



K-9 Packet Sniffer

Draft Disaster Recovery Plan

Disaster Recovery Team: Edward Medina, Tiago Muller, Sharek
Rendon, Carlos Imery, Maritza Medina

Table of Contents

Step 1: The Plan's Objective and Scope.....	3
Step 2: Risk Assessment	3
Step 3: Business Impact Analysis (BIA).....	4
Step 4: Recovery Measures and Procedures	5
Step 5: Testing and Training.....	7

This document serves as a draft Disaster Recovery Plan (DRP) for the packet sniffer software. While it provides a comprehensive framework for addressing potential risks and ensuring system continuity, certain sections are based on theoretical scenarios or planned features that the software does not currently include. As the software evolves, additional considerations, such as enhanced redundancy, advanced security protocols, or extended functionalities, may need to be integrated into the plan. This draft should therefore be treated as a foundational document that will require updates and refinements to align with the software's final design and operational environment.

Step 1: The Plan's Objective and Scope

The Disaster Recovery Plan (DRP) is designed to provide a structured response to packet sniffer software disruptions, ensuring continuity of services such as user authentication, packet capture, and data retrieval. The objective is to minimize downtime, prevent data loss, and safeguard the system's integrity while restoring operations within the defined Recovery Time Objective (RTO) of 4 hours and Recovery Point Objective (RPO) of 1 hour. The scope includes all system components hosted on localhost, including the React-based front-end, Python-driven APIs, K9Data database, and any auxiliary systems used for logging, configuration, and monitoring. The plan addresses threats such as hardware failures, database corruption, cyberattacks, natural disasters, and human errors, focusing on critical services required for operational recovery.

Step 2: Risk Assessment

The Risk Assessment is a comprehensive process that identifies potential vulnerabilities and threats to the system. Key risks include hardware malfunctions, such as disk or server failures; cyber threats like unauthorized access, DDoS attacks, and data breaches; software vulnerabilities, including bugs or misconfigurations; and external risks, such as power outages or natural disasters. Each risk is categorized by likelihood and impact to prioritize mitigation strategies. For example, the risk of unauthorized access is rated high due to sensitive user data being processed, prompting the implementation of multi-factor authentication (MFA) and encrypted backups. Additionally, the assessment includes dependencies on external tools and resources, such as third-party libraries and APIs, to evaluate risks of supply chain vulnerabilities.

Risk	Likelihood	Impact	Severity (Priority)
CWE-78: OS Command Injection	High	High	Critical
CWE-94: Code Injection	High	High	Critical
CWE-605: Multiple Port Binds	Medium	Medium	Moderate
Unused Variables (React)	Low	Low	Minor
Unknown Property 'class' (React)	Medium	Medium	Moderate
Unescaped Entities (React)	High	Medium	High
Missing Props Validation (React)	Medium	Medium	Moderate

Step 3: Business Impact Analysis (BIA)

This software is immensely important in allowing users to conduct different actions on multiple levels like network traffic analysis, manage saved sessions, and ensure real-time network diagnostics. Prolonged downtime or data loss could severely impair user operations, especially those relying on the software for critical troubleshooting or monitoring tasks. Recovery goals are an Recovery Time Objective (RTO) of 4 hours and an Recovery Point Objective (RPO) of 1 hour, ensuring minimal disruption.

Critical Dependencies and Prioritization:

- High-priority components:
 - The K9Data database is essential for storing user credentials, saved sessions, and captured packets. Corruption or inaccessibility of this database would directly impact system usability.
 - The Authentication API ensures secure user access. Without it, no user can interact with the system, resulting in a complete service outage.
 - The Sniffer API facilitates core packet capture and display functions. If it were disrupted, the software would be unusable for its primary purpose.

- Medium-priority components:
 - The Dashboard page is critical for user experience but is recoverable after restoring core functionality (e.g., APIs and database).
 - The Saved Sessions Page is vital for accessing previous packet captures but does not impact real-time sniffing operations.
- Low-priority components:
 - The Settings page and non-essential logs are less critical and can be restored after operational primary functionality.

Impact Metrics:

- Operational downtime: Any downtime exceeding 4 hours could result in users losing confidence in the software's reliability.
- Data loss: Loss of captured packets or saved sessions could damage user trust irreparable.
- Reputational harm: Frequent failures or extended outages could undermine the software's credibility, making it less competitive.

Step 4: Recovery Measures and Procedures

Recovery measures are divided into three key categories: preventative, reactive, and procedural, ensuring holistic preparedness and response to disasters.

Draft Preventative Measures:

1. Automated Backups: As a method to prevent data loss, the K9Data database can undergo hourly, encrypted backups stored both locally and in a secure cloud repository. Differential backups are used to reduce storage overhead.

2. **Secondary Server Setup:** A failover server is maintained on a separate physical or virtual host and configured to replicate the primary server's environment.
3. **Redundant APIs:** Core APIs (Authentication and Sniffer) could be containerized using Docker to allow seamless migration between servers in case of failure.
4. **Network Security Controls:** Firewalls, intrusion detection systems (IDS), and regular vulnerability scans ensure the system remains resilient to external threats.

Draft Reactive Measures:

1. **Incident Detection and Isolation:** Real-time monitoring tools (e.g., Prometheus) flag anomalies, and incidents are immediately isolated to prevent the spread of damage.
2. **Database Restoration:** Upon database corruption, the most recent backup is restored using an automated script. Transactions occurring after the backup are reconciled manually where feasible.
3. **Service Restoration:** APIs, including the Sniffer and Authentication services, are redeployed using the failover server. Services are tested for integrity and security before public availability.
4. **Communication:** Detailed incident reports are communicated to stakeholders, with regular updates on the recovery process.

Procedural Steps:

1. **Activate the DRP:** Notify the disaster recovery team and assign roles based on the predefined recovery plan.
2. **Isolate the Threat:** Identify and contain the root cause, such as a compromised API endpoint or faulty hardware.
3. **Rebuild and Validate:** Restore services incrementally, validating functionality after each step to minimize cascading issues.
4. **Monitor and Secure:** Monitor the restored system to ensure stability and address residual risks.

Step 5: Testing and Training

Regular testing and employee training ensure the DRP's effectiveness and help the team respond to real-world scenarios confidently.

Testing:

1. **Simulated Failure Scenarios:** Quarterly disaster drills simulate failures such as database corruption, DDoS attacks, or physical server outages. These simulations measure the team's ability to restore services within RTO and RPO objectives.
2. **Backup Integrity Testing:** Monthly tests validate the completeness and usability of backups by restoring data in a sandbox environment.
3. **Failover Server Tests:** The secondary server is regularly tested by daily switching operations, ensuring it mirrors the primary server's configuration.
4. **API Redundancy:** The APIs are tested for portability across different servers or cloud environments, ensuring quick redeployment in disasters.
5. **Incident Response Simulations:** Cybersecurity scenarios like ransomware attacks or unauthorized access attempts are conducted biannually to evaluate the team's response capabilities.

Training:

1. **Employee Onboarding:** New team members receive comprehensive DRP training, including understanding system architecture and recovery tools.
2. **Ongoing Training:** Annual workshops focus on advanced recovery techniques, cybersecurity trends, and updates to the DRP.
3. **Role-Based Training:** IT staff receive hands-on training with recovery tools, while developers focus on coding best practices to prevent vulnerabilities.