Ejercicio Guiado: Solución de Observabilidad con Stack GFG

Empresa: CloudEdu

Contexto: Plataforma de cursos online desplegada en Kubernetes sobre AWS. Enfrenta problemas de lentitud, errores y falta de trazabilidad de logs.

🛠️ Paso 1: Diagnóstico del problema

Síntomas identificados:

1. **Logs efímeros**: Los logs desaparecen al reiniciarse los contenedores.
2. **Falta de trazabilidad**: No hay manera rápida de identificar el origen de errores reportados por usuarios.
3. **No hay correlación visual** entre eventos del sistema, rendimiento de servicios y métricas críticas.

Impacto:

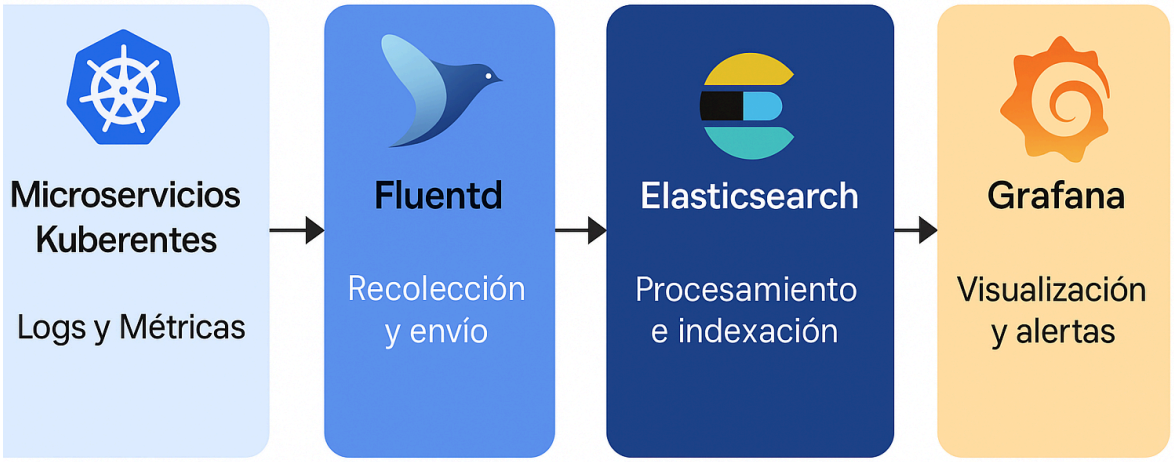
- Aumenta el **MTTR (Mean Time To Resolution)**.
- Afecta la experiencia de usuario.
- Disminuye la capacidad de soporte técnico para actuar de forma proactiva.

Necesidades:

- Persistencia de logs.
- Centralización de eventos.
- Dashboards con visualización clara y alertas proactivas.

🔧 Paso 2: Diseño del flujo con GFG

Diagrama de Flujo de Datos:



Detalles técnicos:

- **Fluentd**:
  - Fuente: `/var/log/containers/*.log`, syslog, logs de pruebas automatizadas.
  - Plugins: `tail`, `gelf`, `record_transformer`.
- **Graylog**:
  - Recibe en GELF UDP.
  - Indexa eventos en Elasticsearch.
  - Permite búsquedas y pipelines de transformación.
- **Grafana**:
  - Conecta con Elasticsearch (`graylog_*`).
  - Dashboards con alertas y análisis en tiempo real.

📈 Paso 3: Casos de uso de observabilidad

Caso de Uso	Tipo de Dato	Fuente	Visualización en Grafana
1. Errores de login por IP	Log de aplicación	Graylog (índice `auth.log`)	Panel por geolocalización o IP
2. Latencia del microservicio de pagos	Métrica custom (ms)	Log estructurado enviado por Fluentd	Gráfico de líneas por intervalo
3. Aumento de errores 5xx	Código HTTP	Logs de NGINX/API Gateway	Alerta si `count(5xx) > 10` en 5 minutos

---

⚖️ Paso 4: Comparativa con otras soluciones

¿Cómo se compara GFG con ELK o Datadog?

Solución	Ventajas	Desventajas
GFG (Graylog, Fluentd, Grafana)	Modular, liviano, fácil de extender	Visualización básica en Graylog
ELK (Elasticsearch, Logstash, Kibana)	Integración más completa	Más pesado, más complejo
Datadog	SaaS, integración rápida	Costoso, no open source
Prometheus + Grafana	Ideal para métricas	No diseñado para logs complejos

¿Cuándo usar GFG?

- Cuando se prioriza open source, modularidad, bajo consumo y facilidad de integración en DevOps.

¿Cuáles serían las posibles dificultades en la implementación?

Las principales dificultades son la configuración inicial compleja, la integración entre componentes, la necesidad de logs bien estructurados, la curva de aprendizaje de las herramientas y los retos de escalabilidad y seguridad en entornos productivos.

🔁 Paso 5: Integración con CI/CD

¿Cómo se podrían automatizar los despliegues de monitoreo con GFG?

Automatización con GitHub Actions:

```
- name: Run tests and log output
  run: |
    npm test | tee test.log

- name: Send logs to Fluentd
  run: |
    curl -X POST -H "Content-Type: application/json" \
      -d @test.log http://fluentd:9880/ci.test
```

¿Qué ventajas trae incluir GFG en el pipeline de desarrollo?

Ventajas:

- Logs desde pruebas automatizadas disponibles en Graylog.
- Alertas inmediatas si fallan los tests.
- Permite trazabilidad completa desde el pipeline hasta el runtime.

¿Quién se haría responsable de mantener y escalar la solución?

Responsable:
Equipo DevOps debe mantener configuración, escalabilidad y seguridad del stack.