Laboratório
SysAdmin

Momento 1

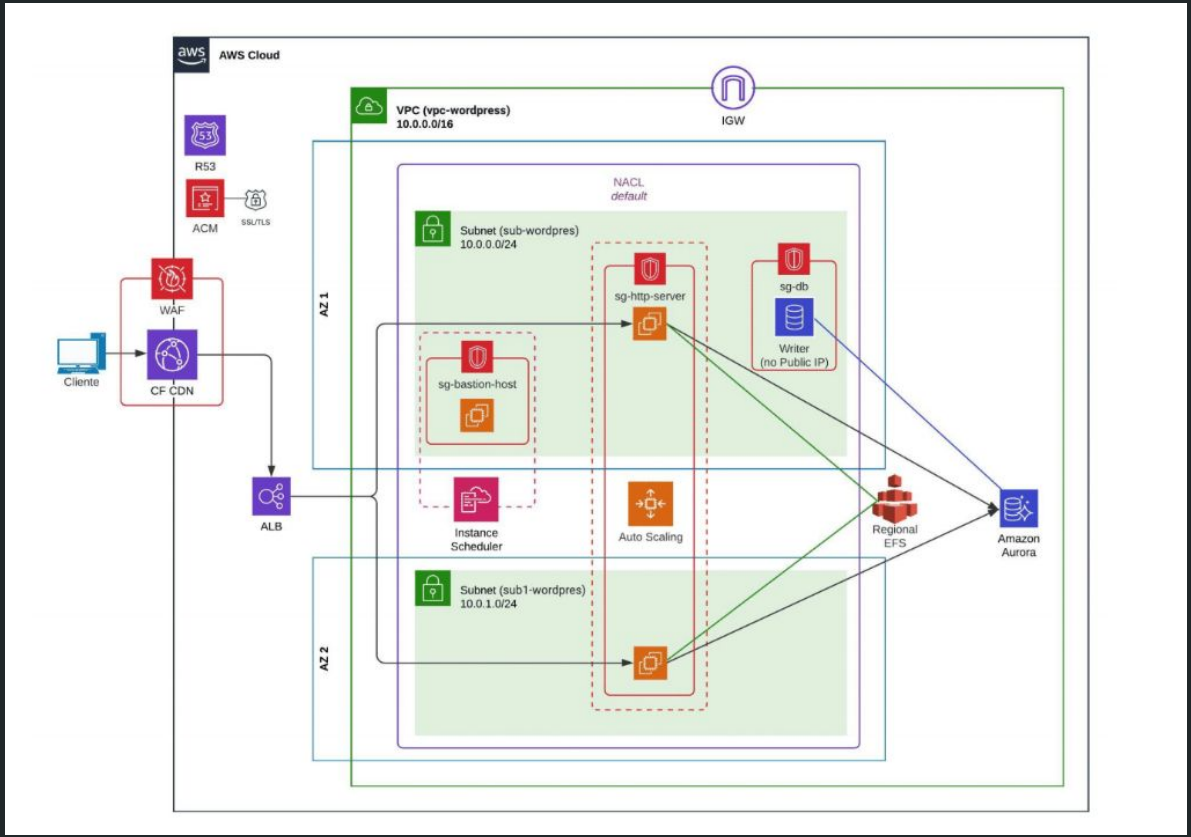
Davi Miranda Macedo Tavares
davi.miranda@datarain.com.br
+55 (84) 98822-6953

v1.0

SUMÁRIO

Arquitetura

Arquitetura



IAM

IAM

Política de senha

Password policy

This AWS account uses the following default password policy:

- Minimum password length is 8 characters
- Include a minimum of three of the following mix of character types: uppercase, lowercase, numbers, and ! @ # $ % ^ & * ( ) _ + - = [ ] { } | '
- Must not be identical to your AWS account name or email address

IAM

Política de MFA

Forçar o uso do MFA para o IAM User

1. O usuário deve ser capaz de gerenciar seu próprio MFA device;
2. Deve ser bloqueada qualquer operação do IAM user se seu MFA device não estiver configurado.

IAM

IAM User

Criar um IAM User

1. O usuário criado deve apenas ter a permissão de gerenciamento do MFA device previamente mencionada;
2. Ele, por si só, não deve ter nenhuma outra permissão atrelada a ele ou ao seu grupo.
3. Criar dois usuários, um administrador e um comum.

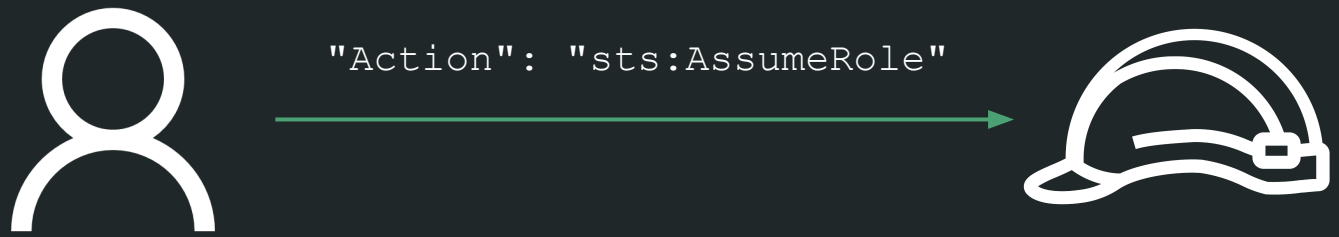
IAM

IAM Role

Criar uma IAM Role

1. Criar duas roles: uma para ser assumida pelo seu usuário SSO e o IAM User administrador, e outra para ser assumida pelo IAM User comum;
2. A role deve conter as permissões necessárias para o usuário operar;
3. O tempo de operação da role deve ser de 4 horas.

IAM User e Role



IAM

IAM User e Role

```
{
  "Credentials": {
      "AccessKeyId": "",
      "SecretAccessKey": "",
      "SessionToken": "",
      "Expiration":
"2022-04-01T16:55:08+00:00"
  },
  "AssumedRoleUser": {
    "AssumedRoleId": "",
      "Arn": ""
  }
}
```

Redes

Redes

Topologia de rede

Criar uma VPC

1. Apagar a VPC default;
2. Criar uma VPC na região N. Virginia (us-east-1);
3. A VPC deve ter como bloco CIDR 10.0.0.0/16;
4. Habilitar DNS hostnames e DNS resolution.

Redes

Topologia de rede

Criar 6 subnets

1. Configurar 3 subnets públicas (10.0.{10,11,12}.0/24) balanceadas nas zonas us-east-1{a,b,c};
2. Configurar 3 subnets privadas (10.0.{0,1,2}.0/24) balanceadas nas zonas us-east-1{a,b,c};

Redes

Regras de segurança

Criar NACL para as subnets públicas e privadas

1. A subnet pública deve ter um NACL permitindo inbound externo;
2. A subnet privada não pode ter inbound externo;
3. As regras devem apenas permitir o necessário.

Redes

Regras de segurança

Criar security groups

1. Configurar um security group para o Bastion Host;
2. Configurar um security group para o Load Balancer externo;
3. Configurar dois security groups para os Application Servers: um para a aplicação em si, outro para acesso SSH pelo Bastion Host;
4. Evitar usar IP source, mas ID de outros security groups como source;
5. As regras devem permitir apenas o necessário.

Servidores

Servidores

Bastion Host

Criar um Bastion Host

1. Configurar uma EC2 como Bastion Host;
2. Ele deve estar na zona us-east-1c;
3. A partir dela deve ser acessada a rede interna;
4. Deve ser configurado um CloudWatch alarme com auto-recovery da instância usando a métrica *StatusCheckFailed_System*;
5. Forçar o IMDSv2;
6. Criar e associar um instance profile para listar as instâncias.

Servidores

Application Server

Criar dois Application Servers

1. Deverá ser configurado dois application servers;
2. Eles devem estar balanceados nas zonas us-east-1{a,b};
3. Deve ser configurado um CloudWatch alarme com auto-recovery da instância usando a métrica *StatusCheckFailed_System*;
4. Forçar IMDSv2.

Servidores

Application Server

Criar dois Application Servers

5. O User data deve expor o domínio “lab-sysadmin.belinelo.com.br” com o endpoint “/“ retornando o header “X-Private-IP” com o IP da instância;
6. No mesmo domínio, o endpoint “/metrics” deve servir um arquivo com:
    a. Timestamp;
    b. Uso de CPU, Memória RAM, SWAP e disco;
    c. Quantidade de tasks rodando no momento.
7. O arquivo do “/metrics” deverá ser atualizado (incremento) a cada 5 minutos com as novas métricas.

Servidores

Application Server

Criar dois Application Servers

8. Configurar o domínio default para servir apenas o endpoint “/health”.

Servidores

Load Balancer

Criar um Load Balancer

1. Criar um load balancer para os dois application servers;
2. Health check configurado para o endpoint “/health”.