ChatGPT

Permissions — GitHub, GHCR, Kubernetes e Grafana Cloud

GitHub Actions (princípios)

- Use o `GITHUB_TOKEN` nativo com **menor privilégio**:

```
permissions:
  contents: read
  id-token: write
```

- Apenas workflows de **build** precisam de acesso ao GHCR (write). O de **deploy** não.

Secrets canônicos

- `KUBE_CONFIG` — kubeconfig (base64) do cluster/namespace de deploy.
- `GRAFANA_CLOUD_OTLP_ENDPOINT` — endpoint OTLP (traces/logs/metrics).
- `GRAFANA_CLOUD_API_TOKEN` — token *write-only* (ingest) para Grafana Cloud.
- `GHCR_USERNAME` / `GHCR_TOKEN` — apenas no pipeline de build (write:packages).
- `GHCR_READ_TOKEN` — se for criar `imagePullSecret` no cluster (read:packages).

Tokens pessoais (quando inevitáveis)

Prefira **Fine-grained PAT** restrito ao repositório (`lichtara/portal`) com permissões mínimas:

- `Contents: Read & Write` (somente se fizer push local).
- `Packages: write` (caso publique no GHCR localmente).
- Expiração curta (30–90 dias) e rotação.

Kubernetes RBAC

- ServiceAccount `ci-deployer` com Role mínima por namespace (Deploy/Service/ConfigMap/Secret + CRDs de monitoring). Sem acesso cluster-wide.

Grafana Cloud (política de acesso)

- Token de ingestão com escopos **apenas de escrita** por recurso que você usa:
- `traces:write`
- `metrics:write` (se enviar métricas)
- `logs:write` (se enviar logs)
- Não conceder: leitura, admin, dashboards, alerting, org-level.

Segregação por função (recomendado)

- **Build**: GHCR write; sem kube.
- **Deploy**: kube + Grafana write; sem GHCR write.
- **Observabilidade**: tokens separados por ambiente (`dev` / `prod`).

Rotação

- Rotacione secrets/tokens a cada 90 dias (ou menos). Monitore a validade.
