Safety of information systems

Lecturer: Roman Danel

Data and databases safety

Databases Security

- Protecting database against abuse
- Securing login information
- Securing communication between applications and databases
- Securing queries against „SQL-injection“

Architecture of secure information systems:

- *Trusted Subject Architecture* – Database system and operating system are one entity
- *Woods Hole Architecture* - Users are working with a set of untrusted interfaces for different security levels. They communicate with a trusted interface (front end), which acts as a reference monitor. Database system itself is again untrustworthy.

Availability

- Data needs to be available at all necessary times
- Data needs to be available to only the appropriate users
- Need to be able to track who has access to and who has accessed what data

Authenticity

- Need to ensure that the data has been edited by an authorized source
- Need to confirm that users accessing the system are who they say they are
- Need to verify that all report requests are from authorized users
- Need to verify that any outbound data is going to the expected receiver

Integrity

- Need to verify that any external data has the correct formatting and other metadata
- Need to verify that all input data is accurate and verifiable

- Need to ensure that data is following the correct work flow rules for your institution/corporation
- Need to be able to report on all data changes and who authored them to ensure compliance with corporate rules and privacy laws.

Confidentiality

- Need to ensure that confidential data is only available to correct people
- Need to ensure that entire database is security from external and internal system breaches
- Need to provide for reporting on who has accessed what data and what they have done with it
- Mission critical and Legal sensitive data must be highly security at the potential risk of lost business and litigation

Databases Built-in Protection

- Password Controls
- Data access based on roles and profiles
- IP restrictions for off site access
- Auditing capabilities of who has run what reports
- Security logging

Examples of attacks

SQL injection

SELECT * **FROM** table1 **WHERE** username = 'x';**DROP TABLE** table1; **SELECT** '1'

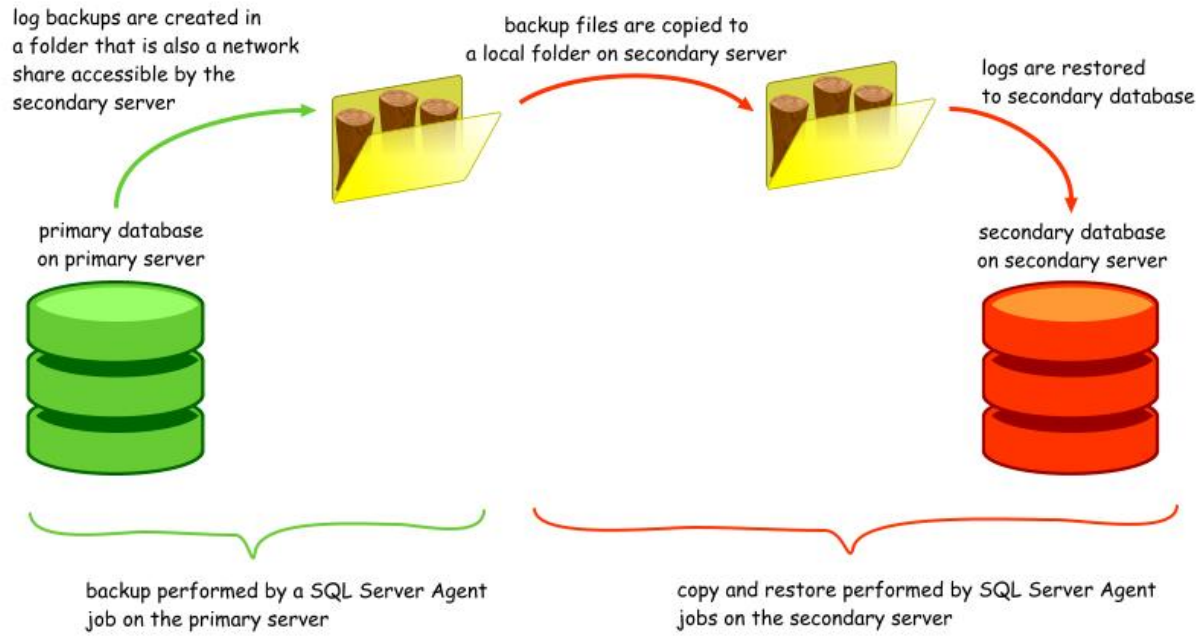
DOS (Denial of Systems)

… =x' AND BENCHMARK(9999999,BENCHMARK(999999,BENCHMARK(999999,MD5(NOW()))))=0 OR '1'='1

Technologies for Databases Safety

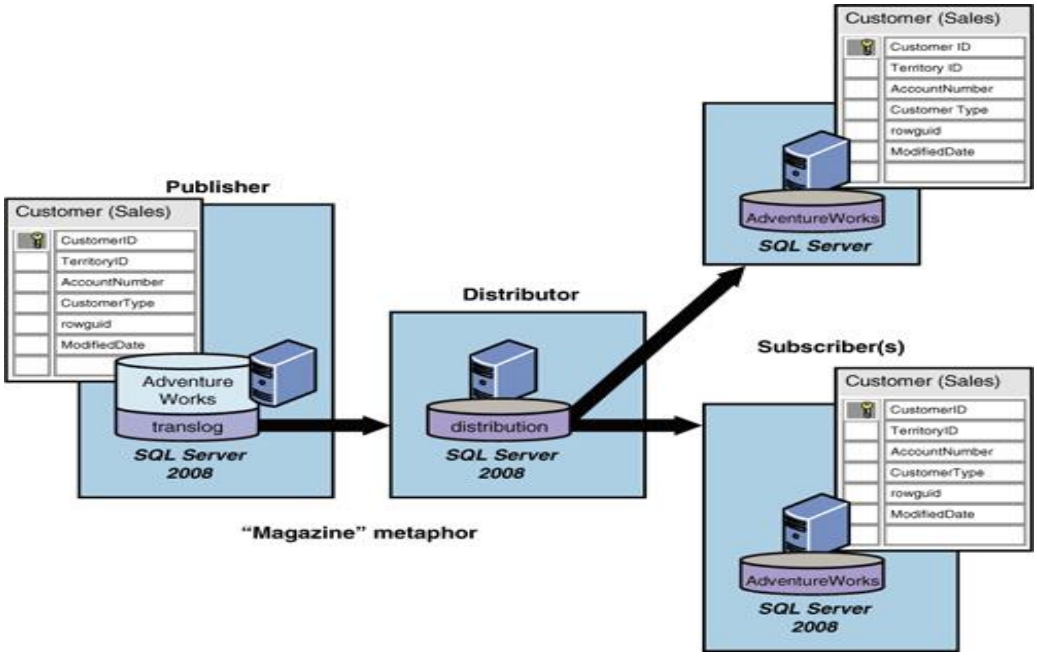
1. log shipping
2. Replication
3. Mirroring
4. Always-On¨
5. Clustering

Log shipping



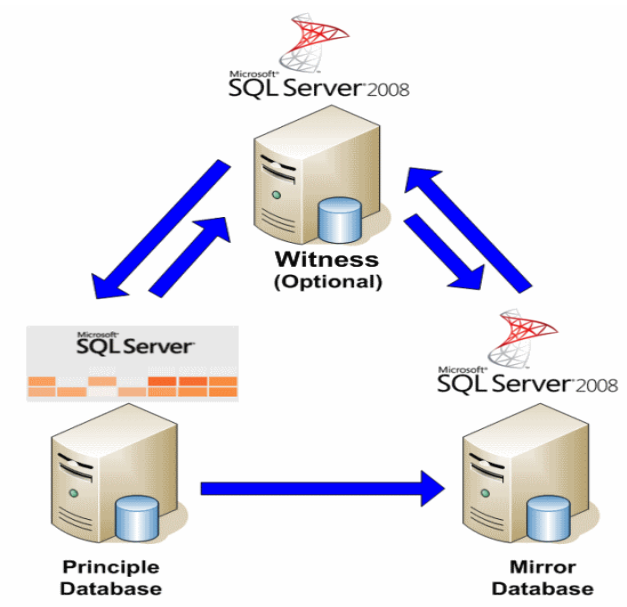
Source: www.sqlbackuprestore.com

Replication

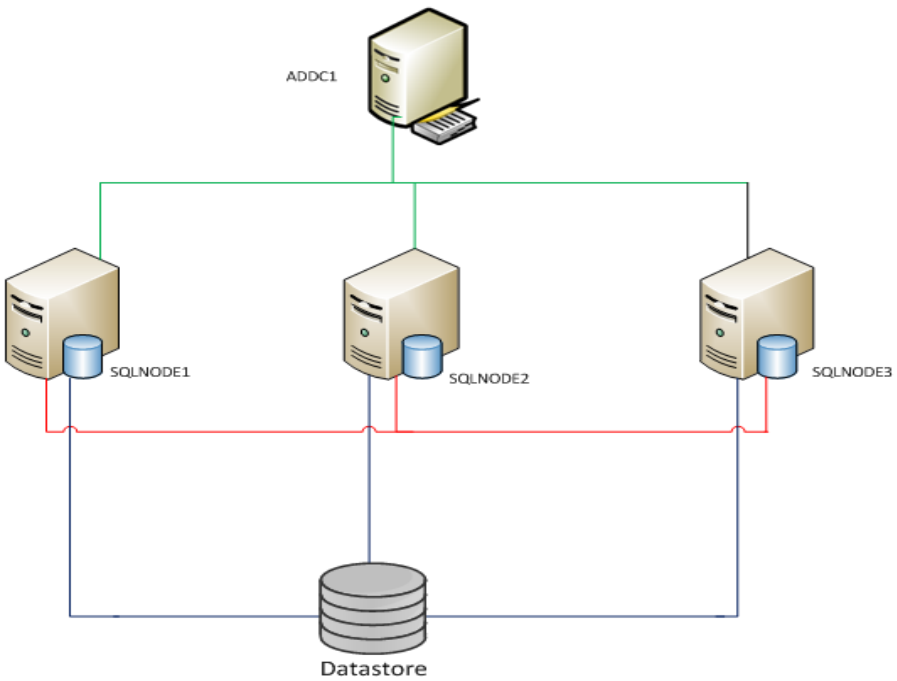


Source: Microsoft MSDN

Mirroring



Always-On (Microsoft SQL Server)



Always On Availability Group (Microsoft SQL Server)