Documento de Configuração de Hardware e Software

Readiness- SELOS do AGRO

CHS

Memorial Descritivo do Documento

FAO – Selos do Agro
Gestor do Projeto
F&S - Tecnologias Agropecuárias
aecio.flores@fstec.agr.br
elizier.santos@fstec.agr.br
+55 51 99913-6826
+55 21 98034-1488

Histórico de Revisão			
Data	**Versão**	**Descrição**	**Autor**
23/10/2023	1.0	Versão Inicial do arquivo	Elizier Santos

1. Requisitos Não-Funcionais

1.1.O projeto Readiness-Selos do AGRO passa pela premissa de desenvolvimento de uma solução para rodar em Nuvem Pública

2. Requisitos de Nível de Serviço(SLA)

2.1. Disponibilidade

O Nível de Serviço desta proposta abrange o SLA dos serviços de nuvem que a mesma utilizará:

As aplicações em containers no AWS possuem SLA de 99.95%, já o banco de dados gerenciado, de acordo com as configurações desta proposta, possui SLA de 99.5%.

2.2. Janela de Manutenção

Estão previstos 4 horas por mês de parada programada do sistema (indisponibilidade) para possíveis reciclagens, correções na aplicação ou ajustes nas configurações do banco de dados e/ou servidores de aplicação.

A janela só será acionada em caso de necessidade e será negociada com o cliente a data/hora da mesma, sendo preferencialmente fora do horário comercial.

3. Ambientes disponíveis

4. **Homologação**: ambiente destinado à testes de conectividade e validação operacional de funcionalidades que já se encontram em produção, não afetando porém os dados reais existentes no banco de dados de produção.
    1. Entende-se como homologação o processo de aprovação de ambiente realizado pelo CONTRATANTE a partir de cada entidade/ator/usuário que valide o ambiente a partir do seu uso e ou integração de seus sistemas. Para cada entidade/ator/usuário será estabelecido um checklist de aprovação contendo sua analise no uso do ambiente de homologação e o parecer de aprovação do mesmo para liberação como ambiente de produção.

5. **Produção**: ambiente operacional real, produzido e suportado pela F&S, para a garantia do protocolo de produção de carnes para exportação. Os dados serão recebidos, mantidos em sigilo e guarda respeitando todos os *compliances* da LGPD e permitindo sua auditoria somente pelos órgãos de controle.

6. Cloud Provider

O provedor de nuvem pública adotado pelo projeto é a Amazon AWS (https://aws.amazon.com/) e utilizará como SGBD oPostgreSQL.

7. Arquitetura de Infraestrutura

Na <Figura 1> o desenho da arquitetura de referência da solução independente de provedor de nuvem.

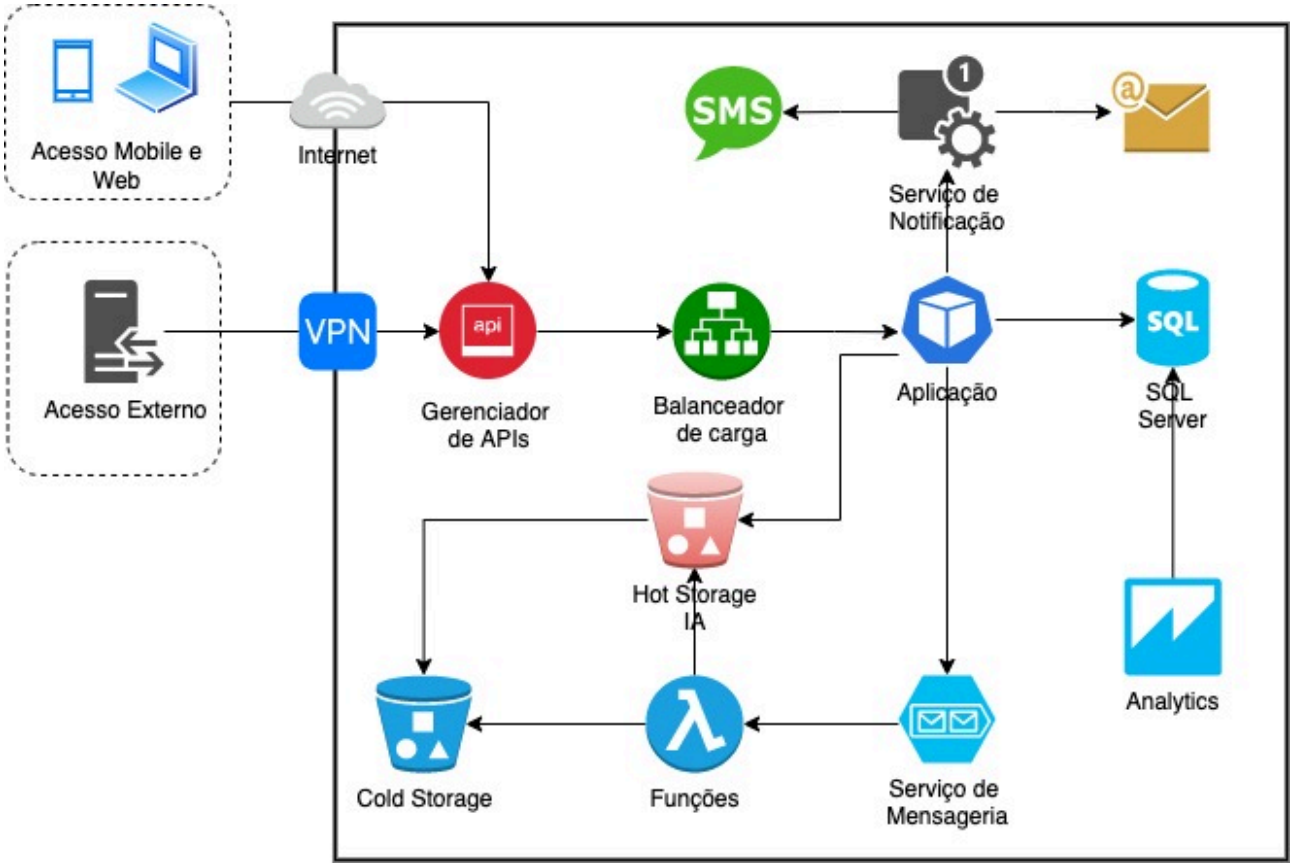


Figura 1: Arquitetura de referência

5.1 Principais componentes da arquitetura

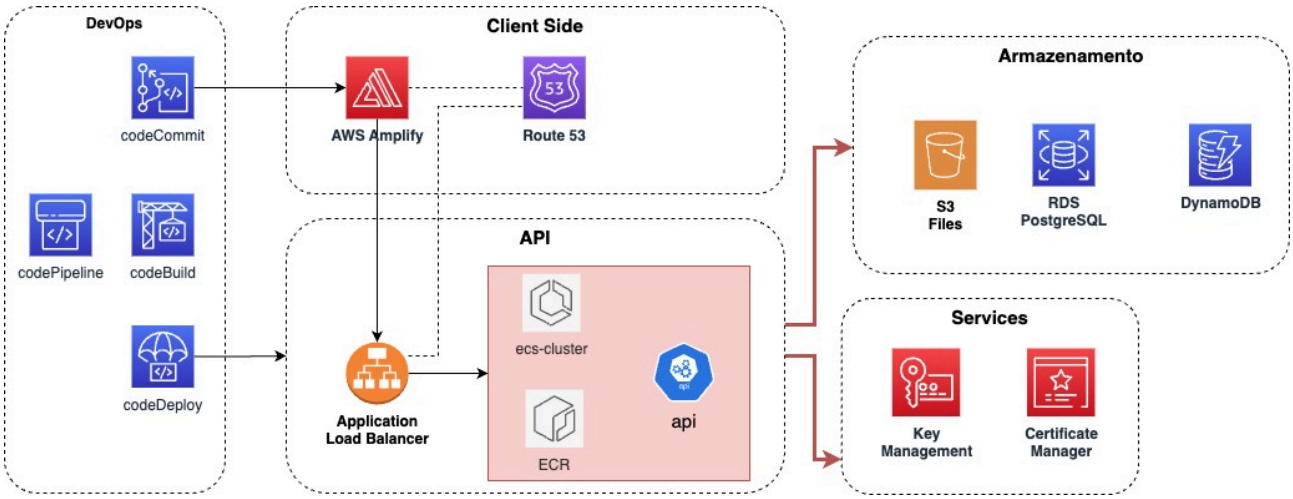
1. **Gerenciador de API** que serve de ponto único de acesso e exposição dos serviços;
2. **Balanceador de Carga** das aplicações disponibilizadas através de containers;
3. **Banco de Dados PostgreSQL gerenciado**;
4. **Ecossistema de orquestração de containers**, Kubernetes (https://kubernetes.io/);
5. **Hot Storage IA**: Armazenamento de objetos quente com acesso infrequente;
6. **Cold Storage IA**: Armazenamento de objetos frio;
7. **Funções como serviço**;
8. **Serviço de mensageria** para funções assíncronas da solução;
9. **Serviço de notificação** para envio de SMS e e-mail por parte da aplicação;
10. **Analytics**: Ferramenta para consultas e extração de insights em cima dos dados da solução;
11. **Web Application Firewall**: Proteção para aplicações Web ou APIs contra bots e exploits comuns na Web que podem afetar a disponibilidade da aplicação;
12. **Anti-DDoS**: Serviço de monitoramento que detecta ataques volumétricos na rede, separando o tráfego legítimo do ilícito;

Dos componentes listados, o orquestrador de containers, o Firewall e o banco de dados serão instanciados na construção do ambiente, os demais componentes são acionados e tarifados de acordo com uso dos mesmos.

8. Arquitetura de Implantação no AWS

Figura 2: Arquitetura no AWS

A. Componentes da solução



• Região: Leste dos EUA (Ohio) - us-east-2

• Availability Zone: Os principais componentes da solução possuem a seguinte configuração de AZs:

- O ambiente de orquestração de containers permeará em duas ou mais AZs, a depender da quantidade de nós necessárias (em um primeiro momento serão dois nós)
- O Banco de Dados será instanciado em somente uma AZ.

B. Organização de Recursos: Serão criadas diversas Tags para identificar e organizar os recursos da solução.

- Nome
- Versão
- Ambiente: Homologação e Produção;
- Status: Em Testes; Em produção; Em manutenção;

C. Rede virtual (Amazon Virtual Private Cloud - VPC): Cada ambiente possuirá uma rede virtual que englobará toda a estrutura de rede necessária para instanciar o projeto.

Componentes a serem instanciados na VPC

1. **Subnet Público:** Segmento de rede alocado para expor os serviços para os usuários e servidor de proxy com a Internet para serviços que necessitem acesso a sites externos;
2. **Subnet Privadas:** Segmento de rede alocado para hospedar o Banco de Dados e a Aplicação WEB;

3. **NAT Gateway:** Componente que visa o acesso possibilitar os serviços criados nas redes privadas acessar e realizar downloads de artefatos provenientes da Internet:
    - **Volume estimado de Data Transfer Out para a Internet:** 50GB/mês. **Obs.:** valores arbitrados, pois não foram informados pelo cliente.
    - **Volume estimado de Data Transfer Out intra VPC:** 200GB/mês. **Obs.:** valores arbitrados, pois não foram informados pelo cliente.

4. **Internet Gateway**: Gateway de roteamento das requisições provenientes da internet para os serviços expostos da solução;
5. **Serviço de Balanceamento de Carga**
    - **Application Load Balancer (ALB):** Um (1) balanceador single-az.

D. Serviço de Segurança

A solução de segurança projetada passa pela premissa que o acesso às aplicações e serviços será feito por um conjunto de máquinas limitado, ou seja, os IPs de origem das requisições serão previamente conhecidos pelos projetistas da solução em nuvem. Desta forma, teremos duas camadas de segurança: Um Web Application Firewall (AWS WAF) que será instanciado na frente do API Gateway de forma a filtrar as requisições por IP de origem, além disso todos os recursos instanciados devem pertencer a Security Groups, os quais funcionam como firewalls virtuais e que também vão filtrar os IPs, criando assim uma segunda camada de segurança.

O uso do WAF e do *Security Group (SG)* é totalmente transparente para os atores que acessam a API do projeto, necessitando somente da liberação do IP nos filtros do WAF e nas regras do tipo *inbound dos SGs.*

O AWS Shield também estará habilitado nos serviços expostos do projeto, este é um serviço gerenciado de proteção contra DDoS (Negação de serviço distribuída).

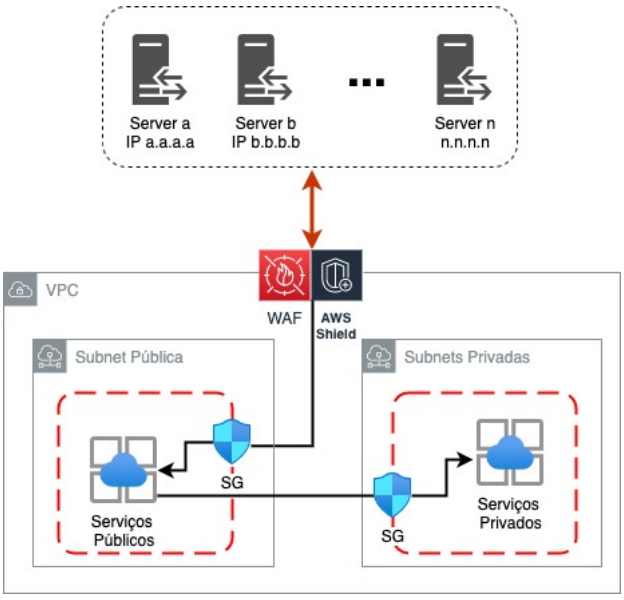


Figura 3 - Segurança dos serviços

Já a nível de aplicação, o acesso a mesma se dá através de TOKENS JWT devidamente criptografados e que são gerados através de serviços de autenticação com login e senha.

E. Serviços de Monitoramento

AWS Cloud Watch: Fornece dados e insights para monitorar aplicativos, responder às alterações de desempenho, otimizar a utilização de recursos e obter uma visualização unificada da integridade operacional.

- Estimado: 10 Métricas
- Armazenamento de logs: 5GB
- Dashboards: 1

F. Serviço de Computação

1. Amazon EC2 - Entreposto
   - Tipo: t3.small – 2 vcpu / 2GB Ram / Disco SSD-GP2 30GB
   - Quantidade: 1
   - Modelo de contratação: Sob Demanda

2. Amazon EKS
   - Quantidade: 1
   - Modelo de contratação: Sob Demanda

3. Amazon EC2 - Nós de Workloads do clister EKS
   - Tipo: m5.large – 4 vcpu / 16GB Ram / Disco SSD-GP3 100GB
   - Quantidade: 2
   - Modelo de contratação: Sob Demanda

4. Amazon ECR: Repositório de Imagens
   - Armazenamento: 5 GB

5. Funções Lambda
   - Solicitações por mês: 100.000
   - Duração de cada solicitação: 5 segundos
   - Memória Alocada: 128 MB
   - Modelo de contratação: Sob Demanda

6. Amazon SQS: Filas de movimentação de registros para discos
   - Solicitações por mês: 1.000.000
   - Modelo de contratação: Sob Demanda

7. Amazon SNS: Serviço de notificação Email
   - Solicitações por mês: 100.000
   - Tipo: e-mail
   - Modelo de contratação: Sob Demanda

G. Serviços de Armazenamento

1. Banco de dados PostgreSQL no RDS
   Tipo: db.m5.xlarge – 4 vcpu / 16 GB Ram

Armazenamento: 1 TB
Backup: 1 TB
Quantidade: 1 (Single AZ)
Modelo de contratação: Sob Demanda

2. Armazenamento de objetos: S3 - Infrequent Access ou Glacier
   Armazenamento: 15 TB
   Modelo de contratação: Sob Demanda

7. Estratégia de Backup

Todo o ambiente de datacenter em nuvem é instanciado no modelo IaC(Infrastructure as Code). Sendo assim, todo este ambiente tem versionamento de seu código mantido e historiado no SCM-GIT(source control management) e sistema de arquivos S3, permitindo assim a qualquer momento e necessidade o re-provisionamento automático do ambiente em seu último estado versionado.

Conforme o item de 6.G Serviços de Armazenamento, o serviço de banco de dados gerenciado pelo cloud-provider, ao ser instanciado este já provê regularidade de backup de dados armazenados, podendo até mesmo este backup ser em zona de nuvem diferente da zona de instanciação do banco.

Toda a estratégia de backup redundante conta com os próprios serviços do cloud-provider. Caso se queira adotar redundâncias externas torna-se necessária a contratação de outro provider para redundância ou disponibilização de storages on-promisse.