



AWS VPC Project: Creating A Secure Network

This presentation walks through the process of setting up an AWS VPC and deploying an application server in a secure environment.

AWS CLI Setup

```
C:\Users\Compumart>aws ec2 create-vpc --cidr-block 10.0.0.0/16 --tag-specifications "ResourceType=vpc,
{
  "Vpc": {
    "CidrBlock": "10.0.0.0/16",
    "DhcpOptionsId": "dopt-0fabfee6c769769ad",
    "State": "pending",
    "VpcId": "vpc-0950a6d0127f968c4",
    "OwnerId": "496842210393",
    "InstanceTenancy": "default",
    "Ipv6CidrBlockAssociationSet": [],
    "CidrBlockAssociationSet": [
      {
        "AssociationId": "vpc-cidr-assoc-026eba95ea96a43aa",
        "CidrBlock": "10.0.0.0/16",
        "CidrBlockState": {
          "State": "associated"
        }
      }
    ]
  },
  "IsDefault": false,
  "Tags": [
    {
      "Key": "Name",
      "Value": "vpc-10.0.0.0/16"
    }
  ]
}
```

Access Lab Environment

Start your lab session as directed.

Run the Lab

Initiate the lab session by clicking "Run Lab".

AWS CLI Access

Navigate to the AWS Details panel and locate the AWS CLI section.



Creating a VPC

1

1. VPC Dashboard

Access the VPC dashboard to view your VPCs.

2

2. Creating the VPC

Create a new VPC for your project, assigning a CIDR block for the network.

3

3. VPC Configuration

Configure the VPC according to your project requirements and security policies.

Creating Subnets

```
C:\Users\Compuar\aws ec2 modify-vpc-attribute --vpc-id vpc-8950a6d0127f968c4 --enable-dns-support
C:\Users\Compuar\aws ec2 modify-vpc-attribute --vpc-id vpc-8950a6d0127f968c4 --enable-dns-hostnames
C:\Users\Compuar\aws ec2 create-subnet --vpc-id vpc-8950a6d0127f968c4 --cidr-block 10.0.0.0/24 --availability-zone us-east-1a --tag-specifications "ResourceType=subnet,Tags=[{key=Name,Value=Public Subnet}]"
{
  "Subnet": {
    "AvailabilityZone": "us-east-1a",
    "AvailabilityZoneId": "us-east-1a",
    "AvailableIpAddressCount": 251,
    "CidrBlock": "10.0.0.0/24",
    "DefaultForAz": false,
    "MapPublicIpOnLaunch": false,
    "State": "available",
    "SubnetId": "subnet-0948af11034ae63a",
    "VpcId": "vpc-8950a6d0127f968c4",
    "OwnerId": "40641218393",
    "AssignIpv6AddressesOnCreation": false,
    "Ipv6CidrBlockAssociationSet": [],
    "Tags": [
      {
        "key": "Name",
        "value": "Public Subnet"
      }
    ]
  }
}
```

Public Subnet

Create a public subnet within your VPC, accessible from the internet.

Private Subnet

Create a private subnet within your VPC, not directly accessible from the internet.

Internet Gateway

VPC Route Table

Access the route table associated with your VPC.

Attach Internet Gateway

Attach an internet gateway to your VPC, enabling communication with the external internet.

Configuring Route Tables



Route Table Association

Associate the route table with your public subnet, allowing internet access.



Security Groups

Configure security groups to control traffic flow within your VPC.

Application Server Security Group

Create Security Group

Create a security group for your application server, restricting access to specific ports.

Inbound and Outbound Rules

Define inbound and outbound rules for the security group, allowing only essential traffic.

```
{
  "placement": {
    "availabilityZone": "us-east-1a",
    "group": null,
    "tenancy": "default"
  },
  "privateIp": "10.0.0.147",
  "privateIpAddress": "10.0.0.147",
  "productCodes": [],
  "publicIp": null,
  "state": {
    "code": 16,
    "name": "pending"
  }
}
```

Launching Application Server

Select Instance Type

Choose the appropriate instance type for your application server.

1

Launch Instance

Launch the instance in your public subnet, ensuring it has access to the internet gateway.

3

2

Configure Instance

Configure the instance with the desired operating system and software.

Access and Connect

