



Documentação de atividade em AWS - Linux

Bolsista : Ricardo Machado Nunes

Team : PB – FW – A – RG – SB – HA

Studio : Cloud & DevSecOps

DC : DCV Ijuí

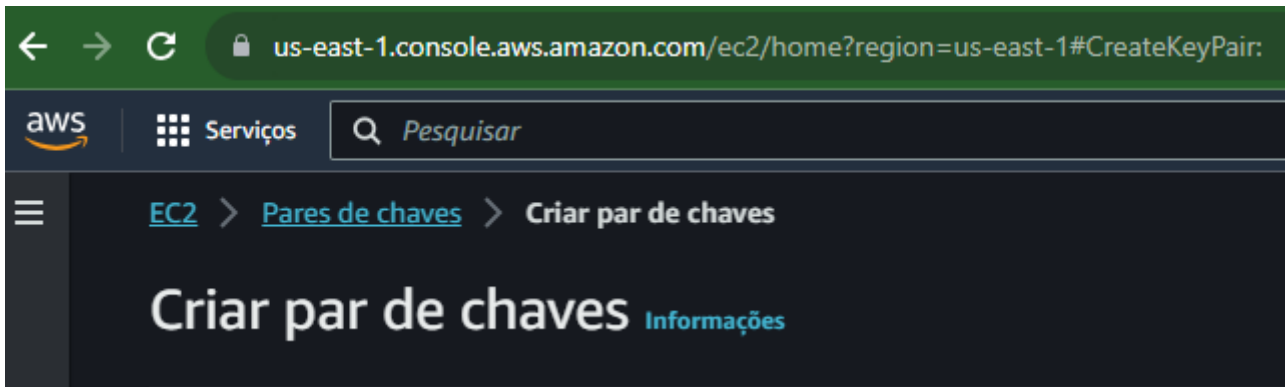
Setembro 2023

Parte 1 – AWS

1. Criação do Key Pair

Primeiramente deve-se viabilizar a forma de acesso as instâncias EC2, neste caso, criaremos um Key Pair.

1.1 Acessando <https://us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#CreateKeyPair:>

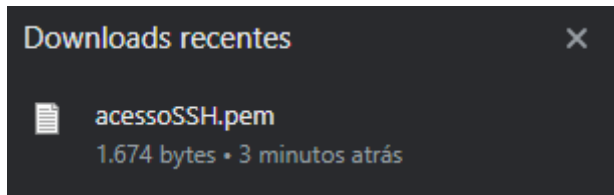


* No endereço do hiperlink acima, está definida a criação de um Key Pair na região **us-east-1**

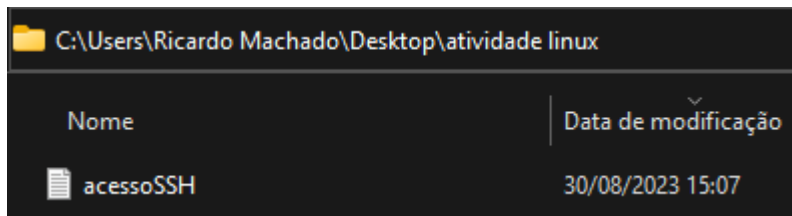
Foi dado o nome de **acessoSSH** ao novo par de chaves criados, do tipo *RSA* com formato *PEM* para viabilizar o acesso via *OpenSSH* da instância EC2;

A imagem mostra o formulário de criação de um par de chaves na AWS. O título é 'Par de chaves' com uma explicação: 'Um par de chaves, que consiste em uma chave privada e uma chave pública, é um conjunto de credenciais de segurança que você usa para provar sua identidade ao se conectar a uma instância.' O campo 'Nome' contém o texto 'acessoSSH' e uma dica: 'O nome pode incluir até 255 caracteres ASCII. Ele não pode incluir espaços iniciais ou finais.' A seção 'Tipo de par de chaves' tem dois botões: 'RSA' (selecionado) e 'ED25519'. A seção 'Formato de arquivo de chave privada' tem dois botões: '.pem' (selecionado, com a dica 'Para uso com OpenSSH') e '.ppk' (com a dica 'Para uso com PuTTY'). A seção 'Tags — opcional' indica 'Nenhuma tag associada ao recurso.' e possui um botão 'Adicionar nova tag'.

Após concluir, a chave criptografada terá seu download automático ao dispositivo local;



Qual deverá ser alocada em um diretório para posteriormente ser utilizada na validação;

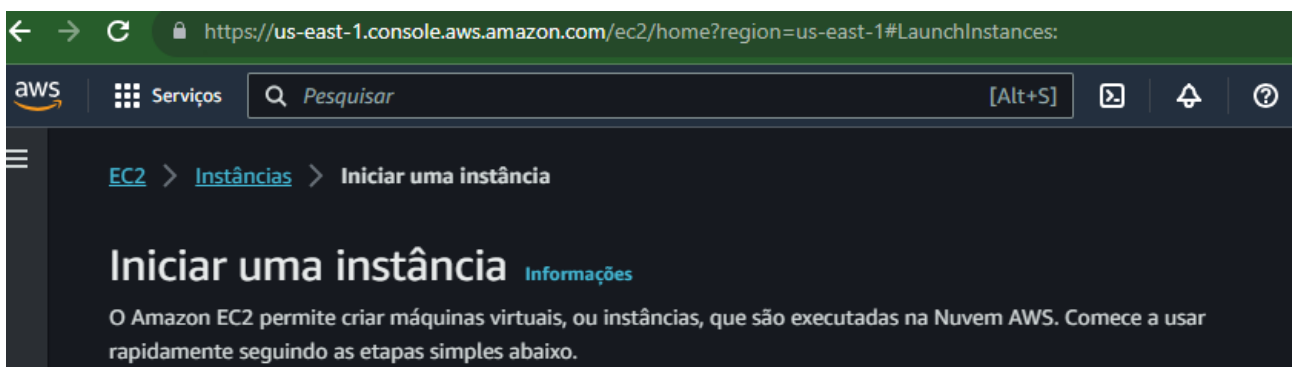


2. Criação da instância EC2

Após o desenvolvimento do instrumento de acesso da instância via SSH através do Key Pair, vamos a criação da instância a ser acessada.

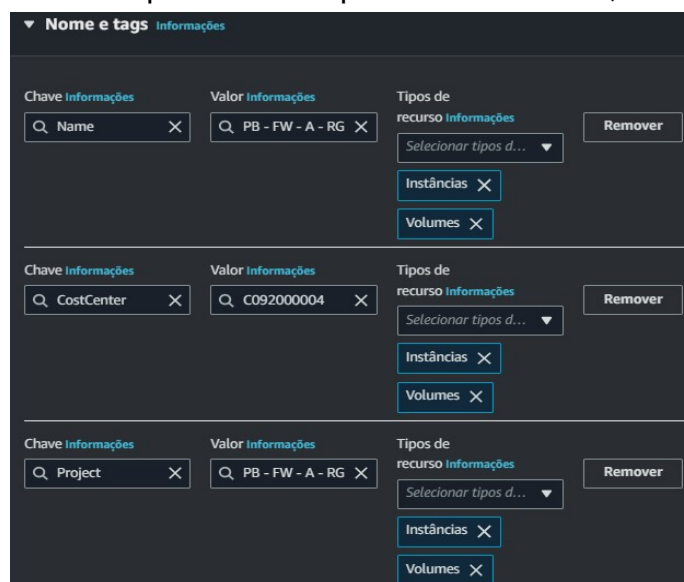
Acesso em Amazon AWS > Serviços > EC2 > Instâncias > Iniciar uma instância

<https://us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#LaunchInstances:>



* No endereço do hiperlink acima, está definida a criação da instância na região **us-east-1**

Foram utilizadas as TAGS disponibilizadas para o treinamento, abaixo descritas.



Conforme determinado para este exercício, a imagem de SO a ser utilizada será a *Amazon Linux 2*

▼ **Imagens de aplicação e de sistema operacional (imagem de máquina da Amazon)** [Informações](#)

Uma AMI é um modelo que contém a configuração do software (sistema operacional, servidor de aplicações e aplicações) necessária para executar a instância. Pesquise ou navegue pelas AMIs se você não estiver vendo o que está buscando abaixo

Início rápido

Amazon Linux
aws

macOS
Mac

Ubuntu
ubuntu

Windows
Microsoft

Red Hat
Red Hat

SUSE L
SUSE



Procurar mais AMIs
Incluindo AMIs da AWS, do Marketplace e da comunidade

Imagem de máquina da Amazon (AMI)

Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type
ami-0f409bae3775dc8e5 (64 bits (x86)) / ami-0f0f7b386be96ec2d (64 bits (Arm))
Virtualização: hvm ENA habilitado: true Tipo de dispositivo raiz: ebs

Qualificado para o nível gratuito ▼

Descrição
Amazon Linux 2 Kernel 5.10 AMI 2.0.20230822.0 x86_64 HVM gp2

Arquitetura
64 bits (x86) ▼

ID da AMI
ami-0f409bae3775dc8e5

Provedor verificado

Conforme determinado, a instância utilizará uma plataforma *t3.small*

▼ **Tipo de instância** [Informações](#)

Tipo de instância

t3.small
Família: t3 2 vCPU 2 GiB Memória Geração atual: true
Sob demanda SUSE base definição de preço: 0.0518 USD por hora
Sob demanda Linux base definição de preço: 0.0208 USD por hora
Sob demanda RHEL base definição de preço: 0.0808 USD por hora
Sob demanda Windows base definição de preço: 0.0392 USD por hora

▼

☐ Todas as gerações

[Comparar tipos de instância](#)

Aqui selecionamos o *Key Pair* criado no passo 1

▼ 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

acessoSSH ▼

↻ Criar novo par de chaves

2.1 Configurações de rede

As configurações de rede são fundamentais para viabilizar o acesso à instância, tão importantes quanto as chaves de acesso, aqui faremos o procedimento de criação de uma *subnet pública* (1) e seleção de um *grupo de segurança* (2).

2.1.1 Subnet

Ao clicar em editar nas configurações de rede, o *layout* ficará da seguinte maneira:

▼ Configurações de rede Informações

VPC - obrigatório Informações

vpc-09cb41c57a0ac7d44 (aws-controltower-VPC)
172.31.0.0/16 ▼

↻

Sub-rede Informações

subnet-0f11fc098ff595080 aws-controltower-PrivateSubnet2A
VPC: vpc-09cb41c57a0ac7d44 Proprietário: 044175277726
Zona de disponibilidade: us-east-1b Endereços IP disponíveis: 4091
CIDR: 172.31.32.0/20 ▼

↻ Criar nova sub-rede

Atribuir IP público automaticamente Informações

Desabilitar ▼

Ao clicar em “Criar nova sub-rede”, irá abrir uma nova janela (<https://us-east-1.console.aws.amazon.com/vpc/home?region=us-east-1#CreateSubnet:>) para a criação da subnet

[VPC](#) > [Sub-redes](#) > Criar sub-rede

Criar sub-rede [Informações](#)

VPC

ID da VPC
Crie sub-redes nessa VPC.

vpc-09cb41c57a0ac7d44 (aws-controltower-VPC) ▼

CIDRs de VPC associados

CIDRs IPv4

172.31.0.0/16

Configurações de sub-rede

Especifique os blocos CIDR e a zona de disponibilidade para a sub-rede.

Sub-rede 1 de 1

Nome da sub-rede
Crie uma tag com a chave 'Nome' e um valor que você especificar.

my-subnet-01

O nome pode ter até 256 caracteres.

Zona de disponibilidade [Informações](#)
Escolha a zona na qual sua sub-rede residirá ou deixe que a Amazon escolha uma para você.

Sem preferência ▼

Bloco CIDR IPv4 [Informações](#)

10.0.0.0/24

▼ Tags - *opcional*

Nenhuma tag associada ao recurso.

Adicionar nova tag

Você pode adicionar mais 50 tags.

No primeiro item será exposto em qual VPC esta subnet será criada, neste caso a final “7d44” Em nosso exercício, as configurações ficaram assim:

Sub-rede 1 de 1

Nome da sub-rede
Crie uma tag com a chave 'Nome' e um valor que você especificar.

subnetpublica

O nome pode ter até 256 caracteres.

Zona de disponibilidade [Informações](#)
Escolha a zona na qual sua sub-rede residirá ou deixe que a Amazon escolha uma para você.

Sem preferência ▼

Bloco CIDR IPv4 [Informações](#)

172.31.0.0/20 X

▼ Tags - *opcional*

Chave	Valor - <i>opcional</i>
Q Name X	Q subnetpublica X
Remover	

Adicionar nova tag

Você pode adicionar mais 49 tags.

2.1.2 Grupo de segurança

Foi criado um novo grupo de segurança para controlar o acesso a esta nova instância, conforme determinado ele deveria liberar as portas de comunicação para acesso público (22/TCP, 111/TCP e UDP, 2049/TCP/UDP, 80/TCP, 443/TCP).

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*

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](#)

Regras do grupo de segurança de entrada

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

Remove

▶ Regra de grupo de segurança 2 (TCP, 111, 0.0.0.0/0)

Remove

▶ Regra de grupo de segurança 3 (UDP, 111, 0.0.0.0/0)

Remove

▶ Regra de grupo de segurança 4 (TCP, 2049, 0.0.0.0/0)

Remove

▶ Regra de grupo de segurança 5 (UDP, 2049, 0.0.0.0/0)

Remove

▶ Regra de grupo de segurança 6 (TCP, 80, 0.0.0.0/0)

Remove

▶ Regra de grupo de segurança 7 (UDP, 443, 0.0.0.0/0)

Remove

Foi determinado que o volume raiz da instância deveria ter 16 gb de armazenamento;

Volumes do EBS [Ocultar detalhes](#)

▼ Volume 1 (Raiz da AMI) (Personalizada)

Tipo de armazenamento Informações	Nome do dispositivo - <i>required</i> Informações	Snapshot Informações
EBS	/dev/xvda	snap-0b41aa919c7bcb5a6
Tamanho (GiB) Informações	Tipo de volume Informações	IOPS Informações
<input type="text" value="16"/>	<div>gp2 ▼</div>	100 / 3000

A instância foi inicializada com a seguinte configuração

▼

Resumo

Número de instâncias

[Informações](#)

1

Imagem do software (AMI)

Amazon Linux 2 Kernel 5.10 AMI...[Ler mais](#)

ami-0f409bae3775dc8e5

Tipo de servidor virtual (tipo de instância)

t3.small

Firewall (grupo de segurança)

Novo grupo de segurança

Armazenamento (volumes)

1 volume(s) - 16 GiB

Cancelar

Executar instância

[Revisar comandos](#)

[EC2](#) > [Instâncias](#) > Iniciar uma instância

✔ **Êxito**

Execução da instância iniciada com êxito ([i-095392564ddb7272f](#))

▼

Log de execução

Inicializando solicitações

✔ Com êxito

Criando grupos de segurança

✔ Com êxito

Criando regras do grupo de segurança

✔ Com êxito

Iniciar inicialização

✔ Com êxito

3. Acesso via AWS CLI

Para realizar o acesso à instância via linha de comando de um dispositivo local, utilizaremos o AWS CLI e realizar os seguintes passos:

3.1 Criação de usuário no IAM

Para realizar o acesso, devemos criar um usuário, assim o faremos no serviço de IAM da AWS (<https://us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/users>)



3.1.1 Especificar detalhes do usuário

Nesta etapa devemos apenas colocar o nome do novo usuário e sem necessidade de selecionar a opção abaixo, pois nosso intuito com este user é apenas o acesso via CLI

Especificar detalhes do usuário

Detalhes do usuário

Nome do usuário

O nome de usuário pode ter até 64 caracteres. Caracteres válidos: A-Z, a-z, 0-9, and + = , . @ _ - (hifen)

☐ Fornecer acesso para os usuários ao Console de Gerenciamento da AWS - *opcional*
Se você está fornecendo acesso ao console para uma pessoa, a [prática recomendada](#) é gerenciar o acesso dela no Centro de Identidade do IAM.

i Se você estiver criando acesso programático por meio de chaves de acesso ou credenciais específicas de serviço para o AWS CodeCommit ou o Amazon Keyspaces, poderá gerá-las depois de criar esse usuário do IAM. [Saiba mais](#)

3.1.2 Definir permissões

Conforme o enunciado do menu, a gestão por grupos é uma prática de gestão para múltiplos usuários. Para fins de exercício e como usuário único, aplicaremos a regra de forma individual, conforme abaixo:

Definir permissões

Adicione usuário a um grupo existente ou crie um novo. Usar grupos é uma prática recomendada para gerenciar as permissões do usuário por funções de trabalho. [Saiba mais](#)

Opções de permissões

☐ Adicionar usuário ao grupo
Adicione o usuário a um grupo existente ou crie um novo grupo. Recomendamos usar grupos para gerenciar permissões de usuário por função de trabalho.

☐ Copiar permissões
Copie todas as associações a grupos, políticas gerenciadas anexadas e políticas em linha de um usuário existente.

☒ Anexar políticas diretamente
Anexe uma política gerenciada diretamente a um usuário. Como prática recomendada, recomendamos anexar políticas a um grupo. Em seguida, adicione o usuário ao grupo apropriado.

Políticas de permissões (1/1122)

Escolha uma ou mais políticas para anexar ao seu novo usuário.

1 2

37 correspondências

<input type="checkbox"/>	Nome da política	Tipo	Associar entidades
<input checked="" type="checkbox"/>	AdministratorAccess	Gerenciadas pela AWS - função de trabalho	4

3.1.3 Revisar e criar

O resumo das atribuições do usuário criado

Revisar e criar

Revise suas escolhas. Depois de criar o usuário, você poderá visualizar e fazer download da senha gerada automaticamente, se ativada.

Detalhes do usuário

Nome do usuário ricardo	Tipo de senha do console None	Exigir redefinição de senha Não
----------------------------	----------------------------------	------------------------------------

Resumo de permissões

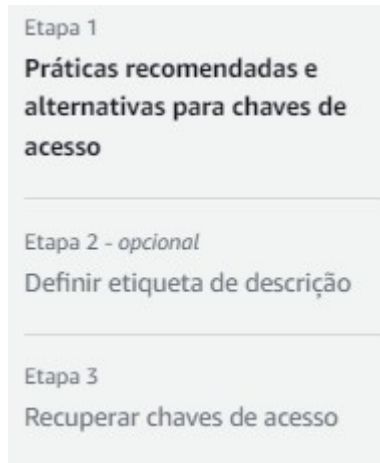
1

Nome	Tipo	Usado como
AdministratorAccess	Gerenciadas pela AWS - função de trabalho	Política de permissões

Após a criação, seremos direcionados ao painel de gestão de usuários (<https://us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/users>) no qual acessaremos o novo usuário criado e acessar as credenciais de segurança clicando em “Criar chave de acesso” (https://us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/users/details/ricardo?section=security_credentials)

3.2 Chave de Acesso

A criação da chave de acesso ocorre em 3 etapas



3.2.1 Caso de uso

Aqui define-se qual será o uso da chave de acesso a ser criada, para nosso exercício é uma chave de acesso para CLI

Práticas recomendadas e alternativas para chaves de acesso

[Informações](#)

Evite usar credenciais de longo prazo, como chaves de acesso, para melhorar sua segurança. Considere os seguintes casos de uso e alternativas.

Caso de uso

☐ Command Line Interface (CLI)
Você planeja usar essa chave de acesso para permitir que a AWS CLI acesse sua conta da AWS.

3.2.2 Etiqueta de descrição

Como uma *tag* da chave, seu uso é opcional.

3.2.3 Recuperar chave de acesso

Nesta página o user pode visualizar a chave de acesso criada e realizar o download da mesma, recomenda-se que o faça, pois **posteriormente não será possível acessá-la.**

Chave de acesso

Se você perder ou esquecer sua chave de acesso secreta, não poderá recuperá-la. Em vez disso, crie uma nova chave de acesso e torne a chave antiga inativa.

Chave de acesso	Chave de acesso secreta
AKIAQUSINH2PFLH37RG3	***** Mostrar

Downloads recentes

ricardo_accessKeys.csv
99 bytes • 3 minutos atrás

3.3 Configuração do acesso

Após a instalação do AWS CLI na máquina local e de posse do usuário, chaves de acesso e instância criada; vamos viabilizar o acesso via terminal local.

```
Windows PowerShell
PS C:\Users\Ricardo Machado> aws configure
AWS Access Key ID [*****]: AKIAQUSINH2PFLH37RG3
AWS Secret Access Key [*****]: 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
Default region name []: us-east-1
Default output format []: json
PS C:\Users\Ricardo Machado>
```

Deve-se criar um internet *gateway* que faça a comunicação entre a VPC qual a subnet da instância está alocada, o *gateway* deve ser associado a Tabela de Rotas da VPC.



3.3.1 Acesso SSH

Serão utilizadas as credenciais criadas no passo anterior (ID e Secret Access Key), a região de acesso e formato de output do arquivo de configuração.

O acesso ocorre através da linha de comando: `ssh -i "C:\Users\Ricardo Machado\Desktop\atividade linux\acessoSSH.pem" ec2-user@44.202.107.153`

```
PS C:\Users\Ricardo Machado> ssh -i "C:\Users\Ricardo Machado\Desktop\atividade linux\acessoSSH.pem" ec2-user@44.202.107.153
Last login: Thu Aug 31 14:45:17 2023 from 189.7.228.119

 _ _ | _ _ | _ )
 _ | ( _ _ /   Amazon Linux 2 AMI
 _ | \ _ _ | _ |

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-172-31-12-156 ~]$
```

4. Elastic IP

Um Elastic IP é associar um IP estático a uma instância EC2 em AWS – podendo também pode ser atribuido a outros serviços – mantendo um endereço fixo e podendo ser reatribuído a outras instâncias conforme a necessidade.

Primeiro vamos cria-lo em EC2 > Rede e Segurança > IPs elásticos

<https://us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#Addresses:>

Após a criação, aparece a seguinte mensagem



Neste ponto clicamos em “Associar” para indexá-lo a instância EC2

Endereço IP elástico: 3.221.177.102

Tipo de recurso
Selecione o tipo de recurso ao qual associar o endereço IP elástico.

☒ Instância
☐ Interface de rede

⚠ Se você associar um endereço IP elástico a uma instância que já tem um endereço IP elástico associado, o endereço IP elástico associado anteriormente será desassociado, mas o endereço ainda estará alocado à sua conta. [Saiba mais](#)

Se nenhum endereço IP privado for especificado, o endereço IP elástico será associado ao endereço IP privado primário.

Instância

🔍 i-095392564ddb7272f ✕ ↻

Endereço IP privado
O endereço IP privado ao qual associar o endereço IP elástico.

🔍 172.31.12.156 ✕

Reassociação
Especifique se o endereço IP elástico pode ser reassociado a um recurso diferente se ele já estiver associado a um recurso.

☒ Permitir que o endereço IP elástico seja reassociado

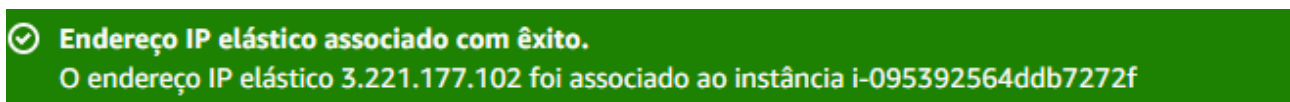
Cancelar Associar

Tipo de recurso: Instância

Instância: Nossa instância criada

Endereço de IP privado : Associação do IP privado ao IP elástico

Selecione a box para permitir a reassociação de instâncias/serviços para este IP



Teste de conectividade

```
PS C:\Users\Ricardo Machado> ssh -i "C:\Users\Ricardo Machado\Desktop\atividade linux\
acessoSSH.pem" ec2-user@3.221.177.102
Last login: Thu Aug 31 18:04:42 2023 from 189.7.228.119

  _ | _ | _ | _ |
  _ | ( _ | _ | /   Amazon Linux 2 AMI
  _ | \ _ | _ | _ |

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-172-31-12-156 ~]$
```

Configuração finalizada.