

Creating Networking Resources in an Amazon Virtual Private Cloud (VPC)

Objectives

In this lab, you will:

- Summarize the customer scenario
- Create a VPC, Internet Gateway, Route Table, Security Group, Network Access List, and EC2 instance to create a routable network within the VPC
- Familiarize yourself with the console
- Develop a solution to the customers issue found within this lab.

The lab is complete once you can successfully utilize the command ping outside the VPC.

Duration

This lab total duration is 60 minutes.

Scenario

Your role is a Cloud Support Engineer at Amazon Web Services (AWS). During your shift, a customer from a startup company requests assistance regarding a networking issue within their AWS infrastructure. The email and an attachment of their architecture is below.

Email from the customer

Hello Cloud Support!

I previously reached out to you regarding help setting up my VPC. I thought I knew how to attach all the resources to make an internet connection, but I cannot even ping outside the VPC. All I need to do is ping! Can you please help me set up my VPC to where it has network connectivity and can ping? The architecture is below. Thanks!

Brock, startup owner



Customer VPC architecture

AWS service restrictions

In this lab environment, access to AWS services and service actions might be restricted to the ones that are needed to complete the lab instructions. You might encounter errors if you attempt to access other services or perform actions beyond the ones that are described in this lab.

Accessing the AWS Management Console

1. At the top of these instructions, choose **Start Lab** to launch your lab.

A **Start Lab** panel opens, and it displays the lab status.

Tip: If you need more time to complete the lab, choose the Start Lab button again to restart the timer for the environment.

2. Wait until you see the message *Lab status: ready*, then close the **Start Lab** panel by choosing the **X**.

3. At the top of these instructions, choose **AWS**.

This opens the AWS Management Console in a new browser tab. The system will automatically log you in.

Tip: If a new browser tab does not open, a banner or icon is usually at the top of your browser with a message that your browser is preventing the site from opening pop-up windows. Choose the banner or icon and then choose **Allow pop ups**.

4. Arrange the AWS Management Console tab so that it displays along side these instructions. Ideally, you will be able to see both browser tabs at the same time so that you can follow the lab steps more easily.

Task 1: Investigate the customer's needs

► Recall

For task 1, you will investigate the customer's request and build a VPC that has network connectivity. You will complete this lab when you can successfully ping from your EC2 instance to the internet showing that the VPC has network connectivity.

In the scenario, Brock, the customer requesting assistance, has requested help in creating resources for his VPC to be routable to the internet. Keep the VPC CIDR at 192.168.0.0/18 and public subnet CIDR of 192.168.1.0/26.

The screenshot shows the AWS VPC Dashboard. On the left, there is a navigation pane with the following structure:

- 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**
 - Network ACLs
 - Security Groups

Figure: A great guide to building a VPC is to follow the left hand navigation pane, starting from "Your VPCs" and working your way down.

Before you start, let's review VPC and its components to make it network compatible.

- A **Virtual Private Gateway (VPC)** is like a data center but in the cloud. It's logically isolated from other virtual networks from which you can spin up and launch your AWS resources within minutes.
- **Private Internet Protocol (IP)** addresses are how resources within the VPC communicate with each other. An instance needs a public IP address for it to communicate outside the VPC. The VPC will need networking resources such as an Internet Gateway (IGW) and a route table in order for the instance to reach the internet.
- An **Internet Gateway (IGW)** is what makes it possible for the VPC to have internet connectivity. It has two jobs: perform network address translation (NAT) and be the target to route traffic to the internet for the VPC. An IGW's route on a route table is always 0.0.0.0/0.
- A **subnet** is a range of IP addresses within your VPC.

- A **route table** contains routes for your subnet and directs traffic using the rules defined within the route table. You associate the route table to a subnet. If an IGW was on a route table, the destination would be 0.0.0.0/0 and the target would be IGW.
- **Security groups and Network Access Control Lists (NACLs)** work as the firewall within your VPC. Security groups work at the instance level and are stateful, which means they block everything by default. NACLs work at the subnet level and are stateless, which means they do not block everything by default.

Steps

5. Select the **AWS** button located in the top right of the Vocareum home environment. This will open the AWS console in a new tab.
6. Once in the AWS console, click **VPC** under **Recently visited services**. If it is not there, navigate to the top left corner, and select **VPC** under **Networking and Content Delivery** in the **Services** navigation pane.

AWS Management Console

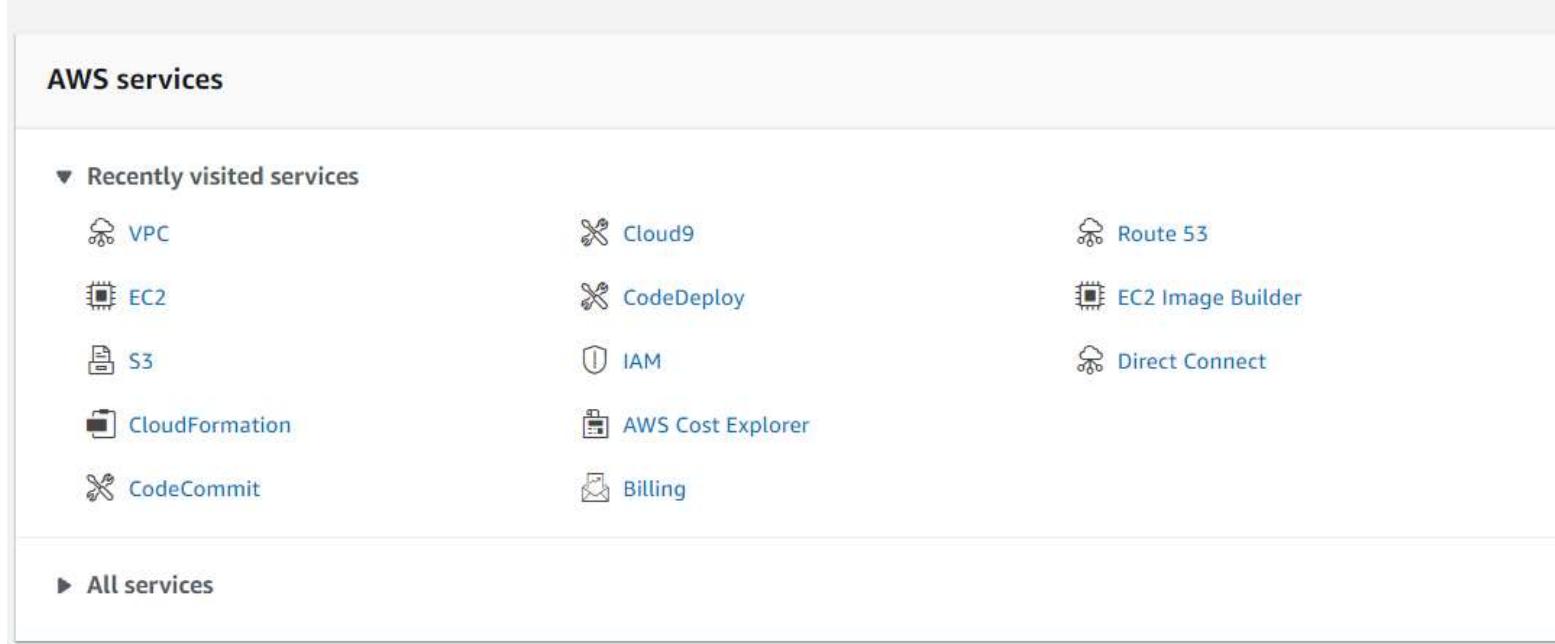


Figure: Recently visited services in the AWS console



★ Favorites

Resource Groups & Tag Editor

Recently visited

- Console Home
- VPC
- EC2
- S3
- CloudFormation
- CodeCommit
- Cloud9
- CodeDeploy
- IAM
- AWS Cost Explorer
- Billing
- Route 53
- EC2 Image Builder
- Direct Connect

All services

Server Migration Service

AWS Transfer Family

AWS Snow Family

DataSync

Networking & Content Delivery

VPC

CloudFront

Route 53

API Gateway

Direct Connect

AWS App Mesh

AWS Cloud Map

Global Accelerator

Media Services

Kinesis Video Streams

MediaConnect

MediaConvert

MediaLive

MediaPackage

MediaStore

MediaTailor

Elemental Appliances & Software

Amazon Interactive Video Service

Elastic Transcoder

Nimble Studio

Figure: Services navigation drop down

Creating the VPC

► Recall

7. Start at the top of the left navigation pane at **Your VPCs** and work your way down. Select **Your VPCs**, navigate to the top right corner, and select **Create VPC**.

Note

Note, you will be using a top-down theory with the top being the VPC.

Your VPCs (2) Info							
	Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR (Network border group)		IPv6 pool
<input type="checkbox"/>	-	vpc-02cd10b2d40459689	Available	172.31.0.0/16	-	-	-
<input type="checkbox"/>	Test VPC	vpc-0524aba7de8ae0a11	Available	192.168.0.0/18	-	-	-

Figure: Navigate to "Your VPCs" and select Create VPC.

8. Name the VPC: Test VPC

IPv4 CIDR block: 192.168.0.0/18

9. Leave everything else as default, and select **Create VPC**.

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](#).

Figure: VPC settings configuration

Creating Subnets

► Recall

10. Now that the VPC is complete, look at the left navigation pane and select **Subnets**. In the top right corner, select **Create subnet**.

Note

Please note: Although almost anything can be created in any order, it is easier to have an approach. Having a flow or an approach will assist you in troubleshooting issues and ensure that you do not forget a resource.

Subnets (4) Info							
	Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR	Available IPv4 a
<input type="checkbox"/>	-	subnet-038ed9e7b38319620	Available	vpc-02cd10b2d40459689	172.31.16.0/20	-	4091
<input type="checkbox"/>	-	subnet-0c364b868f7ef6f7c	Available	vpc-02cd10b2d40459689	172.31.48.0/20	-	4091
<input type="checkbox"/>	-	subnet-03a499f278b913925	Available	vpc-02cd10b2d40459689	172.31.0.0/20	-	4091
<input type="checkbox"/>	-	subnet-0c8cc63299097dec1	Available	vpc-02cd10b2d40459689	172.31.32.0/20	-	4091

Figure: Select Create subnet

11. Configure like the following picture:

VPC

VPC ID

Create subnets in this VPC.

vpc-0524aba7de8ae0a11 (Test VPC)



Associated VPC CIDRs

IPv4 CIDRs

192.168.0.0/18

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

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](#)

192.168.1.0/28



▼ Tags - optional

Key

Name

Value - optional

Public subnet



Remove

Figure: Subnet configuration

Create Route Table

► Recall

12. Navigate to the left navigation pane, and select **Route Tables**. In the top right corner select **Create route table**.

Route tables (2) Info										Actions ▾	Create route table
	Name	Route table ID	Explicit subnet associat...	Edge associations	Main	VPC	Owner ID				
<input type="checkbox"/>	-	rtb-0f4c9ea27f2b30085	-	-	Yes	vpc-0524aba7de8ae0a11 Test VPC	300476415442				
<input type="checkbox"/>	-	rtb-002a7022b83f1641c	-	-	Yes	vpc-02cd10b2d40459689	300476415442				

Figure: Select Create route table.

13. Configure like the following picture:

VPC > Route tables > Create route table

Create route table [Info](#)

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

Route table settings

Name - optional

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

Public route table

VPC

The VPC to use for this route table.

vpc-0524aba7de8ae0a11 (Test VPC)

Tags

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

Name

Public route table

X

Remove

Add new tag

You can add 49 more tags.

Cancel

Create route table

Figure: Route table configuration

Create Internet Gateway and attach Internet Gateway

In this lab

14. From the left navigation pane, select **Internet Gateways**. Create an Internet Gateway (IGW) by selecting **Create internet gateway** at the top right corner.

The screenshot shows the AWS VPC Internet Gateways page. On the left, there's a navigation pane with options like 'New VPC Experience', 'VPC Dashboard', 'EC2 Global View', 'Filter by VPC', 'Select a VPC', 'Your VPCs', 'Subnets', 'Route Tables', and 'Internet Gateways'. The 'Internet Gateways' option is highlighted. The main area displays a table titled 'Internet gateways (1)' with one row. The row contains columns for Name (empty), Internet gateway ID (igw-08d36e215b5765dfe), State (Attached), VPC ID (vpc-02cd10b2d40459689), and Owner (300476415442). A search bar at the top says 'Filter Internet gateways'.

Figure: Select *Create internet gateway*

15. Configure like the following picture:

The screenshot shows the 'Create internet gateway' configuration page. At the top, a breadcrumb trail reads 'VPC > Internet gateways > Create internet gateway'. The main title is 'Create internet gateway' with an 'Info' link. Below it, a text block explains that an internet gateway connects a VPC to the internet and asks to specify a name. The 'Internet gateway settings' section has a 'Name tag' field containing 'IGW test VPC'. The 'Tags - optional' section shows a key-value pair: 'Name' (Key) and 'IGW test VPC' (Value). There's a note saying you can add 49 more tags. At the bottom, there are 'Cancel' and 'Create internet gateway' buttons.

Figure: Internet gateway configuration

16. Once created, attach the **Internet Gateway** to the VPC by selecting **Actions** at the top right corner and clicking **Attach to VPC**.

The screenshot shows the AWS VPC Internet Gateway creation page. At the top, a green banner indicates that an internet gateway has been created. Below the banner, the breadcrumb navigation shows 'VPC > Internet gateways > igw-070bd47bf43135aec'. The main title is 'igw-070bd47bf43135aec / IGW test VPC'. On the right, there is an 'Actions' dropdown menu with options: 'Attach to VPC' (highlighted), 'Detach from VPC', 'Manage tags', and 'Delete'. The 'Details' tab is selected, showing the following information:

Internet gateway ID	igw-070bd47bf43135aec	State	Detached	VPC ID	-	Owner	300476415442
---------------------	-----------------------	-------	----------	--------	---	-------	--------------

Figure: Attaching the IGW that was just created.

Now your IGW is attached! You now need to add its route to the route table and associate the subnet you created to the route table.

Add route to route table and associate subnet to route table

17. Navigate to the **Route Table** section on the left navigation pane. Select **Public Route Table**, and then scroll to the bottom and select the **Routes** tab. Select the **Edit routes** button located in the routes box.

On the Edit routes page, the first IP address is the local route and cannot be changed.

Select **Add route**.

- In the **Destination** section, type **0.0.0.0/0** in the search box. This is the route to the IGW. You are telling the route table that any traffic that needs internet connection will use 0.0.0.0/0 to reach the IGW so that it can reach the internet.
- Click in the **Target** section and select **Internet Gateway** since you are targeting any traffic that needs to go to the internet via the IGW. Once you select the IGW, you will see your **TEST VPC IGW** appear. Select that IGW, navigate to the bottom right, and select **Save changes**.

The screenshot shows the 'Edit routes' page for a route table. The breadcrumb navigation shows 'VPC > Route tables > rtb-0769adc74f663bef > Edit routes'. The table lists routes:

Destination	Target	Status	Propagated
192.168.0.0/18	local	Active	No
0.0.0.0/0	igw-070bd47bf43135aec (IGW test VPC)	-	No

At the bottom, there are buttons for 'Add route', 'Cancel', 'Preview', and 'Save changes'.

Figure: Adding the IGW in the route table (0.0.0.0/0 as the destination and IGW as the target).

Now your traffic has a route to the internet via the IGW.

18. From the Public route table dashboard, select the **Subnet associations** tab. Select the **Edit subnet associations** button.

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (1/1)

Available subnets (1/1)					
<input type="text"/> Filter subnet associations					
Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID	Actions
<input checked="" type="checkbox"/> Public subnet	subnet-09a3b15dff7bdb6e5	192.168.1.0/28	-	Main (rtb-0f4c9ea27f2b30085)	<input type="button" value="Associate"/>

Selected subnets

subnet-09a3b15dff7bdb6e5 / Public subnet <input type="button" value="X"/>

Figure: Associate the Public subnet and select save association.

19. Select Save association.

Note: Every route table needs to be associated to a subnet. You are now associating this route table to this subnet. As you probably noticed, the naming convention is kept the same (public route table, public subnet, etc) in order to associate the same resources together. Keep this in mind when your network and resources grow. You can have multiples of the same resources and it can get confusing to which belongs where.

Creating a Network ACL

► Recall

20. From the left navigation pane, select **Network ACLs**. Navigate to the top right corner and select **Create network ACL** to create a Network Access Control Lists (NACLs).

Network ACLs (1/2)

Network ACLs (1/2)						<input type="button" value="Info"/>	
<input type="text"/> Filter network ACLs						<input type="button" value="Actions"/>	<input type="button" value="Create network ACL"/>
Name	Network ACL ID	Associated with	Default	VPC ID	Inbound rules count		
<input type="checkbox"/> -	acl-078b22b8f69bd038e	4 Subnets	Yes	vpc-02cd10b2d40459689	2 Inbound rules		
<input checked="" type="checkbox"/> -	acl-0c75d86131fc2b175	subnet-09a3b15dff7bdb6e5 / Public subnet	Yes	vpc-0524aba7de8ae0a11 / Test VPC	2 Inbound rules		

acl-0c75d86131fc2b175

-

Details

Network ACL ID <input checked="" type="checkbox"/> acl-0c75d86131fc2b175	Associated with subnet-09a3b15dff7bdb6e5 / Public subnet	Default Yes	VPC ID vpc-0524aba7de8ae0a11 / Test VPC
Owner <input checked="" type="checkbox"/> 300476415442			

Figure: Select Create network ACL

Inbound After creating the NACL, it will look like the following. This indicates there is only one rule number, which is 100, that states that all traffic, all protocols, all port ranges, from any source (0.0.0.0/0) are allowed to enter (inbound) the subnet. The asterisk * indicates that anything else that does not match this rule is denied.

The screenshot shows the AWS VPC NACL configuration for a subnet. At the top, it displays the NACL name (acl-0c75d86131fc2b175), subnet ID (subnet-09a3b15dff7bdb6e5), and status (Public subnet). Below this, the 'Inbound rules' tab is selected. A message indicates that network connectivity can be checked using the Reachability Analyzer. The 'Inbound rules (2)' section lists two rules:

Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

Figure: Default inbound rule configuration for NACL. This will allow all traffic from anywhere and deny anything else that does not match this rule at the subnet level.

Outbound What do you think this rule says?

The screenshot shows the AWS VPC NACL configuration for a subnet. At the top, it displays the NACL name (acl-0c75d86131fc2b175), subnet ID (subnet-09a3b15dff7bdb6e5), and status (Public subnet). Below this, the 'Outbound rules' tab is selected. A message indicates that network connectivity can be checked using the Reachability Analyzer. The 'Outbound rules (2)' section lists two rules:

Rule number	Type	Protocol	Port range	Destination	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

Figure: Default outbound rule configuration for NACL. This will allow all traffic from anywhere and deny anything else that does not match this rule at the subnet level.

Creating a Security Group

► Recall

- From the left navigation pane, select **Security Groups**. Navigate to the top right corner and select **Create security group** to create a security group.

The screenshot shows the AWS Security Groups list page. On the left, a navigation pane includes options like New VPC Experience, Subnets, Route Tables, Internet Gateways, Egress Only Internet Gateways, Carrier Gateways, DHCP Options Sets, Elastic IPs, Managed Prefix Lists, Endpoints, Endpoint Services, NAT Gateways, and Peering Connections. The 'SECURITY' section is expanded, showing Network ACLs and Security Groups, with 'Security Groups' selected. The main area displays a table of security groups:

Security Groups (2) <small>Info</small>							
	Name	Security group ID	Security group name	VPC ID	Description	Owner	Inbound rules count
<input type="checkbox"/>	-	sg-009b5328a08e84f02	default	vpc-02cd10b2d40459689	default VPC security gr...	300476415442	1 Permission entry
<input type="checkbox"/>	-	sg-0985e200161ea6416	default	vpc-0524aba7de8ae0a11	default VPC security gr...	300476415442	1 Permission entry

Figure: Select Create security group

Configure like the following image of the Basic details page:

Note: In the VPC portion, remove the current VPC, and select **Test VPC**.

Basic details

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

Description [Info](#)
allows public access

VPC [Info](#)
 vpc-0524aba7de8ae0a11 X

Figure: Configure the Basic details page

The completed security group is shown below. This indicates that for **Inbound rules** you are allowing SSH, HTTP, and HTTPS types of traffic, each of which has its own protocols and port range. The source from which this traffic reaches your instance can be originating from anywhere. For **Outbound rules**, you are allowing all traffic from outside your instance.

Inbound rules [Info](#)

Type Info	Protocol Info	Port range Info	Source Info	Description - optional Info	Delete
SSH	TCP	22	Anywhere... ▼	<input type="text"/> 0.0.0.0 X	Delete
HTTP	TCP	80	Anywhere... ▼	<input type="text"/> 0.0.0.0 X	Delete
HTTPS	TCP	443	Anywhere... ▼	<input type="text"/> 0.0.0.0 X	Delete

Add rule

Outbound rules [Info](#)

Type Info	Protocol Info	Port range Info	Destination Info	Description - optional Info	Delete
All traffic	All	All	Custom ▼	<input type="text"/> 0.0.0.0 X	Delete

Add rule

Figure: Configuration details for inbound and outbound rules for the security group

You now have a functional VPC. The next task is to launch an EC2 instance to ensure that everything works.

Task 2: Launch EC2 instance and SSH into instance

In task 2, you will launch an EC2 instance within your Public subnet and test connectivity by running the command **ping**. This will validate that your infrastructure is correct, such as security groups and network ACLs, to ensure that they are not blocking any traffic from your instance to the internet and vice versa. This will validate that you have a route to the IGW via the route table and that the IGW is attached.

22. Navigate to Services at the top left, and select **EC2**. From the EC2 dashboard, select **Instances**.

The screenshot shows the AWS EC2 Instances page. On the left, there's a sidebar with 'Instances' selected. Under 'Instances', 'Instances New' is highlighted with a red box. At the top right, there's a large orange 'Launch instances' button with a red border. Below it, a modal window titled 'Select an instance above' is open.

Figure: Launch an EC2 instance by selecting Launch instance

23. Select **Launch instances** from the top right corner. Then complete the following steps:

24. For Step 1, keep the defaults.

This screenshot shows the 'Step 1: Choose an Amazon Machine Image (AMI)' screen. It includes a search bar, a 'Quick Start' sidebar with options like 'My AMIs', 'AWS Marketplace', and 'Community AMIs', and a main content area displaying the 'Amazon Linux 2 AMI (HVM, SSD Volume Type)'. The 'Free tier eligible' badge is visible. On the right, there are buttons for 'Cancel and Exit' and 'Select'.

Figure: Choose the AMI: Amazon Linux 2 AMI in step 1

25. For step 2, keep the defaults.

This screenshot shows the 'Step 2: Choose an Instance Type' screen. It features a table with columns for Family, Type, vCPUs, Memory, Instance Storage, EBS-Optimized Available, Network Performance, and IPv6 Support. The 't2.micro' row is selected, indicated by a blue border and a green 'Free tier eligible' badge. Other rows include 't2.nano' and 't2'. The table has a 'Filter by' dropdown at the top left.

Figure: Choose the instance type, t3.micro, in step 2.

26. For step 3, configure the Instance as shown below:

This screenshot shows the 'Step 3: Configure Instance Details' screen. It includes fields for 'Number of instances' (set to 1), 'Purchasing option' (checkbox for 'Request Spot instances'), 'Network' (VPC selection), 'Subnet' (subnet selection), and 'Auto-assign Public IP' (checkbox set to 'Enable').

Figure: Step 3 is to configure the instance details. An important note here is to enable the "Auto-assign Public IP" if you want a public IP for an instance without having to assign an EIP.

27. For step 4, keep the defaults.

The screenshot shows the 'Step 4: Add Storage' configuration screen. At the top, there is a navigation bar with seven tabs: 1. Choose AMI, 2. Choose Instance Type, 3. Configure Instance, 4. Add Storage (which is highlighted in orange), 5. Add Tags, 6. Configure Security Group, and 7. Review. Below the navigation bar, the title 'Step 4: Add Storage' is displayed in bold. A descriptive text follows: '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.' The main configuration area contains a table with columns: Volume Type, Device, Snapshot, Size (GiB), Volume Type, IOPS, Throughput (MB/s), Delete on Termination, and Encryption. There is one row for the 'Root' volume, which is set to '/dev/xvda', has a 'Snapshot' of 'snap-07fd5ce789f832abe', a 'Size (GiB)' of '8', is a 'General Purpose S' volume type, has 'IOPS' of '100 / 3000', 'Throughput (MB/s)' of 'N/A', 'Delete on Termination' checked, and 'Encryption' set to 'Not Encrypted'. Below the table is a button labeled 'Add New Volume'. A note below the table states: '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.' At the bottom right, there are four buttons: 'Cancel', 'Previous', 'Review and Launch' (which is highlighted in blue), and 'Next: Add Tags' (which is enclosed in a red rectangle).

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encryption
Root	/dev/xvda	snap-07fd5ce789f832abe	8	General Purpose S	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted

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**

Figure: Step 4 has the option to add additional or change the storage. This will be kept at the default storage.

28. For step 5, keep the defaults.

The screenshot shows the 'Step 5: Add Tags' section of the AWS EC2 wizard. At the top, there are tabs for 1. Choose AMI, 2. Choose Instance Type, 3. Configure Instance, 4. Add Storage, 5. Add Tags (which is underlined), 6. Configure Security Group, and 7. Review. Below the tabs, there are fields for 'Key' (128 characters maximum) and 'Value' (256 characters maximum). To the right, there are buttons for 'Instances' (with an info icon), 'Volumes' (with an info icon), and 'Network Interfaces' (with an info icon). A message states 'This resource currently has no tags'. Below this, instructions say 'Choose the Add tag button or click to add a Name tag.' and 'Make sure your IAM policy includes permissions to create tags.' At the bottom, there are buttons for 'Add Tag' (highlighted with a grey box), 'Cancel', 'Previous', 'Review and Launch', and 'Next: Configure Security Group' (highlighted with a red box).

Figure: Step 5 has the option to add tags, which gives the instance a name and value. However, since we are launching just one instance, we will leave this blank. This is a great option when you have multiple resources and need to assign them specific values and names.

29. For step 6, configure the security group as shown below:

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-0985e200161ea6416	default	default VPC security group	Copy to new
<input checked="" type="checkbox"/> sg-01f1d0e46107f965f	public security group	allows public access	Copy to new

Inbound rules for sg-01f1d0e46107f965f (Selected security groups: sg-01f1d0e46107f965f)

Type (i)	Protocol (i)	Port Range (i)	Source (i)	Description (i)
HTTP	TCP	80	0.0.0.0/0	
SSH	TCP	22	0.0.0.0/0	
HTTPS	TCP	443	0.0.0.0/0	

Figure: In step 6, you can always create a new security group or select an existing one. Select the option "Select an existing security group" and select the security group you created, "public security group".

30. For step 7, review your settings. It should look like the following:

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

Edit AMI

AMI Details

	Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-0e5b6b6a9f3db6db8
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 no longer supported.	
Free tier eligible	Root Device Type: ebs Virtualization type: hvm

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-0346d955328b6993e	Public SG	public security group

All selected security groups inbound rules

Type	Protocol	Port Range	Source	Description
HTTP	TCP	80	0.0.0.0/0	
SSH	TCP	22	0.0.0.0/0	
HTTPS	TCP	443	0.0.0.0/0	

Instance Details

Edit instance details

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

Figure: With all the steps followed correctly, the review screen should look like the example.

31. Choose the following key:

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](#)

Figure: You will choose an existing key pair: vockey | RSA. You must acknowledge that you have the corresponding private key file that can be downloaded in the details tab in the Vocreaum lab page.

While waiting for the instance to enter the ready state, open the Details tab located at the top of this lab window and download the **PPK** file, if on Windows, or the **pem** file, if on a Mac.

SSH into the EC2 instance by using PuTTY. You can follow these steps here:

Use SSH to connect to an Amazon Linux EC2 instance

► Ways to connect Amazon Linux EC2

The following instructions vary slightly depending on whether you are using Windows or Mac/Linux.

Windows Users: Using SSH to Connect

► These instructions are specifically for Windows users. If you are using macOS or Linux, [skip to the next section](#).

32. Select the **Details** drop-down menu above these instructions you are currently reading, and then select **Show**. A Credentials window will be presented.
33. Select the **Download PPK** button and save the **labsuser.ppk** file.
Typically your browser will save it to the Downloads directory.
34. Make a note of **PublicInstanceBIP**, the IPV4 server's address you have to connect to.
35. Then exit the Details panel by selecting the **X**.
36. Download **PuTTY** to SSH into the Amazon EC2 instance. If you do not have PuTTY installed on your computer, [download it here](#).
37. Open **putty.exe**.

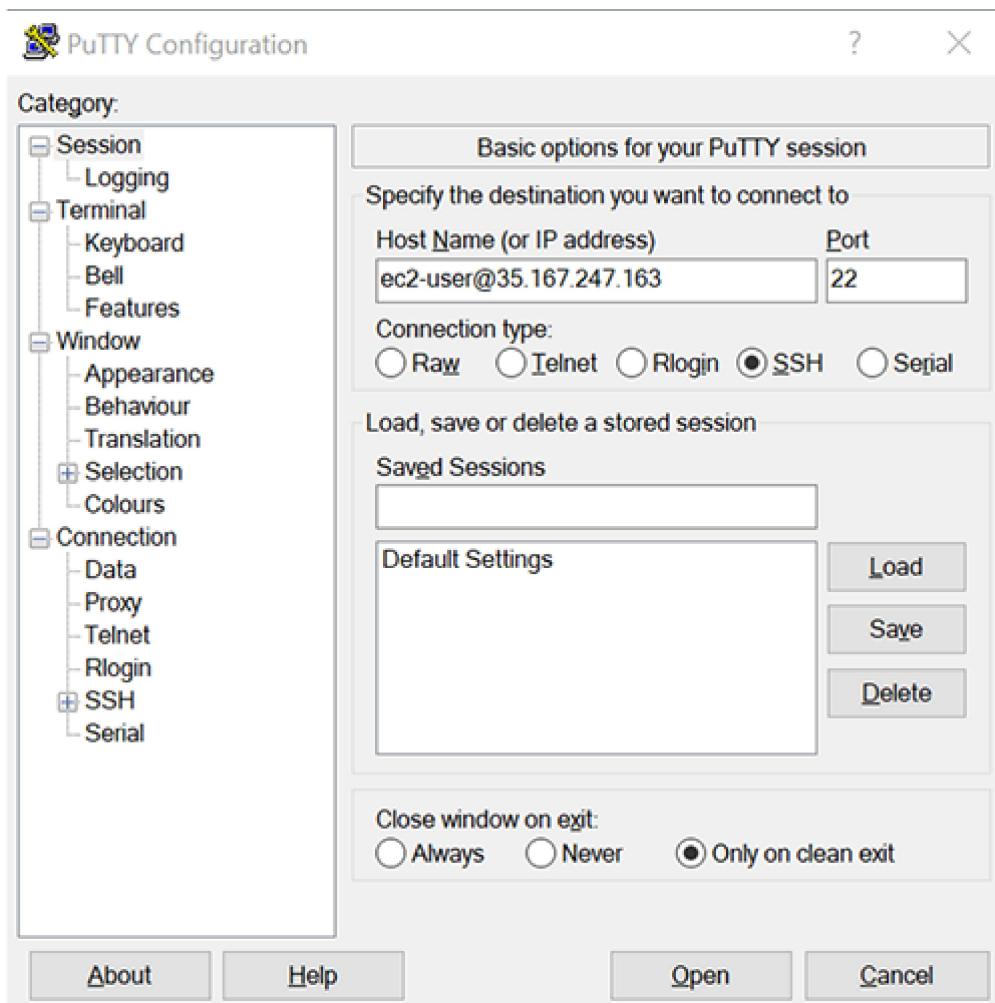


Figure: SSH using Putty for windows.

38. Configure PuTTY timeout to keep the PuTTY session open for a longer period of time.:
 - Select **Connection**
 - Set **Seconds between keepalives** to **30**
39. Configure your PuTTY session:

- o Select **Session**
- o **Host Name (or IP address)**: Paste the server's address of the instance you made a note of earlier.
- o Back in PuTTY, in the **Connection** list, expand **SSH**
- o Select **Auth** (*don't expand it*)
- o Select **Browse**
- o Browse to and select the **labuser.ppk** file that you downloaded
- o Select **Open** to select it
- o Select **Open** again.

40. Select **Yes**, to trust and connect to the host.

41. When prompted **Login as**, enter: **ec2-user**

This will connect you to the EC2 instance.

42. Windows Users: [Select here to skip ahead to the next task.](#)

macOS and Linux Users

These instructions are specifically for Mac/Linux users. If you are a Windows user, [skip ahead to the next task.](#)

43. Select the **Details** drop-down menu above these instructions you are currently reading, and then select **Show**. A Credentials window will be presented.

44. Select the **Download PEM** button and save the **labsuser.pem** file.

45. Make a note of **PublicIP**, the IPV4 server's address you have to connect to.

46. Then exit the Details panel by selecting the **X**.

47. Open a terminal window, and change directory **cd** to the directory where the **labsuser.pem** file was downloaded. For example, if the **labuser.pem** file was saved to your Downloads directory, run this command:

```
cd ~/Downloads
```

48. Change the permissions on the key to be read-only, by running this command:

```
chmod 400 labsuser.pem
```

49. Run the below command (*replace <public-ip> with the server's address you copied earlier*):

```
ssh -i labsuser.pem ec2-user@<public-ip>
```



```
hostname ~]$ ssh -i /path/my-key-pair.pem ec2-user@35.167.247.163
```

Figure: SSH using a terminal for Mac.

50. Type `yes` when prompted to allow the first connection to this remote SSH server.

Because you are using a key pair for authentication, you will not be prompted for a password.

Task 3: Use ping to test internet connectivity

51. Run the following command to test internet connectivity:

```
ping google.com
```

After a few seconds, exit ping by holding **CTRL+C** on Windows or **CMD+C** on Mac to exit. You should get the following result:

Successful ping:

```
[ec2-user@ip-192-168-1-8 ~]$ ping google.com
PING google.com (142.250.217.110) 56(84) bytes of data.
64 bytes from sea09s30-in-f14.1e100.net (142.250.217.110): icmp_seq=1 ttl=93 time=6.02 ms
64 bytes from sea09s30-in-f14.1e100.net (142.250.217.110): icmp_seq=2 ttl=93 time=5.96 ms
64 bytes from sea09s30-in-f14.1e100.net (142.250.217.110): icmp_seq=3 ttl=93 time=6.23 ms
64 bytes from sea09s30-in-f14.1e100.net (142.250.217.110): icmp_seq=4 ttl=93 time=6.01 ms
^C
--- google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 5.969/6.060/6.230/0.126 ms
[ec2-user@ip-192-168-1-8 ~]$
```

Run ping to test connectivity. The above results are saying you have replies from google.com and have 0% packet loss.

If you are getting replies back, that means that you have connectivity.

Lab Complete

 Congratulations! You have completed the lab.

52. Choose  **End Lab** at the top of this page, and then select  **Yes** to confirm that you want to end the lab.

A panel indicates that *You may close this message box now. Lab resources are terminating...*

53. Choose the **X** in the upper-right corner to close the **End Lab** panel.

Recap

► In this lab

Additional Resources

[What is Amazon VPC?](#)

[IP Addressing in your VPC](#)

[Route tables for your VPC](#)

[Internet Gateways](#)

[Network ACLs](#)

[Security Groups](#)

For more information about AWS Training and Certification, see [AWS Training and Certification Opens in new window](#)

Your feedback is welcome and appreciated.

If you would like to share any suggestions or corrections, please provide the details in our [AWS Training and Certification Contact Form Opens in new window](#)

© 2022 Amazon Web Services, Inc. and its affiliates. All rights reserved. This work may not be reproduced or redistributed, in whole or in part, without prior written permission from Amazon Web Services, Inc. Commercial copying, lending, or selling is prohibited.