

Virtual Private Cloud

A **Virtual Private Cloud (VPC)** in AWS is a logically isolated section of the AWS cloud where you can launch AWS resources in a virtual network that you define. It gives you complete control over your networking environment, including IP address ranges, subnets, route tables, and gateways.

Key Features of VPC

1. **Logical Isolation:**
 - Each VPC is isolated from other VPCs and AWS accounts, ensuring a secure environment for your resources.
2. **Custom IP Addressing:**
 - You can choose your own IP address ranges (using IPv4 or IPv6) and create subnets within those ranges.
3. **Subnets:**
 - Subnets divide the VPC into smaller network segments. These can be **public** (accessible from the internet) or **private** (restricted access).
4. **Security:**
 - **Security Groups:** Act as virtual firewalls at the instance level.
 - **Network ACLs (NACLs):** Provide an additional layer of security at the subnet level.
5. **Internet Gateway:**
 - Allows communication between instances in the VPC and the internet for public resources.
6. **Peering and Interconnectivity:**
 - Connect VPCs using **VPC peering**, AWS Transit Gateway, or VPN connections.
7. **Elastic IP Addresses:**
 - Assign a static, public IP address to instances in the VPC for consistent external access.
8. **Endpoint Services:**
 - Use VPC endpoints to privately connect to AWS services without going through the internet.

How VPC Works

1. Creating a VPC:

- When you create a VPC, you define its **CIDR block** (e.g., `10.0.0.0/16`) to specify the IP range.

2. Subnets:

- You create subnets within the CIDR block. For example:
 - **Public Subnet:** Contains instances that need to communicate with the internet (requires an internet gateway).
 - **Private Subnet:** Contains resources that are not directly accessible from the internet (can use a NAT gateway for outbound internet access).

3. Routing:

- Use **route tables** to define how traffic is directed within the VPC and to external resources.

4. Access:

- Instances can use **security groups** and **NACLs** to control traffic to and from the VPC.

5. Connection:

- Connect the VPC to on-premises data centers using VPN or AWS Direct Connect.

Benefits of VPC

1. Security and Isolation:

- Provides a private, isolated environment for your resources.

2. Custom Networking:

- Tailor the network configuration to your application needs.

3. Scalability:

- Easily add or remove subnets, resources, and configurations.

4. Cost-Effective:

- Pay only for the resources you use within the VPC.

5. Flexible Connectivity:

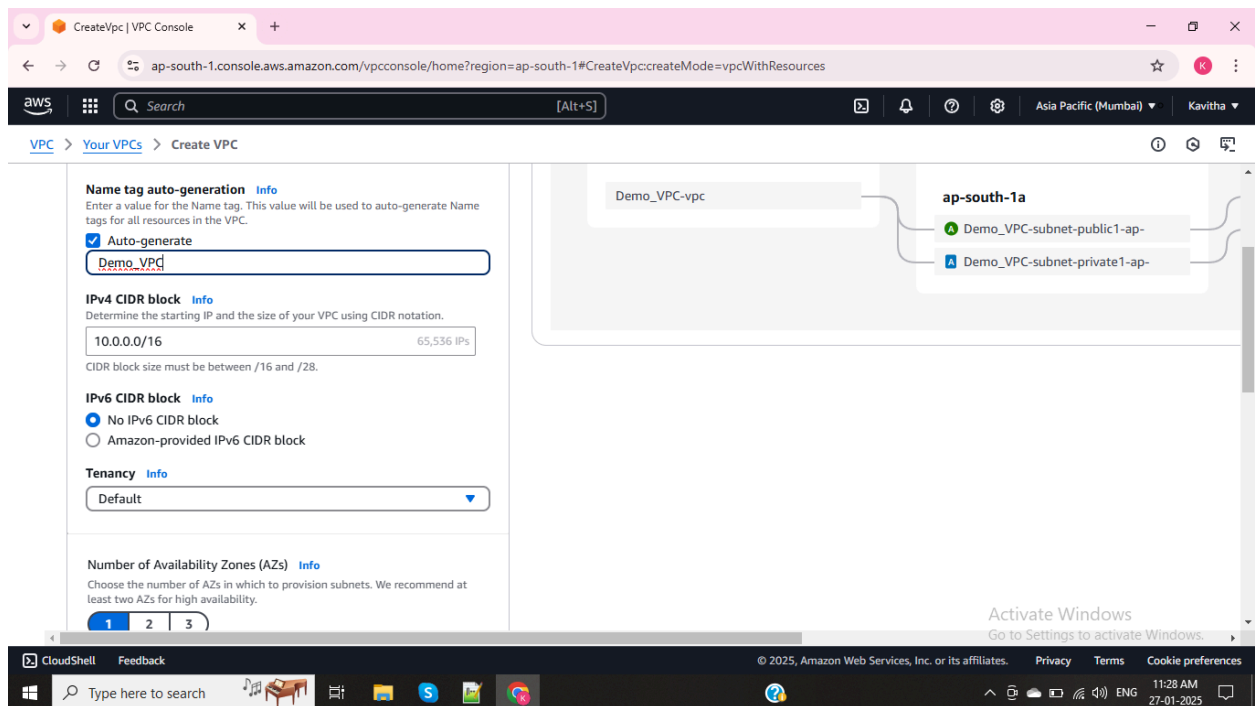
- Support for hybrid cloud environments via VPN and Direct Connect.

Use Cases

1. Hosting public-facing websites in public subnets.
2. Running backend applications in private subnets.
3. Establishing a secure hybrid cloud setup with VPN/Direct Connect.
4. Isolating workloads by project, team, or environment.

Creating a VPC

1. **AWS Management Console:** Navigate to the **VPC Dashboard**
2. Create VPC choose VPC and more
3. Give name in Auto-generated - DEMO-VPC
4. Number of availability zone choose - 1
5. Public subnets choose - 1
6. Private subnets choose - 1
7. Nat Gateway & VPC endpoint - none
8. With this Creation by default route tables and NACLs created



VPC | ap-south-1

ap-south-1.console.aws.amazon.com/vpconsole/home?region=ap-south-1#CreateVpcWizard:

aws [Search] [Alt+S]

VPC > Your VPCs > Create VPC > Create VPC resources

Create VPC workflow

Success

Details

- ✓ Create VPC: vpc-043346c72678a7bad
- ✓ Enable DNS hostnames
- ✓ Enable DNS resolution
- ✓ Verifying VPC creation: vpc-043346c72678a7bad
- ✓ Create subnet: subnet-022effbb5fb4f150e
- ✓ Create subnet: subnet-0bd28089b263017f4
- ✓ Create internet gateway: igw-0eb24bacbcbcc64
- ✓ Attach internet gateway to the VPC
- ✓ Create route table: rtb-0e9ac83be2a2e904a
- ✓ Create route
- ✓ Associate route table
- ✓ Create route table: rtb-0e580fbc2357fde3c
- ✓ Associate route table
- ✓ Verifying route table creation

Activate Windows
Go to Settings to activate Windows

CloudShell Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Type here to search

11:28 AM
27-01-2025

OUTPUT

vpcs | VPC Console

ap-south-1.console.aws.amazon.com/vpconsole/home?region=ap-south-1#vpcs:

aws [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

NAT gateways

Peering connections

Security

Network ACLs

Your VPCs (1/2) Info

Last updated less than a minute ago

Actions Create VPC

Name	VPC ID	State	Block Public...	IPv4 CIDR
-	vpc-03c4ef00c4d76e0aa	Available	Off	172.31.0.0/16
✓ Demo-vpc	vpc-043346c72678a7bad	Available	Off	10.0.0.0/16

vpc-043346c72678a7bad / Demo-vpc

Details Resource map CIDRs Flow logs Tags Integrations

Resource map Info

VPC show details
Your AWS virtual network

Demo-vpc

Subnets (2)
Subnets within this VPC

ap-south-1a

Route tables (3)
Route network traffic to resources

Demo_VPC-rtb-private-1-ap-south-1a

Go to Settings to activate Windows

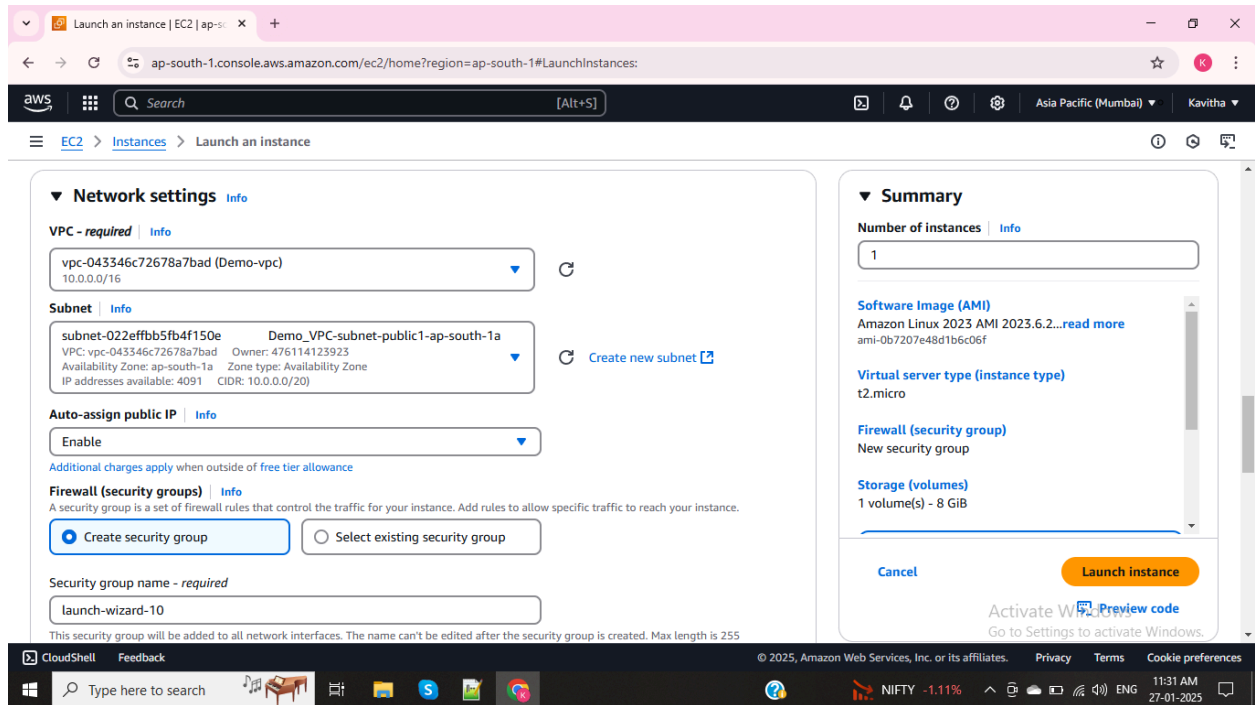
CloudShell Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

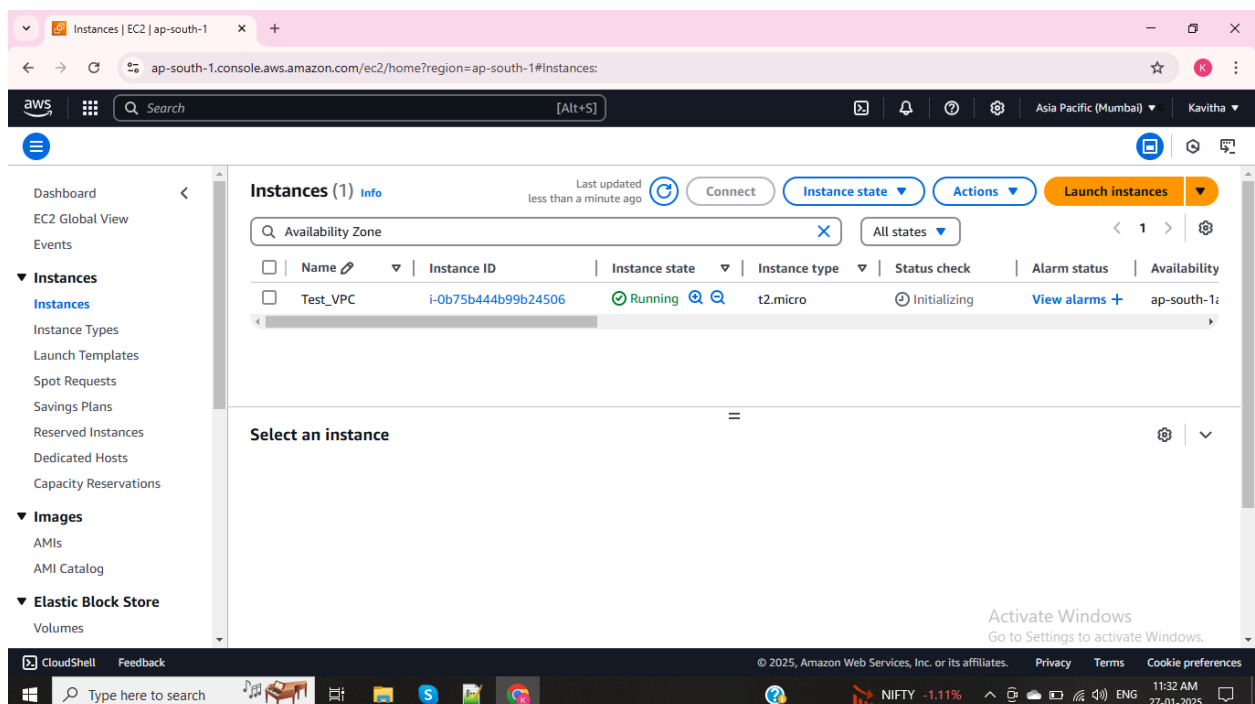
Type here to search

11:29 AM
27-01-2025

Creating an EC2 instance --> Give name --> choose keypair --> choose AMI --> choose instance type --> Edit Network settings --> choose created **DEMO VPC** --> launch instance



Created an EC2 instance



Instance connected with Created DEMO VPC and output

