

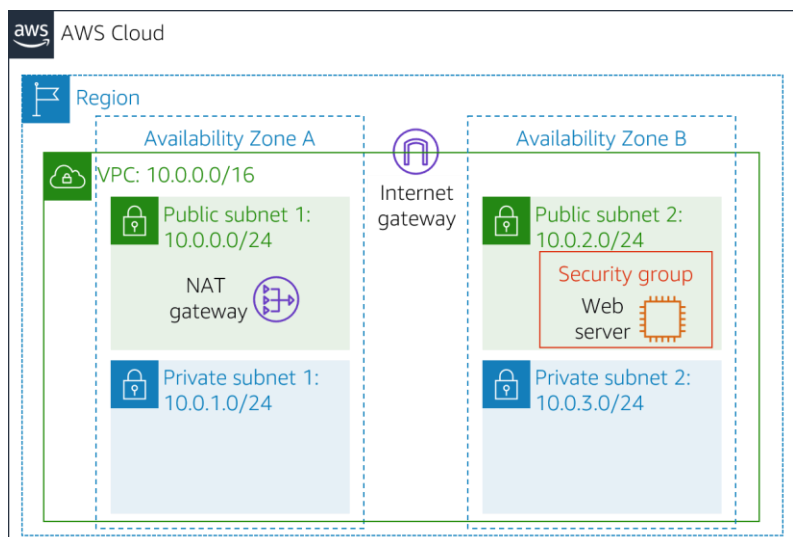
Build your VPC and Launch a Web Server

In this project, you will use Amazon Virtual Private Cloud (VPC) to create your own VPC and add additional components to produce a customized network. You will also create security groups for your EC2 instance. You will then configure and customize an EC2 instance to run a web server and launch it into the VPC.

Amazon Virtual Private Cloud (Amazon VPC) enables you to launch Amazon Web Services (AWS) resources into a virtual network that you defined. This virtual network closely resembles a traditional network that you would operate in your own data center, with the benefits of using the scalable infrastructure of AWS. You can create a VPC that spans multiple Availability Zones.

NOTE THIS PROJECT IS BEING WORK IN THE NEW AWS MANAGEMENT CONSOLE

In this project you build the following infrastructure:



Public Route Table

Destination	Target
10.0.0.0/16	Local
0.0.0.0/0	Internet gateway

Private Route Table

Destination	Target
10.0.0.0/16	Local
0.0.0.0/0	NAT gateway

Project Objectives

- Create a VPC.
- Create subnets.
- Configure a security group.
- Launch an EC2 instance into a VPC.

STEP 1: Create Your VPC

In this step, you will use the VPC Wizard to create a VPC an Internet Gateway and two subnets in a single Availability Zone. An **Internet gateway (IGW)** is a VPC component that allows communication between instances in your VPC and the Internet.

After creating a VPC, you can add **subnets**. Each subnet resides entirely within one Availability Zone and cannot span zones. If a subnet's traffic is routed to an Internet Gateway, the subnet is known as a *public subnet*. If a subnet does not have a route to the Internet gateway, the subnet is known as a *private subnet*.

The wizard will also create a *NAT Gateway*, which is used to provide internet connectivity to EC2 instances in the private subnets.

- ✚ In the **AWS Management Console**, on the **Services** menu, choose **VPC**.
- ✚ Choose **Launch VPC Wizard**
- ✚ In the left navigation pane, choose **VPC with Public and Private Subnets** (the second option).

The screenshot shows the AWS Management Console VPC Dashboard. The left sidebar contains the navigation menu with 'VPC with Public and Private Subnets' selected. The main content area features the 'Launch VPC Wizard' button and a 'Resources by Region' section listing various VPC resources. The right sidebar displays 'Service Health' and 'Settings'.



- ✚ Choose **Select** then configure:


The screenshot shows the 'Step 1: Select a VPC Configuration' wizard. It displays four configuration options, with 'VPC with Public and Private Subnets' selected. A diagram on the right illustrates the network architecture, showing a public subnet, private subnet, and NAT gateway. The 'Select' button is visible at the bottom right.

- ✚ **VPC name:** Lab VPC
- ✚ **Availability Zone:** Select the *first* Availability Zone
- ✚ **Public subnet name:** Public Subnet 1
- ✚ **Availability Zone:** Select the *first* Availability Zone (the same as used above)
- ✚ **Private subnet name:** Private Subnet 1
- ✚ **Elastic IP Allocation ID:** Choose in the box and select the displayed IP address
- ✚ Choose **Create VPC**

Step 2: VPC with Public and Private Subnets

IPv4 CIDR block:	<input type="text" value="10.0.0.0/16"/>	(65531 IP addresses available)
IPv6 CIDR block:	<input checked="" type="radio"/> No IPv6 CIDR Block <input type="radio"/> Amazon provided IPv6 CIDR block <input type="radio"/> IPv6 CIDR block owned by me	
VPC name:	<input type="text" value="Lab VPC"/>	
Public subnet's IPv4 CIDR:	<input type="text" value="10.0.0.0/24"/>	(251 IP addresses available)
Availability Zone:	<input type="text" value="No Preference"/>	
Public subnet name:	<input type="text" value="Public Subnet 1"/>	
Private subnet's IPv4 CIDR:	<input type="text" value="10.0.1.0/24"/>	(251 IP addresses available)
Availability Zone:	<input type="text" value="us-east-1a"/>	
Private subnet name:	<input type="text" value="Private Subnet 1"/>	
You can add more subnets after Amazon Web Services creates the VPC.		
Specify the details of your NAT gateway (NAT gateway rates apply).		
Elastic IP Allocation ID:	<input type="text" value="eipalloc-08186ac0e7e20f64d"/>	
Service endpoints		
<input type="button" value="Add Endpoint"/>		
Enable DNS hostnames:	<input checked="" type="radio"/> Yes <input type="radio"/> No	
Hardware tenancy:	<input type="text" value="Default"/>	
<input type="button" value="Cancel and Exit"/> <input type="button" value="Back"/> <input type="button" value="Create VPC"/>		

 The wizard will create your VPC.
 Once it is complete, choose **OK**

 New VPC Experience
[Learn more](#)

VPC Dashboard
[EC2 Global View](#) New

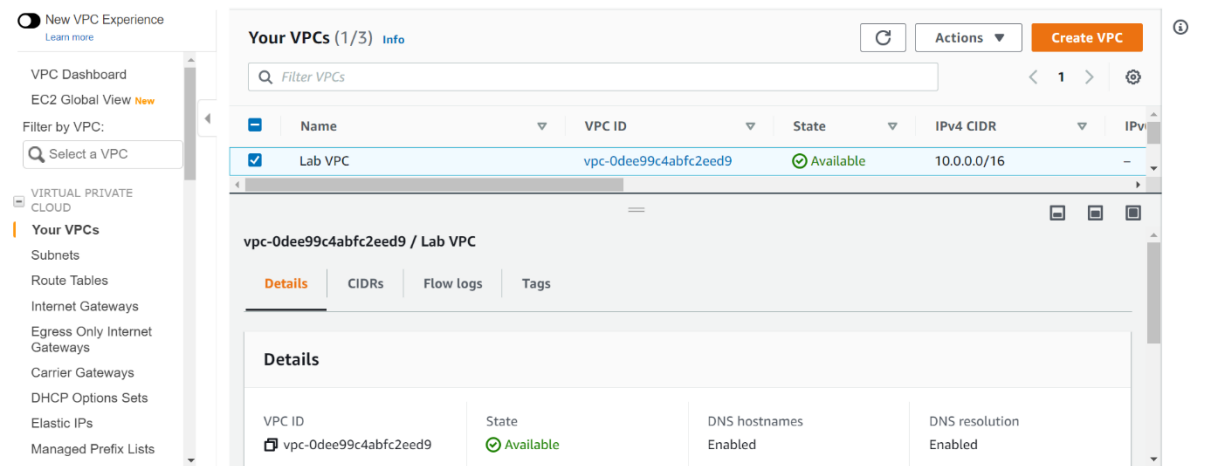
Filter by VPC:

VIRTUAL PRIVATE CLOUD
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
Carrier Gateways
DHCP Options Sets
Elastic IPs
Managed Prefix Lists

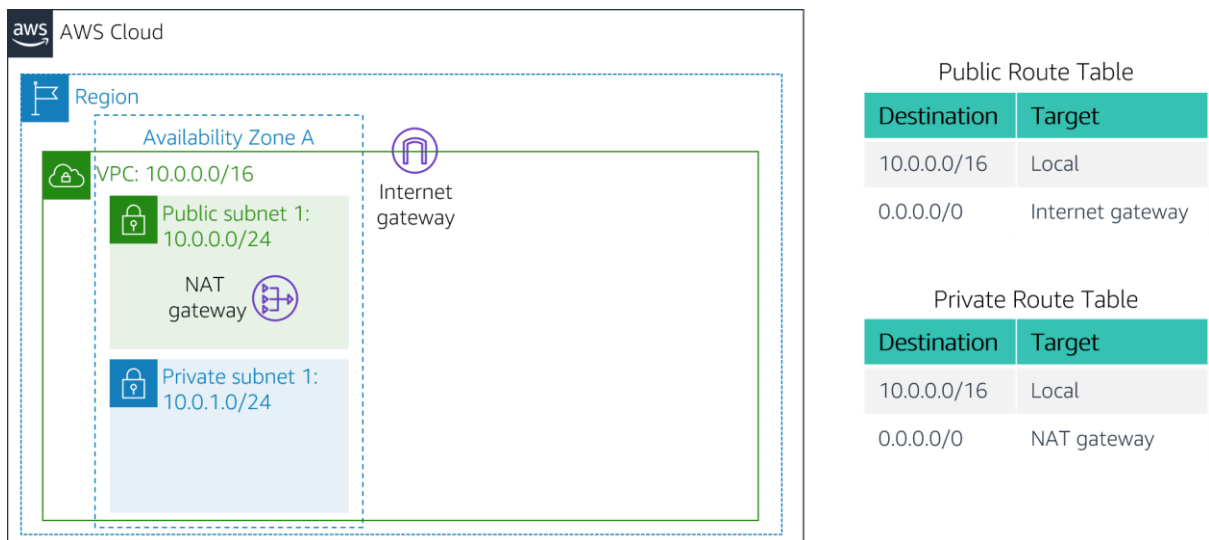
VPC Successfully Created

Your VPC has been successfully created.

You can launch instances into the subnets of your VPC. For more information, see [Launching an Instance into Your Subnet](#).



The wizard has provisioned a VPC with a public subnet and a private subnet in the same Availability Zone, together with route tables for each subnet:



The Public Subnet has a CIDR of **10.0.0.0/24**, which means that it contains all IP addresses starting with **10.0.0.x**.

The Private Subnet has a CIDR of **10.0.1.0/24**, which means that it contains all IP addresses starting with **10.0.1.x**.

STEP 2: Create Additional Subnets

In this task, you will create two additional subnets in a second Availability Zone. This is useful for creating resources in multiple Availability Zones to provide *High Availability*.

In the left navigation pane, choose Subnets.

First, you will create a second Public Subnet.

- Choose **Create subnet** then configure:
- VPC ID:** `Lab VPC`

- **Subnet name:** Public Subnet 2
 - **Availability Zone:** Select the *second* Availability Zone
 - **IPv4 CIDR block:** 10.0.2.0/24
- The subnet will have all IP addresses starting with **10.0.2.x**.
- Choose **Create subnet**

VPC > Subnets > Create subnet

Create subnet [Info](#)

VPC

VPC ID
Create subnets in this VPC.

vpc-0e7795963420d0b33 (Lab VPC)

Associated VPC CIDRs

IPv4 CIDRs

10.0.0.0/16

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.

Public Subnet 2

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.

US East (N. Virginia) / us-east-1b

IPv4 CIDR block [Info](#)

10.0.2.0/24

▼ **Tags - optional**

Key	Value - optional	
Name	Public Subnet 2	Remove

[Add new tag](#)

You can add 49 more tags.

[Remove](#)

[Add new subnet](#)

Cancel [Create subnet](#)

You will now create a second Private Subnet.

Choose **Create subnet** then configure:

- 🚩 **VPC ID:** Lab VPC
- 🚩 **Subnet name:** Private Subnet 2
- 🚩 **Availability Zone:** Select the *second* Availability Zone
- 🚩 **CIDR block:** 10.0.3.0/24
- 🚩 The subnet will have all IP addresses starting with **10.0.3.x**.
- 🚩 Choose **Create subnet**

VPC > Subnets > Create subnet

Create subnet [Info](#)

VPC

VPC ID

Create subnets in this VPC.

vpc-0e7795963420d0b33 (Lab VPC)

Associated VPC CIDRs

IPv4 CIDRs

10.0.0.0/16

Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

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.

Private Subnet 2

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.

US East (N. Virginia) / us-east-1b

IPv4 CIDR block [Info](#)

10.0.3.0/24

Tags - optional

Key

Value - optional

US East (N. Virginia) / us-east-1b

IPv4 CIDR block [Info](#)

10.0.3.0/24

Tags - optional

Key

Value - optional

Q Name X Q Private Subnet 2 X Remove

Add new tag

You can add 49 more tags.

Remove

Add new subnet

Cancel

Create subnet

You will now configure the Private Subnets to route internet-bound traffic to the NAT Gateway so that resources in the Private Subnet are able to connect to the Internet, while still keeping the resources private. This is done by configuring a *Route Table*.

A *route table* contains a set of rules, called *routes*, that are used to determine where network traffic is directed. Each subnet in a VPC must be associated with a route table; the route table controls routing for the subnet.

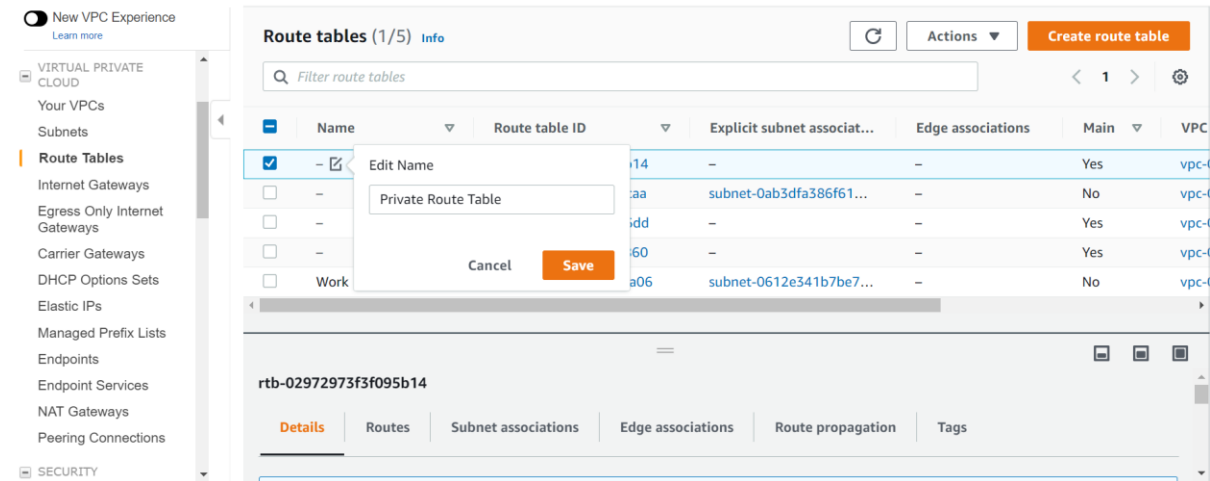
In the left navigation pane, choose **Route Tables**.

	Name	Route table ID	Explicit subnet associat...	Edge associations	Main	VPC
<input type="checkbox"/>	-	rtb-02972973f3f095b14	-	-	Yes	vpc-
<input type="checkbox"/>	-	rtb-077693b43aaec9caa	subnet-0ab3dfa386f61...	-	No	vpc-
<input type="checkbox"/>	-	rtb-0426fab76ee1166dd	-	-	Yes	vpc-
<input type="checkbox"/>	-	rtb-0be313534efc15860	-	-	Yes	vpc-
<input type="checkbox"/>	Work Public Route ...	rtb-0de21339684584a06	subnet-0612e341b7be7...	-	No	vpc-

Select the route table with **Main = Yes** and **VPC = Lab VPC**. (Expand the *VPC ID* column if necessary to view the VPC name.)

ID	Explicit subnet associat...	Edge associations	Main	VPC	Ow...
3f3f095b14	-	-	Yes	vpc-0e7795963420d0b33 Lab VPC	32739..
43aaec9caa	subnet-0ab3dfa386f61...	-	No	vpc-0e7795963420d0b33 Lab VPC	32739..
'6ee1166dd	-	-	Yes	vpc-0ee6f867204ab0bf2	32739..
34efc15860	-	-	Yes	vpc-0f77a7d47cfeacedc Work VPC	32739..
9684584a06	subnet-0612e341b7be7...	-	No	vpc-0f77a7d47cfeacedc Work VPC	32739..







In the **Name** column for this route table, choose the pencil then type **Private Route Table** and choose **Save**



In the lower pane, choose the **Routes** tab.

Note: This means that traffic destined for the internet (0.0.0.0/0) will be sent to the NAT Gateway. The NAT Gateway will then forward the traffic to the internet.

This route table is therefore being used to route traffic from Private Subnets. You will now add a name to the Route Table to make this easier to recognize in future.

-  In the lower pane, choose the **Subnet Associations** tab.
-  You will now associate this route table to the Private Subnets.
-  Choose **Edit subnet associations**
-  Select both **Private Subnet 1** and **Private Subnet 2**.
-  You can expand the *Subnet ID* column to view the Subnet names.
-  Choose **Save associations**

The first screenshot shows the 'Route tables (1/5)' page with the 'Subnet associations' tab selected. It displays 'Explicit subnet associations (0)' and a message: 'No subnet associations. You do not have any subnet associations.'

The second screenshot shows the 'Subnets without explicit associations (3)' section. It lists three subnets:

Subnet ID	IPv4 CIDR	IPv6 CIDR
subnet-0902562f3c88d90ec / Private Subnet 1	10.0.1.0/24	-
subnet-05801abae12849b64 / Private Subnet 2	10.0.3.0/24	-

The third screenshot shows a list of route tables:

Name	Route table ID	Explicit subnet associat...	Edge associations	Main	VPC
Private Route Table	rtb-02972973f3f095b14	2 subnets	-	Yes	vpc-4
-	rtb-077693b43aaec9caa	subnet-0ab3dfa386f61...	-	No	vpc-4
-	rtb-0426fab76ee1166dd	-	-	Yes	vpc-4
-	rtb-0be313534efc15860	-	-	Yes	vpc-4
Work Public Route ...	rtb-0de21339684584a06	subnet-0612e341b7be7...	-	No	vpc-4

At the bottom of the third screenshot, there is a 'Select a route table' button.

You will now configure the Route Table that is used by the Public Subnets.

- Select the route table with **Main = No** and **VPC = Lab VPC** (and deselect any other subnets).
- In the **Name** column for this route table, choose the pencil then type **Public Route Table**, and choose **Save**
- In the lower pane, choose the **Routes** tab.
- You will now associate this route table to the Public Subnets.

	Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
<input type="checkbox"/>	Private Subnet 1	subnet-0902562f3c88d90ec	10.0.1.0/24	-	rtb-02972973f3f095b14 / Private Route Table
<input checked="" type="checkbox"/>	Public Subnet 1	subnet-0ab3dfa386f613aba	10.0.0.0/24	-	rtb-077693b43aaec9caa
<input type="checkbox"/>	Private Subnet 2	subnet-05801abae12849b64	10.0.3.0/24	-	rtb-02972973f3f095b14 / Private Route Table
<input checked="" type="checkbox"/>	Public Subnet 2	subnet-0cf7b81c1f5dd9747	10.0.2.0/24	-	Main (rtb-02972973f3f095b14 / Private Route Table)

Selected subnets

subnet-0cf7b81c1f5dd9747 / Public Subnet 2

subnet-0ab3dfa386f613aba / Public Subnet 1

Cancel

Save associations

New VPC Experience

Learn more

VIRTUAL PRIVATE CLOUD

Your VPCs

Subnets

Route Tables

Internet Gateways

Egress Only Internet Gateways

Carrier Gateways

DHCP Options Sets

Elastic IPs

Managed Prefix Lists

Endpoints

Endpoint Services

NAT Gateways

Peering Connections

SECURITY

You have successfully updated subnet associations for rtb-077693b43aaec9caa.

Route tables (1/5)

Info

Filter route tables

Create route table

	Name	Route table ID	Explicit subnet associat...	Edge associations	Main	VPC
<input type="checkbox"/>	Private Route Table	rtb-02972973f3f095b14	2 subnets	-	Yes	vpc-
<input checked="" type="checkbox"/>	Public Route Table	rtb-077693b43aaec9caa	2 subnets	-	No	vpc-
<input type="checkbox"/>	-	rtb-02972973f3f095b14	-	-	Yes	vpc-
<input type="checkbox"/>	-	rtb-02972973f3f095b14	-	-	Yes	vpc-
<input type="checkbox"/>	Work	rtb-02972973f3f095b14	subnet-0612e341b7be7...	-	No	vpc-

Edit Name

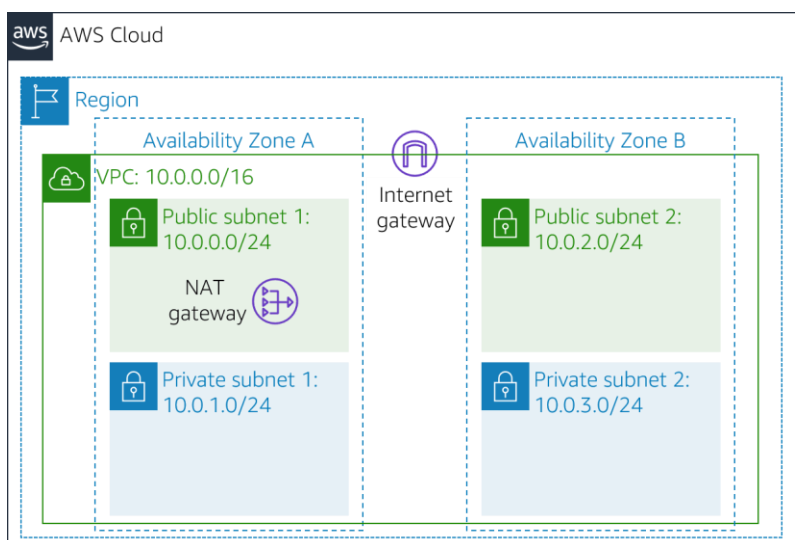
Public Route Table

Cancel

Save

rtb-077693b43aaec9caa

Your VPC now has public and private subnets configured in two Availability Zones:



Public Route Table

Destination	Target
10.0.0.0/16	Local
0.0.0.0/0	Internet gateway

Private Route Table

Destination	Target
10.0.0.0/16	Local
0.0.0.0/0	NAT gateway

STEP 3: Create a VPC Security Group

In this task, you will create a VPC security group, which acts as a virtual firewall. When you launch an instance, you associate one or more security groups with the instance. You can add rules to each security group that allow traffic to or from its associated instances.

In the left navigation pane, choose **Security Groups**.

- Choose **Create security group** and then configure:
- Security group name:** Web Security Group
- Description:** Enable HTTP access
- VPC:** Lab VPC
- In the **Inbound rules** pane, choose **Add rule**
- Configure the following settings:
- Type:** HTTP
- Source:** Anywhere-IPv4
- Description:** Permit web requests
- Scroll to the bottom of the page and choose **Create security group**

The screenshot displays the AWS Management Console interface. On the left, the navigation pane shows the 'Security Groups' link under the 'SECURITY' section. The main content area shows the 'Security Groups (4)' page with a table of existing groups. Below this, the 'Create security group' form is visible, showing the 'Basic details' section with fields for 'Security group name' (Web Security Group), 'Description' (Enable HTTP access), and 'VPC' (vpc-0e7795963420d0b33).

	Name	Security group ID	Security group name	VPC ID	Description
<input type="checkbox"/>	-	sg-022d4e40635943c4c	default	vpc-0e7795963420d0b33	default VPC security group
<input type="checkbox"/>	-	sg-02adb96c988811729	default	vpc-0ee6f867204ab0bf2	default VPC security group
<input type="checkbox"/>	-	sg-05e52c92b46e1f6a6	Ec2SecurityGroup	vpc-0f77a7d47cfeacedc	VPC Security Group
<input type="checkbox"/>	-	sg-0859986d372376451	default	vpc-0f77a7d47cfeacedc	default VPC security group

Create security group

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name [Info](#)
Web Security Group
Name cannot be edited after creation.

Description [Info](#)
Enable HTTP access

VPC [Info](#)
vpc-0e7795963420d0b33

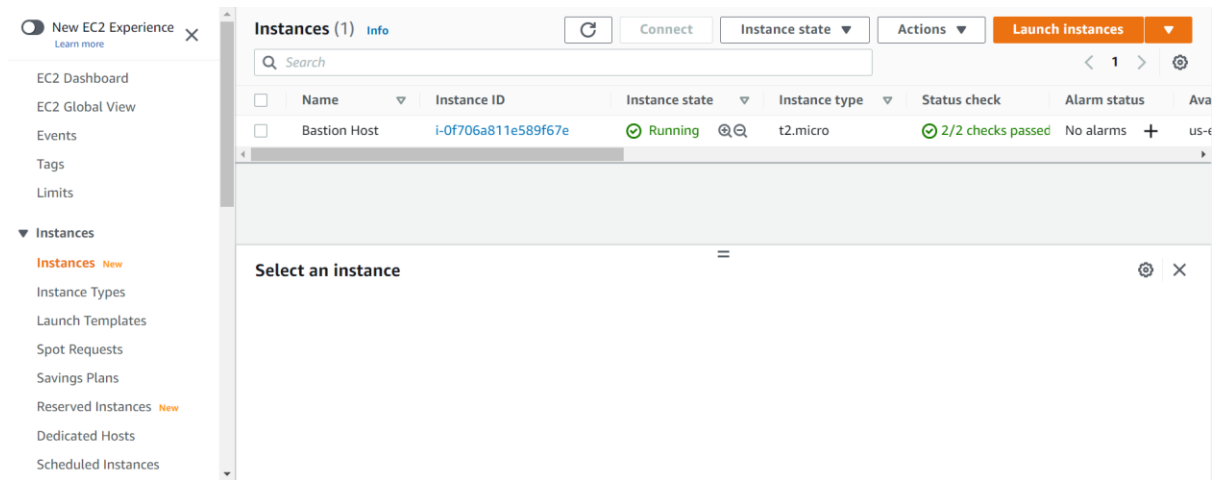
The screenshot displays the AWS Security Groups console interface. It features two main sections: 'Inbound rules' and 'Outbound rules'. The 'Inbound rules' section has a table with columns: Type, Protocol, Port range, Source, and Description - optional. A rule is configured with Type 'HTTP', Protocol 'TCP', Port range '80', Source 'Anywh...' (with a search icon and a text input '0.0.0.0/0'), and Description 'Permit web requests'. An 'Add rule' button is at the bottom left, and a 'Delete' button is at the bottom right. The 'Outbound rules' section has a similar table with columns: Type, Protocol, Port range, Destination, and Description - optional. A rule is configured with Type 'All traffic', Protocol 'All', Port range 'All', Destination 'Custom' (with a search icon and a text input '0.0.0.0/0'), and Description is empty. An 'Add rule' button is at the bottom left, and a 'Delete' button is at the bottom right. Below these sections is a 'Tags - optional' section with a description of tags and an 'Add new tag' button. At the bottom right, there are 'Cancel' and 'Create security group' buttons.

You will use this security group in the next task when launching an Amazon EC2 instance.

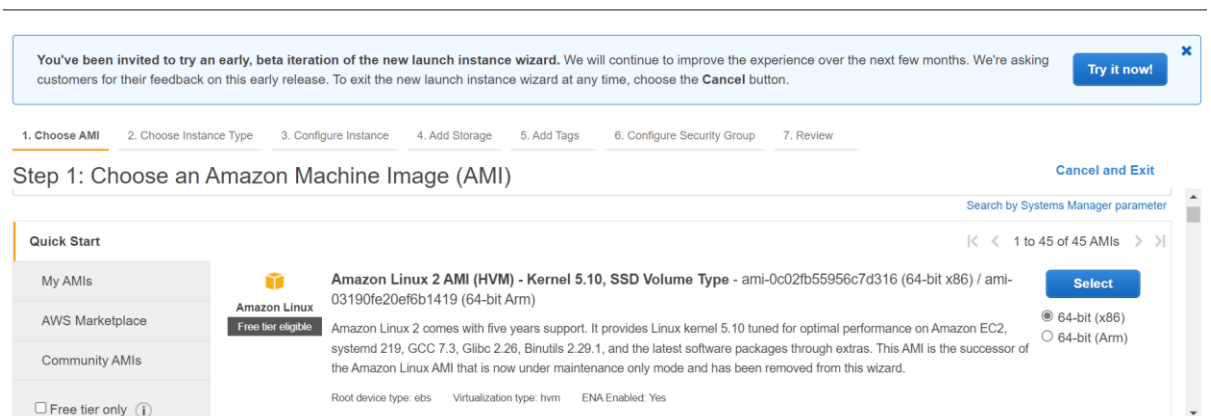
STEP 4: Launch a Web Server Instance

In this task, you will launch an Amazon EC2 instance into the new VPC. You will configure the instance to act as a web server.

- 🔗 On the **Services** menu, choose **EC2**.
- 🔗 Choose **Launch Instance**, and then choose **Launch Instance**

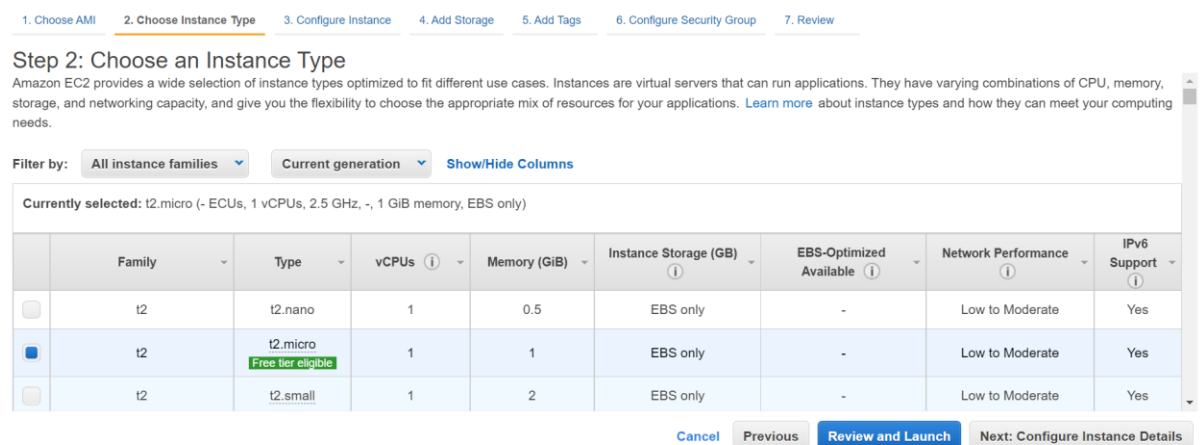


- First, you will select an *Amazon Machine Image (AMI)*, which contains the desired Operating System.
- In the row for **Amazon Linux 2** (at the top), choose **Select**



The *Instance Type* defines the hardware resources assigned to the instance.




- Select **t2.micro** (shown in the *Type* column).

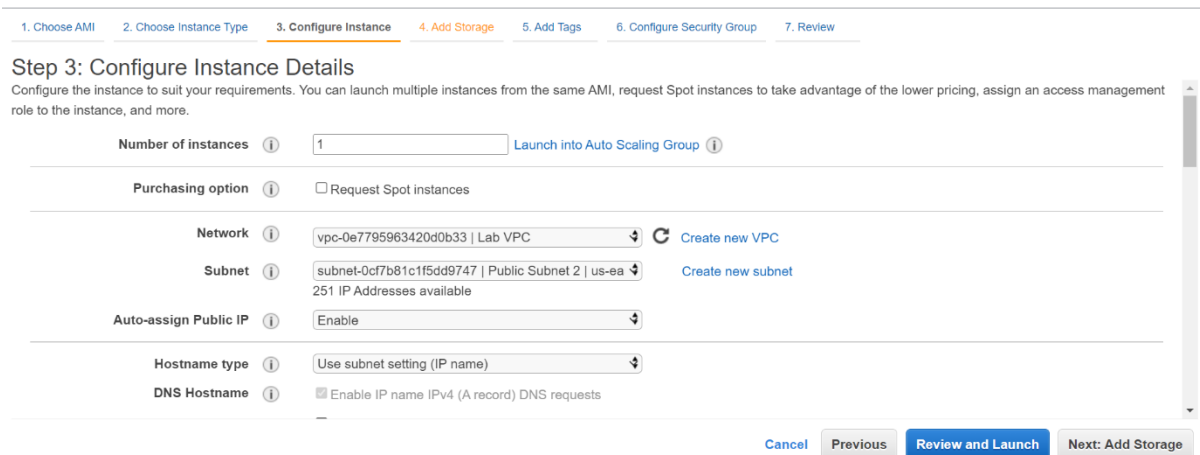


 Choose **Next: Configure Instance Details**

You will now configure the instance to launch in a Public Subnet of the new VPC.

Configure these settings:

-  **Network:** *Lab VPC*
-  **Subnet:** *Public Subnet 2 (not Private!)*
-  **Auto-assign Public IP:** *Enable*



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

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 [Launch into Auto Scaling Group](#)

Purchasing option ☐ Request Spot instances

Network [Create new VPC](#)


Subnet [Create new subnet](#)

Auto-assign Public IP

Hostname type

DNS Hostname ☒ Enable IP name (A record) DNS requests

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

-  Expand the **Advanced Details** section (at the bottom of the page).
-  Copy and paste this code into the **User data** box:

```
#!/bin/bash
# Install Apache Web Server and PHP
yum install -y httpd mysql php
# Download Lab files
wget https://aws-tc-largeobjects.s3.us-west-2.amazonaws.com/CUR-TF-100-ACCLFO-2/2-lab2-vpc/s3/lab-app.zip
unzip lab-app.zip -d /var/www/html/
# Turn on web server
chkconfig httpd on
service httpd start
```

This script will be run automatically when the instance launches for the first time. The script loads and configures a PHP web application.

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

▼ Advanced Details

Enclave	<input type="checkbox"/> Enable
Metadata accessible	Enabled
Metadata version	V1 and V2 (token optional)
Metadata token response hop limit	1
Allow tags in metadata	Disabled
User data	<input checked="" type="radio"/> As text <input type="radio"/> As file <input type="checkbox"/> Input is already base64 encoded

```
wget https://aws-tc-largeobjects.s3.us-west-2.amazonaws.com/CUR-TF-100-ACCLFO-2/2-lab2-vpc/s3/lab-app.zip
unzip lab-app.zip -d /var/www/html/
# Turn on web server
chkconfig httpd on
service httpd start
```

Cancel Previous Review and Launch Next: Add Storage

Choose **Next: Add Storage**

You will use the default settings for storage.

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

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more](#) about storage options in Amazon EC2.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encryption
Root	/dev/xvda	snap-0c1ac78aecd1c4204c	8	General Purpose SSD (gp2)	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypt

Add New Volume

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. [Learn more](#) about free usage tier eligibility and usage restrictions.

Cancel Previous Review and Launch Next: Add Tags

Choose **Next: Add Tags**

Tags can be used to identify resources. You will use a tag to assign a Name to the instance.

Choose **Add Tag** then configure:

Key: Name

Value: Web Server 1

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	Value	Instances	Volumes	Network Interfaces
Name	Web Server 1	<input checked="" type="checkbox"/>	<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](#)

Choose **Next: Configure Security Group**

You will configure the instance to use the *Web Security Group* that you created earlier.

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 ID	Name	Description	Actions
<input type="checkbox"/> sg-022d4e40635943c4c	default	default VPC security group	Copy to new
<input checked="" type="checkbox"/> sg-08dcd4f5198c835be	Web Security Group	Enable HTTP access	Copy to new

Inbound rules for sg-08dcd4f5198c835be (Selected security groups: sg-08dcd4f5198c835be)

Type	Protocol	Port Range	Source	Description
HTTP	TCP	80	0.0.0.0/0	Permit web request...

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

Select **an existing security group**
Select **Web Security Group**

This is the security group you created in the previous task. It will permit HTTP access to the instance.

Choose **Review and Launch**
When prompted with a *warning* that you will not be able to connect to the instance through port 22, choose **Continue**

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.

Warning

You will not be able to connect to this instance as the AMI requires port(s) 22 to be open in order to have access. Your current security group doesn't have port(s) 22 open.

Cancel Continue

Type	Protocol	Port Range	Source	Description
HTTP	TCP	80	0.0.0.0/0	Permit web request...

Cancel Previous Review and Launch

Review the instance information and choose **Launch**

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

Step 7: Review Instance Launch

Instance Type Edit instance type

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t2.micro	-	1	1	EBS only	-	Low to Moderate

Security Groups Edit security groups

Security Group ID	Name	Description
sg-08dcd4f5198c835be	Web Security Group	Enable HTTP access

All selected security groups inbound rules

Cancel Previous Launch

In the **Select an existing keypair** dialog, select **I acknowledge....**
Choose **Launch Instances** and then choose **View Instances**

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

Step 7: Review Instance Launch

Instance Type Edit instance type

Instance Type	ECUs
t2.micro	-

Security Groups Edit security groups

Security Group ID
sg-08dcd4f5198c835be

All selected security groups inbound

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. Amazon EC2 supports ED25519 and RSA key pair types.

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

vockey | RSA

☒ I acknowledge that I have access to the corresponding private key file, and that without this file, I won't be able to log into my instance.

Cancel Launch Instances

Cancel Previous Launch

Launch Status

How to connect to your instances

Your instances are launching, and it may take a few minutes until they are in the **running** state, when they will be ready for you to use. Usage hours on your new instances will start immediately and continue to accrue until you stop or terminate your instances.

Click **View Instances** to monitor your instances' status. Once your instances are in the **running** state, you can **connect** to them from the Instances screen. [Find out](#) how to connect to your instances.

Here are some helpful resources to get you started

- [How to connect to your Linux instance](#)
- [Amazon EC2: User Guide](#)
- [Learn about AWS Free Usage Tier](#)
- [Amazon EC2: Discussion Forum](#)

While your instances are launching you can also

- [Create status check alarms](#) to be notified when these instances fail status checks. (Additional charges may apply)
- [Create and attach additional EBS volumes](#) (Additional charges may apply)
- [Manage security groups](#)

[View Instances](#)

- ✚ Wait until **Web Server 1** shows *2/2 checks passed* in the **Status Checks** column.
- ✚ This may take a few minutes. Choose refresh in the top-right every 30 seconds for updates.
- ✚ You will now connect to the web server running on the EC2 instance.
- ✚ Select **Web Server 1**.
- ✚ Copy the **Public DNS (IPv4)** value shown in the **Description** tab at the bottom of the page.
- ✚ Open a new web browser tab, paste the **Public DNS** value and press Enter.

The screenshot shows the AWS Management Console interface for EC2 instances. On the left, there is a navigation menu with options like 'EC2 Dashboard', 'EC2 Global View', 'Events', 'Tags', 'Limits', and 'Instances'. The main area displays a table of instances. Two instances are listed: 'Bastion Host' and 'Web Server 1'. The 'Web Server 1' instance is selected, and its details are shown in the 'Details' tab. The instance is in the 'Running' state, and its status checks show '2/2 checks passed'. The public IPv4 address is 3.239.249.211, and the public IPv4 DNS is 10.0.2.161.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
Bastion Host	i-0f706a811e589f67e	Running	t2.micro	2/2 checks passed	No alarms	us-east-1
Web Server 1	i-02e2208bd66d629a6	Running	t2.micro	-	No alarms	us-east-1

Instance: i-02e2208bd66d629a6 (Web Server 1)

Details | Security | Networking | Storage | Status checks | Monitoring | Tags

Instance summary [Info](#)

Instance ID	Public IPv4 address	Private IPv4 addresses
i-02e2208bd66d629a6 (Web Server 1)	3.239.249.211 open address	10.0.2.161

IPv6 address | Instance state | Public IPv4 DNS

New EC2 Experience

EC2 Dashboard

EC2 Global View

Events

Tags

Limits

Instances

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Scheduled Instances

Instances (1/2)

Info

Refresh

Connect

Instance state

Actions

Launch Instances

Search

1

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	
<input type="checkbox"/>	Bastion Host	i-0f706a811e589f67e	Running	t2.micro	2/2 checks passed	No alarms	+
<input checked="" type="checkbox"/>	Web Server 1	i-02e2208bd66d629a6	Running	t2.micro	-	No alarms	+

Instance: i-02e2208bd66d629a6 (Web Server 1)

i-02e2208bd66d629a6 (Web Server 1)

3.239.249.211

open address

Public IPv4 DNS copied

Instance state

Running

ec2-3-239-249-211.compute-1.amazonaws.com

open address

Private IP DNS name (IPv4 only)

ip-10-0-2-161.ec2.internal

Answer private resource DNS name

IPv4 (A)

Load Test

RDS

You should see a web page displaying the AWS logo and instance meta-data values.

The complete architecture you deployed is:

Region

Availability Zone A

VPC: 10.0.0.0/16

Public subnet 1: 10.0.0.0/24

NAT gateway

Private subnet 1: 10.0.1.0/24

Internet gateway

Availability Zone B

Public subnet 2: 10.0.2.0/24

Security group

Web server

Private subnet 2: 10.0.3.0/24

Public Route Table

Destination	Target
10.0.0.0/16	Local
0.0.0.0/0	Internet gateway

Private Route Table

Destination	Target
10.0.0.0/16	Local
0.0.0.0/0	NAT gateway