USE CASE DESCRIPTION

Automated Log Analysis and Incident Response System

Use Case Name

Automated Log Analysis and Incident Response

Primary Actors

- Application / Server
- On-call Engineer
- Notification System

Secondary Actors

- Log Collector
- Log Processor
- Rule Engine
- Anomaly Detection Engine
- Response / Automation Engine
- Incident Manager

Description

This use case describes how the system automatically ingests logs from multiple applications, analyzes them to detect failures or anomalies, correlates related events into incidents, and performs automated response actions. When required, the system escalates incidents to on-call engineers and sends notifications.

Preconditions

- Application services are running and generating logs
- Log collector is active and connected to the system
- Detection rules and response playbooks are configured
- Notification system is available

Trigger

An application or server generates log entries during normal operation or failure conditions.

Main Flow (Normal Scenario)

1. Application servers continuously generate logs during execution.
2. The Log Collector collects logs from multiple application instances.
3. The Log Processor parses and normalizes incoming logs.
4. The Rule Engine evaluates logs against predefined rules to detect known failure patterns.
5. The Anomaly Detection Engine analyzes logs to detect abnormal behavior or unknown issues.
6. Detected signals are passed to the Response / Automation Engine.
7. The Incident Manager creates or updates an incident based on correlated log events.
8. If the incident qualifies for automated handling, a response action is triggered.
9. The system executes the response action such as service restart or rollback.
10. The incident status is updated accordingly.
11. Notifications are sent to the notification system for visibility.

Alternate Flow A – Manual Approval Required

1. The Incident Manager identifies a high-impact incident.
2. The system requests manual approval from the on-call engineer.
3. The on-call engineer reviews the incident details.
4. Upon approval, the response action is executed.
5. The incident status is updated and notifications are sent.

Alternate Flow B – Response Failure

1. An automated response action fails due to an error or exception.
2. The failure is recorded by the system.
3. The Incident Manager escalates the incident.
4. A notification is sent to the on-call engineer for manual intervention.

Postconditions

- The incident is resolved automatically or escalated to an engineer
- Incident details, actions, and outcomes are recorded
- Notifications reflect the current incident status

Business Value

- Reduces Mean Time To Recovery (MTTR)
- Minimizes manual intervention for common failures
- Improves system reliability and operational efficiency
- Provides consistent and auditable incident handling