Backup and Disaster Recovery

Overview
AutoSync Cloud Service implements a robust backup and disaster recovery strategy to ensure data durability and business continuity in case of hardware failure, service disruptions, or other disasters. This page outlines our backup strategy, disaster recovery procedures, and the tools used to ensure minimal downtime and data loss.

3.1 Backup Strategy

- **Automated Backups**: Daily backups are taken for both the application data (e.g., synchronization logs, user data) and configurations.
  - **Database Backups**: Full database backups are taken daily using **AWS RDS automated backups** or **MongoDB Atlas** backup features. Incremental backups are taken every 6 hours for faster recovery.
  - **File Storage Backups**: User files and documents are backed up to **AWS S3**, with cross-region replication enabled to ensure data durability in case of regional failures.
  - **Backup Retention**: Backups are retained for 30 days, ensuring that data from any point within the last month can be restored if needed.

3.2 Disaster Recovery Plan

- **Disaster Recovery Testing**: Regular disaster recovery drills are conducted to ensure that the team can restore services within the defined RTO (Recovery Time Objective) and RPO (Recovery Point Objective).
  - **RTO**: The target recovery time is 1 hour for all critical services.
  - **RPO**: The target recovery point is 30 minutes, meaning no more than 30 minutes of data will be lost in the event of a disaster.
- **Hot and Cold Standby**:
  - **Hot Standby**: Active-passive clustering is used for critical services, ensuring that in the event of a failure, traffic is immediately redirected to backup instances.
  - **Cold Standby**: In certain cases, secondary systems are kept in a standby mode, ready to be deployed during a disaster.

3.3 Backup Storage and Recovery

- **Cross-Region Replication**: Backup data is stored in geographically dispersed regions to protect against regional failures.
- **Recovery from Backups**: Backups are restored in the event of data corruption, accidental deletion, or system failure using automated scripts to ensure quick recovery with minimal manual intervention.
- **Manual Recovery**: In the case of a catastrophic failure, the engineering team can manually restore backups from cloud storage (S3, GCS) or external storage devices.