Disaster Recovery Plan for Cloud-Based Infrastructure on OpenStack

Designing a Disaster Recovery (DR) plan for OpenStack requires ensuring resilience against data loss, system failure, and service disruption. The plan must incorporate redundancy, backup mechanisms, and a tested recovery procedure. Following ISO/IEC 27031 guidelines, the DR lifecycle includes risk analysis, preparedness, testing, and continual improvement (ISO, 2011).

Implementation and Tools
OpenStack provides flexibility through modular services (Nova, Neutron, Cinder) that can be replicated across availability zones. To safeguard critical workloads, I implemented scheduled backups using *Duplicity*, an open-source tool supporting encrypted incremental backups to remote storage (Mann & Velickovic, 2018). Backup jobs were configured for daily snapshots of Cinder volumes and Keystone databases, stored in Swift object storage.

A simulated failure scenario was created by deliberately corrupting the primary database instance. Recovery involved deploying a clean database node and restoring from the most recent Duplicity snapshot. The encrypted backups ensured data integrity and compliance with confidentiality standards (Zhou et al., 2013).

Professional Reflection
From my professional experience in IT service environments, I have seen how overlooked DR testing can cause extended downtime. For instance, during a project deploying cloud-based laundry process management systems, a minor database fault led to several hours of service unavailability because backups had not been recently validated. This highlighted that DR is not only about *having* backups but also about *proving* they work. In this simulation, recovery succeeded within the two-hour Recovery Time Objective (RTO), directly contrasting with that earlier incident where delays arose due to insufficient verification.

While effective, the process revealed limitations: Duplicity struggled with larger datasets, suggesting Bacula's enterprise scalability could be better suited (Mann & Velickovic, 2018). Bandwidth also slowed restoration, pointing to the value of deduplication and network planning. Future improvements include automating failover with Ansible and extending geo-replication to reduce single-point risks.

References
ISO (2011) *ISO/IEC 27031:2011 – Information technology – Security techniques – Guidelines for ICT readiness for business continuity*. Geneva: International Organization for Standardization.
Mann, Z. Á. and Velickovic, D. (2018) 'Evaluation of backup solutions for cloud computing', *Future Generation Computer Systems*, 83, pp. 85–96.
Zhou, M., Zhang, R., Xie, W., Qian, W. and Zhou, A. (2013) 'Security and privacy in cloud computing: A survey', *IEEE International Conference on Semantics Knowledge and Grid*, pp. 105–112.