE	READ	EXECUTE	READ		YES
User U102		READ				NO
Advisor Role	READ	READ			READ, INSERT, UPDATE, DELETE	NO
. . .	. . .	. . .	. . .	. . .	. . .	. . .

DATABASE ACCESS CONTROL CONT…

DBA can grant data access to others or to revoke access. Some systems allow the DBA to delegate some of this power, granting users the power to authorize other users to perform operations on the database. However, having many such authorizers can be extremely dangerous. Since authorizers can create other authorizers, the situation can get out of hand very quickly, making it difficult for the DBA to revoke authorizations.

Using Views for Access control in database

Views is a virtual table whose contents are defined by a query. Like a table, a view consists of a set of named columns and rows of data. Unless indexed, a view does not exist as a stored set of data values in a database.

A view can be used to control access to various database objects on users.

DATABASE ACCESS CONTROL CONT…

```
CREATE VIEW CSCMAJ AS
       SELECT stuId, lastName, firstName, credits
       FROM Student
       WHERE major = 'CSC';
```

```
CREATE VIEW StuView1 AS
       SELECT stuId, lastName, firstName, major
       FROM Student;
```

ROLES IN DATABASE

Roles are groupings of privileges that you can use to create different levels of database access. For example, you can create a role for application developers that enable users to create tables and programs.
You can grant privileges and roles to other users only when you possess the necessary privilege.

The granting of roles and privileges starts at the administrator level.
At database creation, the administrative user SYS is created and granted all system privileges and predefined Oracle roles.

User SYS can then grant privileges and roles to other users and also grant those users the right to grant specific privileges to others.

DATABASE ACCESS CONTROL CONT…

DEMONSTRATION ….

BACKUP

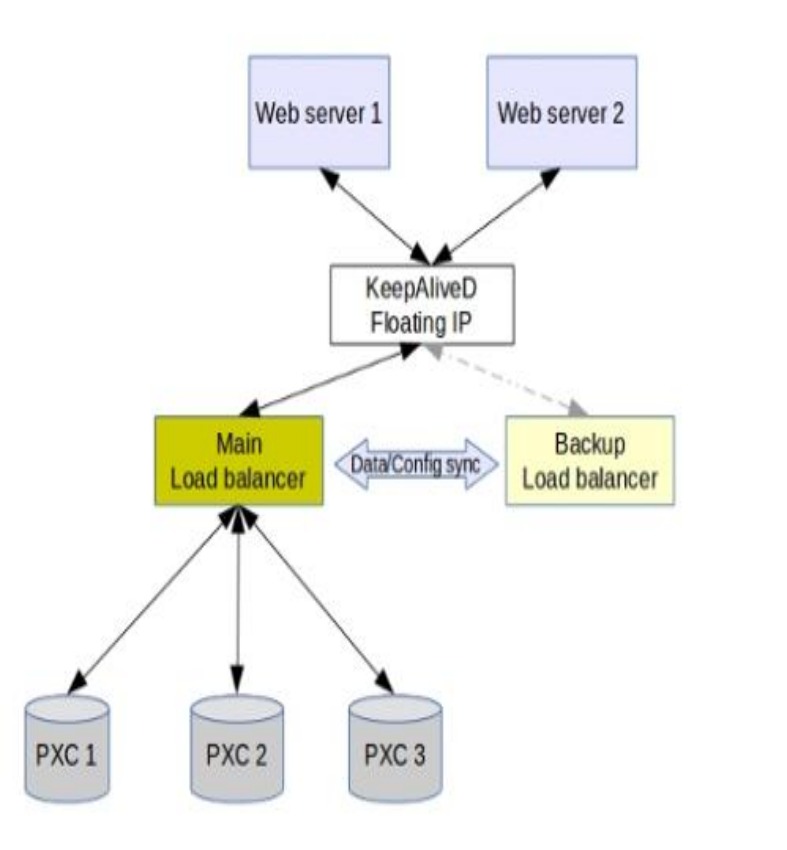
Database backup is the process of backing up the operational state, architecture and stored data of database software. It enables the creation of a duplicate instance or copy of a database in case the primary database crashes, corrupted or lost.

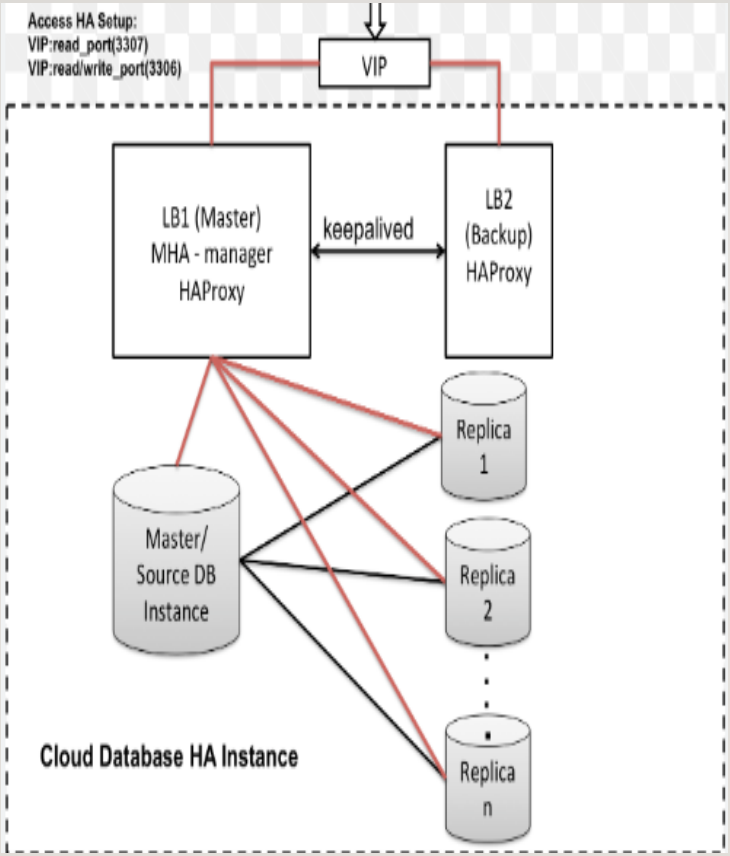
The most common backup types are a full backup, incremental backup and differential backup. Other backup types include synthetic full backups and mirroring.

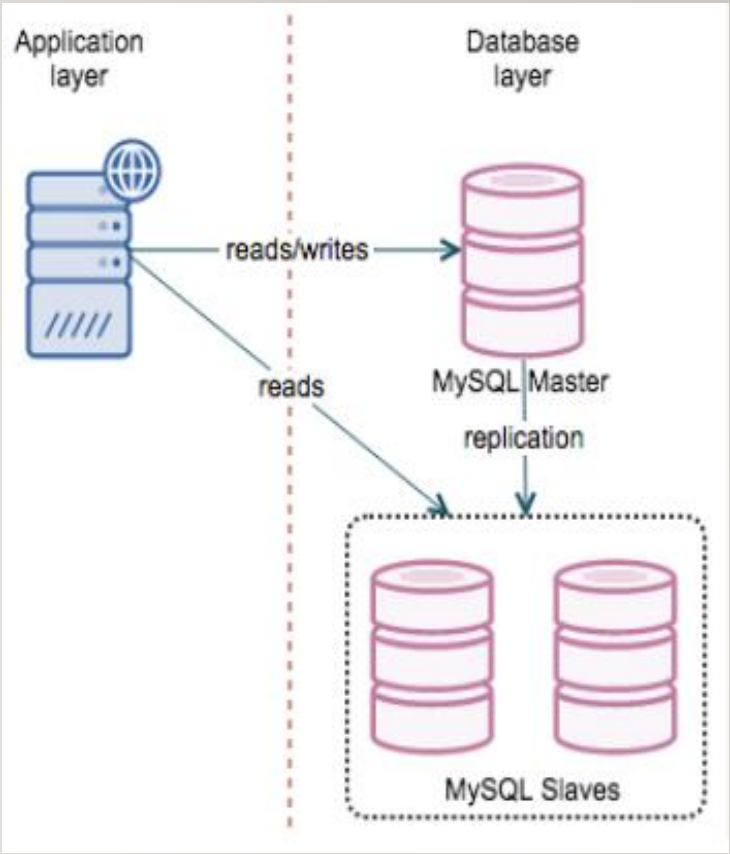
Backup of database is also among the methods of securing database, it increase data availability which in turn results to Business continuity. As one of Government condition to each organization, is to ensure continuity of the business by having different plans on data availability through backup and Disaster recovery.

DATA HIGH AVAILABILITY

- A High Availability (HA) Database is a database system designed to operate continuously with no interruptions in service. So database errors and failures must be handled by automatically failing over to redundant nodes when problems occur.
- High availability database design requires enough nodes to properly distribute the load, and an appropriate consistency requirement. The more nodes, and the stronger the consistency model, the more latency is possible in the system.


Web server 1
Web server 2
KeepAliveD
Floating IP
Main
Load balancer
Data/Config sync
Backup
Load balancer
PXC 1
PXC 2
PXC 3


Access HA Setup:
VIP:read_port(3307)
VIP:read/write_port(3306)
VIP
LB1 (Master)
MHA - manager
HAProxy
keepalived
LB2
(Backup)
HAProxy
Master/
Source DB
Instance
Replica
1
Replica
2
Replica
n
Cloud Database HA Instance


Application
layer
Database
layer
reads/writes
reads
MySQL Master
replication
MySQL Slaves

DISASTER RECOVERY

Is the activities that need to be done to restore the database in the event of a fire, earthquake, vandalism, or other catastrophic events.

A plan for disaster recovery can include one or more of the following:

- A site to be used in the event of an emergency
- A different machine on which to recover the database
- Offsite storage of either database backups, tablespace backups, or both, as well as archived logs.

This is called secondary site. Can be used when primary site is inaccessible.

DISASTER RECOVERY CONT…

Different technology such as Dell EMC, oracle Data guard, Peer-to-peer remote copy are used to copy replicate data from primary site to secondary site.

Data can be copied from storage to storage by using Dell EMC or object to object using oracle data guard in oracle databases.

The organizations suppose to perform DR test each quarter in order to ensure the secondary site is working fine and incase of any emergency to the primary site, it will be able to handle everything.

USEFUL LINKS

https://www.ibm.com/docs/en/db2/11.5?topic=recover-disaster-recovery

https://www.vmware.com/topics/glossary/content/disaster-recovery.html

https://www.oracle.com/cloud/backup-and-disaster-recovery/

Link for oracle education: https://education.oracle.com/

Data access control: https://www.datasunrise.com/professional-info/what-is-access-control/

Roles: https://learn.microsoft.com/en-us/sql/relational-databases/security/authentication-access/database-level-roles?view=sql-server-ver16

https://docs.oracle.com/cd/B16351_01/doc/server.102/b14196/users_secure002.html

ANY QUESTION???

THANK YOU!!!