Disaster Recovery Services

for

SynrgiseLearn

Software as a Service Solutions

PREPARED BY: SynrgiseLearn (Pty) Ltd

VERSION: 2024

TABLE OF CONTENTS

1. Overview

Disaster Recovery (DR) is a critical aspect of maintaining Synrgise's Software as a Service (SaaS) solutions, ensuring continuity and minimal downtime in the event of unforeseen catastrophic failures. This document outlines the DR strategy for Synrgise's SaaS infrastructure, which leverages Dockerized services, multi-region backups, and co-located database servers to provide seamless recovery and failover.

Synrgise has migrated from Azure to a hybrid infrastructure hosted on Xneelo, with additional co-location at Vultr's Johannesburg datacenter for database redundancy. The entire stack is containerized using Docker, enabling rapid service recovery in under four hours. Synrgise also employs both onsite and offsite backup strategies, ensuring robust data availability across multiple disaster scenarios.

2. Disaster Recovery Objectives

2.1. Recovery Time Objective (RTO)

The **Recovery Time Objective (RTO)** refers to the maximum allowable time it takes to restore the services after a disruption before it starts to impact the business operations. In other words, it's the duration of downtime that the organization can tolerate.

Synrgise's RTO:

The RTO for Synrgise SaaS Solutions is set at **four hours**. This means that in the event of any service failure—whether it's related to the application, hardware, network, or an entire datacenter—services must be restored or functional alternatives must be provided within four hours of the incident.

Components Contributing to RTO:

- **Dockerized Infrastructure:** All critical application services are containerized, allowing the team to redeploy instances rapidly. Docker images are ready for deployment both at the primary site (Xneelo) and the backup site (Vultr Johannesburg). Automated orchestration scripts minimize the time required to spin up new instances.
- **Automated Failover:** Pre-configured failover between Xneelo and Vultr ensures that services can automatically switch locations in the event of a failure at Xneelo. This contributes significantly to achieving the four-hour RTO.
- **Database Redundancy:** Databases are continuously synchronized between Xneelo and Vultr. This ensures that the failover database is always up-to-date and can be switched to without manual intervention, further reducing recovery time.

Achieving RTO:

- **Monitoring and Alerts:** Monitoring tools such as New Relic, Grafana, or similar solutions are used to provide real-time visibility into system performance. These tools send automated alerts to the technical team in the event of performance degradation or failures. This ensures that issues are identified immediately, reducing the time spent diagnosing the problem.
- **Disaster Simulation and Testing:** Regular disaster recovery drills are conducted to ensure that recovery procedures are streamlined and the technical team can respond quickly. Tests are performed quarterly, and response times are evaluated to ensure compliance with the four-hour RTO.
- **Pre-Configured Backup Site:** The backup site at Vultr Johannesburg is pre-configured with all necessary software, tools, and environment settings to support the immediate redeployment of services. Automated deployment scripts ensure that applications are launched in their most current state.

2.2. Recovery Point Objective (RPO)

The **Recovery Point Objective (RPO)** refers to the maximum acceptable age of data that can be recovered in the event of a failure. It defines how much data the business is willing to lose as a result of the disaster, often measured in time from the last backup or replication point.

Synrgise's RPO:

The RPO for Synrgise SaaS Solutions is set at **24 hours or less**. This means that, in the event of a catastrophic failure, the maximum amount of data that could be lost would be limited to the last 24 hours of data changes.

Components Contributing to RPO:

- **Database Backup Frequency:** Databases are backed up daily at both the Xneelo and Vultr datacenters. Daily snapshots ensure that even in the worst-case scenario, data loss is limited to changes that occurred in the last 24 hours. The redundancy between onsite and offsite backups ensures that the most recent data can be restored regardless of the failure scenario.
- **Database Replication:** In addition to daily backups, database transactions are continuously replicated between Xneelo and Vultr. This enables near-real-time failover of the database with minimal data loss.
- **Versioning and Retention Policies:** Database backups follow a retention policy that includes daily, weekly, and monthly snapshots stored across multiple locations. In the event of data corruption, the technical team can roll back to the most recent snapshot to minimize data loss.

Achieving RPO:

- **Automated Backup Procedures:** Synrgise uses automated backup tools to create, store, and manage backups across the primary (Xneelo) and secondary (Vultr) locations. Backups are scheduled to run without manual intervention, ensuring consistency.
- **Data Validation and Testing:** Backups are regularly tested for integrity and recoverability. Automated scripts verify the integrity of backup files to ensure they are free from corruption. Periodic recovery tests are conducted to validate the accuracy and completeness of the backups.
- **Offsite Backup Storage:** Offsite backups are an integral part of the disaster recovery strategy, ensuring that even if both Xneelo and Vultr experience failures, the data remains intact. These backups are stored in geographically separate locations to further reduce the risk of complete data loss.

2.3. Service-Level Agreement (SLA) Alignment

The RTO and RPO objectives align with the service-level agreements (SLAs) Synrgise offers to its clients. Synrgise commits to the following service recovery guarantees:

- **RTO of 4 hours:** Services will be restored within 4 hours of any major service disruption.
- **RPO of 24 hours:** In the event of a disaster, no more than 24 hours of data will be lost, with efforts made to minimize this to even shorter periods depending on the specific nature of the failure.

The above objectives are supported by detailed disaster recovery processes, failover systems, and continuous monitoring, ensuring that Synrgise SaaS Solutions remain resilient and capable of rapidly recovering from any disaster..

3. Hosting Environment

Synrgise's SaaS solutions leverage a hybrid hosting environment, primarily relying on **Xneelo** for hosting services, with **Vultr Johannesburg** serving as a secondary site for disaster recovery and database redundancy. Both hosting providers have robust disaster recovery and infrastructure support strategies that enhance the overall reliability and resilience of the Synrgise platform. Here's an in-depth overview of each provider's capabilities:

3.1. Xneelo (Primary Hosting Environment)

Xneelo provides comprehensive disaster recovery (DR) strategies and safeguarding measures across its data centers, which are pivotal for ensuring business continuity. The **Samrand Data Centre** in South Africa, which houses many of Xneelo's servers, is designed for high availability and redundancy.

- **Data Backups:** All managed servers hosted by Xneelo are automatically backed up daily in the early hours of the morning. This backup includes both the home directory and databases of the customer's servers, which are essential for disaster recovery. Customers can restore up to the previous two weeks of backup data through the Xneelo Control Panel. However, Xneelo recommends keeping local copies of critical data to avoid potential data loss during a disaster.
- **Physical Security:** The data center is equipped with 24/7 surveillance using over 55 strategically placed cameras, biometric access controls, and high-voltage security fences. These measures ensure that only authorized personnel have access to server racks and data storage areas.
- **Power and Fire Redundancy:** Xneelo maintains a robust fire prevention system using a Very Early Smoke Detection Apparatus (VESDA) to detect even the slightest traces of smoke. In the event of power outages, the data center is powered by an 11kV municipal feed, redundant UPS systems, and on-site backup generators with seven days of continuous fuel supply. This ensures uninterrupted power for all critical infrastructure.
- **Network and DDoS Protection:** The network infrastructure at Xneelo is highly resilient, utilizing multiple redundant uplinks from Tier 1 providers and peering partners. Their **DDoS mitigation system** ensures that malicious traffic is filtered without impacting legitimate users. Additionally, VLAN reverse path forwarding protection and advanced firewall rules are implemented at both the network edge and core for enhanced network security.
- **Monitoring and Management:** Xneelo's managed servers are monitored 24/7 for critical services and hardware health. Automated alerts and escalation protocols ensure that issues are addressed promptly to minimize downtime.

These disaster recovery strategies and physical security measures allow Synrgise to maintain high availability and data redundancy at the primary hosting site.

3.2. Vultr (Secondary Disaster Recovery Site)

Vultr is used as the secondary site to enhance redundancy and ensure that the Synrgise platform remains available even in the event of a complete failure at Xneelo. Vultr provides a range of disaster recovery features that make it an ideal backup environment:

- **Global Data Centers and Redundancy:** Vultr operates data centers globally, with the Johannesburg location being used for Synrgise's co-located database servers. This distributed infrastructure ensures that critical services and data are not confined to a single geographic region, reducing the risk of widespread outages.
- **Snapshot Backups:** Vultr offers automated snapshot backups, which capture the full state of servers. These snapshots can be taken at regular intervals (daily, weekly, or monthly), allowing the Synrgise team to quickly restore services with minimal data loss in the event of a disaster.
- **High Availability:** Vultr's platform includes built-in support for high availability (HA) and failover configurations. By using these features, Synrgise ensures that, in the event of failure at the primary Xneelo site, services and databases can be seamlessly transferred to Vultr with minimal downtime.
- **Low Latency and High-Speed Connectivity:** With high-speed, low-latency connections and scalable compute resources, Vultr ensures that the backup environment can scale quickly to handle full production loads if needed.

4. Disaster Scenarios and Response

4.1. Application Failure

Scenario:

An error in the application (code-level bugs, configuration errors, etc.) results in system downtime without hardware or operating system failure.

Mitigation Strategy:

- **Containerized Services:** All services are containerized with Docker. In the event of an application failure, new instances of the affected service can be spun up within the specified RTO. Docker images are stored and maintained to ensure consistent service replication across both Xneelo and Vultr.
- **Monitoring and Alerts:** Real-time monitoring and telemetry systems are in place to detect failure conditions and automatically notify administrators to take corrective action.
- **Manual Failover:** In cases where application errors are critical, a manual failover procedure is triggered to restore services from backup instances or new containers.

4.2. Data Corruption

Scenario:

Accidental deletion, modification, or corruption of the database or critical data components.

Mitigation Strategy:

- **Daily, Weekly, Monthly Backups:** Databases are backed up on a daily, weekly, and monthly basis. These backups are stored at both Xneelo and Vultr with rolling retention (30 days daily, 52 weeks weekly, and 24 months monthly).
- **Backup Validation:** Regular validation of backup integrity is performed, ensuring that corrupted backups are identified and discarded before they can be used for restoration.
- **Recovery Process:** Upon detection of data corruption, the system administrator can restore the latest uncorrupted backup within the four-hour RTO. Should more complex issues arise, data from Vultr (offsite) will be used for cross-validation and recovery.

4.3. Network Outage

Scenario:

Network connectivity loss at Xneelo or between primary and secondary sites (Vultr).

Mitigation Strategy:

- **Database Failover:** Synrgise uses a multi-location database failover strategy. In the event of network failure at Xneelo, Vultr's database server will take over as the primary database.
- **Traffic Redirection:** DNS records are dynamically updated to route user traffic to the backup infrastructure hosted at Vultr. Failover mechanisms are in place to ensure minimal service disruption during DNS propagation.
- **Onsite and Offsite Backups:** Daily offsite backups ensure that, even in prolonged network outages, data and services can be recovered from Vultr or other third-party providers.

4.4. Region-Wide Service Disruption

Scenario:

A critical disruption affecting Xneelo's entire datacenter, rendering services completely unavailable.

Mitigation Strategy:

- **Co-Located Services:** Critical components such as databases and backup services are co-located at Vultr's Johannesburg datacenter. Should Xneelo experience a region-wide outage, failover to Vultr's environment is automatically triggered.
- **Automated Docker Deployments:** New instances of Dockerized services will be spun up at Vultr within the RTO window.
- **Geo-Redundant Backup Replication:** All data is replicated between Xneelo and Vultr to ensure no data loss during a region-wide failure.

4.5. Widespread Service Disruption (Xneelo and Vultr)

Scenario:

In the event that both Xneelo and Vultr experience outages simultaneously.

Mitigation Strategy:

- **Offsite Backups:** Offsite backups (on a separate physical location) are regularly stored to ensure data remains available even in widespread regional failures. These backups can be restored in a third-party environment to quickly spin up services.
- **Third-Party Data Centers:** Agreements with other cloud providers (e.g., AWS, Google Cloud) can be triggered, enabling the rapid deployment of services to an alternate hosting environment should both Xneelo and Vultr experience downtime.

5. Data Backup and Recovery Strategies

5.1. Database Backups

Synrgise ensures data continuity through a structured backup policy that involves:

- **Daily Backups:** A rolling 30-day retention policy for daily backups.
- **Weekly Backups:** A rolling 52-week retention policy for weekly backups.
- **Monthly Backups:** A rolling 24-month retention policy for monthly backups.

Each backup is stored both onsite at Xneelo and offsite at Vultr Johannesburg. The use of two geographically separate locations ensures high availability and redundancy.

Backup Storage:

- **Onsite:** Xneelo datacenter.
- **Offsite:** Vultr Johannesburg and encrypted remote storage for additional redundancy.

5.2. Reference Data Recovery

Reference data such as images, videos, and static assets (CSS, JavaScript) is stored in both Xneelo and Vultr environments. Due to the infrequent changes in reference data, these assets are pre-deployed in all failover environments, reducing RTO.

6. Failover and Recovery Procedures

6.1. Failover Architecture

Synrgise employs a failover architecture that ensures minimal disruption during hardware or service outages:

- **Primary:** Xneelo hosts the primary instance of all services.
- **Secondary:** Vultr Johannesburg serves as the failover location for both database services and Dockerized applications.
- **Automated Failover:** Failover between Xneelo and Vultr is handled via automated scripts that initiate DNS redirection and launch of Docker instances.

6.2. Manual Failover Procedures

If automated failover mechanisms fail, administrators will follow a manual failover procedure. This involves:

1. **Service Validation:** Verifying the current health of services at Xneelo.
2. **Backup Verification:** Ensuring that the latest available backup (onsite or offsite) is intact and available.
3. **Service Deployment:** Using Dockerized images to manually launch services at Vultr.
4. **DNS Propagation:** Manually updating DNS records to redirect traffic to the new environment.

7. Testing and Review

A robust disaster recovery (DR) strategy is not only about the systems and processes put in place but also about the regular testing and review of these systems to ensure they perform as expected during a disaster. Testing and reviewing are critical components of Synrgise's DR plan. These activities ensure that the team is prepared to handle various failure scenarios effectively and minimize downtime. Synrgise follows a rigorous testing schedule and continuous review processes to ensure that all disaster recovery mechanisms remain up-to-date and reliable.

7.1. Quarterly Failover Tests

Failover testing ensures that Synrgise's infrastructure can automatically switch over to the secondary site (Vultr) without manual intervention in the event of a failure at Xneelo.

Test Scope:

- **Simulated Xneelo Downtime:** During these tests, Xneelo services are intentionally taken offline, and automated failover to Vultr is triggered. The objective is to confirm that the platform can switch traffic, spin up Dockerized containers, and restore databases from replication backups with no more than the agreed-upon **four-hour RTO**.
- **Full Environment Check:** The test includes validating the entire application stack at Vultr, including database integrity, service accessibility, and DNS updates.

Expected Outcomes:

- **Successful Traffic Redirection:** DNS traffic is successfully redirected to the Vultr environment, and services are brought online without intervention.
- **Service Availability Check:** All services are functional and responsive at the secondary site, matching production performance expectations.
- **Post-Test Review:** After failover tests, any issues or unexpected delays are analyzed, documented, and addressed to ensure smoother future failovers.

7.2. Backup and Restoration Testing

Regularly testing backups is critical to ensuring data integrity and compliance with the 24-hour RPO. The following processes are undertaken to ensure the effectiveness of backup and restoration:

Frequency of Backup Tests:

- **Quarterly Full Backup Restorations:** Synrgise performs full restoration tests of the daily, weekly, and monthly backups at least once per quarter. This involves restoring a complete backup to a separate environment to verify its integrity and correctness.
- **Incremental Backup Tests:** In addition to full backups, incremental backups are restored periodically to verify that individual point-in-time recovery (PITR) processes work effectively.

Key Test Areas:

- **Backup Integrity Validation:** Tests confirm that no data corruption exists in the backup files and that all necessary data has been captured.
- **Time to Restore:** The time taken to restore backups is monitored closely, ensuring that the restoration process is swift and efficient.
- **Cross-Region Backup Tests:** Backups stored offsite (at Vultr) are restored to validate the effectiveness of both local and remote recovery strategies.

Review and Improvements:

Post-restoration, the DR team reviews the results to:

- Assess any delays or challenges encountered during restoration.
- Implement enhancements to ensure faster recovery times, if needed.

7.3. Disaster Simulation Exercises

Disaster simulation exercises mimic real-world disaster scenarios to test how well the DR plan handles specific events. These simulations include:

- **Application and Database Failures:** Simulating specific application crashes or database corruption events to verify the recovery procedures for these components.
- **Power and Network Outages:** Simulating a complete power or network outage at Xneelo and testing how quickly services can be restored at Vultr.

Exercise Objectives:

- Validate the disaster recovery process.
- Measure team readiness to respond to unexpected disasters.
- Ensure that both manual and automated failover processes function correctly.

These exercises are conducted at least annually, but additional ad-hoc simulations may occur if there are significant infrastructure changes or after a real incident has been handled.

7.4. Review of Backup Retention Policies

Regular review of the backup retention policies ensures that Synrgise is adhering to both business and compliance requirements regarding data storage. The policies include:

- **Rolling Retention Strategy:** Backup retention policies (30 days for daily backups, 52 weeks for weekly backups, and 24 months for monthly backups) are reviewed annually to ensure they meet business needs.
- **Data Compliance:** Regular reviews ensure that Synrgise is compliant with any local or international regulations related to data storage and privacy, such as GDPR or POPIA.

7.5. Annual DR Plan Review

In addition to the technical testing of infrastructure and backup processes, an annual review of the overall DR plan is conducted. This review is aimed at:

- **Updating Processes:** As technology evolves, so do the components of the DR plan. The annual review includes updating any procedures related to failover, backup, and infrastructure changes.
- **Addressing New Risks:** Any new potential risks, such as emerging cybersecurity threats or changes in the regulatory environment, are incorporated into the disaster recovery strategy.
- **Incorporating Stakeholder Feedback:** Stakeholder feedback, particularly from any actual disaster recovery events, is used to improve the plan and ensure that it is as effective as possible.

7.6. Documentation and Reporting

Each test and simulation is followed by detailed documentation and reports. This documentation serves multiple purposes:

- **Test Results:** Provides a log of whether the test succeeded or encountered issues.
- **Recommendations for Improvements:** Captures any challenges or delays and suggests changes to improve processes.
- **Audits:** These documents can also be used for audits to show that regular testing and reviews are taking place.

7.7. Continuous Improvement

Disaster recovery is an evolving field, and Synrgise's DR team is committed to ongoing improvements. Following each testing cycle, post-mortem analysis is conducted to:

- Identify inefficiencies.
- Implement new best practices or tools.
- Stay up-to-date with the latest disaster recovery technologies and methodologies to ensure optimal performance.

This testing and review strategy ensures that Synrgise is fully prepared for a wide range of potential disaster scenarios, maintaining a high level of system resilience and readiness to minimize downtime and data loss.