AWS VPC (Virtual Private Cloud) Documentation

Overview

Amazon VPC (Virtual Private Cloud) lets you provision a logically isolated section of the AWS cloud where you can launch AWS resources in a virtual network that you define. It mimics a traditional network that you might operate in your own data center but with the scalable infrastructure of AWS.

VPC Architecture Diagram

Refer to AWS official documentation for the latest architecture diagrams: https://docs.aws.amazon.com/vpc/latest/userguide/

Key Components

Component	Description
VPC	The isolated network you create in AWS.
Subnets	Sub-segments within a VPC. Can be public or private.
Route Table	Controls traffic routing within the VPC.
Internet Gateway (IGW)	Allows public traffic into your VPC.
NAT Gateway	Allows private subnets to access the internet securely.
Security Groups	Acts as a virtual firewall for your resources.
Network ACLs	Controls inbound and outbound traffic at the subnet level.

How to Create a VPC

Step 1: Open the VPC Dashboard

Go to AWS Console → Search “VPC” → Open VPC Dashboard

Step 2: Create VPC

Click Create VPC
Choose “VPC only” or “VPC with Subnets”
Enter:
- Name tag: MyVPC
- IPv4 CIDR block: 10.0.0.0/16

Choose No IPv6 CIDR (optional)
Click Create VPC

Create Subnets

Go to Subnets → Click Create subnet
Choose your VPC
Add:
- Subnet name: PublicSubnet1
- AZ: us-east-1a
- CIDR block: 10.0.1.0/24

Repeat for private subnets

Attach Internet Gateway

Go to Internet Gateways → Create internet gateway
Name it: MyIGW
Click Attach to VPC → Select your VPC

Configure Route Tables

Go to Route Tables → Select the main one or create a new one
Edit routes:
- Destination: 0.0.0.0/0
- Target: Internet Gateway

Associate it with your public subnet

Configure Security Groups

Go to Security Groups → Create new
Add:
- Inbound Rule: Allow SSH (port 22), HTTP (port 80), and HTTPS (port 443)
- Source: Anywhere or specific IP

NAT Gateway (Optional for Private Subnets)

Go to NAT Gateways → Click Create
Select a public subnet
Assign an Elastic IP
Update private subnet's route table:
- Destination: 0.0.0.0/0
- Target: NAT Gateway

Sample Use Case Diagram

Refer to this diagram for an example setup:
https://aws.amazon.com/architecture/icons/

Best Practices

- Use multiple availability zones for high availability.
- Use private subnets for databases and backend systems.
- Enable VPC Flow Logs for traffic monitoring.
- Apply least privilege principle in security groups and NACLs.

References

• https://docs.aws.amazon.com/vpc/

• https://aws.amazon.com/vpc/faqs/

• https://www.kerno.io/learn/what-is-aws-vpc-tutorial

• https://www.davidc.net/sites/default/subnets/subnets.html (For Calculate Subnets)