AWS How-To-Guide – Setting up a multi-tier VPC Architecture

© IaaS Academy Limited | https://iaasacademy.com

In this AWS how-to guide, you will learn how to build out a multi-tier Virtual Private Cloud (VPC) on AWS. The following diagram illustrates the core components of the VPC you will be building. You will need access to an AWS account to complete this step-by-step guide. You can easily create a free tier account at https://aws.amazon.com/free/

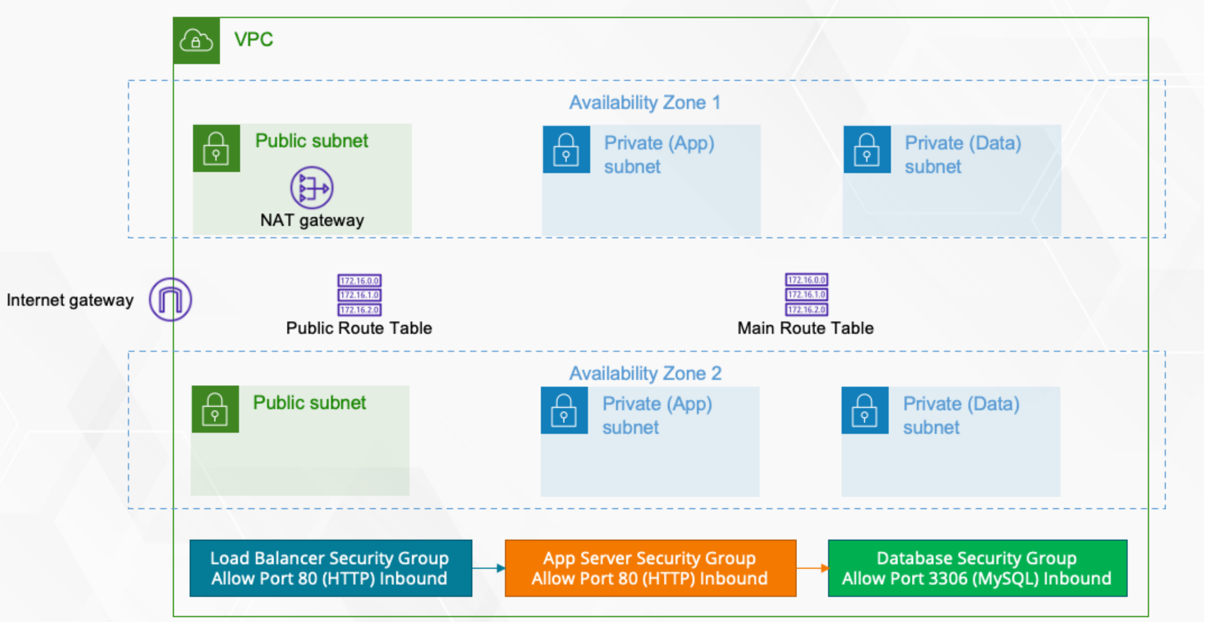


Figure – Basic three-tier VPC configuration (minimal)

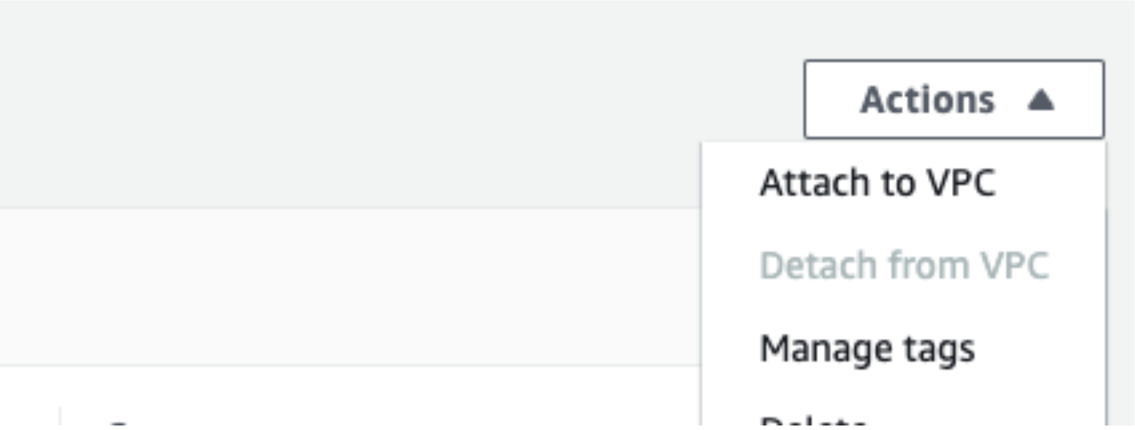
Configuration Steps

Step 1 – Create Base VPC

1. Login to your AWS account
2. Navigate to the VPC console.
3. Ensure that you are in the right region. For exercises provided by IaaS Academy training, ensure that you are in the us-east-1 region.
4. From the left-hand menu, click **Your VPCs**
5. Next, from the right-hand pane, click **Create VPC**
6. In the **Create VPC** settings page, select **VPC only**, and provide a name for your VPC such as **my-vpc.**
7. For the IPv4 CIDR block range, set the CIDR range to **10.0.0.0/16**
8. Next, click the **Create VPC** button at the bottom of the page. This creates your base VPC

Step 2 – Configure your VPC with an Internet Gateway

1. From the left-hand menu, click **Internet gateways.**
2. Next, from the right-hand pane, click the **Create internet gateway** button
3. Provide a name for your Internet gateway, e.g. **my-vpc-igw** and click the **Create internet gateway** button
4. You will be redirected to the Internet gateway console. From the right-hand pane, select the **Attach to VPC** option under the **Action** drop-down menu.



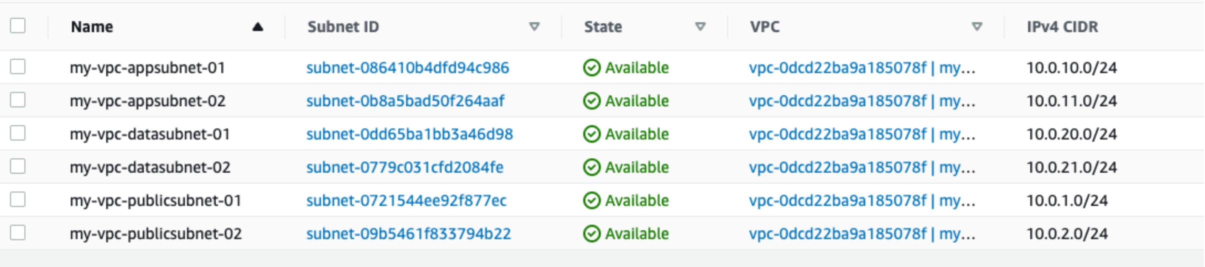
5. Next, click the search box under Available **VPCs** to select **my-vpc** you created earlier and then click the **Attach internet gateway** button.

Step 3 – Create Subnets

1. From the left-hand menu, click **Subnets.** You will be creating six subnets, two of which will be public subnets and four private subnets, as per the diagram provided at the start of this how-to guide.
2. Select the **my-vpc** from the VPC ID drop-down menu.
3. Next, under **Subnet settings,** for **Subnet 1 of 1:**
    a. Set the subnet name as my-vpc-publicsubnet-01 (this will be the first public subnet in your list).
    b. Select **us-east-1a** under **Availability Zone**
    c. Set the **IPv4 CIDR block** to **10.0.1.0/24.**
4. Next, click the **Add new subnet** button. This will allow you to define the settings for **Subnet 2 of 2:**
    a. Set the subnet name as **my-vpc-publicsubnet-02** (this will define the settings for the second public subnet)
    b. Select **us-east-1b** under **Availability Zone**
    c. Set the **IPv4 CIDR block** to **10.0.2.0/24.**
5. Next, click the **Add new subnet** button. This will allow you to define the settings for **Subnet 3 of 3:**
    a. Set the subnet name as **my-vpc-appsubnet-01** (this will define the settings for the first private subnet to host your application servers)
    b. Select **us-east-1a** under **Availability Zone**
    c. Set the **IPv4 CIDR block** to **10.0.10.0/24.**
6. Next, click the **Add new subnet** button. This will allow you to define the settings for **Subnet 4 of 4:**
    a. Set the subnet name as **my-vpc-appsubnet-02** (this will define the settings for the second private subnet to host your application servers)
    b. Select **us-east-1b** under **Availability Zone**
    c. Set the **IPv4 CIDR block** to **10.0.11.0/24.**
7. Next, click the **Add new subnet** button. This will allow you to define the settings for **Subnet 5 of 5:**

    a. Set the subnet name as **my-vpc-datasubnet-01** (this will define the settings for the third private subnet to host your database instance)
    b. Select **us-east-1a** under **Availability Zone**
    c. Set the **IPv4 CIDR block** to **10.0.20.0/24.**
8. Next, click the **Add new subnet** button. This will allow you to define the settings for **Subnet 6 of 6:**
    a. Set the subnet name as **my-vpc-datasubnet-02** (this will define the settings for the fourth private subnet to host your database instance)
    b. Select **us-east-1b** under **Availability Zone**
    c. Set the **IPv4 CIDR block** to 10.0.21.0/24
9. Click the **Create subnet** button at the bottom of the page.

Your VPC will now be configured with six subnets as per the diagram. The following is a screenshot of what the resulting list of subnets may look like your console:



□	Name ▲	Subnet ID ▽	State ▽	VPC ▽	IPv4 CIDR
□	my-vpc-appsubnet-01	subnet-086410b4dfd94c986	✓ Available	vpc-0dcd22ba9a185078f | my...	10.0.10.0/24
□	my-vpc-appsubnet-02	subnet-0b8a5bad50f264aaf	✓ Available	vpc-0dcd22ba9a185078f | my...	10.0.11.0/24
□	my-vpc-datasubnet-01	subnet-0dd65ba1bb3a46d98	✓ Available	vpc-0dcd22ba9a185078f | my...	10.0.20.0/24
□	my-vpc-datasubnet-02	subnet-0779c031cfd2084fe	✓ Available	vpc-0dcd22ba9a185078f | my...	10.0.21.0/24
□	my-vpc-publicsubnet-01	subnet-0721544ee92f877ec	✓ Available	vpc-0dcd22ba9a185078f | my...	10.0.1.0/24
□	my-vpc-publicsubnet-02	subnet-09b5461f833794b22	✓ Available	vpc-0dcd22ba9a185078f | my...	10.0.2.0/24

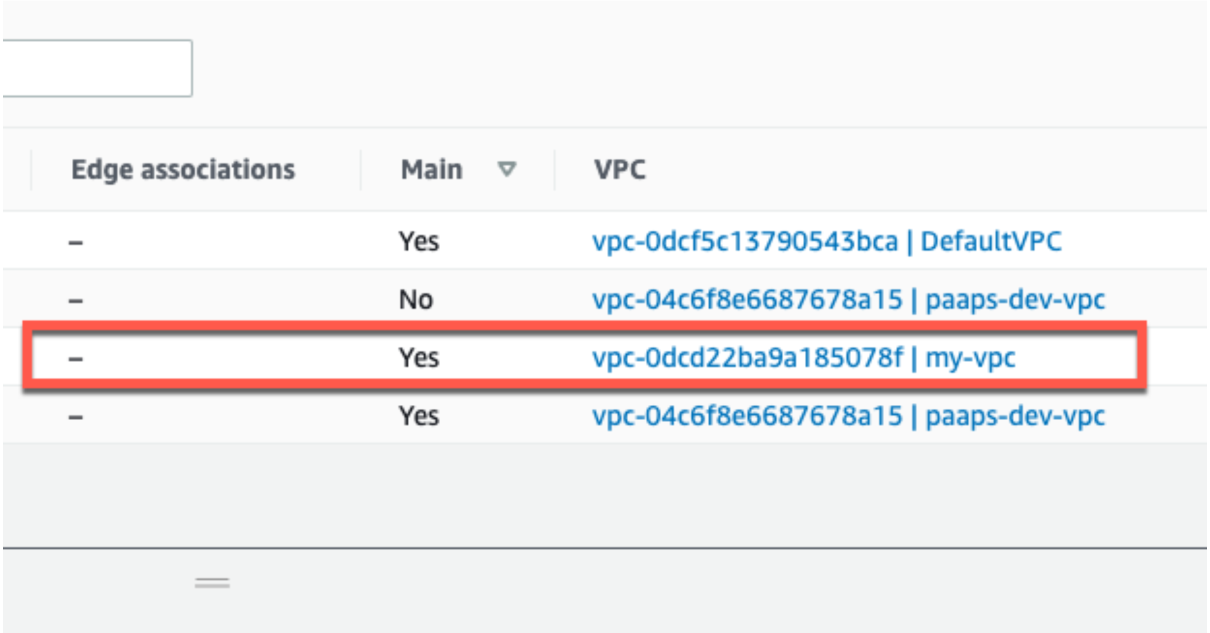
Step 4 – Configure NAT Gateway

In this step, you will configure a NAT gateway if you need to route Internet-bound traffic or access public services on AWS from instances in your private subnet. If you are using this VPC for the Session Manager lab, then the NAT gateway is mandatory.

1. From the left-hand menu, click **NAT gateways**
2. From the right-hand pane, click **Create NAT gateway**
3. Next, provide a name for your NAT gateway such as **my-vpc-natgw**
4. Under **Subnet,** select **my-vpc-publicsubnet-01**. We will be placing the NAT gateway in one of the public subnets
5. Click **Allocate Elastic IP** button to automatically allocate a new elastic IP to your NAT gateway
6. Click the **Create NAT gateway** button at the bottom of the page.

Step 5 – Configure Route Tables

1. From the left-hand menu, click **Route tables**
2. Expand the VPC column in the right hand pane to identity the main route table of your VPC.



Edge associations	Main	VPC
–	Yes	vpc-0dcf5c13790543bca | DefaultVPC
–	No	vpc-04c6f8e6687678a15 | paaps-dev-vpc
–	Yes	vpc-0dcd22ba9a185078f | my-vpc
–	Yes	vpc-04c6f8e6687678a15 | paaps-dev-vpc

3. You can then hover in the same row under the **Name** column to give you the option to provide a name for your main route table. Set the name to **my-vpc-mainrt**
4. In the bottom half of the page, click **Route**
5. Click **Edit routes**
6. Click **Add route**
7. Set the destination to **0.0.0.0/0**
8. Under **Target,** click **NAT gateway** and select the NAT gateway you created in step 4
9. Click the **Save changes** button
10. From the left-hand menu, click **Route tables** again
11. Click **Create route table** from the right-hand pane
12. Provide a name such as **my-vpc-publicrt**
13. Select **my-vpc** from the **VPC** drop-down list
14. Click the **Create route table** button
15. Next, select **Routes** in the bottom half of the page. Click **Edit routes**
16. Next, click **Add route**
17. Under **Destination,** type in 0.0.0.0/0 and under **Target,** select **Internet gateway**
18. Choose the **Internet gateway** you configure in step 2.
19. Click **Save changes.**

Step 6 – Setup Security Groups

In this step you will configure security groups for this exercise and for future exercises.

1. From the left-hand menu, click **Security groups**
2. In the right-hand pane, click **Create security group**
3. Provide a security group name such as **my-vpc-alb-sg**. This security group will be used for your Load Balancers in other exercises
4. Provide a description for your security group

5. In the VPC search box, select the **my-vpc** VPC
6. Click **Add rule** under **Inbound rules**
    a. Select **HTTP** under Type
    b. In the **Source** search box, select **0.0.0.0/0**
    c. Click the **Create security group** button
7. Click **Security groups** from the left-hand menu again. This time we will create one for our EC2 instances
    a. Provide a name for your security group such as **my-vpc-app-sg.**
    b. Provide a description for your security group
    c. In the VPC search box, select the **my-vpc** VPC
    d. Click **Add rule** under **Inbound rules**
    e. Select **HTTP** under Type
    f. In the **Source** search box, select **my-vpc-alb-sg** security group
    g. Click the **Create security group** button
8. Click **Security groups** from the left-hand menu again. This time we will create one for your database instances
    a. Provide a name for your security group such as **my-vpc-data-sg.**
    b. Provide a description for your security group
    c. In the VPC search box, select the **my-vpc** VPC
    d. Click **Add rule** under **Inbound rules**
    e. Select **MySQL/Aurora** under Type
    f. In the **Source** search box, select **my-vpc-app-sg** security group
    g. Click the **Create security group** button

You have now created your security groups for the resources to be deployed in your VPC.