Step 1: Create VPC

1. Sign in to AWS Console
2. Navigate to **VPC Dashboard**
3. Click **Create VPC**
4. Configure:
    - **Resources to create**: VPC only
    - **Name tag**: MyProductionVPC
    - **IPv4 CIDR block**: 10.0.0.0/16
    - **IPv6 CIDR block**: No IPv6
    - **Tenancy**: Default
5. Click **Create VPC**

Step 2: Create Subnets

Public Subnet 1:

1. In VPC Dashboard, click **Subnets** → **Create subnet**
2. Configure:
    - **VPC**: Select MyProductionVPC
    - **Subnet name**: PublicSubnet-AZ1
    - **Availability Zone**: Select first AZ (e.g., us-east-1a)
    - **IPv4 CIDR block**: 10.0.1.0/24
3. Click **Create subnet**

Public Subnet 2:

1. Click **Create subnet** again
2. Configure:
    - **VPC**: Select MyProductionVPC
    - **Subnet name**: PublicSubnet-AZ2
    - **Availability Zone**: Select second AZ (e.g., us-east-1b)
    - **IPv4 CIDR block**: 10.0.2.0/24
3. Click **Create subnet**

Private Subnet 1:

1. Click **Create subnet**

2. Configure:
    - **VPC**: Select MyProductionVPC
    - **Subnet name**: PrivateSubnet-AZ1
    - **Availability Zone**: Same as PublicSubnet-AZ1
    - **IPv4 CIDR block**: 10.0.11.0/24
3. Click **Create subnet**

Private Subnet 2:

1. Click **Create subnet**
2. Configure:
    - **VPC**: Select MyProductionVPC
    - **Subnet name**: PrivateSubnet-AZ2
    - **Availability Zone**: Same as PublicSubnet-AZ2
    - **IPv4 CIDR block**: 10.0.12.0/24
3. Click **Create subnet**

Step 3: Create and Attach Internet Gateway

1. In VPC Dashboard, click **Internet Gateways** → **Create internet gateway**
2. Configure:
    - **Name tag**: MyProductionIGW
3. Click **Create internet gateway**
4. Select the created IGW, click **Actions** → **Attach to VPC**
5. Select MyProductionVPC and click **Attach internet gateway**

Step 4: Create NAT Gateway

1. Click **NAT Gateways** → **Create NAT gateway**
2. Configure:
    - **Name**: MyProductionNAT-AZ1
    - **Subnet**: Select PublicSubnet-AZ1
    - **Connectivity type**: Public
    - **Elastic IP allocation ID**: Click **Allocate Elastic IP**
3. Click **Create NAT gateway**

4. Wait 2-3 minutes for it to become available (status: Available)

Step 5: Create Route Tables

Public Route Table:

1. Click **Route Tables** → **Create route table**
2. Configure:
    - **Name**: PublicRouteTable
    - **VPC**: Select MyProductionVPC
3. Click **Create route table**
4. Select the created route table, go to **Routes** tab
5. Click **Edit routes** → **Add route**:
    - **Destination**: 0.0.0.0/0
    - **Target**: Internet Gateway → Select MyProductionIGW
6. Click **Save changes**
7. Go to **Subnet associations** tab → **Edit subnet associations**
8. Select both PublicSubnet-AZ1 and PublicSubnet-AZ2
9. Click **Save associations**

Private Route Table:

1. Click **Create route table**
2. Configure:
    - **Name**: PrivateRouteTable
    - **VPC**: Select MyProductionVPC
3. Click **Create route table**
4. Select it, go to **Routes** tab
5. Click **Edit routes** → **Add route**:
    - **Destination**: 0.0.0.0/0
    - **Target**: NAT Gateway → Select MyProductionNAT-AZ1
6. Click **Save changes**
7. Go to **Subnet associations** tab → **Edit subnet associations**
8. Select both PrivateSubnet-AZ1 and PrivateSubnet-AZ2
9. Click **Save associations**

Step 6: Enable Auto-assign Public IP (1 minute)

1. Go to **Subnets**
2. Select PublicSubnet-AZ1
3. Click **Actions** → **Edit subnet settings**
4. Check **Enable auto-assign public IPv4 address**
5. Click **Save**
6. Repeat for PublicSubnet-AZ2

Step 7: Create Security Groups (5 minutes)

Web Server Security Group:

1. Click **Security Groups** → **Create security group**
2. Configure:
    - **Security group name**: WebServer-SG
    - **Description**: Allow HTTP and HTTPS traffic
    - **VPC**: Select MyProductionVPC
3. **Inbound rules** → **Add rule**:
    - Rule 1: Type: HTTP, Source: 0.0.0.0/0
    - Rule 2: Type: HTTPS, Source: 0.0.0.0/0
    - Rule 3: Type: SSH, Source: Your IP (for management)
4. Click **Create security group**

Database Security Group:

1. Click **Create security group**
2. Configure:
    - **Security group name**: Database-SG
    - **Description**: Allow traffic from web servers
    - **VPC**: Select MyProductionVPC
3. **Inbound rules** → **Add rule**:
    - Type: MySQL/Aurora (3306), Source: Custom → Select WebServer-SG
4. Click **Create security group**

Step 8: Enable VPC Flow Logs

1. Go to **Your VPCs**
2. Select MyProductionVPC
3. Go to **Flow logs** tab → **Create flow log**
4. Configure:
    - **Name**: MyVPC-FlowLogs
    - **Filter**: All
    - **Destination**: Send to CloudWatch Logs
    - **Destination log group**: Click **Set up permissions** (creates IAM role automatically)
    - Log group name: /aws/vpc/flowlogs
5. Click **Create flow log**