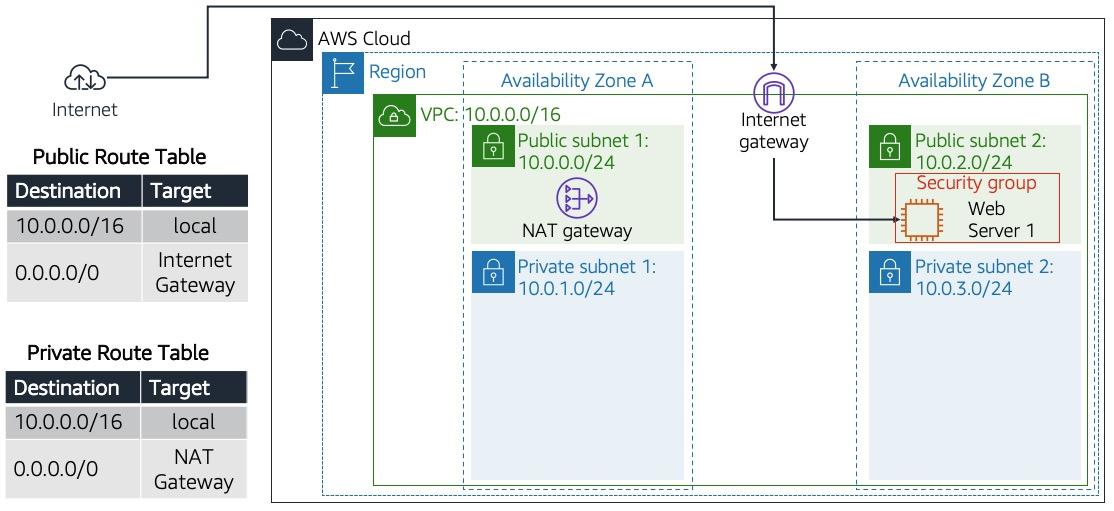
# **Build Your VPC and Launch a Web Server**

In this lab, you will use Amazon Virtual Private Cloud (VPC) to create your own VPC and add additional components to produce a customized network. You will also create security groups for your EC2 instance. You will then configure and customize an EC2 instance to run a web server and launch it into the VPC.

**Amazon Virtual Private Cloud (Amazon VPC)** enables you to launch Amazon Web Services (AWS) resources into a virtual network that you defined. This virtual network closely resembles a traditional network that you would operate in your own data center, with the benefits of using the scalable infrastructure of AWS. You can create a VPC that spans multiple Availability Zones.

**Scenario**

In this lab you build the following infrastructure:



**Objectives**

After completing this lab, you can:

* Create a VPC.
* Create subnets.
* Configure a security group.
* Launch an EC2 instance into a VPC.

## **Accessing the AWS Management Console**

At the top of these instructions, select Start Lab to launch your lab.

1. A Start Lab panel opens displaying the lab status.
2. Wait until you see the message "**Lab status: ready**", then select the **X** to close the Start Lab panel.

Select the Details drop down menu above these instructions, and then select Show. Copy all the lab details such as **BastionHost**, **Region** etc and save them in a text editor such as [Atom](https://atom.io/), [Sublime Text](https://www.sublimetext.com/) or [Visual Studio Code](https://code.visualstudio.com/).

1. The information you have saved will be referred to as *Lab Details* in the lab.

At the top of these instructions, select AWS

This will open the AWS Management Console in a new browser tab. The system will automatically log you in.

1. **Tip**: If a new browser tab does not open, there will typically be a banner or icon at the top of your browser indicating that your browser is preventing the site from opening pop-up windows. Select the banner or icon and choose "Allow pop-ups."

Arrange the AWS Management Console tab so that it displays alongside these instructions. Ideally, you will be able to see both browser tabs at the same time, to make it easier to follow the lab steps.

1. **Do not change the Region unless instructed to do so**.

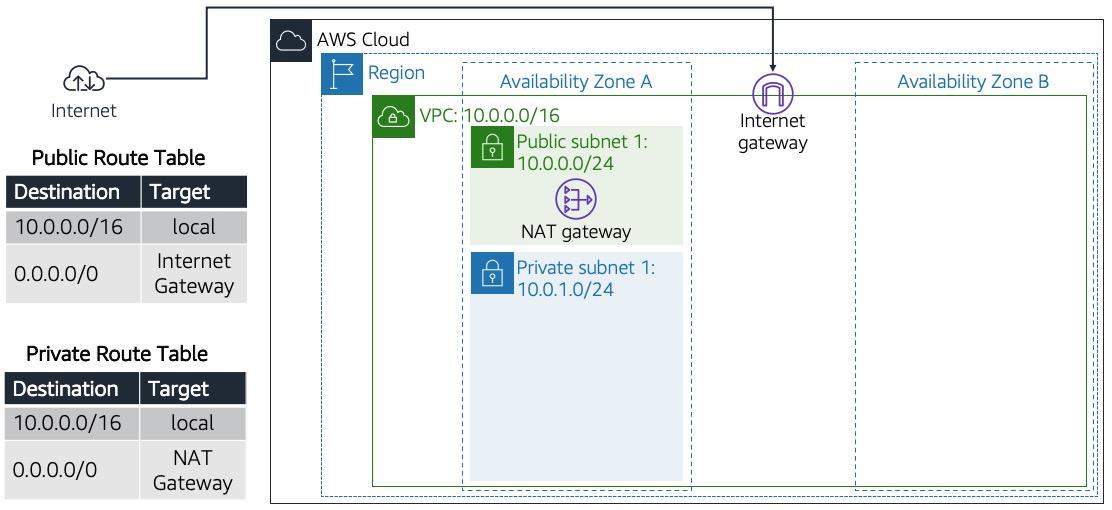
## **Task 1: Create Your VPC**

In this task, you will use the VPC Wizard to create a VPC an Internet Gateway and two subnets in a single Availability Zone. An **Internet gateway (IGW)** is a VPC component that allows communication between instances in your VPC and the Internet.

After creating a VPC, you can add **subnets**. Each subnet resides entirely within one Availability Zone and cannot span zones. If a subnet's traffic is routed to an Internet Gateway, the subnet is known as a *public subnet*. If a subnet does not have a route to the Internet gateway, the subnet is known as a *private subnet*.

The wizard will also create a *NAT Gateway*, which is used to provide internet connectivity to EC2 instances in the private subnets.

1. In the **AWS Management Console**, on the **Services** menu, click **VPC**.
2. Click **Launch VPC Wizard**
3. In the left navigation pane, click **VPC with Public and Private Subnets** (the second option).
4. Click **Select** then configure:
   * **VPC name:** Lab VPC
   * **Availability Zone:** Select the *first* Availability Zone
   * **Public subnet name:** Public Subnet 1
   * **Availability Zone:** Select the *first* Availability Zone (the same as used above)
   * **Private subnet name:** Private Subnet 1
   * **Elastic IP Allocation ID:** Click in the box and select the displayed IP address
5. Click **Create VPC**The wizard will create your VPC.
6. Once it is complete, click **OK**The wizard has provisioned a VPC with a public subnet and a private subnet in the same Availability Zone, together with route tables for each subnet:

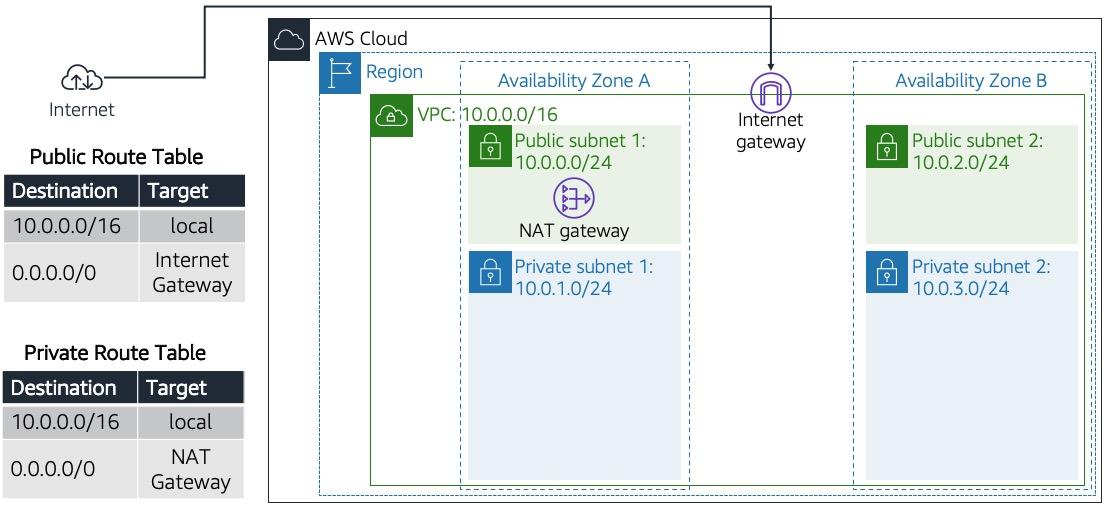


The Public Subnet has a CIDR of **10.0.0.0/24**, which means that it contains all IP addresses starting with **10.0.0.x**.  
The Private Subnet has a CIDR of **10.0.1.0/24**, which means that it contains all IP addresses starting with **10.0.1.x**.

## **Task 2: Create Additional Subnets**

In this task, you will create two additional subnets in a second Availability Zone. This is useful for creating resources in multiple Availability Zones to provide *High Availability*.

1. In the left navigation pane, click **Subnets**.  
   First, you will create a second Public Subnet.
2. Click **Create subnet** then configure:
   * **Name tag:** Public Subnet 2
   * **VPC:** *Lab VPC*
   * **Availability Zone:** Select the *second* Availability Zone
   * **IPv4 CIDR block:** 10.0.2.0/24
3. The subnet will have all IP addresses starting with **10.0.2.x**.
4. Click **Create** then click **Close**You will now create a second Private Subnet.
5. Click **Create subnet** then configure:
   * **Name tag:** Private Subnet 2
   * **VPC:** *Lab VPC*
   * **Availability Zone:** Select the *second* Availability Zone
   * **CIDR block:** 10.0.3.0/24
6. The subnet will have all IP addresses starting with **10.0.3.x**.
7. Click **Create** then click **Close**You will now configure the Private Subnets to route internet-bound traffic to the NAT Gateway so that resources in the Private Subnet are able to connect to the Internet, while still keeping the resources private. This is done by configuring a *Route Table*.  
   A *route table* contains a set of rules, called *routes*, that are used to determine where network traffic is directed. Each subnet in a VPC must be associated with a route table; the route table controls routing for the subnet.
8. In the left navigation pane, click **Route Tables**.
9. Select the route table with **Main = Yes** and **VPC = Lab VPC**. (Expand the *VPC ID* column if necessary to view the VPC name.)
10. In the lower pane, click the **Routes** tab.  
    Note that **Destination 0.0.0.0/0** is set to **Target nat-xxxxxxxx**. This means that traffic destined for the internet (0.0.0.0/0) will be sent to the NAT Gateway. The NAT Gateway will then forward the traffic to the internet.  
    This route table is therefore being used to route traffic from Private Subnets. You will now add a name to the Route Table to make this easier to recognize in future.
11. In the **Name** column for this route table, click the pencil then type Private Route Table and click
12. In the lower pane, click the **Subnet Associations** tab.  
    You will now associate this route table to the Private Subnets.
13. Click **Edit subnet associations**
14. Select both **Private Subnet 1** and **Private Subnet 2**.  
     You can expand the *Subnet ID* column to view the Subnet names.
15. Click **Save** You will now configure the Route Table that is used by the Public Subnets.
16. Select the route table with **Main = No** and **VPC = Lab VPC** (and deselect any other subnets).
17. In the **Name** column for this route table, click the pencil then type Public Route Table, and click
18. In the lower pane, click the **Routes** tab.  
     Note that **Destination 0.0.0.0/0** is set to **Target igw-xxxxxxxx**, which is the Internet Gateway. This means that internet-bound traffic will be sent straight to the internet via the Internet Gateway.  
     You will now associate this route table to the Public Subnets.
19. Click the **Subnet Associations** tab.
20. Click **Edit subnet associations**
21. Select both **Public Subnet 1** and **Public Subnet 2**.
22. Click **Save** Your VPC now has public and private subnets configured in two Availability Zones:



## **Task 3: Create a VPC Security Group**

In this task, you will create a VPC security group, which acts as a virtual firewall. When you launch an instance, you associate one or more security groups with the instance. You can add rules to each security group that allow traffic to or from its associated instances.

1. In the left navigation pane, click **Security Groups**.
2. Click **Create security group** and then configure:
   * **Security group name:** Web Security Group
   * **Description:** Enable HTTP access
   * **VPC:** *Lab VPC*
3. You will now add a rule to the security group to permit inbound web requests.
4. In the **Inbound rules** section, click **Add rule**, then configure:
   * **Type:** *HTTP*
   * **Source:** *Anywhere*
   * **Description:** Permit web requests
5. Scroll to the bottom of the screen, then click **Create security group**You will use this security group in the next task when launching an Amazon EC2 instance.

## **Task 4: Launch a Web Server Instance**

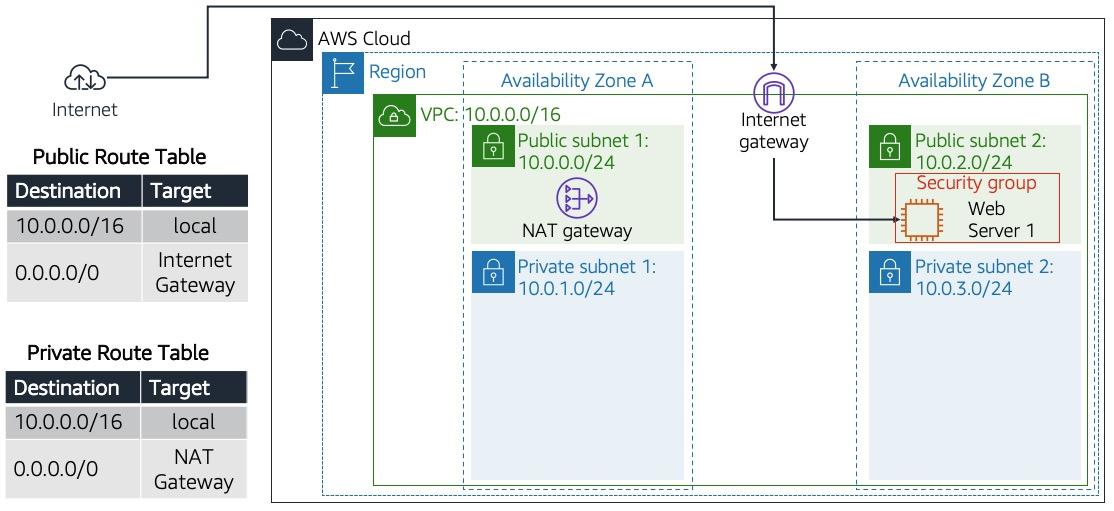
In this task, you will launch an Amazon EC2 instance into the new VPC. You will configure the instance to act as a web server.

1. On the **Services** menu, click **EC2**.
2. Click **Launch instance** > **Launch instance**.  
   First, you will select an *Amazon Machine Image (AMI)*, which contains the desired Operating System.
3. In the row for **Amazon Linux 2** (at the top), click **Select**The *Instance Type* defines the hardware resources assigned to the instance.

Select **t3.micro** (shown in the *Type* column).

1. **Note**: If you experience an error related to the t3.micro instance type not being available, then rerun this task by selecting t2.micro instead.
2. Click **Next: Configure Instance Details**You will now configure the instance to launch in a Public Subnet of the new VPC.
3. Configure these settings:
   * **Network:** *Lab VPC*
   * **Subnet:** *Public Subnet 2* (*not* Private!)
   * **Auto-assign Public IP:** *Enable*
4. Expand the **Advanced Details** section (at the bottom of the page).
5. Copy and paste this code into the **User data** box:

#!/bin/bash  
# Install Apache Web Server and PHP  
yum install -y httpd mysql php  
# Download Lab files  
wget https://aws-tc-largeobjects.s3.amazonaws.com/ILT-TF-100-TUFOUN-1/4-lab-vpc-web-server/lab-app.zip  
unzip lab-app.zip -d /var/www/html/  
# Turn on web server  
chkconfig httpd on  
service httpd start

1. This script will be run automatically when the instance launches for the first time. The script loads and configures a PHP web application.
2. Click **Next: Add Storage**You will use the default settings for storage.
3. Click **Next: Add Tags**Tags can be used to identify resources. You will use a tag to assign a Name to the instance.
4. Click **Add Tag** then configure:
   * **Key:** Name
   * **Value:** Web Server 1
5. Click **Next: Configure Security Group** You will configure the instance to use the *Web Security Group* that you created earlier.
6. Select **Select an existing security group**
7. Select **Web Security Group**.  
    This is the security group you created in the previous task. It will permit HTTP access to the instance.
8. Click **Review and Launch**
9. When prompted with a *warning* that you will not be able to connect to the instance through port 22, click **Continue**
10. Review the instance information and click **Launch**
11. In the **Select an existing keypair** dialog, select **I acknowledge...**.
12. Click **Launch Instances** and then click **View Instances**
13. Wait until **Web Server 1** shows *2/2 checks passed* in the **Status Checks** column.  
     This may take a few minutes. Click refresh in the top-right every 30 seconds for updates.  
     You will now connect to the web server running on the EC2 instance.
14. Copy the **Public DNS (IPv4)** value shown in the **Description** tab at the bottom of the page.
15. Open a new web browser tab, paste the **Public DNS** value and press Enter.  
     You should see a web page displaying the AWS logo and instance meta-data values. You will use this web application in the next lab.  
     The complete architecture you deployed is:  
     

## **Lab Complete**

Congratulations! You have completed the lab.

​

Select End Lab at the top of this page and then select **Yes** to confirm that you want to end the lab.

1. A panel will appear, indicating that "DELETE has been initiated... You may close this message box now."

Select the **X** in the top right corner to close the panel.

1. ​

LAB DETASILS 62021

**Cloud Labs**

Remaining session time: 01:58:40(119 minutes)

Session started at: 2021-06-24T07:19:26-0700

Session to end at: 2021-06-24T09:19:26-0700

Accumulated lab time: 00:01:20 (2 minutes)

No running instance

SSH key ShowDownload PEMDownload PPK

AWS SSO Download URL