



Cloud Treinamentos

# Oficina de Projetos 8



## Proposta Técnica

---

# **Proposta Técnica de Migração da Plataforma TeamPass para a Cloud AWS**

**Cliente:** Upper Med  
**Local:** São Paulo - SP  
**Data:** 09/02/2023

**Proposta:** 132548-x

Versão: V2

1. Propriedade
2. Institucional
  - 2.1 Quem é a Cloud Solução ?
3. Implantação
  - 3.1 Escopo
  - 3.2 Cenário atual
4. Proposta Técnica
  - 4.1 Arquitetura Proposta
  - 4.2 Requisitos da Aplicação
  - 4.3 Cronograma de Execução
  - 4.4 Custos de implantação (AWS)
  - 4.4 Proposta Comercial
5. Serviços AWS
  - 5.1 VPC e Sub Redes
  - 5.1 Tabela de Rotas
  - 5.2 Network ACLs
  - 5.2 Security Groups
  - 5.3 Internet Gateway
  - 5.4 Amazon ELB (Elastic Load Balancer)
  - 5.5 Target Group
  - 5.5 Amazon Route 53
  - 5.6 Amazon WAF
  - 5.7 Amazon Auto Scaling
  - 5.9 Amazon Certificate Manager
  - 5.10 EFS (Amazon Elastic File System)
  - 5.11 Amazon CloudWatch
  - 5.12 Amazon SNS ( Simple Notification Service )
  - 5.13 Amazon IAM (Identify and Access Management)
  - 5.15 Instâncias EC2 ( Elastic Compute Cloud )
  - 5.16 AWS Lambda
  - 5.17 Secret Manager
6. Terraform
7. Teste de Stress
8. TeamPass em Execução

9. Docker

10. Contas AWS - Organização

11. Integrantes do Grupo 3

# 1. Propriedade

## Restrições de Uso e Divulgação da Proposta (NDA)

As informações contidas em todas as folhas desta proposta são confidenciais, sejam elas técnicas, financeiras ou comerciais. As informações fornecidas à **Upper Med** não podem ser usadas ou divulgadas sem prévia autorização da **Cloud Solução** para propósitos que não sejam os de avaliação da proposta.

Da mesma forma, a **Cloud Solução** compromete-se a não divulgar ou fornecer dados e informações referentes aos fornecimentos realizados, a menos que expressamente autorizado pela **Upper Med**, mantendo absoluta confidencialidade em relação às atividades desenvolvidas.

As propostas da **Cloud Solução** poderão ser submetidas via e-mail e mídia eletrônica para sua conveniência. Se o conteúdo diferenciar entre as cópias impressas e o formato eletrônico, o conteúdo da impressa será garantido pela **Cloud Solução**.

# 2. Institucional

## 2.1 Quem é a Cloud Solução ?

Fundada em 2022 no Curso Especialista AWS e contando com colaboradores, altamente qualificados, a **Cloud Solução** é uma empresa com foco em soluções inovadoras e de alto valor agregado para Infraestrutura de Tecnologia da Informação que oferece ao mercado os melhores produtos, serviços gerenciados, soluções em nuvem (privada, pública ou híbrida) e consultoria.

Atuando em praticamente todo o território nacional, a **Cloud Solução** é reconhecida pela experiência em projetos de TI, pelo time de profissionais certificados e por uma oferta completa de hardware, software e serviços que atendem às principais necessidades de tecnologia em seus clientes de todos os portes e segmentos, contribuindo decisivamente para o aumento da eficiência

operacional e para a redução de custos e de riscos através de soluções inteligentes e customizadas.

A **Cloud Solução**, é uma das maiores integradoras de soluções em TI do Brasil, está pronta para ajudar a sua empresa a enfrentar seus desafios de negócios e os impactos gerados pela *"TRANSFORMAÇÃO DIGITAL"*.

## 3. Implantação

### 3.1 Escopo

O objetivo deste projeto é realizar a criação de uma infraestrutura em cloud AWS como foi realizada com o sistema MediaWiki, tendo em vista centralizar todos os sistemas utilizados pela TI da UpperMed e consequentemente diminuindo recursos on-premise.

No intuito de resolver os problemas supracitados e de segurança, foi proposta uma arquitetura moderna em AWS onde iremos resolver problemas de indisponibilidade do gerenciador de senhas e prover flexibilidade no acesso às credenciais.

### 3.2 Cenário atual

Segundo o gerente de TI da UpperMed, o objetivo da migração é centralizar todos os sistemas utilizados pela TI na AWS, diminuindo assim recursos on-premise e utilizando cada vez mais Cloud. Além deste objetivo, a empresa busca resolver problemas de indisponibilidade do gerenciador de senhas e também prover mais flexibilidade no acesso às credenciais deste gerenciador.

O problema de indisponibilidade é devido a máquina virtual que comporta a solução estar com poucos recursos de memória e processador, fazendo com que a VM trave ou tenha alguns períodos de lentidão. E a questão da flexibilidade é porque quando é necessário fazer algum atendimento local em alguma das lojas, se o funcionário da TI precisar consultar alguma credencial neste gerenciador, ele não consegue.

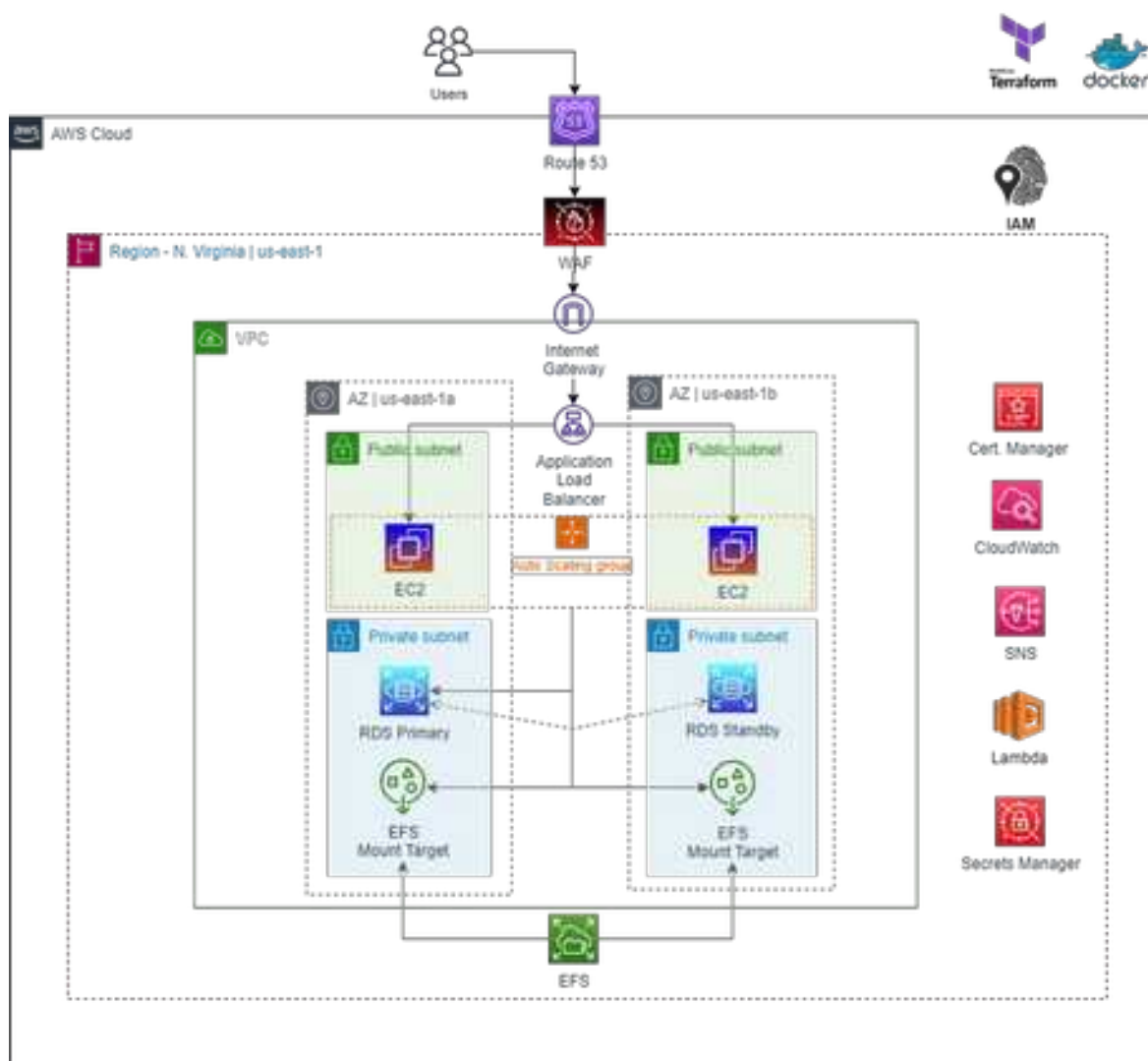
Atualmente o TeamPass está rodando em uma VM, com sistema operacional CentOS 7.0.1406. Possui 10 GB de memória RAM e 2 vCPU. O banco de dados é o MariaDB 10.1 e também está instalado nesta mesma VM. Utiliza como Web Server o Apache. O banco de dados consome 15 GB de armazenamento. O horário de

funcionamento do setor de TI é das 09:00 às 19:00 de segunda a sexta-feira e das 09:00 às 13:00 aos sábados.

## 4. Proposta Técnica

### 4.1 Arquitetura Proposta

A arquitetura proposta se baseia em nuvem utilizando recursos disponibilizados pela AWS (Amazon Web Services) visando garantir segurança, disponibilidade, velocidade e escalabilidade sob demanda. E para isso foi montado o diagrama a seguir.



### 4.2 Requisitos da Aplicação

- ☐ **Instância com servidor Linux Debian 11, Apache e PHP (7.4.3+)**



□ Banco de dados MariaDB

## 4.3 Cronograma de Execução



## 4.4 Custos de implantação (AWS)

Opção AWS - I



## Estimativa de custos mensais com AWS - I

Serviço	Descrição	Valor/dolar	Valor em R\$
AWS Web Application Firewall	WAF	16,00	83,20
Amazon EC2 - t3.micro	EC2	8,23	42,80
Amazon Elastic File System	EFS	18,03	93,76
Amazon RDS - db.t3.small	MariaDB	18,91	98,33
Amazon Route 53	Route 53	0,50	2,60
Elastic Load Balancing	ALB	16,43	85,44
Lambda		0,20	1,04
Secret Manager		0,45	2,34
<b>Total</b>		<b>78,75</b>	<b>409,50</b>

## Opção AWS - II

### Estimativa de custos mensais com AWS - II

Serviço	Descrição	Valor/dolar	Valor em R\$
AWS Web Application Firewall	WAF	16,00	83,20
Amazon EC2 - c6a.large	EC2	56,48	293,70
Amazon Elastic File System	EFS	18,03	93,76
Amazon RDS - db.m6i.large	MariaDB	131,43	683,44
Amazon Route 53	Route 53	0,50	2,60
Elastic Load Balancing	ALB	16,43	85,44
Lambda		0,20	1,04
Secret Manager		0,45	2,34
<b>Total</b>		<b>239,52</b>	<b>1.245,50</b>

## 4.4 Proposta Comercial

### Opção Gestão I

Proposta para Projeto AWS - I				
Item	Descrição	Valor/dolar	Valor em R\$	Pagamento
1	Projeto AWS - Com a migração do sistema	4.000,00	20.800,00	Único
2	Infraestrutura AWS *	78,75	409,50	Mensal
3	Treinamento de Gestão da Infra AWS	300,00	1.560,00	Único
4	Suporte Gestão da Infra AWS *	300,00	1.560,00	Mensal
5	<b>Investimento Total / Migração</b>	<b>4.678,75</b>	<b>24.329,50</b>	<b>10 x R\$ 2432,95</b>
6	<b>Investimento Mensal / Fixo (AWS+Gestão)</b>	<b>378,75</b>	<b>1.969,50</b>	<b>Mensal</b>
Custo 1 dolar = R\$ 5,20 em 08/02/2023		5,20		

### Opção Gestão II

Proposta para Projeto AWS - II				
Item	Descrição	Valor/dolar	Valor em R\$	Pagamento
1	Projeto AWS - Com a migração do sistema	4.000,00	20.800,00	Único
2	Infraestrutura AWS *	239,52	1.245,50	Mensal
3	Treinamento de Gestão da Infra AWS	300,00	1.560,00	Único
4	Suporte Gestão da Infra AWS *	300,00	1.560,00	Mensal
5	<b>Investimento Total/Migração</b>	<b>4.839,52</b>	<b>25.165,50</b>	<b>10 x R\$ 2.165,55</b>
6	<b>Investimento Mensal/Fixo (AWS+Gestão)</b>	<b>539,52</b>	<b>2.805,50</b>	<b>Mensal</b>
Custo 1 dolar = R\$ 5,20 em 08/02/2023		5,20		

**Implantação + Gestão (10x): R\$ 1924,90 / R\$ 2.805,50**

\*1 USD = 5,20 BRL - Cotação 08/02/23

Sujeito a taxas e impostos. <https://aws.amazon.com/pt/tax-help/Brasil/>

**Valores de Investimentos Aproximados!**

## 5. Serviços AWS

### 5.1 VPC e Sub Redes

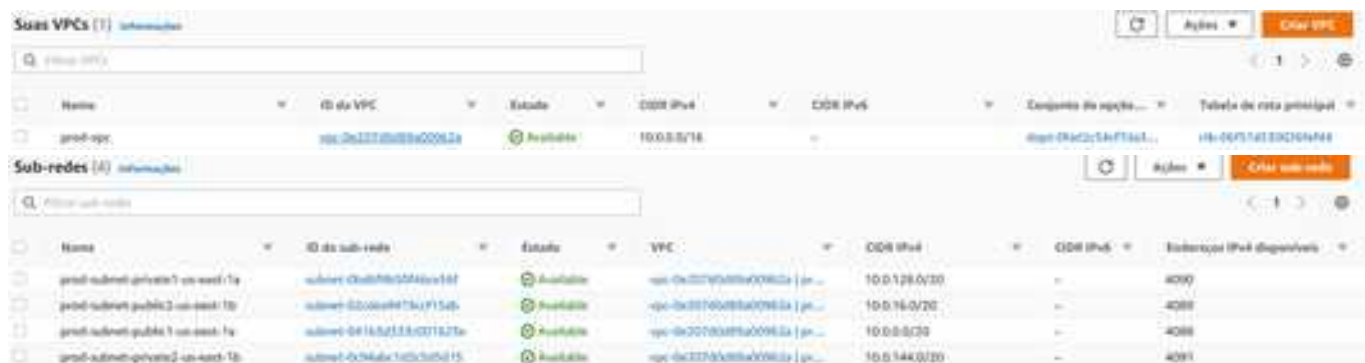
No projeto será utilizado 1 (uma) VPC contendo quatro sub-redes, onde duas são públicas e duas privadas. As instâncias EC2 ficarão nas sub-redes públicas, protegidas por firewall de borda e aplicação. As instâncias EC2 acessarão outros serviços da AWS, tais como o banco de dados MariaDB e o armazenamento elástico EFS, onde serão armazenados todos os arquivos atuais e futuros.

A VPC será criada na região da Virgínia, onde os custos dos serviços são menores, pois a aplicação não tem restrição de ser hospedada no Brasil e não tem demanda para baixa latência a ponto de precisar usar uma região em SP.

**Nome: prod-vpc**

**IPv4 CIDR: 10.0.0.0/16**

**Habilitamos o DNS hostnames e DNS Resolution**



The screenshot shows the AWS Management Console interface. The top section displays the 'prod-vpc' VPC with its ID 'vpc-0a33740d08ba00962a' and CIDR '10.0.0.0/16'. Below it, the 'Sub-redes' section lists four subnets:

Nome	ID da sub-rede	Estado	VPC	CIDR IPv4	CIDR IPv6	Endereço IPv4 disponível
prod-subnet-private1-us-east-1a	subnet-04b0f6c5d4a1a16f	Disponível	vpc-0a33740d08ba00962a   pr...	10.0.128.0/20	-	4090
prod-subnet-public2-us-east-1b	subnet-020a0e471ba1f15ab	Disponível	vpc-0a33740d08ba00962a   pr...	10.0.16.0/20	-	4088
prod-subnet-public1-us-east-1a	subnet-0e1652338c031827a	Disponível	vpc-0a33740d08ba00962a   pr...	10.0.8.0/20	-	4088
prod-subnet-private2-us-east-1b	subnet-0x74b4a1a1c3a0d15	Disponível	vpc-0a33740d08ba00962a   pr...	10.0.144.0/20	-	4091

### 5.1 Tabela de Rotas

As rotas foram definidas para atender à necessidade das subnets públicas e privadas, onde apenas a subnet pública tem acesso à internet.

Rota pública:

- A rota pública foi associada às subnets públicas.
- Na edição de rotas liberamos qualquer destino para o nosso internet gateway.

Rota privada:

- A rota privada foi associada às subnets privadas.

Tabelas de rotas (4) [Informações](#)

Q: Filtrar tabelas de rotas

Nome	ID da tabela de rotas	Associações explícitas	Associações de S...	Área...	VPC	ID da propriedade
+	rtb-009f1e032209f0f4	—	—	Sim	vpc-0a2070a0b0a0b0a0a / pr...	at1545465497
gmd-rfb-public	rtb-009f1e032209f0f4	2 sub-redes	—	Não	vpc-0a2070a0b0a0b0a0a / pr...	at1545465497
gmd-rfb-private2-us-east-1a	rtb-0a7194a72170a0a	subnet-0c3b0e1c315a...	—	Não	vpc-0a2070a0b0a0b0a0a / pr...	at1545465497
gmd-rfb-private1-us-east-1a	rtb-0a7194a72170a0a	subnet-0c3b0e1c315a...	—	Não	vpc-0a2070a0b0a0b0a0a / pr...	at1545465497

## 5.2 Network ACLs

Serão utilizados Network ACLs para fornecer uma camada de segurança em toda a VPC, controlando todo tráfego de entrada e saída das sub-redes. Uma *network access control list* (ACL) permite, ou nega, tráfego específico de entrada (*inbound*) ou saída (*outbound*) no nível de sub-rede. Você pode usar a ACL de rede padrão para sua VPC, ou pode criar uma ACL de rede personalizada para sua VPC com regras semelhantes às regras de seus grupos de segurança para adicionar uma camada adicional de segurança à sua VPC.

### ACL

#### Pública: acl-publica

Associamos na mesma as duas subnets públicas

Criamos regras de entrada (inbound rules) e saída (outbound rules) liberando o acesso HTTP e SSH para qualquer destino. Criamos regras de acesso à portas efêmeras 1024-65535 para se ter tráfego interno e externo aplicando tais regras para entrada e saída

#### Privada: acl-privada

Associamos na mesma as duas subnets públicas

Criamos regra de saída liberando todo o tráfego

Criamos regra de entrada liberando somente a faixa da VPC (10.1.0.0/16)

Network ACLs (1/1) [Informações](#)

Q: Filtrar Network ACLs

Nome	ID da Network ACL	Associada a	Política	ID da VPC	Contagem de regras de...	Contagem de regras...
+	acl-07b0411b0a0a0a0a	4 sub-redes	Sim	vpc-0a2070a0b0a0b0a0a / pr...	2 Regras de entrada	2 Regras de saída



The first screenshot shows the 'Ingress rules' (Regras de entrada) tab for security group sg-03e04115. It displays a table with two rules: Rule 100 (Allow all traffic) and Rule \* (Deny all traffic).

Número da regra	Tipo	Protocolo	Intervalo de portas	Origem	Permitir/negar
100	Tudo o tráfego	Tudo	Tudo	0.0.0.0/0	Allow
*	Tudo o tráfego	Tudo	Tudo	0.0.0.0/0	Deny

The second screenshot shows the 'Egress rules' (Regras de saída) tab for the same security group. It displays a table with two rules: Rule 100 (Allow all traffic) and Rule \* (Deny all traffic).

Número da regra	Tipo	Protocolo	Intervalo de portas	Destino	Permitir/negar
100	Tudo o tráfego	Tudo	Tudo	0.0.0.0/0	Allow
*	Tudo o tráfego	Tudo	Tudo	0.0.0.0/0	Deny

The third screenshot shows the 'Subnet associations' (Associações de sub-rede) tab for the security group. It displays a table with four associations to subnets in the us-east-1a availability zone.

Nome	ID da sub-rede	Associação	Zona de disponibilidade	10G IPv4	10G IPv6
prod-subnet-private-1-us-east-1a	subnet-0c3d78b0f94a73d0	sg-03e04115:sg-03e04115	us-east-1a	10.0.128.0/20	-
prod-subnet-private-2-us-east-1a	subnet-0c3d78b0f94a73d0	sg-03e04115:sg-03e04115	us-east-1a	10.0.144.0/20	-
prod-subnet-private-3-us-east-1a	subnet-0c3d78b0f94a73d0	sg-03e04115:sg-03e04115	us-east-1a	10.0.160.0/20	-
prod-subnet-public-1-us-east-1a	subnet-0c3d78b0f94a73d0	sg-03e04115:sg-03e04115	us-east-1a	10.0.0.0/20	-

## 5.2 Security Groups

Um grupo de segurança controla o tráfego que tem permissão para acessar e sair dos recursos aos quais está associado. Por exemplo, depois de associar um grupo de segurança a uma instância do EC2, ele controla o tráfego de entrada e saída da instância. Um grupo de segurança ou *security group* atua como firewall virtual para as instâncias do EC2 visando controlar o tráfego de entrada e de saída.

Criou-se um security group dentro da VPC para liberar acesso a instância Linux e com algumas regras específicas para a necessidade do cliente conforme pode ser conferido nas imagens abaixo.

**Grupos de segurança** (7) Automação

🔍 Filtrar grupos de segurança

🔄 Atões

Executar grupos de segurança para (0)

[Criar grupo de segurança](#)

Nome	ID do grupo de seg...	Nome do grupo de ...	ID da VPC	Descrição	Proprietário	Número de regras ...	Número de regras ...
sg-0b84b344f5a6b0c0	sg-postgres_rds	sg-postgres_rds	vpc-0a2c7d508b000962e	Somente RDS Postgres	415543465497	1 Entrada de permissão	1 Entrada de permissão
sg-035322a51c7f8a6a	default	default VPC security gr...	vpc-0a2c7d508b000962e	default VPC security gr...	415543465497	1 Entrada de permissão	1 Entrada de permissão
sg-0a40f3a1878f844e	sg_mysql_rds	Somente Maria DB	vpc-0a2c7d508b000962e	Somente Maria DB	415543465497	1 Entrada de permissão	1 Entrada de permissão
sg-01a6b0a2ff0a1989	sg_ssh	Somente SSH	vpc-0a2c7d508b000962e	Somente SSH	415543465497	1 Entrada de permissão	1 Entrada de permissão
sg-02713c3e51a0f1c3	sg_port_80	Somente Porta 80	vpc-0a2c7d508b000962e	Somente Porta 80	415543465497	1 Entrada de permissão	1 Entrada de permissão
sg-0b551d4a0c7f0b7a9	sg_port_443	Somente 443	vpc-0a2c7d508b000962e	Somente 443	415543465497	1 Entrada de permissão	1 Entrada de permissão
sg-0a0d834d62a42c207	sg_efs	Somente EFS	vpc-0a2c7d508b000962e	Somente EFS	415543465497	1 Entrada de permissão	1 Entrada de permissão

**sg-0a0d834d62a42c207 - sg\_efs**

[Atões](#)

**Detalhes**

Nome do grupo de segurança sg_efs	ID do grupo de segurança sg-0a0d834d62a42c207	Descrição Somente EFS	ID da VPC vpc-0a2c7d508b000962e
Proprietário 415543465497	Número de regras de entrada 1 Entrada de permissão	Número de regras de saída 1 Entrada de permissão	

[Regras de entrada](#) [Regras de saída](#) [Tags](#)

ⓘ Agora, você pode verificar a conectividade de rede com a Reachability Analyzer

[Executar Reachability Analyzer](#) ✕

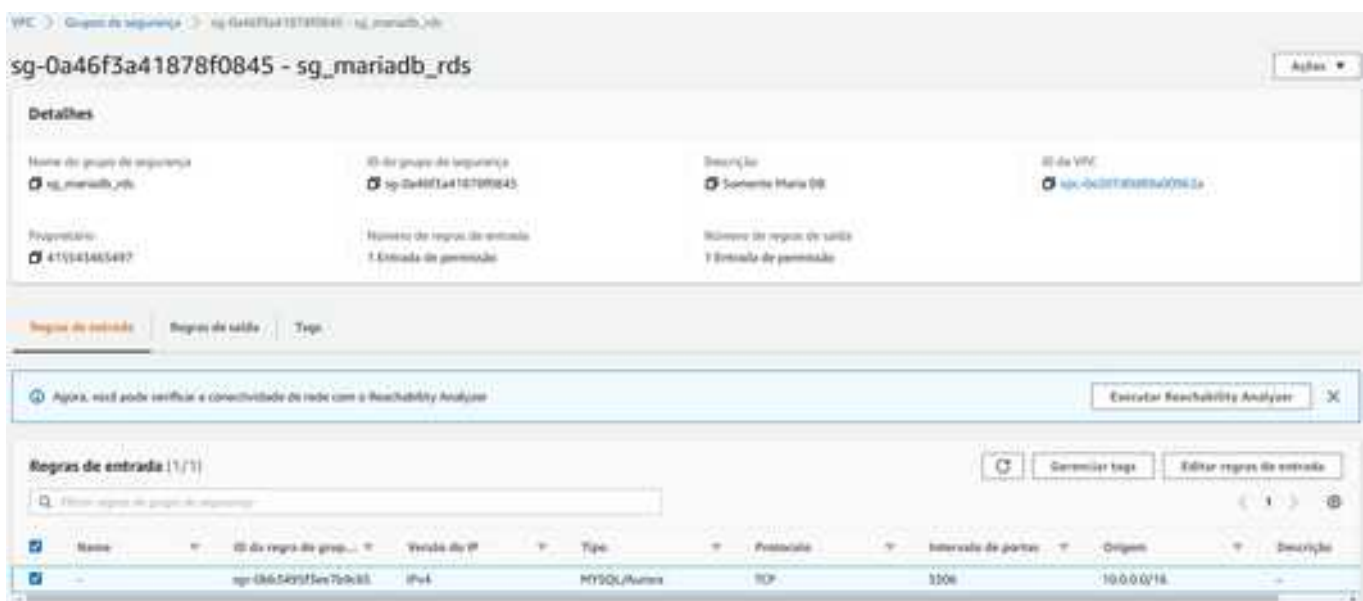
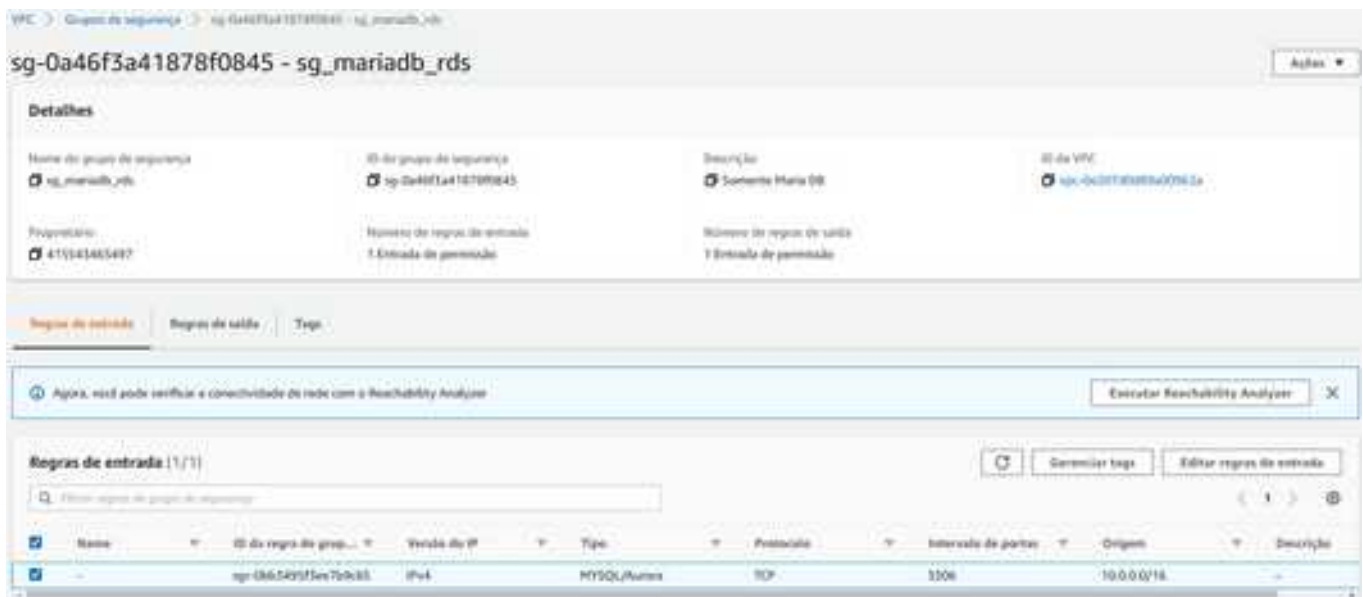
**Regras de entrada** (1/1)

🔍 Filtrar regras de grupo de segurança

🔄 Executar tags [Editar regras de entrada](#)

Nome	ID da regra de grupo...	Variação de IP	Tipo	Protocolo	Intervalo de portas	Origem	Descrição
sg-079993178b0b0c07	sg-079993178b0b0c07	IPv4	NFS	TCP	2049	10.0.0.0/16	





## 5.3 Internet Gateway

Internet Gateway é um componente da VPC horizontalmente dimensionado, redundante e altamente disponível que permite a comunicação entre a VPC e a Internet.

Se uma sub-rede estiver associada a uma tabela de rotas que tem o direcionamento para um gateway da Internet, ela é conhecida como sub-rede pública. Se uma sub-rede estiver associada a uma tabela de rotas que não tem um direcionamento para um gateway da Internet, ela é conhecida como sub-rede privada.

Foi criado um gateway de internet e associado à VPC para permitir acesso à internet, conforme imagem abaixo.

Gateways da internet (1/1) <small>Informações</small>					Ações		Colar gateway da internet
Filtre por nome do gateway da internet							
Nome	ID do gateway da Internet	Estado	ID da VPC	Proprietário			
prod-igw	igw-074b2a5d74407330b	Ativo	vpc-0a027d2a083a009c2a   prod-vpc	4155A5465497			

## 5.4 Amazon ELB (Elastic Load Balancer)

Amazon Elastic Load Balancer distribui automaticamente as requisições externas para as instâncias (servidores), mantendo o equilíbrio distribuindo a carga entre os servidores, monitorando a saúde das instâncias e aplicações que estiverem disponíveis no cluster no momento em que as requisições são recebidas. Seguem algumas imagens do load balancer aplicado, configurados para acesso por HTTP (80) e HTTPS (443).

EC2 > Load balancers

**Load balancers (1)**

O Elastic Load Balancing mede automaticamente a capacidade de seu balancer de carga em resposta a alterações no tráfego de entrada.

Filtre por nome do balancer de carga

Nome	Nome do DNS	Estado	ID da VPC	Zonas de disponibilidade	Tipo	Data criada
elb	elb-1688411498.us-east-1.elb.amazonaws.com (Registro A)	Ativo	vpc-0a027d2a083a009c2a	2 Zonas de disponibilidade subnet-02c0dc0d75a7f15ab us-east-1b (us-east-1a)	application	January 12, 2023, 10:17:37 UTC-05:00

**Detalhes**

arn:aws:elasticloadbalancing:us-east-1:4155A5465497:loadbalancer:app/027154c7a0d0e0140d

Tipo de balancer de carga Application	Nome do DNS elb-1688411498.us-east-1.elb.amazonaws.com (Registro A)	Status Ativo	VPC vpc-0a027d2a083a009c2a
Tipo de interface IP IPv4	Frequência Internet-facing	Zonas de disponibilidade subnet-02c0dc0d75a7f15ab us-east-1b (us-east-1a) subnet-04f165d555b007627e us-east-1a (us-east-1a)	Zona de disponibilidade us-east-1a (us-east-1a)
Data criada January 12, 2023, 10:17:37 UTC-05:00			

Links | Mapeamento de rede | Segurança | Monitoramento | Integrações | Atributos | Tags

**Listeners (2)**

Um receptor verifica se há solicitações de conexão em sua porta e protocolo, e o tráfego recebido pelo receptor é roteado de acordo com suas regras.

Procurar

Protocolo	Porta	ARN	Política de segurança	Certificado SSL padrão	Regra de roteamento padrão	Regras	Tags
HTTP (80)	80	ARN	Não aplicável	Não aplicável	1. Redirecione para HTTPS://elb-1688411498.us-east-1.elb.amazonaws.com - Código de status: HTTP_301		
HTTPS (443)	443	ARN	ELBSecurityPolicy-2016-08	aws-ssl-cloudfront-us-east-1	1. Avance para - target-grp (1.000%) - Permissibilidade em nível de grupo: Desativar		

Listeners

Mapeamento de rede

Segurança

Monitoramento

Integrações

Atributos

Tags

Mapeamento de rede

Informações

TargetGroup is the endpoint where traffic is routed. You can create a target group using the IP address or DNS.

Editar tipo de endereço IP

Editar sub-rede

VPC

vpc-6a307f8800a000000000000000000000

IPv4: 10.0.0.0/16

IPv6: -

Tipo de endereço IP

IPv4

Mapeamentos

Os endpoints são usados para rotear o tráfego para o endpoint de destino de acordo com o endereço IP ou o nome.

Zona	Sub-rede	Endereço IPv4	Endereço IPv4 privado	Endereço IPv6
us-east-1b (us-east-1a)	subnet-047f8800000000000000000000000000	Atribuído pela AWS	Atribuído do CIDR 10.0.0.0/20	Não aplicável
us-east-1a (us-east-1a)	subnet-047f8800000000000000000000000000	Atribuído pela AWS	Atribuído do CIDR 10.0.0.0/20	Não aplicável

## 5.5 Target Group

Cada grupo de destino é usado para rotear solicitações para um ou mais destinos registrados. Ao criarmos cada regra do listener, especificamos um grupo de destino e condições. Quando uma condição da regra é atendida, o tráfego é encaminhado para o grupo de destino correspondente. Podemos criar grupos de destino diferentes para tipos de solicitações diferentes. Por exemplo, podemos criar um grupo de destino para solicitações gerais e outros grupos de destino para solicitações para os micros serviços do aplicativo.

Definimos as configurações de verificação de integridade para o load balancer por grupo de destino. Após especificar um grupo de destino em uma regra para um listener, o load balancer monitora continuamente a integridade de todos os destinos registrados com o grupo de destino que estiverem em uma Zona de disponibilidade habilitada para o mesmo. O load balancer roteia solicitações para os destinos registrados que estão íntegros.

target-lb						Actions
<b>Detalhes</b> <a href="#">arn:aws:elasticloadbalancing:us-east-1:123456789012:targetgroup/target-lb/1234567890123456</a>						
Tipo de destino	Protocolo / Porta		Serviço do protocolo	VPC		
instância	HTTP: 80		HTTP	<a href="#">vpc-6a307f8800a000000000000000000000</a>		
Tipo de endereço IP	Load balancer					
IPv4						
Total de destinos	Integro	Não integro	Não confirmado	Inicial	Desconhecido	
1	1	0	0	0	0	
Destinos Monitoramento Verificação de integridade Atributos Tags						
<b>Destinos registrados (1)</b> <input type="text"/> <input type="button" value="Adicionar destino"/> <input type="button" value="Remover destino"/> <input type="button" value="Registrar destino"/>						
ID de instância	Nome	Porta	Zona	Status de integridade	Detalhes do status de integridade	
<a href="#">i-001172007f8800000000000000000000</a>	target-lb	80	us-east-1a	Healthy		



## 5.5 Amazon Route 53

O Amazon Route 53 é um serviço web *Domain Name System* (DNS) na nuvem, com nível muito alto de disponibilidade e escalável. Projetado para oferecer aos desenvolvedores e empresas um meio altamente confiável e econômico de direcionar os usuários finais aos aplicativos de Internet, convertendo nomes para endereços IP numéricos, usados pelos computadores para se conectarem entre si.

Publicação pelo domínio: [cloudsolucao.com.br](http://cloudsolucao.com.br)

Certificate Manager - DNS validation

Certificado que contempla os acessos abaixo: <http://teampass.cloudsolucao.com.br>



Route 53 > Zonas hospedadas > cloudsolucao.com.br

**cloudsolucao.com.br** [Info](#)

[Excluir zona](#) [Testar registro](#) [Configurar registro em log de consultas](#)

► Detalhes da zona hospedada [Editar zona hospedada](#)

[Registros \(4\)](#) [Assinatura DNSSEC](#) [Tags de zona hospedada \(0\)](#)

**Registros (4)** [Info](#)

O modo Automático é o comportamento de pesquisa atual pré-definido para obter os melhores resultados de filtro. Para alterar os modos, acesse as configurações.

[Excluir registro](#) [Importar arquivo de zona](#) [Criar registro](#)

Filtrar registros por propriedade ou valor

<input type="checkbox"/>	Nome do registro	Tipo	Política...	Difer...	Valor/rotar tráfego para
<input type="checkbox"/>	cloudsolucao.com.br	NS	Simple	-	ns-604.awsdns-11.net. ns-353.awsdns-43.com. ns-1799.awsdns-32.co.uk. ns-1415.awsdns-48.org.
<input type="checkbox"/>	cloudsolucao.com.br	SOA	Simple	-	ns-604.awsdns-11.net. awsdns-hostmaster.amazon.com. 1 720...
<input type="checkbox"/>	trampas.cloudsolucao.com.br	A	Simple	-	dualstack.lb-1608431498-us-east-1.elb.amazonaws.com
<input type="checkbox"/>	_53ccac4ad86ebd09a469a4...	CNAME	Simple	-	_85291dxc9f52f275a58660bd30ce54.xmkgffzlvd.com-valida...

## 5.6 Amazon WAF

O AWS WAF é um firewall de aplicações Web que ajuda a proteger suas aplicações Web ou APIs contra bots e exploits comuns na Web que podem afetar a disponibilidade, comprometer a segurança ou consumir recursos em excesso. Oferece controle sobre como o tráfego atinge suas aplicações, permitindo que criemos regras de segurança que controlam o tráfego de bots e bloqueiam padrões de ataque comuns. Agiliza a propagação e as atualizações de regras de segurança permitindo atualizarmos rapidamente a segurança em seu ambiente quando surgirem problemas.

### Web ACL details

Name

WAF\_ACL

The name must have 1-128 characters. Valid characters: A-Z, a-z, 0-9, -, (hyphen), and \_ (underscore).

Description - optional

The description can have 1-256 characters.

CloudWatch metric name

WAF\_ACL

The name must have 1-128 characters. Valid characters: A-Z, a-z, 0-9, -, (hyphen), and \_ (underscore).

Resource type

Choose the type of resource to associate with this web ACL.

- ☐ CloudFront distributions
- ☒ Regional resources (Application Load Balancer, API Gateway, AWS AppSync, Amazon Cognito User Pools)

Region

Choose the AWS region to create this web ACL in.

US East (N. Virginia)

### Associated AWS resources - optional

Remove

Add AWS resources

Find associated AWS resources

< 1 > 🔍

<input type="checkbox"/>	Name	Resource type	Region
<input type="checkbox"/>	lb	Application Load Balancer	US East (N. Virginia)



## Add rules and rule groups [Info](#)

A rule defines attack patterns to look for in web requests and the action to take when a request matches the patterns. Rule groups are reusable collections of rules. You can use managed rule groups offered by AWS and AWS Marketplace sellers. You can also write your own rules and use your own rule groups.

### Rules

If a request matches a rule, take the corresponding action. The rules are prioritized in order they appear.

[Edit](#)[Delete](#)[Add rules ▼](#)

<input type="checkbox"/>	Name	Capacity	Action
<input type="checkbox"/>	AWS-AWSManagedRulesAdminProtectionRuleSet	100	Use rule actions
<input type="checkbox"/>	AWS-AWSManagedRulesAnonymousIpList	50	Use rule actions
<input type="checkbox"/>	AWS-AWSManagedRulesCommonRuleSet	700	Use rule actions
<input type="checkbox"/>	AWS-AWSManagedRulesLinuxRuleSet	200	Use rule actions
<input type="checkbox"/>	AWS-AWSManagedRulesPHPRuleSet	100	Use rule actions
<input type="checkbox"/>	AWS-AWSManagedRulesUnixRuleSet	100	Use rule actions
<input type="checkbox"/>	AWS-AWSManagedRulesSQLiRuleSet	200	Use rule actions

### Web ACL rule capacity units used

The total capacity units used by the web ACL can't exceed 1500.

1450/1500 WCUs



## Set rule priority [Info](#)

### Rules

If a request matches a rule, take the corresponding action. The rules are prioritized in order they appear.

▲ Move up

▼ Move down

	Name	Capacity	Action
<input checked="" type="radio"/>	AWS-AWSManagedRulesLinuxRuleSet	200	Use rule actions
<input type="radio"/>	AWS-AWSManagedRulesAdminProtectionRuleSet	100	Use rule actions
<input type="radio"/>	AWS-AWSManagedRulesAnonymousIpList	50	Use rule actions
<input type="radio"/>	AWS-AWSManagedRulesCommonRuleSet	700	Use rule actions
<input type="radio"/>	AWS-AWSManagedRulesPHPRuleSet	100	Use rule actions
<input type="radio"/>	AWS-AWSManagedRulesUnixRuleSet	100	Use rule actions
<input type="radio"/>	AWS-AWSManagedRulesSQLiRuleSet	200	Use rule actions

Cancel

Previous

Next

## Set rule priority [Info](#)

### Rules

If a request matches a rule, take the corresponding action. The rules are prioritized in order they appear.

▲ Move up

▼ Move down

	Name	Capacity	Action
<input checked="" type="radio"/>	AWS-AWSManagedRulesLinuxRuleSet	200	Use rule actions
<input type="radio"/>	AWS-AWSManagedRulesAdminProtectionRuleSet	100	Use rule actions
<input type="radio"/>	AWS-AWSManagedRulesAnonymousIpList	50	Use rule actions
<input type="radio"/>	AWS-AWSManagedRulesCommonRuleSet	700	Use rule actions
<input type="radio"/>	AWS-AWSManagedRulesPHPRuleSet	100	Use rule actions
<input type="radio"/>	AWS-AWSManagedRulesUnixRuleSet	100	Use rule actions
<input type="radio"/>	AWS-AWSManagedRulesSQLiRuleSet	200	Use rule actions

Cancel

Previous

Next

AWS WAF > Web ACLs

### Web ACLs [Info](#)

US East (N. Virginia)

Copy ARN

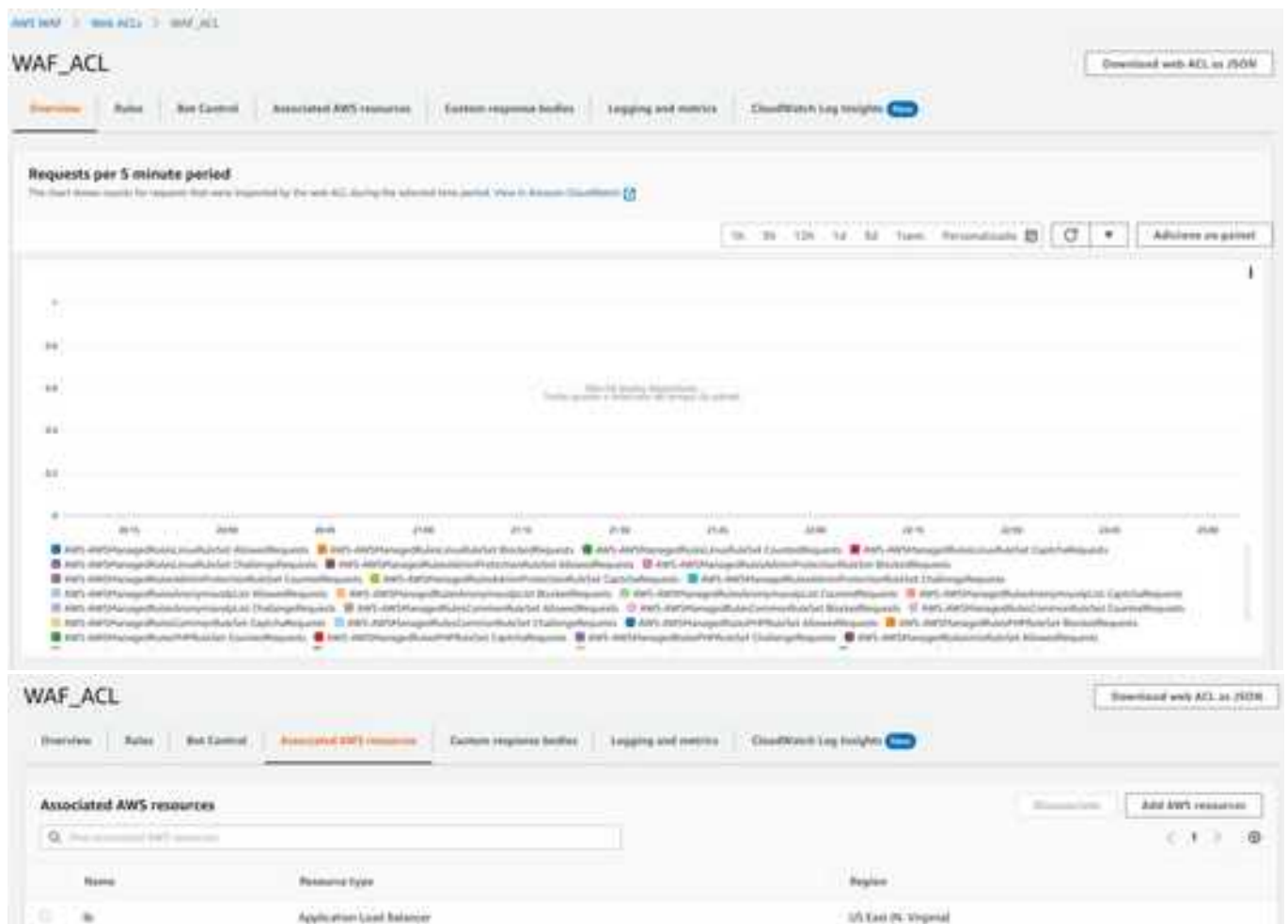
Delete

Create web ACL

Find web ACLs

1

Name	Description	
WAF_ACL		83f46c1-17b1-480b-840b-00b402d015e



## 5.7 Amazon Auto Scaling

O AWS Auto Scaling monitora os recursos das instâncias e ajusta automaticamente a capacidade para manter um desempenho constante e previsível pelo menor custo possível.

Permite definir os níveis de utilização pretendidos para vários recursos, além de criar planos de escalabilidade que automatizam a forma como grupos de recursos diferentes respondem às flutuações de demanda, priorizando disponibilidade, custos ou um equilíbrio entre os dois. Com AWS Auto Scaling, é fácil configurar a escalabilidade de recursos de EC2 em questão de minutos.



## grupo\_auto\_scaling\_teampass

Detalhes	Atividade	Escalabilidade automática	Servenciamento de instâncias	Monitoramento	Atualização de instância																								
<div>Detalhes do grupo</div> <div>Editar</div> <table><tr><td>Capacidade desejada</td><td>1</td><td colspan="4">Nome do grupo do Auto Scaling grupo_auto_scaling_teampass</td></tr><tr><td>Capacidade mínima</td><td>1</td><td colspan="4">Data de criação Sun Jan 22 2023 20:11:02 GMT-0300 (Horário Padrão de Brasília)</td></tr><tr><td>Capacidade máxima</td><td>2</td><td colspan="4">Nome de recurso da Amazon (ARN) arn:aws:autoscaling:us-east-1:415543465497:autoScalingGroup:704028a2-2182-4c7e-b6a2-a07ef79d6c3b:autoScalingGroupName:grupo_auto_scaling_teampass</td></tr></table>						Capacidade desejada	1	Nome do grupo do Auto Scaling grupo_auto_scaling_teampass				Capacidade mínima	1	Data de criação Sun Jan 22 2023 20:11:02 GMT-0300 (Horário Padrão de Brasília)				Capacidade máxima	2	Nome de recurso da Amazon (ARN) arn:aws:autoscaling:us-east-1:415543465497:autoScalingGroup:704028a2-2182-4c7e-b6a2-a07ef79d6c3b:autoScalingGroupName:grupo_auto_scaling_teampass									
Capacidade desejada	1	Nome do grupo do Auto Scaling grupo_auto_scaling_teampass																											
Capacidade mínima	1	Data de criação Sun Jan 22 2023 20:11:02 GMT-0300 (Horário Padrão de Brasília)																											
Capacidade máxima	2	Nome de recurso da Amazon (ARN) arn:aws:autoscaling:us-east-1:415543465497:autoScalingGroup:704028a2-2182-4c7e-b6a2-a07ef79d6c3b:autoScalingGroupName:grupo_auto_scaling_teampass																											
<div>Modelo de execução</div> <div>Editar</div> <table><tr><td>Modelo de execução modelo_teampass</td><td>it-034112912548a57bc</td><td>ID da AMI ami-0c0757c8b0590a1a</td><td colspan="3">Tipo de instância t2.micro</td></tr><tr><td>Versão Default</td><td></td><td>Grupo de segurança -</td><td colspan="3">ID de grupo de segurança -</td></tr><tr><td>Descrição teampass</td><td></td><td>Nome do par de chaves par_vingra_teampass</td><td colspan="3">Armazenamento (volumes) /dev/xvda</td></tr><tr><td>Solicitar instâncias spot</td><td></td><td>Horário de criação Sun Jan 22 2023 20:27:36 GMT-0300 (Horário Padrão de Brasília)</td><td colspan="3">Criado por aws-iam::415543465497:root</td></tr></table>						Modelo de execução modelo_teampass	it-034112912548a57bc	ID da AMI ami-0c0757c8b0590a1a	Tipo de instância t2.micro			Versão Default		Grupo de segurança -	ID de grupo de segurança -			Descrição teampass		Nome do par de chaves par_vingra_teampass	Armazenamento (volumes) /dev/xvda			Solicitar instâncias spot		Horário de criação Sun Jan 22 2023 20:27:36 GMT-0300 (Horário Padrão de Brasília)	Criado por aws-iam::415543465497:root		
Modelo de execução modelo_teampass	it-034112912548a57bc	ID da AMI ami-0c0757c8b0590a1a	Tipo de instância t2.micro																										
Versão Default		Grupo de segurança -	ID de grupo de segurança -																										
Descrição teampass		Nome do par de chaves par_vingra_teampass	Armazenamento (volumes) /dev/xvda																										
Solicitar instâncias spot		Horário de criação Sun Jan 22 2023 20:27:36 GMT-0300 (Horário Padrão de Brasília)	Criado por aws-iam::415543465497:root																										

## grupo\_auto\_scaing\_teampass

Detalhes

Atividade

Tolerabilidade automática

Servenciamento de instâncias

Monitoramento

Atualização de instância

Notificações de atividades (0)

grupo\_auto\_scaling\_teampass

Detalhes Atividade Escalabilidade automática Gerenciamento de instâncias Monitoramento Atualização da instância

As políticas de escalabilidade redimensionam o grupo de Auto Scaling para atender às alterações na demanda. Com políticas de escalabilidade dinâmica reativas, você pode monitorar métricas específicas do CloudWatch e tomar medidas quando o limite de alarme do CloudWatch for atingido. Uma política de escalabilidade proativa juntamente com políticas de escalabilidade dinâmicas quando a demanda da aplicação muda rapidamente, mas tem um padrão recorrente, ou quando as instâncias do EC2 exigem mais tempo para serem iniciadas.

Política de escalabilidade dinâmica criada ou editada com êxito

Políticas de escalabilidade dinâmica (2) [ver](#)

50%

Escalabilidade simples

Habilitado

Alarme\_30

Ativa o limite de alarme: CPUUtilization > 50 para 1 período consecutivo de 300 segundos para as dimensões de métrica:

AutoScalingGroupName = Group\_AutoScaling

Remover 1 unidades de capacidade

300 segundos antes de permitir outra ação de escalabilidade

70%

Escalabilidade simples

Habilitado

Alarme\_70

Ativa o limite de alarme: CPUUtilization > 70 para 1 período consecutivo de 300 segundos para as dimensões de métrica:

AutoScalingGroupName = Group\_AutoScaling

Adicionar 1 unidades de capacidade

300 segundos antes de permitir outra ação de escalabilidade

grupo\_auto\_scaling\_teampass

Detalhes Atividade Escalabilidade automática Gerenciamento de instâncias Monitoramento Atualização da instância

Instâncias (1)

Adicionar instâncias

ID de instância	Nome de vida	Tipo de instância	Capacidade po...	Métrica/métric...	Data de dispon...	Status de integ...	Protegido contra
i-4424200000000000000	teampass	Linux	-	cpuutilization (5)	on-demand	Healthy	

Ganchos do ciclo de vida (0) [ver](#)

Adicionar ganchos do ciclo de vida

Nome	Transição do ciclo de vida	Resultado padrão	Tempo limite de publicação...	Ativação de destino de notifica...	Ativação de função
Não há nenhum gancho do ciclo de vida configurado no momento.					

Os ganchos do ciclo de vida permitem você a executar ações personalizadas em instâncias conforme elas são criadas e antes de serem destruídas.

Criar gancho do ciclo de vida

## 5.9 Amazon Certificate Manager

O AWS Certificate Manager é um serviço que permite provisionar, gerenciar e implantar certificados de forma fácil e segura, Secure Sockets Layer (SSL)/Transport Layer Security (TLS) para uso com os serviços da AWS e os recursos internos conectados. Os certificados SSL/TLS são usados para proteger comunicações de rede e estabelecer a identidade de sites na Internet e de recursos em redes privadas. O AWS Certificate Manager elimina processos manuais demorados como compra, upload e renovação de certificados SSL/TLS. Este serviço é utilizado para

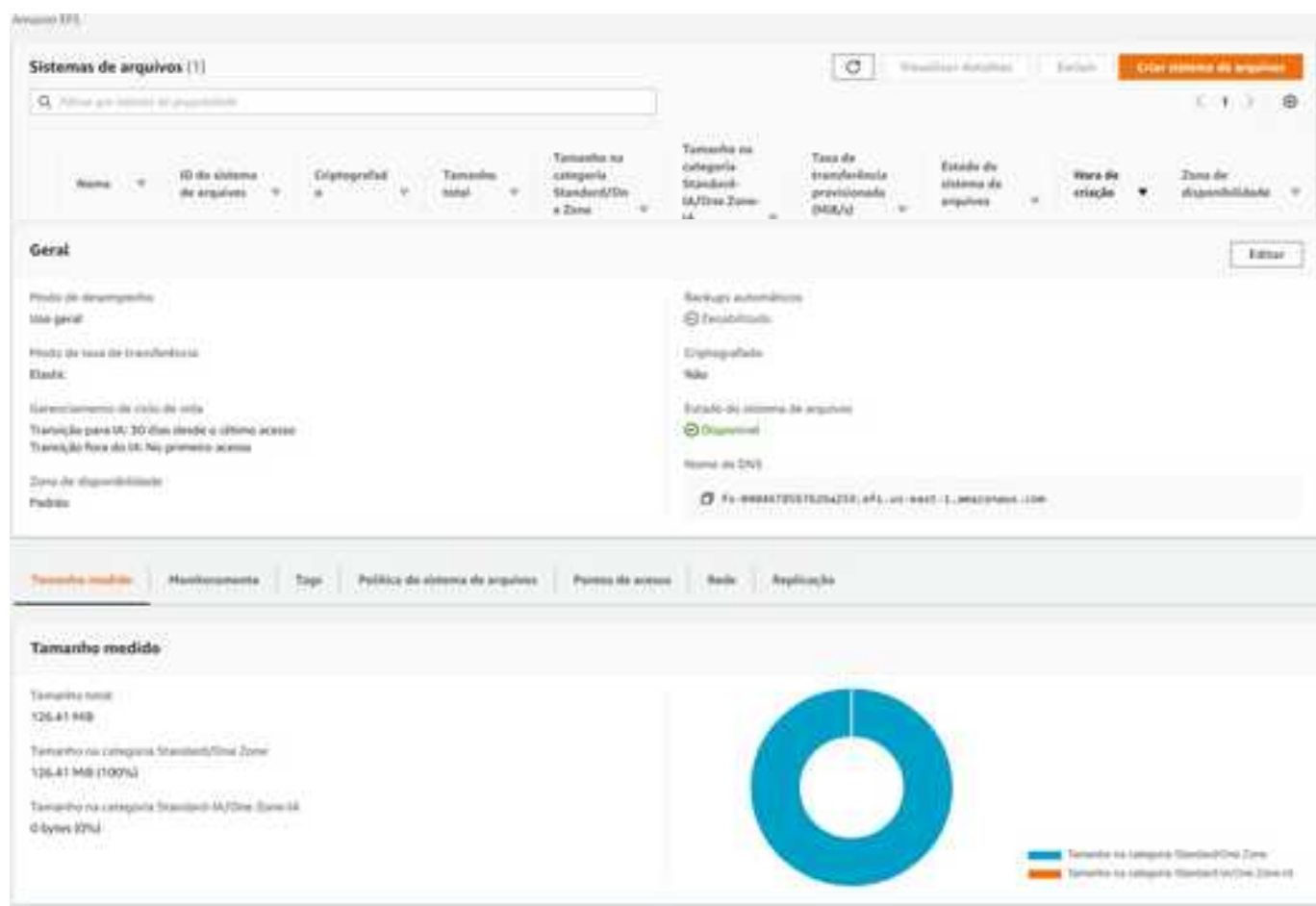


ID do certificado	Nome de domínio	Tipo	Status	Em uso?	Qualificação para renovação	Algoritmo de chave
647c7f7d-4145-4409-8a84-3a307924b61a	tsamparo.cloudsolução.com.br	Emitido pela Amazon	Em uso	Sim	Qualificado	RSA 2048

disponibilizar certificado SSL para o CloudFront e possibilitar a entrega do site como ambiente seguro, em HTTPS.

## 5.10 EFS (Amazon Elastic File System)

O Amazon Elastic File System (EFS) aumenta e diminui automaticamente conforme você adiciona e remove arquivos, sem a necessidade de gerenciamento ou provisionamento.



**Sistemas de arquivos (1)**

Nome	ID do sistema de arquivos	Criptografia	Tamanho total	Tamanho na categoria Standard/On-Zone	Tamanho na categoria Standard-IA/One Zone-IA	Taxa de transferência provisionada (MiB/s)	Estado do sistema de arquivos	Meta de criação	Zona de disponibilidade
tsamparo	fs-0000072057L204210_efs_uf-0007-1_0000070000_1000	Não	126.41 MiB	126.41 MiB (100%)	0 bytes (0%)	100	Disponível	Padrão	uf-0007-1

**Geral**

Proteção de desempenho: Não geral

Proteção de taxa de transferência: Elástico

Gerenciamento de ciclo de vida: Transição para IA: 30 dias desde o último acesso; Transição para On-Zone: no primeiro acesso

Zona de disponibilidade: Padrão

Serviços automáticos: Encabeçalho: Não; Criptografia: Não; Estado do sistema de arquivos: Disponível; Nome do DNS: fs-0000072057L204210\_efs\_uf-0007-1\_0000070000\_1000


**Tamanho medido**

Tamanho total: 126.41 MiB

Tamanho na categoria Standard/On-Zone: 126.41 MiB (100%)

Tamanho na categoria Standard-IA/One Zone-IA: 0 bytes (0%)

**Visualização de gráfico**



Standard/On-Zone: 100%  
Standard-IA/One Zone-IA: 0%



**Acessar**

Monte o sistema de arquivos de Amazon EFS em uma instância do Linux. Saiba mais.

☒ Montar via DNS
 ☐ Montar via IP

Usando o assistente de montagem do EFS:

sudo mount -t efs -o fsid=fs-444478027525a259,rsid=rs-444478027525a259 /efs /

Usando o cliente do NFS:

sudo mount -t nfs -o nfsvers=4.1,rsize=1048576,wsid=rs-444478027525a259,hard,timeo=600,tcpnodelay,cache=on /efs fs-444478027525a259.efs.us-west-1.amazonaws.com:/efs

Consulte nossa guia de usuário para obter mais informações. Saiba mais.

Fechar



## 5.11 Amazon CloudWatch

O Amazon CloudWatch é um serviço de monitoramento projetado para coleta de dados, análise de infraestruturas, que pode gerar alertas e notificações de toda a infraestrutura implementada dentro da AWS, para gestores, técnicos e responsáveis por essa infraestrutura. O CloudWatch fornece dados e insights úteis para monitorar as aplicações, responder às mudanças de performance de todo o sistema e otimizar a utilização dos recursos alocados. Coleta dados operacionais e de monitoramento na forma de logs, métricas e eventos. Permitindo assim uma visão unificada da integridade operacional e visibilidade completa de seus recursos, aplicações e serviços da AWS em execução.

## 5.12 Amazon SNS ( Simple Notification Service )

O Amazon Simple Notification Service (Amazon SNS) é um serviço de mensagens totalmente gerenciado para a comunicação de aplicação para aplicação (A2A) e de aplicação para pessoa (A2P). A funcionalidade pub/sub de A2A fornece tópicos para sistemas de mensagens de alta taxa de transferência baseados em push e de muitos para muitos entre sistemas distribuídos, microserviços e aplicações sem servidor orientadas por eventos. Usando tópicos do Amazon SNS, seus sistemas editores podem repassar mensagens para um grande número de sistemas de assinantes, incluindo filas do Amazon SQS, funções do AWS Lambda e endpoints HTTPS e o Amazon Kinesis Data Firehose para processamento paralelo. A funcionalidade A2P permite enviar mensagens para usuários em grande escala por SMS, push de dispositivos móveis e e-mail.

## 5.13 Amazon IAM (Identify and Access Management)

O AWS Identity and Access Management (IAM) é um serviço da AWS que ajuda você a criar e controlar usuários, funções e políticas para os seus recursos alocados com segurança o acesso aos recursos da AWS. O IAM é utilizado para controlar permissões de acesso a usuários e serviços, exemplo, política EC2 tem permissão para escrever em S3, também controla funções e políticas, que podem ser utilizadas, com praticamente todos os recursos da AWS.

## 5.14 Amazon RDS MariaDB

O Amazon RDS MariaDB é uma configuração sob demanda e de auto escalabilidade do Amazon RDS. O Amazon RDS MariaDB ajuda a automatizar os processos de monitoramento da workload e ajustar a capacidade para seus bancos de dados. A capacidade é ajustada automaticamente com base na demanda da aplicação. Você será cobrado apenas pelos recursos que seus clusters de banco de

dados consumirem. Dessa forma, o Amazon RDS MariaDB pode ajudar você a ficar dentro do orçamento e evitar pagar pelos recursos computacionais não utilizados.

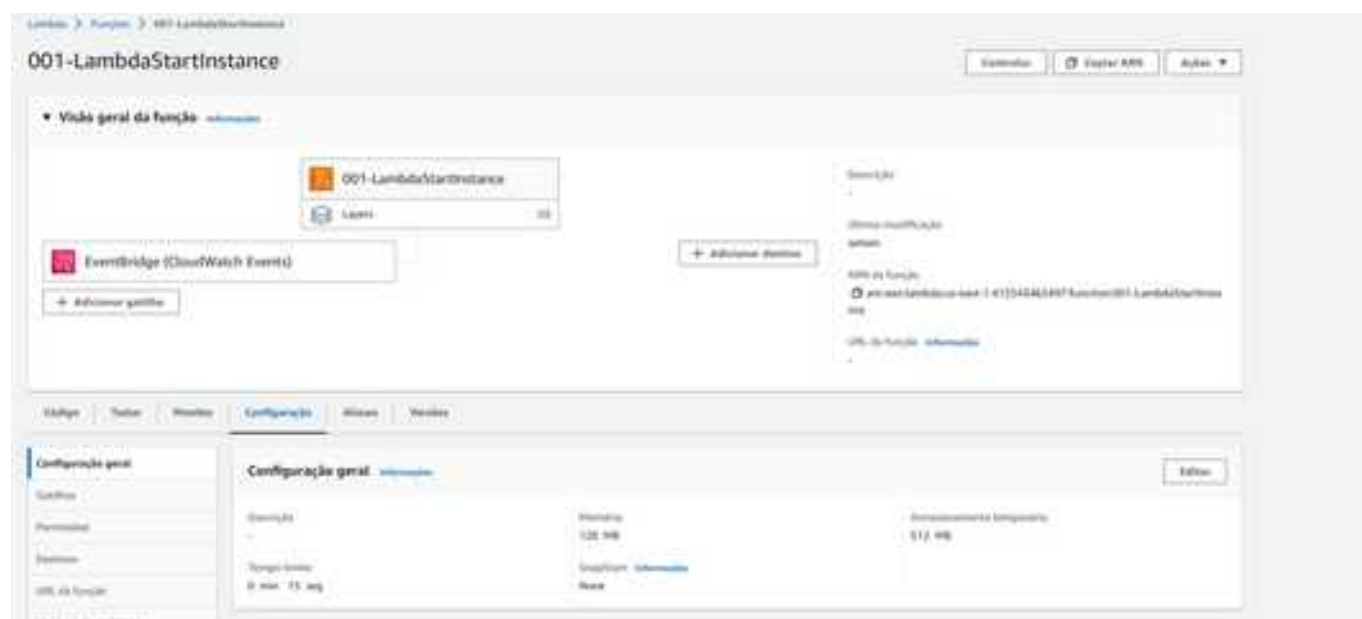
## 5.15 Instâncias EC2 ( Elastic Compute Cloud )

O Amazon Elastic Compute Cloud (Amazon EC2) oferece a plataforma de computação mais ampla e profunda, com mais de 500 instâncias e opções do processador, armazenamento, redes, sistema operacional e modelo de compra mais recentes para ajudar você a atender melhor às necessidades da sua workload.

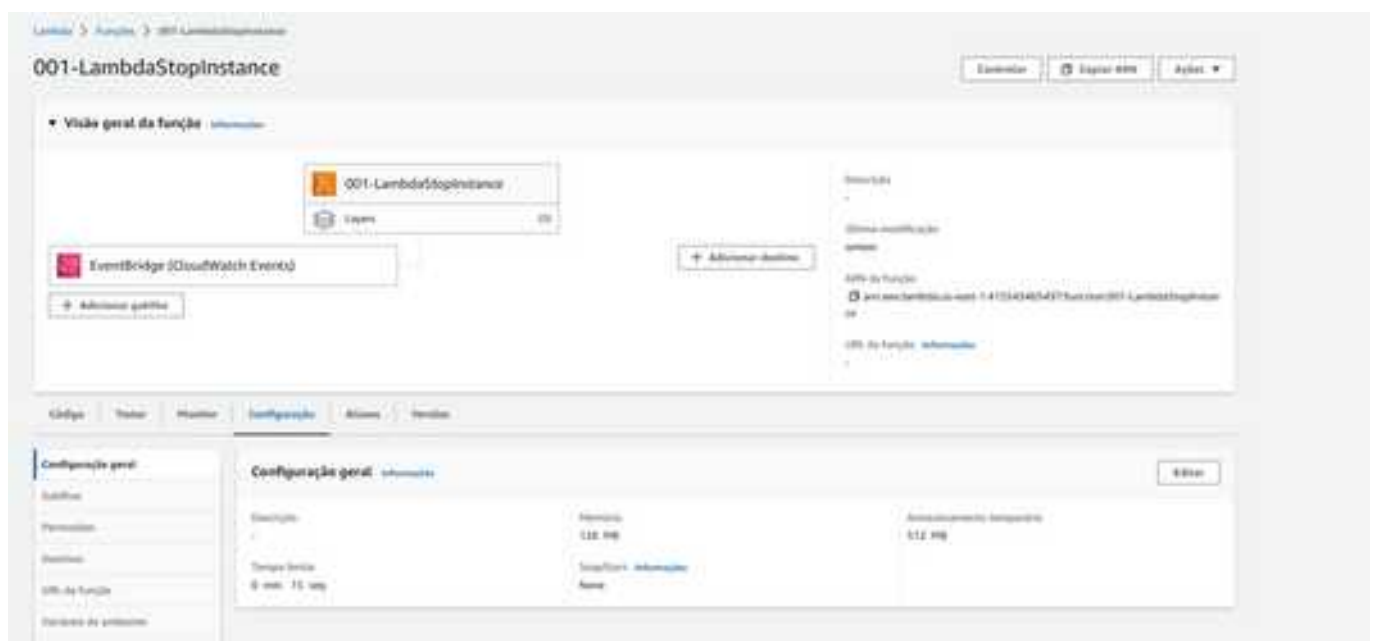
## 5.16 AWS Lambda

O AWS Lambda é um serviço de computação sem servidor e orientado a eventos que permite executar código para praticamente qualquer tipo de aplicação ou serviço de backend sem provisionar e gerenciar servidores.

Exemplo de Config. Lambda Start Instance



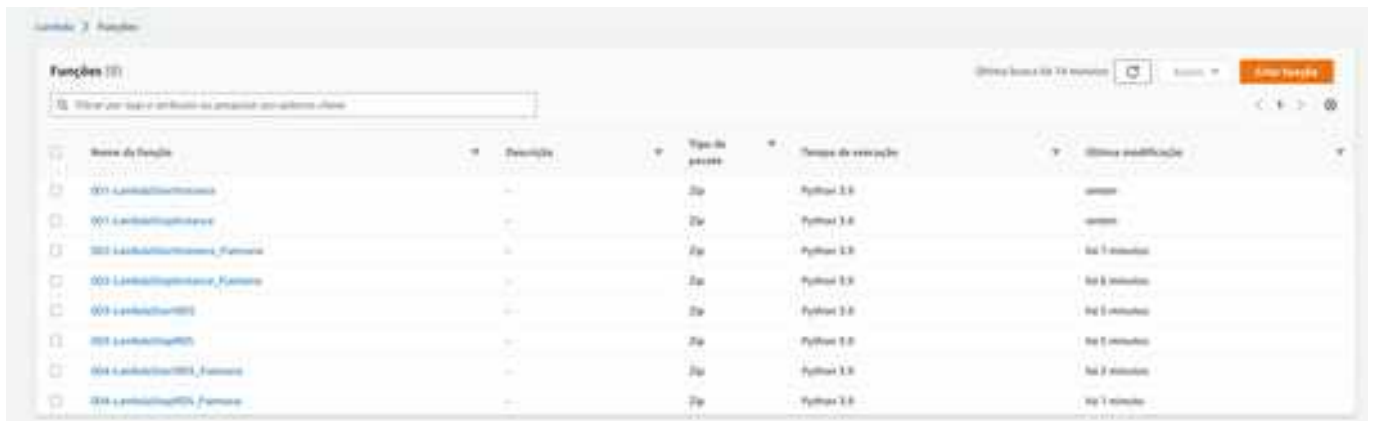
## Exemplo de Config. Lambda Stop Instance



## O Exemplo abaixo demonstra como economizar dinheiro com AWS nos horários desejados da empresa.

Instâncias e RDS serão ligadas e desligadas automaticamente de Segunda à Sexta nos horários das 8 às 20hs.

Instâncias e RDS serão ligadas e desligadas automaticamente aos Sábados nos horários das 8 às 13hs.



Funções (10)

Última busca há 24 minutos

Adicionar função

Nome da função	Descrição	Tipo de pacote	Tempo de execução	Última modificação
001-LambdaFunctionTeste	...	Zip	Python 3.8	sem erro
001-LambdaFunctionTeste	...	Zip	Python 3.8	sem erro
002-LambdaFunctionTeste_Funciona	...	Zip	Python 3.8	há 5 minutos
003-LambdaFunctionTeste_Funciona	...	Zip	Python 3.8	há 5 minutos
003-LambdaFunctionTeste	...	Zip	Python 3.8	há 5 minutos
004-LambdaFunctionTeste_Funciona	...	Zip	Python 3.8	há 5 minutos
004-LambdaFunctionTeste	...	Zip	Python 3.8	há 5 minutos
004-LambdaFunctionTeste_Funciona	...	Zip	Python 3.8	há 5 minutos

## 5.17 Secret Manager

Uma forma segura de guardar segredos, não expondo os dados do host dbname em uma aplicação.



Segredos

Última recuperação há 24 minutos

Adicionar novo segredo

Nome do segredo	Descrição	Última recuperação (UTC)
prod/hostname	...	1/1/2021

**A forma tradicional e insegura**

```
1  <?php
2  // DATABASE connexion parameters
3  define("DB_HOST", "prod-rds-mariadb.cytufidb0c9g.us-east-1.rds.amazonaws.com");
4  define("DB_USER", "admin");
5  define("DB_PASSWD", "def5020087c773336af5e250b7f51f1888d9e49bb98882fb09702a5ea51b15101e23a3c9d5c0ca5f2606ae6fb83");
6  define("DB_NAME", "db_teampass");
7  define("DB_PREFIX", "teampass_");
8  define("DB_PORT", "3306");
9  define("DB_ENCODING", "utf8");
10 define("DB_SSL", array(
11     "key" => "",
12     "cert" => "",
13     "ca_cert" => "",
14     "ca_path" => "",
15     "cipher" => ""
16 ));
17 define("DB_CONNECT_OPTIONS", array(
18     MYSQLI_OPT_CONNECT_TIMEOUT => 10
19 ));
20 define("SECUREPATH", "/var/www/html/teampass/includes");
21
22 if (isset($_SESSION['settings']['timezone']) == true) {
23     date_default_timezone_set($_SESSION['settings']['timezone']);
24 }
25
```

## A forma segura

```
1 <?php
2
3 require '/var/www/html/teampass/vendor/autoload.php';
4
5 use Aws\Credentials\CredentialProvider;
6 use Aws\SecretsManager\SecretsManagerClient;
7 use Aws\Exception\AwsException;
8
9 $provider = CredentialProvider::defaultProvider();
10
11 $client = new SecretsManagerClient( [
12     'credentials' => $provider,
13     'version' => 'latest',
14     'region' => 'us-east-1'
15 ] );
16
17 $secretName = 'prod/teampass';
18
19 try {
20     $result = $client->getSecretValue( [
21         'SecretId' => $secretName,
22     ] );
23 } catch ( AwsException $e ) {
24     $error = $e->getAwsErrorCode();
25     if ( $error == 'DecryptionFailureException' ) { // Não é possível descriptografar o texto secreto protegido
26         throw $e;
27     }
28 }
```

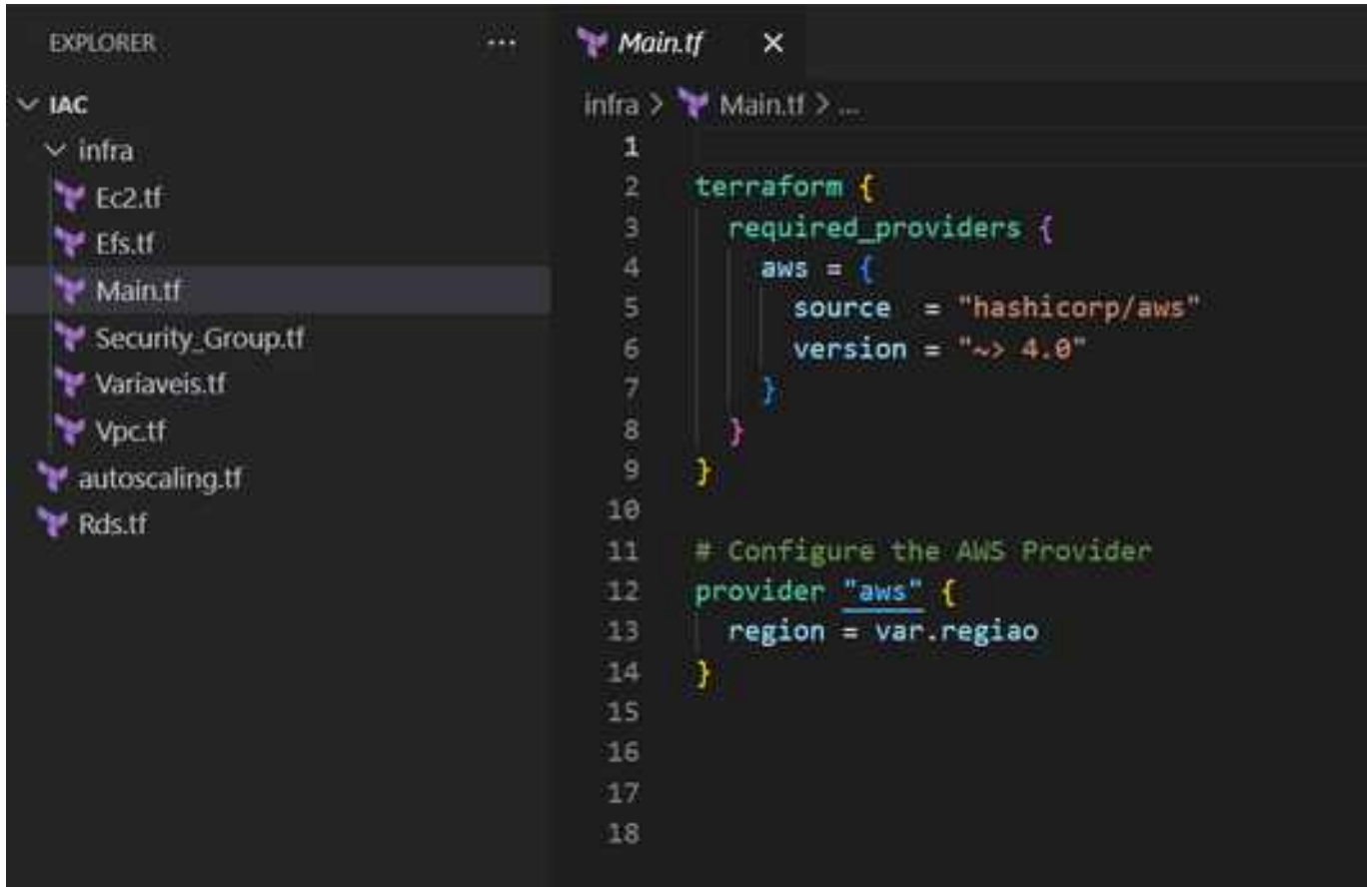
```
55
56
57 // DATABASE connexion parameters
58 define("DB_HOST", $Secret_DB_HOST);
59 define("DB_USER", $Secret_DB_USERNAME);
60 define("DB_PASSWD", "def5020087c773336af5e250b7f51f1888d9e49bb98882fb09702a5ea51b15101e23a3c9d5c0ca5f2606ae6fb82");
61 define("DB_NAME", $Secret_DB_NAME);
62 define("DB_PREFIX", "teampass_");
63 define("DB_PORT", $Secret_DB_PORT);
64 define("DB_ENCODING", "utf8");
65 define("DB_SSL", array(
66     "key" => "",
67     "cert" => "",
68     "ca_cert" => "",
69     "ca_path" => "",
70     "cipher" => ""
71 ));
72 define("DB_CONNECT_OPTIONS", array(
73     MYSQLI_OPT_CONNECT_TIMEOUT => 10
74 ));
75 define("SECUREPATH", "/var/www/html/teampass/includes");
76
77 if (isset($_SESSION['settings']['timezone']) == true) {
78     date_default_timezone_set($_SESSION['settings']['timezone']);
79 }
80
```

Lembrando que o mesmo foi criada uma role para não expor dados de credenciais e anexado na instância.



## 6. Terraform

Terraform é apenas uma forma de poupar tempo na criação da infraestrutura.

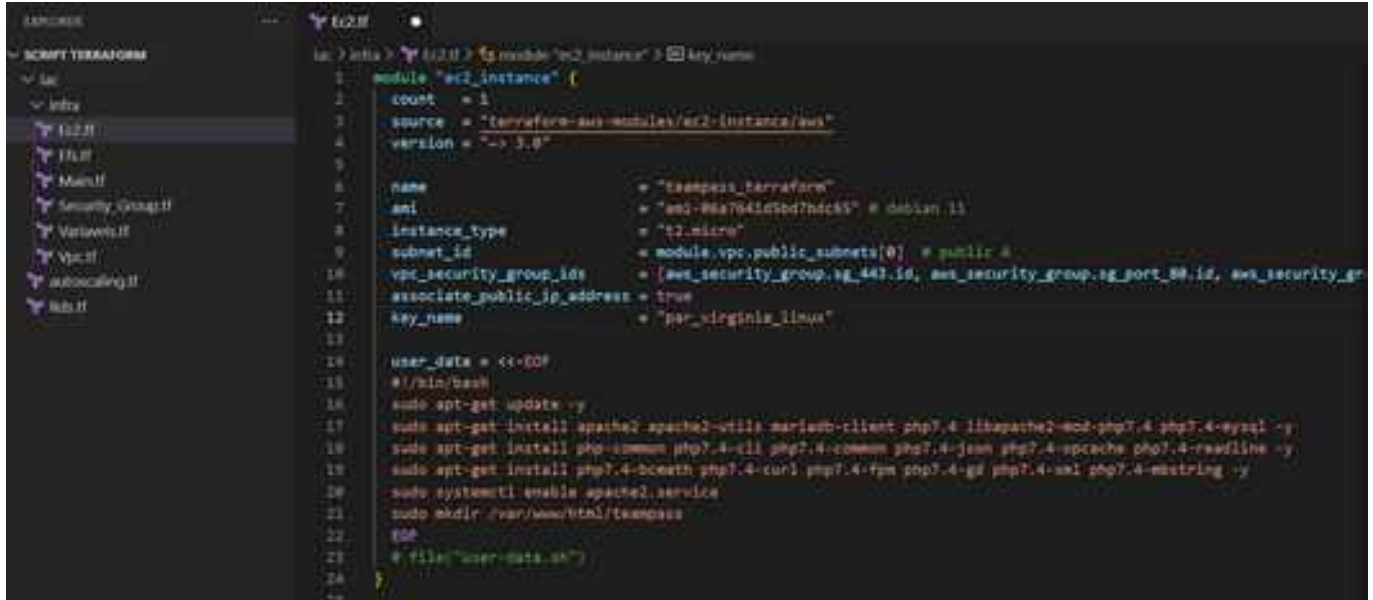


The screenshot shows a code editor with a dark theme. On the left, the 'EXPLORER' sidebar displays a file tree under the 'IAC' folder, with 'infra' expanded and 'Main.tf' selected. The main editor area shows the content of 'Main.tf' with line numbers 1 through 18. The code configures the Terraform AWS provider.

```
1
2 terraform {
3   required_providers {
4     aws = {
5       source = "hashicorp/aws"
6       version = "~> 4.0"
7     }
8   }
9 }
10
11 # Configure the AWS Provider
12 provider "aws" {
13   region = var.regiao
14 }
15
16
17
18
```



Demonstração da criação da instância utilizando Terraform.

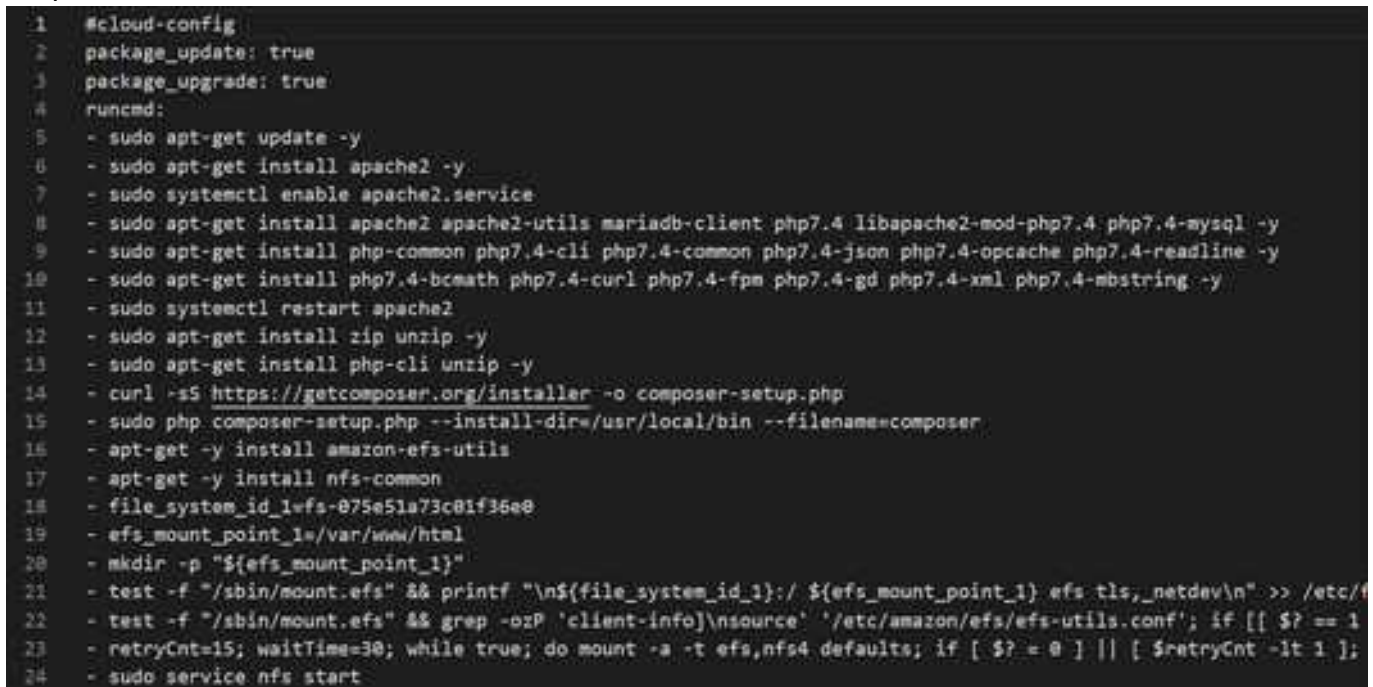


```

1 module "ec2_instance" {
2   count = 1
3   source = "terraform-aws-modules/ec2-instance/aws"
4   version = "~> 3.0"
5
6   name = "terraform-terraform"
7   ami = "ami-06a7041d7bdc45" # debian 11
8   instance_type = "t2.micro"
9   subnet_id = module.vpc.public_subnets[0] # public
10  vpc_security_group_ids = [aws_security_group.sg_443.id, aws_security_group.sg_port_80.id, aws_security_group.sg_ssh.id]
11  associate_public_ip_address = true
12  key_name = "per_virginia_linux"
13
14  user_data = <<<EOF
15  #!/bin/bash
16  sudo apt-get update -y
17  sudo apt-get install apache2 apache2-utils mariadb-client php7.4 libapache2-mod-php7.4 php7.4-mysql -y
18  sudo apt-get install php-common php7.4-cli php7.4-common php7.4-json php7.4-opcache php7.4-readline -y
19  sudo apt-get install php7.4-bcmath php7.4-curl php7.4-fpm php7.4-gd php7.4-xml php7.4-mbstring -y
20  sudo systemctl enable apache2.service
21  sudo mkdir /var/www/html/terraform
22  cd
23  # file "user-data.sh"
24  EOF
25

```

O arquivo “user-data.sh” seria mais interessante de ser usado pois, deixaria o código mais limpo.



```

1 #cloud-config
2 package_update: true
3 package_upgrade: true
4 runcmd:
5 - sudo apt-get update -y
6 - sudo apt-get install apache2 -y
7 - sudo systemctl enable apache2.service
8 - sudo apt-get install apache2 apache2-utils mariadb-client php7.4 libapache2-mod-php7.4 php7.4-mysql -y
9 - sudo apt-get install php-common php7.4-cli php7.4-common php7.4-json php7.4-opcache php7.4-readline -y
10 - sudo apt-get install php7.4-bcmath php7.4-curl php7.4-fpm php7.4-gd php7.4-xml php7.4-mbstring -y
11 - sudo systemctl restart apache2
12 - sudo apt-get install zip unzip -y
13 - sudo apt-get install php-cli unzip -y
14 - curl -sS https://getcomposer.org/installer -o composer-setup.php
15 - sudo php composer-setup.php --install-dir=/usr/local/bin --filename=composer
16 - apt-get -y install amazon-efs-utils
17 - apt-get -y install nfs-common
18 - file_system_id_1=fs-075e51a73c01f36e0
19 - efs_mount_point_1=/var/www/html
20 - mkdir -p "${efs_mount_point_1}"
21 - test -f "/sbin/mount.efs" && printf "\n${file_system_id_1}:/ ${efs_mount_point_1} efs tls,_netdev\n" >> /etc/fstab
22 - test -f "/sbin/mount.efs" && grep -oP 'client-info\nsource' '/etc/amazon/efs/efs-utils.conf'; if [[ $? == 1
23 - retryCnt=15; waitTime=30; while true; do mount -a -t efs,nfs4 defaults; if [ $? = 0 ] || [ $retryCnt -lt 1 ];
24 - sudo service nfs start

```

## 7. Teste de Stress

Teste realizado com apenas uma instância da família T2.micro, provando que a mesma suporta várias conexões simultâneas sem a necessidade de hardware mais robusto, levando em consideração que a empresa necessita de acesso para 8 usuários.

A figura abaixo mostra o teste de 5.000 acessos simultâneos.

```
root@nb0019:~# ab -n 500 -c 200 https://teampass.cloudsolucao.com.br/
This is ApacheBench, Version 2.3 <$Revision: 1807734 $>
Copyright 1996 Adam Twiss, Zeus Technology Ltd, http://www.zeustech.net/
Licensed to The Apache Software Foundation, http://www.apache.org/

Benchmarking teampass.cloudsolucao.com.br (be patient)
Completed 500 requests
Completed 1000 requests
Completed 1500 requests
Completed 2000 requests
Completed 2500 requests
Completed 3000 requests
Completed 3500 requests
Completed 4000 requests
Completed 4500 requests
Completed 5000 requests
Finished 5000 requests


Server Software:      Apache/2.4.54
Server Hostname:      teampass.cloudsolucao.com.br
Server Port:          443
SSL/TLS Protocol:     TLSv1.2,ECDHE-RSA-AES128-GCM-SHA256,2048,128
TLS Server Name:      teampass.cloudsolucao.com.br

Document Path:        /
Document Length:       121826 bytes

Concurrency Level:     200
Time taken for tests:   107.638 seconds
Complete requests:     5000
Failed requests:        32
  (Connect: 0, Receive: 0, Length: 32, Exceptions: 0)
Non-2xx responses:     1
Total transferred:     608056151 bytes
HTML transferred:      605231690 bytes
Requests per second:   46.45 [#/sec] (mean)
Time per request:      4305.510 [ms] (mean)
Time per request:      21.528 [ms] (mean, across all concurrent requests)
Transfer rate:         5516.70 [Kbytes/sec] received

Connection Times (ms)
  min  mean[+/-sd] median  max
Connect:  471  652 211.6   590  2168
Processing: 157  3556 4148.1  2792 37889
Waiting:  157  2790 4123.3  2129 37541
Total:    896  4208 4198.5  3381 38379
```

```
root@nb0019:~# nslookup teampass.cloudsolucao.com.br
Server:      10.25.1.1
Address:     10.25.1.1#53

Non-authoritative answer:
Name:   teampass.cloudsolucao.com.br
Address: 3.216.56.7
Name:   teampass.cloudsolucao.com.br
Address: 52.3.196.67

root@nb0019:~# nslookup teampass.cloudsolucao.com.br
Server:      10.25.1.1
Address:     10.25.1.1#53

Non-authoritative answer:
Name:   teampass.cloudsolucao.com.br
Address: 18.214.183.163
Name:   teampass.cloudsolucao.com.br
Address: 52.20.234.79
```

Agora um teste de 20.000 acessos simultâneos.

```
root@nb0019:~# ab -s 1000 -n 20000 -c 500 https://teampass.cloudsolucao.com.br/
This is ApacheBench, Version 2.3 <Revision: 1807734 >
Copyright 1996 Adam Twiss, Zeus Technology Ltd, http://www.zeustech.net/
Licensed to The Apache Software Foundation, http://www.apache.org/

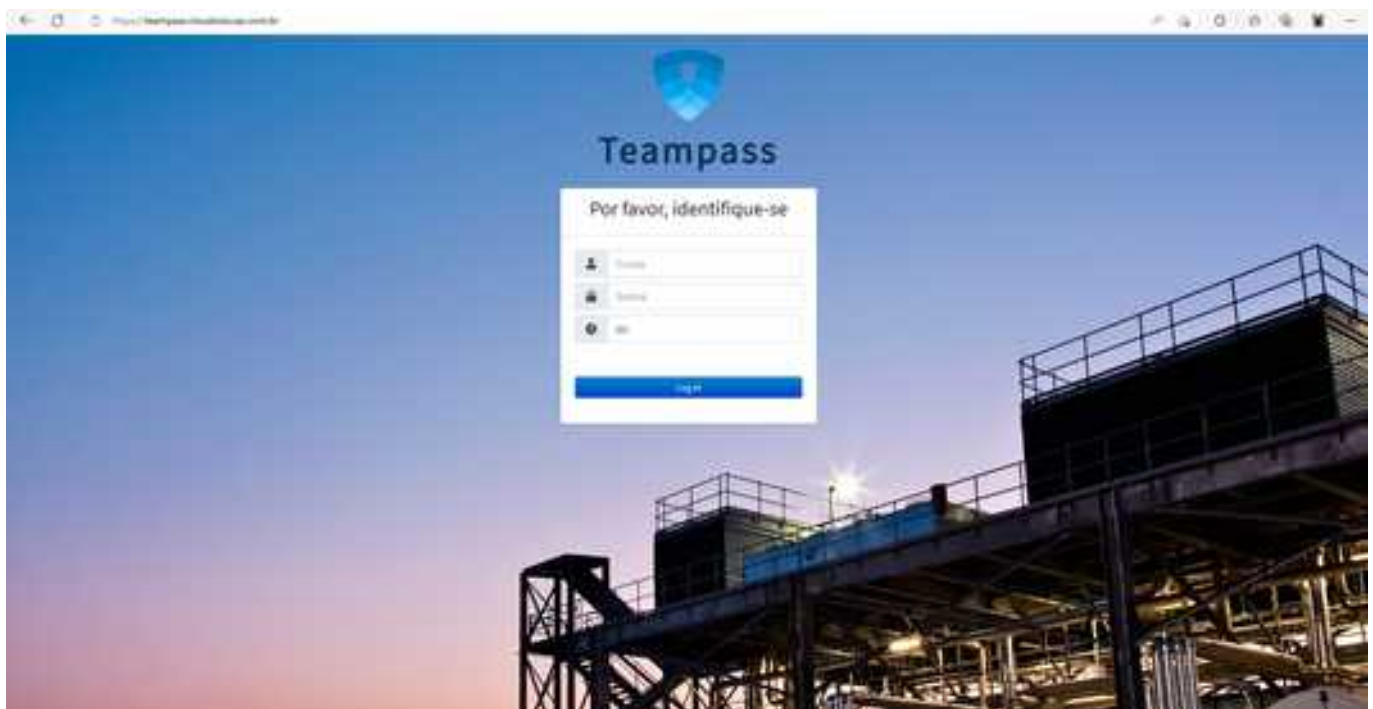
Benchmarking teampass.cloudsolucao.com.br (be patient)
Completed 2000 requests
Completed 4000 requests
Completed 6000 requests
Completed 8000 requests
Completed 10000 requests
Completed 12000 requests
SSL read failed (5) - closing connection
Completed 14000 requests
SSL read failed (5) - closing connection
Completed 16000 requests
Completed 18000 requests
```

## 8. TeamPass em Execução

Config do apache

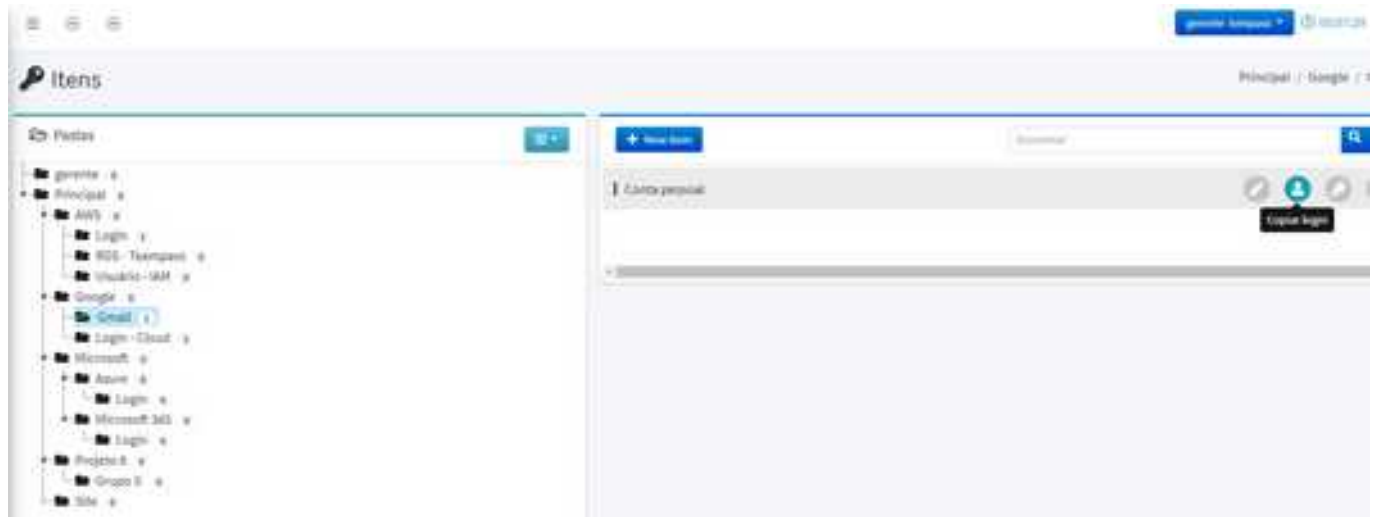
```
1 <VirtualHost *:80>
2     ServerAdmin admin@example.com
3     DocumentRoot /var/www/html/teampass
4     ServerName http://teampass.cloudsoulucao.com.br
5     DirectoryIndex index.html index.php
6     <Directory /var/www/html/teampass/>
7         Options +FollowSymlinks
8         AllowOverride All
9         Require all granted
10    </Directory>
11    ErrorLog ${APACHE_LOG_DIR}/teampass_error.log
12    CustomLog ${APACHE_LOG_DIR}/teampass_access.log combined
13 </VirtualHost>
```

Demonstração da página de acesso ao TeamPass.



Hierarquia das senhas





Configuração de página 404 configurada. Apenas uma forma mais agradável de dizer que a página não existe.



## 9. Docker

A grande vantagem de um container é encapsular todas as dependências necessárias para rodá-lo, como bibliotecas, o runtime e o código da aplicação. Tudo isso em um único pacote chamado de imagem, que pode ser versionado e de fácil distribuição.

Figura abaixo mostra os containers ativos

```
[ec2-user@ip-10-1-11-103 ~]$ docker ps
```

CONTAINER ID	IMAGE	COMMAND	CREATED	STATUS	PORTS	NAMES
85e35a7ebdae	teampass	"bash"	2 days ago	Up 2 days	0.0.0.0:80→80/tcp, :::80→80/tcp, 443/tcp	blissful_bhaskara

```
[ec2-user@ip-10-1-11-103 ~]$
```



```
1  #cloud-config
2  package_update: true
3  package_upgrade: true
4  runcmd:
5  - sudo yum update -y
6  - sudo yum install nano -y
7  - sudo yum search docker -y
8  - sudo yum info docker -y
9  - sudo yum install docker -y
10 - sudo usermod -a -G docker ec2-user
11 - id ec2-user
12 - newgrp docker
13 - sudo yum install python3-pip -y
14 - sudo pip3 install docker-compose # with root access
15 - sudo systemctl enable docker.service
16 - sudo systemctl start docker.service
17 - sudo systemctl status docker.service
18 - echo "$PATH"
19 - export PATH=$PATH:/usr/local/bin
20 - sudo find / -name "docker-compose" -ls
21 - docker version
22 - docker-compose version
23 - sudo systemctl start docker.service
24 - sudo systemctl stop docker.service
25 - sudo systemctl restart docker.service
26 - sudo systemctl status docker.service
27 - sudo yum install -y php-cli unzip
```

```
28 - curl -sS https://getcomposer.org/installer -o composer-setup.php
29 - sudo php /composer-setup.php --install-dir=/usr/local/bin --filename=composer
30 - sudo mkdir -p /var/www/html
31 - yum install -y amazon-efs-utils
32 - apt-get -y install amazon-efs-utils
33 - yum install -y nfs-utils
34 - apt-get -y install nfs-common
35 - file_system_id_1=fs-075e51a73c01f36e0
36 - efs_mount_point_1=/var/www/html
37 - mkdir -p "${efs_mount_point_1}"
38 - test -f "/sbin/mount.efs" && printf "\n${file_system_id_1}:/ ${efs_mount_point_1} efs tls,_netdev\n" >> /etc/fstab
39 - test -f "/sbin/mount.efs" && grep -oP 'client-info\|source' '/etc/amazon/efs/efs-utils.conf'; if [[ $? = 1
40 - retryCnt=15; waitTime=30; while true; do mount -a -t efs,nfs4 defaults; if [ $? = 0 ] || [ $retryCnt -lt 1 ];
41 - sudo service nfs start
42
```

## Mapeamento

- docker volume create meu-volume
- efs\_mount\_point\_1=/var/lib/docker/volumes/meu-volume/\_data

```
docker run -d -p 80:80 --name=tempass -v meu-volume:/var/www/html tempass
```

## 10. Contas AWS - Organização

A proposta de se utilizar a AWS Organizations é para gerenciar a conta da empresa de forma centralizada.



The screenshot displays the AWS Organizations console interface. At the top, the breadcrumb navigation shows 'AWS Organizations' followed by 'Contas da AWS'. The main heading is 'Contas da AWS', with an orange button 'Adicionar uma conta da AWS' to its right. Below the heading, a descriptive paragraph states that listed accounts are members of the organization and that the management account is responsible for paying bills. A search bar is present with the placeholder text 'Encontre contas da AWS por nome, e-mail ou ID da conta. Encontre uma UO pelo ID exato'. To the right of the search bar are two tabs: 'Hierarquia' (selected) and 'Lista'. Below the search bar, the 'Estrutura organizacional' section shows a tree view with a single node labeled 'Root' and a sub-label 'r-zell'. A column header 'Data de criação/ingresso da conta' is visible on the right side of the tree view.

## 11. Integrantes do Grupo 3

### Participantes

1. Agnaldo Oliveira
2. Alex E G Coimbra
3. Andre Do Amaral
4. Claudio Fernandes Rejes Junior
5. Clayton Roberto Da Silva
6. Daniel Martins Reis
7. Danilo Dias
8. Edinaldo Vieira Da Silva
9. Edson J P Lima
10. Eduardo C. Vilaro
11. Giovanni Grippo
12. Jorge Staub
13. Luan Fernandes Dos Santos
14. Luciano Junior
15. Marcelo Cares Oliveira
16. Mauricio Domingues Madrigal
17. Ricardo Vieira Soares
18. Thiago Amâncio Da Silva
19. Yan Moreira
20. Carlos Roberto de Oliveira
21. Felipe Nery Machado
22. José Tadeu da Mota Silveira
23. Ramon Alberto Lima Cruz