

CURSO: DEVOPS SENIOR

Módulo 10: AIOps & Incident Management

Ejercicio Práctico 1

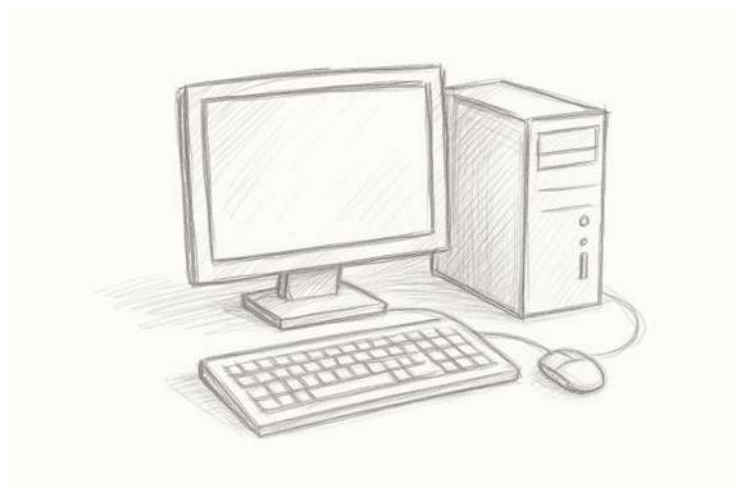
**Simulación AIOps + Auto-Remediation con Prometheus +
Alertmanager + Webhook Custom + Runbooks**

Objetivo:

Configurar un flujo de monitoreo que detecte incidentes, los agrupe y genere acciones automáticas de remediación usando un webhook personalizado y reglas de Prometheus Alertmanager. Se simula el comportamiento de una herramienta AIOps (como Moogsoft o PagerDuty AIOps).

Resultado esperado:

Diseñar un flujo automatizado de detección, agrupación y remediación de incidentes usando herramientas open source y simula el comportamiento inteligente de plataformas AIOps.



INSTRUCCIONES:

- **Entorno sugerido:**
 - Clúster Kubernetes local (Minikube/Kind).
 - Prometheus + Alertmanager instalados (Helm).
 - Script local de auto-remediación (Bash, Python o webhook server en Node.js).

- **Actividad guiada paso a paso:**

Simulación de microservicios con fallas:

- Despliegue un pod que consuma mucha CPU o se reinicie constantemente.
- Prometheus detecta el patrón y lanza una alerta.

- **Configuración de Alertmanager:**

- Defina un grupo de alertas que se disparen por tipo de fallo.

- **Agregue un receiver de tipo webhook:**

```
yaml

receivers:
- name: 'remediation-hook'
  webhook_configs:
  - url: 'http://remediator.default.svc.cluster.local:8080'
```

- **Implementación del webhook de auto-remediación:**

- Script que reinicia el deployment afectado (kubectl rollout restart) o escala réplicas.
- Agregue logging detallado de qué acción se ejecutó.

- **Validación del flujo:**
 - Simule múltiples fallos seguidos (alta latencia, errores HTTP 500).
 - Verifique que se agrupan como un solo evento.
 - Asegúrese de que se ejecuta una sola acción correctiva por evento.

- **Feedback técnico esperado:**
 - Alertas agrupadas correctamente (AIOps-like correlation).
 - Auto-remediación ejecutada según runbook lógico.
 - Reducción del tiempo entre alerta y acción (simulación MTTR).