High Availability & Disaster Recovery In Database Systems

BATCH - UGC25-26_04

Faculty
Ms. S.F.Shaikh

Team Members

22510064 Parshwa Herwade

22510070 Suyash Yadav

22510089 Purva Markam

22510112 Harshavardhan Bamane

Table of Content

22510070 Suyash Yadav

Introduction & High Availability Concepts

DEFINITION:

High Availability refers to a system's ability to remain operational and accessible for a high percentage of time, minimizing downtime.

Importance of Uptime:

- 99.99% availability means less than 53 minutes downtime/year.
- Directly impacts user trust, business continuity, and revenue.

Application Industries:

- Banking & Finance – 24/7 transactions.
- E-commerce – Online sales depend on uptime.
- Healthcare – Access to patient data in emergencies.

Uptime (%)	Downtime per Year
99,9	8,8 hours
99,95	4,4 hours
99,99	52,6 minutes
99,999	5,3 minutes

22510070 Suyash Yadav

High Availability Concepts

Key Concepts:

- Clustering: Grouping multiple servers/databases to act as one.
- Failover: Automatic switch to backup when primary fails.
- Redundancy: Having duplicate components to avoid single points of failure.

Architectures:

- Active-Active: All nodes handle traffic simultaneously.
- Active-Passive: One active node, one standby.

How HA is Achieved in Databases:

- Replication: Copying data to multiple servers.
- Load Balancing: Distributing traffic across servers.
- Failover Clustering: Automatic role switch on failure.

Examples:1.MySQL Cluster – Synchronous replication for HA.

2.Oracle RAC – Multiple instances accessing the same database.

22510089 Purva Markam

What is Disaster Recovery (DR)?

Disaster Recovery (DR) is the set of policies, tools, and procedures that enable an organization to restore IT systems, data, and business operations after a disruptive event — such as a natural disaster, cyberattack, hardware failure, or human error.
It's a subset of Business Continuity (BC), but focuses specifically on recovering technology and data rather than all business processes.

22510089 Purva Markam

Types of DR Sites

1.Hot Site

Definition: A fully equipped backup facility that mirrors the primary site in real-time.

Features:

- Real-time or near-real-time data replication
- All hardware, software, and network connections ready
- Can take over operations immediately after a disaster

2.Warm Site

Definition: A partially equipped facility with hardware and network in place but limited data synchronization.

Features:

- Some infrastructure pre-installed
- Data replicated periodically (e.g., daily)
- Requires some configuration before going live

3. Cold Site

Definition: An empty facility with basic power, cooling, and networking but no pre-installed hardware or live data.

Features:

- Only physical space is prepared
- Equipment and data must be brought in after the disaster

22510064 Parshwa Herwade

Real World Case Study

AWS S3 Outage (2017)

In February 2017, a human error during a routine debugging operation resulted in the unintentional removal of critical capacity from AWS S3 in the US-EAST-1 region.

A debugging command aimed at a small subset of servers was mistakenly executed on a much broader set of S3 servers. This error caused a significant disruption, affecting hundreds of websites and services reliant on S3 for data storage and hosting.

Widespread service disruption affecting a multitude of web applications globally. Sparked urgent discussions on improving change management and adopting resilient, multi-region cloud architectures.

22510064 Parshwa Herwade

Real World Case Study

Capital One Breach (2019)

In July 2019, attackers exploited a misconfigured AWS S3 bucket and a vulnerable web application firewall. This misconfiguration allowed unauthorized access to sensitive customer data.

The breach resulted in the exposure of personal information (names, addresses, credit scores, and in some cases, Social Security numbers) for over 100 million customers.

Massive data breach impacting millions of users. Created widespread industry awareness about the need for stringent cloud configuration audits.

22510112 Harshavardhan Bamane

Best Practices & Emerging Technologies in HA/DR

Best Practices

- Regular disaster recovery drills – Simulate real outages to identify gaps before an actual failure happens.
- Continuous monitoring & alerting – Detect issues instantly to minimize downtime.
- Multi-region deployment – Avoid single points of failure by distributing workloads across regions.
- Automated failover & recovery – Reduce human intervention time and prevent mistakes during emergencies.

Emerging Technologies

- Cloud-native disaster recovery – Elastic scaling and built-in redundancy from cloud providers.
- AI-driven outage prediction – Machine learning models that predict failures before they occur.
- Edge computing for fast failover – Keep services running locally even if the central system is down.

22510112 Harshavardhan Bamane

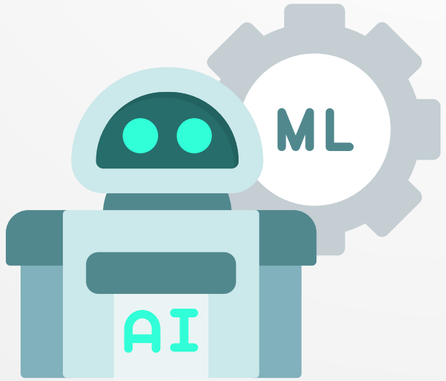
Future Trends & Conclusion

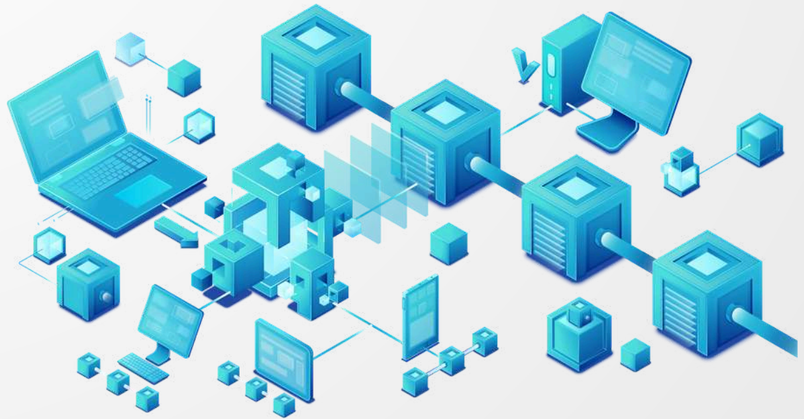
Future Trends

- AI/ML-powered automated recovery – Systems that detect and fix failures without manual action.
- Blockchain-based backups – Tamper-proof, verifiable storage for critical data.
- Global active-active architectures – Systems running in multiple regions simultaneously for zero downtime.

Conclusion

- Why it matters: High Availability (HA) and Disaster Recovery (DR) ensure business continuity.
- Key action: Plan well, implement effectively, and test regularly.
- Final thought: "Failure is inevitable — downtime doesn’t have to be."





THANK YOU