DATABASE AUDITY AND MAINTENANCE

PRACTICAL CHAPTER 1

DATABASE ADMINISTRATION AND MANAGEMENT (IT-507)

Database Auditing

- Database auditing is the process of monitoring and recording activities and events that occur within a database system.
- It is a critical component of database management and security.
- The primary goal of auditing is to ensure the accountability of users, maintain data integrity, and detect and respond to security breaches or unauthorized access.

Database Auditing

Here's a breakdown of key concepts within database auditing.

- **Monitoring**
- **Accountability**
- **Security**
- **Regulatory Compliance**

Database Auditing (Monitoring)

- Auditing involves continuously monitoring the actions and operations performed within a database. This includes tracking who accesses the database, what they do once inside, and any changes made to the data.

Database Auditing (Accountability)

- Auditing creates a trail of evidence that can be used to establish accountability. In case of data breaches or unauthorized actions, audit logs can be crucial in identifying the responsible parties.

Database Auditing (Security)

- One of the primary purposes of auditing is to enhance the security of the database. It helps in detecting and preventing security vulnerabilities and unauthorized access attempts.

Database Auditing (Regulatory Compliance)

- Many industries and organizations are subject to regulations that require them to maintain audit logs.
- For instance, healthcare organizations need to comply with the Health Insurance.

Types of Database Auditing:

- User Auditing
- Data Auditing
- Privilege Auditing

Types of Database Auditing:

1. **User Auditing**

Definition: User auditing involves monitoring the actions of database users, such as login attempts, queries executed, and data modifications.

Example: Tracking when a user logs into the database, what queries they run, and when they log out. This helps in identifying suspicious or unauthorized activities.

Types of Database Auditing:

2. Data Auditing

Definition: Data auditing focuses on tracking changes made to data records, including insertions, updates, and deletions.

Example: Recording when a customer's address is updated in a customer database, including the previous and new values. This ensures data accuracy and can be critical for compliance.

Types of Database Auditing:

3. Privilege Auditing

Definition: Privilege auditing involves monitoring user privileges and access controls to ensure that users only have access to what they are authorized to see or modify.

Example: Tracking changes to user roles and permissions. For instance, if a user's access level is elevated, the audit log should capture this change.

Common Audit Events

- **Login and Logout Events:**

  Recording when users log into and out of the database.
- **DDL (Data Definition Language) Statements:**

  Capturing changes to database structures, such as creating or altering tables and views.
- **DML (Data Manipulation Language) Statements:**

  Logging data modifications, including inserts, updates, and deletes.
- **Security-Related Events:**

  Monitoring failed login attempts and changes to access control settings.
- **Database Errors and Exceptions:**

  Recording database errors, which can be helpful for troubleshooting.

Tools and Techniques for Auditing:

- **Database Logs and Audit Trails**: Most DBMSs provide built-in logging and auditing features. For example, Oracle Database has the Oracle Audit Vault and Database Firewall for comprehensive auditing

- **Third-Party Auditing Tools**: Organizations may also use third-party auditing and security information and event management (SIEM) solutions like Splunk, IBM QRadar, or McAfee Enterprise Security Manager (ESM) for more advanced auditing capabilities.

Auditing Best Practices

- **Setting Audit Policies and Thresholds:**

  Define which events to audit and set thresholds for capturing and retaining audit data based on business and security requirements.

- **Regular Review of Audit Logs:**

  Ensure that audit logs are routinely reviewed for suspicious activities or compliance violations.

- **Responding to Security Incidents:**

  Establish procedures for responding to security incidents based on audit log findings.

Advice for Database Auditing

- Auditing can be a large consumer of system resources. When the audit queue is full, tasks that generate audit records will wait until the auditing task can resume.
- Place the system catalog tables that store security-related information on a separate, inactive disk . This will enhance auditing performance by decreasing head contention.
- Ensure that the data set or table used to store audit data does not fill up. When the audit data set is full, auditing will be disabled, records in the current audit queue will be lost, and any user task attempting to send data to the audit queue will be cancelled.

Basic Example of Audit how it works

Suppose you have a database that stores customer information, and you want to audit user access. You set up user auditing to capture login and logout events. A user named "John" logs into the database at 10:00 AM and logs out at 11:30 AM. The audit log records these events, including the timestamp.

```
Audit Log Entry:
User: John
Event: Login
Timestamp: 10:00 AM

User: John
Event: Logout
Timestamp: 11:30 AM
```

DATABASE AUDITY

THE END