 Marwadi University Marwadi Chandarana Group	Marwadi University Faculty of Technology Department of Information and Communication Technology	
Subject: Cloud Technical Essentials – 01CT0823	Aim: Create a VPC and perform the following task. <ul style="list-style-type: none"> • Create subnets. • Configure a security group. • Launch an EC2 instance into a VPC. 	
Experiment No: 02	Date: 01/02/24	Enrolment No: 92000133037

Aim: Create a VPC and perform the following task.

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

Lab overview and objectives

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 a security group. You will then configure and customize an EC2 instance to run a web server and you will launch the EC2 instance to run in a subnet in 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.

After completing this lab, you should be able to do the following:

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

Duration

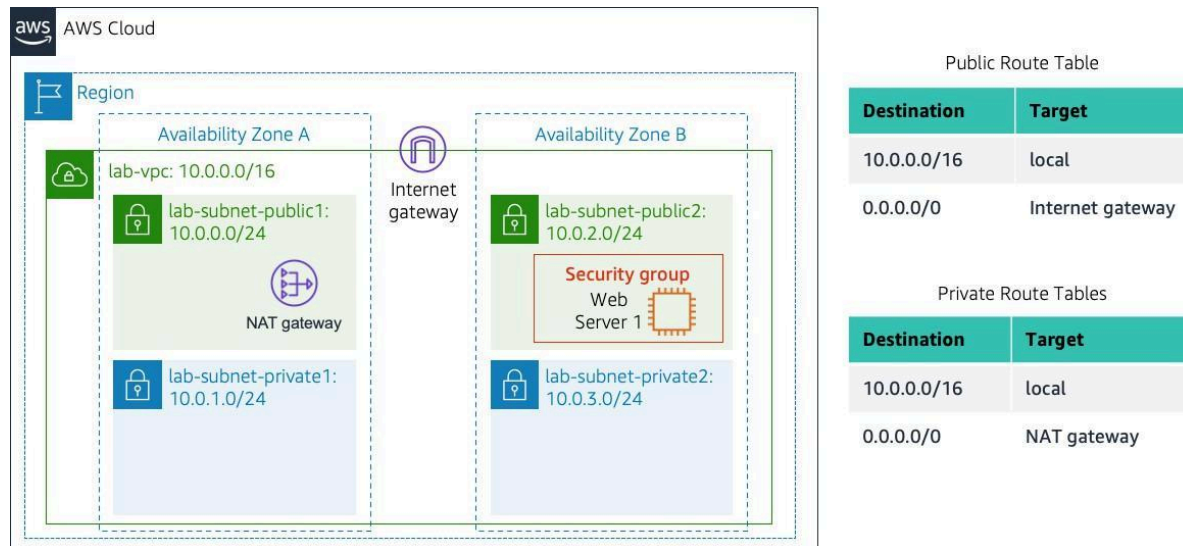
This lab takes approximately **30 minutes** to complete.

AWS service restrictions

In this lab environment, access to AWS services and service actions might be restricted to the ones that are needed to complete the lab instructions. You might encounter errors if you attempt to access other services or perform actions beyond the ones that are described in this lab.

Scenario

In this lab you build the following infrastructure:



Accessing the AWS Management Console

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

A Start Lab panel opens displaying the lab status.

2. Wait until you see the message "**Lab status: ready**", then choose the **X** to close the Start Lab panel
3. At the top of these instructions, choose AWS

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

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. Choose on the banner or icon and choose "Allow pop ups."

4. Arrange the AWS Management Console tab so that it displays along side 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.

Task 1: Create Your VPC

In this task, you will use the *VPC and more* option in the VPC console to create multiple resources, including a *VPC*, an *Internet Gateway*, a *public subnet* and a *private subnet* in a single Availability Zone, two *route tables*, and a *NAT Gateway*.

5. In the search box to the right of **Services**, search for and choose **VPC** to open the VPC console.
6. Begin creating a VPC.
 - In the top left of the screen, verify the **New VPC Experience** is toggled *on*. If it is not, toggle it on now.
 - Choose the **VPC dashboard** link which is also towards the top left of the console.
 - Next, choose Create VPC.

Note: If you do not see a button with that name, choose the Launch VPC Wizard button instead.

7. Configure the VPC details in the *VPC settings* panel on the left:
 - Choose **VPC and more**.
 - Under **Name tag auto-generation**, keep *Auto-generate* selected, however change the value from project to lab.
 - Keep the **IPv4 CIDR block** set to 10.0.0.0/16
 - For **Number of Availability Zones**, choose **1**.
 - For **Number of *public* subnets**, keep the **1** setting.
 - For **Number of *private* subnets**, keep the **1** setting.
 - Expand the **Customize subnets CIDR blocks** section
 - Change **Public subnet CIDR block in us-east-1a** to 10.0.0.0/24
 - Change **Private subnet CIDR block in us-east-1a** to 10.0.1.0/24
 - Set **NAT gateways** to **In 1 AZ**.
 - Set **VPC endpoints** to **None**.
 - Keep both **DNS hostnames** and **DNS resolution** *enabled*.
8. In the *Preview* panel on the right, confirm the settings you have configured.
 - **VPC:** lab-vpc
 - **Subnets:**
 - us-east-1a
 - **Public subnet name:** lab-subnet-public1-us-east-1a
 - **Private subnet name:** lab-subnet-private1-us-east-1a
 - **Route tables**
 - lab-rtb-public
 - lab-rtb-private1-us-east-1a
 - **Network connections**
 - lab-igw
 - lab-nat-public1-us-east-1a
 -
9. At the bottom of the screen, choose Create VPC

AIM: Build your VPC and Launch a Web Server

The VPC resources are created. The NAT Gateway will take a few minutes to activate.

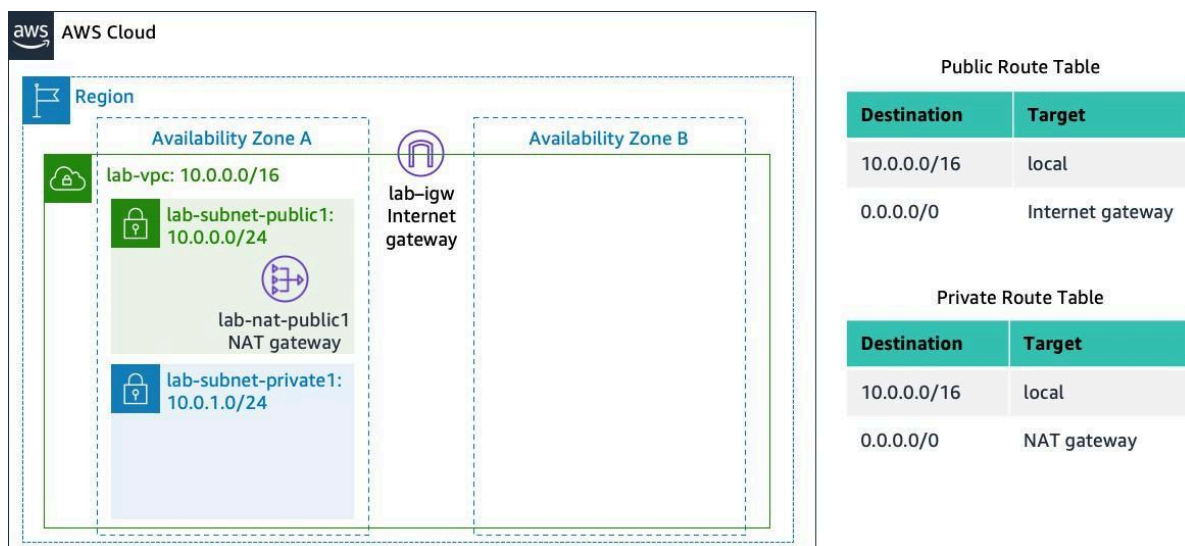
Please wait until *all* the resources are created before proceeding to the next step.

10. Once it is complete, choose View VPC

AIM: Build your VPC and Launch a Web Server

The wizard has provisioned a VPC with a public subnet and a private subnet in one Availability Zone with route tables for each subnet. It also created an Internet Gateway and a NAT Gateway.

To view the settings of these resources, browse through the VPC console links that display the resource details. For example, choose **Subnets** to view the subnet details and choose **Route tables** to view the route table details. The diagram below summarizes the VPC resources you have just created and how they are configured.



An *Internet gateway* is a VPC resource that allows communication between EC2 instances in your VPC and the Internet.

The lab-subnet-public1-us-east-1a 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 fact the route table associated with this public subnet routes 0.0.0.0/0 network traffic to the internet gateway is what makes it a public subnet.

A *NAT Gateway*, is a VPC resource used to provide internet connectivity to any EC2 instances running in *private* subnets in the VPC without those EC2 instances needing to have a direct connection to the internet gateway.

The lab-subnet-private1-us-east-1a 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**.

AIM: Build your VPC and Launch a Web Server

The screenshot displays the AWS Management Console interface. The top navigation bar includes the AWS logo, a search bar, and user information for 'voclabs/user3031298=Aniket' in the 'N. Virginia' region. The left sidebar shows the 'Virtual private cloud' section with 'Your VPCs' selected. The main content area shows the details for VPC 'vpc-0cd3660c9896cb588 / lab-vpc'. The 'Details' tab is active, displaying a table of VPC attributes. Below the details, there are tabs for 'Resource map', 'CIDRs', 'Flow logs', 'Tags', and 'Integrations'. The 'Resource map' tab is currently selected. The bottom of the console shows a Windows taskbar with various application icons and system information.

vpc-0cd3660c9896cb588 / lab-vpc			
VPC ID vpc-0cd3660c9896cb588	State Available	DNS hostnames Enabled	DNS resolution Enabled
Tenancy Default	DHCP option set dopt-0223e6647b98500c0	Main route table rtb-017e2915c5e473dc5	Main network ACL acl-0d41189d3e4943851
Default VPC No	IPv4 CIDR 10.0.0.0/16	IPv6 pool -	IPv6 CIDR (Network border group) -
Network Address Usage metrics Disabled	Route 53 Resolver DNS Firewall rule groups -	Owner ID 654654201744	

Task 2: Create Additional Subnets

In this task, you will create two additional subnets for the VPC in a second Availability Zone. Having subnets in multiple Availability Zones within a VPC is useful for deploying solutions that provide *High Availability*.

After creating a VPC as you have already done, you can still configure it further, for example, by adding more **subnets**. Each subnet you create resides entirely within one Availability Zone.

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

First, you will create a second *public* subnet.

12. Choose Create subnet then configure:

- **VPC ID:** **lab-vpc** (select from the menu).
- **Subnet name:** lab-subnet-public2
- **Availability Zone:** Select the *second* Availability Zone (for example, us-east-1b)
- **IPv4 CIDR block:** 10.0.2.0/24

The subnet will have all IP addresses starting with **10.0.2.x**.

13. Choose Create subnet

The second *public* subnet was created. You will now create a second *private* subnet.

14. Choose Create subnet then configure:

- **VPC ID:** lab-vpc
- **Subnet name:** lab-subnet-private2
- **Availability Zone:** Select the *second* Availability Zone (for example, us-east-1b)
- **IPv4 CIDR block:** 10.0.3.0/24

The subnet will have all IP addresses starting with **10.0.3.x**.

15. Choose Create subnet

The second *private* subnet was created.

You will now configure this new *private* subnet to route internet-bound traffic to the NAT Gateway so that resources in the second 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.

16. In the left navigation pane, choose **Route tables**.

17. Select the **lab-rtb-private1-us-east-1a** route table.

18. In the lower pane, choose the **Routes** tab.

Note that **Destination 0.0.0.0/0** is set to **Target nat-xxxxxxx**. 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.

19. Choose the **Subnet associations** tab.

You created this route table in task 1 when you chose to create a VPC and multiple resources in the VPC. That action also created *lab-subnet-private-1* and associated that subnet with this route table.

Now that you have created another private subnet, *lab-subnet-private-2*, you will associate this route table with that subnet as well.

20. Choose Edit subnet associations

21. Leave **lab-subnet-private1-us-east-1a** selected, but also select **lab-subnet-private2**.

22. Choose Save associations

You will now configure the Route Table that is used by the Public Subnets.

23. Select the **lab-rtb-public** route table (and deselect any other subnets).

24. In the lower pane, choose the **Routes** tab.

Note that **Destination 0.0.0.0/0** is set to **Target igw-xxxxxxx**, 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 second public subnet you created.

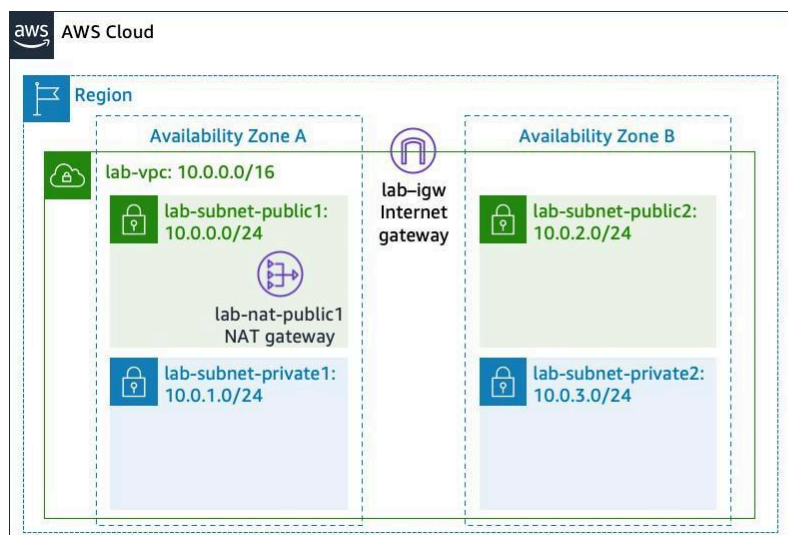
25. Choose the **Subnet associations** tab.

26. Choose Edit subnet associations

27. Leave **lab-subnet-public1-us-east-1a** selected, but also select **lab-subnet-public2**.

28. Choose Save associations

Your VPC now has public and private subnets configured in two Availability Zones. The route tables you created in task 1 have also been updated to route network traffic for the two new subnets.



Public Route Table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	Internet gateway

Private Route Table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	NAT gateway

AIM: Build your VPC and Launch a Web Server

aws

Services

Search

[Alt+S]

N. Virginia

voclabs/user3031298-Aniket @ 6546-5420-1744

VPC dashboard

EC2 Global View

Filter by VPC:
Select a VPC

Virtual private cloud

Your VPCs

Subnets

Route tables

Internet gateways

Egress-only internet gateways

Carrier gateways

DHCP option sets

Elastic IPs

Managed prefix lists

Endpoints

Endpoint services

NAT gateways

You have successfully updated subnet associations for rtb-0f04fa4594793d4e4 / lab-rtb-public.

Route tables (1/6)

Find resources by attribute or tag

< 1 >

Actions

Create route table

	Name	Route table ID	Explicit subnet associ...	Edge associations	Main
<input type="checkbox"/>	-	rtb-0e4b0f9d1f37cd666	-	-	Yes
<input type="checkbox"/>	lab-rtb-private1-us-east-1a	rtb-06d52070f0d40b731	2 subnets	-	No

Details

Routes

Subnet associations

Edge associations

Route propagation

Tags

Explicit subnet associations (2)

Find subnet association

< 1 >

Edit subnet associations

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
lab-subnet-public1-us-east-1a	subnet-0774632376972a6cc	10.0.0.0/24	-
lab-subnet-public2	subnet-07e513ea5ec92c350	10.0.2.0/24	-

Subnets without explicit associations (0)

Find subnet association

< 1 >

Edit subnet associations

CloudShell

Feedback

© 2024, Amazon Web Services, Inc. or its affiliates.

Privacy

Terms

Cookie preferences

27°C
Clear

Search

ENG
US

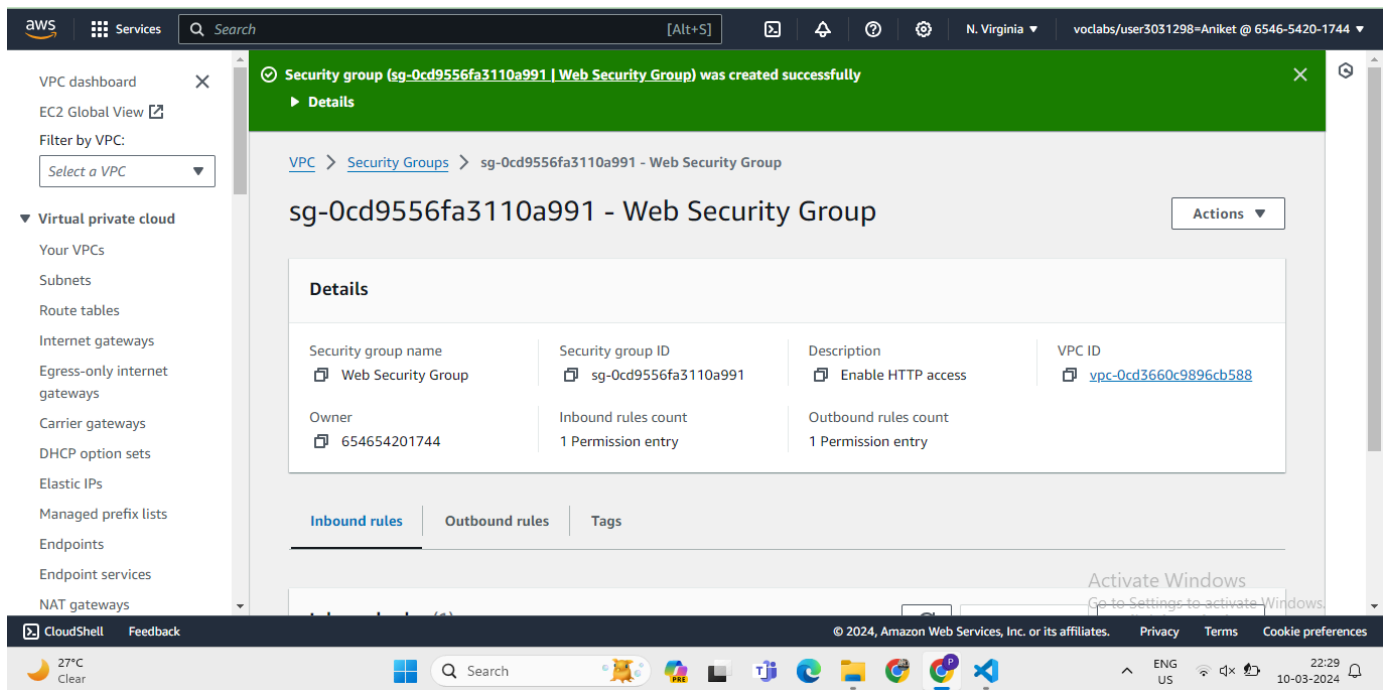
22:26
10-03-2024

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.

29. In the left navigation pane, choose **Security groups**.
30. Choose Create security group and then configure:
 - **Security group name:** Web Security Group
 - **Description:** Enable HTTP access
 - **VPC:** choose the X to remove the currently selected VPC, then from the drop down list choose **lab-vpc**
31. In the **Inbound rules** pane, choose Add rule
32. Configure the following settings:
 - **Type:** *HTTP*
 - **Source:** *Anywhere-IPv4*
 - **Description:** Permit web requests
33. Scroll to the bottom of the page and choose 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.

34. In the search box to the right of **Services**, search for and choose **EC2** to open the EC2 console.

35. From the Launch instance menu choose **Launch instance**.

36. Name the instance:

- Give it the name Web Server 1

When you name your instance, AWS creates a tag and associates it with the instance. A tag is a key value pair. The key for this pair is **Name**, and the value is the name you enter for your EC2 instance.

37. Choose an AMI from which to create the instance:

- In the list of available *Quick Start* AMIs, keep the default **Amazon Linux** AMI selected.
- Also keep the default **Amazon Linux 2 AMI (HVM)** selected.

The type of *Amazon Machine Image (AMI)* you choose determines the Operating System that will run on the EC2 instance that you launch.

38. Choose an Instance type:

- In the *Instance type* panel, keep the default **t2.micro** selected.

The *Instance Type* defines the hardware resources assigned to the instance.

39. Select the key pair to associate with the instance:

- From the **Key pair name** menu, select **vockey**.

The vockey key pair you selected will allow you to connect to this instance via SSH after it has launched. Although you will not need to do that in this lab, it is still required to identify an existing key pair, or create a new one, when you launch an instance.

40. Configure the Network settings:

- Next to Network settings, choose **Edit**, then configure:
 - **Network:** *lab-vpc*
 - **Subnet:** *lab-subnet-public2* (not Private!)
 - **Auto-assign public IP:** *Enable*
- Next, you will configure the instance to use the *Web Security Group* that you created earlier.
 - Under Firewall (security groups), choose **Select an existing security group**.
 - For **Common security groups**, select **Web Security Group**.

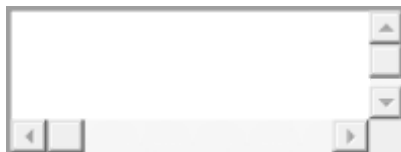
This security group will permit HTTP access to the instance.

41. In the *Configure storage* section, keep the default settings.

Note: The default settings specify that the *root volume* of the instance, which will host the Amazon Linux 2 guest operating system that you specified earlier, will run on a general purpose SSD (*gp2*) hard drive that is 8 GiB in size. You could alternatively add more storage volumes, however that is not needed in this lab.

42. Configure a script to run on the instance when it launches:

- Expand the **Advanced details** panel.
- Scroll to the bottom of the page and then copy and paste the code shown below 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.us-west-2.amazonaws.com/CUR-TF-100-ACCLFO-2-
9026/2-lab2-vpc/s3/lab-app.zip
unzip lab-app.zip -d /var/www/html/
```

AIM: Build your VPC and Launch a Web Server

Turn on web server

AIM: Build your VPC and Launch a Web Server

```
chkconfig httpd on
service httpd start
```

This script will run with root user permissions on the guest OS of the instance. It will run automatically when the instance launches for the first time. The script installs a web server, a database, and PHP libraries, and then it downloads and installs a PHP web application on the web server.

43. At the bottom of the **Summary** panel on the right side of the screen choose Launch

instance You will see a Success message.

44. Choose View all instances

45. Wait until **Web Server 1** shows *2/2 checks passed* in the **Status check** column.

This may take a few minutes. Choose the refresh icon at the top of the page every 30 seconds or so to more quickly become aware of the latest status of the instance.

You will now connect to the web server running on the EC2 instance.

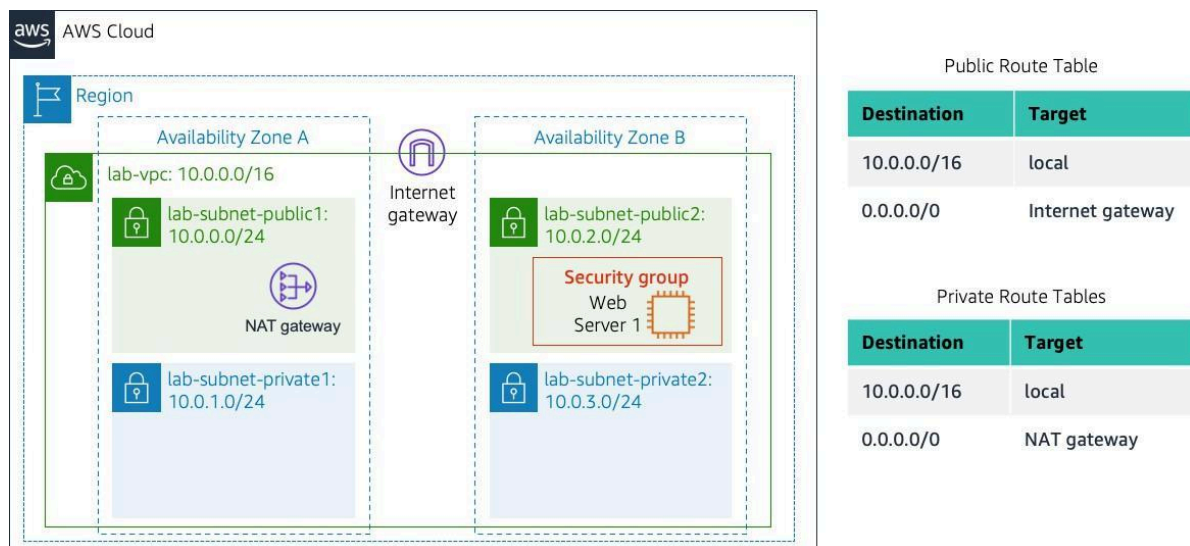
46. Select **Web Server 1**.

47. Copy the **Public IPv4 DNS** value shown in the **Details** tab at the bottom of the page.

48. 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.

The complete architecture you deployed is:



AIM: Build your VPC and Launch a Web Server

aws

Services

Search

[Alt+S]

N. Virginia

voclabs/user3031298-Aniket @ 6546-5420-1744

EC2 Dashboard

EC2 Global View

Events

Console-to-Code

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Capacity Reservations

Images

AMI Catalog

Instances (1/2) Info

Find Instance by attribute or tag (case-sensitive)

Any state

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
<input checked="" type="checkbox"/>	Web Server 1	i-0713d39cb18e4a44e	Running	t2.micro	-	View alarms +	us-east-1b
<input type="checkbox"/>	Bastion Host	i-0e947f075791691df	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1a

Instance: i-0713d39cb18e4a44e (Web Server 1)

DetailsStatus and alarmsNewMonitoringSecurityNetworkingStorageTags

Instance summary Info

Instance ID

i-0713d39cb18e4a44e (Web Server 1)

Public IPv4 address

3.238.153.106open address

Private IPv4 addresses

10.0.2.94

Instance state

Running

Public IPv4 DNS

ec2-3-238-153-106.compute-1.amazonaws.comopen address

CloudShell

Feedback

© 2024, Amazon Web Services, Inc. or its affiliates.

Privacy

Terms

Cookie preferences

27°C Clear

Search

ENG US

22:37

10-03-2024

Lab Complete

Congratulations! You have completed the lab.

49. Choose End Lab at the top of this page and then choose Yes to confirm that you want to end the lab.

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

50. Choose the **X** in the top right corner to close the panel.

Conclusion