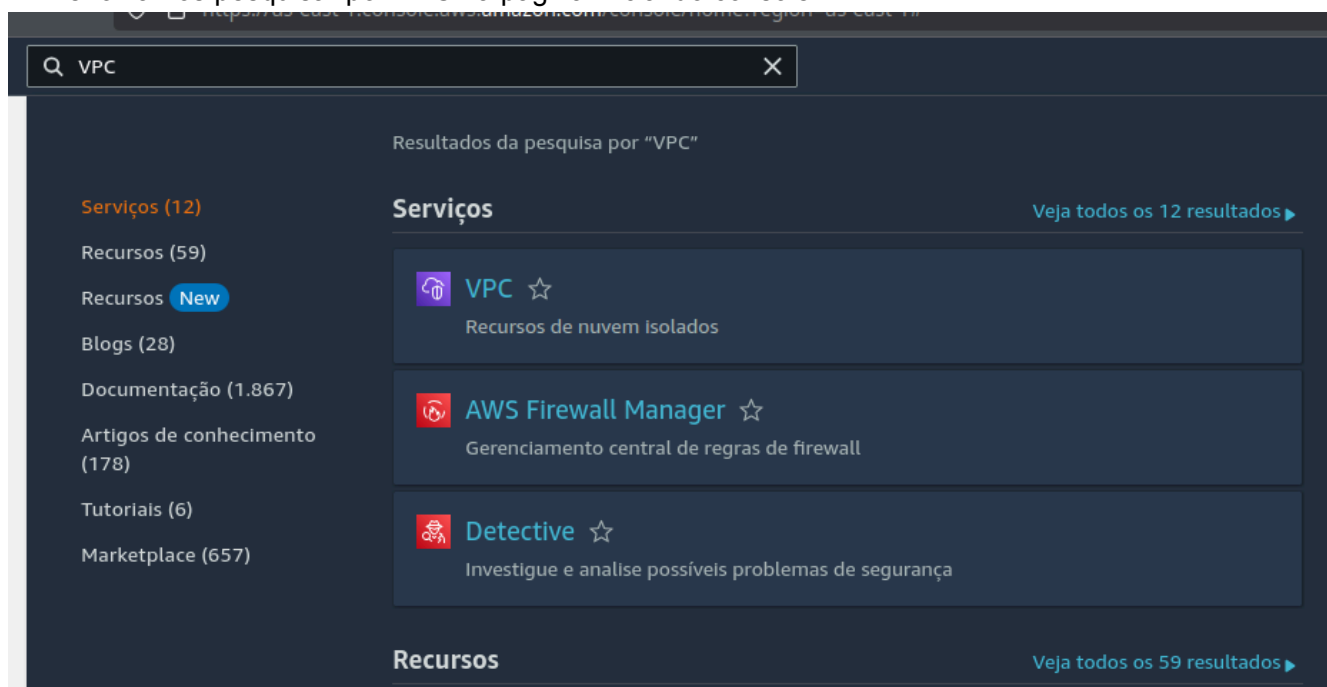


Exemplo - Rede e Conectividade - Comp Nuvem 2024

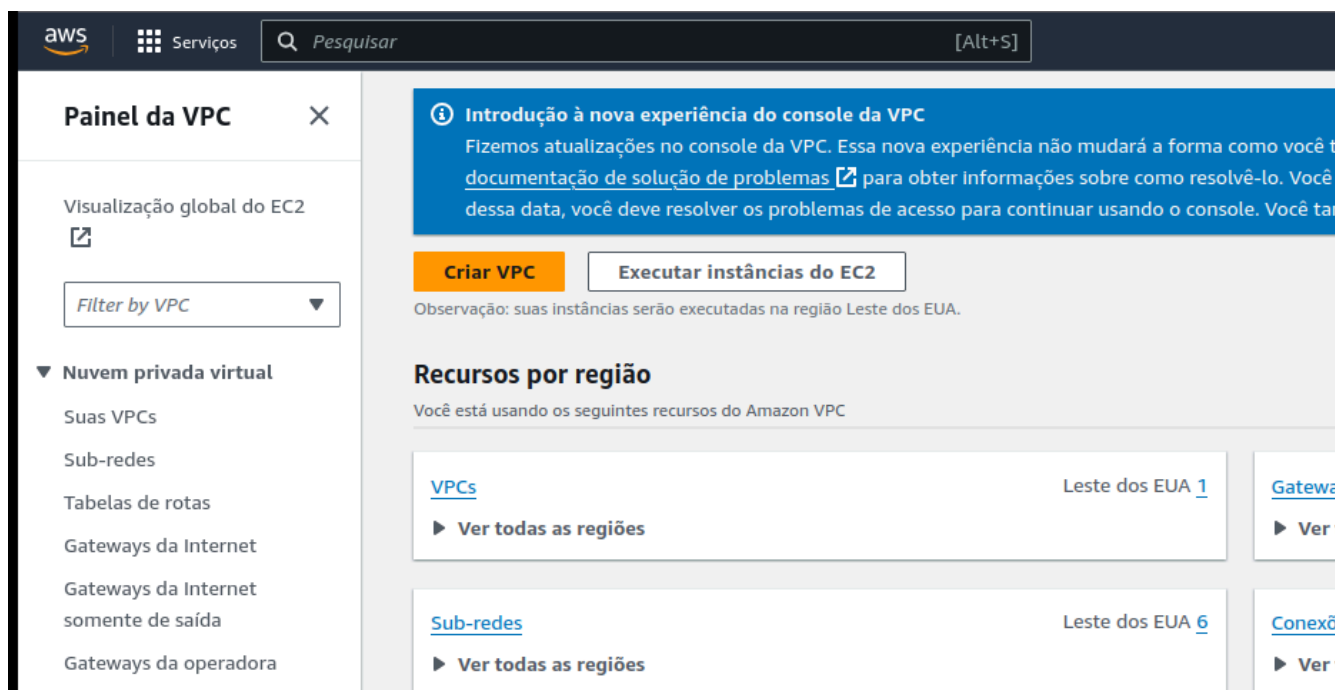
Neste exemplo será feita a criação de uma VPC, duas máquinas ec2 públicas e duas máquinas RDS privadas, o código que será utilizado está em no site do [github](#)

Criando a VPC

Primeiro vamos pesquisar por VPC na página inicial do console



Clicaremos em criar VPC



Vamos alterar o bloco CIDR IPv4 com o valor `10.50.0.0/16` a escolha do valor é arbitrária é feita apenas para facilitar as configurações necessárias posteriormente

Também vamos colocar para 0 o número de redes privadas, isso será importante posteriormente.

Depois é clicar em criar VPC

Configurações da VPC

Recursos a serem criados [Informações](#)

Crie apenas o recurso da VPC ou a VPC e outros recursos de rede.

☐ Somente VPC

☒ VPC e muito mais

Geração automática da etiqueta de nome [Informações](#)

Insira um valor para a etiqueta de nome. Esse valor será usado para gerar automaticamente etiquetas de Nome para todos os recursos na VPC.

☒ Gerar automaticamente

projeto

Bloco CIDR IPv4 [Informações](#)

Passo 1

Determine o IP inicial e o tamanho da VPC usando notação CIDR.

10.50.0.0/16

65,536 IPs

O tamanho do bloco CIDR deve estar entre /16 e /28.

Bloco CIDR IPv6 [Informações](#)

☒ Nenhum bloco CIDR IPv6

☐ Bloco CIDR IPv6 fornecido pela Amazon

Localização [Informações](#)

Padrão

Número de zonas de disponibilidade (AZs) [Informações](#)

Escolha o número de AZs em que as sub-redes deverão ser provisionadas. Para alta disponibilidade, recomendamos pelo menos duas AZs.

1

2

3

► Personalizar AZs

Número de sub-redes públicas [Informações](#)

O número de sub-redes públicas a serem adicionadas à sua VPC. Use sub-redes públicas para aplicações Web que precisam estar publicamente acessíveis pela Internet.

0

2

Número de sub-redes privadas [Informações](#)

O número de sub-redes privadas a serem adicionadas à sua VPC. Use sub-redes privadas para proteger recursos de backend que não precisam de acesso público.

0

2

4

Passo 2

► Personalizar blocos CIDR de sub-redes

Gateways NAT (USD) [Informações](#)

Escolha o número de zonas de disponibilidade (AZs) nas quais criar gateways NAT. Observe que há uma cobrança para cada gateway NAT.

Nenhuma

Em 1 AZ

1 por AZ

Endpoints da VPC [Informações](#)

Os endpoints podem ajudar a reduzir as cobranças do gateway NAT e melhorar a segurança acessando o S3 diretamente da VPC. Por padrão, a política de acesso integral será usada. Você pode personalizar essa política a qualquer momento.

Nenhuma **Gateway do S3**

Opções de DNS [Informações](#)

- ☒ Habilitar nomes de host DNS
- ☒ Habilitar resolução de DNS

► **Tags adicionais** Passo 3

Cancelar **Criar VPC**

Criando as instâncias EC2

Na página principal do EC2, clicaremos em *Executar instância*.

The screenshot shows the AWS Management Console for the EC2 service. The left sidebar contains navigation links for 'Painel EC2', 'Instâncias', 'Imagens', and 'Elastic Block Store'. The main content area displays 'Recursos' (Resources) with a table of usage metrics for the 'Região Leste dos EUA (Norte da Virgínia)'. Below this, the 'Executar instância' (Launch Instance) button is highlighted with a red rectangle. The 'Integridade do serviço' (Service Health) section shows the region as 'Leste dos EUA (Norte da Virgínia)' and the status as 'Status'.

Recursos	
Instâncias (em execução)	2
Grupos de posicionamento	0
Grupos do Auto Scaling	0
Instâncias	2
Load balancers	0
Snapshots	0
Capacity Reservations	0
Grupos de segurança	3
Hosts dedicados	0
IPs elásticos	0
Pares de chaves	1
Volumes	2

Executar instância

Para começar, execute uma instância do Amazon EC2, que é um servidor virtual na nuvem.

Executar instância ▼

Migrar um servidor

Integridade do serviço

AWS Health Dashboard

Região: Leste dos EUA (Norte da Virgínia)

Status

Na página de criação de uma instância, primeiro vamos nomear a instância como `_servidor-web-1`

NÃO alteraremos *Imagens de aplicação e de sistema operacional (imagem de máquina da Amazon)* e *Tipo de instância*

Em *Par de chaves (login)* deixaremos como `vockey`, mas pode ser qualquer chave a sua escolha.

▼ Par de chaves (login) [Informações](#)

Você pode usar um par de chaves para se conectar com segurança à sua instância. Certifique-se de ter acesso ao par de chaves selecionado antes de executar a instância.

Nome do par de chaves - *obrigatório*

vockey ▼

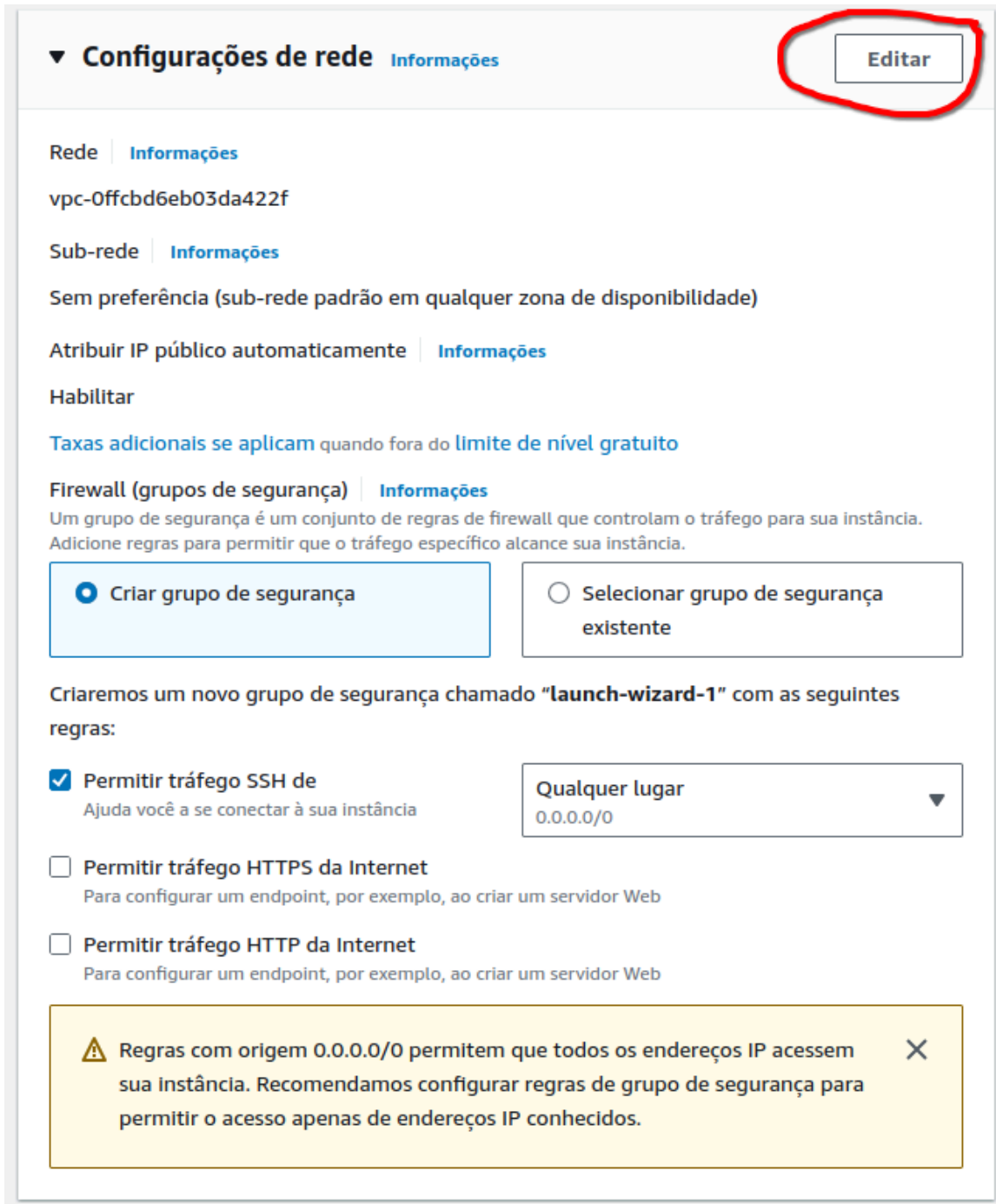


[Criar novo par de chaves](#)

Configurações de rede

Uma das partes mais importantes deste experimento, **é importante muita cautela!**

Primeiro clicamos em *editar*.



▼ **Configurações de rede** [Informações](#) **Editar**

Rede | [Informações](#)
vpc-0ffc6d6eb03da422f

Sub-rede | [Informações](#)
Sem preferência (sub-rede padrão em qualquer zona de disponibilidade)

Atribuir IP público automaticamente | [Informações](#)
Habilitar

[Taxas adicionais se aplicam](#) quando fora do limite de nível gratuito

Firewall (grupos de segurança) | [Informações](#)
Um grupo de segurança é um conjunto de regras de firewall que controlam o tráfego para sua instância. Adicione regras para permitir que o tráfego específico alcance sua instância.

☒ Criar grupo de segurança ☐ Selecionar grupo de segurança existente

Criaremos um novo grupo de segurança chamado **"launch-wizard-1"** com as seguintes regras:

☒ Permitir tráfego SSH de Qualquer lugar 0.0.0.0/0
Ajuda você a se conectar à sua instância

☐ Permitir tráfego HTTPS da Internet
Para configurar um endpoint, por exemplo, ao criar um servidor Web

☐ Permitir tráfego HTTP da Internet
Para configurar um endpoint, por exemplo, ao criar um servidor Web

⚠ Regras com origem 0.0.0.0/0 permitem que todos os endereços IP acessem sua instância. Recomendamos configurar regras de grupo de segurança para permitir o acesso apenas de endereços IP conhecidos. ✕

Trocamos o VPC para o que nós criamos anteriormente, para identificar a VPC, basta checar o número em cinza que será o mesmo número que colocamos anteriormente, nesse caso será 10.50.0.0/16 .

Importante! Habilite também a atribuição de IP público automaticamente

Também escreva o nome do grupo de segurança para facilitação da configuração de outra EC2

E configure para abrir a porta 8080, para que o EC2 consiga se conectar ao RDS, no final, a sua configuração deverá se parecer com esta debaixo, com as partes importantes marcadas em vermelho.

▼ Configurações de rede Informações

VPC - obrigatório Informações

vpc-019e61ab62cd819aa (projeto-vpc)
10.50.0.0/16



Sub-rede Informações

subnet-0160f0612421015b9
projeto-subnet-public2-us-east-1b
VPC: vpc-019e61ab62cd819aa Proprietário: 055999873194
Zona de disponibilidade: us-east-1b
Zone type: Zona de disponibilidade
Endereços IP disponíveis: 4091 CIDR: 10.50.16.0/20



[Criar nova sub-rede](#)

Atribuir IP público automaticamente Informações

Habilitar

[Taxas adicionais se aplicam](#) quando fora do [limite de nível gratuito](#)

Firewall (grupos de segurança) Informações

Um grupo de segurança é um conjunto de regras de firewall que controlam o tráfego para sua instância. Adicione regras para permitir que o tráfego específico alcance sua instância.

☒ Criar grupo de segurança

☐ Selecionar grupo de segurança existente

Nome do grupo de segurança - obrigatório

experimento-vpc

Esse grupo de segurança será adicionado a todas as interfaces de rede. Não é possível editar o nome após a criação do grupo de segurança. O comprimento máximo é de 255 caracteres. Os caracteres válidos são: a-z, A-Z, 0-9, espaços e _-./()#@+=&;[]!\$*

Descrição - obrigatório Informações

Criacao de experimento-vpc para a materia de computacao em nuvem

Regras do grupo de segurança de entrada

▶ Regra de grupo de segurança 1 (TCP, 22, 0.0.0.0/0)

Remover

▼ Regra de grupo de segurança 2 (TCP, 8080, 0.0.0.0/0)

Remover

Tipo Informações

TCP personalizado

Protocolo Informações

TCP

Intervalo de portas Informações

8080

Tipo de origem Informações

Qualquer lugar

Origem Informações

Adicionar CIDR, lista de prefixos ou grupo

0.0.0.0/0 X

Descrição (opcional) Informações

p. ex. SSH para a área de trabalho do admin

⚠ Regras com origem 0.0.0.0/0 permitem que todos os endereços IP acessem sua instância. Recomendamos configurar regras de grupo de segurança para permitir o acesso apenas de endereços IP conhecidos. ✕

Adicionar regra de grupo de segurança

► Configuração avançada de rede

Após verificar se está tudo certo, é só clicar em criar a instância.

E nós vamos fazer a mesma configuração na segunda instância.

No caso criamos a instância chamada de *servidor-web-2* só que nesse caso a configuração de rede deverá se parecer com isto

▼ Configurações de rede [Informações](#)

VPC - obrigatório [Informações](#)

vpc-019e61ab62cd819aa (projeto-vpc)
10.50.0.0/16

Sub-rede [Informações](#)

subnet-0160f0612421015b9 projeto-subnet-public2-us-east-1b
VPC: vpc-019e61ab62cd819aa Proprietário: 055999873194
Zona de disponibilidade: us-east-1b Zone type: Zona de disponibilidade
Endereços IP disponíveis: 4090 CIDR: 10.50.16.0/20

Atribuir IP público automaticamente [Informações](#)

Habilitar

Taxas adicionais se aplicam quando fora do limite de nível gratuito

Firewall (grupos de segurança) [Informações](#)

Um grupo de segurança é um conjunto de regras de firewall que controlam o tráfego para sua instância. Adicione regras para permitir que o tráfego específico alcance sua instância.

☐ Criar grupo de segurança

☒ Selecionar grupo de segurança existente

Grupos de segurança comuns [Informações](#)

Selecionar grupos de segurança

experimento-vpc sg-0b30f58a3f7a91372 ✕
VPC: vpc-019e61ab62cd819aa

Os grupos de segurança que você adicionar ou remover aqui serão adicionados ou removidos em todas as suas interfaces de rede.

► Configuração avançada de rede

Iniciando as instâncias RDS

Da mesma forma, vamos na barra de pesquisa e pesquisar por RDS e criar as novas instâncias, no painel principal, clicaremos em *criar banco de dados*

The screenshot shows the Amazon RDS console interface. On the left is a sidebar with navigation links: Painel, Bancos de dados, Editor de consultas, Performance Insights, Snapshots, Exportações no Amazon S3, Backups automatizados, Instâncias reservadas, Proxies, Grupos de sub-redes, Grupos de parâmetros, Grupos de opções, Versões personalizadas do mecanismo, Integrações sem ETL (Novo), Eventos, Assinaturas de eventos, Recomendações (0), and Atualização de certificado. The main content area is titled 'Recursos' and shows usage for the US East (N. Virginia) region. It lists various resource categories like 'Instâncias de banco de dados (0/40)', 'Armazenamento alocado (0 TB/100 TB)', 'Grupos de parâmetros (1)', etc. Below this, there's a section titled 'Criar banco de dados' which includes a description of RDS and a button labeled 'Criar banco de dados' (highlighted with a red box). To the right of this button is a 'Restaurar do S3' button. A note at the bottom states: 'Note: your DB Instances will launch in the US East (N. Virginia) region'.

Usaremos a criação padrão, em modelos, selecionaremos a versão gratuita.

The screenshot shows the 'Modelos' (Templates) section of the Amazon RDS console. It prompts the user to 'Escolha um modelo de exemplo para atender a seu caso de uso.' (Choose an example model to meet your use case). There are three options: 'Produção' (Production) with a radio button, 'Dev/Test' (Development/Test) with a radio button, and 'Nível gratuito' (Free tier) which is selected with a blue radio button. The 'Nível gratuito' option includes a description: 'Use o nível gratuito do RDS para desenvolver novas aplicações, testá-las ou obter uma experiência prática com o Amazon RDS. Informações'.

Em configurações colocaremos a senha aulacn2024

Configurações

Identificador da instância de banco de dados [Informações](#)

Digite um nome para a instância de banco de dados. O nome deve ser exclusivo entre todas as instâncias de banco de dados de propriedade de sua conta da AWS na região atual da AWS.

O identificador da instância de banco de dados não diferencia maiúsculas de minúsculas, mas é armazenado com todas as letras minúsculas (como em "mydbinstance"). Restrições: 1 a 60 caracteres alfanuméricos ou hífens. O primeiro caractere deve ser uma letra. Não pode conter dois hífens consecutivos. Não pode terminar com um hífen.

▼ Configurações de credenciais

Nome do usuário principal [Informações](#)

Digite um ID de login para o usuário principal de sua instância de banco de dados.

De um a 16 caracteres alfanuméricos. O primeiro caractere deve ser uma letra.

Gerenciamento de credenciais

Você pode usar o AWS Secrets Manager ou gerenciar suas credenciais de usuário principal.

☐ Gerenciado no AWS Secrets Manager - *mais seguro*
O RDS gera uma senha para você e a gerencia durante todo o ciclo de vida usando o AWS Secrets Manager.

☒ Autogerenciada
Crie sua própria senha ou faça com que o RDS crie uma senha para você gerenciar.

☐ Gerar senha automaticamente

O Amazon RDS pode gerar uma senha para você, ou você pode especificar sua própria senha.

Senha principal [Informações](#)

Password strength **Strong**

Restrições mínimas: pelo menos 8 caracteres ASCII imprimíveis. Não pode conter nenhum dos seguintes símbolos: / ' " @

Confirmar senha principal [Informações](#)



Conectividade [Informações](#)



Recurso de computação

Escolha se deseja configurar uma conexão com um recurso de computação para esse banco de dados. A configuração de uma conexão altera automaticamente as configurações de conectividade, para que o recurso de computação possa se conectar a esse banco de dados.

☐ Não se conectar a um recurso de computação do EC2

Não configure uma conexão com um recurso de computação para esse banco de dados. Você poderá configurar uma conexão com um recurso de computação manualmente mais tarde.

☒ Conectar-se a um recurso de computação do EC2

Configure uma conexão com um recurso de computação do EC2 para esse banco de dados.

Instância do EC2 [Informações](#)

Escolha a instância do EC2 a ser adicionada como o recurso de computação desse banco de dados. Um grupo de segurança de VPC é adicionado a essa instância do EC2. Um grupo de segurança de VPC também é adicionado ao banco de dados com uma regra de entrada que permite que a instância do EC2 acesse esse banco de dados.

i-02b571d1d087e8e3f
servidor-web-1



Algumas configurações de VPC não podem ser alteradas quando um recurso de computação é adicionado

A ação de adicionar um recurso de computação do EC2 seleciona automaticamente a VPC, o grupo de sub-redes de banco de dados e as configurações de acesso público desse banco de dados. Para permitir que a instância do EC2 acesse o banco de dados, um grupo de segurança de VPC rds-ec2-X é adicionado ao banco de dados e outro chamado ec2-rds-X é adicionado à instância do EC2. Apenas é possível remover o novo grupo de segurança do banco de dados removendo o recurso de dados.

Nuvem privada virtual (VPC) [Informações](#)

Escolha a VPC. A VPC define o ambiente de rede virtual dessa instância de banco de dados.

projeto-vpc (vpc-019e61ab62cd819aa)
2 Sub-redes, 2 Zonas de disponibilidade

Somente as VPCs com um grupo de sub-redes de banco de dados correspondente são listadas.



Depois de criar o banco de dados, não é possível alterar a VPC.

Em Monitoramento, desative o performance insights

Monitoramento

☐ Ativar o Performance Insights

► Configuração adicional

Monitoramento aprimorado

E em configuração adicional, desative backup, criptografia e manutenção, todas essas desativações são apenas para acelerar criação do RDS

No terminal do EC2

Primeiro vamos se conectar às duas instâncias EC2's

EC2 > Instâncias > i-02b571d1d087e8e3f

Resumo da instância para i-02b571d1d087e8e3f (servidor-web-1) Informações

Atualizado há less than a minute

ID da instância
i-02b571d1d087e8e3f (servidor-web-1)

Endereço IPv6
-

Tipo de nome do host
Nome do IP: ip-10-50-27-133.ec2.internal

Endereço IPv4 público
52.204.226.242 | endereço aberto

Estado da instância
Executando

Nome do DNS de IP privado (somente IPv4)
ip-10-50-27-133.ec2.internal

Endereços IPv4 privados
10.50.27.133

DNS IPv4 público
ec2-52-204-226-242.compute-1.amazonaws.com | endereço aberto

Conectar

Estado da instância

Ações

Conectar-se à instância Informações


Conecte-se à sua instância i-02b571d1d087e8e3f (servidor-web-1) usando qualquer uma destas opções

Conexão de instância do EC2

Gerenciador de sessões

Cliente SSH

Console de série do EC2

**A porta 22 (SSH) está aberta para todos os endereços IPv4**
No momento, a porta 22 (SSH) está aberta para todos os endereços IPv4, indicados por **0.0.0.0/0** na regra de entrada do [seu grupo de segurança](#). Para maior segurança, considere restringir o acesso somente aos endereços IP do serviço do EC2 Instance Connect para sua região: 18.206.107.24/29. [Saiba mais](#).

ID da instância
i-02b571d1d087e8e3f (servidor-web-1)

Tipo de conexão

☒ Conectar-se usando o EC2 Instance Connect
Conecte-se usando o cliente baseado em navegador do EC2 Instance Connect, com um endereço IPv4 público.


☐ Conectar-se usando o endpoint do EC2 Instance Connect
Conecte-se usando o cliente baseado em navegador do EC2 Instance Connect, com um endereço IPv4 privado e um endpoint da VPC.

Endereço IP público
52.204.226.242

Nome de usuário
Insira o nome de usuário definido na AMI usada para iniciar a instância. Se você não definiu um nome de usuário personalizado, use o nome de usuário padrão, ec2-user.

ec2-user

X

**Observação:** na maioria dos casos, o nome de usuário padrão, ec2-user, está correto. No entanto, leia as instruções de uso da AMI para verificar se o proprietário da AMI alterou o nome de usuário da AMI padrão.

Cancelar

Conectar

Após se conectar, copie e cole estes comandos:

```
sudo yum update -y && sudo yum install git -y &&
git clone https://github.com/Pedro-V/aula-cn-experimento-redes.git &&
cd aula-cn-experimento-redes &&
./run.sh
```

depois no terminal ele deve pedir o ip do banco RDS então vá para a tela de RDS

Bancos de dados (2)									
<div><div>Filtrar por bancos de dados</div><div><div>Recurso do grupo</div><div>Modificar</div><div>Ações ▾</div><div>Restaurar do S3</div><div>Criar banco de dados</div></div></div>									
<div><div>Identificador de banco de dados ▲</div><div>Status ▾</div><div>Função ▾</div><div>Mecanismo ▾</div><div>Região e AZ ▾</div><div>Tamanho ▾</div><div>Recomendações ▾</div><div>CPU ▾</div><div>Atividade atual ▾</div><div>Ma</div></div>									
<div><div></div><div>database-1</div></div>	<div><div></div><div>Disponível</div></div>	<div><div></div><div>Instância</div></div>	<div><div></div><div>PostgreSQL</div></div>	<div><div></div><div>us-east-1b</div></div>	<div><div></div><div>db.t3.micro</div></div>	<div><div></div><div></div></div>	<div><div></div><div>5.32%</div></div>	<div><div></div><div>0 Conexões</div></div>	
<div><div></div><div>database-2</div></div>	<div><div></div><div>Disponível</div></div>	<div><div></div><div>Instância</div></div>	<div><div></div><div>PostgreSQL</div></div>	<div><div></div><div>us-east-1b</div></div>	<div><div></div><div>db.t3.micro</div></div>	<div><div></div><div></div></div>	<div><div></div><div>4.33%</div></div>	<div><div></div><div>1 Conexões</div></div>	

E seleciona para cada EC2, o seu RDS respectivo.

database-1

↺

Modificar

Ações ▾

Resumo

Identificador de banco de dados

database-1

CPU

4,27%

Status

✔

Disponível

Classe

db.t3.micro

Função

Instância

Atividade atual

0 Conexões

Mecanismo

PostgreSQL

Região e AZ

us-east-1b

Recomendações

Segurança e conexão

Monitoramento

Logs e eventos

Configuração

Manutenção e backups

Tags

Recomendações

Segurança e conexão

Endpoint e porta

Endpoint

📄

aws.com

Porta

5432

Redes

Zona de disponibilidade

us-east-1b

VPC

projeto-vpc (vpc-019e61ab62cd819aa)

Grupo de sub-redes

rds-ec2-db-subnet-group-1

Segurança

Grupos de segurança da VPC

rds-ec2-1 (sg-0b3218cae6748e7e4)

✔

Ativo

Publicamente acessível

Não

Autoridade de certificação

Informações

Criando o Elastic Load Balancer

Criando grupo de destino

Na página inicial do EC2 clique em grupos de destino

Painel EC2



Visualização Global do EC2

Eventos

Console-to-Code [Prévia](#)

▼ Instâncias

Instâncias

Tipos de Instância

Modelos de execução

Solicitações spot

Savings Plans

Instâncias reservadas

Hosts dedicados

Reservas de capacidade

[Novo](#)

▼ Imagens

AMIs

Catálogo de AMIs

▼ Elastic Block Store

Volumes

Snapshots

Lifecycle Manager

▼ Rede e segurança

Security groups

IPs elásticos

Placement groups

Pares de chaves

Interfaces de rede

▼ Balanceamento de carga

Load balancers

Grupos de destino

Trust Stores [Novo](#)

▼ Auto Scaling

Grupos Auto Scaling

Clique em criar um grupo de destino

Grupos de destino

Informações

Ações ▾

Criar grupo de destino

Q

Filtrar grupos de destino

<

1

>

Nome ▾

ARN ▾

Porta ▾

Protocolo

Nenhum grupo de destino

Você não tem nenhum grupo de destino em us-east-1

Criar grupo de destino

Nesta aba altere apenas a parte de nome do grupo de destino e a VPC que nós criamos anteriormente

Especificar detalhes do grupo

O load balancer 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 depois que o grupo de destino é criado.

Escolha um tipo de destino

☒ Instâncias

- Oferece suporte ao balanceamento de carga para instâncias dentro de uma VPC específica.
- Facilita o uso do [Amazon EC2 Auto Scaling](#) para gerenciar e escalar sua capacidade do 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.
- Oferece suporte a destinos IPv6, permitindo a comunicação IPv6 de ponta a ponta e NAT de IPv4 para IPv6.

☐ Função Lambda

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

☐ Application Load Balancer

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

Nome do grupo de destino

aula-cn-grupo-destino

É permitido um máximo de 32 caracteres alfanuméricos, incluindo hífens, mas o nome não deve começar ou terminar com um hífen.

Protocolo : Porta

Escolha um protocolo para seu grupo de destino que corresponda ao tipo de balanceador de carga que roteará o tráfego para ele. Alguns protocolos agora incluem a detecção de anomalias para os destinos e você poderá definir opções de mitigação depois que seu grupo de destino for criado. Essa escolha não poderá ser alterada após a criação

HTTP

80

1-65535


Tipo de endereço IP

Somente destinos com o tipo de endereço IP indicado podem ser registrados nesse grupo de destino.

☒ IPv4

Cada instância tem uma interface de rede padrão (eth0) atribuída ao endereço IPv4 privado primário. O endereço IPv4 privado primário da instância é aquele que será aplicado ao destino.

☐ IPv6

Cada instância que você registrar deve ter um endereço IPv6 primário atribuído. Isso é configurado na interface de rede padrão da instância (eth0). [Saiba mais](#) 

VPC

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

projeto-vpc

vpc-019e61ab62cd819aa

CIDR de VPC IPv4: 10.50.0.0/16



Versão do protocolo

☒ HTTP1

Enviar solicitações para destinos usando o HTTP/1.1. Compatível quando o protocolo de solicitação é HTTP/1.1 ou HTTP/2.

☐ HTTP2

Enviar solicitações para destinos usando o HTTP/2. Compatível quando o protocolo de solicitação é HTTP/2 ou gRPC, mas recursos específicos do gRPC não estão disponíveis.

☐ gRPC

Enviar solicitações para destinos usando o gRPC. Compatível quando o protocolo de solicitação é gRPC.

Depois registre os dois EC2s, selecionando as duas portas como 8080, depois clique em criar grupo de destino

Registrar destinos

Esta é uma etapa opcional para criar um grupo de destino. No entanto, para garantir que seu balanceador de carga roteie o tráfego para esse grupo de destino, você deve registrar seus destinos.

Instâncias disponíveis (2/2)

< 1 > ⚙

<input checked="" type="checkbox"/>	ID de instância	Nome	Estado
<input checked="" type="checkbox"/>	I-02b571d1d087e8e3f	servidor-web-1	✓ Em execução
<input checked="" type="checkbox"/>	I-09de56327c1bbbe9b	servidor-web-2	✓ Em execução

2 selecionado

Portas para as instâncias selecionadas

Portas para rotear o tráfego para as instâncias selecionadas

1-65535 (separar várias portas com vírgulas)

Incluir como pendente abaixo

2 seleções abaixo estão pendentes. Inclua mais ou registre destinos quando estiverem prontos.

Examinar destinos

Destinos (2)

Remover todos os pendentes

☐ Mostrar somente pendentes

< 1 > ⚙

ID de instância	Nome	Porta	Estado	Grupos de
I-02b571d1d087e8e3f	servidor-web-1	8080	✓ Em execução	experimen
I-09de56327c1bbbe9b	servidor-web-2	8080	✓ Em execução	experimen

2 pendentes

Cancelar

Anterior

Criar grupo de destino

Criando Loab Balancers

Depois clicaremos em load balancers

Painel EC2

Visualização Global do EC2

Eventos

Console-to-Code

▼ Instâncias

Instâncias

Tipos de instância

Modelos de execução

Solicitações spot

Savings Plans

Instâncias reservadas

Hosts dedicados

Reservas de capacidade

▼ Imagens

AMIs

Catálogo de AMIs

▼ Elastic Block Store

Volumes

Snapshots

Lifecycle Manager

▼ Rede e segurança

Security groups

IPs elásticos

Placement groups

Pares de chaves

Interfaces de rede

▼ Balanceamento de carga

Load balancers

Grupos de destino

Trust Stores

EC2 > Load balancers

Passo 2

Load balancers

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

Filtrar balanceadores de carga

Nome

Nome do DNS

Estado

ID da VPC

Nenhum balanceador de carga

Você não tem nenhum balanceador de carga em us-east-1

Criar load balancer

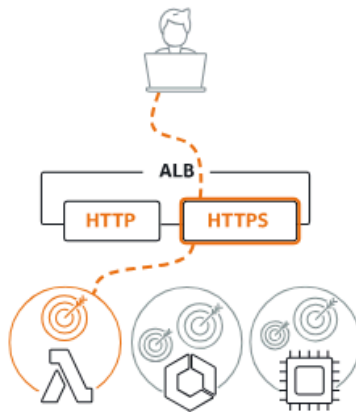
0 balanceadores de carga selecionados

Selecione um balanceador de carga acima.

Clicaremos em Application Load Balancer

Tipos de load balancer

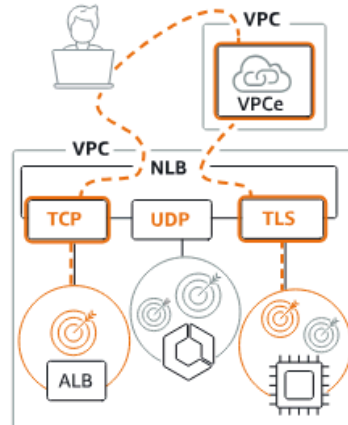
Application Load Balancer [Informações](#)



Escolha um Application Load Balancer quando precisar de um conjunto de recursos flexível para suas aplicações com tráfego HTTP e HTTPS. Operando no nível da solicitação, os Application Load Balancers fornecem roteamento avançado e recursos de visibilidade direcionados a arquiteturas de aplicações, incluindo **microsserviços** e contêineres.

[Criar](#)

Network Load Balancer [Informações](#)



Escolha um Network Load Balancer quando precisar de desempenho altíssimo, descarga de TLS em escala, implantação de certificados centralizada, suporte para UDP e endereços IP estáticos para sua aplicação. Operando no nível da conexão, os Network Load Balancers são capazes de atender a milhões de solicitações por segundo com segurança, enquanto mantêm latências extremamente baixas.

[Criar](#)

Gateway Load Balancer [Informações](#)



Escolha um Gateway Load Balancer quando precisar implantar e gerenciar uma frota de dispositivos virtuais de terceiros compatíveis com GENEVE. Esses dispositivos permitem que você melhore a segurança, a conformidade e os controles de políticas.

[Criar](#)

► **Classic Load Balancer** - *geração anterior*

[Fechar](#)

Selecionaremos o VPC que criamos e duas zonas de disponibilidades **públicas**

Mapeamento de rede [Informações](#)

O load balancer roteia o tráfego para destinos nas sub-redes selecionadas e de acordo com suas configurações de endereço IP.

VPC [Informações](#)

The load balancer will exist and scale within the selected VPC. The selected VPC is also where the load balancer targets must be hosted unless routing to Lambda or on-premises targets, or if using VPC peering. To confirm the VPC for your targets, view [target groups](#). For a new VPC, [create a VPC](#).

projeto-vpc

vpc-019e61ab62cd819aa

CIDR de VPC IPv4: 10.50.0.0/16



Mapeamentos [Informações](#)

Selecione pelo menos duas zonas de disponibilidade e uma sub-rede por zona. O balanceador de carga roteia o tráfego para destinos somente nessas zonas de disponibilidade. Zonas de disponibilidade não compatíveis com o balanceador de carga ou a VPC não estão disponíveis para seleção.

Zonas de disponibilidade

☒ us-east-1a (use1-az2)

Sub-rede

subnet-0726fdcba69b78a5b

IPv4 subnet CIDR: 10.50.0.0/20

projeto-subnet-public1-us-east-1a



Endereço IPv4

Atribuído pela AWS

☒ us-east-1b (use1-az4)

Sub-rede

subnet-0160f0612421015b9

IPv4 subnet CIDR: 10.50.16.0/20

projeto-subnet-public2-us-east-1b



Endereço IPv4

Atribuído pela AWS

☐ us-east-1c (use1-az6)

☐ us-east-1e (use1-az3)

☐ us-east-1f (use1-az5)

Depois em listeners e roteamento escolheremos o grupo de destino

Listeners e roteamento [Informações](#)

O listener é um processo que verifica solicitações de conexão usando a porta e o protocolo configurados. As regras que você define para um listener determinam como o balanceador de carga encaminhará solicitações aos destinos registrados.

▼ Listener HTTP:80

Remover

Protocolo

HTTP



Porta

80

1-65535

Ação padrão

[Informações](#)

Avançar para

aula-cn-grupo-destino

Tipo de destino: Instância, IPv4

HTTP



[Criar grupo de destino](#)

Tags do listener - *opcional*

Considere adicionar tags ao seu listener. As tags permitem que você categorize os seus recursos da AWS para que possa gerenciá-los com mais facilidade.

Adicionar tag de listener

Você pode adicionar até 50 outras tags.

Adicionar listener

Finalizado a configuração, o load balancer irá fazer o balanceamnto de cargadas requisições da porta pública.