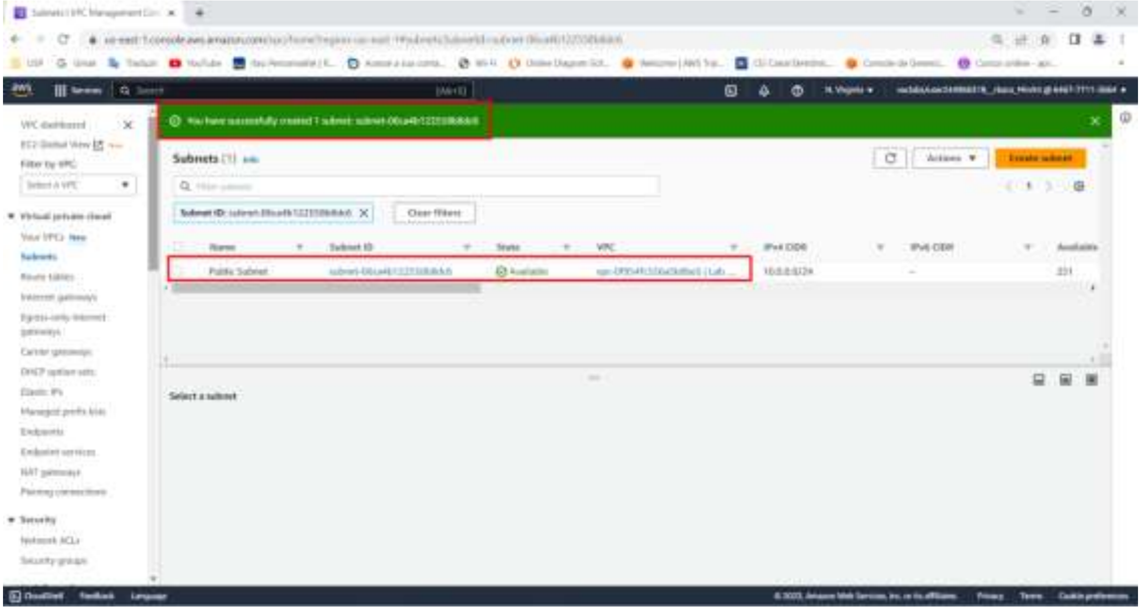
Laboratório de Desafios – Criando um Ambiente de Rede VPC para o Café

1.) Desafio nº 1

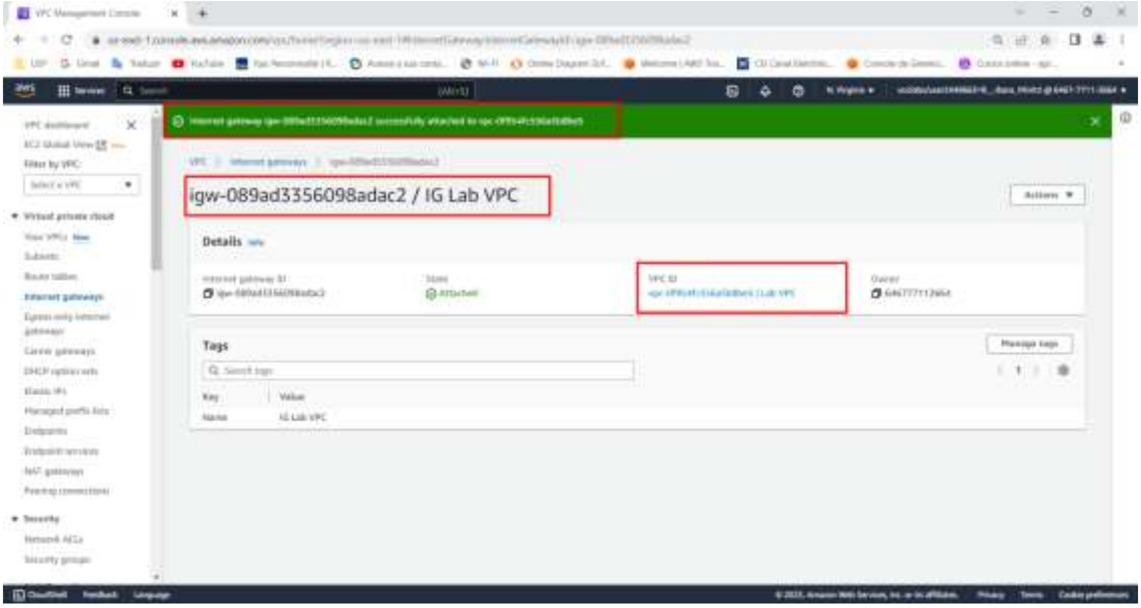
Criar uma subrede pública



You have successfully created 1 subnet: subnet-06ca4b[illegible]

Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR	Available
Public Subnet	subnet-06ca4b[illegible]	Available	vpc-[illegible] | Lab ...	10.0.0.0/24	–	251

Criar internet gateway e anexar a Lab VPC



Internet gateway igw-089ad3356098adac2 successfully attached to vpc-[illegible]

igw-089ad3356098adac2 / IG Lab VPC

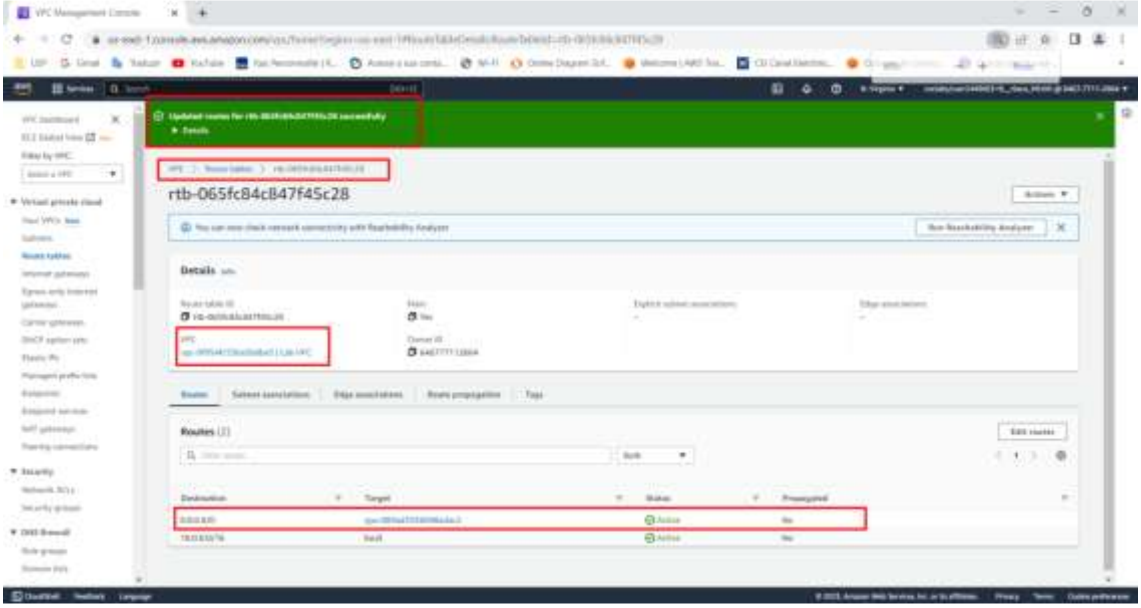
Details

Internet gateway ID	State	VPC ID	Owner
igw-089ad3356098adac2	Attached	vpc-[illegible] | Lab VPC	[illegible]

Tags

Key	Value
Name	IG Lab VPC

Incluir na tabela de rotas da Lab VPC, a rota 0.0.0.0/0 para o internet gateway criado na etapa anterior.



Updated routes for rtb-065fc84c847f45c28 successfully

rtb-065fc84c847f45c28

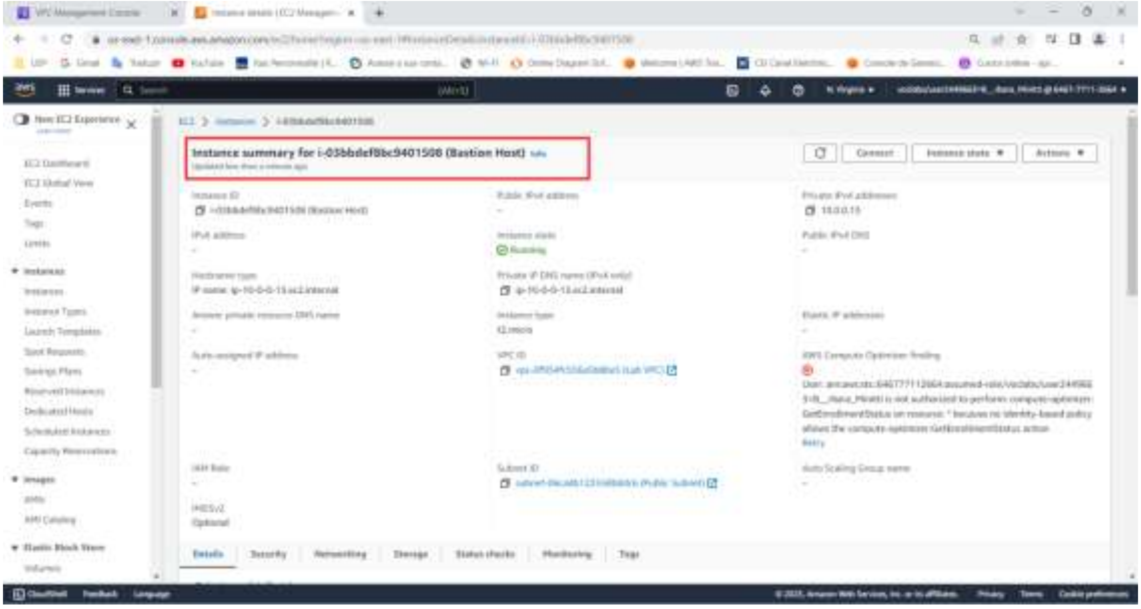
Details

Routes (2)

Destination	Target	Status	Propagated
0.0.0.0/0	igw-[illegible]	Active	No
10.0.0.0/16	local	Active	No

Tarefa2

Criar bastion host



Instance summary for i-03bbdef8bc9401508 (Bastion Host)

Instance ID: i-03bbdef8bc9401508 (Bastion Host)

Private IPv4 addresses: 10.0.0.15

Instance state: Running

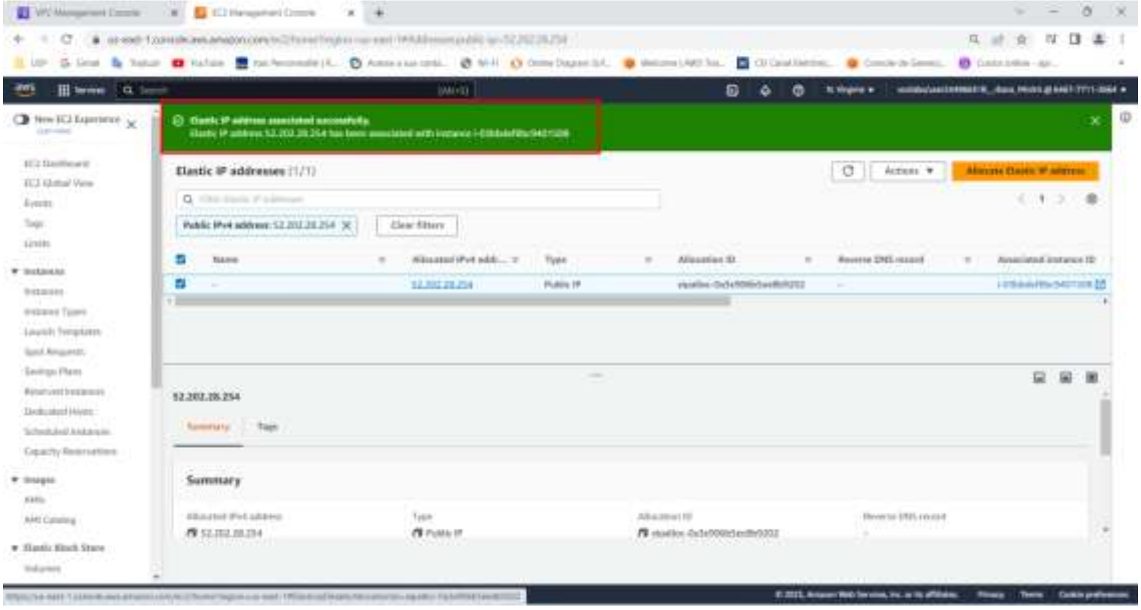
Hostname type: IP name: ip-10-0-0-15.ec2.internal

Private IP DNS name (IPv4 only): ip-10-0-0-15.ec2.internal

Instance type: t2.micro

Tarefa3

Alocar um elastic IP para o bastion host



Elastic IP address associated successfully.
Elastic IP address 52.202.28.254 has been associated with instance [illegible]

Elastic IP addresses (1/1)

Public IPv4 address: 52.202.28.254

Name	Allocated IPv4 add...	Type	Allocation ID	Reverse DNS record	Associated instance ID
–	52.202.28.254	Public IP	[illegible]	–	[illegible]

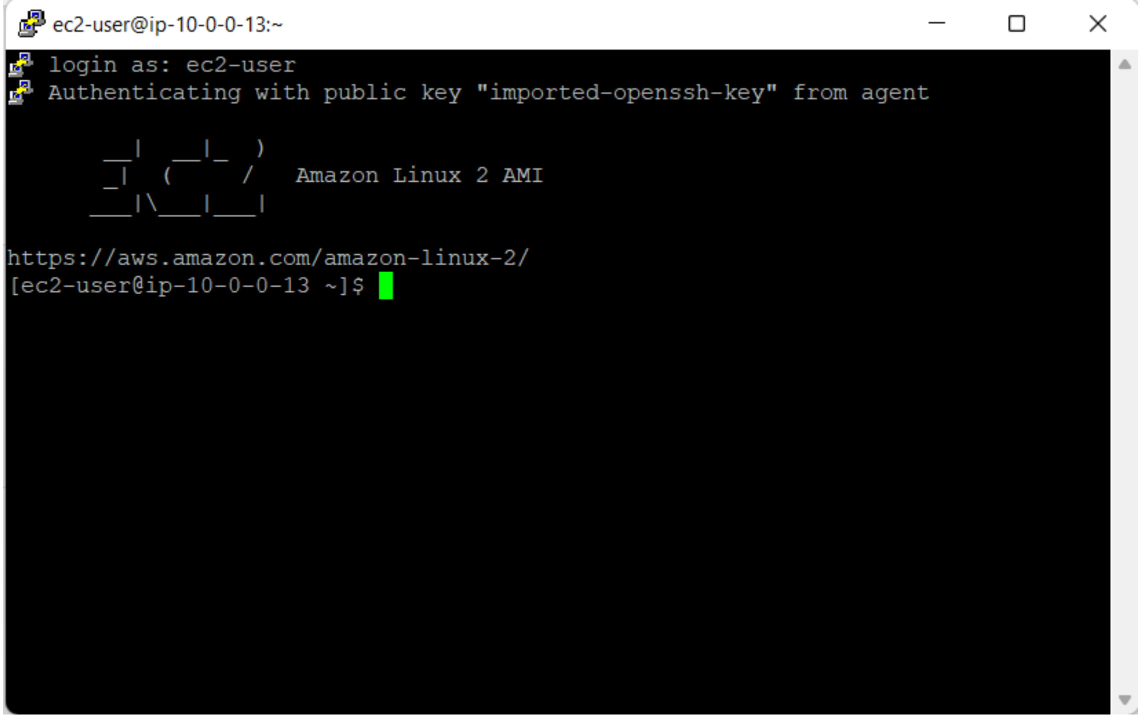
52.202.28.254

Summary

Allocated IPv4 address	Type	Allocation ID	Reverse DNS record
52.202.28.254	Public IP	[illegible]	–

Tarefa4

Testar a conexão com o bastion host

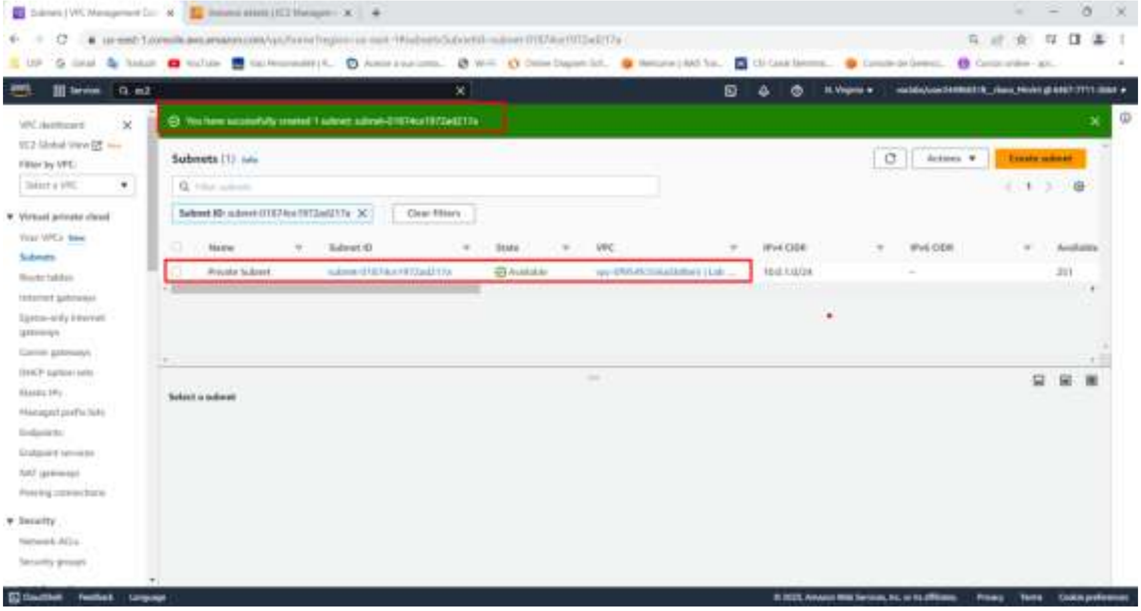


ec2-user@ip-10-0-0-13:~

```
login as: ec2-user
Authenticating with public key "imported-openssh-key" from agent

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

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-0-0-13 ~]$ 
```

Tarefa5

Criar uma subrede privada



You have successfully created 1 subnet: subnet-01874ce1972ad217a

Subnets (1)

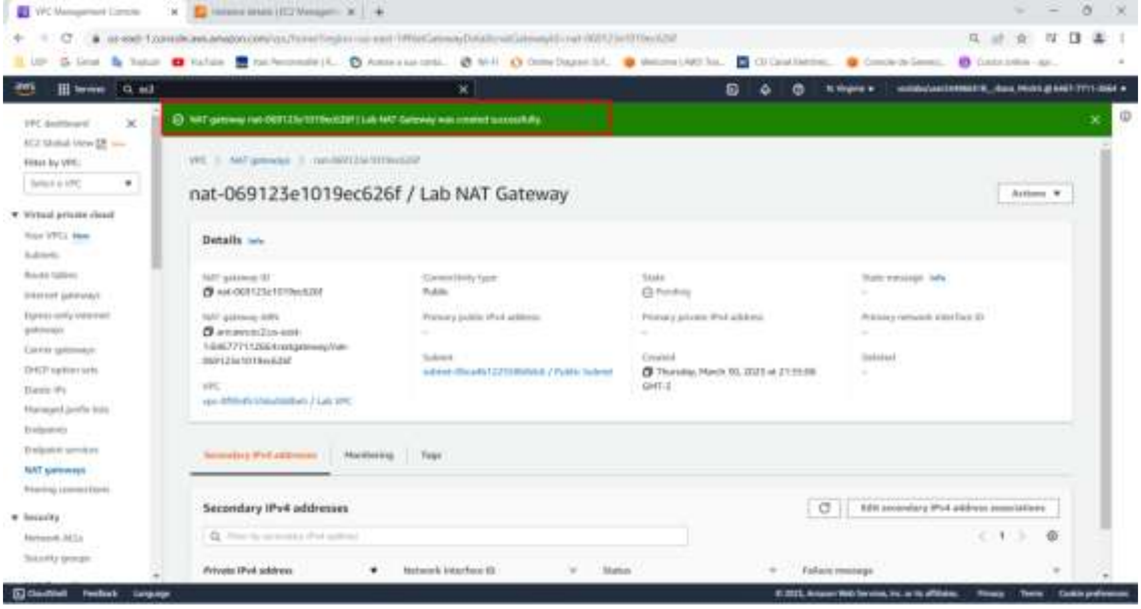
Subnet ID: subnet-01874ce1972ad217a

Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR	Available
Private Subnet	subnet-01874ce1972ad217a	Available	vpc-0f6fd5356a0b8a0 | Lab ...	10.0.1.0/24	–	251

Select a subnet

Tarefa6

Criar um gateway NAT



NAT gateway nat-069123e1019ec626f | Lab NAT Gateway was created successfully

nat-069123e1019ec626f / Lab NAT Gateway

Details

NAT gateway ID: nat-069123e1019ec626f

Connectivity type: Public

State: Pending

State message: –

NAT gateway ARN: arn:aws:ec2:us-east-1:646777112664:natgateway/nat-069123e1019ec626f

Primary public IPv4 address: –

Primary private IPv4 address: –

Primary network interface ID: –

Subnet: subnet-0fca4b1221f0ff6b6 / Public Subnet

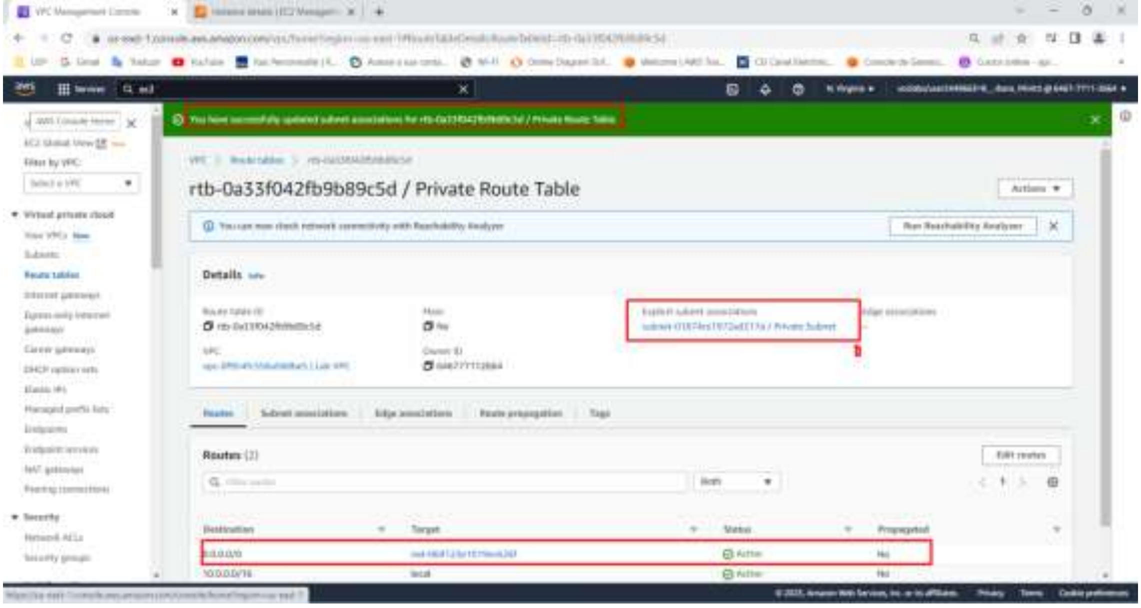
Created: Thursday, March 30, 2023 at 21:55:08 GMT-3

Deleted: –

VPC: vpc-0f6fd5356a0b8a0 / Lab VPC

Secondary IPv4 addresses

Criar uma tabela de rota, adicionar o destino 0.0.0.0/0 para o Nat Gateway criado na etapa anterior.



You have successfully updated subnet associations for rtb-0a33f042fb9b89c5d / Private Route Table

rtb-0a33f042fb9b89c5d / Private Route Table

Details

Route table ID: rtb-0a33f042fb9b89c5d

Main: No

Explicit subnet associations: subnet-01874e[illegible] / Private Subnet

Edge associations: -

VPC: vpc-[illegible] | Lab VPC

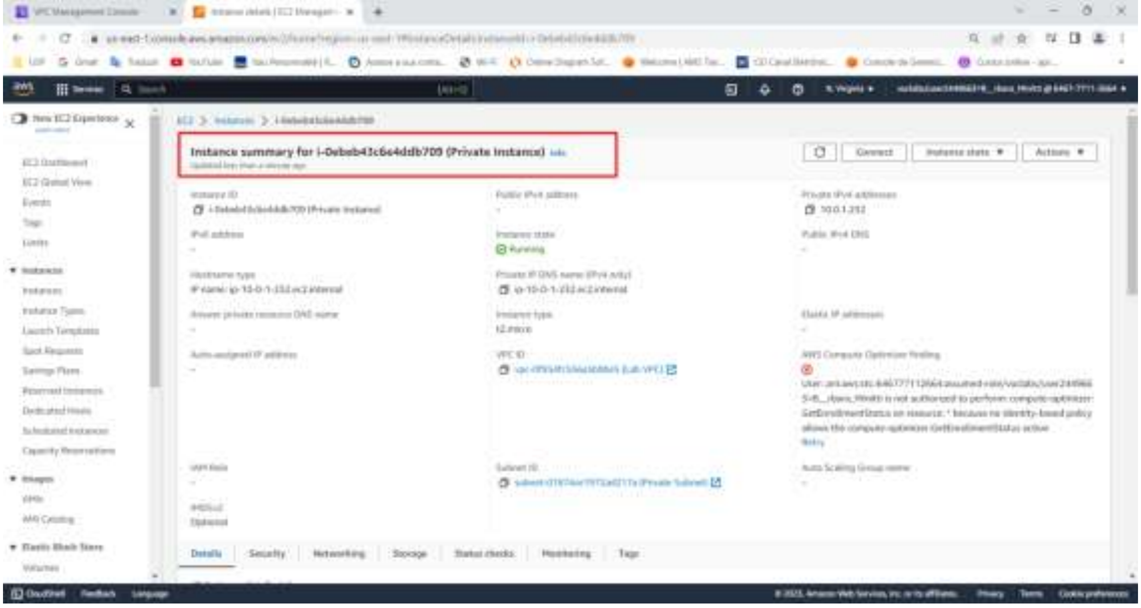
Owner ID: 646777112664

Routes (2)

Destination	Target	Status	Propagated
0.0.0.0/0	nat-[illegible]	Active	No
10.0.0.0/16	local	Active	No

Tarefa7

Criar instância EC2 na sub-rede privada



Instance summary for i-0ebeb43c6e4ddb709 (Private Instance)

Instance ID: i-0ebeb43c6e4ddb709 (Private Instance)

Public IPv4 address: -

Private IPv4 addresses: 10.0.1.232

IPv6 address: -

Instance state: Running

Public IPv4 DNS: -

Hostname type: IP name: ip-10-0-1-232.ec2.internal

Private IP DNS name (IPv4 only): ip-10-0-1-232.ec2.internal

Answer private resource DNS name: -

Instance type: t2.micro

Elastic IP addresses: -

Auto-assigned IP address: -

VPC ID: vpc-[illegible] (Lab VPC)

AWS Compute Optimizer finding: [illegible]

IAM Role: -

Subnet ID: subnet-01874e[illegible] (Private Subnet)

Auto Scaling Group name: -

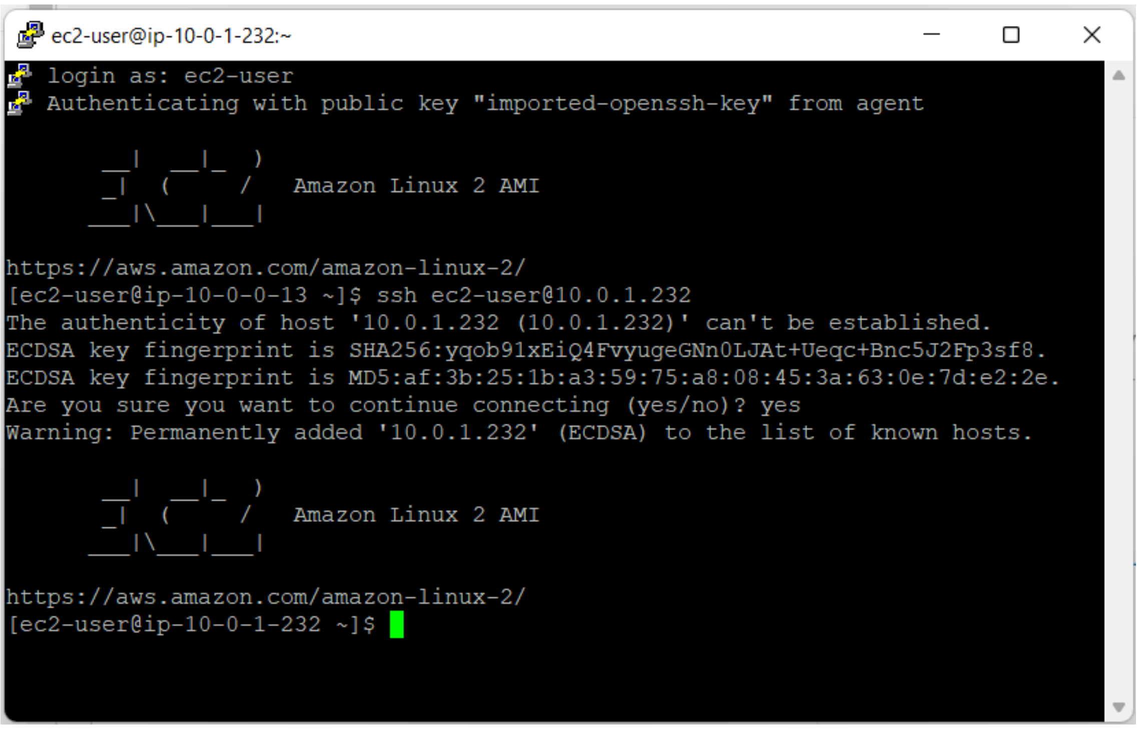
IMDSv2: Optional

Tarefa8 / Tarefa 9

Configurar o cliente SSH para passagem SSH

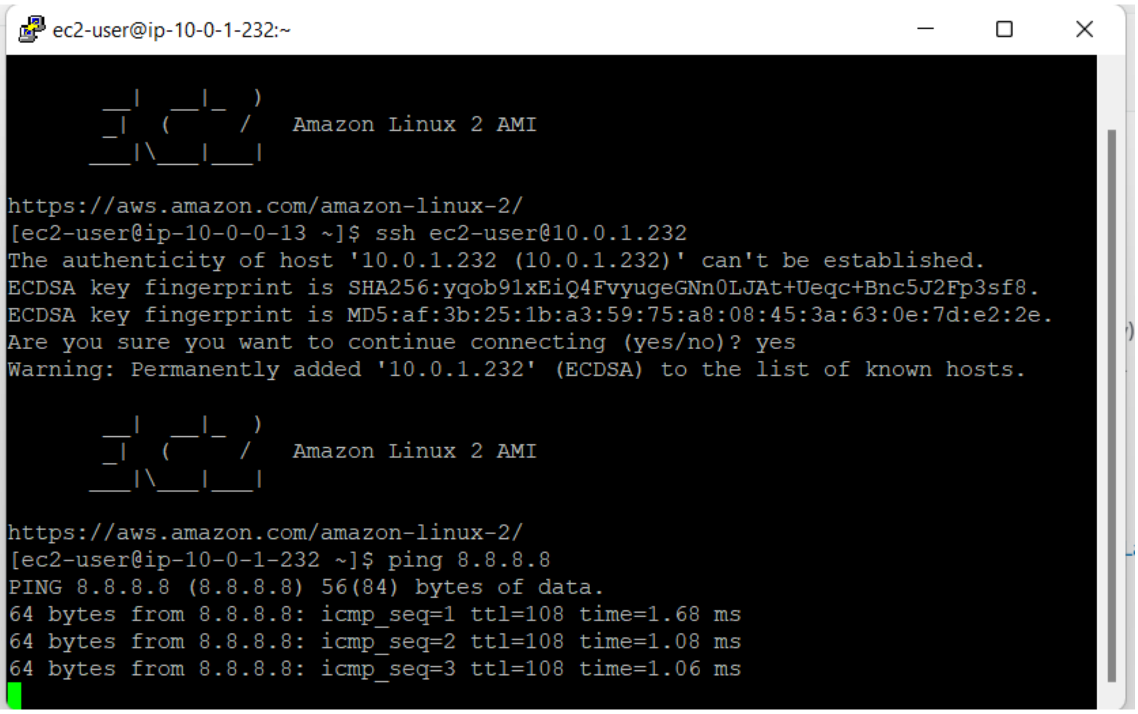
Testar a conexão SSH do Bastion Host

Testar a conexão instância privada através do bastion host



```
login as: ec2-user
Authenticating with public key "imported-openssh-key" from agent

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

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-0-0-13 ~]$ ssh ec2-user@10.0.1.232
The authenticity of host '10.0.1.232 (10.0.1.232)' can't be established.
ECDSA key fingerprint is SHA256:yqob91xEiQ4FvyugeGNn0LJAt+Ueqc+Bnc5J2Fp3sf8.
ECDSA key fingerprint is MD5:af:3b:25:1b:a3:59:75:a8:08:45:3a:63:0e:7d:e2:2e.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.1.232' (ECDSA) to the list of known hosts.

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

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-0-1-232 ~]$
```

Testar a conexão com a internet através da instância privada

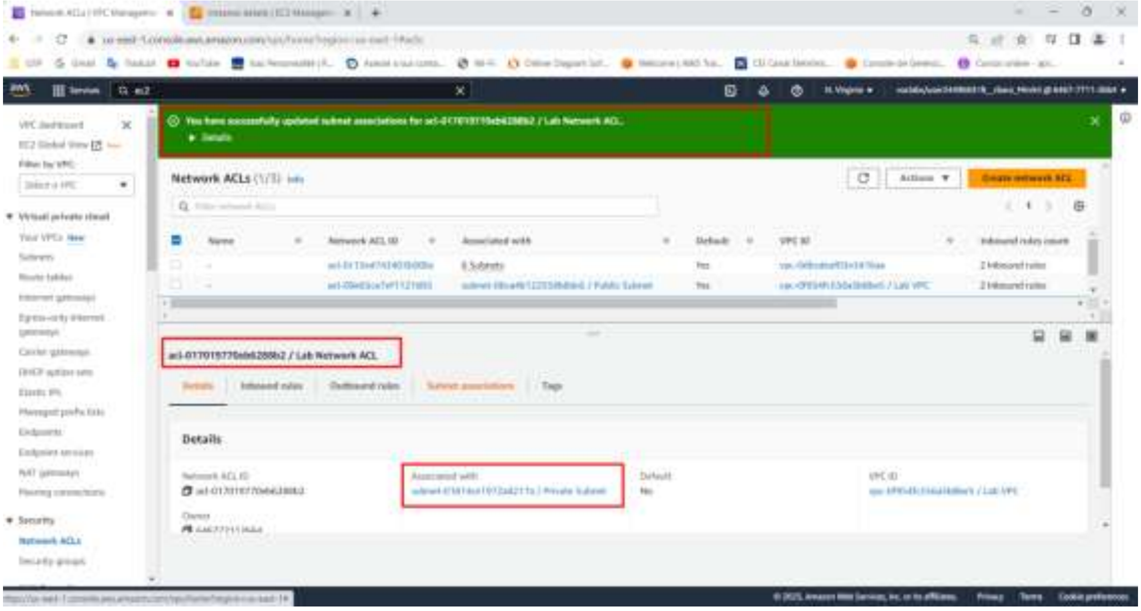


```
       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-0-0-13 ~]$ ssh ec2-user@10.0.1.232
The authenticity of host '10.0.1.232 (10.0.1.232)' can't be established.
ECDSA key fingerprint is SHA256:yqob91xEiQ4FvyugeGNn0LJAt+Ueqc+Bnc5J2Fp3sf8.
ECDSA key fingerprint is MD5:af:3b:25:1b:a3:59:75:a8:08:45:3a:63:0e:7d:e2:2e.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.1.232' (ECDSA) to the list of known hosts.

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

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-0-1-232 ~]$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=108 time=1.68 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=108 time=1.08 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=108 time=1.06 ms
```

2.) Desafio nº 2

Tarefa10

Criar uma Network ACL



You have successfully updated subnet associations for acl-017019770eb6288b2 / Lab Network ACL.

Network ACLs (1/3)

Name	Network ACL ID	Associated with	Default	VPC ID	Inbound rules count
–	acl-[illegible]	6 Subnets	Yes	vpc-[illegible]	2 Inbound rules
–	acl-[illegible]	subnet-[illegible] / Public Subnet	Yes	vpc-[illegible] / Lab VPC	2 Inbound rules

acl-017019770eb6288b2 / Lab Network ACL

Details

Network ACL ID	Associated with	Default	VPC ID
acl-017019770eb6288b2	subnet-[illegible] / Private Subnet	No	vpc-[illegible] / Lab VPC

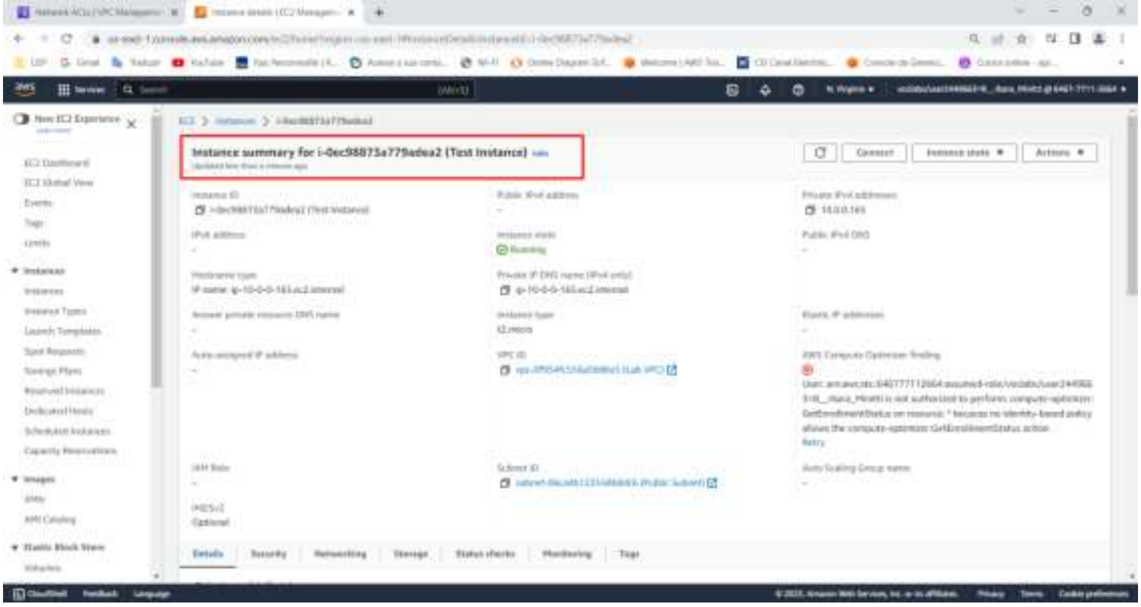
Owner
[illegible]

© 2025, Amazon Web Services, Inc. or its affiliates.

Tarefa11

Testar a Network ACL personalizada

Criar uma Test Instance

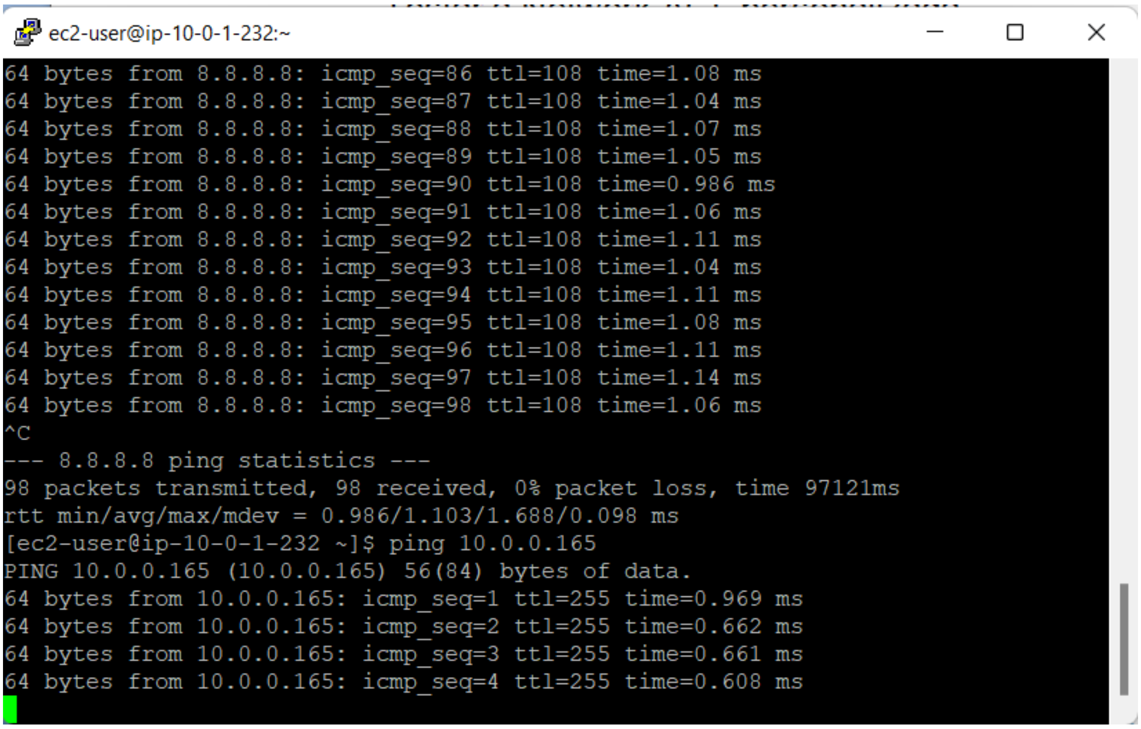


Instance summary for i-0ec98873a779adea2 (Test Instance)

Instance ID i-0ec98873a779adea2 (Test Instance)	Public IPv4 address –	Private IPv4 addresses 10.0.0.165
IPv6 address –	Instance state Running	Public IPv4 DNS –
Hostname type IP name: ip-10-0-0-165.ec2.internal	Private IP DNS name (IPv4 only) ip-10-0-0-165.ec2.internal	
Answer private resource DNS name –	Instance type t2.micro	Elastic IP addresses –
Auto-assigned IP address –	VPC ID vpc-[illegible] (Lab VPC)	AWS Compute Optimizer finding [illegible] is not authorized to perform: compute-optimizer:GetEnrollmentStatus on resource: * because no identity-based policy allows the compute-optimizer:GetEnrollmentStatus action Retry
IAM Role –	Subnet ID subnet-[illegible] (Public Subnet)	Auto Scaling Group name –
IMDSv2 Optional		

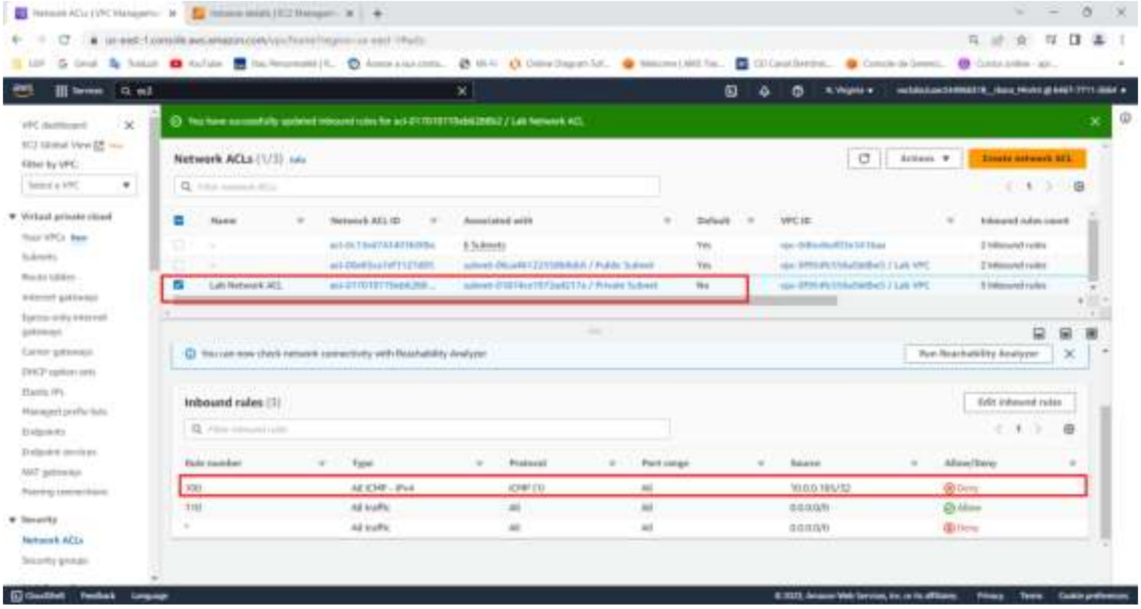
© 2025, Amazon Web Services, Inc. or its affiliates.

Ping Test Instance através da Private Instance



```
64 bytes from 8.8.8.8: icmp_seq=86 ttl=108 time=1.08 ms
64 bytes from 8.8.8.8: icmp_seq=87 ttl=108 time=1.04 ms
64 bytes from 8.8.8.8: icmp_seq=88 ttl=108 time=1.07 ms
64 bytes from 8.8.8.8: icmp_seq=89 ttl=108 time=1.05 ms
64 bytes from 8.8.8.8: icmp_seq=90 ttl=108 time=0.986 ms
64 bytes from 8.8.8.8: icmp_seq=91 ttl=108 time=1.06 ms
64 bytes from 8.8.8.8: icmp_seq=92 ttl=108 time=1.11 ms
64 bytes from 8.8.8.8: icmp_seq=93 ttl=108 time=1.04 ms
64 bytes from 8.8.8.8: icmp_seq=94 ttl=108 time=1.11 ms
64 bytes from 8.8.8.8: icmp_seq=95 ttl=108 time=1.08 ms
64 bytes from 8.8.8.8: icmp_seq=96 ttl=108 time=1.11 ms
64 bytes from 8.8.8.8: icmp_seq=97 ttl=108 time=1.14 ms
64 bytes from 8.8.8.8: icmp_seq=98 ttl=108 time=1.06 ms
^C
--- 8.8.8.8 ping statistics ---
98 packets transmitted, 98 received, 0% packet loss, time 97121ms
rtt min/avg/max/mdev = 0.986/1.103/1.688/0.098 ms
[ec2-user@ip-10-0-1-232 ~]$ ping 10.0.0.165
PING 10.0.0.165 (10.0.0.165) 56(84) bytes of data.
64 bytes from 10.0.0.165: icmp_seq=1 ttl=255 time=0.969 ms
64 bytes from 10.0.0.165: icmp_seq=2 ttl=255 time=0.662 ms
64 bytes from 10.0.0.165: icmp_seq=3 ttl=255 time=0.661 ms
64 bytes from 10.0.0.165: icmp_seq=4 ttl=255 time=0.608 ms
```

Alterar a Network ACL personalizada para negar todo trafego ICMP – IPV4



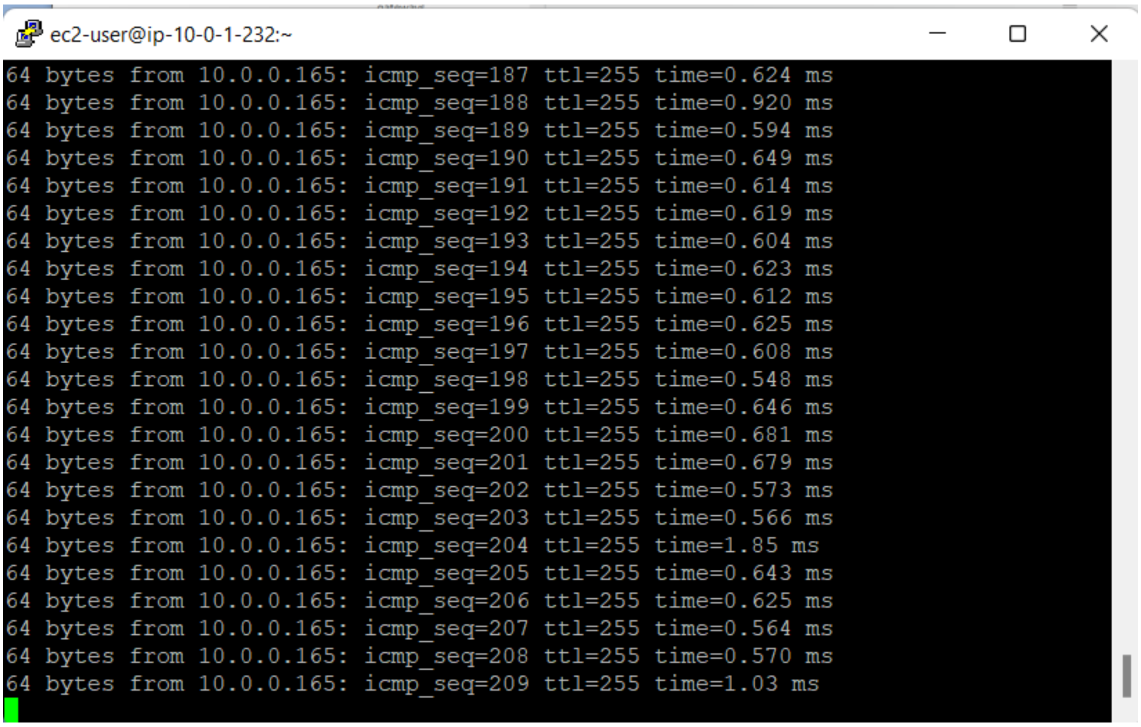
You have successfully updated inbound rules for acl-[illegible] / Lab Network ACL

Name	Network ACL ID	Associated with	Default	VPC ID	Inbound rules count
-	[illegible]	6 Subnets	Yes	[illegible]	2 Inbound rules
-	[illegible]	[illegible] / Public Subnet	Yes	[illegible] / Lab VPC	2 Inbound rules
Lab Network ACL	[illegible]	[illegible] / Private Subnet	No	[illegible] / Lab VPC	3 Inbound rules

You can now check network connectivity with Reachability Analyzer

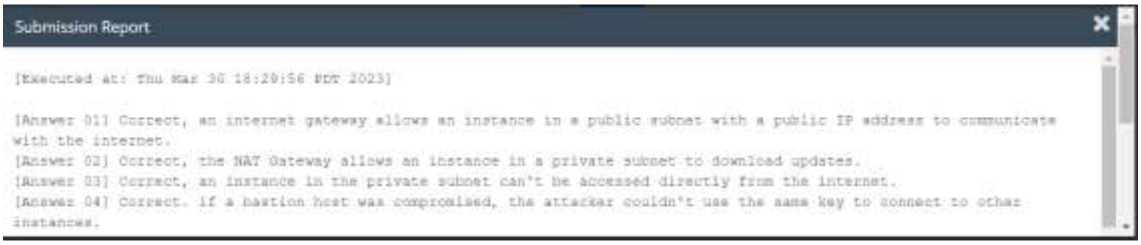
Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	All ICMP - IPv4	ICMP (1)	All	10.0.0.185/32	Deny
110	All traffic	All	All	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

A Test Instance parou de “pingar”

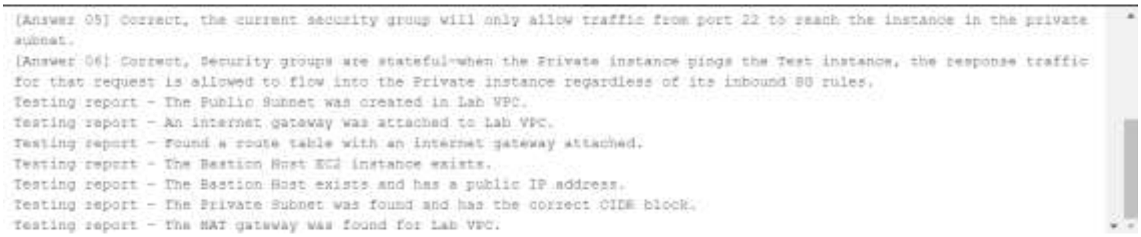


```
64 bytes from 10.0.0.165: icmp_seq=187 ttl=255 time=0.624 ms
64 bytes from 10.0.0.165: icmp_seq=188 ttl=255 time=0.920 ms
64 bytes from 10.0.0.165: icmp_seq=189 ttl=255 time=0.594 ms
64 bytes from 10.0.0.165: icmp_seq=190 ttl=255 time=0.649 ms
64 bytes from 10.0.0.165: icmp_seq=191 ttl=255 time=0.614 ms
64 bytes from 10.0.0.165: icmp_seq=192 ttl=255 time=0.619 ms
64 bytes from 10.0.0.165: icmp_seq=193 ttl=255 time=0.604 ms
64 bytes from 10.0.0.165: icmp_seq=194 ttl=255 time=0.623 ms
64 bytes from 10.0.0.165: icmp_seq=195 ttl=255 time=0.612 ms
64 bytes from 10.0.0.165: icmp_seq=196 ttl=255 time=0.625 ms
64 bytes from 10.0.0.165: icmp_seq=197 ttl=255 time=0.608 ms
64 bytes from 10.0.0.165: icmp_seq=198 ttl=255 time=0.548 ms
64 bytes from 10.0.0.165: icmp_seq=199 ttl=255 time=0.646 ms
64 bytes from 10.0.0.165: icmp_seq=200 ttl=255 time=0.681 ms
64 bytes from 10.0.0.165: icmp_seq=201 ttl=255 time=0.679 ms
64 bytes from 10.0.0.165: icmp_seq=202 ttl=255 time=0.573 ms
64 bytes from 10.0.0.165: icmp_seq=203 ttl=255 time=0.566 ms
64 bytes from 10.0.0.165: icmp_seq=204 ttl=255 time=1.85 ms
64 bytes from 10.0.0.165: icmp_seq=205 ttl=255 time=0.643 ms
64 bytes from 10.0.0.165: icmp_seq=206 ttl=255 time=0.625 ms
64 bytes from 10.0.0.165: icmp_seq=207 ttl=255 time=0.564 ms
64 bytes from 10.0.0.165: icmp_seq=208 ttl=255 time=0.570 ms
64 bytes from 10.0.0.165: icmp_seq=209 ttl=255 time=1.03 ms
```

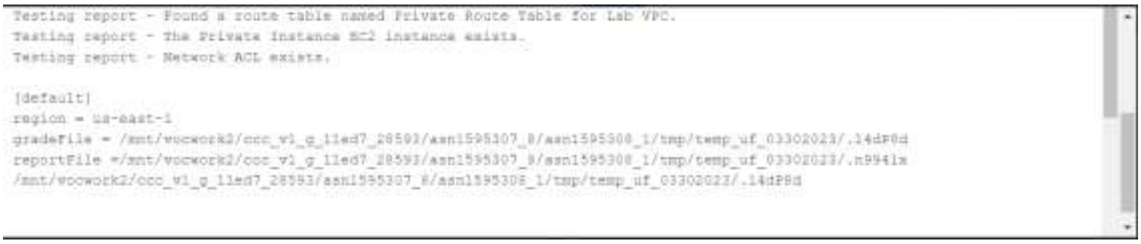
Report



```
[Executed at: Thu Mar 30 18:20:56 PDT 2023]

[Answer 01] Correct, an internet gateway allows an instance in a public subnet with a public IP address to communicate
with the internet.
[Answer 02] Correct, the NAT Gateway allows an instance in a private subnet to download updates.
[Answer 03] Correct, an instance in the private subnet can't be accessed directly from the internet.
[Answer 04] Correct. if a bastion host was compromised, the attacker couldn't use the same key to connect to other
instances.
```



```
[Answer 05] Correct, the current security group will only allow traffic from port 22 to reach the instance in the private
subnet.
[Answer 06] Correct, Security groups are stateful-when the Private instance pings the Test instance, the response traffic
for that request is allowed to flow into the Private instance regardless of its inbound 80 rules.
Testing report - The Public Subnet was created in Lab VPC.
Testing report - An internet gateway was attached to Lab VPC.
Testing report - Found a route table with an internet gateway attached.
Testing report - The Bastion Host EC2 instance exists.
Testing report - The Bastion Host exists and has a public IP address.
Testing report - The Private Subnet was found and has the correct CIDR block.
Testing report - The NAT gateway was found for Lab VPC.
```



```
Testing report - Found a route table named Private Route Table for Lab VPC.
Testing report - The Private Instance EC2 instance exists.
Testing report - Network ACL exists.

[default]
region = us-east-1
gradeFile = /mnt/vocwork2/ccc_v1_g_11ed7_28593/asn1595307_8/asn1595308_1/tmp/temp_uf_03302023/.14dF8d
reportFile =/mnt/vocwork2/ccc_v1_g_11ed7_28593/asn1595307_8/asn1595308_1/tmp/temp_uf_03302023/.n9941x
/mnt/vocwork2/ccc_v1_g_11ed7_28593/asn1595307_8/asn1595308_1/tmp/temp_uf_03302023/.14dF8d
```