Unit 8 – Formative Activity

This post presents an analysis of a recent disaster recovery (DR) exercise conducted in a lab environment. In this case, Duplicity, an open-source tool, was utilised to perform a full backup and restore of an OpenStack deployment (Li, Chen and Deng, 2020). While successful, this exercise serves as a crucial point of reflection on the stark contrast between a basic, dirty, lab-based approach and the sophisticated methodologies employed in a professional enterprise setting.

The DR Process and Tools

The DR process was executed in a series of deliberate steps. The initial and most critical action involved ensuring data consistency by halting the Microstack services with the command `sudo snap stop microstack`. This manual intervention was essential to prevent data corruption during the backup procedure. The core of the activity was the Duplicity tool, which performed a full backup of the `/var/snap/microstack/common/` directory, where all crucial files for the Microstack environment are stored, to a local file path. As per the attached log file, the process successfully backed up 3.34 GB of data in under 150 seconds, with all files secured using a GnuPG passphrase to encript the backup. Next, the previously mentioned folder was manualy deleted. After this step a full restore was performed with the command `sudo duplicity restore` before the Microstack services where restarted.

Analysis and Reflection

This exercise effectively demonstrated the fundamental principles of data backup and recovery. Duplicity's command-line interface and use of GnuPG encryption provide a robust, straightforward method for ensuring data integrity and confidentiality. However, the manual nature of this process, particularly the requirement to stop services, highlights its unsuitability for an enterprise environment. In a professional context, downtime is an unacceptable consequence.

Enterprise-grade DR strategies are designed around stringent Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO) (Akula, 2025). These solutions, such as those from Trilio or Hystax, operate on principles of continuous, non-disruptive, and automated replication. Unlike the manual process, these tools provide cloud-native, single-click recovery of entire workloads to a secondary, often geographically separate, site (Morrison, 2023). They are not merely tools for data transfer; they are comprehensive platforms that ensure business continuity. The manual process used here, while instructive, lacks the automation, scalability, and high-availability features required for a robust enterprise solution. It serves as a formative lesson, underscoring the shift from isolated tasks to integrated, automated systems that prioritise resilience and continuous operation.

Word count: 395

References:

Akula, N. (2025) ‘Optimizing Regional Disaster Recovery in OpenShift: A Multi-Cluster Approach with RHACM and ODF’, *International Journal of Computational Mathematical Ideas*, 17(01). Available at: https://doi.org/10.70153/ijcmi/2025.17101

Li, Z., Chen, G.G. and Deng, Y. (2020) ‘Duplicacy: A New Generation of Cloud Backup Tool Based on Lock-Free Deduplication’, *IEEE Transactions on Cloud Computing*, pp. 1–1. Available at: https://doi.org/10.1109/tcc.2020.3047403

Morrison, R. (2023) *OpenStack Backup and Recovery: Cinder, Nova and Swift*, *Bacula Systems*. Available at: https://www.baculasystems.com/blog/openstack-backup-and-recovery-best-practices/ (Accessed: 22 September 2025)