Macrocomm Fleet Analytics

Disaster Recovery and Business Continuity Plan

Table of Contents

1. Introduction:

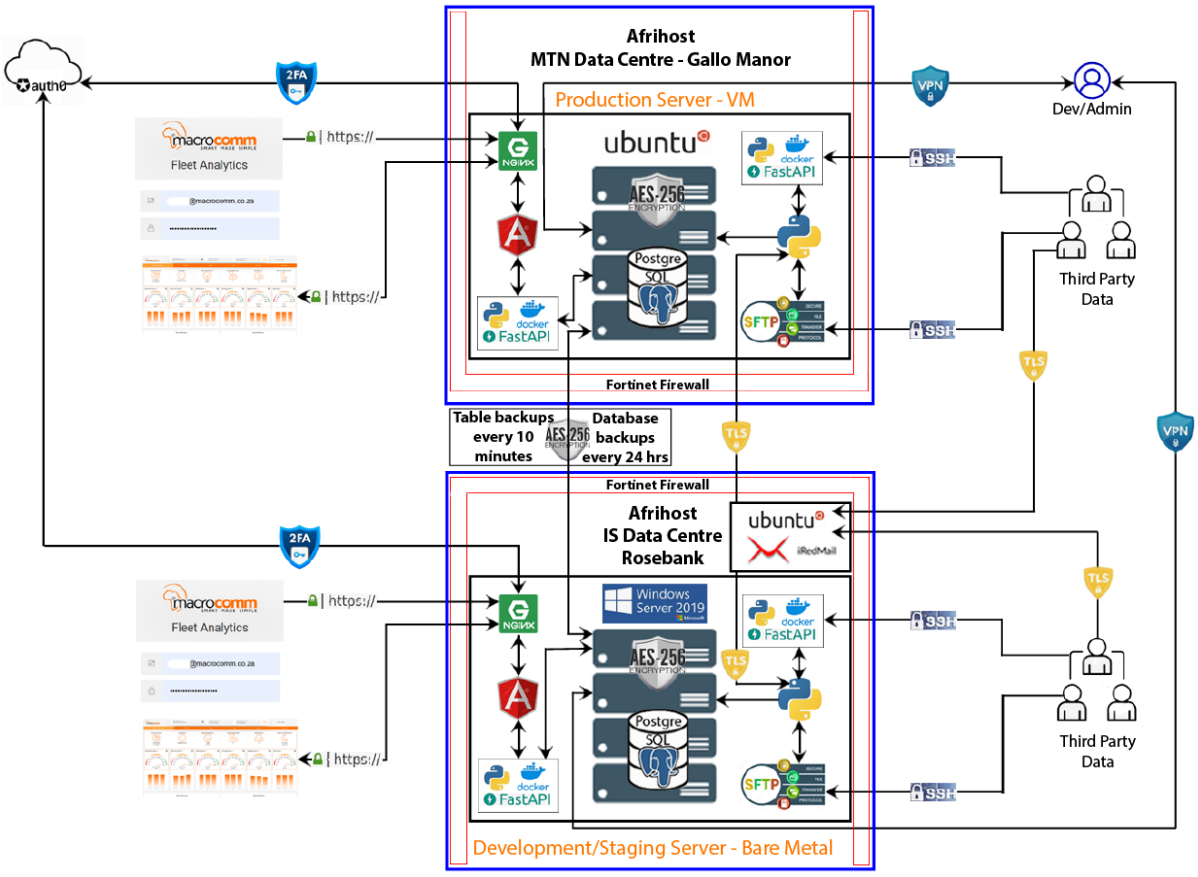
MFA operates a SaaS-based fleet analytics system that serves to assist commercial fleet owners in the day-to-day optimisation of their fleet operations. Trip data, driver behaviour data and cost data are ingested from multiple sources, via multiple means, for processing and analysis, delivering actionable insights around fleet optimisation.

Considering the sensitivity of the data, legislation governing the flow and storage of data and the reliance of MFA clients on the business-critical insights revealed by the analytics SaaS, this Disaster Recovery Plan (DRP) outlines the necessary procedures and protocols to be followed in the event of a disaster affecting the Macrocomm Fleet Analytics (MFA) fleet management system. It ensures minimal downtime, data integrity, and business continuity.

Unless otherwise indicated/detailed, Dev Ops is appointed Single Point of Contact (SPOC) and communications procedures are as stipulated in section 11. Communication Plan.

2. System Overview:

The system architecture diagram below serves to depict the tech stack, data flows, methodologies employed to secure data in transit and data at rest, and systems/services employed to mitigate risks associated with data security as well as failovers to mitigate system failures.



- The three servers are housed within data centres, gaining advantage from 99.9% uptime SLAs with the data centre providers.
- The Production Server stands alone from the Development & Staging Server and Mail Server.
- The Production Server is a VM, benefiting from non-disruptive scalability of processing power, RAM and disk storage.
- The Staging Server - housed in a geographically separated data centre - mirrors the Production Server as a failover in the event of a catastrophic failure at Production Server level.
- Source/third party data is ingested via API calls, push to SFTP or delivery of CSV or XLSX files as email attachments to bespoke mailboxes, per client, on the Mail Server.
- Data in transit is over SSH secured connections, and in the event of email transfer, TLS 2 encrypted.
- Data at rest is AES-256 encrypted.
- Database tables are backed up, incrementally, from the Production Server to the Staging Server every 10 minutes.
- The entire database is backed up from the Production Server to the Staging Server every 24 hours.
- Developer/Admin access to all servers is via VPN, with Role-Based Access Control (RBAC) strictly enforced to ensure least privilege access.

- Ingested data is normalised via Python scripts and processed by a combination of Python scripts and Postgre SQL stored procedures.
- Client access to processed/aggregated data is delivered over the internet by the Production Server, housing its own web server in the form of Nginx, via Angular making secure API calls to the Production Server through a Docker containerised FastAPI layer.
- Inbound client connections are Multi Factor Authentication controlled via the Auth0 cloud service.
- Inbound connections to all servers pass through a Fortinet Firewall.

3. Disaster Recovery (DR) Personnel Organigram:

<table>
<tr><td colspan="3">Data Security Officer (DSO)</td></tr>
<tr><td>Head Developer</td><td>Database Administrator</td><td>Server Administrator</td></tr>
<tr><td colspan="2">Dev Ops</td><td>Client Liaison Officer (CLO)</td></tr>
</table>

4. Risk Assessment:

- Server failure – bare metal (storage, NIC, RAM, processor, motherboard, automatic update to OS).
- Software failure (database corruption, patch/upgrade failure).
- Cybersecurity threats (ransomware, DDoS attacks, unauthorised access, data breach).
- Data centre disruptions (fire, flooding, power outages).
- Human error (accidental deletion, misconfigurations).

5. Disaster Recovery Objectives:

- RTO (Recovery Time Objective): Maximum allowable downtime is 4 hours.
- RPO (Recovery Point Objective): Maximum allowable data loss is 10 minutes.

6. Backup Strategy:

- Database tables are incrementally backed up from the Production Server to the Staging Server every 10 minutes.
- Full database backups from the Production Server to the Staging Server are executed, after 00:00, every 24 hours.
- The Staging Server database tables are updated from the 10-minute incremental backups to effect a full failover environment in the event of a catastrophic Production Server failure. Live synching too risky in terms of SQL compromise or ransomware.

- A manual A-pointer change will be implemented to redirect inbound client traffic, once it is established that such a re-direct will not compromise the failover server – maximum 1 hour.
- A full-tin backup image of the Staging Server is made to a Multi Factor Authentication protected location on the Production Server, after 03:00, every 24 hours, to facilitate a rebuild of a new bare metal Staging Server in the event of a catastrophic Staging Server failure – maximum 4 hours.
- Automated daily reports, via email and Telegram, to Dev Ops confirming the daily backups have run successfully and detailing the creation timestamp and size of backup files, along with remaining storage space on the servers.
- Any failure in the backup routines to be thoroughly investigated by Dev Ops, rectified, as well as documented, using the Server Exception report template, detailing the failure and remedy and distributed via email to all members of the DR team.
- Backup files are archived for 5 years.

7. Disaster Recovery Procedures:

7.1 Hardware Failure – Bare Metal

- Dev Ops to immediately inform all members of the DR team of the failure and enlist all available DR team members, as well as data centre support agents, to identify the nature of the failure.
- Dev Ops to immediately open a DR Exception report and record the date and time of the occurrence.
- Dev Ops to identify the nature of the failure and engage the specialist member/s of the DR team, commensurate with the nature of the failure, who will run lead during the implementation of the remedy.
- Dev Ops to appoint a Single Point of Contact (SPOC) from the DR specialist team.
- SPOC to determine/estimate the timespan for remedial action and communicate the cause and remedy to the rest of the DR team.
- Re-direct incremental database tables to a suitable local machine controlled/owned by one of the DR team.
- CLO to inform impacted staging clients, via email, if services cannot be restored within 5 minutes.
- CLO to inform impacted staging clients, via email, of anticipated downtime.
- SPOC to, if necessary, engage the data centre to spin up a new server, restoring the latest full-tin backup as soon as the new server goes live.
- SPOC to manually synch the databases once the new server has been fully restored.
- Appointed lead DR team member to manually run any automated backups that were missed while the old server was down.
- CLO to inform impacted staging clients, via email, that services are restored.
- SPOC to complete the Server Exception Report, accurately detailing the cause of failure, the remedial action taken, as well as the course of action to be implemented prevent such a failure from reoccurring.

- SPOC to submit the Server Exception report to the DSO.
- DSO to document and implement any change controls that may arise from the failure as well as update the DR plan, in accordance with ISO guidelines surrounding change control and policy document updates.

7.2 Hardware Failure – Virtual Machine

- Dev Ops to immediately inform all members of the DR team of the failure and enlist all available DR team members, as well as data centre support agents, to identify the nature of the failure.
- Dev Ops to immediately open a DR Exception report and record the date and time of the occurrence.
- Dev Ops to identify the nature of the failure and engage the specialist member/s of the DR team, commensurate with the nature of the failure, who will run lead during the implementation of the remedy.
- Dev Ops to appoint a Single Point of Contact (SPOC) from the DR specialist team.
- SPOC to determine/estimate the timespan for remedial action and communicate the cause and remedy to the rest of the DR team.
- Re-direct incremental database tables to a suitable local machine controlled/owned by one of the DR team.
- CLO to inform impacted clients, via email, if services cannot be restored within 5 minutes.
- CLO to inform impacted staging clients, via email, of anticipated downtime.
- SPOC to, if necessary, engage the data centre to spin up a new server, restoring the latest full-tin backup as soon as the new server goes live.
- If the entire data centre is down, SPOC to engage an alternate data centre – listed on https://www.datacentermap.com/south-africa/johannesburg/ - to spin up a VM of identical or higher specification and restore the latest full-tin backup as soon as the new server goes live.
- SPOC to manually synch the databases once the new server has been fully restored.
- SPOC to manually set the A pointer of the domain to the new server IP address and set the TTL to 300 seconds on https://www.domains.co.za/client/services/domains/manage-dns/103506.
- SPOC to manually run any automated backups that were missed while the old server was down.
- CLO to inform impacted staging clients, via email, that services are restored.
- SPOC to complete the DR Exception report, accurately detailing the cause of failure, the remedial action taken, as well as the course of action to be implemented prevent such a failure from reoccurring.
- SPOC to submit the DR Exception report to the DSO.
- DSO to document and implement any change controls that may arise from the failure as well as update the DR plan, in accordance with ISO guidelines surrounding change control and policy document updates.

7.3 Software Failure

- Dev Ops to immediately inform all members of the DR team of the failure and enlist all available DR team members to identify the nature of the failure.
- Dev Ops to immediately open a DR Exception report and record the date and time of the occurrence.
- Dev Ops to identify the nature of the failure and engage the specialist member/s of the DR team, commensurate with the nature of the failure, who will run lead during the implementation of the remedy.
- Dev Ops to appoint a Single Point of Contact (SPOC) from the DR specialist team.
- SPOC to determine/estimate the timespan for remedial action and communicate the cause and remedy to the rest of the DR team.
- CLO to inform impacted clients, via email, if services cannot be restored within 5 minutes of the estimated downtime.
- SPOC to complete the DR Exception report, detailing the cause and remedy as well as total downtime and implementations to prevent recurrence.
- Appointed lead DR team member to submit the DR Exception report to the DSO.
- DSO to document and implement any change controls that may arise from the failure as well as update the DR plan, in accordance with ISO guidelines surrounding change control and policy document updates.

7.4 Kubernetes Failure

Recovery Scenarios & Tailored Actions

- Node Failure
- Trigger: Physical host crash, Ubuntu node OS corruption
- Actions:
    - Provision a new Ubuntu VM via MTN Gallo Manor.
    - Install Kubernetes and join the node using:

```bash
kubeadm join <control-plane>:6443 --token <token> ...
```

    Kubernetes reschedules pods automatically.
- Verify:

```bash
kubectl get nodes -o wide
```

    Make sure PVs are backed by non-node-specific storage (e.g., NFS, CSI).

Frontend Failure (Angular + Nginx)

- Symptoms: Angular app inaccessible, Nginx misroutes.
- Actions:
- Redeploy Angular container from GitLab CI pipeline or Helm chart.
- Restore or redeploy Nginx ingress config:

```bash
kubectl apply -f ingress.yaml
```

- Test:

```bash
curl -I https://yourdomain.com
```

etcd or Control Plane Failure

- Symptoms: kubectl fails; cluster completely non-functional.
- Actions:
- SSH to control plane node, stop kubelet.
- Restore etcd from recent snapshot:

```bash
ETCDCTL_API=3 etcdctl snapshot restore snapshot.db \
  --data-dir /var/lib/etcd-restored
```

- Point kube-apiserver to the restored data directory.
- Restart control plane services:

```bash
systemctl restart kubelet
```

Namespace or Microservice Deletion

- Trigger: Accidental kubectl delete ns prod-backend
- Actions:
    - Redeploy via GitOps/Helm:

```bash
helm upgrade --install backend ./charts/backend -n prod
```

- Restore PVs using Velero:

```bash
velero restore create --from-backup backend-prod-backup
```

Cluster-Wide Failure (Disaster)

- Trigger: Data center outage, all VMs lost.
- Actions:
- Provision new VMs at MTN or cloud (use Ansible or Terraform).
- Rebuild Kubernetes with kubeadm init.
- Restore etcd (if available).
- Redeploy manifests from Git/Helm:

```bash
kubectl apply -f cluster-state/
```

- Restore volumes with Velero:

```bash
velero install
velero restore ...
```

- Practice full disaster recovery once per quarter in a test environment.

8. Cybersecurity Threats

8.1 Ransomware Attack Response Plan (Hosted Servers)

Immediate Detection and Containment

- Goal: Stop the spread, isolate affected systems, preserve evidence.
- Identify signs: Unusual CPU/disk usage, encrypted files, ransom notes, blocked access.
- Disconnect affected server(s) from the network immediately:
- Disable NIC (network interface card).
- Remove from load balancers or virtual networks.
- Disable shared drives/storage mounted from the infected server.
- Block external communications (firewall rules, outbound traffic) to prevent data exfiltration or C2 (command-and-control) contact.
- ⚠️ Do not reboot or wipe the system yet — preserve evidence for forensic analysis.

Activate Incident Response Team

- Bring together all key personnel and resources.
- Notify internal incident response team (IR team).
- Escalate to executive management, legal, and PR teams as needed.
- Involve forensic analysts (DSO and Cyber Africa).
- Appoint a single point of contact (SPOC) for managing communications and updates.

Forensic Analysis & Impact Assessment

- Goal: Understand the scope and identify the entry point.
- Preserve a full image of the infected server for analysis.
- Review:
    - Access logs
    - System event logs (e.g., /var/log/auth.log, /var/log/syslog)
    - Recent process activity (ps aux, top, history)
    - Network traffic
- Determine:
    - Infection vector (phishing, RDP, unpatched vulnerability)

    - Files and data affected
    - Any data exfiltration or unauthorized access
- Record file hashes, timestamps, ransom note contents, and any attacker contact info.

Contain and Eliminate the Threat

- Goal: Remove the malware and any persistence mechanisms.
- Terminate malicious processes (kill, pkill, top).
- Identify and delete:
- Malicious binaries/scripts
- Unauthorized users or SSH keys
- Cron jobs or systemd timers used for persistence
- Patch all known vulnerabilities on all affected and adjacent systems.
- Rotate credentials:
    - System users
    - API keys
    - Database credentials
    - VPN and remote access accounts
- Reassess all servers in the hosted environment, even if only one appears affected.

Restore Operations from Backups

- Goal: Recover to a clean, known-good state.
- Do NOT restore over the infected server.
- Rebuild the server (format disk, reinstall OS and apps).
- Apply all security patches.
- Verify backup integrity and timestamps.
- Restore from offline or immutable backup (not mounted to the infected host).
- Scan restored data before putting back into production.
- Gradually reintroduce server to the network, under monitoring.
- If backups are encrypted or compromised, escalate to cyber insurance/legal.

Communication & Reporting

- Goal: Legal compliance, customer assurance, and team coordination.
- Notify affected clients (if PI, financial, or regulated data was exposed).
- Report the incident to:
    - State Security Agency for criminal investigation
    - South African Police Service (SAPS) for criminal investigation
    - Information Regulator as required by POPIA
- Prepare internal and external statements.
- Ensure clear communication with internal staff to avoid rumour spread.

Post-Incident Review & Hardening

- Goal: Learn and strengthen defences.
- Conduct a root cause analysis.

- Review and improve:
    - Patch management process
    - Access controls (SSH, VPN, admin rights)
    - User awareness and phishing training
    - Firewall and IDS/IPS rules

8.2 DDoS Attack Response & Mitigation Plan

Initial Triage

- Identify type:
    - Layer 3/4 (network) or Layer 7 (application)?
    - Small-scale botnet or volumetric?
- Determine source patterns:
- IPs, headers, countries, user-agents

Mitigation (During Attack)

- **Network/Infrastructure Level Mitigation**
- Engage upstream provider (e.g., MTN, Afrihost, Azure) to:
    - Block traffic at their edge
    - Apply upstream null-routing / sinkholing
- Enable:
    - "Under Attack Mode"
    - IP reputation filtering
    - Rate limiting rules

- **Server/Application-Level Mitigation**
- Temporarily enable aggressive rate limits and bot detection in Nginx/FastAPI:

```nginx
limit_conn addr 5;
limit_req_zone $binary_remote_addr zone=api:10m rate=1r/s;
```

- Use fail2ban to block IPs with malicious patterns.
- Disable endpoints or services being targeted.

- Drop malformed or suspicious packets using iptables:

```bash
iptables -A INPUT -p tcp --syn -m limit --limit 1/s -j ACCEPT
```

Divert/Scale Traffic

- Redirect traffic to cloud-based scrubbing centres.
- Spin up additional instances or containers in alternate zones to absorb traffic.

Post-Attack Recovery

- Assess and Restore
    - Review logs for origin and extent of attack
    - Re-enable temporarily disabled services
    - Monitor for residual or repeat attacks
    - Revert any temporary rate limits if performance is degraded

Report & Communicate

- Document the event:
    - Time of onset and resolution
    - Attack type and volume
    - Mitigation measures taken
- Notify clients if service was impacted (transparently).
- Report attack to upstream ISP and/or law enforcement if it involved criminal extortion.

9. Data Centre Disruptions

- Dev Ops to immediately inform all members of the DR team of the failure and enlist all available DR team members, as well as data centre support agents, to identify the nature of the failure.
- Dev Ops to immediately open a DR Exception report and record the date and time of the occurrence.
- Dev Ops to identify the nature of the failure and engage the specialist member/s of the DR team, commensurate with the nature of the failure, who will run lead during the implementation of the remedy.
- Dev Ops to appoint a Single Point of Contact (SPOC) from the DR specialist team.
- SPOC to determine/estimate the timespan for remedial action and communicate the cause and remedy to the rest of the DR team.
- If necessary:
    - Re-direct incremental database tables to a suitable local machine controlled/owned by one of the DR team.
    - CLO to inform impacted clients, via email, if services cannot be restored within 5 minutes.
    - CLO to inform impacted staging clients, via email, of anticipated downtime.
    - SPOC to, if necessary, engage the data centre to spin up a new server, restoring the latest full-tin backup as soon as the new server goes live.
    - If the entire data centre is down, SPOC to engage an alternate data centre – listed on https://www.datacentermap.com/south-africa/johannesburg/ - to spin up a VM of identical or higher specification and restore the latest full-tin backup as soon as the new server goes live.
    - SPOC to manually synch the databases once the new server has been fully restored.

    - SPOC to manually set the A pointer of the domain to the new server IP address and set the TTL to 300 seconds on https://www.domains.co.za/client/services/domains/manage-dns/103506.
    - SPOC to manually run any automated backups that were missed while the old server was down.
- CLO to inform impacted clients, via email, that services are restored.
- SPOC to complete the DR Exception report, accurately detailing the cause of failure, the remedial action taken, as well as the course of action to be implemented prevent such a failure from reoccurring.
- SPOC to submit the DR Exception report to the DSO.
- DSO to document and implement any change controls that may arise from the failure as well as update the DR plan, in accordance with ISO guidelines surrounding change control and policy document updates.

10. Human Error

- Restore data from backup immediately.
- Implement stricter access controls and logging mechanisms.
- Conduct additional training for personnel.

11. Communication Plan

- **Incident Reporting:** All incidents must be reported to the DSO by the SPOC.
- **Stakeholder Notification:** Via email and any additional communications means deemed necessary, SPOC to notify key stakeholders, including executive management and CLO to notify affected clients.
- **Exception Report:** This report must be opened ,by Dev Ops/SPOC, immediately any disruptive exception occurs, completed meticulously, signed and delivered via email to the DSO.
- **Regular Updates:** SPOC to provide DSO and stakeholders with progress reports every hour until resolution.
- **Change Control:** DSO to document and implement any change controls that may arise from exceptions as well as update the DR plan, in accordance with ISO guidelines surrounding change control and policy document updates.

12. Testing and Maintenance

- **Quarterly DR Drills:** Simulate disaster scenarios and validate response times.
- **Annual Full-System Restoration Test:** Ensure backups are functional and data integrity is maintained.
- **Ongoing Monitoring:** Implement automated alerts for potential system failures.

13. Conclusion

By following this DRP, MFA ensures business continuity, minimizes downtime, and protects critical fleet analytics data. Regular reviews and updates will be conducted to align with evolving risks and technology advancements.