Correlação Inteligente de Alarmes com IA-ML

Last updated by | Thiago Guimaraes | 28/11/2025 at 14:21 GMT-3

1. Visão Geral

Este documento descreve a iniciativa de implementação de **Inteligência Artificial (IA)** e **Machine Learning (ML)** no sistema de *Fault Management*, com o objetivo de identificar **correlações entre alarmes**, reduzir ruído operacional, detectar **cadeias causais** e auxiliar na determinação de **causa raiz**.

O sistema atualmente recebe dezenas de alarmes por minuto provenientes de diversas camadas da infraestrutura (aplicações, pods, nós físicos, storage, rede, APIs, etc.). Esses alarmes chegam de forma isolada, sem contexto, dificultando a análise.

A iniciativa busca evoluir para um mecanismo inteligente de **correlação automática de eventos**, alinhado às práticas modernas de **AIOps**.

2. Problema Atual

- Os alarmes são tratados individualmente, mesmo quando fazem parte do mesmo incidente.
- Eventos correlacionados em diferentes camadas não são agrupados automaticamente.
- Há grande volume de ruído operacional.
- A determinação da causa raiz é lenta e depende de análise manual.
- O sistema não aprende com incidentes anteriores.

3. Objetivo da Iniciativa

Adicionar uma camada de inteligência ao *Fault Management* para:

1. **Correlacionar alarmes automaticamente**, com base em padrões históricos e relações causais.
2. **Agrupar alarmes relacionados** em um incidente unificado (“episódio”).
3. **Identificar prováveis causas raiz** de forma automatizada.
4. **Reduzir o ruído operacional** e priorizar eventos realmente importantes.
5. **Acelerar a detecção e resolução de incidentes** (redução de MTTR).

4. Exemplo Prático – Ambiente OpenShift

Cenário

- Um pod específico de um cluster OpenShift começa a apresentar **uso anormal de CPU**.
- O nó físico que o hospeda dispara um alarme de **CPU alta**.
- Outros pods no mesmo node passam a sofrer **throttling** e degradação.

Comportamento Esperado do Sistema

Em vez de gerar alarmes isolados, o sistema deve consolidar em um único incidente:

```
Incidente correlacionado: Saturação de recursos no Node Y Causa raiz provável: Pod X com CPU anômala Impacto: Pods Z, W e K em throttling Recomendação: Investigar Pod X (pico de carga ou comportamento anômalo)
```

5. Escopo Inicial (MVP)

1. Analisar e categorizar os alarmes existentes.
2. Criar pipeline de dados com metadados operacionais e de topologia.
3. Implementar protótipo usando:
    - Correlação temporal
    - Clusterização de alarmes
    - Grafo inicial de relacionamentos
4. Gerar primeiros episódios correlacionados.
5. Validar com o time de operações.

6. Roadmap de Evolução

- Evoluir os modelos para GNNs e causalidade probabilística.
- Implementar ranking de causa raiz com pesos dinâmicos.
- Integrar com automações (ações corretivas recomendadas).
- Criar *feedback loop* supervisionado para melhorar as previsões.
- Criar painel visual de incidentes correlacionados.

7. Conclusão

A correlação inteligente de alarmes com IA/ML representa uma evolução significativa no sistema de Fault Management.

A solução permitirá identificar relações complexas entre eventos, reduzir o volume de alarmes irrelevantes e aumentar a eficiência da operação.

Essa iniciativa posiciona o ambiente no caminho dos **AIOps modernos**, transformando dados brutos em informações acionáveis e inteligentes.