Engine da Observabilidade

Introdução

A Engine de Observabilidade do cluster é o conjunto de serviços responsáveis por coleta, armazenamento, consulta e visualização de logs, métricas e eventos operacionais de toda a plataforma.

O objetivo da observabilidade é permitir:

- Diagnóstico rápido de problemas
- Monitoramento de serviços
- Análise de comportamento de aplicações
- Auditoria de eventos
- Criação de alertas
- Visualização de méttricas
- Troubleshooting operacional
- Análise histórica de falhas e incidentes

A observabilidade é tratada como parte fundamental da infraestrutura, e não como um recurso opcional.

Arquitetura da Observabilidade

A arquitetura da observabilidade do cluster é composta pelos seguintes componentes:

Componente	Função
Alloy	Coleta e roteamento de logs
Loki	Armazenamento e consulta de logs
Prometheus	Coleta de métricas
Grafana	Visualização e dashboards
Node Exporter	Métricas dos servidores
cAdvisor	Métricas dos containers

Fluxo de Logs

`Container → Docker Logging → Alloy → Loki → Grafana`

Fluxo de Métricas

`Node Exporter / cAdvisor → Prometheus → Grafana`

Coleta de Logs com Alloy

Todos os containers do cluster enviam seus logs através do Docker Logging Driver utilizando o protocolo Syslog.

Os logs não são enviados diretamente para o Loki. Existe uma camada intermediária chamada **Alloy**, que atua como agente de coleta e roteamento de logs.

Vantagens dessa arquitetura

- Desacoplamento entre aplicações e backend de logs
- Padronização de logs
- Controle centralizado
- Possibilidade de mudar o backend sem alterar aplicações
- Coletor local em cada nó
- Baixa latência
- Menor tráfego de rede overlay

Cada nó do cluster executa uma instância do Alloy em modo global, funcionando como endpoint local de ingestão de logs.

Os containers enviam logs para:

`tcp://127.0.0.1:51893`

Isso garante que os logs sempre sejam enviados localmente ao nó, evitando dependência de rede overlay.

Armazenamento de Logs com Loki

O Loki é o sistema responsável pelo armazenamento e consulta de logs do cluster.

Diferente de sistemas tradicionais de logs, o Loki não indexa o conteúdo dos logs, apenas labels. Isso reduz drasticamente o consumo e armazenamento.

Os logs são indexados principalmente pelos seguints labels:

- stack
- service
- container
- node
- level (quando disponível)

Isso permite consultas como:

- Logs de um serviço específico
- Logs de uma stack
- Logs de um nó
- Logs de erro
- Logs de um intervalo de tempo

O Loki funciona como backend de logs e é consultado através do Grafana.

Métricas com Prometheus

O Prometheus é responsável pela coleta de métricas do cluster e dos serviços.

As métricas coletadas incluem:

Métricas de Infraestrutura

- CPU
- Memória
- Disco
- Rede
- Load average
- IO

Métricas de Containers

- Uso de CPU por container
- Uso de memória por container
- Network IO
- Restart de containers
- Número de replicas
- Estado de serviços

As métricas são coletadas principalmente através de:

Exporter	**Função**
Node Exporter	Métricas do host
cAdvisor	Métricas dos containers
Prometheus	Coleta e armazenamento

Visualização com Grafana

O Grafana é a interface de visualização da observabilidade.

Atravéd do Grafana é possível:

- Visualizar logs
- Criar dashboards
- Criar alertas
- Monitorar serviços
- Monitorar infraestrutura
- Analisar incidentes
- Visualizar métricas históricas

O grafana funciona como interface única de observabilidade da plataforma.

Filosofia da Observabilidade

A observabilidade do cluster foi projetada seguindo alguns princípios:

Logs são obrigatórios

Todo serviço deve gerar logs.

Logs centralizados

Nenhum log deve ficar apenas dentro do container.

Métricas antes de problemas

Problemas devem ser detectados por métricas antes de usuários perceberem.

Troubleshooting deve ser rápido

Deve ser possível descobrir o problema em minutos, não horas.

Observabilidade faz parte da plataforma

Não é responsabilidade de cada aplicação individual.

Tudo deve ser observável

- Infraestrutura
- Containers
- Serviços
- Filas
- APIs
- Banco
- Jobs
- Deploys

Resumo da Engine de Observabilidade

A Engine de Observabilidade do cluster é composta por:

Camada	Ferramenta
Coleta de Logs	Alloy
Armazenamento de Logs	Loki
Coleta de Métricas	Prometheus
Métricas de Host	Node Exporter
Métricas de Containers	cAdvisor
Visualização	Grafana

Diagrama resumido