

ESTRUTURA DE CONTAS AWS

Network Account

- AW SNS
- AWS CLOUDWATCH
- AWS GUARDDUTY
- ELASTIC LOAD
 BALANCER
- AWS CONFIG
- AWS CLOUDTRAIL
- AWS X-RAY
- AWS WAF
- AWS NETWORK
 FIREWALL
- TRANSIT GATEWAY

Application Account

- VPC
- AMAZON EKS CLUSTER
- AMAZON ECR
- AWS CODEPIPELINE
- AWS RDS (MULTIAZ)
- AWS S3
- AWS LAMBDA
- AWS BACKUP
- AWS SNS
- AWS SQS
- AWS CLOUDWATCH
- AWS GUARDDUTY
- AWS CLOUDTRAIL
- AWS KMS
- AWS COGNITO

BENEFÍCIOS:

- ISOLAMENTO DE RECURSOS
- CONTROLE GRANULAR DE ACESSO
- FATURAMENTO SEPARADO
- CONFORMIDADE E GOVERNANÇA APRIMORADAS



ARQUITETURA DE REDE

COMPONENTES PRINCIPAIS:

- AWS ROUTE 53 PARA DNS
- AWS CLOUDFRONT PARA CDN
- TRANSIT GATEWAY PARA CONECTIVIDADE CENTRALIZADA
- NETWORK FIREWALL PARA SEGURANÇA DE REDE AVANÇADA
- DIRECT CONNECT E VPN PARA CONEXÃO COM ON-PREMÍSE

SEGURANÇA DE REDE:

- AWS WAF NA CAMADA DE APLICAÇÃO
- GUARDDUTY PARA DETECÇÃO DE ÁMEAÇAS
- AWS SHIELD (IMPLÍCITO) PARA PROTEÇÃO CONTRA DDOS

MONITORAMENTO E COMPLIANCE:

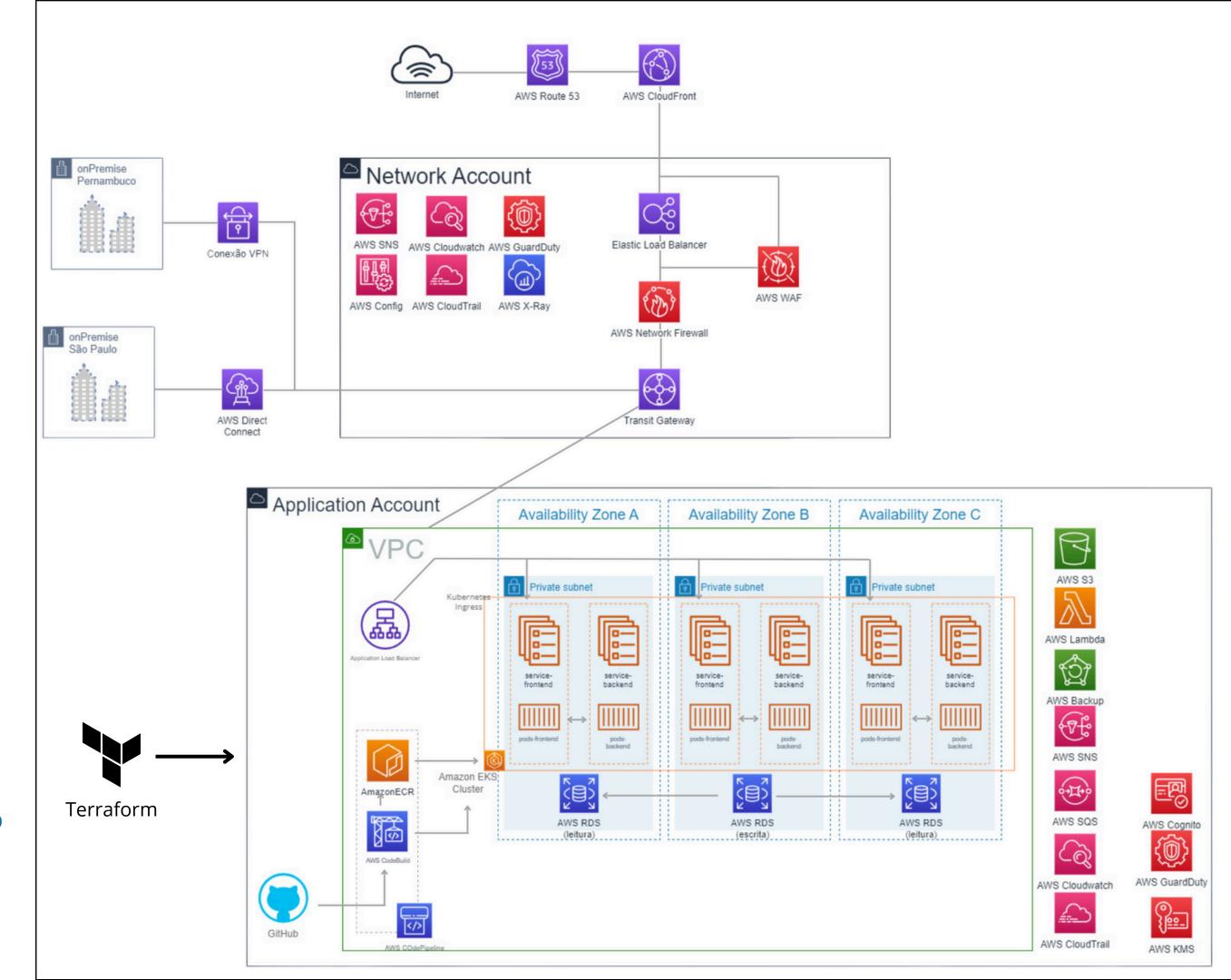
- AWS CLOUDTRAIL PARA AUDITORIA
- AWS CONFIG PARA CONFORMIDADE
- AWS X-RAY PARA ANÁLISE DE PERFORMANCE

IAC.

TERRAFORM

CONECTIVIDADE HÍBRIDA:

• INTEGRAÇÃO DE ESCRITÓRIOS EM PERNAMBUCO E SÃO PAULO



ARQUITETURA DA APLICAÇÃO

INFRAESTRUTURA:

- VPC DISTRIBUÍDA EM 3 AVAILABILITY ZONES
- SUBNETS PRIVADAS PARA ISOLAMENTO DE RECURSOS

COMPONENTES:

- AMAZON ECS COM CLUSTERS PARA CONTAINERIZAÇÃO
- EKS WORKERS PARA APLICAÇÃO
- APPLICATION LOAD BALANCER PARA DISTRIBUIÇÃO DE TRÁFEGO
- AMAZON RDS MULTI-AZ PARA ALTA DISPONIBILIDADE DE BANCO DE DADOS
- AWS LAMBDA PARA COMPUTAÇÃO SERVERLESS

ARMAZENAMENTO E MENSAGERIA:

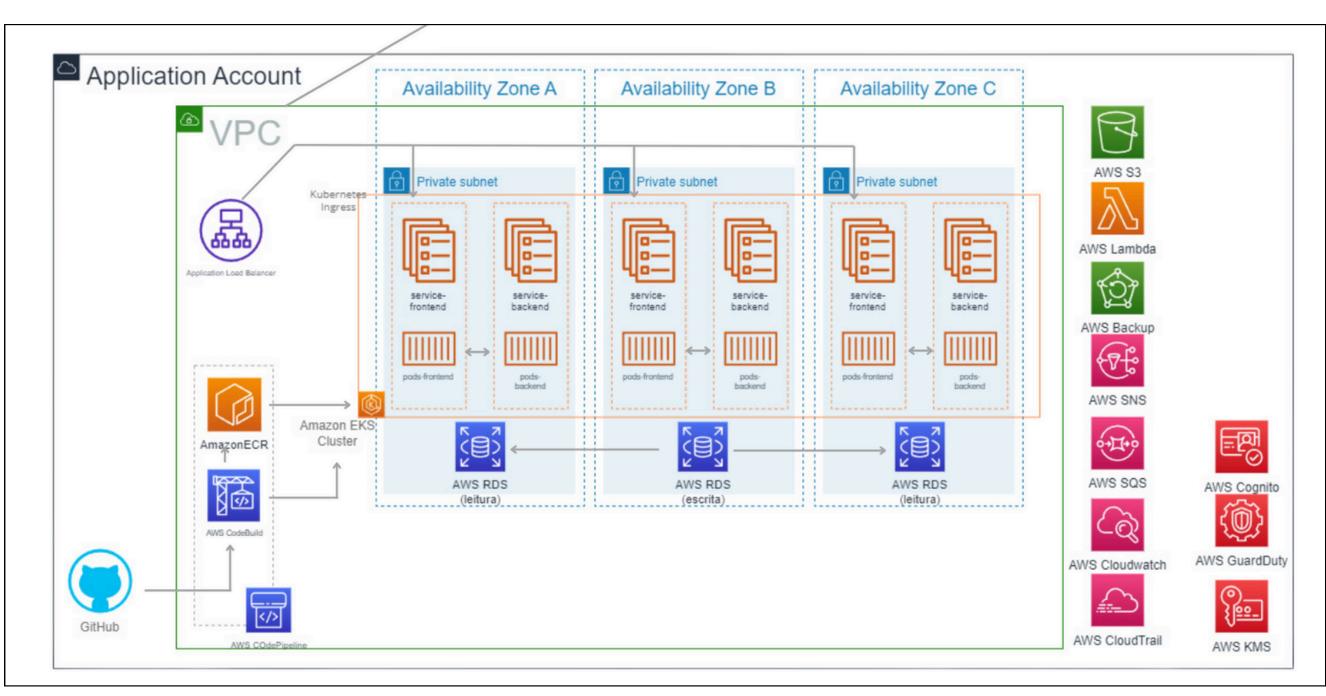
- AMAZON S3 PARA ARMAZENAMENTO DE OBJETOS
- AWS SNS PARA NOTIFICAÇÕES E MENSAGERIA

CI/CD E CONTROLE DE VERSÃO:

- INTEGRATION COM GITHUB PARA CONTROLE DE CÓDIGO
- AWS CODEDEPLOY PARA AUTOMAÇÃO DE DEPLOYMENTS

ESCALABILIDADE:

- AUTO SCALING
- READ REPLICAS PARA RDS



SUPONDO QUE A APLICAÇÃO É DINAMICA(REACT) O FRONT-END FOI MANTIDO NO AWS EKS.

COMUNICAÇÃO ENTRE FRONT-END E BACK-END
SERVICES: NO KUBERNETES FOI UTILIZADO SERVIÇOS DO TIPO CLUSTERIP PARA PERMITIR QUE O FRONT-END SE COMUNIQUE EXCLUSIVAMENTE COM O BACK-END.

INGRESS CONTROLLER(EX: NGINX) PARA EXPOR A APLICAÇÃO FRONT-END PARA O PÚBLICO EXTERNO. O AWS ALB PARA DIRECIONAR O TRÁFEGO EXTERNO AO INGRESS.

ESTRATÉGIA DE DISASTER RECOVERY

ABORDAGEM MULTI-AZ:

- DISTRIBUIÇÃO DE RECURSOS EM 3 AVAILABILITY ZONES
- RDS MULTI-AZ PARA ALTA DISPONIBILIDADE DE DADOS

BACKUP E RESTAURAÇÃO:

- AWS BACKUP PARA BACKUPS AUTOMATIZADOS
- S3 PARA ARMAZENAMENTO DE BACKUPS DE LONGO PRAZO

REPLICAÇÃO:

- S3 COM VERSIONAMENTO E REPLICAÇÃO CROSS-REGION (IMPLÍCITO)
- RDS COM REPLICAÇÃO SÍNCRONA ENTRE AZS

RECUPERAÇÃO:

- AUTO SCALING PARA RECUPERAÇÃO AUTOMÁTICA DE INSTÂNCIAS
- LAMBDA PARA FUNÇÕES DE RECUPERAÇÃO SERVERLESS
- IAC PERMITE RECRIAR RAPIDAMENTE AMBIENTES EM CASO DE FALHAS

MONITORAMENTO E ALERTAS:

- CLOUDWATCH PARA MONITORAMENTO DE MÉTRICAS
- SNS PARA NOTIFICAÇÕES DE EVENTOS CRÍTICOS

TESTES:

- SIMULAÇÕES REGULARES DE FAILOVER ENTRE AZS
- DOCUMENTAÇÃO E PLAYBOOKS DE DR

ESTRATÉGIAS DE DEPLOYMENT

CI/CD PIPELINE:

- INTEGRAÇÃO COM GITHUB PARA CONTROLE DE VERSÃO
- AWS CODEDEPLOY PARA AUTOMAÇÃO DE DEPLOYMENTS

BLUE-GREEN DEPLOYMENT:

- UTILIZAÇÃO DE MÚLTIPLOS TARGET GROUPS NO ALB
- SWAP DE TRÁFEGO CONTROLADO PELO ALB

CANARY DEPLOYMENT:

- ROTEAMENTO DE TRÁFEGO GRADUAL COM ALB
- MONITORAMENTO DE MÉTRICAS COM CLOUDWATCH

BENEFÍCIOS:

- MINIMIZAÇÃO DE DOWNTIME
- FACILIDADE DE ROLLBACK
- TESTES EM PRODUÇÃO COM RISCO REDUZIDO

TERRAFORM:

- AUTOMAÇÃO: ELIMINA A NECESSIDADE DE CONFIGURAÇÕES MANUAIS.
- CI/CD: FACILITA DEPLOYS AUTOMÁTICOS E CONSISTENTES.
- INFRAESTRUTURA IMUTÁVEL: GARANTE MUDANÇAS SEGURAS E CONTROLADAS.
- ESCALABILIDADE: AJUSTA A INFRAESTRUTURA CONFORME A DEMANDA.
- CONSISTÊNCIA: ASSEGURA QUE TODOS OS AMBIENTES SEJAM IDÊNTICOS.

MONITORAMENTO E OBSERVABILIDADE

Ferramentas:

- Amazon CloudWatch: métricas, logs e alarmes
- AWS X-Ray: análise e debugging de aplicações distribuídas
- AWS CloudTrail: auditoria de atividades na conta

Aspectos Monitorados:

- Saúde da infraestrutura (EKS, RDS)
- Performance da aplicação
- Segurança e conformidade (GuardDuty, Config)
- Custos e utilização de recursos

Alertas:

- SNS para notificações em tempo real
- Integração com sistemas de ticketing (opcional)

Dashboards:

- CloudWatch Dashboards para visualização de KPIs
- Integrações possíveis com Grafana ou Kibana

AUTENTICAÇÃO E AUTORIZAÇÃO

Serviços Utilizados:

- AWS Cognito: gerenciamento de usuários e autenticação
- AWS IAM: controle de acesso granular
- AWS KMS: gerenciamento de chaves de criptografia

Implementação:

- Cognito para autenticação de usuários finais
- IAM para controle de acesso aos recursos AWS
- Integração possível com Identity Providers corporativos

Controle de Acesso:

- RBAC (Role-Based Access Control) com IAM
- Least Privilege Principle aplicado às políticas

Segurança Adicional:

- AWS GuardDuty para detecção de ameaças
- AWS WAF para proteção da camada de aplicação
- Network Firewall para segurança da rede

Auditoria:

AWS CloudTrail para logging de atividades

Integração com SIEM para análise avançada de segurança

OTIMIZAÇÃO DE CUSTOS (FINOPS)

DIMENSIONAMENTO E AUTOSCALING:

AJUSTAR O TAMANHO
DOS RECURSOS (EKS,
RDS) E UTILIZAR
AUTOSCALING PARA
EVITAR
SOBREPROVISIONAMEN
TO.

INSTÂNCIAS RESERVADAS/ SAVINGS PLANS:

APLICAR INSTÂNCIAS RESERVADAS PARA EKS, RDS, LAMBDA, E ECONOMIZAR EM LONGO PRAZO.

MONITORAMENTO DE CUSTOS:

UTILIZAR AWS
COST EXPLORER E
TRUSTED ADVISOR
PARA IDENTIFICAR E
ELIMINAR
RECURSOS
OCIOSOS.

ARMAZENAMENTO OTIMIZADO:

USAR CLASSES DE ARMAZENAMENTO EFICIENTES (S3 GLACIER, S3-IA) E REVISAR POLÍTICAS DE BACKUP.



OTIMIZAR USO DE DIRECT
CONNECT E VPN PARA REDUZIR
CUSTOS DE TRÁFEGO.
TAGGING E VISIBILIDADE: APLICAR
TAGS PARA CONTROLAR
CUSTOS POR
AMBIENTE/APLICAÇÃO E
FACILITAR A ALOCAÇÃO DE
DESPESAS.

