

Karthik Pradeep Hegadi

2KE20CS032

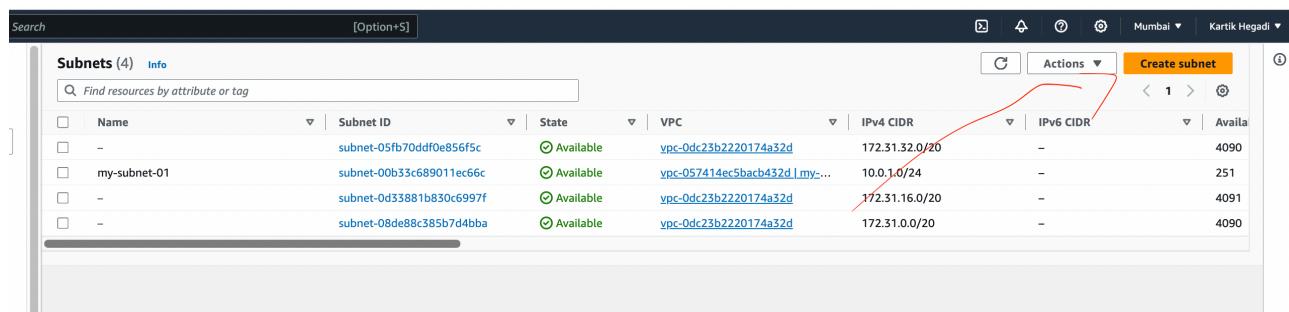
Assignment 33

Understood. To follow the provided instructions and create the files/directory using the same name and case as provided in the task steps, please provide me with the specific names and case instructions for the files/directory you want to create.

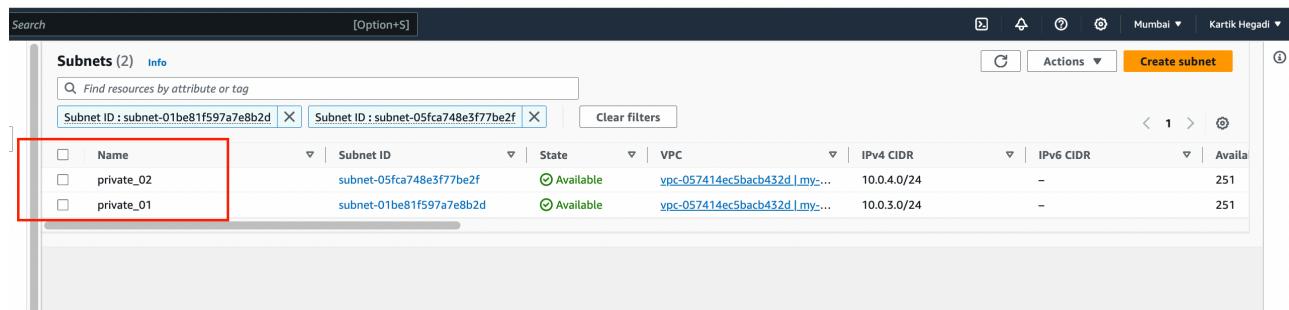
AWS-2

Assignment - 2 -Configure EC2 private Instance in AWS (create two private subnets ,two private instances, 1 Route Tables)

1. Login to your AWS console and choose the region where you have created your VPC
2. Click on "Create subnet" select the VPC that you have created previously



Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR	Available
-	subnet-05fb70ddf0e856f5c	Available	vpc-0dc23b2220174a32d	172.31.32.0/20	-	4090
my-subnet-01	subnet-00b33c689011ec66c	Available	vpc-057414ec5bacb432d my...	10.0.1.0/24	-	251
-	subnet-0d33881b830c6997f	Available	vpc-0dc23b2220174a32d	172.31.16.0/20	-	4091
-	subnet-08de88c385b7d4bba	Available	vpc-0dc23b2220174a32d	172.31.0.0/20	-	4090



Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR	Available
private_02	subnet-05fca748e3f77be2f	Available	vpc-057414ec5bacb432d my...	10.0.4.0/24	-	251
private_01	subnet-01be81f597a7e8b2d	Available	vpc-057414ec5bacb432d my...	10.0.3.0/24	-	251

3. In the subnet settings(subnet 1 of 1) , provide the name of the subnet ex: private_01 ,select the AZ that you have given for public instance, provide the IPV4

CIDR block as 10.0.3.0/24 (Note : you can provide your own CIDR block)

4. Click on Add new subnet and provide the name of the subnet ex: private_02
select the AZ select the AZ that you have given for public instance provide the IPV4
CIDR block as 10.0.4.0/24 (Note : you can provide your own CIDR block)

5. Now click on "create subnet" to get created

Subnet 1 of 2

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](#)

10.0.3.0/24

▼ Tags - optional

Key

Value - optional



You can add 49 more tags.

Subnet 2 of 2

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](#)

10.0.4.0/24

▼ Tags - optional

Key

Value - optional



You can add 49 more tags.

6. Create a Route table private subnets

Rout table for 1st

Your VPCs [New](#)

Subnets

Route tables 1

- Internet gateways
- Egress-only internet gateways
- DHCP option sets
- Elastic IPs
- Managed prefix lists
- Endpoints
- Endpoint services
- NAT gateways
- Peering connections

▼ Security

- Network ACLs
- Security groups

▼ DNS firewall

- Rule groups
- Domain lists

▼ Network Firewall

- Firewalls

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
private_rt	rtb-040ea9caf07f4a886	-	-	No rtb-057414ec5bacb432d my... 280005775301

rtb-040ea9caf07f4a886 / private_rt 3

Details | Routes | **Subnet associations** 3 | Edge associations | Route propagation | Tags

Explicit subnet associations (0)

Edit subnet associations < 1 > ⌂

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
No subnet associations. You do not have any subnet associations.				

4

8. Now create instances for private subnets, navigate to EC2 and click on Launch

Instance

VPC > Route tables > rtb-040ea9caf07f4a886 > Edit subnet associations

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (1/3)

<input type="checkbox"/>	Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
<input type="checkbox"/>	my-subnet-01	subnet-00b33c689011ec66c	10.0.1.0/24	-	rtb-06d5016a6dad9350d / public_rt
<input type="checkbox"/>	private_02	subnet-05fca748e5f7be2f	10.0.4.0/24	-	Main (rtb-0a446091bb5a6ff66)
<input checked="" type="checkbox"/>	private_01	subnet-01be81f597a7e8b2d	10.0.3.0/24	-	Main (rtb-0a446091bb5a6ff66)

1 Selected subnets

subnet-01be81f597a7e8b2d / private_01 2

Cancel Save associations

9. Select the AMI as below

▼ Application and OS Images (Amazon Machine Image) [Info](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS images

Quick Start

 [Browse more AMIs](#)
Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Amazon Linux 2023 AMI ami-06791f9213ccb608b (64-bit (x86)) / ami-0ee08895e8a84a697 (64-bit (Arm))
Virtualization: hvm ENA enabled: true Root device type: ebs Free tier eligible ▾

Description
Amazon Linux 2023 AMI 2023.2.20231018.2 x86_64 HVM kernel-6.1

Architecture 64-bit (x86) ▾ **AMI ID** ami-06791f9213ccb608b Verified provider

10. Click "Next" in the step2 as default is selected

11. In the Network, select the VPC that you have created, in the subnets select

the private 01 subnet that you have created. Click on "Next : Add Storage"

12. In storage the default options are selected , you can click "Next : Add Tags" provide the Name and Value as below, (it is your choice to provide any values) and click on 'configure security groups'

13. In 'configure security groups' add the following rules

(Note : Select my ip from the source)

14. Click on Launch in the Last step, it will be selecting the existing keypair by

default, make a check on acknowledge and click launch instance

Your private Instance is created as below

15. Similarly create another private Instance

11. In the Network, select the VPC that you have created, in the subnets select the private 01 subnet that you have created. Click on "Next : Add Storage"

12. In storage the default options are selected , you can click "Next : Add Tags" provide the Name and Value as below, (it is your choice to provide any values) and click on 'configure security groups

▼ Network settings [Info](#)

VPC - required [Info](#)
vpc-057414ec5bacb432d (my-vpc-01)
10.0.0.0/16 [G](#)

Subnet Info
subnet-01be81f597a7e8b2d private_01
VPC: vpc-057414ec5bacb432d Owner: 280005775301
Availability Zone: ap-south-1a IP addresses available: 251 CIDR: 10.0.3.0/24) [C](#) Create new subnet [Z](#)

Auto-assign public IP [Info](#)
Disable [▼](#)

Firewall (security groups) [Info](#)
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.
 Create security group Select existing security group

Security group name - required
launch-wizard-4

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and _-:/()#@[]+=&;!\$^*

Description - required [Info](#)
launch-wizard-4 created 2023-10-28T13:00:18.011Z

Inbound Security Group Rules

▼ Security group rule 1 (TCP, 22, 0.0.0.0/0) [Remove](#)

Type Info	Protocol Info	Port range Info
ssh ▼	TCP	22
Source type Info	Source Info	Description - optional Info
Anywhere ▼	<input type="text"/> Add CIDR, prefix list or security 0.0.0.0/0 X	e.g. SSH for admin desktop

Route tables (5) [Info](#)

Find resources by attribute or tag

<input type="checkbox"/>	Name	Route table ID	Explicit subnet associations	Edge associations
<input type="checkbox"/>	-	rtb-0a446091bb5a6ff66	-	-
<input type="checkbox"/>	-	rtb-08220544a6d57ceb6	-	-
<input type="checkbox"/>	private_rt_1	rtb-040ea9caf07f4a886	subnet-01be81f597a7e8...	-
<input type="checkbox"/>	public_rt	rtb-06d5016a6dad9350d	subnet-00b33c689011ec...	-
<input checked="" type="checkbox"/>	private_rt_2	rtb-0d122ea89b0b7d536	-	-

Subnets

Route tables [Edit](#) [Details](#) [Logs](#)

<input checked="" type="checkbox"/>	private_rt_2	rtb-0d122ea89b0b7d536	-	-	No	ypc-057414ec5bach432d my...	280005775301
-------------------------------------	--------------	-----------------------	---	---	----	-------------------------------	--------------

Details Routes Subnet associations Edge associations Route propagation Tags

Explicit subnet associations (0)

Find subnet association

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
No subnet associations			
You do not have any subnet associations.			

Edit subnet associations [Edit](#) [Cancel](#) [Save associations](#)

VPC > Route tables > rtb-0d122ea89b0b7d536 > Edit subnet associations

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (1/3)

Filter subnet associations

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
my-subnet-01	subnet-00b33c689011ec66c	10.0.1.0/24	-	rtb-06d5016a6dad9350d / public_rt
<input checked="" type="checkbox"/> private_02	subnet-05fca748e3f77be2f	10.0.4.0/24	-	Main (rtb-0a446091bb5a6ff66)
<input type="checkbox"/> private_01	subnet-01be81f597a7e8b2d	10.0.3.0/24	-	rtb-040ea9caf07f4a886 / private_rt_1

Selected subnets

subnet-05fca748e3f77be2f / private_02 [X](#)

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

13. In 'configure security groups' add the following rules

(Note : Select my ip from the source)

14. Click on Launch in the Last step, it will be selecting the existing keypair by

default, make a check on acknowledge and click launch instance
Your private Instance is created as below

The screenshot shows the 'Network settings' configuration page for a Lambda function. It includes fields for VPC (selected: 'vpc-057414ec5bacb432d (my-vpc-01) 10.0.0.0/16'), Subnet ('subnet-05fca748e3f77be2f private_02'), Auto-assign public IP ('Disable'), Firewall security groups ('Create security group' selected), Security group name ('launch-wizard-5'), and a Description ('launch-wizard-5 created 2023-10-28T13:12:43.479Z').

VPC - required Info
vpc-057414ec5bacb432d (my-vpc-01)
10.0.0.0/16

Subnet Info
subnet-05fca748e3f77be2f private_02
VPC: vpc-057414ec5bacb432d Owner: 280005775301 Availability Zone: ap-south-1a IP addresses available: 251 CIDR: 10.0.4.0/24

Auto-assign public IP Info
Disable

Firewall (security groups) Info
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group Select existing security group

Security group name - required
launch-wizard-5

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and ._-:/()#,@[]+=;&;!\$*

Description - required Info
launch-wizard-5 created 2023-10-28T13:12:43.479Z

15. Similarly create another private Instance(created two instances)

The screenshot shows the 'Instances' list with four entries. The first two instances, 'private_01' and 'private_02', are highlighted with a red border. The table columns include Name, Instance ID, Instance state, Instance type, Status check, Alarm status, Availability Zone, and Public IPv4.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4
<input type="checkbox"/> Find Instance by attribute or tag (case-sensitive)							
<input type="checkbox"/> private_01	i-004f53e19155e1649	Running	t2.micro	2/2 checks passed	No alarms	ap-south-1a	-
<input type="checkbox"/> private_02	i-0932ec2bc487a717	Running	t2.micro	Initializing	No alarms	ap-south-1a	-

16. Your Instances will be successfully running but you cannot access them since it is a private instance.(we cant access)

```
base ~/Desktop/ssh-keys  
ssh -i "public_instance.pem" ec2-user@10.0.3.56
```

Method 2 to connect private instance

Docx to refer :: 1 <https://aws.amazon.com/blogs/compute/secure-connectivity-from-public-to-private-introducing-ec2-instance-connect-endpoint-june-13-2023/>

Video : https://www.youtube.com/watch?v=CN-_Y3uqC44&list=PPSV

Docx to refer :: 2 <https://bobbyhadz.com/blog/aws-cli-could-not-connect-to-endpoint-url>

Docx to refer :: 2 <https://docs.aws.amazon.com/cli/latest/userguide/cli-authentication-user.html#cli-authentication-user-create>

vpc-006f7f751f903aabf / project-vpc

Details **Info**

VPC ID vpc-006f7f751f903aabf	State Available	DNS hostnames Enabled	DNS resolution Enabled
Tenancy Default	DHCP option set dopt-0ef58e43ff0c9a11	Main route table rtb-0d46f78668f047f68	Main network ACL acl-0d8c503c81533aabf
Default VPC No	IPv4 CIDR 10.0.0.0/16	IPv6 pool -	IPv6 CIDR (Network border group) -
Network Address Usage metrics Disabled	Route 53 Resolver DNS Firewall rule groups -	Owner ID 405819896469	

Resource map [New](#) [CIDRs](#) [Flow logs](#) [Tags](#) [Integrations](#)

Resource map **Info**

Was the resource map helpful today?
Give us feedback as often as possible. We are improving continually.

Details

Subnet ID subnet-02b4f902e82c572bd	Subnet ARN arn:aws:ec2:ap-south-1:405819896469:subnet/subnet-02b4f902e82c572bd	State Available	IPv4 CIDR 10.0.144.0/20
Available IPv4 addresses 4090		Availability Zone ap-south-1b	Availability Zone ID aps1-az3
Network border group ap-south-1		Route table rtb-084db2cdd7dec84af project-rtb-private2-ap-south-1b	Network ACL acl-0d8c503c81533aabf
Default subnet No		Auto-assign IPv6 address No	Auto-assign customer-owned IPv4 address No
Customer-owned IPv4 pool -		IPv4 CIDR reservations -	IPv6 CIDR reservations -
IPv6-only No		Resource name DNS AAAA record Disabled	Resource name DNS AAAA record Disabled
DNS64 Disabled			

Flow logs [Route table](#) [Network ACL](#) [CIDR reservations](#) [Sharing](#) [Tags](#)

Flow logs

Name	Flow log ID	Filter	Destination type	Destination name	IAM role ARN
No flow logs found in this Region					

VPC > Route tables > rtb-0e4a7f2d1cbe87db7

rtb-0e4a7f2d1cbe87db7 / project-rtb-private1-ap-south-1a

Actions ▾

Details		Info	
Route table ID rtb-0e4a7f2d1cbe87db7	Main No	Explicit subnet associations subnet-0de8811713f71127c / project-subnet-private1-ap-south-1a	Edge associations -
VPC vpc-006f7f751f903aabf project-vpc	Owner ID 405819896469		

Routes | Subnet associations | Edge associations | **Route propagation** | Tags

Routes (2)

Filter routes

Destination	Target	Status	Propagated
pl-78a54011	vpc-0f44962c69f4a0a82	Active	No
10.0.0.0/16	local	Active	No

Security Groups (26) Info

Find resources by attribute or tag

Actions ▾ Export security groups to CSV Create security group

Name	Security group ID	Security group name	VPC ID	Description	Owner
-	sg-0cab4b170231fc155	OpenVPN Access Server (5 Connected ...)	vpc-0e190ca43b317839f	OpenVPN Access Server (5 Connected ...)	4058198964
-	sg-04d1850b57ff020d	launch-wizard-9	vpc-05e7b46b0c143e52b	launch-wizard-9 created 2023-11-06T...	4058198964
-	sg-0800c2a7e136d0008	launch-wizard-1	vpc-0e190ca43b317839f	launch-wizard-1 created 2023-11-02T...	4058198964
-	sg-037f705c1ac976417	launch-wizard-6	vpc-0e190ca43b317839f	launch-wizard-6 created 2023-11-06T...	4058198964
-	sg-0e40e6692d5d47545	launch-wizard-2	vpc-0e190ca43b317839f	launch-wizard-2 created 2023-11-02T...	4058198964
-	sg-0db352cf80f10970b	launch-wizard-3	vpc-0e190ca43b317839f	launch-wizard-3 created 2023-11-02T...	4058198964
-	sg-0344a824061110e7	eic-endpoint-01	vpc-0e190ca43b317839f	create-group-01	4058198964

Connect to instance Info

Connect to your instance i-0884ea2dc8c4f00b3 (ec2-connect) using any of these options

EC2 Instance Connect

Session Manager

SSH client

EC2 serial console

Instance ID

[i-0884ea2dc8c4f00b3 \(ec2-connect\)](#)

Connection Type

Connect using EC2 Instance Connect
Connect using the EC2 Instance Connect browser-based client, with a public IPv4 address.

Connect using EC2 Instance Connect Endpoint
Connect using the EC2 Instance Connect browser-based client, with a private IPv4 address and a VPC endpoint.

Private IP address

10.0.150.20

User name

Enter the user name defined in the AMI used to launch the instance. If you didn't define a custom user name, use the default user name, ec2-user.

ec2-user

Max tunnel duration (seconds)

The maximum allowed duration of the SSH connection. Must comply with the maxTunnelDuration condition (if specified) in the IAM policy.

3600

Min 1 second. Max 3600 seconds (1 hour).

EC2 Instance Connect Endpoint

Only endpoints that have completed the creation process can be selected.

eice-03c9c2c75517a9574



Note: In most cases, the default user name, ec2-user, is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI user name.

Cancel

Connect

```
test.py 5 Untitled-1
1
2
3
4 ssh -i key.pem ec2-user@i-0884ea2dc8c4f00b3
5
6
7 ssh ec2-user@i-0884ea2dc8c4f00b3 \
8   -i key.pem \
9   -o ProxyCommand='aws ec2-instance-connect open-tunnel \
10   --instance-id %h'
11
12
13 aws ec2-instance-connect ssh --instance-id i-0884ea2dc8c4f00b3
14
15
16 aws ec2 create-instance-connect-endpoint \
17   --subnet-id subnet-02b4f902e82c572bd \
18   --security-group-id sg-0ec4772cfb46c3508
19
20
21 aws ec2-instance-connect ssh --instance-id i-0884ea2dc8c4f00b3
```

```
"ProductCodes": []},  
$ kartikhegadi@Kartiks-MacBook-Air aws.02 % aws ec2-instance-connect ssh --instance-id i-0884ea2dc8c4f00b3  
The authenticity of host '10.0.150.20 (<no hostip for proxy command>)' can't be established.  
ED25519 key fingerprint is SHA256:q4m4owrk4DUwOHHtM0yLTFD9wFKYd99ky2m57plLvT4.  
This key is not known by any other names  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '10.0.150.20' (ED25519) to the list of known hosts.  
Last login: Fri Nov 10 14:26:35 2023 from ip-10-0-142-226.ap-south-1.compute.internal  
.      #  
~\_ ##### Amazon Linux 2  
~~ \_\#\#\#\_\#  
~~ \#\#\#\| AL2 End of Life is 2025-06-30.  
~~ \#/ \#\#\#\_\#  
~~ V~,\_\_> / A newer version of Amazon Linux is available!  
~~ ._. / /  
~/m/\_\_ / Amazon Linux 2023, GA and supported until 2028-03-15.  
https://aws.amazon.com/linux/amazon-linux-2023/  
[ec2-user@ip-10-0-150-20 ~]$
```