



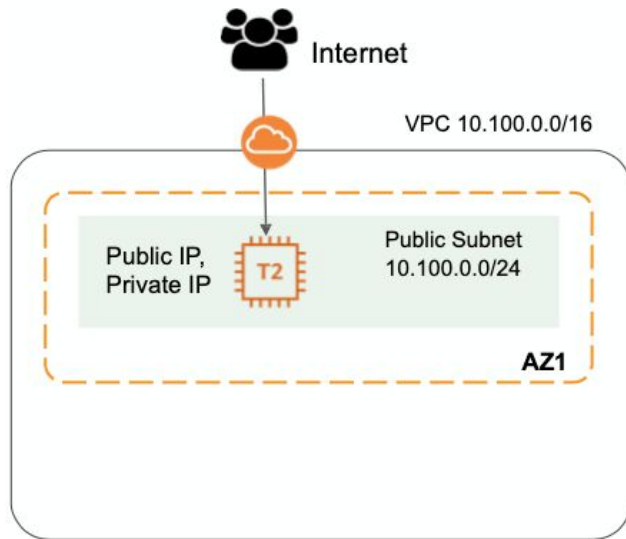
DevOps

CERTIFICACIÓN
Universitaria

 UNC  FCEyN | mE

LAB-VPC-1

VPC with Single Public Subnet



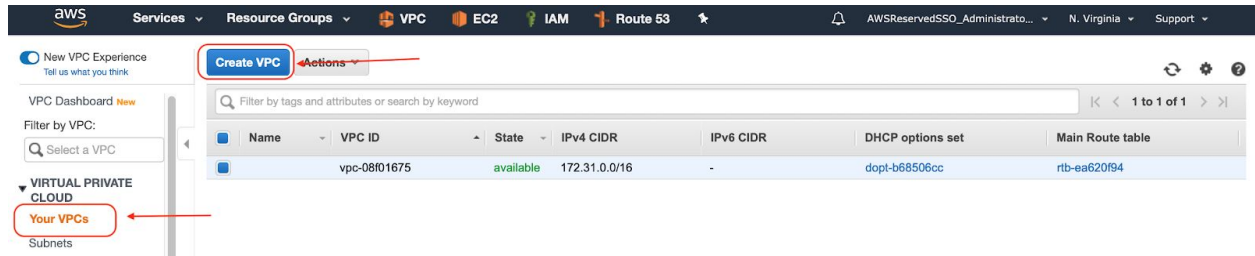
Public Subnet Route Table

Destination	Target
10.100.0.0/16	local
0.0.0.0/0	igw-xxx

Resolution

Create VPC

Go to VPC service -> Your VPCs -> Create VPC (Name: MyVPC, CIDR: 10.100.0.0/16) -> Create



VPCs > Create VPC

Create VPC

A VPC is an isolated portion of the AWS cloud populated by AWS resources, such as Amazon EC2 instances. You must specify an IPv4 address range for your VPC. Specify the IPv4 address range as a Classless Inter-Domain Routing (CIDR) block; for example, 10.0.0.0/16. You cannot specify an IPv4 CIDR block larger than /16. You can optionally associate an IPv6 CIDR block with the VPC.

Name tag ⓘ

IPv4 CIDR block* ⓘ

IPv6 CIDR block ☒ No IPv6 CIDR Block ⓘ
☐ Amazon provided IPv6 CIDR block
☐ IPv6 CIDR owned by me

Tenancy ⓘ

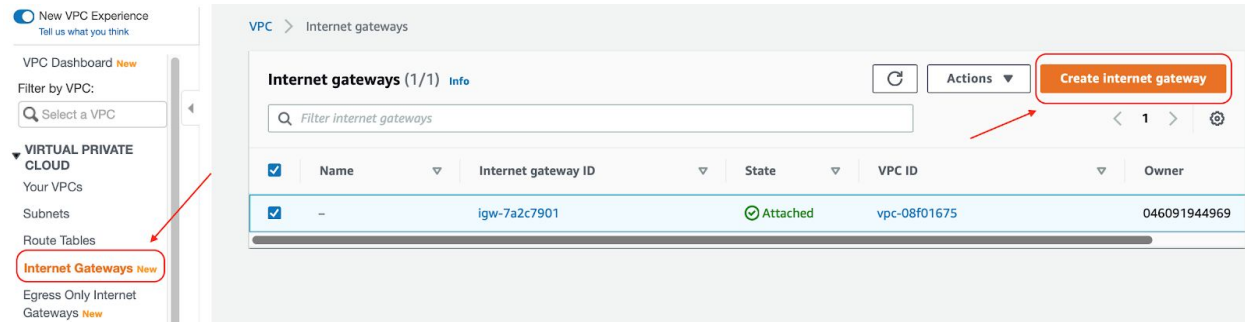
* Required

Cancel

Create

Create Internet Gateway

Go to Internet Gateways -> Create internet gateway



New VPC Experience
Tell us what you think

VPC Dashboard **New**

Filter by VPC:
Select a VPC

VIRTUAL PRIVATE CLOUD

- Your VPCs
- Subnets
- Route Tables
- Internet Gateways **New****
- Egress Only Internet Gateways **New**

VPC > Internet gateways

Internet gateways (1/1) **Info**

Filter internet gateways

Actions **Create Internet gateway**

<input checked="" type="checkbox"/>	Name	Internet gateway ID	State	VPC ID	Owner
<input checked="" type="checkbox"/>	-	igw-7a2c7901	Attached	vpc-08f01675	046091944969

Create internet gateway **Info**

An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.

Internet gateway settings

Name tag

Creates a tag with a key of 'Name' and a value that you specify.

myvpc-igw

Tags - optional

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key

Name

Value - optional

myvpc-igw

Remove

Add new tag

You can add 49 more tags.

Cancel

Create internet gateway

Attach Internet Gateway to VPC

Select Internet gateway -> Actions -> Attach to VPC -> Select your VPC

VPC > Internet gateways > igw-025b12c2889cf5210

igw-025b12c2889cf5210 / myvpc-igw

Details [Info](#)

Internet gateway ID	State	VPC ID	Owner
igw-025b12c2889cf5210	Detached	-	046091944900

Tags [Manage tags](#)

Search tags

Key	Value
Name	myvpc-igw

VPC > Internet gateways > Attach to VPC (igw-025b12c2889cf5210)

Attach to VPC (igw-025b12c2889cf5210) [Info](#)

VPC
Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.

Available VPCs
Attach the internet gateway to this VPC.

Q vpc-0df4e6d3766e1e51f X

► **AWS Command Line Interface command**

Cancel **Attach internet gateway**

VPC > Internet gateways > igw-025b12c2889cf5210

igw-025b12c2889cf5210 / myvpc-igw

Actions

Details Info

Internet gateway ID igw-025b12c2889cf5210	State Attached	VPC ID vpc-0df4e6d3766e1e51f MyVPC	Owner 046091944969
--	-------------------	---	-----------------------

Create Subnet

Subnets -> Create subnet (Name: MyVPC-Public, VPC: MyVPC, AZ: Select first az - us-east-1a, CIDR: 10.100.0.0/24)

New VPC Experience
Tell us what you think

VPC Dashboard New

Filter by VPC:
Select a VPC

VIRTUAL PRIVATE CLOUD

Your VPCs

Subnets

Route Tables

Internet Gateways New

Create subnet

Filter by tags and attributes or search by keyword

Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4
	subnet-2266ea2c	available	vpc-08f01675	172.31.64.0/20	4091
	subnet-5152850e	available	vpc-08f01675	172.31.32.0/20	4091
	subnet-68da100e	available	vpc-08f01675	172.31.0.0/20	4091
	subnet-8d7960b3	available	vpc-08f01675	172.31.48.0/20	4091
	subnet-b00298fd	available	vpc-08f01675	172.31.16.0/20	4091
	subnet-ff9a4ade	available	vpc-08f01675	172.31.80.0/20	4091

Subnets > Create subnet

Create subnet

Specify your subnet's IP address block in CIDR format; for example, 10.0.0.0/24. IPv4 block sizes must be between a /16 netmask and /28 netmask, and can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.

Create subnet | VPC Management Console

Name tag MyVPC-Public

VPC* vpc-0df4e6d3766e1e51f

Select MyVPC

Availability Zone us-east-1a

VPC CIDRs

CIDR	Status	Status Reason
10.100.0.0/16	associated	

IPv4 CIDR block* 10.100.0.0/24

* Required

Cancel

Create

Select Subnet -> Action -> Modify Auto Assign Public IP -> Enable -> Save

Create subnet **Actions**

- Delete subnet
- Create flow log
- Modify auto-assign IP settings**
- Edit IPv6 CIDRs
- Edit network ACL association
- Edit route table association
- Share subnet
- Add/Edit Tags

Name	State	VPC	IPv4 CIDR	Available IPv4	IPv6 CIDR
MyVPC-Pu	available	vpc-0df4e6d3766e1e51f ...	10.100.0.0/24	251	-

Subnet: subnet-0aada8ff5fd454ec3

Description	Flow Logs	Route Table	Network ACL	Tags	Sharing
Subnet ID subnet-0aada8ff5fd454ec3					
VPC vpc-0df4e6d3766e1e51f MyVPC					
Available IPv4 Addresses 251					
Availability Zone us-east-1a (use1-az6)					
Network ACL acl-0e0afca1fa18d7865					
Auto-assign public IPv4 address No					
Customer-owned IPv4 pool -					
Outpost ID -					
State available					
IPv4 CIDR 10.100.0.0/24					
IPv6 CIDR -					
Route Table rtb-02bd9ba65d04e853b					
Default subnet No					
Auto-assign customer-owned IPv4 address No					
Auto-assign IPv6 address No					
Owner 046091944969					

[Subnets](#) > Modify auto-assign IP settings

Modify auto-assign IP settings

Enable the auto-assign IP address setting to automatically request a public IPv4 or IPv6 address for an instance launched in this subnet. You can override the auto-assign IP settings for an instance at launch time.

Subnet ID subnet-0aada8ff5fd454ec3

Auto-assign IPv4 ☒ Enable auto-assign public IPv4 address ⓘ

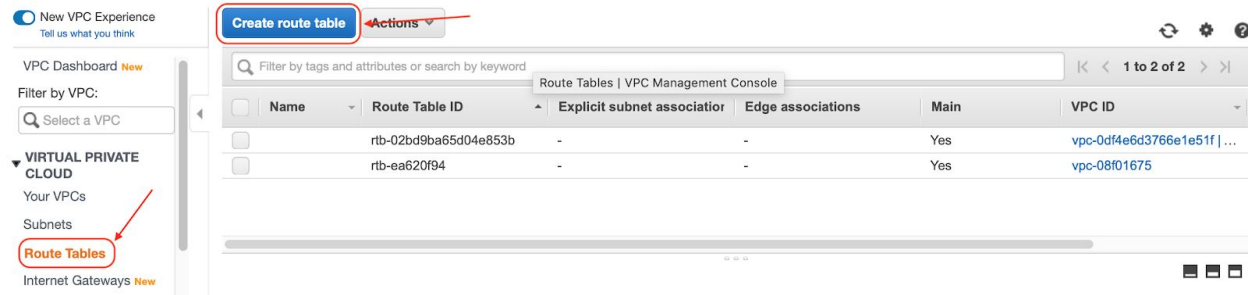
Auto-assign Co-IP ☐ Enable auto-assign customer-owned IPv4 address ⓘ

* Required

[Cancel](#) [Save](#)

Create Route Table

Route Tables -> Create Route Table (Name: MyVPC-Public, VPC: MyVPC)



Actions

Filter by tags and attributes or search by keyword

Name	Route Table ID	Explicit subnet association	Edge associations	Main	VPC ID
	rtb-02bd9ba65d04e853b	-	-	Yes	vpc-0df4e6d3766e1e51f ...
	rtb-ea620f94	-	-	Yes	vpc-08f01675

[Route Tables](#) > Create route table

Create route table

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

Name tag ⓘ

VPC* ⓘ ⓘ **Select MyVPC**

Key	(128 characters maximum)	Value	(256 characters maximum)
This resource currently has no tags			

Add Tag 50 remaining (Up to 50 tags maximum)

* Required

[Cancel](#) [Create](#)

Add route to send all traffic that is not local to Internet Gateway

Select Route table -> Routes -> Edit -> Add another route (Destination: 0.0.0.0/0, Target: Internet gateway -> igw-xxx) -> Save

Route Tables > Edit routes

AWSReservedSSO_AdministratorAccess_03764b
ac4500cab0/rnieva @ 046091944969

Edit routes

Destination	Target	Status	Propagated
10.100.0.0/16	local	active	No
0.0.0.0/0	igw-		No

Add route

igw-025b12c2889cf5210 myvpc-igw

* Required

Cancel Save routes

Associate Route table with Subnet to make it Public Subnet

Select Route table -> Subnet Associations -> Edit -> Check the MyVPC-Public subnet -> Save

Create route table Actions

Name: MyVPC-Public-RT Add filter

Name	Route Table ID	Explicit subnet association	Edge associations	Main	VPC ID	Owner
MyVPC-Pu...	rtb-02ca5122d39719980	-	-	No	vpc-0df4e6d3766e1e51f ...	046091944969

Route Table: rtb-02ca5122d39719980

Summary Routes Subnet Associations Edge Associations Route Propagation Tags

Edit subnet associations

Subnet ID	IPv4 CIDR	IPv6 CIDR
-----------	-----------	-----------

You do not have any subnet associations.

Edit subnet associations

Route table rtb-02ca5122d39719980 (MyVPC-Public-RT)

Associated subnets subnet-0aada8ff5fd454ec3

Filter by attributes or search by keyword			
1 to 1 of 1			
<input type="checkbox"/> Subnet ID	IPv4 CIDR	IPv6 CIDR	Current Route Table
<input checked="" type="checkbox"/> subnet-0aada8ff5fd454ec3 MyVPC-Pu...	10.100.0.0/24	-	Main

* Required

Cancel Save

Launch EC2 instance in newly created Public Subnet

Step 3: Configure Instance Details

Number of instances [Launch into Auto Scaling Group](#)

Purchasing option ☐ Request Spot instances

Network [Create new VPC](#)

Subnet [Create new subnet](#)

Auto-assign Public IP

Placement group ☐ Add instance to placement group

Capacity Reservation [Create new Capacity Reservation](#)

IAM role [Create new IAM role](#)

Shutdown behavior

Stop - Hibernate behavior ☐ Enable hibernation as an additional stop behavior

Enable termination protection ☐ Protect against accidental termination

Monitoring ☐ Enable CloudWatch detailed monitoring

Cancel Previous **Review and Launch** **Next: Add Storage**

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. A copy of a tag can be applied to volumes, instances or both.

Tags will be applied to all instances and volumes. [Learn more](#) about tagging your Amazon EC2 resources.

Key (128 characters maximum)	Value (256 characters maximum)	Instances	Volumes
Name	My-EC2-A	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[Add another tag](#) (Up to 50 tags maximum)

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Configure Security Group](#)

Configure Security Group

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: ☒ Create a new security group ☐ Select an existing security group

Security group name: MyVPC-SG

Description: MyVPC-SG

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	My IP 186.13.114.75/32	e.g. SSH for Admin Desktop

[Add Rule](#)

[Cancel](#) [Previous](#) [Review and Launch](#)

Select an existing key pair or create a new key pair



A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Create a new key pair

Key pair name
rnieva-keypair

Download Key Pair

You have to download the **private key file** (*.pem file) before you can continue. **Store it in a secure and accessible location.** You will not be able to download the file again after it's created.

Cancel

Launch Instances

Launch Instance

Connect

Actions

search : i-09d843b215b20c666

Add filter

	Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP
	MyEC2-A	i-09d843b215b20c666	t2.micro	us-east-1a	running	2/2 checks ...	None		54.211.247.181

Instance: i-09d843b215b20c666 (MyEC2-A)

Public IP: 54.211.247.181

Description

Status Checks

Monitoring

Tags

Instance ID

Instance state

Instance type

Finding

Private DNS

Private IPs

Secondary private IPs

VPC ID

Subnet ID

Network interfaces

i-09d843b215b20c666

running

t2.micro

Opt-in to AWS Compute Optimizer for recommendations. [Learn more](#)

ip-10-100-0-139.ec2.internal

10.100.0.139

vpc-0df4e6d3766e1e51f (MyVPC)

subnet-0aada8ff5fd454ec3 (MyVPC-Public)

eth0

Public DNS (IPv4)

IPv4 Public IP

IPv6 IPs

Elastic IPs

Availability zone

Security groups

Scheduled events

AMI ID

Platform details

Usage operation

-

54.211.247.181

-

-

us-east-1a

MyVPC-SG. [view inbound rules](#). [view outbound rules](#)

No scheduled events

amzn2-ami-hvm-2.0.20200617.0-x86_64-gp2 (ami-08f3d892de259504d)

Linux/UNIX

RunInstances

Connect to EC2 instance using the public IP from your laptop using linux terminal
(ec2-user)

```
$ chmod 600 rnieva-keypair.pem
```

```
$ ls -l rnieva-keypair.pem
```

```
-rw-----@ 1 rnieva  staff  1692 Jul 24 16:56 rnieva-keypair.pem
```

```
$ ssh -i rnieva-keypair.pem ec2-user@54.211.247.181
```

```
The authenticity of host '54.211.247.181 (54.211.247.181)' can't be established.
```

```
ECDSA key fingerprint is
```

```
SHA256:gPaH78Hue2C+uPgXbB0+wdrx/q5UqQZ6MWZR78qDvLo.
```

```
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
```

```
Warning: Permanently added '54.211.247.181' (ECDSA) to the list of known hosts.
```

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

```
https://aws.amazon.com/amazon-linux-2/
```

```
14 package(s) needed for security, out of 31 available
```

```
Run "sudo yum update" to apply all updates.
```

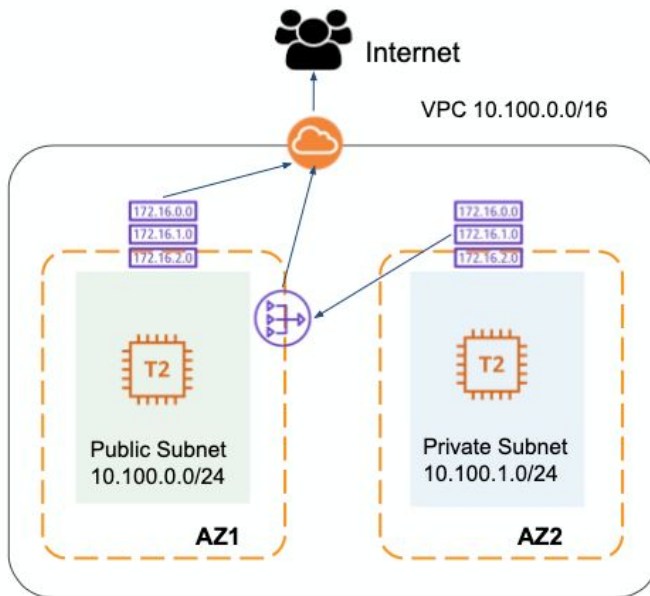
```
-bash: warning: setlocale: LC_CTYPE: cannot change locale (UTF-8): No such file or directory
```

```
[ec2-user@ip-10-100-0-139 ~]$ uptime
```

```
20:07:48 up 10 min,  1 user,  load average: 0.00, 0.01, 0.00
```

LAB-VPC-1

VPC with Public and Private Subnet



Public Subnet Route Table

Destination	Target
10.100.0.0/16	local
0.0.0.0/0	igw-xxx

Private Subnet Route Table

Destination	Target
10.100.0.0/16	local

Solution:

Create a Private Subnet

Create subnet (Name: MyVPC-Private, VPC: MyVPC, AZ: Select different az (us-east-1b), CIDR: 10.100.1.0/24) 2. Create Private route table

[Subnets](#) > Create subnet

Create subnet

Specify your subnet's IP address block in CIDR format; for example, 10.0.0.0/24. IPv4 block sizes must be between a /16 netmask and /28 netmask, and can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.

Name tag ⓘ

VPC* ⓘ Choose subnet MyVPC-Public

Availability Zone ⓘ

VPC CIDRs	CIDR	Status	Status Reason
	10.100.0.0/16	associated	

IPv4 CIDR block* ⓘ

* Required

[Cancel](#) [Create](#)

Create Private route table

Route Tables -> Create Route Table (Name: MyVPC-Private, VPC: MyVPC)

[Route Tables](#) > Create route table

Create route table

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

Name tag ⓘ

VPC: MyVPC VPC* ⓘ [Refresh](#)

Key	(128 characters maximum)	Value	(256 characters maximum)
This resource currently has no tags			
Add Tag	50 remaining	(Up to 50 tags maximum)	

* Required

[Cancel](#) [Create](#)

Associate Route table with Subnet to make it Private subnet
Select Route table -> Subnet Associations -> Edit -> Check the MyVPC-Private subnet -> Save

[Create route table](#) [Actions](#)

Route Table ID : rtb-0aec07a9b768ad4b2 [Add filter](#) << < 1 to 1 of 1 > >>

<input type="checkbox"/>	Name	Route Table ID	Explicit subnet association	Edge associations	Main
<input checked="" type="checkbox"/>	MyVPC-Private-RT	rtb-0aec07a9b768ad4b2	-	-	No

Route Table: rtb-0aec07a9b768ad4b2

[Summary](#) [Routes](#) [Subnet Associations](#) [Edge Associations](#) [Route Propagation](#) [Tags](#)

[Edit subnet associations](#)

<< < None found > >>

Subnet ID	IPv4 CIDR	IPv6 CIDR
-----------	-----------	-----------

You do not have any subnet associations.

[Route Tables](#) > Edit subnet associations

Edit subnet associations

Route table rtb-0aec07a9b768ad4b2 (MyVPC-Private-RT)

Associated subnets [subnet-0ab00ecc35cca6298](#)

Filter by attributes or search by keyword << < 1 to 2 of 2 > >>

<input type="checkbox"/>	Subnet ID	IPv4 CIDR	IPv6 CIDR	Current Route Table
<input checked="" type="checkbox"/>	subnet-0ab00ecc35cca6298 MyVPC-Private	10.100.1.0/24	-	Main
<input type="checkbox"/>	subnet-0aada8ff5fd454ec3 MyVPC-Public	10.100.0.0/24	-	rtb-02ca5122d39719980

* Required

[Cancel](#) [Save](#)

Launch another EC2 instance in same VPC but in newly created Private subnet

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 3: Configure Instance Details

Number of instances [Launch into Auto Scaling Group](#)

Purchasing option ☐ Request Spot instances

Network [Create new VPC](#)

Subnet [Create new subnet](#)

Auto-assign Public IP

Placement group ☐ Add instance to placement group

Capacity Reservation [Create new Capacity Reservation](#)

IAM role [Create new IAM role](#)

Shutdown behavior

Stop - Hibernate behavior ☐ Enable hibernation as an additional stop behavior

Enable termination protection ☐ Protect against accidental termination

Monitoring ☐ Enable CloudWatch detailed monitoring
[Additional charges apply.](#)

Tenancy [Additional charges may apply when launching Dedicated instances.](#)

Elastic Inference ☐ Add an Elastic Inference accelerator

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Add Storage](#)

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.

A copy of a tag can be applied to volumes, instances or both.

Tags will be applied to all instances and volumes. [Learn more](#) about tagging your Amazon EC2 resources.

Key (128 characters maximum)	Value (256 characters maximum)	Instances	Volumes
<input type="text" value="Name"/>	<input type="text" value="My-EC2-B"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[Add another tag](#) (Up to 50 tags maximum)

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Configure Security Group](#)

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: ☒ Create a new security group
☐ Select an existing security group

Security group name: MyVPC-Private-SG

Description: MyVPC-Private-SG

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	Custom 10.100.0.0/24	Public Subnet
All ICMP - IP	ICMP	0 - 65535	Custom 10.100.0.0/24	e.g. SSH for Admin Desktop

Add Rule

Cancel

Previous

Review and Launch

Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Choose an existing key pair
Select a key pair
rnieva-keypair

☒ I acknowledge that I have access to the selected private key file (rnieva-keypair.pem), and that without this file, I won't be able to log into my instance.

Cancel

Launch Instances

Note down the My-EC2-B private IP address.

The screenshot shows the AWS Management Console interface for an EC2 instance named 'My-EC2-B'. The instance is in a 'running' state. The 'Description' tab is selected, displaying various instance details. Key information includes:

- Instance ID:** i-0ab7fa62a9fe8152a
- Instance type:** t2.micro
- Availability Zone:** us-east-1b
- Private DNS:** ip-10-100-1-216.ec2.internal
- Private IPs:** 10.100.1.216 (highlighted with a red box and an arrow)
- Secondary private IPs:** VPC ID vpc-0df4e6d3766e1e51f (MyVPC) (highlighted with a red box)
- Subnet ID:** subnet-0ab00ecc35cca6298 (MyVPC-Private)
- Public DNS (IPv4):** -
- IPv4 Public IP:** - (highlighted with a red box)
- IPv6 IPs:** -
- Elastic IPs:** -
- Availability zone:** us-east-1b
- Security groups:** MyVPC-Private-SG. view inbound rules. view outbound rules
- Scheduled events:** No scheduled events
- AMI ID:** amzn2-ami-hvm-2.0.20200617.0-x86_64-gp2 (ami-08f3d892de259504d)
- Platform details:** Linux/UNIX

Try to ping EC2-B private IP from EC2-A instance

```
[ec2-user@ip-10-100-0-139 ~]$ ping -c 5 10.100.1.216
PING 10.100.1.216 (10.100.1.216) 56(84) bytes of data.
64 bytes from 10.100.1.216: icmp_seq=1 ttl=255 time=1.22 ms
64 bytes from 10.100.1.216: icmp_seq=2 ttl=255 time=0.868 ms
64 bytes from 10.100.1.216: icmp_seq=3 ttl=255 time=0.701 ms
64 bytes from 10.100.1.216: icmp_seq=4 ttl=255 time=0.725 ms
64 bytes from 10.100.1.216: icmp_seq=5 ttl=255 time=0.739 ms

--- 10.100.1.216 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4073ms
rtt min/avg/max/mdev = 0.701/0.850/1.221/0.197 ms
```

Create a NAT gateway in your VPC

VPC -> NAT Gateways -> Create NAT Gateway

[NAT Gateways](#) > Create NAT Gateway

Create NAT Gateway

Create a NAT gateway and assign it an Elastic IP address. [Learn more.](#)

Subnet* subnet-0ab00ecc35cca6298

choose MyVPC-Public

Elastic IP Allocation ID* eipalloc-03f97d7aeef7e65bf

Allocate Elastic IP address

Elastic IP address (34.194.248.98) allocated.

Key (128 characters maximum)

Value (256 characters maximum)

Name

MyVPC-Private-NATGW

Add Tag

49 remaining (Up to 50 tags maximum)

* Required

Cancel

Create a NAT Gateway

Add a route in Private subnet for internet traffic and route through NAT Gateway

Route Tables -> Select MyVPC-Private route table

Routes -> Edit -> Add another route

Destination: 0.0.0.0/0

Target: nat-gateway

Save

Create route table

Actions

Name: MyVPC-Private-RT

Name	Route Table ID	Explicit subnet association	Edge associations	Main	VPC ID
MyVPC-Private-RT	rtb-0aec07a9b768ad4b2	subnet-0ab00ecc35cca6298	-	No	vpc-0df4e6d3766e1e51

Route Table: rtb-0aec07a9b768ad4b2

Summary

Routes

Subnet Associations

Edge Associations

Route Propagation

Tags

Edit routes

View All routes

Destination	Target	Status	Propagated
10.100.0.0/16	local	active	No

Route Tables > Edit routes

Edit routes

Destination Target Status Propagated

10.100.0.0/16	local	active	No
0.0.0.0/0	nat-		No

Add route

* Required

Cancel Save routes

Create route table Actions

Name: MyVPC-Private-RT Add filter

Name	Route Table ID	Explicit subnet association	Edge associations	Main	VPC ID
MyVPC-Private-RT	rtb-0aec07a9b768ad4b2	subnet-0ab00ecc35cca6298	-	No	vpc-0df4e6d3766e1e51

Route Table: rtb-0aec07a9b768ad4b2

Summary Routes Subnet Associations Edge Associations Route Propagation Tags

Edit routes

View All routes

Destination	Target	Status	Propagated
10.100.0.0/16	local	active	No
0.0.0.0/0	nat-0926aae31403a48e5	active	No

Try to connect to EC2-B instance from EC2-A

```
[ec2-user@ip-10-100-0-139 ~]$ touch rnieva-keypair.pem
[ec2-user@ip-10-100-0-139 ~]$ vi rnieva-keypair.pem
[ec2-user@ip-10-100-0-139 ~]$ chmod 600 rnieva-keypair.pem
[ec2-user@ip-10-100-0-139 ~]$ ssh -i rnieva-keypair.pem ec2-user@10.100.1.216
The authenticity of host '10.100.1.216 (10.100.1.216)' can't be established.
ECDSA key fingerprint is SHA256:200tS7bQDvWk06Gr0mhornCZepZVwUMj0xFFTharR7U.
ECDSA key fingerprint is MD5:1c:2d:3f:43:40:ec:f1:4d:67:22:8b:31:3b:b0:04:d7.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.100.1.216' (ECDSA) to the list of known hosts.
```

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

<https://aws.amazon.com/amazon-linux-2/>

```
[ec2-user@ip-10-100-1-216 ~]$ uptime
21:40:06 up 19 min, 1 user, load average: 0.00, 0.00, 0.00
```

Try to ping google.com from MyEC2-B

```
[ec2-user@ip-10-100-1-216 ~]$ ping -c 3 google.com
PING google.com (172.217.8.14) 56(84) bytes of data.
64 bytes from iad23s59-in-f14.1e100.net (172.217.8.14): icmp_seq=1 ttl=113
time=2.43 ms
64 bytes from iad23s59-in-f14.1e100.net (172.217.8.14): icmp_seq=2 ttl=113
time=1.89 ms
64 bytes from iad23s59-in-f14.1e100.net (172.217.8.14): icmp_seq=3 ttl=113
time=1.85 ms

--- google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 1.852/2.061/2.437/0.268 ms
```