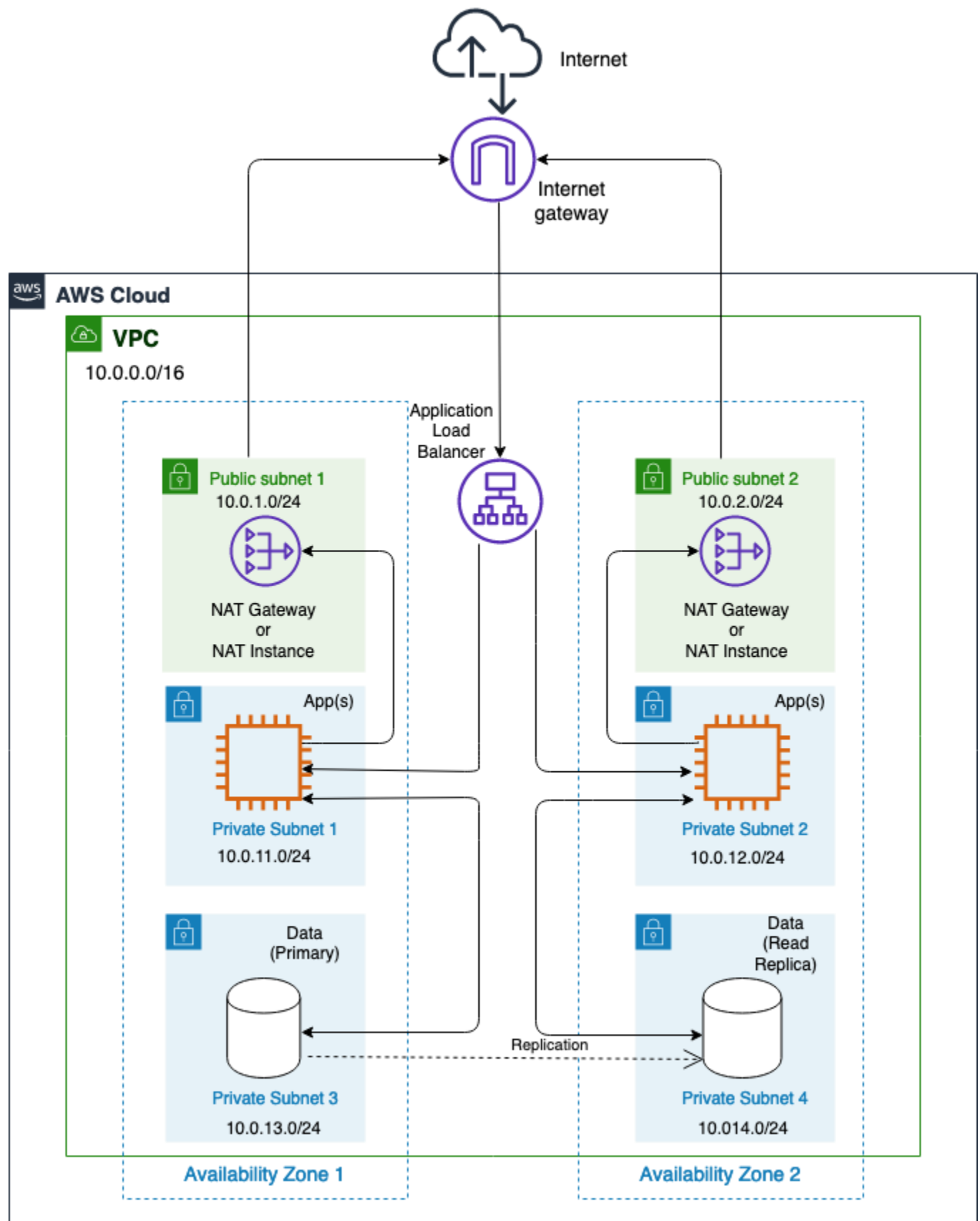


# Configuring and Deploying Amazon VPC for a 3-tier Web App

## Lab Overview

This lab demonstrates how to set up a VPC infrastructure to support a basic 3-tier web application in your AWS Cloud environment. The VPC will be built across multiple Availability Zones so that your application is highly available. Let's get a quick overview of what a VPC is and how Elastic Load Balancing works.



**Amazon Virtual Private Cloud (Amazon VPC)** lets you provision a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways. You can use both IPv4 and IPv6 in your VPC for secure and easy access to resources and applications.

You can easily customize the network configuration of your Amazon VPC. For example, you can create a public-facing subnet for your web servers that have access to the internet. You can also place your backend systems, such as databases or application servers, in a private-facing subnet with no internet access. You can use multiple layers of security, including security groups and network access control lists, to help control access to Amazon EC2 instances in each subnet.

For more information about VPC you can view the AWS Documentation using the following link:

<https://docs.aws.amazon.com/vpc/latest/userguide/how-it-works.html>

## Topics Covered

- Build a VPC
- Create public and private subnets
- Configure the internet gateway and NAT gateway
- Ensure your resources are securely deployed within the VPC

## Technical Knowledge Prerequisites

To successfully complete this lab, you should be familiar with basic navigation of the AWS Management Console and be comfortable editing scripts using a text editor.

# Task 1: Creating a VPC

In this task, you create a new VPC in the AWS Cloud.

- In the AWS Management Console, choose **Services** and select **VPC**. (You may also type VPC in the search bar and choose VPC.)
- Choose **Your VPCs** on the left navigation menu.

**Note:** You will see a default VPC (one is created whenever an AWS account is created). To learn more about default VPC, go to [Default VPC and default subnets](#)

- Choose **Create VPC** on the right side of the console.
- In the Create VPC section, enter the following:
- **Name tag:** Enter
- **IPv4 CIDR block:** Enter

**Note:** This VPC will not have an IPv6 CIDR block, and we will leave it with default tenancy.

- Choose **Create VPC**

A VPC with the specified CIDR block has been created. Now, let's create the subnets.

# Task 2: Creating subnets

A subnet is a range of IP addresses in your VPC. You can launch AWS resources into a specified subnet. Use a public subnet for resources that must be connected to the internet and a private subnet for resources that won't be connected to the internet. To protect the AWS resources in each subnet, you can use multiple layers of security, including security groups and network access control lists (ACL).

In this task, you create two public subnets and four private subnets in the Lab VPC (as shown in the Lab Overview's architecture diagram above).

## Create public subnets

The public subnets will be for internet-facing resources.

- In the left navigation pane, choose **Subnets**.

**Note:** You will see subnets for the default VPC. You can ignore them and go to the next step.

- Choose **Create subnet** and configure it with the following details:
- **VPC ID:** Select *LabVPC*
- **Subnet name:** Enter
- **Availability Zone:** Select the first Availability Zone in the list
- **IPv4 CIDR block:** Enter
- Choose **Create subnet**

**Note:** When you create a VPC, you must specify an IPv4 CIDR block for the VPC. The allowed block size is between a /16 netmask (65,536 IP addresses) and /28 netmask (16 IP addresses). The CIDR block of a subnet can be the same as the CIDR block for the VPC (for a single subnet in the VPC) or a subset of the CIDR block for the VPC (for multiple subnets). If you create more than one subnet in a VPC, the CIDR blocks of the subnets cannot overlap.

Tools are available on the internet to help you calculate and create IPv4 subnet CIDR blocks; for example, [IPv4 Address Planner](#).

One public subnet has been created. Now, create the other public subnet with the following details:

- **VPC ID:** Select
- **Subnet name:** Enter
- **Availability Zone:** Select the second Availability Zone in the list
- **IPv4 CIDR block:**

**Note:** Even though we named these subnets PublicSubnet, they are not yet public. A public subnet must have an internet gateway, which you will create and attach later in the lab.

## Create private subnets

The private subnets are for resources that remain isolated from the internet. In this lab, we create two private subnets for the EC2 instances and two private subnets for the RDS instances.

- Create the four private subnets with the following details:
- **PrivateSubnet1:**
  1. **VPC ID:** Select *LabVPC*
  2. **Subnet name:** Enter
  3. **Availability Zone:** Select the first Availability Zone in the list
  4. **IPv4 CIDR block:** Enter
- **PrivateSubnet2:**
  1. **VPC ID:** Select *LabVPC*
  2. **Subnet name:** Enter
  3. **Availability Zone:** Select the second Availability Zone in the list
  4. **IPv4 CIDR block:** Enter
- **PrivateSubnet3:**
  1. **VPC ID:** Select *LabVPC*
  2. **Subnet name:** Enter
  3. **Availability Zone:** Select the first Availability Zone in the list
  4. **IPv4 CIDR block:** Enter
- **PrivateSubnet4:**
  1. **VPC ID:** Select *LabVPC*
  2. **Name tag:** Enter
  3. **Availability Zone:** Select the second Availability Zone in the list
  4. **IPv4 CIDR block:** Enter

Your VPC now has six subnets in total: two public subnets for the Application Load Balancer in two different Availability Zones, two subnets for the EC2 instances in two different Availability Zones, and two subnets for the RDS instances in two different Availability Zones.

## Task 3: Creating an internet gateway

An internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between instances in a VPC and the internet. An internet gateway does not impose availability risks or bandwidth constraints on network traffic.

An internet gateway serves two purposes:

- Provide a target in route tables to connect to the internet
- Perform network address translation (NAT) for instances that have been assigned public IPv4 addresses

In this task, you create an internet gateway so that internet traffic can access the public subnets.

- In the left navigation pane, choose **Internet Gateways**.

**Note:** A default internet gateway was created with the default VPC. You can ignore this and proceed with the next step.

- Choose **Create internet gateway** and configure:
- **Name tag:** Enter
- Choose **Create internet gateway**

Once it's created, you need to attach the internet gateway to your Lab VPC.

- Choose **Actions** > **Attach to VPC**.
- For **VPC**, select *LabVPC*
- Choose **Attach internet gateway**

The internet gateway is now attached to your Lab VPC. You have created an internet gateway and attached it to your VPC, and you must now configure the route table of the public subnets to use the internet gateway. You'll do that after you create your NAT gateway.

## Task 4: Creating a NAT gateway

You can use a network address translation (NAT) gateway to enable instances in a private subnet to connect to the internet or other AWS services. The NAT gateway also prevents the internet from initiating a connection with those instances. For more information, see [NAT](#).

In this task, you create a NAT gateway so that the private subnets can connect to the internet.

- In the left navigation pane, choose **NAT Gateways**.
- Choose **Create NAT gateway** and configure:
  - **Name:** Enter
  - **Subnet:** Select *PublicSubnet1*
  - **Elastic IP allocation ID:** Choose

This will generate an Elastic IP address and will allocate it to the NAT gateway.

*An Elastic IP address is a public IPv4 address that is reachable from the internet. If your instance does not have a public IPv4 address, you can associate an Elastic IP address with your instance to enable communication with the internet. For example, this allows you to connect to your instance from your local computer.*

- Choose **Create NAT gateway**

The NAT gateway has been created. You must now configure the route table of the private subnets to use the NAT gateway.

## Task 5: Configuring route tables



A route table contains a set of rules, called *routes*, used to determine where network traffic is directed. Each subnet in a VPC must be associated with a route table, which controls the routing for the subnet. A subnet can only be associated with one route table at a time, but you can associate multiple subnets with the same route table.

In this task, you configure two route tables, one for the public subnets and one for the private subnets.

## Configure public route table

To use an internet gateway, a subnet's route table must contain a route that directs internet-bound traffic to the internet gateway. This subnet is called a *public subnet*.

You will:

- Create a public route table for internet-bound traffic
- Add a route to the route table to direct internet-bound traffic to the internet gateway
- Associate the public subnets with the new route table
- In the left navigation pane, choose **Route Tables**.

Several route tables are displayed, but there is only one route table associated with the Lab VPC. This is the main route table.

- Choose **Create route table** and configure:
  - **Name tag:** Enter
  - **VPC:** Select *LabVPC*
  - Choose **Create** and then choose **Close**
- Select **PublicRouteTable** and choose the **Routes** tab.
- Choose **Edit routes**

Now, add a route to direct internet-bound traffic (0.0.0.0/0) to the internet gateway.

- Choose **Add route** and configure:
- **Destination:** Enter
- **Target:** Select *Internet Gateway* and *LabVPCInternetGateway*.
- Choose **Save routes** and then choose **Close**

The last step is to associate this new route table with the public subnets.

- Choose the **Subnet Associations** tab.
- Choose **Edit subnet associations**
- On the Edit subnet associations page, select the rows with *PublicSubnet1* and *PublicSubnet2*.
- Choose **Save**

The PublicSubnet is now public because it has a route table entry that sends traffic to the internet via the internet gateway.

## Configure private route table

To use a NAT gateway, you must update the route table associated with one or more of your private subnets to point internet-bound traffic to the NAT gateway. This enables instances in your private subnets to communicate with the internet, mainly for any upgrades that needs to be installed.

You will:

- Create a private route table for private subnets
- Add a route to the route table for the NAT gateway
- Associate the private subnets with the new route table
- Choose **Create route table** and configure it with the following details:
- **Name tag:** Enter
- **VPC:** Select *LabVPC*
- Choose **Create** and then choose **Close**
- Select **PrivateRouteTable** and choose the **Routes** tab.

- Choose **Edit routes**

In the next step, you add a route to direct internet-bound traffic (0.0.0.0/0) to the NAT gateway.

- Choose **Add route** and configure:
- **Destination:** Enter 0.0.0.0/0
- **Target:** Select *NAT Gateway* and *LabVPCNATGateway*.
- Choose **Save routes** and then choose **Close**

The last step is to associate this new route table with the private subnets.

- Choose the **Subnet Associations** tab.
- Choose **Edit subnet associations**
- On the Edit subnet associations page, select all of the rows with *PrivateSubnet*.

**Note:** You may need to expand the Subnet ID column to see their full names.

- Choose **Save**

You have successfully created a route table and associated the private subnets to the NAT gateway in the public subnet so that the incoming traffic can reach the private subnets.

**Note:** If you have resources in multiple Availability Zones that share one NAT gateway, and if the NAT gateway's Availability Zone is down, resources in the other Availability Zones lose internet access. To create an AZ-independent architecture, create a NAT gateway in at least two Availability Zones that Amazon CloudWatch can monitor and configure your routing to ensure resources use the NAT gateway in the same Availability Zone.

## Task 6: Creating security groups

A security group acts as a virtual firewall for instances, controlling inbound and outbound traffic. Security groups operate at the instance network interface level, not the subnet level. Therefore, each instance can have its own firewall that controls traffic. If you do not specify a particular security group at launch time, the instance is automatically assigned to the default security group for the VPC.

In this task, you create three security groups for this lab: one for the RDS instances, one for the EC2 instances, and one for the Application Load Balancer (ALB). *The ALBSecurityGroup allows the application to be accessed from the internet.*

- In the left navigation pane, choose **Security Groups**.
- Choose **Create security group** and configure it with the following details:
  - **Security group name:** Enter
  - **Description:** Enter
  - **VPC:** Select *LabVPC*
  - For **Inbound rules**, choose **Add rule** and configure it with the following details:
    - **Type :** Select *All traffic*
    - **Source:** Select *0.0.0.0/0 (Anywhere)*
    - For **Tags - optional**, choose **Add new tag** and configure it with the following details:
      - **Key:** Enter
      - **Value:** Enter

**Note:** By adding tags, it will be easy to identify the subnets in the subnet list.

- At the bottom of the page, choose **Create security group**
- The inbound rules determine what traffic is permitted to reach the instance. You have configured it to permit HTTP (port 80) traffic coming from anywhere on the internet (0.0.0.0/0).

You will create the security group for the EC2 instances. *Only the ALBSecurityGroup will be allowed to talk to the EC2 instances.*

- In the left navigation pane, choose **Security Groups**.
- Create another new security group with the following details:
- **Security group name:** Enter
- **Description:** Enter
- **VPC:** Select *LabVPC*
- For **Inbound rules**, choose  and configure it with the following details:
  - **Type:** Select *Custom TCP*
  - **Port range:** Select *80*
  - **Source:** Select *LabVPCALBSG*
- Create another inbound rule with the following details:
  - **Type:** Select *Custom TCP*
  - **Port range:** Select *8443*
  - **Source:** Select *LabVPCALBSG*
- Create a new tag with the following details:
  - **Key:** Enter
  - **Value:** Enter
- Choose **Create security group**

You have configured the inbound rules to permit ALB (ports 80 and 8443) traffic to the EC2 instances.

Now, you will create an RDS Security Group so the EC2 instances can communicate to the RDS instances.

- In the left navigation pane, choose **Security Groups**.
- Create the last security group with the following details:
- **Security group name:** Enter
- **Description:** Enter
- **VPC:** Select *LabVPC*
- Add the following inbound rule:
  - **Type:** Select *MYSQL/Aurora*
  - **Port range:** *3306*
  - **Source:** Select *LABVPCEC2SG*
- Add the following tag:

- **Key:** Enter
- **Value:** Enter

This will allow the EC2 instances to communicate with the RDS instances on port 3306.

**Note:** You can grant access to a specific CIDR range, or to another security group in your VPC or in a peer VPC (requires a VPC peering connection). When you specify a security group as the source for a rule, traffic is allowed from the network interfaces that are associated with the source security group for the specified protocol and port. Incoming traffic is allowed based on the private IP addresses of the network interfaces that are associated with the source security group (and not the public IP or Elastic IP addresses). Adding a security group as a source does not add rules from the source security group.

## Task 7: Launch web app instances and database resources, and deploy the application

In this task, you provision the RDS and EC2 instances in the private subnets and configure an Application Load Balancer in the public subnets. To test the VPC, you also deploy a web application to read a population census.

### Create the database in the private subnets

Create a DB (database) subnet group so that the RDS will be deployed within the subnets you want to use.

- On the **Services** menu, type RDS in the search bar and choose RDS.

- In the left navigation pane, choose *Subnet groups*.
- Choose **Create DB subnet group** and configure it with the following details:
- **Name:** Enter
- **Description:** Enter
- **VPC:** Select *LabVPC*
- **Availability Zones:** Select the two Availability Zones you used to create the subnets (they should be the first two listed).
- **Subnets:** Choose *10.0.13.0/24* and *10.0.14.0/24*
- Choose **Create**

The DB subnet group has been created successfully. Now let's create the database.

- In the left navigation pane, choose **Databases**.
- Choose **Create database** and configure it with the following details:
- **Choose a database creation method:** *Standard Create*
- **Engine Options:**
  1. **Engine type:** Select *MySQL*
  2. **Templates:** *Free tier*
  3. In the settings Section, configure
- **Templates:** Select *Free tier*
- **Settings:**
  1. **DB Cluster identifier:** Enter
  2. **Master username:** Leave the default as
  3. **Master password:** Enter
  4. **Confirm password:** Enter
- In the **Storage** Section
  1. Disable **Enable storage autoscaling**
- **Connectivity:**
  1. **Virtual private cloud(VPC):** Select *LabVPC*
- **Subnet group:** Select *LabVPCRDSSubnetgroup*
- **Public access:** Select *No*
- **VPC security group:** Select *Choose existing*

- **Existing VPC security groups:** Select *LabVPCRDSSG* and remove *default*
- **Database port:** Select 3306
- Choose **Additional Configuration**
- **Initial database name:** Enter
- Uncheck *automatic backups* in the **Backup** section.

The other values will be left to the default values selected.

- Choose **Create database**

This will create a writer instance in one Availability Zone and a reader instance in the other Availability Zone. It will take few minutes to complete. Choose the refresh button to see the status updated. You can proceed once you receive the *Successfully created database* message.

- Choose *LabVPCDBCluster* under **DB identifier** and then copy the *Endpoint name* under **Endpoints** for the *Writer* type and the *Reader* type. These will be needed when the application is deployed on the EC2 instances.

**Note:** The database may initially show two *Reader* types, but it will show the *Writer* type once the creation is complete.

## Configure the EC2 instances

The next step is to create the EC2 instances and deploy the application code. If you want the application to be highly available in different Availability Zones, it's a good practice to create a *launch template* and reuse it for deploying the EC2 instance instead of creating from scratch every time.

You will create the launch template first.

- On the **Services** menu, choose EC2.
- In the left navigation pane, choose **Launch templates**.
- Choose **Create launch template** and configure it with the following details:
- **Launch template name and description:**



1. **Launch template name:** Enter
  2. **Template version description:**  
Enter
- **Amazon machine image (AMI):**
    1. **AMI:** Select *Amazon Linux 2 AMI (HVM), SSD Volume Type*
  - **Instance type:**
    1. **Instance type:** Select *t2.micro*
  - **Key pair:**
    1. **Key pair name:** Select your keypair name
  - **Network settings:**
    1. **Networking platform:** Select *Virtual Private Cloud (VPC)*
    2. **Security groups:** Select *LabVPCEC2SG*
  - **Resource tags:** Click Add tag and add the following

▼ **Resource tags** [Info](#)

Key <a href="#">Info</a>	Value <a href="#">Info</a>	Resource types <a href="#">Info</a>
<input type="text" value="Name"/>	<input type="text" value="web-server"/>	<input type="text" value="Select resource types"/>
		<input type="button" value="Instances"/>

49 remaining (Up to 50 tags maximum)

- Choose **Advanced details**
- **User data:** Copy and paste the following script into the empty field.

```
#!/bin/sh
yum -y install httpd php
chkconfig httpd on
systemctl start httpd.service
cd /var/www/html
wget https://s3-us-west-2.amazonaws.com/us-west-2-aws-training/awsu-spl/spl-03/scripts/examplefiles-elb.zip
unzip examplefiles-elb.zip
```

*This script deploys the application on the EC2 instance along with the EC2 launch process.*

- De-select **User data has already been base64 encoded.**
- Choose **Create launch template**
- At the bottom of the page, choose **View launch templates**

- Select launch template
- Click > **Action** > and select **Launch instance from template**
- Click **Launch instance**

## Create an Application Load Balancer

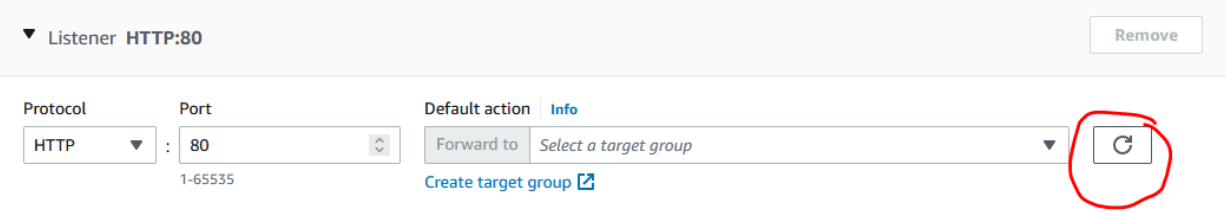
You will create an Application Load Balancer in the public subnets to access the application from a browser.

- In the left navigation pane, choose **Load Balancers**.
- Choose **Create Load Balancer**
- Choose **Create** in the **Application Load Balancer** column.
- Configure the **Configure Load Balancer** tab with the following details:
  - **Basic Configuration:**
    1. **Load balancer name:** Enter
  - Scheme: **Internet-facing**
  - **Availability Zones:**
    1. **VPC:** Select
    2. **Mappings:**
      1. Select the check box for the first Availability Zone listed, and select  from the subnet list.
      2. Select the check box for the second Availability Zone listed, and select  from the subnet list.
  - **Security group**
    1. Select **LabVPCEC2SG**
  - **Listeners and routing**
  - Click on **Create target group** to open a new tab
  - **Target group name:** Enter

- Protocol: **HTTP**
- Port: **80**
- Select VPC
- Click **Next:** and configure the following:
- **Available instances:**
  1. Select the EC2 instance that has been deployed in the previous steps.
  2. Click **Include as pending below**

The instance will now appear under the **Registered targets** at the top.

- Click **Create target group group**
- Choose **Close**
- Navigate to the previous tab and click on the refresh icon refresh



▼ Listener HTTP:80 Remove

Protocol: HTTP Port: 80 Default action: Info

Forward to: Select a target group ↻

1-65535 [Create target group](#)

- Click on the drop down and select newly created target group
- Click **Create load balancer**

The load balancer will appear to be in the *provisioning* state for few minutes and will then change to *active*.

- Select the check box for the load balancer **LabVPC/**.
- From the **Description** tab, copy the **DNS Name** and paste the value in a new browser to invoke the load balancer.

You should see the application **Population Facts** displayed with two fields: **Choose year** and **Choose Country**. Press the **Submit** button to test the application. You should see the results related to the census for that particular

country and year. To keep testing, use the back button to go back and select other values.

## Conclusion

Congratulations! You now have successfully:

- Created a VPC
- Created public and private subnets
- Created an internet gateway and a NAT gateway
- Configured route tables and associated them to subnets
- Deployed a 3-tier web application to the VPC