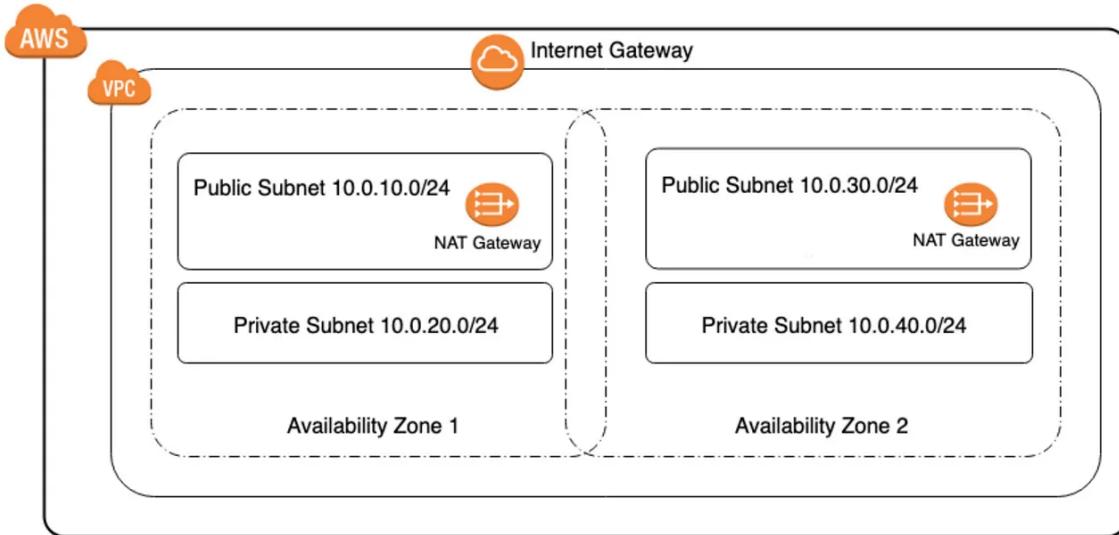


#4 Task: Create VPC, Public & Private Subnets.



What is a VPC and why is it important?

Amazon Virtual Private Cloud (Amazon VPC) enables you to launch AWS resources into a virtual network that you've defined. This virtual network closely resembles a traditional network that you'd operate in your own data center, with the benefits of using the scalable infrastructure of AWS.

Amazon VPC enables you to build a virtual network in the AWS cloud — no VPNs, hardware, or physical data centers required. You can define your own network space, and control how your network and the Amazon EC2 resources inside your network are exposed to the Internet.

What is the importance of having private and public subnets?

The instances in the public subnet can send outbound traffic directly to the internet, whereas the instances in the private subnet can't. Instead, the instances in the private subnet can access the internet by using a network address translation (NAT) gateway that resides in the public subnet.

Requirements:

- AWS Console → <https://aws.amazon.com/free/>
- Patience...

The Process:

- Follow the steps below. Use the same IPv4 CIDR block numbers. You can make the names of the VPC, subnets, route tables, IGW, NAT gateways unique to whatever you want.

1. Create VPC from VPC Dashboard from AWS Console.

VPC settings

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

levelup

IPv4 CIDR block [Info](#)

10.0.0.0/16

IPv6 CIDR block [Info](#)

No IPv6 CIDR block
 Amazon-provided IPv6 CIDR block
 IPv6 CIDR owned by me

Tenancy [Info](#)

Default

● Click on Create button which will create a VPC

<input checked="" type="checkbox"/>	levelup	vpc-04e2d18df72...	 Available	10.0.0.0/16	-
-------------------------------------	---------	--------------------	---	-------------	---

2. Create subnets now, we'll start with creating a public subnet now.

Create subnet Info

VPC

VPC ID

Create subnets in this VPC.

vpc-04e2d18df728f30d1 (levelup) ▾

Associated VPC CIDRs

IPv4 CIDRs

10.0.0.0/16

VPC ID is the vpc you created

Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name

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

leveluppubsub>

The name can be up to 256 characters long.

Availability Zone [Info](#)

Choose the zone in which your subnet will reside, or let Amazon choose one for you.

No preference



IPv4 CIDR block [Info](#)

10.0.1.0/24



► Tags - optional

[Remove](#)

Availability Zone I left as no preference for this particular project.



leveluppub

[subnet-00dff853d8d5...](#)

Available

[vpc-04e2d18df728f30...](#)

10.0.1.0/24

3. Let's create a private subnet now.

This can be created using Subnets options from left hand side list in VPC Dashboard. Same process as the public subnet, except we are using a different IPv4 CIDR block.

Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name

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

The name can be up to 256 characters long.

Availability Zone [Info](#)

Choose the zone in which your subnet will reside, or let Amazon choose one for you.



IPv4 CIDR block [Info](#)



► Tags - optional

- Click on create subnet button.



leveluppriv

subnet-0b0389431e6f...

Available

vpc-04e2d18df728f30...

10.0.2.0/24

What is an AWS CIDR block?

- When you create a VPC, you must specify a range of IPv4 addresses for the VPC in the form of a Classless Inter-Domain Routing (CIDR) block; for example, 10.0.0.0/16. This is the primary CIDR block for your VPC.

4. Modify Auto assign IP by right clicking on public subnet.

AWS Services ▾ Search for services, features, marketplace products, and docs [Option+S]

VPC > Subnets > subnet-00dff853d8d5802ef > Modify auto-assign IP settings

Modify auto-assign IP settings Info

Enable the auto-assign IP address setting to automatically request a public IPv4 or IPv6 address for a new network interface in this subnet.

Settings

Subnet ID
 subnet-00dff853d8d5802ef

Auto-assign IPv4 Info
 Enable auto-assign public IPv4 address

Auto-assign customer-owned IPv4 address Info
 Enable auto-assign customer-owned IPv4 address
Option disabled because no customer owned pools found.

Cancel **Save**

5. Create an Internet Gateway to use with our Public Subnet.

Internet gateway settings

Name tag

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

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



Value - optional



Remove

Add new tag

You can add 49 more tags.

Cancel

Create internet gateway

Yes, it's really as easy as just creating a tag.

Internet gateways (3) Info					C	Actions ▾	Create internet gateway
<input type="text"/> Filter internet gateways					<	1	>
<input type="checkbox"/>	Name	Internet gateway ID	State	VPC ID	Owner		
<input type="checkbox"/>	levelupIGW	igw-095c663837110bfe5	Attached	vpc-04e2d18df728f30d1 le...	493078487722		

6. Attach Internet Gateway to VPC.

- When you right click on internet gateway, it will show you Attach to VPC option as below.
- Select the VPC you created and click on attach.

VPC > Internet gateways > igw-095c663837110bfe5

igw-095c663837110bfe5 / levelupIGW

Actions ▾

Details		Info	
Internet gateway ID igw-095c663837110bfe5	State Attached	VPC ID vpc-04e2d18df728f30d1 levelup	Owner 493078487722

7. Create NAT Gateway.

- You can use a network address translation (NAT) gateway to enable instances in a private subnet to connect to the internet or other AWS services, but prevent the internet from initiating a connection with those instances.
- Important: In order to access internet to your private subnet, NAT Gateway must be added to Public Subnet only.

aws Services ▾ X

ⓘ Elastic IP address 54.153.0.243 (eipalloc-b2e29f86) allocated.

NAT gateway settings

Name - *optional*
Create a tag with a key of 'Name' and a value that you specify.

The name can be up to 256 characters long.

Subnet
Select a public subnet in which to create the NAT gateway.

Elastic IP allocation ID [Info](#)
Assign an Elastic IP address to the NAT gateway.

Allocate Elastic IP

click on allocate elastic IP to attach elastic IP allocation ID

VPC	>	NAT gateways	>	nat-0edd6441f8767349d	
nat-0edd6441f8767349d / levelupNAT					Delete
Details Info					
NAT gateway ID nat-0edd6441f8767349d	State Available	State message Info -	Elastic IP address 52.9.145.90		
Private IP address 10.0.1.78	Network interface ID eni-0d844b6367003ee5a	VPC vpc-04e2d18df728f30d1 / levelup	Subnet subnet-00dff853d8d5802ef / leveluppub		
Created 2021/05/08 22:15 GMT-7	Deleted -				

8. Create Route Tables.

- A route table contains a set of rules, called routes, that are used to determine where network traffic from your subnet or gateway is directed. To put it simply, a route table tells network packets which way they need to go to get to their destination.

[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 [i](#)

VPC* [C](#) [i](#)

vpc-1d2ed07b	
vpc-04e2d18df728f30d1	levelup

This resource currently has no tags

[Add Tag](#) 50 remaining (Up to 50 tags maximum)

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

public 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 Info

VPC* Cancel Info

Value (256 characters maximum)

Add Tag 50 remaining (Up to 50 tags maximum)

This resource currently has no tags

* Required
[Cancel](#)
[Create](#)

private route table

- Add Internet Gateway to Public Route Table. Click ADD routes and attach.

Route Table: rtb-03088dab4ca8c0f28

Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No
0.0.0.0/0	igw-095c663837110bfe5	active	No

public route table

- Add NAT gateway to Private Route Table. Click ADD routes and attach.

Route Table: rtb-0e6c4fa8c7cf87020

Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No
0.0.0.0/0	nat-0edd6441f8767349d	active	No

private route table

- Since we added NAT Gateway to public subnet, it will also have access to the internet.

9. Edit Subnet Association

- Repeat steps for both your public and private Route Tables.

- Click Edit Subnet Association button.

Route Table: rtb-03088dab4ca8c0f28

Subnet ID	IPv4 CIDR	IPv6 CIDR
subnet-00dff853d8d5802ef...	10.0.1.0/24	-

public route table

Route table rtb-03088dab4ca8c0f28 (levelupRT)

Associated subnets [subnet-00dff853d8d5802ef](#)

Subnet ID	IPv4 CIDR	IPv6 CIDR	Current Route Table
<input type="checkbox"/> subnet-0b0389431e6f755c0 leveluppriv	10.0.2.0/24	-	Main
<input checked="" type="checkbox"/> subnet-00dff853d8d5802ef leveluppub	10.0.1.0/24	-	rtb-03088dab4ca8c0f28

* Required

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

public route table

You do not have any subnet associations.

The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:

Subnet ID	IPv4 CIDR	IPv6 CIDR
subnet-0b0389431e6f755...	10.0.2.0/24	-

private route table

Route table rtb-0e6c4fa8c7cf87020 (levelupRTPrivate)

Associated subnets subnet-0b0389431e6f755c0

Subnet ID	IPv4 CIDR	IPv6 CIDR	Current Route Table
subnet-0b0389431e6f755c0 leveluppriv	10.0.2.0/24	-	rtb-0e6c4fa8c7cf87020
subnet-00dff853d8d5802ef leveluppub	10.0.1.0/24	-	rtb-03088dab4ca8c0f28

* Required Cancel Save

private route table

10. Create public and private EC2 instances.

- Follow process for both public and private instances.
- Pay attention to steps for what is particular to a certain instance.
- First step, choose an AMI.

Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-04468e03c37242e1e (64-bit x86) / ami-03d381434ef0c36bf (64-bit Arm)

Select

Amazon Linux Free tier eligible

Amazon Linux 2 comes with five years support. It provides Linux kernel 4.14 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibc 2.26, Binutils 2.29.1, and the latest software packages through extras. This AMI is the successor of the Amazon Linux AMI that is approaching end of life on December 31, 2020 and has been removed from this wizard.

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

64-bit (x86) 64-bit (Arm)

- Instance Type.

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

Step 2: Choose an Instance Type

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
<input type="checkbox"/>	t2	t2.nano	1	0.5	EBS only	-	Low to Moderate
<input checked="" type="checkbox"/>	t2	t2.micro <small>Free tier eligible</small>	1	1	EBS only	-	Low to Moderate
<input type="checkbox"/>	t2	t2.small	1	2	EBS only	-	Low to Moderate

- Public Configure Details

us-west-1.console.aws.amazon.com/ec2/v2/home?region=us-west-1#LaunchInstanceWizard:

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances	<input type="text" value="1"/>	Launch into Auto Scaling Group
Purchasing option	<input type="checkbox"/> Request Spot instances	
Network	vpc-04e2d18df728f30d1 levelup	<input type="button" value="Create new VPC"/>
Subnet	subnet-00dff853d8d5802ef leveluppub us-west-1c	<input type="button" value="Create new subnet"/> 249 IP Addresses available
Auto-assign Public IP	<input type="button" value="Use subnet setting (Enable)"/>	
Placement group	<input type="checkbox"/> Add instance to placement group	
Capacity Reservation	<input type="button" value="Open"/>	
Domain join directory	<input type="button" value="No directory"/>	
IAM role	<input type="button" value="None"/>	
Shutdown behavior	<input type="button" value="Stop"/>	

Buttons: Cancel Previous Review and Launch Next: Add Storage

public instance

- Private Configure Details

us-west-1.console.aws.amazon.com/ec2/v2/home?region=us-west-1#LaunchInstanceWizard:

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances	<input type="text" value="1"/>	Launch into Auto Scaling Group
Purchasing option	<input type="checkbox"/> Request Spot instances	
Network	vpc-04e2d18df728f30d1 levelup	<input type="button" value="Create new VPC"/>
Subnet	subnet-0b0389431e6f755c0 leveluppriv us-west-1c	<input type="button" value="Create new subnet"/> 250 IP Addresses available
Auto-assign Public IP	<input type="button" value="Use subnet setting (Disable)"/>	
Placement group	<input type="checkbox"/> Add instance to placement group	
Capacity Reservation	<input type="button" value="Open"/>	
Domain join directory	<input type="button" value="No directory"/>	
IAM role	<input type="button" value="None"/>	
Shutdown behavior	<input type="button" value="Stop"/>	

Buttons: Cancel Previous Review and Launch Next: Add Storage

configure instance details should be the same for both instance, except the public and private subnets.

- Copy and paste User Data from below into PUBLIC instance.

```
#!/bin/bash
yum install httpd -y
yum update -y
service httpd start
chkconfig httpd on
```

- Configure Security Group. Make sure to add HTTP port 80 to both public and private instances. SSH port 22 will already be there when created.

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: launch-wizard-15

Description: launch-wizard-15 created 2021-04-02T14:28:44.644+05:30

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	Custom 0.0.0.0/0	e.g. SSH for Admin Desktop
HTTP	TCP	80	Custom 0.0.0.0/0, ::/0	e.g. SSH for Admin Desktop

[Add Rule](#)

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

configure security group is the same for both public and private instances

Instances (2) Info		C	Connect	Instance state	Actions	Launch instances	▼	
		Filter instances						
	Name	Instance ID	Instance ...	Instanc...	Status check	Alarm st...	Availabilit...	Public IPv4
<input type="checkbox"/>	LevelUpPriv	i-0cf2ddf53b463f...	Running  	t2.micro	✓ 2/2 checks p: No ala... 	us-west-1c	-	
<input type="checkbox"/>	LevelUpPub	i-0db6f514930a6...	Running  	t2.micro	✓ 2/2 checks p: No ala... 	us-west-1c	-	

public and private instances should be running as so

- Create a keypair or using an existing keypair.

Select an existing key pair or create a new key pair X

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

levelupkeypair

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

[Cancel](#) [Launch Instances](#)

11. Testing the EC2 Instances.

Public Instance:

- right click on box next to name of instance and click connect

Connect to instance Info

Connect to your instance i-0db6f514930a6f7ba (LevelUpPub) using any of these options

EC2 Instance Connect

Session Manager

SSH client

Instance ID

[i-0db6f514930a6f7ba \(LevelUpPub\)](#)

1. Open an SSH client.
2. Locate your private key file. The key used to launch this instance is levelupkeypair.pem
3. Run this command, if necessary, to ensure your key is not publicly viewable.
 chmod 400 levelupkeypair.pem
4. Connect to your instance using its Public IP:
 13.57.26.125

Example:

ssh -i "levelupkeypair.pem" ec2-user@13.57.26.125

ssh steps to connecting to public instance

```
jerryc.quiles@Jerrys-MacBook-Pro ~/d/devops> chmod 400 levelupkeypair.pem
jerryc.quiles@Jerrys-MacBook-Pro ~/d/devops> ssh -i "levelupkeypair.pem" ec2-user@13.57.26.125
The authenticity of host '13.57.26.125 (13.57.26.125)' can't be established.
ECDSA key fingerprint is SHA256:2xIX63IFcwyXC62HpATCYhUim/du0vISzaGXo5PuP7E.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '13.57.26.125' (ECDSA) to the list of known hosts.
Last login: Sun May  9 06:44:18 2021 from c-73-241-240-172.hsd1.ca.comcast.net
```

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

```
https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-0-1-233 ~]$
```

terminal of successfully connecting public instance

This page is used to test the proper operation of the Apache HTTP server after it has been installed. If you can read this page, it means that the Apache HTTP server installed at this site is working properly.

If you are a member of the general public:

The fact that you are seeing this page indicates that the website you just visited is either experiencing problems, or is undergoing routine maintenance.

If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster" and directed to the website's domain should reach the appropriate person.

For example, if you experienced problems while visiting www.example.com, you should send e-mail to "webmaster@example.com".

If you are the website administrator:

You may now add content to the directory `/var/www/html/`. Note that until you do so, people visiting your website will see this page, and not your content. To prevent this page from ever being used, follow the instructions in the file `/etc/httpd/conf.d/welcome.conf`.

You are free to use the image below on web sites powered by the Apache HTTP Server:

Powered by  2.4

apache test page from our public instance IP address

Private Instance:

- We'll now connect to our private instance through our public instance.
- Inside your public instance create a file for your keypair.
- Create a file for your keypair.

yum install vim

vim keypair.pem

:wq

- Copy and paste contents of keypair inside your newly created keypair.pem file, your keypair file will look like the following below.



chmod 600 keypair.pem

ssh -i keypair.pem ec2-user@private-ip-address

```
[ec2-user@ip-10-0-1-233 ~]$ vim levelupkeypair.pem
[ec2-user@ip-10-0-1-233 ~]$ chmod 600 levelupkeypair.pem
[ec2-user@ip-10-0-1-233 ~]$ ssh -i levelupkeypair.pem ec2-user@10.0.2.165
Last login: Sun May  9 06:52:49 2021 from 10.0.1.233
```

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

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

```
[ec2-user@ip-10-0-2-165 ~]$ █
```

12. Conclusion.

- In conclusion, the machines on a private subnet can access the Internet because the default route on a private subnet is not the VPC “Internet Gateway” object — it is an EC2 instance configured as a NAT instance. A NAT instance is an instance on a public subnet with a public IP, and specific configuration.