Data Administrator (DA) and Database Administrator (DBA) functions are related to the management of an organization's data resources yet different in terms of duties and responsibilities. Although both are important to make certain that data is well collected, stored, and utilized, their roles are quite different.

A **Data Administrator** emphasizes the responsibilities involved in planning, directing, and organizing the data as an entity as well as being responsible for enforcing data policies and standards. A Database Administrator is more focused on the technical aspects of physical and logical Database Management and is responsible for managing the smooth and unhampered running of databases, with security being a major factor too. It is important to differentiate between these roles and this paper will help organizations in achieving the best in data management and technical database performances.

What is Data Administrator (DA)?

A Data Administrator is a person who is responsible for processing data into a convenient data model. The person is in charge of figuring out which data is relevant to be stored in the database. Data Administrator is less of a technical role and more of a business role with some technical knowledge. This role is also known as Data Analyst. So, it is mostly a high-level function that is responsible for the overall management of data resources in an organization.

Responsibilities :

- Filters out relevant data
- Monitor the data flow throughout the organization
- Designs concept-based data model
- Analyze and break down the data to be understood by the non-tech person
- Developing and implementing data policies and standards that ensure the accuracy, completeness, and consistency of data across the organization.
- Planning and implementing data architecture, which includes defining the data models, data integration, and data flow across different systems.

What is database security?

Database security refers to the range of tools, controls and measures designed to establish and preserve database confidentiality, integrity and availability. Confidentiality is the element that's compromised in most data breaches.

Database security must address and protect the following:

- The data in the database.
- The database management system (DBMS).
- Any associated applications.
- The physical database server or the virtual database server and the underlying hardware.
- The computing or network infrastructure that is used to access the database.

  Database security is a complex and challenging endeavor that involves all aspects of information security technologies and practices

Authentication and authorization are two vital information security processes that administrators use to protect systems and information. Authentication verifies the identity of a user or service, and authorization determines their access rights.

Fixed server roles are those roles that have permissions associated with the server itself, and fixed database roles are those roles that are associated with permissions for the database. These roles are called fixed because they cannot be changed or removed.

Backup

Database backup is the process of creating a copy of a company's master and transaction data files.

As consumers, we need extra supplies when our typical resources aren't usable. For instance, in case of a blackout, one would want candles, flashlights, and canned goods.

Similarly, a database backup is a copy of key data you can access in case of a cyberattack, natural disaster, accidental deletion, or other threat.

What Are the Types of Database Backup?

There are three general types of database backup:

- A **full backup** is, as the name implies, a copy of all your data, or the whole database or database instance.
- An **incremental backup** is when only data that changed since the last backup is updated in a new backup file. For example, if accounting posted three new transactions, only those new transactions would be copied to a new accounting files backup.
- A **differential backup** is used to back up all files that have changed since the last full backup was done.

A **binary file** is a file that contains data in a format that is not human-readable but is meant for direct processing by a computer. It is stored as a sequence of bytes (binary data) and can include any type of information, such as text, images, videos, executable programs, or database files.

An **on-premise backup** refers to a data backup strategy where all backup processes and storage are performed locally within an organization's own physical infrastructure, rather than relying on cloud-based services. This backup method is typically used for maintaining control over data and ensuring quick access during recovery.

Feature	Logical Backup	Physical Backup
Format	Human-readable (SQL, dumps)	Binary files, raw data blocks
Portability	High (cross-platform)	Low (system-specific)
Performance	Slower (export/import operations)	Faster (file copy operations)
Granularity	Highly granular	Typically full database or nothing
Use Case	Migration, partial backups, flexibility	Disaster recovery, faster restores

Into to NoSql Database Management System

Velocity in Science stance for how fast the object **when gravity first applies force on the object.**

Speed = Distance / Time

In Summary:

NoSQL offers several advantages over SQL databases, particularly when you need:

- Scalability to handle huge amounts of data or users.
- Flexibility to store and process dynamic, unstructured, or semi-structured data.
- Performance for high-throughput, low-latency operations.
- High availability and fault tolerance for ensuring uptime even during failures.

While SQL databases remain powerful and ideal for highly structured data and complex transactions, NoSQL is a better fit for modern, large-scale applications that require flexibility, speed, and scalability.