Relatório Técnico

Grupo 8

Enzo Quental

Gustavo Pacheco

Sérgio Ramella

1. Introdução

Este relatório descreve detalhadamente a implementação de um ambiente seguro na AWS para hospedar um ambiente de desenvolvimento e testes escalável. O projeto foi realizado utilizando o Terraform para garantir a infraestrutura como código, proporcionando consistência, reprodutibilidade e facilidade de gerenciamento.

---

2. Descrição da Arquitetura do Sistema

A arquitetura do sistema foi projetada para isolar componentes críticos e seguir as melhores práticas de segurança na nuvem AWS. Os principais elementos da arquitetura incluem:

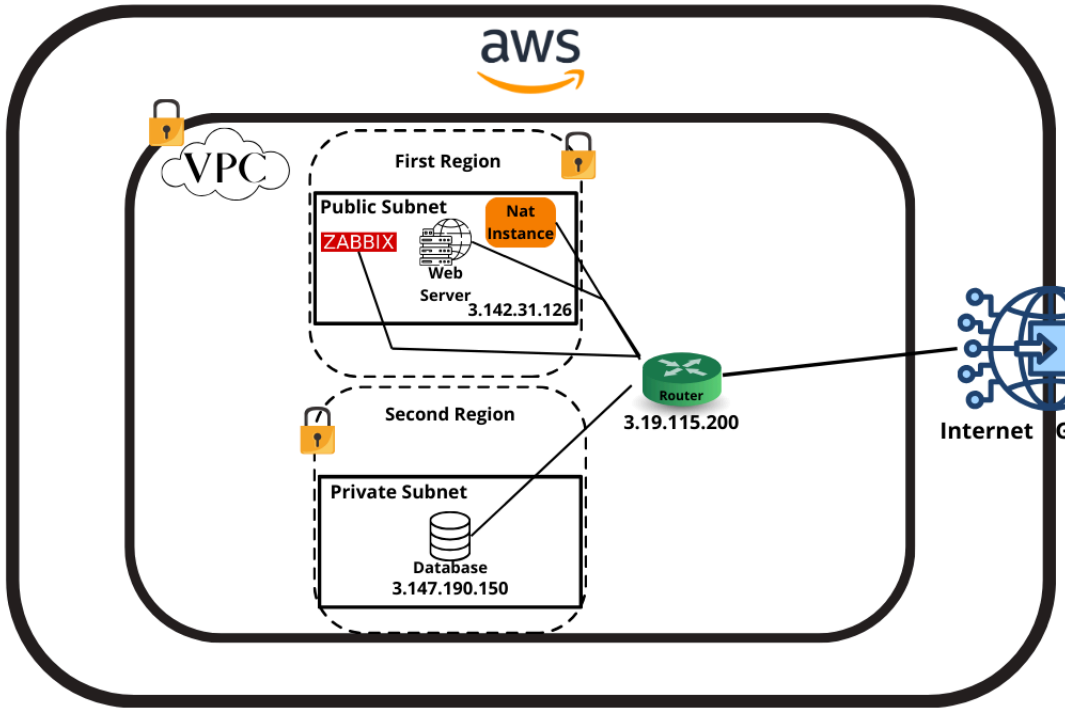
- **VPC (Virtual Private Cloud):**
  - Criamos uma VPC dedicada para o projeto, permitindo o controle total sobre o ambiente de rede virtual, incluindo a seleção de intervalos de endereços IP, criação de sub-redes e configuração de tabelas de rotas.
- **Sub-redes (Subnets):**
  - **Sub-rede Pública:** Criada em uma região específica (por exemplo, us-east-1a), esta sub-rede hospeda a instância de desenvolvimento que requer acesso à internet pública para atualizações, downloads de pacotes e outras interações externas.
  - **Sub-rede Privada:** Localizada em outra região (por exemplo, us-east-1b), esta sub-rede hospeda as instâncias do banco de dados e do Zabbix. Por estarem em uma sub-rede privada, essas instâncias não são acessíveis diretamente da internet, aumentando a segurança.
- **Instâncias EC2:**
  - **Instância de Desenvolvimento (Pública):** Uma instância EC2 T3.micro executando o Ubuntu, configurada para permitir que os desenvolvedores acessem e trabalhem no ambiente de desenvolvimento. Ela possui um Elastic IP associado para facilitar o acesso.

    - **Instância de Banco de Dados (Privada):** Uma instância EC2 T3.micro executando o Ubuntu, dedicada ao banco de dados. Por estar em uma sub-rede privada, é protegida contra acesso direto da internet. A comunicação com esta instância é feita apenas a partir da instância de desenvolvimento e do Zabbix.
    - **Instância do Zabbix (Privada):** Uma instância EC2 T3.micro executando o Ubuntu, responsável pelo monitoramento do ambiente. O Zabbix foi configurado para realizar conexões passivas, monitorando as outras instâncias e coletando métricas de desempenho e disponibilidade.
- **Security Groups:**
    - Criamos três Security Groups distintos, um para cada instância, para controlar o tráfego de rede de entrada e saída. Cada Security Group possui regras específicas que definem quais portas e protocolos são permitidos e de quais fontes.
- **Elastic IPs:**
    - Cada instância recebeu um Elastic IP para garantir endereços IP públicos estáveis, evitando a necessidade de atualizar configurações após reinicializações ou recriações das instâncias.

---

3. Diagrama de Arquitetura

A arquitetura projetada para o ambiente seguro e escalável na AWS está representada no diagrama abaixo. Ele descreve a organização dos recursos dentro da VPC (Virtual Private Cloud) e destaca as camadas de segurança implementadas, com o uso de Security Groups para proteger cada instância de forma granular. Esta configuração segue as melhores práticas de segurança e isolamento de recursos na nuvem AWS.



Custom Route Table

destination	target
10.0.0.0/16	local
0.0.0.0/0	igw-id

Main Route Table

destination	target
10.0.0.0/16	local
0.0.0.0/0	nat-instance-id

Descrição do Diagrama

1. **VPC (Virtual Private Cloud):**
    - A VPC foi configurada com o intervalo de endereços IP **10.0.0.0/16**, permitindo a criação de sub-redes para diferentes funções. Esta rede virtual fornece o isolamento necessário para hospedar instâncias em um ambiente seguro.
2. **Sub-redes:**
    - **Sub-rede Pública (First Region):**
        - Hospeda o **Web Server** e a **NAT Instance**, ambos acessíveis pela Internet, mas protegidos por regras de **Security Groups**.
        - O **Web Server**, com o IP público **3.142.31.126**, serve como ponto de entrada para o ambiente, permitindo acesso via HTTP/HTTPS (portas 80 e 443) e SSH (porta 22) apenas de IPs autorizados.
        - A **NAT Instance**, com o IP público **3.19.115.200**, fornece acesso à Internet para recursos localizados na sub-rede privada, como o banco de dados e o Zabbix.
    - **Sub-rede Privada (Second Region):**
        - Contém o **Database Server**, protegido contra acesso direto à Internet.
        - O banco de dados, com o IP privado **3.147.190.150**, é acessível apenas por tráfego interno autorizado, como do Web Server e do Zabbix, usando a porta 3306.
3. **Segurança e Isolamento:**
    - Cada instância está associada a um **Security Group** que define regras específicas de entrada (Inbound) e saída (Outbound), representadas graficamente por ícones de cadeado no diagrama:
        - **Web Server:** Permite acesso via SSH apenas de IPs autorizados e tráfego HTTP/HTTPS de qualquer origem.
        - **NAT Instance:** Permite tráfego de saída para a Internet, garantindo que os recursos privados tenham conectividade externa segura.
        - **Database Server:** Permite tráfego somente do Web Server e do Zabbix na porta 3306, restringindo qualquer outro tipo de acesso.
    - O uso de Security Groups garante que o ambiente seja isolado e seguro contra acessos não autorizados.
4. **Internet Gateway:**
    - Conectado à sub-rede pública, o **Internet Gateway** permite que o tráfego da VPC seja roteado para a Internet. Isso é essencial para os recursos que precisam de conectividade externa, como atualizações de software.
5. **Tabelas de Roteamento:**
    - **Tabela de Roteamento Pública:**
        - Associada à sub-rede pública, direciona o tráfego para o **Internet Gateway** para conectividade externa.
    - **Tabela de Roteamento Privada:**
        - Associada à sub-rede privada, direciona o tráfego para a **NAT Instance**, permitindo que os recursos privados acessem a Internet de forma segura e controlada.
6. **Monitoramento com Zabbix:**

- O **Zabbix Server**, hospedado na sub-rede pública, foi configurado para monitorar o Web Server e o banco de dados. Ele coleta métricas como uso de CPU, memória e disco, além de verificar a disponibilidade de serviços essenciais. Todo o tráfego do Zabbix para os recursos monitorados é protegido por regras específicas nos Security Groups.

---

4. Código Fonte Utilizado para a Configuração da Infraestrutura

Utilizamos o Terraform para definir a infraestrutura como código. O código está organizado em arquivos que declaram os recursos necessários:

- **Arquivo `main.tf`:**
  - Define o provedor AWS e recursos principais como VPC, sub-redes e tabelas de rotas.
- **Arquivo `variables.tf`:**
  - Configura variáveis para maior flexibilidade, como região, tipo de instância e IPs autorizados.
- **Arquivo `outputs.tf`:**
  - Declara saídas importantes, como IPs públicos e privados das instâncias.

O código completo está disponível no repositório do GitHub do projeto.

5. Configuração dos Security Groups

Os Security Groups foram configurados para proteger os recursos da infraestrutura ao controlar estritamente o tráfego de entrada e saída. Abaixo estão os detalhes de cada um:

- **Development Security Group (sg-0c50a8cd423f3fbd1)**
  - **Portas abertas:**
    - **22 (SSH):** Permite acesso SSH para administração da instância.
    - **10050 (Zabbix Agent):** Permite comunicação com o Zabbix Server para coleta de dados de monitoramento.
  - **Regras de origem:** Apenas IPs autorizados (como o do Zabbix Server) podem acessar estas portas.

- **Zabbix Security Group (sg-0b60d371a1f6a10b0)**
  - **Portas abertas:**
    - **22 (SSH):** Permite administração remota da instância Zabbix Server.
    - **80 (HTTP):** Permite acesso à interface web do Zabbix.
    - **10051 (Zabbix Server):** Permite comunicação do Zabbix Server com os agentes configurados nas instâncias monitoradas.
  - **Regras de origem:** IPs da infraestrutura e administradores autorizados.

- **Database Security Group (sg-004ba8059b27dd087)**
    - **Portas abertas:**
        - **3306 (MySQL):** Permite conexão ao banco de dados apenas a partir das instâncias autorizadas, como o Zabbix Server e a instância Development.
    - **Regras de origem:** Restrito a IPs internos da VPC.

---

6. Monitoramento com Zabbix

A instância do Zabbix foi configurada para monitorar as outras duas instâncias (desenvolvimento e banco de dados) através de conexões passivas:

- **Configuração do Zabbix Server:**
    - Instalamos o Zabbix Server na instância privada.
    - Configuramos o Zabbix para coletar dados das instâncias monitoradas usando agentes Zabbix instalados nelas.
- **Agentes Zabbix nas Instâncias Monitoradas:**
    - Instalamos o Zabbix Agent nas instâncias de desenvolvimento e banco de dados.
    - Configuramos os agentes para permitir conexões do Zabbix Server.
- **Itens Monitorados:**
    - Utilização de CPU, memória e disco.
    - Status de serviços essenciais.
    - Disponibilidade e tempo de resposta.
- **Gráficos e Alertas:**
    - Criamos gráficos para visualizar tendências de desempenho.
    - Configuramos triggers para alertar em caso de anomalias ou falhas.

---

7. Elastic IPs para Estabilidade de Endereçamento

Cada instância recebeu um Elastic IP para:

- **Consistência nos Endereços IP:**
    - Garantir que o endereço IP público das instâncias não mude, mesmo após reinicializações ou recriações.
- **Facilidade de Gerenciamento:**
    - Evitar a necessidade de atualizar configurações de acesso ou monitoramento devido a alterações de IP.
- **Acesso Simplificado:**
    - Facilitar conexões SSH e outras interações que dependem de endereços IP estáveis.

---

8. Conclusão

A implementação realizada atende aos requisitos estabelecidos para o Conceito C:

- **Isolamento de Recursos:**
  - As instâncias de desenvolvimento, banco de dados e monitoramento estão devidamente isoladas, garantindo segurança e desempenho.
- **Configurações de Segurança:**
  - Security Groups cuidadosamente configurados controlam o tráfego de rede, permitindo apenas o acesso necessário.
- **Monitoramento Efetivo:**
  - O Zabbix fornece visibilidade sobre o ambiente, permitindo a detecção proativa de problemas.
- **Infraestrutura como Código:**
  - O uso do Terraform assegura que a infraestrutura seja facilmente replicável e gerenciável.

---

9. Referências

- **Repositório do GitHub:**
  - O código fonte completo e a documentação adicional estão disponíveis no repositório do projeto no GitHub.