

# **Cloud Security and Management Assignment-1**

**Name :- Maanav Singh**

**Batch :- 3 (CCVT)**

**SAP ID :- 500108304**

**Enrollment no. :-R2142220977**

**Faculty :- Dr. Avita Katal**

**Objective:- This assignment focuses on understanding and configuring a Virtual Private Cloud (VPC) in a cloud environment, with both theoretical concepts and practical implementation using a cloud platform like AWS.**

### **Part 1: Theoretical Assignment**

#### **Questions:**

- 1. Define VPC and explain its concept in detail.**
- 2. Discuss the benefits of using VPCs in cloud computing.**
- 3. Describe the key components of a VPC. Include Subnets, Route Tables, Internet Gateway, NAT Gateway, and Security Groups.**
- 4. Compare VPC with traditional on-premises networking.**
- 5. Explain how VPC differs from traditional LANs and VPNs.**
- 6. What is the significance of subnets in a VPC?**
- 7. Discuss the difference between public and private subnets.**
- 8. Explain the role of Security Groups and Network Access Control Lists (NACLs) in securing a VPC. Compare and contrast Security Groups and NACLs.**
- 9. Explain why a NAT Gateway is necessary and where it is typically used in a VPC architecture. How does a NAT Gateway work in a VPC?**
- 10. Describe the process of peering two VPCs, its use cases, and potential challenges?**

Name → Maanav Singh  
SAPID → 500108304

M	T	W	T	F	S	S
Page No.	YOUVA					
Date:						

Q-1 Define VPC and explain its concept in detail.

→ A Virtual Private Cloud (VPC) is a logically isolated section of the cloud, such as AWS, where you can launch instance resources like EC2 instances in a virtual network. You have complete control over your VPC, including IP address ranges, subnets, route tables, and internet gateways. VPCs allow organizations to simulate the experience of having a private, on-premises network while utilizing cloud infrastructure. This concept enables users to securely connect their cloud resources to the internet, other VPCs, or on-premises data centers.

Q-2 Discuss the benefits of using VPCs in cloud computing.

- The key benefits of using VPCs include :-
- Isolation → Logical separation from other virtual networks ensures data privacy.
  - Security → Users can configure security measures like security groups and NACLs.
  - Flexibility → VPC allows users to customize IP ranges, subnets and routing rules.
  - Scalability → Cloud-based VPCs can scale on demand without physical hardware limits.
  - Hybrid connectivity → VPCs can connect with on-premises data centers through VPNs or Direct Connect.

Q-3 Describe the key components of a VPC.

- Key components of a VPC include :-
- Subnets → Logical subdivisions of the VPC network. Subnets can be public or private, with resources deployed in different subnets based on accessibility.

- Route Tables → Define rules that control how traffic is directed within the VPC. Each subnet is associated with a route table.
- Internet Gateway → Enables communication between instances in the VPC and the internet.
- NAT Gateway → Allows instances in a private subnet to access the internet without exposing them to inbound traffic.
- Security Groups → Stateful firewalls that control inbound and outbound traffic to and from resources like EC2 instances.

Q-4 Compare VPC with traditional on-premises networking.

- VPCs are similar to on-premises networks but hosted in the cloud. In traditional on-premises networks :-
- Infrastructure Management → you manage all physical devices, such as routers and switches, whereas in a VPC, this infrastructure is total virtual and managed by cloud provider.
- Scalability → On-premises networks have limited scalability based on hardware, while VPCs can easily scale in the cloud.
- Cost → On-premises requires up-front capital investment, while VPCs are more cost-effective with a pay-as-you-go model.

Q-5 Explain how VPC differs from traditional LANs and VPNs.

- • VPC v/s LANs → While both provide network segmentation, VPCs are virtual networks within the cloud, whereas LANs are physical networks confined to a specific location.

- VPC v/s VPNs → VPNs are secure, encrypted connections between two networks (e.g. a corporate LAN and the cloud). VPCs are complete cloud-based virtual networks with their own components like subnets and route tables.

Q-6 What is the significance of subnets in a VPC?

- Subnets divide the VPC's IP address range into smaller segments, allowing you to group resources based on security or accessibility needs. Subnets enable logical separation of resources (e.g. web servers in public subnets and databases in private subnets) and control traffic flow.

Q-7 Discuss the difference between public and private subnets.

- Public Subnets → Resources in public subnets have direct access to the internet via an Internet Gateway. Typically used for public-facing resources like web servers.
- Private Subnets → Resources in private subnets do not have direct internet access. They use a NAT gateway for outbound communication while remaining inaccessible from the internet.

Q-8 Explain the role of Security Groups and Network Access Control Lists (NACLs) in securing a VPC. Compare and contrast Security Groups and NACLs.

- Security Groups → Act as stateful firewalls controlling inbound and outbound traffic to instances. They remember outgoing requests, allowing return traffic automatically.
- NACLs → Stateless firewalls that control traffic at the subnet level. They check every request individually for both inbound and outbound rules.

### Comparison

- Scope → Security Groups are applied at the instance level, while NACLs operate at the subnet level.
- Statefulness → Security Groups are stateful, while NACLs are stateless.
- Rules → Security Groups only allow "allow" rules, whereas NACLs allow both "allow" and "deny" rules.

Q-9 Explain why a NAT gateway is necessary and where it is typically used in a VPC architecture. How does NAT gateway work in VPC?

- A NAT gateway is necessary to allow instances in private subnets to access the internet (e.g. for software updates) while preventing inbound internet traffic. It works by translating private IP addresses to public IP addresses for outbound traffic and then translating the responses back. NAT gateways are usually placed in public subnets, and private subnets route internet-bound traffic through them.

Q-10 Describe the process of peering two VPCs, its use cases, and potential challenges.

- VPC peering allows two VPCs to communicate privately without routing traffic through the internet.

The process involves :-

- 1) Creating a VPC peering connection request from one VPC to another.
- 2) Accepting the peering request in the target VPC.
- 3) Updating the route tables in both VPCs to enable communication.

Use cases include inter-region data transfer, multi-VPC architectures, and microservices.

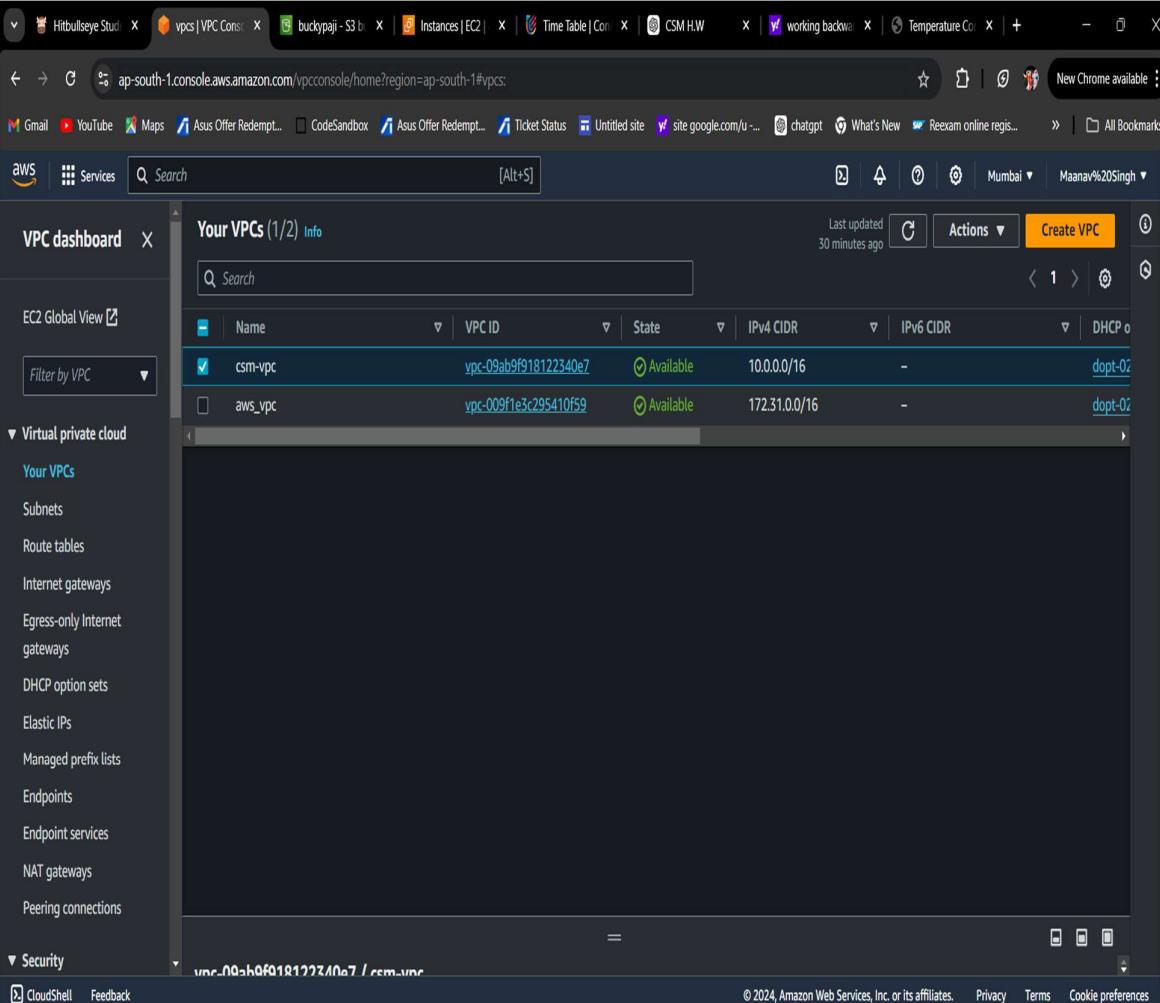
Challenges include managing route tables and ensuring IP address ranges do not overlap, as overlapping IP ranges prevent successful peering.

## Part 2: Practical Assignment

**Objective:** To provide hands-on experience in setting up and configuring a Virtual Private Cloud (VPC) on a cloud platform (AWS)

**Task: 1. You will create and configure a VPC with the following specifications:**

- Create a VPC with a custom IP address range.
- Use the CIDR block: 10.0.0.0/16.



The screenshot shows the AWS VPC Dashboard. On the left, there's a sidebar with options like EC2 Global View, Filter by VPC, Virtual private cloud (with sub-options: Your VPCs, Subnets, Route tables, Internet gateways, Egress-only Internet gateways, DHCP option sets, Elastic IPs, Managed prefix lists, Endpoints, Endpoint services, NAT gateways, Peering connections), Security, CloudShell, and Feedback. The main area is titled "Your VPCs (1/2) Info" and displays a table with two rows of VPC information. The columns are: Name, VPC ID, State, IPv4 CIDR, IPv6 CIDR, and DHCP option set. The first VPC, "csm-vpc", has an IPv4 CIDR of 10.0.0.0/16 and a DHCP option set of "dopt-02". The second VPC, "aws\_vpc", has an IPv4 CIDR of 172.31.0.0/16 and a DHCP option set of "dopt-02". The table also includes a "Actions" button and a "Create VPC" button.

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP option set
csm-vpc	vpc-09ab9f918122340e7	Available	10.0.0.0/16	-	dopt-02
aws_vpc	vpc-009f1e3c295410f59	Available	172.31.0.0/16	-	dopt-02

VPC dashboard > [VPC](#) > [Your VPCs](#) > [vpc-09ab9f918122340e7 / csm-vpc](#)

[Actions](#)

Details		Info	
VPC ID	vpc-09ab9f918122340e7	State	Available
Tenancy	Default	DNS hostnames	Disabled
Default VPC	No	Main route table	rtb-0b0eb1fb9d6a5c203
Egress-only Internet gateways		IPv6 pool	-
DHCP option sets	Disabled	Route 53 Resolver DNS Firewall rule groups	Owner ID 654654341426
Elastic IPs			
Managed prefix lists			
Endpoints			
Endpoint services			
NAT gateways			
Peering connections			
Security			

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

**Resource map** [Info](#)

[VPC Show details](#) [Subnets \(2\)](#) [Route tables \(3\)](#) [Network interfaces \(0\)](#)

© 2024, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

VPC dashboard > [VPC](#) > [Your VPCs](#) > [vpc-09ab9f918122340e7 / csm-vpc](#)

[Actions](#)

Default		rtb-0b0eb1fb9d6a5c203	
Default VPC	No	IPv4 CIDR	10.0.0.16
Network Address Usage metrics	Disabled	Route 53 Resolver DNS Firewall rule groups	Owner ID 654654341426

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

**Resource map** [Info](#)

[VPC Show details](#) [Subnets \(2\)](#) [Route tables \(3\)](#) [Network interfaces \(0\)](#)

Your AWS virtual network  
csm-vpc

**Subnets (2)** Subnets within this VPC  
ap-south-1a  
csm-public-subnet  
csm-private-subnet

**Route tables (3)** Route network traffic to resources  
rtb-0b0eb1fb9d6a5c203  
csm-private-rt  
csm-public-rt  
csm-private-n

**Network interfaces (0)** igw-csm  
csm-private-n

© 2024, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

## 2. Create subnets:

- Create one public subnet in Availability Zone A with CIDR 10.0.1.0/24.
- Create one private subnet in Availability Zone A with CIDR 10.0.2.0/24.

The screenshot shows the AWS VPC Subnets list page. The table displays the following information:

Name	Subnet ID	State	VPC	IPv4 CIDR
-	subnet-0a17bf4d55e8147e5	Available	vpc-009f1e3c295410f59   aws...	172.31.32.0/20
-	subnet-0153ffbb3ac0854dd	Available	vpc-009f1e3c295410f59   aws...	172.31.16.0/20
-	subnet-0db309ce8e28fe3e	Available	vpc-009f1e3c295410f59   aws...	172.31.0.0/20
csm-public-subnet	subnet-00da190102bd11ecd	Available	vpc-09ab9f918122340e7   csm...	10.0.1.0/24
csm-private-subnet	subnet-0c4f4591717ed5af9	Available	vpc-09ab9f918122340e7   csm...	10.0.2.0/24

The screenshot shows the AWS VPC Subnet details page for subnet-00da190102bd11ecd. The table displays the following configuration:

Details			
Subnet ID subnet-00da190102bd11ecd	Subnet ARN arn:aws:ec2:ap-south-1:654654341426:subnet/subnet-00da190102bd11ecd	State Available	IPv4 CIDR 10.0.1.0/24
Available IPv4 addresses 249	IPv6 CIDR -	IPv6 CIDR association ID -	Availability Zone ap-south-1a
Availability Zone ID aps1-az1	Network border group ap-south-1	VPC vpc-09ab9f918122340e7   csm-vpc	Route table rtb-0b7c8d78cd037fb7   csm-public-rt
Network ACL acl-0f5ed5bd82e2ab700	Default subnet No	Auto-assign public IPv4 address No	Auto-assign IPv6 address No
Auto-assign customer-owned IPv4 address No	Customer-owned IPv4 pool -	Outpost ID -	IPv4 CIDR reservations -
IPv6 CIDR reservations -	IPv6-only No	Hostname type IP name	Resource name DNS A record Disabled
Resource name DNS AAAA record Disabled	DNS64 Disabled	Owner 654654341426	

Hitbullseye Stud | SubnetDetails | buckypaji - S3 b | Instances | EC2 | Time Table | Com | CSM H.W | working backw | Temperature Co | +

Gmail YouTube Maps Asus Offer Redempt... CodeSandbox Asus Offer Redempt... Ticket Status Untitled site site google.com/u ... chatgpt What's New Reexam online regis... All Bookmarks

aws Services Search [Alt+S]

VPC dashboard ×

EC2 Global View Filter by VPC

Virtual private cloud Your VPCs Subnets Route tables Internet gateways Egress-only Internet gateways DHCP option sets Elastic IPs Managed prefix lists Endpoints Endpoint services NAT gateways Peering connections Security CloudShell Feedback

Network ACL **acl-0f5ed5bd82e2ab700**

Auto-assign customer-owned IPv4 address No

IPv6 CIDR reservations -

Resource name DNS AAAA record Disabled

Network border group **ap-south-1**

Default subnet No

Customer-owned IPv4 pool -

IPv6-only No

DNS64 Disabled

Auto-assign public IPv4 address No

Outpost ID -

Customer-owned IPv4 pool -

IPV6-only No

DNS64 Disabled

Auto-assign IPv6 address No

IPv4 CIDR reservations -

Hostname type IP name

Owner 654654341426

Auto-assign public IPv4 address No

Outpost ID -

Hostname type IP name

Owner 654654341426

Auto-assign IPv6 address No

IPv4 CIDR reservations -

Resource name DNS A record Disabled

Flow logs Route table Network ACL CIDR reservations Sharing Tags

Route table: **rtb-0b7c8d78cd037fbf7 / csm-public-rt** Edit route table association

Routes (2) Filter routes

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	<a href="#">igw-0f4e1b4bdfbe1c5a7</a>

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

This screenshot shows the Route table section of the AWS VPC console. It displays two routes: one for the local network (10.0.0.0/16) and one pointing to the internet gateway (igw-0f4e1b4bdfbe1c5a7). The interface includes tabs for Flow logs, Route table, Network ACL, CIDR reservations, Sharing, and Tags.

Hitbullseye Stud | SubnetDetails | buckypaji - S3 b | Instances | EC2 | Time Table | Com | CSM H.W | working backw | Temperature Co | +

Gmail YouTube Maps Asus Offer Redempt... CodeSandbox Asus Offer Redempt... Ticket Status Untitled site site google.com/u ... chatgpt What's New Reexam online regis... All Bookmarks

aws Services Search [Alt+S]

VPC dashboard ×

VPC > Subnets > **subnet-0c4f4591717ed5af**

Actions

subnet-0c4f4591717ed5af / csm-private-subnet

Details

Subnet ID **subnet-0c4f4591717ed5af**

Available IPv4 addresses 250

Availability Zone ID **aps1-a21**

Network ACL **acl-0f5ed5bd82e2ab700**

Auto-assign customer-owned IPv4 address No

IPv6 CIDR reservations -

Resource name DNS AAAA record Disabled

Subnet ARN **arn:aws:ec2:ap-south-1:654654341426:subnet/subnet-0c4f4591717ed5af**

IPv6 CIDR -

IPv6-only No

DNS64 Disabled

State Available

IPv6 CIDR association ID -

IPV6-only No

Outpost ID -

Customer-owned IPv4 pool -

IPV6-only No

Owner 654654341426

Auto-assign public IPv4 address No

Default subnet No

Customer-owned IPv4 pool -

IPV6-only No

Hostname type IP name

Owner 654654341426

Auto-assign IPv6 address No

Outpost ID -

Customer-owned IPv4 pool -

IPV6-only No

Hostname type IP name

Owner 654654341426

Auto-assign public IPv4 address No

IPv4 CIDR 10.0.2.0/24

Availability Zone ap-south-1a

Route table **rtb-027acce95d47f5dcc / csm-private-rt**

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

This screenshot shows the Details section of the AWS VPC Subnet configuration for subnet-0c4f4591717ed5af. It lists various subnet settings like subnet ID, availability zone, and network ACL, along with their corresponding ARNs and state. It also shows the associated route table (rtb-027acce95d47f5dcc).

**VPC dashboard**

**Subnets**

**Route table**

**Route table:** rtb-027acce95d47f5dcc / csm-private-rt

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	nat-09a89fe349aa4df27

## Creating Route Tables for both subnets.

**Route tables (2/4) Info**

Name	Route table ID	Explicit subnet associations	Edge associations	Main	VPC
-	rtb-0426fab6f79133c09	-	-	Yes	vpc-009f1e5c295410f59
csm-private-rt	rtb-027acce95d47f5dcc	subnet-0c4f4591717ed5...	-	No	vpc-09ab9f918122340e7
csm-public-rt	rtb-0b7c8d78cd037fb7	subnet-00da190102bd11...	-	No	vpc-09ab9f918122340e7
-	rtb-0b0eb1fb9d6a5c203	-	-	Yes	vpc-09ab9f918122340e7

RouteTableDetail x buckypaji - S3 b x Instances | EC2 | x Time Table | Con x CSM H.W x working backwa x Temperature Co x +

Gmail YouTube Maps Asus Offer Redempt... CodeSandbox Asus Offer Redempt... Ticket Status Untitled site site google.com/u ... chatgpt What's New Reexam online regis... All Bookmarks

aws Services Search [Alt+S]

VPC dashboard > VPC > Route tables > rtb-027acce95d47f5dcc / csm-private-rt

rtb-027acce95d47f5dcc / csm-private-rt

Details Info

Route table ID	Main	Explicit subnet associations	Edge associations
rtb-027acce95d47f5dcc	No	subnet-0c4f4591717ed5af / csm-private-subnet	-
VPC	Owner ID		
vpc-09ab9f918122340e7   csm-vpc	654654341426		

Routes Subnet associations Edge associations Route propagation Tags

Routes (2)

Destination	Target	Status	Propagated
0.0.0.0	nat-09a89fe349aa4df27	Active	No
10.0.0.16	local	Active	No

Both Edit routes < 1 > @

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

CloudShell Feedback

RouteTableDetail x buckypaji - S3 b x Instances | EC2 | x Time Table | Con x CSM H.W x working backwa x Temperature Co x +

Gmail YouTube Maps Asus Offer Redempt... CodeSandbox Asus Offer Redempt... Ticket Status Untitled site site google.com/u ... chatgpt What's New Reexam online regis... All Bookmarks

aws Services Search [Alt+S]

VPC dashboard > VPC > Route tables > rtb-027acce95d47f5dcc

rtb-027acce95d47f5dcc / csm-private-rt

Actions

Details Info

Route table ID	Main	Explicit subnet associations	Edge associations
rtb-027acce95d47f5dcc	No	subnet-0c4f4591717ed5af / csm-private-subnet	-
VPC	Owner ID		
vpc-09ab9f918122340e7   csm-vpc	654654341426		

Routes Subnet associations Edge associations Route propagation Tags

Explicit subnet associations (1)

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
csm-private-subnet	subnet-0c4f4591717ed5af	10.0.2.0/24	-

Edit subnet associations < 1 > @

Subnets without explicit associations (0)

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

Find subnet association
-------------------------

Edit subnet associations < 1 > @

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

CloudShell Feedback

Hitbullseye Studi X RouteTableDetail X buckypaji - S3 b X Instances | EC2 | X Time Table | Con X CSM H.W X working backwa X Temperature Co X +

Gmail YouTube Maps Asus Offer Redempt... CodeSandbox Asus Offer Redempt... Ticket Status Untitled site site google.com/u ... chatgpt What's New Reexam online regis... All Bookmarks

aws Services Search [Alt+S]

VPC dashboard > VPC > Route tables > rtb-0b7c8d78cd037fbf7 / csm-public-rt Actions

Details Info

Route table ID rtb-0b7c8d78cd037fbf7	Main No	Explicit subnet associations subnet-00da190102bd11ecd / csm-public-subnet	Edge associations -
VPC vpc-09ab9f918122340e7   csm-vpc	Owner ID 654654341426		

Routes Subnet associations Edge associations Route propagation Tags

Routes (2) Both Edit routes

Destination	Target	Status	Propagated
0.0.0.0/0	igw-0f4e1b4bdfeb1c5a7	Active	No
10.0.0.16	local	Active	No

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

This screenshot shows the AWS VPC Route Table Details page for route table ID rtb-0b7c8d78cd037fbf7. The 'Details' tab is selected, displaying basic information like the route table ID, main status (No), explicit subnet associations (subnet-00da190102bd11ecd / csm-public-subnet), and edge associations (-). The 'Routes' tab is also visible, showing two routes: one to igw-0f4e1b4bdfeb1c5a7 (Status: Active, Propagated: No) and one to local (Status: Active, Propagated: No).

Hitbullseye Studi X RouteTableDetail X buckypaji - S3 b X Instances | EC2 | X Time Table | Con X CSM H.W X working backwa X Temperature Co X +

Gmail YouTube Maps Asus Offer Redempt... CodeSandbox Asus Offer Redempt... Ticket Status Untitled site site google.com/u ... chatgpt What's New Reexam online regis... All Bookmarks

aws Services Search [Alt+S]

VPC dashboard > VPC > Route tables > rtb-0b7c8d78cd037fbf7 / csm-public-rt Actions

Details Info

Route table ID rtb-0b7c8d78cd037fbf7	Main No	Explicit subnet associations subnet-00da190102bd11ecd / csm-public-subnet	Edge associations -
VPC vpc-09ab9f918122340e7   csm-vpc	Owner ID 654654341426		

Routes Subnet associations Edge associations Route propagation Tags

Explicit subnet associations (1) Edit subnet associations

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
csm-public-subnet	subnet-00da190102bd11ecd	10.0.1.0/24	-

Subnets without explicit associations (0) Edit subnet associations

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

Find subnet association
-------------------------

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

This screenshot shows the AWS VPC Route Table Details page for route table ID rtb-0b7c8d78cd037fbf7. The 'Subnet associations' tab is selected, displaying one explicit subnet association: csm-public-subnet (Subnet ID: subnet-00da190102bd11ecd, IPv4 CIDR: 10.0.1.0/24). The 'Explicit subnet associations' section shows this association with an 'Edit subnet associations' button. The 'Subnets without explicit associations' section indicates there are none.

### 3. Internet Gateway: Attach an Internet Gateway to the VPC.

- Configure the public subnet to route traffic to the Internet Gateway.

The screenshot shows the AWS VPC dashboard with the 'Internet gateways' section selected. A table lists one internet gateway:

Name	Internet gateway ID	State	VPC ID	Owner
igw-csm	igw-0f4e1b4bdfeb1c5a7	Attached	vpc-09ab9f918122340e7   csm-vpc	654654341426

The screenshot shows the details page for the attached internet gateway 'igw-0f4e1b4bdfeb1c5a7'. The 'Details' tab is selected, showing the following information:

Internet gateway ID	State	VPC ID	Owner
igw-0f4e1b4bdfeb1c5a7	Attached	vpc-09ab9f918122340e7   csm-vpc	654654341426

The 'Tags' section shows a single tag: Name = igw-csm.

## 4. NAT Gateway: Set up a NAT Gateway in the public subnet.

- **Modify the route table of the private subnet to allow instances in the private subnet to access the internet via the NAT Gateway.**

The screenshot shows the AWS VPC dashboard with the 'NAT gateways' section selected. A single NAT gateway named 'csm-private-nat' is listed. The table includes columns for Name, NAT gateway ID, Connectivity type, State, Primary public IPv4 address, and Primary private IPv4 address. The gateway is marked as 'Available' with a green status icon.

Name	NAT gateway ID	Connectivity...	State	Primary public I...	Primary priva...
csm-private-nat	nat-09a89fe349aa4df27	Public	Available	13.201.217.248	10.0.1.141

The screenshot shows the detailed view of the NAT gateway 'nat-09a89fe349aa4df27'. The 'Details' tab is selected, displaying information such as the NAT gateway ID, ARN, connectivity type (Public), state (Available), and primary network interface ID. The 'Secondary IPv4 addresses' tab is also visible at the bottom.

NAT gateway ID	Connectivity type	State	State message
nat-09a89fe349aa4df27	Public	Available	Info

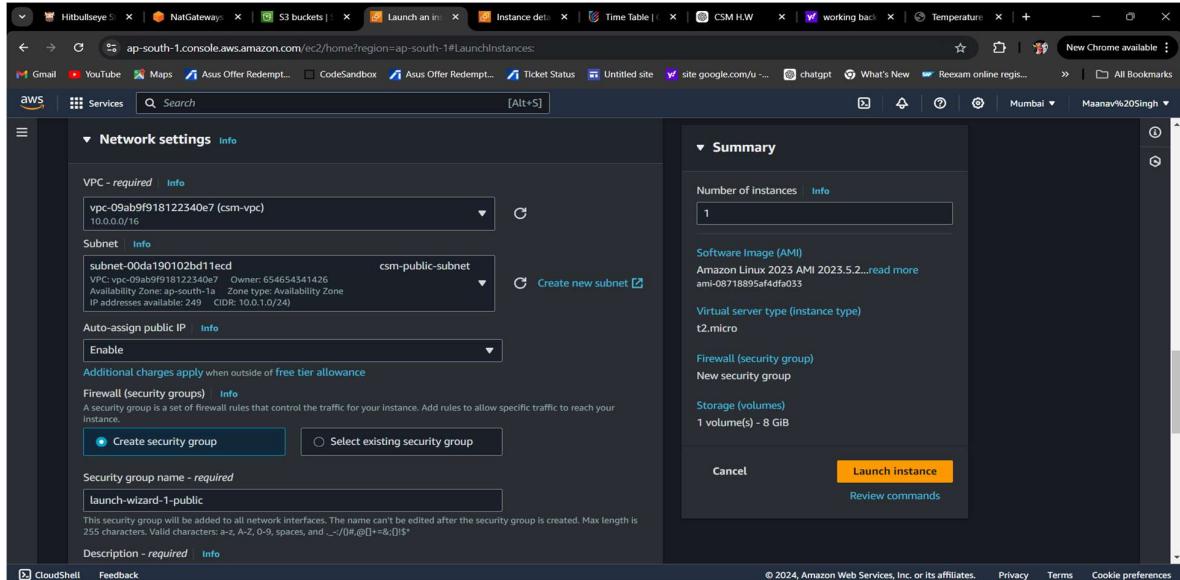
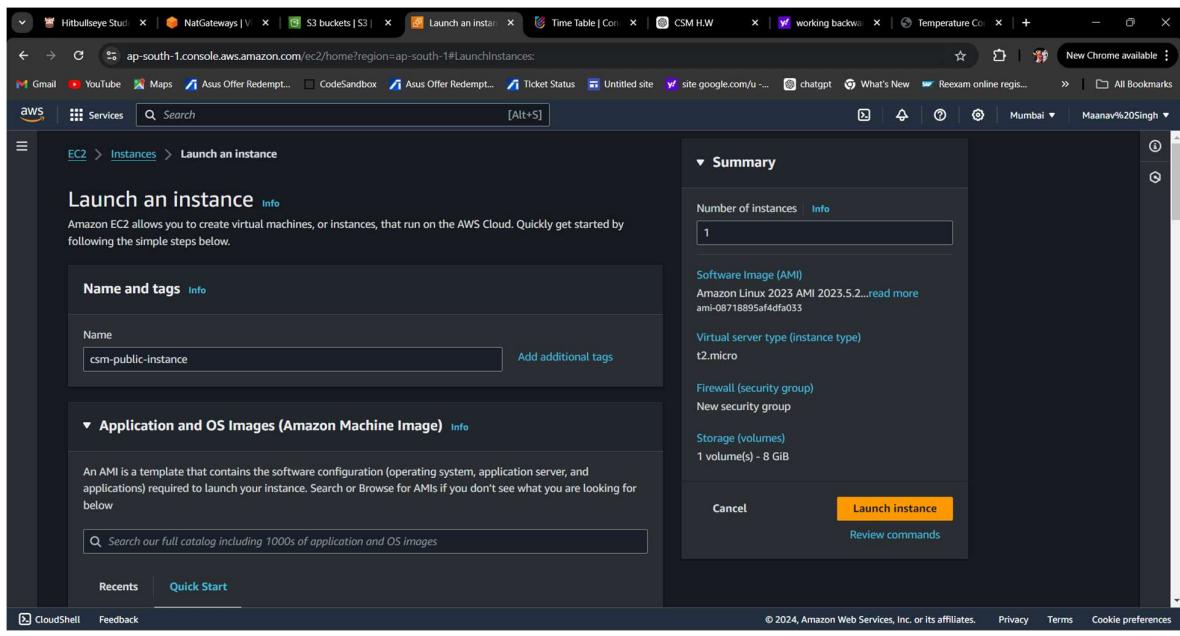
# Creating S3 for Testing Connectivity for public instance using SSH

The screenshot shows the AWS S3 service page. In the top navigation bar, the URL is `ap-south-1.console.aws.amazon.com/s3/buckets?region=ap-south-1&bucketType=general&region=ap-south-1`. The main heading is "Amazon S3 > Buckets". Below it, there's an "Account snapshot - updated every 24 hours" section and a "View Storage Lens dashboard" button. Under "General purpose buckets", there is one entry: "buckypaji" (Info, All AWS Regions). The table shows columns for Name, AWS Region, IAM Access Analyzer, and Creation date. The "buckypaji" row has a "Copy ARN" button. At the bottom right of the table, there are buttons for "Create bucket", "Empty", and "Delete". The footer includes links for CloudShell, Feedback, and copyright information: "© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences".

The screenshot shows the contents of the "buckypaji" bucket. The URL is `ap-south-1.console.aws.amazon.com/s3/buckets/buckypaji?region=ap-south-1&bucketType=general&tab=objects`. The left sidebar has sections for Buckets, Access Grants, Access Points, Object Lambda Access Points, Multi-Region Access Points, Batch Operations, IAM Access Analyzer for S3, Block Public Access settings for this account, Storage Lens, Dashboards, Storage Lens groups, AWS Organizations settings, and Feature spotlight (7). The main area shows the "buckypaji" bucket details with tabs for Objects, Properties, Permissions, Metrics, Management, and Access Points. The "Objects" tab is selected, showing one object: "AWS Website Project.zip" (Info). The table lists the object with columns for Name, Type, Last modified, Size, and Storage class. The "Actions" button is highlighted in orange. The footer includes links for CloudShell, Feedback, and copyright information: "© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences".

## 5. Launch EC2 instances (or similar on other platforms):

- Launch one instance in the public subnet and one instance in the private subnet.
- Ensure the public instance can be accessed from the internet using an Elastic IP.
- Ensure the private instance can access the internet but cannot be accessed directly from the internet.



The screenshot shows the AWS EC2 Launch Instances wizard. On the left, under 'Inbound Security Group Rules', two rules are defined:

- Security group rule 1 (TCP, 22, 0.0.0.0/0)**: Type: ssh, Protocol: TCP, Port range: 22. Source type: Anywhere. Description: e.g. SSH for admin desktop.
- Security group rule 2 (TCP, 0, 10.0.2.237)**: Type: Custom TCP, Protocol: TCP, Port range: 0. Source type: Custom. Description: e.g. SSH for admin desktop.

A warning message at the bottom states: "⚠️ 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." On the right, the 'Summary' section shows:

- Number of instances: 1
- Software Image (AMI): Amazon Linux 2023 AMI 2023.5.2... (ami-08718895af4df0a033)
- Virtual server type (instance type): t2.micro
- Firewall (security group): New security group
- Storage (volumes): 1 volume(s) - 8 GiB

At the bottom right are 'Cancel', 'Launch instance' (highlighted in orange), and 'Review commands' buttons.

The screenshot shows the AWS EC2 Launch Instances wizard. The current step is 'Launch an instance'. The 'Name and tags' section shows a name 'private\_instance' and a 'Search our full catalog including 1000s of application and OS images' input field.

The 'Application and OS Images (Amazon Machine Image)' section provides information about AMIs and includes a search bar: "Search our full catalog including 1000s of application and OS images".

The 'Summary' section on the right is identical to the one in the previous screenshot, showing:

- Number of instances: 1
- Software Image (AMI): Amazon Linux 2023 AMI 2023.5.2... (ami-08718895af4df0a033)
- Virtual server type (instance type): t2.micro
- Firewall (security group): New security group
- Storage (volumes): 1 volume(s) - 8 GiB

At the bottom right are 'Cancel', 'Launch instance' (highlighted in orange), and 'Review commands' buttons.

The screenshot shows the AWS EC2 Launch Instances wizard. On the left, under 'Network settings', the 'Subnet' dropdown is set to 'csm-private-subnet'. Below it, the 'Auto-assign public IP' dropdown is set to 'Disable'. On the right, the 'Summary' panel shows 'Number of instances' as 1, 'Software Image (AMI)' as Amazon Linux 2023 AMI 2023.5.2..., 'Virtual server type (instance type)' as t2.micro, and 'Storage (volumes)' as 1 volume(s) - 8 GiB. At the bottom right are 'Cancel', 'Launch instance', and 'Review commands' buttons.

The screenshot shows the AWS EC2 Launch Instances wizard. On the left, under 'Firewall (security groups)', there is a 'Create security group' button. The 'Security group name' field contains 'private\_SG'. Below it, the 'Description' field contains 'launch-wizard-3 created 2024-09-22T08:53:58.383Z'. Under 'Inbound Security Group Rules', there is one rule: 'Security group rule 1 (TCP, 22, 0.0.0.0/0)'. The 'Type' dropdown is 'ssh', 'Protocol' is 'TCP', and 'Port range' is '22'. The 'Source type' dropdown is 'Anywhere'. On the right, the 'Summary' panel shows 'Number of instances' as 1, 'Software Image (AMI)' as Amazon Linux 2023 AMI 2023.5.2..., 'Virtual server type (instance type)' as t2.micro, and 'Storage (volumes)' as 1 volume(s) - 8 GiB. At the bottom right are 'Cancel', 'Launch instance', and 'Review commands' buttons.

EC2 > Instances > i-050e06a78d6663098

Instance summary for i-050e06a78d6663098 (csm-public-instance) [Info](#)

Updated less than a minute ago

Instance ID	Public IPv4 address	Private IPv4 addresses
i-050e06a78d6663098 (csm-public-instance)	15.207.8.172   <a href="#">open address</a>	10.0.1.8
IPv6 address	-	Public IPv4 DNS
Hostname type	Running	-
IP name: ip-10-0-1-8.ap-south-1.compute.internal	Private IP DNS name (IPv4 only)	
Answer private resource DNS name	ip-10-0-1-8.ap-south-1.compute.internal	
-	Instance type	Elastic IP addresses
Auto-assigned IP address	t2.micro	15.207.8.172 (csm-elastic-ip) [Public IP]
-	VPC ID	AWS Compute Optimizer finding
IAM Role	vpc-09ab9f918122340e7 (csm-vpc)	<a href="#">Opt-in to AWS Compute Optimizer for recommendations.</a>
IMDSv2	Subnet ID	<a href="#">Learn more</a>
Required	subnet-00da190102bd11ecd (csm-public-subnet)	Auto Scaling Group name
Instance ARN	-	-
arn:aws:ec2:ap-south-1:654654341426:instance/i-050e06a78d6663098	-	-

© 2024, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

EC2 > Instances > i-050e06a78d6663098

Details [Status and alarms](#) [Monitoring](#) [Security](#) [Networking](#) [Storage](#) [Tags](#)

Instance details [Info](#)

Platform	AMI ID	Monitoring
Amazon Linux (Inferred)	ami-08718895af4dfa033	disabled
Platform details	AMI name	Termination protection
Linux/UNIX	al2023-ami-2023.5.20240916.0-kernel-6.1-x86_64	Disabled
Stop protection	Launch time	AMI location
Disabled	Thu Sep 19 2024 22:02:27 GMT+0530 (India Standard Time) (18 minutes)	amazon/al2023-ami-2023.5.20240916.0-kernel-6.1-x86_64
Instance auto-recovery	Lifecycle	Stop-hibernate behavior
Default	normal	Disabled
AMI Launch index	Key pair assigned at launch	State transition reason
0	test-key	-
Credit specification	Kernel ID	State transition message
standard	-	-
Usage operation	RAM disk ID	Owner
RunInstances	-	654654341426
Enclaves Support	Boot mode	Current instance boot mode
-	uefi-preferred	legacy-bios

© 2024, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

Screenshot of the AWS EC2 Security Details page for instance i-050e06a78d6663098.

**Security details:**

- IAM Role: -
- Owner ID: 654654341426
- Launch time: Sun Sep 22 2024 14:30:49 GMT+0530 (India Standard Time)
- Security groups:
  - sg-026fe98b133190110 (launch-wizard-1-public)

**Inbound rules:**

Name	Security group rule ID	Port range	Protocol	Source	Security group
-	sgr-0083fb8a79f407275	22	TCP	0.0.0.0/0	launch-wiza
-	sgr-06222af7fa64faef4	0	TCP	10.0.2.237/32	launch-wiza
-	sgr-03da90c6602ff5feb	0 - 65535	TCP	12.0.0.0/16	launch-wiza
-	sgr-0089c43d978df6246	80	TCP	0.0.0.0/0	launch-wiza
-	sgr-0dd4e2883b905666c	All	ICMP	12.0.0.0/16	launch-wiza

**Outbound rules:**

Screenshot of the AWS EC2 Instance Summary page for instance i-0f386c2a104e8d0f0.

**Instance summary for i-0f386c2a104e8d0f0 (private\_instance) [Info](#)**

Updated less than a minute ago

Instance ID	Public IPv4 address	Private IPv4 addresses
i-0f386c2a104e8d0f0 (private_instance)	-	10.0.2.237
IPv6 address	Instance state	Public IPv4 DNS
-	Running	-
Hostname type	Private IP DNS name (IPv4 only)	Elastic IP addresses
IP name: ip-10-0-2-237.ap-south-1.compute.internal	ip-10-0-2-237.ap-south-1.compute.internal	-
Answer private resource DNS name	Instance type	AWS Compute Optimizer finding
-	t2.micro	<a href="#">Opt-in to AWS Compute Optimizer for recommendations.</a>
Auto-assigned IP address	VPC ID	<a href="#">Learn more</a>
-	vpc-09ab9f918122340e7 (csm-vpc)	
IAM Role	Subnet ID	Auto Scaling Group name
-	subnet-0c4f4591717ed5af (csm-private-subnet)	-
IMDSv2	Instance ARN	
Required	arn:aws:ec2:ap-south-1:654654341426:instance/i-0f386c2a104e8d0f0	

Screenshot of the AWS EC2 Details page for instance i-0f386c2a104e8d0f0.

**Details Tab:**

Setting	Value	Setting	Value
Platform	Amazon Linux (Inferred)	AMI ID	ami-08718895af4dfa033
Platform details	Linux/UNIX	AMI name	al2023-ami-2023.5.20240916.0-kernel-6.1-x86_64
Stop protection	Disabled	Launch time	Sun Sep 22 2024 14:24:28 GMT+0530 (India Standard Time) (5 minutes)
Instance auto-recovery	Default	Lifecycle	normal
AMI Launch index	0	Key pair assigned at launch	private.pem
Credit specification	standard	Kernel ID	-
AMI Catalog	Usage operation	RAM disk ID	-
Elastic Block Store	RunInstances	Boot mode	uefi-preferred
Volumes	Enclaves Support	Owner	654654341426
Snapshots	-	Current instance boot mode	legacy-bios

**CloudShell:** CloudShell Feedback

**Footer:** © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Screenshot of the AWS EC2 Security tab for instance i-0f386c2a104e8d0f0.

**Security Tab:**

**Security Details:**

Setting	Value
IAM Role	-
Owner ID	654654341426
Launch time	Sun Sep 22 2024 14:24:28 GMT+0530 (India Standard Time)

**Inbound Rules:**

Name	Security group rule ID	Port range	Protocol	Source	Security group
-	sgr-04dcbef2d2b5b14bbe	22	TCP	0.0.0.0/0	private_SG

**Outbound Rules:**

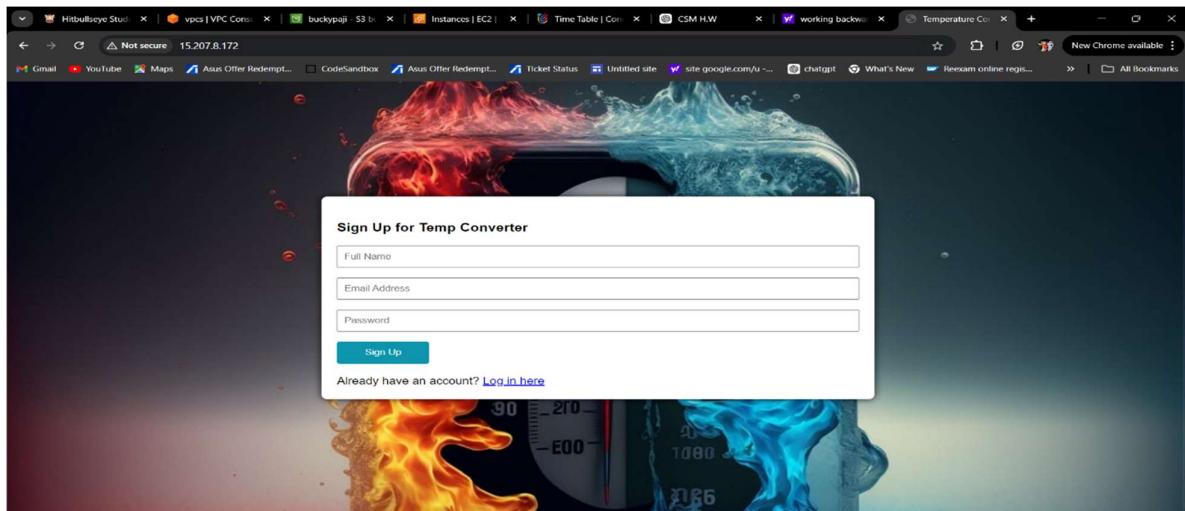
Name	Security group rule ID	Port range	Protocol	Destination	Security group
-	sgr-0785ab829ab920103	All	All	0.0.0.0/0	private_SG

**CloudShell:** CloudShell Feedback

**Footer:** © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

## 7. Test Connectivity: Connect to the public instance using SSH.

- From the public instance, SSH into the private instance using its private IP.



Run commands to check private instance connectivity it is written in screenshot below:

```
Last login: Fri Sep 20 08:39:45 2024 from 13.233.177.5
[ec2-user@ip-10-0-1-8 ~]$ ls
[ec2-user@ip-10-0-1-8 ~]$ vi private.pem
[ec2-user@ip-10-0-1-8 ~]$ chmod 400 private.pem
[ec2-user@ip-10-0-1-8 ~]$ ssh -i ec2-user@10.0.2.237
Warning: Identity file /root/.ssh/ec2-user@10.0.2.237 not accessible: No such file or directory.
usage: ssh [-46AcCfGgKMMngStVxXy] [-B bind_interface]
           [-b bind_address] [-c cipher_spec] [-D [bind_address:]port]
           [-E log_file] [-e escape_char] [-F config_file] [-I pkcs11]
           [-i identity_file] [-J [user@]host[:port]] [-L address]
           [-l login_name] [-m mac_spec] [-O ctl_cmd] [-o option] [-p port]
           [-Q query_option] [-R address] [-S ctl_path] [-W host:port]
           [-w local_tun[:remote_tun]] destination [command]
[ec2-user@ip-10-0-1-8 ~]$ ssh -i private.pem ec2-user@10.0.2.237
The authenticity of host '10.0.2.237 (10.0.2.237)' can't be established.
ED25519 key fingerprint is SHA256:y5ETM020Ab71541bsmejpUjX54dw4tco0CU4uB8.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.237' (ED25519) to the list of known hosts.

#
Amazon Linux 2023

i-050e06a78d6663098 (csm-public-instance)
PublicIPs: 15.207.8.172 PrivateIPs: 10.0.1.8
```

```

ED25519 key fingerprint is SHA256:y5ETM020AB7I541bsmejpL1J+XJ54bdW4tco0CU4ub8.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.237' (ED25519) to the list of known hosts.

,   #
~\  #####
~~ \####\
~~ \###|
~~ \\\| https://aws.amazon.com/linux/amazon-linux-2023
~~ V- ->
~~ / \
~~ / /
/m/` 

[ec2-user@ip-10-0-2-237 ~]$ ssh --help
unknown option -- -
usage: ssh [-4GAcCfGgKMMngsttvXxy] [-B bind_interface]
           [-b bind_address] [-c cipher_spec] [-D [bind_address:]port]
           [-E log_file] [-e escape_char] [-F configfile] [-i pkcs11]
           [-i identity_file] [-J [user@]host[:port]] [-L address]
           [-l login_name] [-m mac_spec] [-O ctl_cmd] [-o option] [-p port]
           [-Q query_option] [-R address] [-S ctl_path] [-W host:port]
           [-w local_tun[:remote_tun]] destination [command]
[ec2-user@ip-10-0-2-237 ~]$ exit
logout
Connection to 10.0.2.237 closed.
[ec2-user@ip-10-0-1-8 ~]$ 

i-050e06a78d6663098 (csm-public-instance)
PublicIP: 15.207.8.172 PrivateIP: 10.0.1.8

```

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

**8. VPC Peering (optional advanced task for bonus marks): If you have created two separate VPCs, peer them and configure the route tables to allow instances in both VPCs to communicate.**

### a) Create 2<sup>nd</sup> VPC.

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP opti
csm-vpc	vpc-09ab9f918122340e7	Available	10.0.0.0/16	-	dopt-02a9
csm-vpc-2	vpc-05625df217ce1cead	Available	12.0.0.0/16	-	dopt-02a9
aws_vpc	vpc-009f1e3c295410f59	Available	172.31.0.0/16	-	dopt-02a9

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Screenshot of the AWS VPC console showing the details of a VPC named 'csm-vpc-2'. The VPC ID is 'vpc-03623df217ce1cead'. The 'Details' tab is selected, displaying information such as State (Available), Tenancy (Default), Default VPC (No), and Network Address Usage metrics (Disabled). The 'Resource map' tab is also visible.

VPC ID: vpc-03623df217ce1cead

State: Available

Tenancy: Default

Default VPC: No

Network Address Usage metrics: Disabled

DNS hostnames: Disabled

Main route table: rtb-0018b8c94adab8304

IPv6 pool: -

Owner ID: 654654341426

DNS resolution: Enabled

Main network ACL: acl-01955c8fc1ac9ef4b

IPv6 CIDR (Network border group): -

Screenshot of the AWS VPC console showing the details of a VPC named 'csm-vpc-2'. The VPC ID is 'vpc-03623df217ce1cead'. The 'Details' tab is selected, displaying information such as State (Available), Tenancy (Default), Default VPC (No), and Network Address Usage metrics (Disabled). The 'Resource map' tab is selected, showing a diagram of the VPC resources.

VPC ID: vpc-03623df217ce1cead

State: Available

Tenancy: Default

Default VPC: No

Network Address Usage metrics: Disabled

Main route table: rtb-0018b8c94adab8304

IPv6 pool: -

Owner ID: 654654341426

Main network ACL: acl-01955c8fc1ac9ef4b

IPv6 CIDR (Network border group): -

**Resource map**

- VPC**: Show details
- Subnets (1)**: Subnets within this VPC
  - ap-south-1a: subnet-vpc-2
- Route tables (2)**: Route network traffic to resources
  - rtb-0018b8c94adab8304
  - csm-rt-vpc-2
- Network con**: Connections to other

## b) create subnet for vpc-2

The screenshot shows the AWS VPC Subnets list page. The left sidebar is the VPC dashboard with a 'Subnets' section selected. The main area displays a table of subnets:

Name	Subnet ID	State	VPC	IPv4 CIDR
subnet-vpc-2	subnet-05bdea4489973755a	Available	vpc-03623df217ce1cead   csm-...	12.0.1.0/24
-	subnet-0a17bf4d35e8147e5	Available	vpc-009f1e5c295410f59   aws...	172.31.32.0/20
-	subnet-0153ffbb3ac0854dd	Available	vpc-009f1e5c295410f59   aws...	172.31.16.0/20
-	subnet-0db309ce8e28fea3e	Available	vpc-009f1e3c295410f59   aws...	172.31.0.0/20
csm-public-subnet	subnet-00da190102bd11ecd	Available	vpc-09ab9f918122340e7   csm...	10.0.1.0/24
csm-private-subnet	subnet-0c4f4591717ed5af9	Available	vpc-09ab9f918122340e7   csm...	10.0.2.0/24

The screenshot shows the AWS VPC Subnet details page for subnet-05bdea4489973755a. The left sidebar is the VPC dashboard with a 'Subnets' section selected. The main area displays the following details:

Details			
Subnet ID: subnet-05bdea4489973755a	Subnet ARN: arn:aws:ec2:ap-south-1:654654341426:subnet/subnet-05bdea4489973755a	State: Available	IPv4 CIDR: 12.0.1.0/24
Available IPv4 addresses: 250	IPv6 CIDR: -	IPv6 CIDR association ID: -	Availability Zone: ap-south-1a
Availability Zone ID: aps1-az1	Network border group: ap-south-1	VPC: vpc-03623df217ce1cead   csm-vpc-2	Route table: rtb-01ddcf720777973f   csm-rt-vpc-2
Network ACL: acl-01955c8fc1ac9ef4b	Auto-assign public IPv4 address: No	Auto-assign IPv4 address: No	Auto-assign IPv6 address: No
Auto-assign customer-owned IPv4 address: No	Customer-owned IPv4 pool: -	Outpost ID: -	IPv4 CIDR reservations: -
IPv6 CIDR reservations: -	IPv6-only: No	Hostname type: IP name	Resource name DNS A record: Disabled
Resource name DNS AAAA record: Disabled	DNS64: Disabled	Owner: 654654341426	

**VPC dashboard**

**Subnets**

**Route table:** rtb-010ddcf720777973f / csm-rt-vpc-2

Route	Destination	Target
10.0.0.0/16	pox-08dd367538ad31578	
12.0.0.0/16	local	
0.0.0.0/0	igw-01d0e3a2e4413fa06	

### c) create route table for subnet.

**Route tables (6) Info**

Name	Route table ID	Explicit subnet assoc...	Main	VPC
-	rtb-0018b8c94adab8304	-	Yes	vpc-03623df217ce1cead   csr
csm-rt-vpc-2	rtb-010ddcf720777973f	subnet-05bdea448997375...	No	vpc-03623df217ce1cead   csr
-	rtb-0426fab6f79133c09	-	Yes	vpc-009f1e3c295410f59   aw
csm-private-rt	rtb-027acce95d47f5dcc	subnet-0c4f4591717ed5...	No	vpc-09ab9f918122340e7   cs
csm-public-rt	rtb-0b7c8d78cd037fb7	subnet-00da190102bd11...	No	vpc-09ab9f918122340e7   cs
-	rtb-0b0eb1fb9d6a5c203	-	Yes	vpc-09ab9f918122340e7   cs

The screenshot shows the AWS VPC Route Table Details page for route table ID `rtb-010ddcf720777973f`. The main content area displays the following details:

Route table ID	rtb-010ddcf720777973f	Main	No	Explicit subnet associations	subnet-05bdea448997375a / subnet-vpc-2	Edge associations	-	
VPC	vpc-03623df217ce1cead   csm-vpc-2	Owner ID	654654341426					

Below this, there are tabs for **Routes**, **Subnet associations**, **Edge associations**, **Route propagation**, and **Tags**. The **Routes** tab is selected, showing three routes:

Destination	Target	Status	Propagated
0.0.0.0/0	igw-01d0e3a2e4413fa06	Active	No
10.0.0.0/16	pxc-08dd367538ad31578	Active	No
12.0.0.0/16	local	Active	No

At the bottom right of the main content area, there is a link to [Edit routes](#).

The left sidebar lists various VPC components under **Virtual private cloud**: Your VPCs, Subnets, **Route tables** (selected), Internet gateways, Egress-only Internet gateways, DHCP option sets, Elastic IPs, Managed prefix lists, Endpoints, Endpoint services, NAT gateways, and Peering connections.

At the bottom of the page, there are links to [CloudShell](#) and [Feedback](#).

This screenshot shows the same route table details as the first one, but the **Subnet associations** tab is now selected. It displays the following information:

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
subnet-vpc-2	subnet-05bdea448997375a	12.0.1.0/24	-

Below this, there is a section titled **Subnets without explicit associations (0)** which states: "The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table." There is also a link to [Edit subnet associations](#).

The left sidebar and footer are identical to the first screenshot.

## d) create internet gateway for vpc-2.

The screenshot shows the AWS VPC dashboard with the 'Internet gateways' section selected. The table displays two entries:

Name	Internet gateway ID	State	VPC ID	Owner
igw-vpc-2	igw-01d0e3a2e4413fa06	Attached	vpc-03623df217ce1cead   csm-vpc-2	654654341426
igw-csm	igw-0f4e1b4bdfb1c5a7	Attached	vpc-09ab9f918122340e7   csm-vpc	654654341426

A message at the bottom of the list says "Select an internet gateway above".

The screenshot shows the details page for the internet gateway 'igw-01d0e3a2e4413fa06 / igw-vpc-2'. The 'Details' tab is selected, showing the following information:

Internet gateway ID	igw-01d0e3a2e4413fa06	State	Attached	VPC ID	vpc-03623df217ce1cead   csm-vpc-2	Owner	654654341426
---------------------	-----------------------	-------	----------	--------	-----------------------------------	-------	--------------

The 'Tags' section shows one tag: Name: igw-vpc-2.

## e) create instance for vpc-2.

The screenshot shows the AWS EC2 Instances page. The left sidebar is collapsed. The main area displays a table of instances. One instance, 'vpc-2-instance' (ID: i-0b812e2932abae25d), is highlighted with a blue selection bar. The table columns include Name, Instance ID, Instance state, Instance type, Status check, Alarm status, Availability Zone, and Public IPv4 DNS. The instance 'vpc-2-instance' is listed as 'Running' with t2.micro type and 2/2 checks passing. It is located in ap-south-1a. The table header has a search bar and dropdown filters for 'All states'. A 'Launch instances' button is visible at the top right of the table area.

The screenshot shows the AWS EC2 Instance summary page for the instance 'i-0b812e2932abae25d (vpc-2-instance)'. The left sidebar is collapsed. The main area displays detailed information about the instance. Key details include:

- Instance ID: i-0b812e2932abae25d (vpc-2-instance)
- Public IPv4 address: 3.109.60.3
- Private IPv4 address: 12.0.1.151
- Instance state: Running
- Private IP DNS name (IPv4 only): ip-12-0-1-151.ap-south-1.compute.internal
- Instance type: t2.micro
- VPC ID: vpc-03623df217ce1ced (csm-vpc-2)
- Subnet ID: subnet-05bdea4489973755a (subnet-vpc-2)
- Instance ARN: arn:aws:ec2:ap-south-1:654654341426:instance/i-0b812e2932abae25d

Screenshot of the AWS EC2 Instance Details page (Details tab selected).

**Instance details**

Parameter	Value	Setting
Platform	Amazon Linux (Inferred)	Monitoring disabled
Platform details	Linux/UNIX	Termination protection Disabled
Stop protection	Disabled	AMI location
Instance auto-recovery	Default	Stop-hibernate behavior
AMI Launch index	0	State transition reason
Credit specification	standard	State transition message
Usage operation	RunInstances	Owner
Enclaves Support	-	Current instance boot mode
AMI ID	ami-08718895af4dfa033	
AMI name	al2023-ami-2023.5.20240916.0-kernel-6.1-x86_64	
Launch time	Sun Sep 22 2024 14:43:03 GMT+0530 (India Standard Time) (2 minutes)	
Lifecycle	normal	
Key pair assigned at launch	vpc-key	
Kernel ID	-	
RAM disk ID	-	
Boot mode	uefi-preferred	

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Screenshot of the AWS EC2 Instance Security tab.

**Security details**

Parameter	Value	Setting
IAM Role	-	Owner ID
Security groups	sg-0619a2c354e96552e (launch-wizard-2)	Launch time

**Inbound rules**

Name	Security group rule ID	Port range	Protocol	Source	Security group
-	sgr-00215f96469e193f2	22	TCP	0.0.0.0/0	launch-wiza
-	sgr-0f068f7ac27dd9f17	All	ICMP	10.0.0.0/16	launch-wiza
-	sgr-08e4486a2e986ccc8	0 - 65535	TCP	10.0.0.0/16	launch-wiza
-	sgr-09e581ea49ff00d2	80	TCP	0.0.0.0/0	launch-wiza

**Outbound rules**

Name	Security group rule ID	Port range	Protocol	Destination	Security group
-	-	-	-	-	-

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

## f) create peering connection for vpc's.

The screenshot shows the AWS VPC Peering connections page. On the left, there is a navigation sidebar with options like Your VPCs, Subnets, Route tables, Internet gateways, Egress-only Internet gateways, DHCP option sets, Elastic IPs, Managed prefix lists, Endpoints, Endpoint services, NAT gateways, and Peering connections. The Peering connections option is selected. The main content area displays a table titled "Peering connections (1) Info". The table has columns for Name, Peering connection ID, Status, Requester VPC, and Acceptor VPC. One row is listed: "vpc-peering-try" with Peering connection ID "pcx-08dd367538ad31578", Status "Active", Requester VPC "vpc-09ab9f918122340e7 / csm...", and Acceptor VPC "vpc-03623df217ce1cead / csm...". There is a "Create peering connection" button at the top right of the table.

The screenshot shows the AWS VPC Peering connection details page for the connection "pcx-08dd367538ad31578 / vpc-peering-try". The left sidebar is identical to the previous screenshot. The main content area is titled "pcx-08dd367538ad31578 / vpc-peering-try". It has a "Details" tab selected, showing various configuration parameters. These include Requester owner ID (654654341426), Acceptor owner ID (654654341426), Peering connection ID (pcx-08dd367538ad31578), Requester VPC (vpc-09ab9f918122340e7 / csm-vpc), Requester CIDR (10.0.0.0/16), Requester Region (Mumbai (ap-south-1)), Acceptor VPC (vpc-03623df217ce1cead / csm-vpc-2), Acceptor CIDR (12.0.0.0/16), and Acceptor Region (Mumbai (ap-south-1)). Below the details, there are tabs for DNS, Route tables, and Tags. Under the DNS tab, there is a "DNS settings" section with a "Edit DNS settings" button. At the bottom, there is a note about allowing the accepter VPC to resolve DNS of hosts in the requester VPC to private IP addresses.

Screenshot of the AWS VPC console showing the Peering connection details for a connection between two VPCs.

**Peering connection ID:** pcx-08dd367538ad31578

**Status:** Active

**Requester VPC:** vpc-09ab9f918122340e7 / csm-vpc

**Requester CIDRs:** 10.0.0.0/16

**Requester Region:** Mumbai (ap-south-1)

**Acceptor VPC:** vpc-03623df217ce1cead / csm-vpc-2

**Acceptor CIDRs:** 12.0.0.0/16

**Acceptor Region:** Mumbai (ap-south-1)

**DNS settings:**

- Requester VPC (vpc-09ab9f918122340e7 / csm-vpc) [Info](#)
  - Allow accepter VPC to resolve DNS of hosts in requester VPC to private IP addresses
  - Disabled
- Acceptor VPC (vpc-03623df217ce1cead / csm-vpc-2) [Info](#)
  - Allow requester VPC to resolve DNS of hosts in accepter VPC to private IP addresses
  - Disabled

**Route tables:**

Route table ID	VPC ID	Main	Associated with
rtb-010ddcf720777973f / csm-rt-vpc-2	vpc-03623df217ce1cead / csm-vpc-2	No	subnet-05bdea4489973755a
rtb-0b7c8d78cd037fbf7 / csm-public-rt	vpc-09ab9f918122340e7 / csm-vpc	No	subnet-00da190102bd11ecd

Screenshot of the AWS VPC console showing the Details page for the same peering connection.

**Requester owner ID:** 654654341426

**Requester VPC:** vpc-09ab9f918122340e7 / csm-vpc

**Requester CIDRs:** 10.0.0.0/16

**Requester Region:** Mumbai (ap-south-1)

**Acceptor owner ID:** 654654341426

**Acceptor VPC:** vpc-03623df217ce1cead / csm-vpc-2

**Acceptor CIDRs:** 12.0.0.0/16

**Acceptor Region:** Mumbai (ap-south-1)

**VPC Peering connection ARN:** arn:aws:ec2:ap-south-1:654654341426:vpc-peering-connection/pcx-08dd367538ad31578

**Route tables:**

Route table ID	VPC ID	Main	Associated with
rtb-010ddcf720777973f / csm-rt-vpc-2	vpc-03623df217ce1cead / csm-vpc-2	No	subnet-05bdea4489973755a
rtb-0b7c8d78cd037fbf7 / csm-public-rt	vpc-09ab9f918122340e7 / csm-vpc	No	subnet-00da190102bd11ecd

**g) Go to instances and choose public instance of vpc-1 and edit the inbound and outbound rules.**

The screenshot shows the AWS EC2 Instances page. A specific instance, 'csm-public-instance' (with ID i-050e06a78d6663098), is selected. The 'Inbound rules' section is open, listing the following rules:

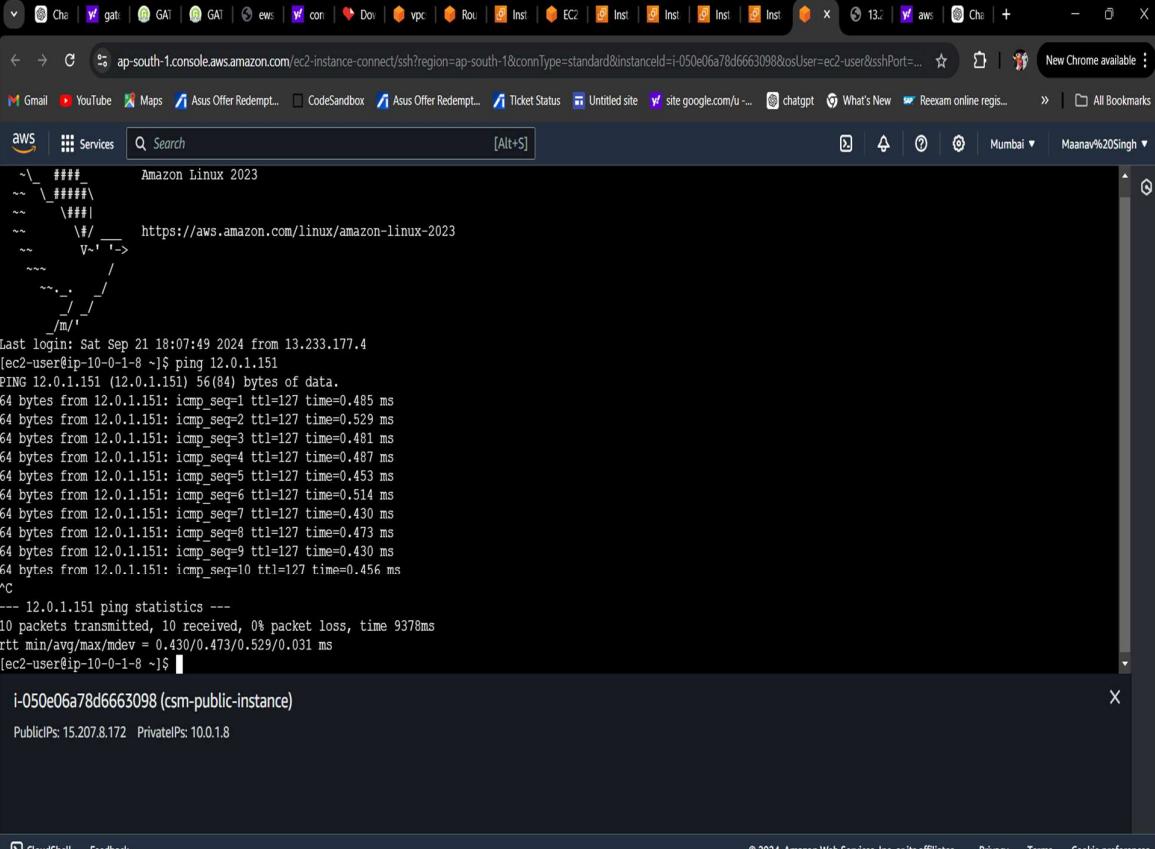
Name	Security group rule ID	Port range	Protocol	Source	Security groups
-	sgr-0083fb8a79f407275	22	TCP	0.0.0.0/0	launch-wizard-1-public
-	sgr-06222af7fa64faef4	0	TCP	10.0.2.237/32	launch-wizard-1-public
-	sgr-03da90c6602ff5feb	0 - 65535	TCP	12.0.0.0/16	launch-wizard-1-public
-	sgr-0089c43d978df6246	80	TCP	0.0.0.0/0	launch-wizard-1-public
-	sgr-0dd4e2883b905666c	All	ICMP	12.0.0.0/16	launch-wizard-1-public

The screenshot shows the AWS EC2 Instances page. A specific instance, 'vpc-2-instance' (with ID i-0b812e2932abae25d), is selected. The 'Inbound rules' section is open, listing the following rules:

Name	Security group rule ID	Port range	Protocol	Source	Security groups
-	sgr-00215f96469e193f2	22	TCP	0.0.0.0/0	launch-wizard-2
-	sgr-0f068f7ac27dd9f17	All	ICMP	10.0.0.0/16	launch-wizard-2
-	sgr-08e4486a2e986cc8	0 - 65535	TCP	10.0.0.0/16	launch-wizard-2
-	sgr-09e581ea49fff00d2	80	TCP	0.0.0.0/0	launch-wizard-2

**h) after editing the inbound and outbound rules connect the public instance of vpc-1 and run the following command:**

**ping private-ip-of-vpc-2-instance (in my case it is 12.0.1.151).**



The screenshot shows a terminal window titled "CloudShell" with the URL "ap-south-1.console.aws.amazon.com/ec2-instance-connect/ssh?region=ap-south-1&connType=standard&instanceId=i-050e06a78d6663098&osUser=ec2-user&sshPort=22" in the address bar. The terminal content is as follows:

```
Amazon Linux 2023
https://aws.amazon.com/linux/amazon-linux-2023

Last login: Sat Sep 21 18:07:49 2024 from 13.233.177.4
[ec2-user@ip-10-0-1-8 ~]$ ping 12.0.1.151
PING 12.0.1.151 (12.0.1.151) 56(84) bytes of data.
64 bytes from 12.0.1.151: icmp_seq=1 ttl=127 time=0.485 ms
64 bytes from 12.0.1.151: icmp_seq=2 ttl=127 time=0.529 ms
64 bytes from 12.0.1.151: icmp_seq=3 ttl=127 time=0.481 ms
64 bytes from 12.0.1.151: icmp_seq=4 ttl=127 time=0.487 ms
64 bytes from 12.0.1.151: icmp_seq=5 ttl=127 time=0.453 ms
64 bytes from 12.0.1.151: icmp_seq=6 ttl=127 time=0.514 ms
64 bytes from 12.0.1.151: icmp_seq=7 ttl=127 time=0.430 ms
64 bytes from 12.0.1.151: icmp_seq=8 ttl=127 time=0.473 ms
64 bytes from 12.0.1.151: icmp_seq=9 ttl=127 time=0.430 ms
64 bytes from 12.0.1.151: icmp_seq=10 ttl=127 time=0.456 ms
^C
--- 12.0.1.151 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9378ms
rtt min/avg/max/mdev = 0.430/0.473/0.529/0.031 ms
[ec2-user@ip-10-0-1-8 ~]$
```

i-050e06a78d6663098 (csm-public-instance)

PublicIPs: 15.207.8.172 PrivateIPs: 10.0.1.8

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences