



Relatório de Infraestrutura OCI

(tf_oci_clusters)

Este relatório detalha os recursos e a arquitetura provisionados pelo repositório `tf_oci_clusters` para os ambientes de Desenvolvimento (DEV), Homologação (HML) e Produção (PROD).



Visão Geral dos Ambientes

A infraestrutura é dividida em três ambientes principais, cada um com objetivos distintos:

RECURSO	DEV / HML	PROD (HA)
Identidade	Federação Azure AD (SSO)	Federação Azure AD (SSO)
Clusters OKE	3 Clusters ativos (8h-18h)	3 Clusters Always-On
Nodes por Cluster	1-3 (Auto-stop via CronJob)	3-12 (Autoscaling ativo)
Configuração Node	2 OCPUs / 16GB RAM	4 OCPUs / 32GB RAM
Alta Disponibilidade	Single Availability Domain	Multi-AZ (3 ADs)
Visibilidade	Privada (via VPN/Bastion)	Endpoints Públicos (opcional)



Rede e Segurança (Networking)

A base de rede é sólida e segue as melhores práticas da OCI:

- **VCN (`vcn-oke`)**: CIDR `/16` (ex: `10.110.0.0/16` para DEV).
- **Gateways**:
 - **Internet Gateway**: Para saída/entrada direta em subnets públicas.
 - **NAT Gateway**: Permite que nodes privados acessem a internet sem exposição externa.
 - **Service Gateway**: Acesso direto aos serviços OCI (Object Storage, Registry) sem sair pela internet.
- **Identidade e Federação (IAM)**:
 - **Azure AD Federation**: Integração SAML2 que permite o login na console OCI e clusters usando credenciais corporativas.
 - **JIT (Just-in-Time)**: Criação automática de usuários OCI no primeiro login.
 - **RBAC OKE**: Mapeamento de grupos do Azure para grupos OCI (`oke-admin` , `oke-dev` , `oke-readonly`).
- **Subnets (Regionais)**:
 - **Workers (`sbn-workers-*`)**: 3 subnets para os nós do Kubernetes.
 - **Load Balancer (`sbn-lb-*`)**: 2 subnets públicas para balanceadores de carga.
 - **API Gateway (`sbn-api-gateway`)**: Subnet privada dedicada para o serviço de API.
 - **Bastion Instance**: Provisionada opcionalmente para acesso SSH seguro aos nós privados.



Kubernetes (OKE - Oracle Kubernetes Engine)

Cada ambiente provisiona **3 clusters independentes**: 1. `cls-{env}-nexus` (Core Application) 2. `cls-{env}-barramento` (Messaging/Integration) 3. `cls-{env}-observabilidade` (Métricas e Logs)

Características dos Clusters:

- **Node Pools Flexíveis:** Uso de formas `VM.Standard.E4.Flex` permitindo ajuste fino de CPU e Memória.
- **Arquitetura Híbrida:** Suporte para nodes ARM (`aarch64`) e Intel/AMD (`x86_64`).
- **Bootstrap Seguro:** Entrega automatizada de certificados TLS durante a inicialização dos nodes.



Aplicações e GitOps

O gerenciamento das aplicações utiliza uma abordagem moderna de GitOps:

- **ArgoCD (HA):**
 - Instalado via Helm em todos os clusters.
- **SSO via OIDC:** Integração com **OCI Identity Domains** (App OIDC) para permitir login via Azure AD.
- **RBAC Integrado:** Permissões baseadas em grupos do Identity Domains (`invista-oke-admin` , `invista-oke-dev`).
- **API Gateway (Micro-Frontends):**
 - Gateway Público para servir 6 MFEs: `user` , `shell` , `auth` , `person` , `formalization` , `poc` .
 - Integração direta com **Object Storage** (Bucket) para servir aplicações SPA de forma performática e barata.



Observabilidade

Monitoramento nativo integrado ao Tenancy: - **Log Groups**: Centralização de logs de infraestrutura e aplicações. - **Alarms & Notifications**: Tópicos SNS configurados para alertas críticos. - **Dashboards**: Dashboards OCI importados automaticamente via JSON.



Automação de Custo (FinOps)

Para os ambientes **DEV e HML**, existe uma automação via CronJobs que: - **08:00 BRT**: Escala o número de nodes para 3. - **18:00 BRT**: Escala o número de nodes para 0 (desligamento total fora do horário comercial). - Economia estimada de ~70% em custos de infraestrutura não-produtiva.

Relatório gerado em 27 de Fevereiro de 2026.

Relatório gerado automaticamente em 27 de Fevereiro de 2026.