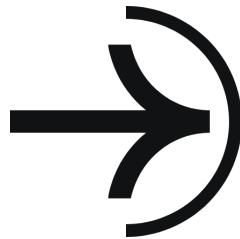


AWS & DEVSECOPS



Atividade referente aos Conhecimento em AWS e
Docker

Claudio Gabriel Kosooski

Frederico Westphalen, 23/10/2023

1. instalação e configuração do DOCKER ou CONTAINERD no host EC2;
Ponto adicional para o trabalho utilizar a instalação via script de Start Instance (user_data.sh)
 2. Efetuar Deploy de uma aplicação Wordpress com:
container de aplicação
RDS database Mysql
 3. configuração da utilização do serviço EFS AWS para estáticos do container de aplicação Wordpress
 4. configuração do serviço de Load Balancer AWS para a aplicação Wordpress
- Pontos de atenção:
- o não utilizar ip público para saída dos serviços WP
(Evitem publicar o serviço WP via IP Público)
 - o sugestão para o tráfego de internet sair pelo LB (Load Balancer Classic)
 - o pastas públicas e estáticos do wordpress sugestão de utilizar o EFS (Elastic File System)
 - o Fica a critério de cada integrante (ou dupla) usar Dockerfile ou Dockercompose;
 - o Necessário demonstrar a aplicação wordpress funcionando (tela de login)
 - o Aplicação Wordpress precisa estar rodando na porta 80 ou 8080;
 - o Utilizar repositório git para versionamento;
 - o Criar documentação

1.0 - Ambiente AWS:

- **Criação de um par de chaves;**

A criação da chave pública ocorre no momento da criação da instância EC2, onde, o ideal é criar uma chave RSA para acesso a instância via SSH denominada `minha_chave_pb.pem`.

▼ Key pair (login) [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

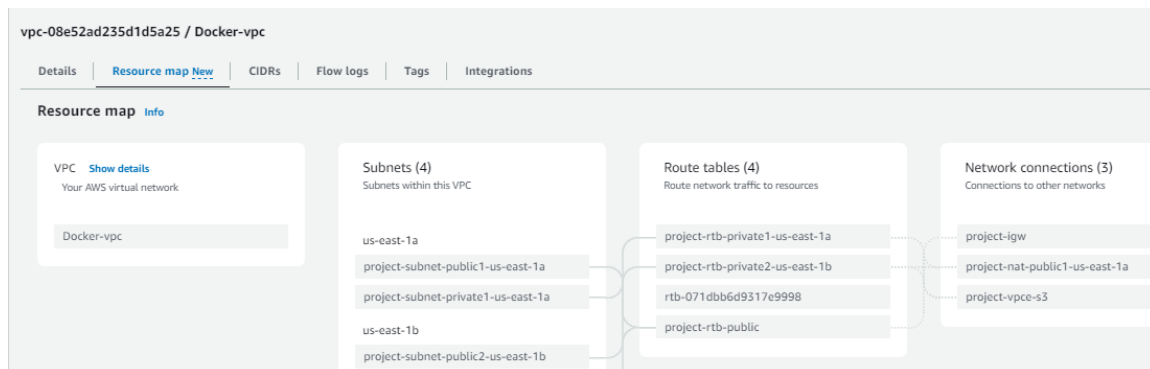
Key pair name - *required*

minha_chave_pb ▼

↻ [Create new key pair](#)

- **Criação de uma VPC e devidas Subnets;**

Para a configuração do ambiente, é necessária a criação de uma VPC apontando para duas zonas de disponibilidade diferentes, como faz se necessário para prover um ambiente de alta disponibilidade com Load Balancer



- **Criação de um Security Group;**

Neste caso o criei no momento da criação da VPC e vinculei na mesma

sg-04c4e6706e5a55356	My_docker_sg	vpc-08e52ad235d1d5a25
----------------------	--------------	-----------------------

- **Reserva de um Elastic IP para a configuração do Load Balancer**

No menu Elastic IP, em Allocate Elastic IP address, é possível alocar um determinado IP4 ou IP6 público

1.1 - Criar 2 instâncias EC2 com o sistema operacional Amazon Linux 2 (Família t3.small, 16 GB SSD);

Durante a criação, atentar para as Tags padrões de criação durante o PB além da opção “volumes”, as configurações de armazenamento e de processamento, a seleção da VPC correta e a subnet (1 instância com subnet diferente da outra para não dar conflito de zona de disponibilidade igual)

▼ Network settings Info

VPC - required Info

vpc-08e52ad235d1d5a25 (Docker-vpc)
10.0.0.0/16

↻

Subnet Info

subnet-0dba6c2cf8974106a project-subnet-public1-us-east-1a
VPC: vpc-08e52ad235d1d5a25 Owner: 335505840552
Availability Zone: us-east-1a IP addresses available: 4090 CIDR: 10.0.0.0/20

↻ Create new subnet

Auto-assign public IP Info

Enable

Firewall (security groups) Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☐ Create security group

☒ Select existing security group

Common security groups Info

Select security groups

My_docker_sg sg-04c4e6706e5a55356 X
VPC: vpc-08e52ad235d1d5a25

↻ Compare security group rules

Security groups that you add or remove here will be added to or removed from all your network interfaces.

► Advanced network configuration


▼ Configure storage Info Advanced

1x 16 GiB gp2 Root volume (Not encrypted)

Para as instâncias que serão iniciadas pelo auto scaling que será configurado nos próximos passos, foi criado um script para automatizar toda a configuração inicial das máquinas, como Atualização do sistema, instalação do Docker, do Wordpress, do Apache e demais configurações necessárias.

User data - optional [Info](#)

Upload a file with your user data or enter it in the field.

 Choose file

```
#!/bin/bash
sudo su
yum update -y # Atualiza o sistema
yum install docker -y # Instala o Docker
service docker start # Inicia o serviço Docker
systemctl enable docker # iniciar serviço sempre
usermod -aG docker ec2-user # Adiciona o usuário ec2-user ao grupo docker

# Instala o Docker Compose
curl -L "https://github.com/docker/compose/releases/latest/download/docker-
compose-$(uname -s)-$(uname -m)" -o /usr/local/bin/docker-compose
chmod +x /usr/local/bin/docker-compose

# Cria um diretório para armazenar os arquivos do Docker Compose
mkdir -p /opt/wordpress
```

☐ User data has already been base64 encoded

#!/bin/bash

sudo su

Atualiza o sistema

yum update -y

Instala o Docker

yum install docker -y

service docker start

systemctl enable docker

usermod -aG docker ec2-user

Instala o Docker Compose

curl -L

"https://github.com/docker/compose/releases/latest/download/docker-compose-\$(una
me -s)-\$(uname -m)" -o /usr/local/bin/docker-compose

chmod +x /usr/local/bin/docker-compose

Cria um diretório para armazenar os arquivos do Docker Compose

mkdir -p /opt/wordpress

Docker Compose YAML

cat <<EOL > /opt/wordpress/docker-compose.yml

version: '3'

services:

wordpress:

image: wordpress

ports:

- "80:80"

environment:

WORDPRESS_DB_HOST: docker.crqtaqvrgwhj.us-east-1.rds.amazonaws.com

WORDPRESS_DB_USER: admin

WORDPRESS_DB_NAME: docker

WORDPRESS_DB_PASSWORD: dbdocker

volumes:

- /var/www/html:/var/www/html

EOL

Executa o Docker Compose

cd /opt/wordpress

sudo ln -s /usr/local/bin/docker-compose /usr/bin/docker-compose

docker-compose up -d

```
[root@ip-10-0-15-202 wordpress]# docker-compose --version
bash: docker-compose: command not found
[root@ip-10-0-15-202 wordpress]# sudo ln -s /usr/local/bin/docker-compose /usr/bin/docker-compose
[root@ip-10-0-15-202 wordpress]# docker-compose --version
Docker Compose version v2.23.0
[root@ip-10-0-15-202 wordpress]#
```

1.2 - Criar o Banco de Dados RDS;

MySQL 8.0.33

Templates

Choose a sample template to meet your use case.

☐ Production
Use defaults for high availability and fast, consistent performance.

☐ Dev/Test
This instance is intended for development use outside of a production environment.

☒ Free tier
Use RDS Free Tier to develop new applications, test existing applications, or gain hands-on experience with Amazon RDS.
[Info](#)

Availability and durability

Deployment options [Info](#)
The deployment options below are limited to those supported by the engine you selected above.

- ☒ Multi-AZ DB Cluster - *new*
Creates a DB cluster with a primary DB instance and two readable standby DB instances, with each DB instance in a different Availability Zone (AZ). Provides high availability, data redundancy and increases capacity to serve read workloads.
- ☐ Multi-AZ DB instance (not supported for Multi-AZ DB cluster snapshot)
Creates a primary DB instance and a standby DB instance in a different AZ. Provides high availability and data redundancy, but the standby DB instance doesn't support connections for read workloads.
- ☐ Single DB instance (not supported for Multi-AZ DB cluster snapshot)
Creates a single DB instance with no standby DB instances.

Settings

DB instance identifier [Info](#)
Type a name for your DB instance. The name must be unique across all DB instances owned by your AWS account in the current AWS Region.

docker

The DB instance identifier is case-insensitive, but is stored as all lowercase (as in "mydbinstance"). Constraints: 1 to 60 alphanumeric characters or hyphens. First character must be a letter. Can't contain two consecutive hyphens. Can't end with a hyphen.

[Credentials Settings](#)

Services

Search

[Alt+S]

Docker-vpc (vpc-08e52ad235d1d5a25)
4 Subnets, 2 Availability Zones

▼

Only VPCs with a corresponding DB subnet group are listed.

ⓘ After a database is created, you can't change its VPC.

DB subnet group

Info

Choose the DB subnet group. The DB subnet group defines which subnets and IP ranges the DB instance can use in the VPC that you selected.

default-vpc-08e52ad235d1d5a25
4 Subnets, 2 Availability Zones

▼

Public access

Info

☒ Yes

RDS assigns a public IP address to the database. Amazon EC2 instances and other resources outside of the VPC can connect to your database. Resources inside the VPC can also connect to the database. Choose one or more VPC security groups that specify which resources can connect to the database.

☐ No

RDS doesn't assign a public IP address to the database. Only Amazon EC2 instances and other resources inside the VPC can connect to your database. Choose one or more VPC security groups that specify which resources can connect to the database.

VPC security group (firewall)

Info

Choose one or more VPC security groups to allow access to your database. Make sure that the security group rules allow the appropriate incoming traffic.

☒ Choose existing
Choose existing VPC security groups

☐ Create new
Create new VPC security group

Existing VPC security groups

Choose one or more options

▼

My_docker_sg

×

Availability Zone

Info

No preference

▼

▼ Additional configuration

Database options, encryption turned on, backup turned on, backtrack turned off, maintenance, CloudWatch Logs, delete protection turned off.

Database options

Initial database name [Info](#)

If you do not specify a database name, Amazon RDS does not create a database.

DB parameter group [Info](#)

Option group [Info](#)

Backup

☒ Enable automated backups

Creates a point-in-time snapshot of your database

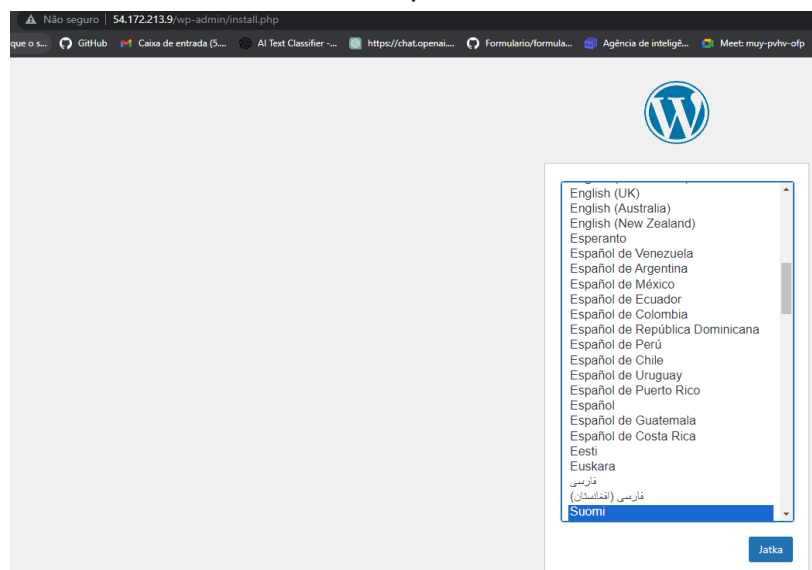
⚠ Please note that automated backups are currently supported for InnoDB storage engine only. If you are using MyISAM, refer to details [here](#).

Backup retention period [Info](#)

The number of days (1-35) for which automatic backups are kept.

day

Acesso ok na instância, BD e Wordpress



1.3 Load Balancer

Selecionar subnet pública

Basic configuration

Load balancer name
Name must be unique within your AWS account and can't be changed after the load balancer is created.

A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

Scheme | [Info](#)
Scheme can't be changed after the load balancer is created.

☒ **Internet-facing**
An internet-facing load balancer routes requests from clients over the internet to targets. Requires a public subnet. [Learn more](#)

☐ **Internal**
An internal load balancer routes requests from clients to targets using private IP addresses.

Network mapping | [Info](#)
The load balancer routes traffic to targets in the selected subnets, and in accordance with your network settings.

VPC | [Info](#)
Select the virtual private cloud (VPC) for your targets or you can [create a new VPC](#). Only VPCs with an internet gateway are available for selection. The selected VPC cannot be changed after the load balancer is created. When selecting a VPC for your load balancer, ensure each subnet has a CIDR block with at least a /27 bitmask and at least 8 free IP addresses. [Learn more](#)

Docker-vpc
vpc-08e52ad235d1d5a25
IPv4: 10.0.0.0/16

▼

↺

Mappings
Select at least one Availability Zone and one subnet for each zone. We recommend selecting at least two Availability Zones. The load balancer will route traffic only to targets in the selected Availability Zones. Availability Zones that are not supported by the load balancer or the VPC are not available for selection.

☒ **us-east-1a (use1-az4)**

Subnet

subnet-0dba6c2cf8974106a

project-subnet-public1-us-east-1a ▼

IPv4 address

Assigned by AWS

☒ **us-east-1b (use1-az6)**

Subnet

subnet-0baaf72237cee29d9

project-subnet-public2-us-east-1b ▼

IPv4 address

Assigned by AWS

Security groups | [Info](#)
A security group is a set of firewall rules that control the traffic to your load balancer. Select an existing security group, or you can create a new security group.

Security groups

Select up to 5 security groups

▼

↺

My_docker_sg
sg-04c4e6706e5a55356 VPC: vpc-08e52ad235d1d5a25

×

Colocar as TAGS padrão no ambiente

Instances (0)

[Remove](#)[Add](#)

You can add instances to register as targets of the load balancer. Alternatively, after your load balancer is created, you can add it to an Amazon EC2 Auto Scaling group to ensure the correct number of instances to handle the load for your application. For maximum fault tolerance, we recommend maintaining approximately equivalent numbers of instances in each Availability Zone.



Instance ID	Name	State	Security groups
-------------	------	-------	-----------------

No instances added

Attributes

Creating your load balancer using the console gives you the opportunity specify additional features at launch. You can also find and adjust these settings in the load balancer's section after your load balancer is created.

☒ Enable cross-zone load balancing

With cross-zone load balancing, each load balancer node for your Classic Load Balancer distributes requests evenly across the registered instances in all enabled Availability Zones. If cross-zone load balancing is disabled, each load balancer node distributes requests evenly across the registered instances in its Availability Zone only. Classic Load Balancers created before 2015 have cross-zone load balancing disabled by default. After you create a Classic Load Balancer, you can enable or disable cross-zone load balancing at any time.

☒ Enable connection draining

Applicable to instances that are deregistering, this feature allows existing connections to complete (during a specified draining interval) before reporting the instance as deregistered. [Learn more](#)

Timeout (draining interval)

The maximum time for the load balancer to allow existing connections to complete. When the maximum time limit is reached, the load balancer forcibly closes any remaining connections and reports the instance as deregistered.

 seconds

Valid values: 1-3600 (integers only)

▼ Load balancer tags - optional

Consider adding tags to your load balancer. Tags enable you to categorize your AWS resources so you can more easily manage them. The 'Key' is required, but 'Value' is optional. For example, you can have Key = production-webserver, or Key = webserver, and Value = production.

Key	Value - optional	
<input type="text" value="Name"/>	<input type="text" value="PB - FW - A - RG - SB - HA"/>	Remove
<input type="text" value="CostCenter"/>	<input type="text" value="C092000004"/>	Remove
<input type="text" value="Project"/>	<input type="text" value="PB - FW - A - RG - SB - HA"/>	Remove

[Add new tag](#)

You can add up to 47 more tags.

Criação dos Target-group

EC2 > Grupos-alvo > Criar grupo-alvo

Passo 1

Especifique os detalhes do grupo

Passo 2

Registrar alvos

Especifique os detalhes do grupo

Seu balanceador de carga roteia solicitações para os destinos em um grupo de destino e executa verificações de integridade nos destinos.

Configuração básica

As configurações nesta seção não podem ser alteradas após a criação do grupo de destino.

Escolha um tipo de destino

☒ Instâncias

- Oferece suporte ao balanceamento de carga para instâncias em uma VPC específica.
- Facilita o uso do [Amazon EC2 Auto Scaling](#) para gerenciar e dimensionar sua capacidade EC2.

☐ Endereços IP

- Oferece suporte ao balanceamento de carga para VPC e recursos locais.
- Facilita o roteamento para vários endereços IP e interfaces de rede na mesma instância.
- Oferece flexibilidade com arquiteturas baseadas em microsserviços, simplificando a comunicação entre aplicativos.
- Suporta alvos IPv6, permitindo comunicação IPv6 ponta a ponta e NAT IPv4 para IPv6.

☐ Função Lambda

- Facilita o roteamento para uma única função Lambda.
- Acessível apenas para Application Load Balancers.

☐ Balanceador de carga de aplicativos

- Oferece flexibilidade para um Network Load Balancer aceitar e rotear solicitações TCP em uma VPC específica.
- Facilita o uso de endereços IP estáticos e PrivateLink com um Application Load Balancer.

Nome do grupo-alvo

tgDocker

São permitidos no máximo 32 caracteres alfanuméricos incluindo hífens, mas o nome não deve começar ou terminar com hífen.

Protocolo

Porta

TCP

:

80

1-65535

IP address type

Only targets with the indicated IP address type can be registered to this target group.

☒ IPv4

Each instance has a default network interface (eth0) that is assigned the primary private IPv4 address. The instance's primary private IPv4 address is the one that will be applied to the target.

☐ IPv6

Each instance you register must have an assigned primary IPv6 address. This is configured on the instance's default network interface (eth0). [Learn more](#)

VPC

Selecione a VPC com as instâncias que você deseja incluir no grupo de destino. Somente VPCs compatíveis com o tipo de endereço IP selecionado acima estão disponíveis nesta lista.

Docker-vpc

vpc-08e52ad235d1d5a25

selecionando instâncias

EC2 > Grupos-alvo > Criar grupo-alvo

Passo 1

[Especificar detalhes do grupo](#)

Passo 2

Registrar alvos

Registrar targets

This is an optional step to create a target group. However, to ensure that your load balancer routes traffic to this target group you must register your targets.

Available instances (2/5)

Filter instances

Instance ID	Name	State	Security groups	Zone	Private IPv4 address	Subnet ID
<input type="checkbox"/> i-027992e11a65e100	PE - FW - A - RG - SB - HA	Running	My_docker_sg	us-east-1a	10.0.1.76	subnet-0dbdc2f8974106a
<input checked="" type="checkbox"/> i-098a19050a0169d74	PE - FW - A - RG - SB - HA	Running	My_docker_sg	us-east-1a	10.0.5.82	subnet-0dbdc2f8974106a
<input type="checkbox"/> i-09b0998971e09c133	PE - FW - A - RG - SB - HA	Running	My_docker_sg	us-east-1a	10.0.5.125	subnet-0dbdc2f8974106a
<input checked="" type="checkbox"/> i-053938676c133c5d	PE - FW - A - RG - SB - HA	Running	My_docker_sg	us-east-1b	10.0.22.157	subnet-0baaf72237cae29d9
<input type="checkbox"/> i-04ab7816200b0275c	PE - FW - A - RG - SB - HA	Running	My_docker_sg	us-east-1b	10.0.27.218	subnet-0baaf72237cae29d9

2 selected

Ports for the selected instances

Ports for routing traffic to the selected instances.

80

1-65535 (separate multiple ports with commas)

Include as pending below

Target group

Successfully created target group: tg001

EC2 > Target groups

Target groups (1) [Info](#)

[Refresh](#) [Actions](#) [Create target group](#)

<input type="checkbox"/>	Name	ARN	Port	Protocol	Target type	Load balancer	VPC ID
<input type="checkbox"/>	tg001	arn:aws:elasticloadbalanci...	80	HTTP	Instance	None associated	vpc-08e52ad235d1d5a25


configurações padrão na criação

<input checked="" type="checkbox"/>	Name	DNS name	State	VPC ID	Availability Zones	Type	Date created
<input checked="" type="checkbox"/>	balancer01	balancer01-828884222.us...	Active	vpc-08e52ad235d1d5a25	2 Availability Zones	application	October 26, 2023, 00:58 (UTC-03:00)

Instância inicial funcionando com o LoadBalancer

balancer01-828884222.us-east-1.elb.amazonaws.com/wp-admin/install.php

Caixa de entrada (5....) AI Text Classifier -... https://chat.openai... Formulario/formula... Agência de inteligê... Meet: muy-pvhv-ofp



English (United States)
Afrikaans
አማርኛ
Aragonés
العربية
العربية المغربية
অসমীয়া
گۆنئی آذربایجان
Azerbaijani dili
Беларуская мова
Български
বাংলা
བོད་སྐད་
Bosanski
Català
Cebuano
Čeština
Cymraeg
Dansk
Deutsch (Österreich)
Deutsch (Sie)
Deutsch

Continue

Choose launch template Info

Specify a launch template that contains settings common to all EC2 instances that are launched by this Auto Scaling group.

Name

Auto Scaling group name
Enter a name to identify the group.

asg001

Must be unique to this account in the current Region and no more than 255 characters.

Launch template Info

i For accounts created after May 31, 2023, the EC2 console only supports creating Auto Scaling groups with launch templates. Creating Auto Scaling groups with launch configurations is not recommended but still available via the CLI and API until December 31, 2023.

Launch template
Choose a launch template that contains the instance-level settings, such as the Amazon Machine Image (AMI), instance type, key pair, and security groups.

myinstance1a

[Create a launch template](#)

Version

1

[Create a launch template version](#)

Description	Launch template	Instance type
1	myinstance1a ↗ lt-0bf33b1a92c7332fd	t3.small
AMI ID	Security groups	Request Spot Instances
ami-01eccbf80522b562b	-	No
Key pair name	Security group IDs	
minha_chave_pb	sg-04c4e6706e5a55356 ↗	

Additional details

Storage (volumes)	Date created
/dev/xvda	Thu Oct 26 2023 00:14:16 GMT-0300 (Horário Padrão de Brasília)

Cancel **Next**

Configure group size and scaling policies - *optional* [Info](#)

Set the desired, minimum, and maximum capacity of your Auto Scaling group. You can optionally add a scaling policy to dynamically scale the number of instances in the group.

Group size - *optional* [Info](#)

Specify the size of the Auto Scaling group by changing the desired capacity. You can also specify minimum and maximum capacity limits. Your desired capacity must be within the limit range.

Desired capacity type

Choose the unit of measurement for the desired capacity value.

Desired capacity

Minimum capacity

Maximum capacity

Scaling policies - *optional*

Choose whether to use a scaling policy to dynamically resize your Auto Scaling group to meet changes in demand. [Info](#)

☐ Target tracking scaling policy
Choose a desired outcome and leave it to the scaling policy to add and remove capacity as needed to achieve that outcome.

☒ None

Instance scale-in protection - *optional*

Instance scale-in protection

If protect from scale in is enabled, newly launched instances will be protected from scale in by default.

☐ Enable instance scale-in protection

[Cancel](#)

[Skip to review](#)

[Previous](#)

[Next](#)

BWS	Services	Search	[Alt+S]	N. Virginia	AdministratorAccess/taudio.kozoski.ph@compasso.com.br
IAM	Launch Templates (1) Info	Search	Actions	Create launch template	
Launch Template ID	Launch Template Name	Default Version	Latest Version	Create Time	Created By
lt-02b936c9ff34c34223	TemplateDocker	1	1	2023-10-23T01:00:59.000Z	arn:aws:sts:335505840552:assumed-role/AWSReservedSSO_AdministratorAccess_f69ca08f6ac166d5/cia...

Network mapping [Info](#)

The load balancer routes traffic to targets in the selected subnets, and in accordance with your IP address settings.

VPC [Info](#)

Select the virtual private cloud (VPC) for your targets or you can create a new VPC [🔗](#). Only VPCs with an internet gateway are enabled for selection. The selected VPC can't be changed after the load balancer is created. To confirm the VPC for your targets, view your target groups [🔗](#).

Docker-vpc
vpc-08e52ad235d1d5a25
IPv4: 10.0.0.0/16



Mappings [Info](#)

Select at least two Availability Zones and one subnet per zone. The load balancer routes traffic to targets in these Availability Zones only. Availability Zones that are not supported by the load balancer or the VPC are not available for selection.

☒ **us-east-1a (use1-az4)**

Subnet
subnet-0dba6c2cf8974106a project-subnet-public1-us-east-1a ▼

IPv4 address
Assigned by AWS

☒ **us-east-1b (use1-az6)**

Subnet
subnet-0baaf72237cee29d9 project-subnet-public2-us-east-1b ▼

IPv4 address
Assigned by AWS

Security groups [Info](#)

A security group is a set of firewall rules that control the traffic to your load balancer. Select an existing security group, or you can create a new security group [🔗](#).

Security groups

Select up to 5 security groups

My_docker_sg
sg-04c4e6706e5a55356 VPC: vpc-08e52ad235d1d5a25 ✕

Listeners and routing [Info](#)

A listener is a process that checks for connection requests using the port and protocol you configure. The rules that you define for a listener determine how the load balancer routes requests to its registered targets.

▼ Listener HTTP:80

Remove

Protocol HTTP ▼

Port 80
1-65535

Default action [Info](#)
Forward to tg001
Target type: Instance, IPv4
[Create target group 🔗](#)

HTTP ▼

Listener tags - optional

Consider adding tags to your listener. Tags enable you to categorize your AWS resources so you can more easily manage them.

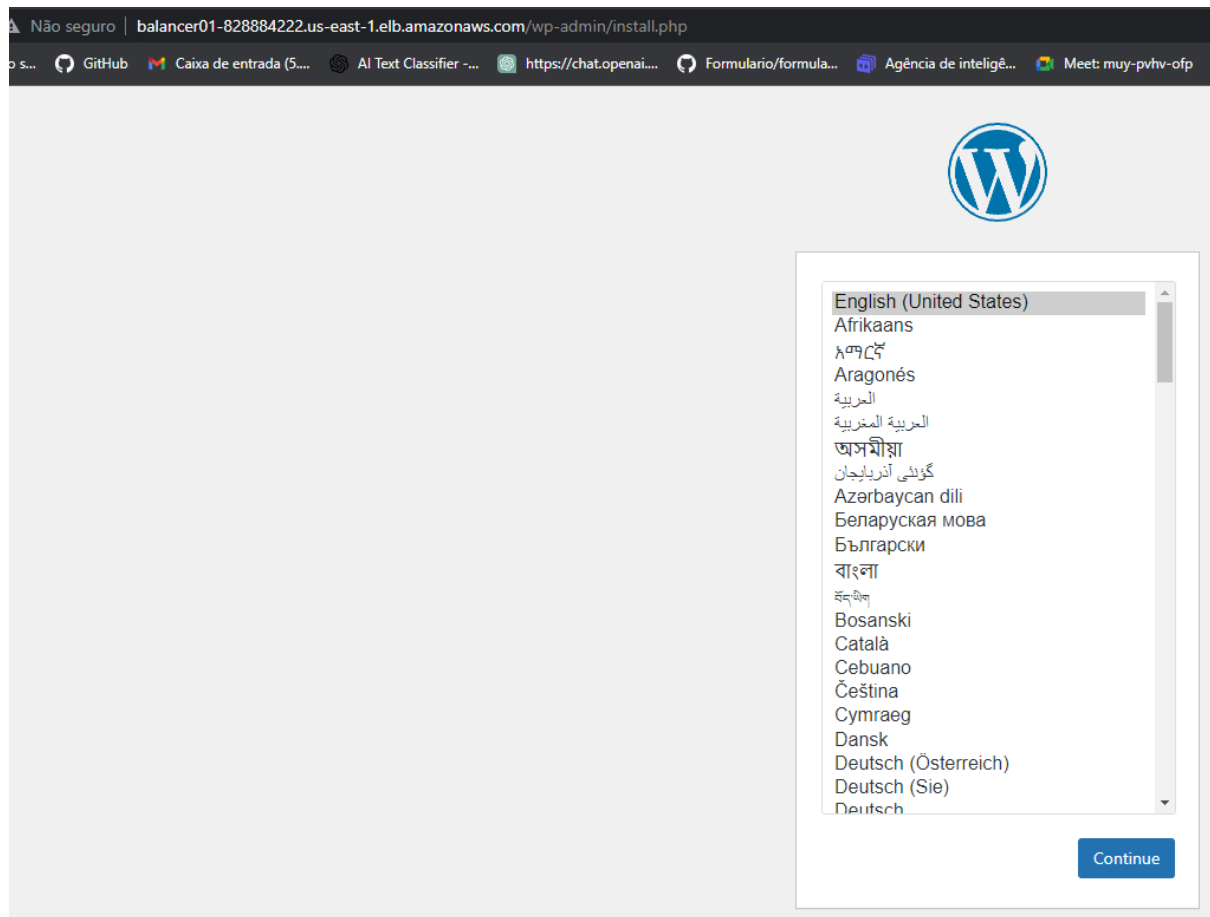
Add listener tag

You can add up to 50 more tags.

Add listener

selecciona a vpc e as zonas/subnets que deseja

<input checked="" type="checkbox"/>	Name	DNS name	State	VPC ID	Availability Zones	Type	Date created
<input checked="" type="checkbox"/>	balancer01	balancer01-828884222.us-...	Active	vpc-08e52ad235d1d5a25	2 Availability Zones	application	October 26, 2023, 00:58 (UTC-03:00)



2.0 Criação do EFS

...