Business & Functional Requirements Document

Automated Network Fault Detection & Root Cause Analysis (RCA) System

Project Purpose

The purpose of this project is to automate the detection of network faults and perform real-time root cause analysis (RCA) using AI-powered agents. This system aims to reduce downtime, improve operational efficiency, and enhance customer satisfaction by providing faster incident resolution.

Technologies Used

• Azure OpenAI-powered multi-agent orchestration
• Azure Semantic Kernel for agent coordination
• Python 3.11+ for orchestration and automation
• Log analytics and AI-driven RCA
• Vector-based RCA report storage
• Azure Monitor & Application Insights integration

Business Requirements

• Automate detection of network faults in real-time to reduce downtime.
• Provide early alerts to network operations teams for faster response.
• Leverage AI agents to analyze logs and pinpoint root causes of failures.
• Improve operational efficiency by reducing manual troubleshooting.
• Enable data-driven decisions based on historical incident patterns.
• Ensure high system availability and improve customer satisfaction.
• Integrate seamlessly with existing network monitoring and ticketing systems.
• Maintain comprehensive RCA reports for compliance and audit purposes.
• Facilitate predictive maintenance using AI-driven insights.
• Scale to support increasing network traffic and complex fault patterns.

Functional Requirements

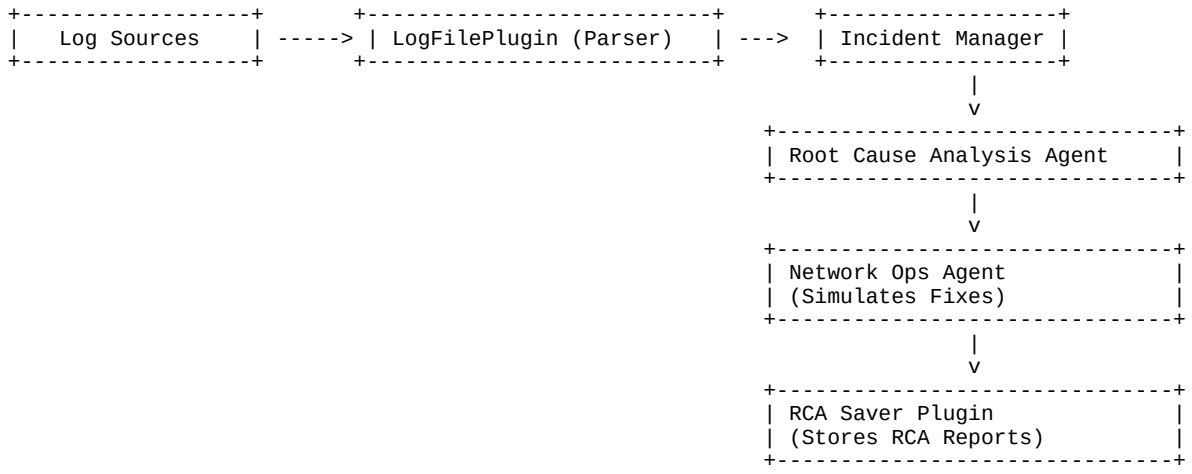
• System must parse and analyze incoming log files from multiple network sources.
• Detect anomalies and potential network faults using AI-powered agents.
• Trigger an Incident Manager Agent to assess issue severity and escalate if needed.
• Forward relevant logs to the Root Cause Analysis Agent for deeper investigation.
• Use Network Ops Agent to simulate and suggest corrective actions.
• Save RCA reports automatically using RCA Saver Plugin.
• Support integration with APIs for log ingestion and incident resolution.
• Maintain an audit trail of all incidents, RCA results, and remediation steps.
• Provide configurable alerting thresholds and escalation policies.
• Ensure system resilience and handle concurrent log streams efficiently.

Agent & Plugin Mapping

Agent / Plugin	Role / Functionality
Incident Manager Agent	Scans incoming logs, detects incidents, and initiates escalation.
Root Cause Analysis Agent	Performs deep RCA by correlating logs and identifying failure patterns.
Network Ops Agent	Suggests corrective actions and simulates fixes for identified issues.
LogFilePlugin	Handles reading and parsing of incoming log files.
NetworkOpsPlugin	Interfaces with network systems to simulate resolutions.
RCASaverPlugin	Saves RCA reports to persistent storage for auditing.

System Architecture Overview

The diagram below represents the end-to-end flow of the Automated Network Fault Detection & RCA System:



Non-Functional Requirements

• System should handle at least 10,000 logs per minute with minimal latency.
• Ensure 99.95% uptime for production deployment.
• Implement secure log handling and encrypted RCA report storage.
• Provide horizontal scalability to accommodate growing network complexity.
• Support observability and monitoring with integrated dashboards.
• Maintain role-based access control for authorized users only.
• Ensure GDPR and compliance readiness for audit trails.