

Install Apache Server on EC2 instance

1-Create Security Group

Inbound rules (3)

Filter security group rules

< 1 >

⚙

<input type="checkbox"/>	Name	Security group rule...	IP version	Type	Protocol	Port range
<input type="checkbox"/>	-	sgr-0d36c7facfb14de19	IPv4	All ICMP - IPv4	ICMP	All
<input type="checkbox"/>	-	sgr-0a1c0a510b795f4e7	IPv4	HTTP	TCP	80
<input type="checkbox"/>	-	sgr-0353764da22bc54...	IPv4	SSH	TCP	22

Outbound rules (1)

Filter security group rules

⌂

<input type="checkbox"/>	Name	Security group rule...	IP version	Type
<input type="checkbox"/>	-	sgr-0e027533e65f636b6	IPv4	All traffic

2-Create and Launch Instance

-Create instance by default settings then select already created security group then install instance pair keys to access server

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="radio"/> sg-c7adad8d	default	default VPC security group	Copy to new
<input type="radio"/> sg-073dfc11268ccac	launch-wizard-1	launch-wizard-1 created 2021-09-09T14:20:02.201+02:00	Copy to new
<input checked="" type="radio"/> sg-0c5359cf7c97c1d27	test-webserver	lgggg	Copy to new

Warning

Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Inbound rules for sg-0c5359cf7c97c1d27 (Selected security groups: sg-0c5359cf7c97c1d27)

Type	Protocol	Port Range	Source	Description
HTTP	TCP	80	0.0.0.0/0	
SSH	TCP	22	0.0.0.0/0	
All ICMP - IPv4	All	N/A	0.0.0.0/0	

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

-I already created key pairs so I will use them in this instance

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

hello | 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

3-Access Instance and install and Launch Apache Server on it

-Access Instance through pair key using ssh command

```
C:\Programming\Embedded course>ssh -i hello.pem ec2-user@3.21.166.126
The authenticity of host '3.21.166.126 (3.21.166.126)' can't be established.
ECDSA key fingerprint is SHA256:vhSFAG+/aGUWdh8B1UJ/BQnhv5eh/E10o8NQvefB+lc.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '3.21.166.126' (ECDSA) to the list of known hosts.

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

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-172-31-38-36 ~]$ sudo su
```

-then give root access then by applying the following commands:

```
yum update -y
yum install -y httpd
systemctl start httpd
systemctl enable httpd
echo "<h1>Hello World from $(hostname -f)</h1>" > /var/www/html/index.html
```

The Result



Create and Configure VPC

1-Create VPC

VPC settings

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

IPv4 CIDR block [Info](#)

IPv6 CIDR block [Info](#)

☒ No IPv6 CIDR block

☐ Amazon-provided IPv6 CIDR block

☐ IPv6 CIDR owned by me

Tenancy [Info](#)

Default ▼

2-Create Public Subnet

VPC ID
Create subnets in this VPC.

vpc-0ff8989215b1f2145 (Demo-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.

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 (Ohio) / us-east-2a ▼

IPv4 CIDR block [Info](#)

▼ Tags - optional

Key

Value - optional

3-Create Private Subnet

Create subnets in this VPC.

vpc-Off8989215b1f2145 (Demo-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.

Demo-Private-SubnetB

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 (Ohio) / us-east-2b ▼

IPv4 CIDR block [Info](#)

Q 10.0.1.0/24 X

10.0.1.0/24

Key

Value - optional

4-Create NAT

NAT gateway settings

Name - optional

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

Demo-Nat-Gateway-PublicA

The name can be up to 256 characters long.

Subnet

Select a subnet in which to create the NAT gateway.

subnet-0e7a9b472718f4d0d (Demo-Public-SubnetA) ▼

Connectivity type

Select a connectivity type for the NAT gateway.

☒ Public

☐ Private

Elastic IP allocation ID [Info](#)

Assign an Elastic IP address to the NAT gateway.

Select an Elastic IP ▼

Allocate Elastic IP

5-Create Internet Gateway

Internet gateway settings

Name tag

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

6-Create Router

Route table settings

Name - optional

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

VPC

The VPC to use for this route table.


Edit routes

Destination	Target	Status
10.0.0.0/16	<input type="text" value="local"/>	Active
Propagated		
No		

Edit routes

Destination	Target	Status
<input type="text" value="0.0.0.0/0"/>	<input type="text" value="nat-0a4c5954745d1cce0"/>	-
Propagated		
No		


6-Create EC2 on Public Subnet

Network ⓘ ↕  [Create new VPC](#)

Subnet ⓘ ↕ [Create new subnet](#)
250 IP Addresses available

Assign Public IP ⓘ ↕

7-Create EC2 on Private Subnet

Network ⓘ ↕  [Create new VPC](#)

Subnet ⓘ ↕ [Create new subnet](#)
251 IP Addresses available

Auto-assign Public IP ⓘ ↕
