

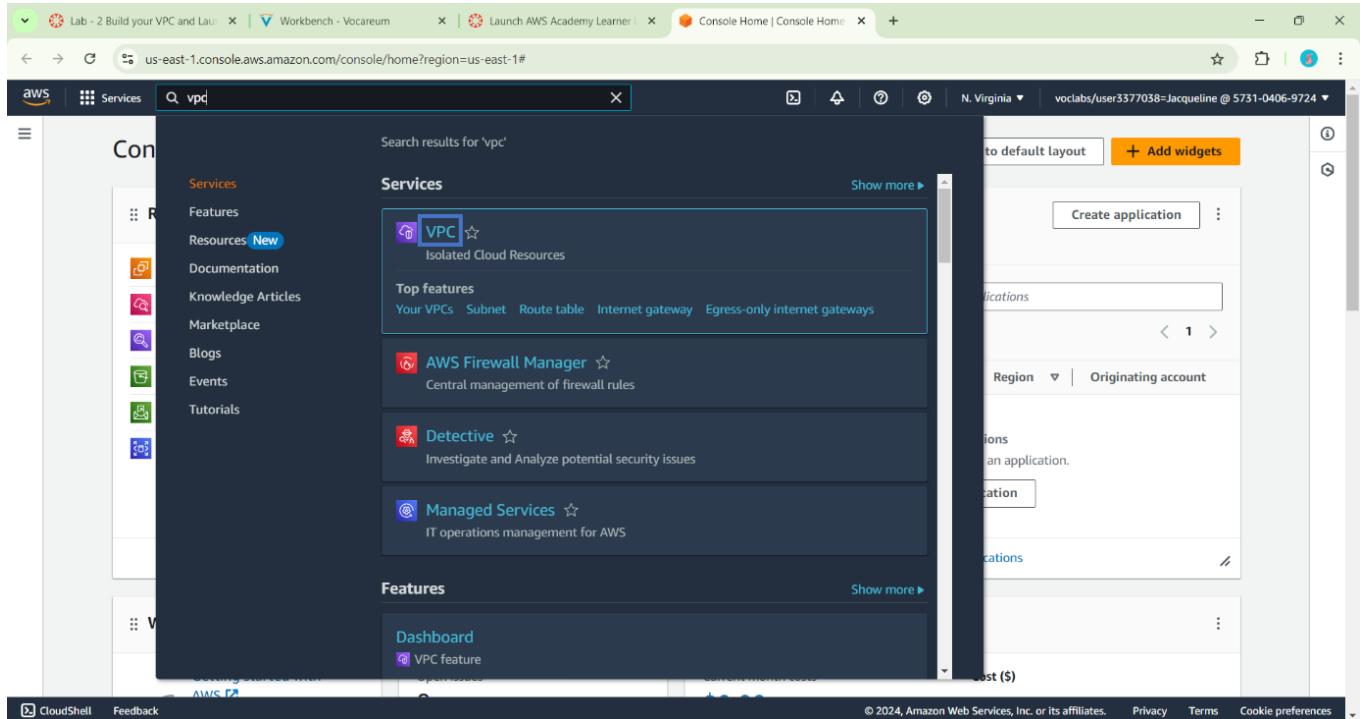
Implementation of VPC using AWS.

Prepare Screen shots file and also write down the steps.

Make single word or PDF file.

Task 1: Create Your VPC

Step 1: Search for and choose VPC to open the VPC console.



Step 2: Choose the VPC dashboard link which is towards the top left of the console and then choose Create VPC.

The screenshot shows the AWS VPC Console Home page. At the top, there are tabs for 'Lab - 2 Build your VPC and Lau' (active), 'Workbench - Vocareum', 'Launch AWS Academy Learner', and 'Home | VPC Console'. The main content area is titled 'VPC dashboard' and features a 'Create VPC' button and a 'Launch EC2 Instances' button. Below these are sections for 'Resources by Region' and 'Service Health'. The 'Resources by Region' section lists various VPC components with counts: VPCs (2), Subnets (7), Route Tables (3), Internet Gateways (2), and Egress-only Internet Gateways (0). The 'Service Health' section shows 'N. Virginia' with a status of 'OK'. On the left sidebar, there's a 'Virtual private cloud' section with links for Your VPCs, Subnets, Route tables, Internet gateways, Carrier gateways, DHCP option sets, Elastic IPs, Managed prefix lists, Endpoints, Endpoint services, NAT gateways, and Peering connections. A 'Security' section is also present. At the bottom, there are links for CloudShell and Feedback.

Step 3: Configure the VPC details in the VPC settings panel on the left as done below:

The screenshot shows the 'CreateVpc | VPC Console' page. The top navigation bar includes tabs for 'Lab - 2 Build your VPC and Lau' (active), 'Workbench - Vocareum', 'Launch AWS Academy Learner', and 'CreateVpc | VPC Console'. The main content area has two sections: 'VPC settings' on the left and 'Preview' on the right. In the 'VPC settings' section, under 'Resources to create', the 'VPC and more' radio button is selected. Under 'Name tag auto-generation', the 'Auto-generate' checkbox is checked and the value 'lab' is entered. Under 'IPv4 CIDR block', the value '10.0.0.0/16' is specified, which is noted to provide 65,536 IPs. Under 'IPv6 CIDR block', the 'No IPv6 CIDR block' radio button is selected. Under 'Tenancy', the 'Default' option is chosen. The 'Preview' section shows a diagram of the VPC structure: a central 'VPC' box labeled 'Show details' and 'Your AWS virtual network' with the name 'lab-vpc'. It branches into two 'Subnets (2)' boxes, each containing two subnets: 'us-east-1a' (with subnets 'lab-subnet-public1-us-east-1a' and 'lab-subnet-private1-us-east-1a') and 'us-east-1b' (with subnets 'lab-subnet-public2-us-east-1b' and 'lab-subnet-private2-us-east-1b'). These subnets are connected to a single 'Route tables (2)' box labeled 'Route network traffic to' with the name 'lab-rtb-public'. The bottom of the page includes standard AWS footer links for CloudShell, Feedback, Privacy, Terms, and Cookie preferences.

Screenshot of the AWS VPC Console 'CreateVpc' wizard, Step 1: Set VPC parameters.

Number of Availability Zones (AZs) (Info)
Choose the number of AZs in which to provision subnets. We recommend at least two AZs for high availability.
1 **2** **3**

Number of public subnets (Info)
The number of public subnets to add to your VPC. Use public subnets for web applications that need to be publicly accessible over the internet.
0 **1** **2**

Number of private subnets (Info)
The number of private subnets to add to your VPC. Use private subnets to secure backend resources that don't need public access.
0 **1** **2**

Public subnet CIDR block in us-east-1a
10.0.0.0/24 256 IPs

Private subnet CIDR block in us-east-1a
10.0.1.0/24 256 IPs

NAT gateways (\$) (Info)
Choose the number of Availability Zones (AZs) in which to create NAT gateways. Note that there is a charge for each NAT gateway.
None **In 1 AZ** **1 per AZ**

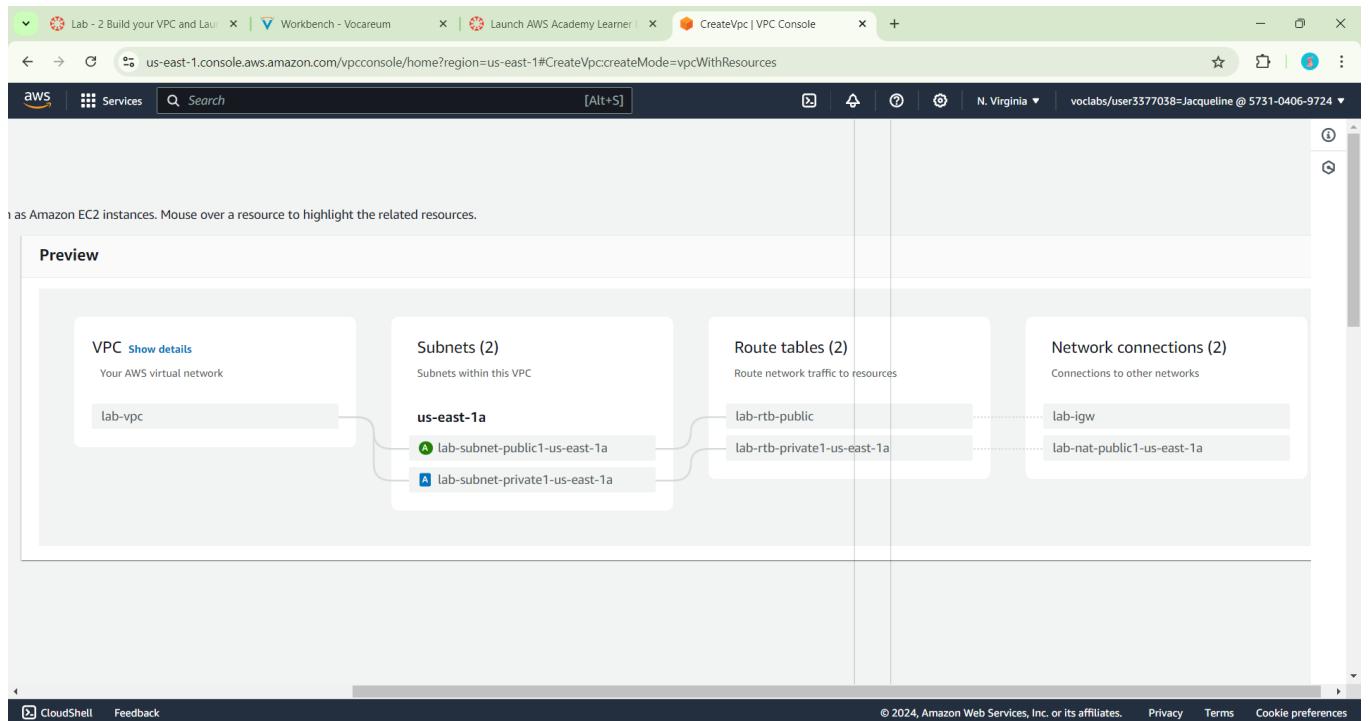
VPC endpoints (Info)
Endpoints can help reduce NAT gateway charges and improve security by accessing S3 directly from the VPC. By default, full access policy is used. You can customize this policy at any time.
None **S3 Gateway**

DNS options (Info)
 Enable DNS hostnames
 Enable DNS resolution

Additional tags

Create VPC

Step 4: In the Preview panel on the right, confirm the settings you have configured.



Step 5: At the bottom of the screen, choose Create VPC.

The screenshot shows the 'Create VPC' configuration page. It includes fields for 'Public subnet CIDR block in us-east-1a' (10.0.0.0/24) and 'Private subnet CIDR block in us-east-1a' (10.0.1.0/24). Under 'NAT gateways (\$)', there are three options: 'None', 'In 1 AZ', and '1 per AZ', with 'In 1 AZ' selected. Under 'VPC endpoints', there are two options: 'None' and 'S3 Gateway', with 'None' selected. Under 'DNS options', there are two checked checkboxes: 'Enable DNS hostnames' and 'Enable DNS resolution'. At the bottom, there are 'Cancel' and 'Create VPC' buttons, with 'Create VPC' highlighted.

Step 6: It will look like this then choose View VPC.

The screenshot shows the 'Create VPC workflow' page in the AWS VPC console. A 'Success' message is displayed at the top. Below it, a 'Details' section lists 21 completed tasks, each with a green checkmark and a link icon. The tasks include creating the VPC, enabling DNS hostnames and resolution, verifying VPC creation, creating subnets, creating an internet gateway, attaching it to the VPC, creating route tables, associating them with subnets, allocating elastic IPs, creating NAT gateways, and waiting for them to activate. At the bottom right is a yellow 'View VPC' button.

Task 2: Create Additional Subnets

Step 7: In the left navigation pane, choose Subnets and then choose create subnet then configure as shown below and click create subnet. (Subnet name: lab-subnet-public2)

The screenshot shows the 'Subnets (7) Info' page in the AWS VPC console. On the left, a navigation pane has 'Subnets' selected under the 'Virtual private cloud' section. The main area displays a table of 7 existing subnets with columns for Name, Subnet ID, State, VPC, and IPv4 CIDR. A 'Create subnet' button is located at the top right of the table. Below the table, a 'Select a subnet' dropdown menu is open, showing options to select a specific subnet or create a new one.

Lab - 2 Build your VPC and Lau... | Workbench - Vocareum | Launch AWS Academy Learner | CreateSubnet | VPC Console

us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#CreateSubnet:

Services Search [Alt+S]

lab-subnet-public2

Name can be up to 256 characters long.

Availability Zone **Info**
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
US East (N. Virginia) / us-east-1

IPv4 VPC CIDR block **Info**
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.
10.0.0.0/16

IPv4 subnet CIDR block
10.0.2.0/24 256 IPs

Tags - optional

Key	Value - optional
Q Name	Q lab-subnet-public2

Add new tag
You can add 49 more tags.
Remove

Add new subnet

Cancel **Create subnet**

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Step 8: Again, choose Create subnet then configure as done below and click create subnet. (Subnet name: lab-subnet-private2)

Lab - 2 Build your VPC and Lau... | Workbench - Vocareum | Launch AWS Academy Learner | subnets | VPC Console

us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#subnets:subnetId=subnet-013cc8efe49ca2c31

VPC dashboard

Subnets (1) **Info**

You have successfully created 1 subnet: subnet-013cc8efe49ca2c31

Last updated less than a minute ago Actions **Create subnet**

Find resources by attribute or tag Subnet ID : subnet-013cc8efe49ca2c31 Clear filters

Name	Subnet ID	State	VPC	IPv4 CIDR
lab-subnet-public2	subnet-013cc8efe49ca2c31	Available	vpc-0c89aa4ac7bfe8ae0 lab-vpc	10.0.2.0/24

Select a subnet

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Lab - 2 Build your VPC and Lau | Workbench - Vocareum | Launch AWS Academy Learner | CreateSubnet | VPC Console

us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#CreateSubnet:

Services Search [Alt+S]

Name: lab-subnet-private2
Name can be up to 256 characters long.

Availability Zone: US East (N. Virginia) / us-east-1

IPv4 VPC CIDR block: 10.0.0.0/16

IPv4 subnet CIDR block: 10.0.3.0/24 (256 IPs)

Tags - optional: Name: lab-subnet-private2

Create subnet

Step 9: In the left navigation pane, choose Route tables. Select the lab-rtb-private1-us-east-1a route table.

Lab - 2 Build your VPC and Lau | Workbench - Vocareum | Launch AWS Academy Learner | RouteTables | VPC Console

us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#RouteTables:

VPC dashboard

Name	Route table ID	Explicit subnet assoc...	Edge associations	Main	VPC
lab-rtb-public	rtb-05457dae0a3b5361f	subnet-01096ecf68aae7f...	-	No	vpc-0c89aa4ac7bfe8ae0 lab
-	rtb-079861962ca1a3ba9	-	-	Yes	vpc-0c89aa4ac7bfe8ae0 lab
Work Public Route Table	rtb-0de0decba3f001437	subnet-0c2ec6f81d63b5...	-	No	vpc-0fe43107c3b1e00cc Work
<input checked="" type="checkbox"/> lab-rtb-private1-us-east-1a	rtb-0d14ddb9bef814666	subnet-0ad9811c2a67ea...	-	No	vpc-0c89aa4ac7bfe8ae0 lab
-	rtb-00ed5e08a95c7d543	-	-	Yes	vpc-0fe43107c3b1e00cc Work
-	rtb-0729672237fbab48d	-	-	Yes	vpc-0a825a07341195b28

rtb-0d14ddb9bef814666 / lab-rtb-private1-us-east-1a

Details | Routes | Subnet associations | Edge associations | Route propagation | Tags

Details

Route table ID: rtb-0d14ddb9bef814666	Main: No	Explicit subnet associations: subnet-0ad9811c2a67ea538 / lab-subnet-private1-us-east-1a	Edge associations: -
VPC:	Owner ID:		

Step 10: Choose the Subnet associations tab. In that Explicit subnet associations panel, choose Edit subnet associations.

Name	Route table ID	Explicit subnet assoc...	Main	VPC
lab-rtb-public	rtb-05457dae0a3b5361f	subnet-01096ecf68aae7f...	No	vpc-0c89aa4ac7bfe8ae0 lab
-	rtb-079861962ca1a3ba9	-	Yes	vpc-0c89aa4ac7bfe8ae0 lab
Work Public Route Table	rtb-0de0decba3f001437	subnet-0c2ec6f81d63b5...	No	vpc-0fe43107c3b1e00cc Wo
lab-rtb-private1-us-east-1a	rtb-0d14ddb9bef814666	subnet-0ad9811c2a67ea...	No	vpc-0c89aa4ac7bfe8ae0 lab
-	rtb-00ed5e08a95c7d543	-	Yes	vpc-0fe43107c3b1e00cc Wo
-	rtb-0729672237fbab48d	-	Yes	vpc-0a825a07341195b28

Explicit subnet associations (1)			
Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
lab-subnet-private1-us-east-1a	subnet-0ad9811c2a67ea538	10.0.1.0/24	-

Step 11: Leave lab-subnet-private1-us-east-1a selected, but also select lab-subnet-private2 and click save associations.

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
lab-subnet-public1-us-east-1a	subnet-01096ecf68aae7f5a	10.0.0.0/24	-	rtb-05457dae0a3b5361f / lab-rtb-public
lab-subnet-public2	subnet-013cc8efe49ca2c31	10.0.2.0/24	-	Main (rtb-079861962ca1a3ba9)
lab-subnet-private1-us-east-1a	subnet-0ad9811c2a67ea538	10.0.1.0/24	-	rtb-0d14ddb9bef814666 / lab-rtb-priv...
lab-subnet-private2	subnet-0540cfefddda700a01	10.0.3.0/24	-	Main (rtb-079861962ca1a3ba9)

Selected subnets	
subnet-0ad9811c2a67ea538 / lab-subnet-private1-us-east-1a	X
subnet-0540cfefddda700a01 / lab-subnet-private2	X

Step 12: Select the lab-rtb-public route table (and deselect any other subnets).

The screenshot shows the AWS VPC Management Console. In the left sidebar, under 'Virtual private cloud', 'Route tables' is selected. The main area displays a table of route tables. One row, 'lab-rtb-public', has a blue selection bar at the top and is highlighted with a blue border. The table columns include Name, Route table ID, Explicit subnet associations, Edge associations, Main, and VPC. The 'lab-rtb-public' row has 'subnet-01096ecf68aae7f5a / lab-subnet-public1-us-east-1a' listed under 'Explicit subnet associations'. Below the table, a detailed view of 'rtb-05457dae0a3b5361f / lab-rtb-public' is shown, with tabs for Details, Routes, Subnet associations, Edge associations, Route propagation, and Tags. The 'Subnet associations' tab is active, showing one entry: 'lab-subnet-public1-us-east-1a' associated with 'subnet-01096ecf68aae7f5a'. The right side of the screen shows standard AWS navigation and footer links.

Step 13: Choose the Subnet associations tab. In that Explicit subnet associations panel, choose Edit subnet associations.

This screenshot is from the same AWS VPC Management Console session as the previous one. The 'Subnet associations' tab is now active in the 'rtb-05457dae0a3b5361f / lab-rtb-public' details view. In the 'Explicit subnet associations' section, there is a single entry: 'lab-subnet-public1-us-east-1a' associated with 'subnet-01096ecf68aae7f5a'. To the right of this list is a blue-bordered rectangular box containing the text 'Edit subnet associations'. The rest of the interface is identical to the previous screenshot, including the sidebar and the bottom navigation bar.

Step 14: Leave lab-subnet-public1-us-east-1a selected, but also select lab-subnet-public2 and click save associations.

Available subnets (2/4)					
	Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
<input checked="" type="checkbox"/>	lab-subnet-public1-us-east-1a	subnet-01096ecf68aae7f5a	10.0.0.0/24	-	rtb-05457dae0a3b5361f / lab-rtb-public
<input checked="" type="checkbox"/>	lab-subnet-public2	subnet-013cc8efe49ca2c31	10.0.2.0/24	-	Main (rtb-079861962ca1a3ba9)
<input type="checkbox"/>	lab-subnet-private1-us-east-1a	subnet-0ad9811c2a67ea538	10.0.1.0/24	-	rtb-0d14ddb9bef814666 / lab-rtb-private
<input type="checkbox"/>	lab-subnet-private2	subnet-0540cfcdada700a01	10.0.3.0/24	-	rtb-0d14ddb9bef814666 / lab-rtb-private

Selected subnets

- [subnet-01096ecf68aae7f5a / lab-subnet-public1-us-east-1a](#)
- [subnet-013cc8efe49ca2c31 / lab-subnet-public2](#)

[Cancel](#) [Save associations](#)

Task 3: Create a VPC Security Group

Step 15: In the left navigation pane, choose Security groups and click choose “Create security group” and then configure: Security group name as “Web Security Group” and Description as “Enable HTTP access”. VPC: Remove all vpc and select lab-vpc.

Security Groups (4) Info					
	Name	Security group ID	Security group name	VPC ID	Description
<input type="checkbox"/>	-	sg-023fe8f4d9c15c39	default	vpc-0a825a07341195b28	default VPC sec
<input type="checkbox"/>	-	sg-0e522a22b01d8c69e	default	vpc-0c89aa4ac7bfe8ae0	default VPC sec
<input type="checkbox"/>	-	sg-04e796b5d414bee57	default	vpc-0fe43107c3b1e00cc	default VPC sec
<input type="checkbox"/>	-	sg-0f4b3d0cee12dad1c	Ec2SecurityGroup	vpc-0fe43107c3b1e00cc	VPC Security Gr

Actions [Create security group](#)

Security

- Network ACLs
- Security groups**
- DNS firewall
- Rule groups
- Domain lists

Network Firewall

[CloudShell](#) [Feedback](#) © 2024, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

The screenshot shows the 'Create security group' page in the AWS VPC console. In the 'Basic details' section, the security group name is 'Web Security Group' and the description is 'Enable HTTP access'. The VPC is set to 'vpc-0c89aa4ac7bfe8ae0 (lab-vpc)'. In the 'Inbound rules' section, there is one rule: Type: HTTP, Protocol: TCP, Port range: 80, Source: Anywhere (0.0.0.0/0), Description: Permit web requests. A note at the bottom of the page says: 'Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.'

Step 16: In the Inbound rules pane, choose Add rule. Configure the following settings as done below and click create security group.

The screenshot shows the 'Create security group' page with two additional inbound rules added. The first rule is for HTTP (TCP port 80) from 0.0.0.0/0 with the description 'Permit web requests'. The second rule is for HTTPS (TCP port 443) from 0.0.0.0/0 with the description 'Permit web requests'. The 'Add rule' button is visible at the bottom of the 'Inbound rules' section. A warning message at the bottom states: 'Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.'

The screenshot shows the 'CreateSecurityGroup | VPC Console' page. In the 'Outbound rules' section, there is a single rule: 'All traffic' to '0.0.0.0/0'. A warning message states: '⚠ Rules with destination of 0.0.0.0 or ::/0 allow your instances to send traffic to any IPv4 or IPv6 address. We recommend setting security group rules to be more restrictive and to only allow traffic to specific known IP addresses.' Below this, there is a 'Tags - optional' section with a note about tags being optional labels for AWS resources. The 'Create security group' button is highlighted in orange at the bottom right.

Task 4: Launch a Web Server Instance

Step 17: Search and choose EC2 to open the EC2 console.

The screenshot shows the 'EC2' search results page. The left sidebar includes sections for 'VPC dashboard', 'Virtual private cloud' (with links to 'Your VPCs', 'Subnets', 'Route tables', etc.), and 'Security'. The main content area displays 'Search results for "ec2"' under the 'Services' heading. The 'EC2' service card is highlighted with a blue border, showing it as 'Virtual Servers in the Cloud'. Other services listed include 'EC2 Image Builder', 'Recycle Bin', and 'Amazon Inspector'. Below this, under 'Features', there is a 'Dashboard' card. On the right side, there is a green sidebar with 'Actions' and 'Edit inbound rules' buttons, and a table showing a single row with 'VPC ID' and its value 'vpc-0c89aa4ac7bfe8ae0'.

Step 18: Click launch instance.

The screenshot shows the AWS EC2 Dashboard. On the left sidebar, under the 'Instances' section, there is a 'Launch instance' button. This button is highlighted with a yellow box, indicating it is the next step to be clicked. The main content area contains sections for 'Launch instance', 'Service health', and 'Additional information'.

Step 19: Name the instance and select the key pair name and select vockey.

The screenshot shows the 'Launch an instance' wizard. In the 'Name and tags' step, the 'Name' field is filled with 'Web Server 1'. The 'Summary' section on the right shows the number of instances set to 1. Below the summary, there are sections for 'Software Image (AMI)', 'Virtual server type (instance type)', 'Firewall (security group)', and 'Storage (volumes)'. A note about the free tier is displayed. At the bottom, there are 'Cancel', 'Launch instance', and 'Review commands' buttons.

The screenshot shows the AWS EC2 'Launch Instances' wizard. In the 'Instance type' section, a t2.micro instance is selected, described as 'Free tier eligible'. In the 'Key pair (login)' section, 'vokey' is chosen as the key pair name. The 'Network settings' section is partially visible on the left. On the right, the 'Summary' pane shows one instance being launched with the AMI 'Amazon Linux 2023 AMI 2023.5.2...', a 't2.micro' virtual server type, and a 'New security group'. A tooltip for the 'Free tier' indicates it includes 750 hours of t2.micro or t3.micro usage in specific regions. The 'Launch instance' button is prominently displayed at the bottom.

Step 20: Configure the network settings as done below:

This screenshot shows the 'Network settings' configuration step of the EC2 launch wizard. It includes fields for selecting a VPC (vpc-0c89aa4ac7bfe8ae0), a subnet (subnet-013cc8efef49ca2c51), and enabling auto-assign public IP. Under 'Firewall (security groups)', the 'Select existing security group' option is chosen, pointing to a 'Web Security Group'. The 'Common security groups' section lists the same 'Web Security Group'. The 'Summary' pane on the right remains largely the same as in the previous screenshot, showing one instance launch with the specified network configuration.

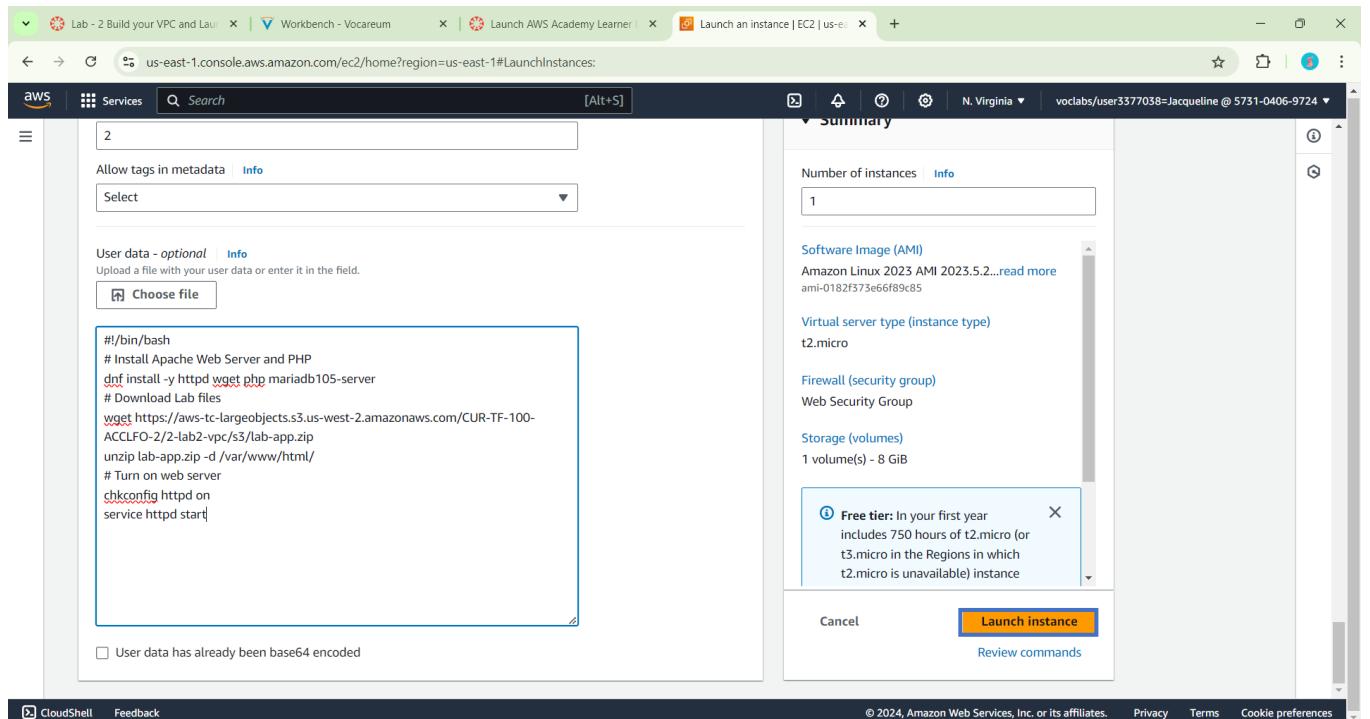
Step 21: Configure the instance, choose Select existing security group. For Common security groups, select Web Security Group.

The screenshot shows the AWS EC2 'Launch Instances' wizard at the 'Network settings' step. The 'Security group' dropdown is set to 'Web Security Group'. A callout box highlights the 'Select existing security group' button. The 'Free tier' information is visible on the right.

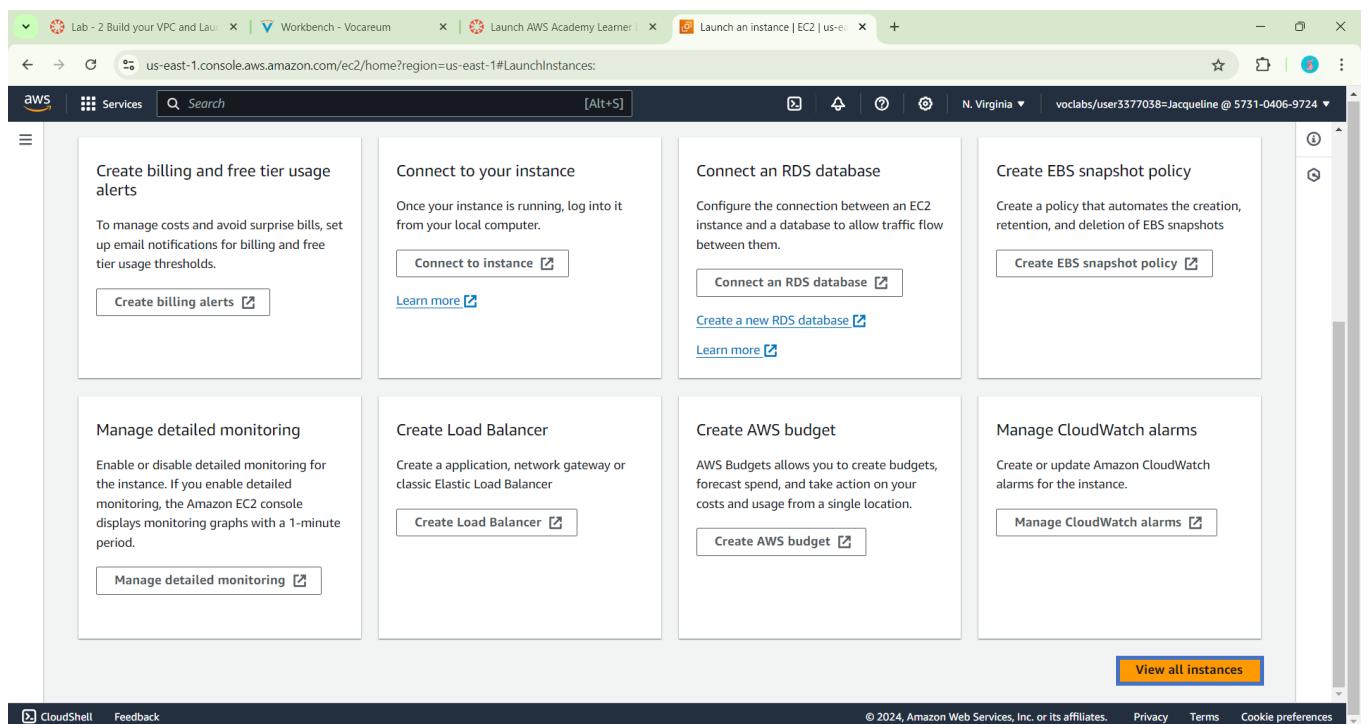
Step 22: Expand the Advanced details panel. Scroll to the bottom of the page and then paste the code as done below:

The screenshot shows the AWS EC2 'Launch Instances' wizard at the 'Advanced details' step. The 'User data' field contains a shell script for installing Apache, PHP, and MariaDB. A large blue box highlights this script. The 'Free tier' information is visible on the right.

Step 23: At the bottom of the Summary panel on the right side of the screen choose Launch instance.



Step 24: Click view all instances and select the created instance.

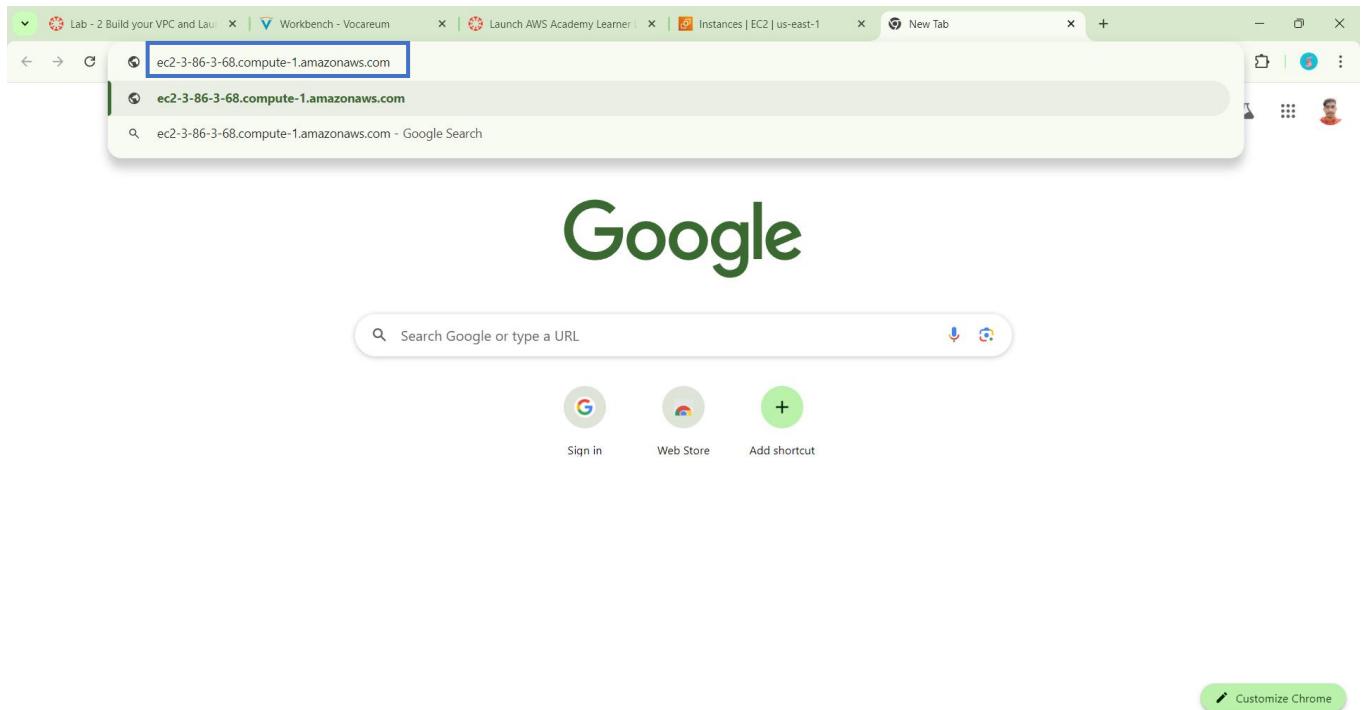


The screenshot shows the AWS EC2 Instances page. The left sidebar includes sections for EC2 Dashboard, EC2 Global View, Events, Console-to-Code Preview, Instances (with sub-options for Instances, Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations), Images (AMIs, AMI Catalog), and Elastic Block Store (Volumes, Snapshots). The main content area displays a table of instances. The table has columns for Name, Instance ID, Instance state, Instance type, Status check, Alarm status, Availability Zone, and Public IP. Two instances are listed: 'Bastion Host' (i-00aa7e9555ba07710) which is Running and t2.micro, and 'Web Server 1' (i-05836db5bea1e9d52) which is also Running and t2.micro. Below the table, a detailed view for 'Web Server 1' is shown under the heading 'i-05836db5bea1e9d52 (Web Server 1)'. The 'Details' tab is selected, showing the instance summary. Key details include: Instance ID (i-05836db5bea1e9d52), Public IPv4 address (3.86.3.68), Private IPv4 address (10.0.2.166), Instance state (Running), Public IPv4 DNS (ec2-3-86-3-68.compute-1.amazonaws.com), and Instance type (t2.micro). A note at the bottom right of the screenshot indicates '© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences'.

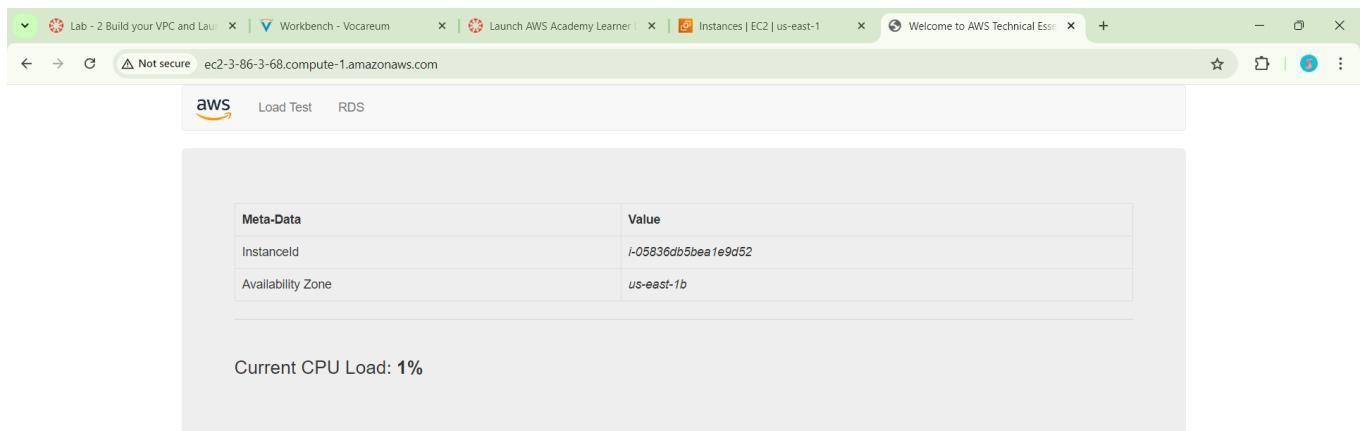
Step 25: Copy the Public IPv4 DNS value shown in the Details tab at the bottom of the page.

This screenshot is identical to the one above, showing the AWS EC2 Instances page with the same interface and data. The 'Details' tab for 'Web Server 1' is still selected, displaying the instance summary. The Public IPv4 DNS field contains the value 'ec2-3-86-3-68.compute-1.amazonaws.com'. A tooltip or status message 'Public IPv4 DNS copied' appears over the 'open address' link, indicating that the value has been copied to the clipboard. The copyright notice at the bottom right is also present.

Step 26: Open a new web browser tab, paste the Public DNS value and press Enter.



Step 27: View the web page displaying the AWS logo and instance meta-data values.



Step 28: Stop and terminate all the instances.

The screenshot shows the AWS EC2 Instances page. A modal window titled "Terminate (delete) instance?" is open. It contains a warning message: "On an EBS-backed instance, the default action is for the root EBS volume to be deleted when the instance is terminated. Storage on any local drives will be lost." Below this, a question "Are you sure you want to terminate these instances?" is asked. The modal displays the instance ID "i-05836db5bea1e9d52 (Web Server 1)" and indicates that "Termination protection" is "Disabled". At the bottom right of the modal are "Cancel" and "Terminate (delete)" buttons. The main EC2 dashboard shows a list of instances, including "Bastion Host" and "Web Server 1". The "Instances" section of the sidebar is expanded, showing options like Instance Types, Launch Templates, and Spot Requests.

Step 29: Sign out and end the lab.

The screenshot shows the AWS EC2 Dashboard. On the right side, a vertical navigation menu is open, showing account information (Account ID: 5731-0406-9724, Federated user: voclabs/user3377038=Jacqueline), links for GuardDuty, Account, Organization, Service Quotas, and Billing and Cost Management, and a "Switch role" and "Sign out" button. The main content area shows the EC2 Dashboard with sections for Migrate a server, Status (operating normally), Zones (listing availability zones: us-east-1a, us-east-1b, us-east-1c, us-east-1d, us-east-1e, us-east-1f), Instance alarms (0 in alarm, 0 OK, 0 insufficient data), Scheduled events (No scheduled events), and Migrate a server. The left sidebar is expanded, showing the "Instances" section with options like Instances, Instance Types, and Launch Templates.

The screenshot shows a web browser window with the URL awsacademy.instructure.com/courses/86436/modules/items/7859818. The page title is "Launch AWS Academy Learner Lab". On the left, there is a sidebar with navigation links: Account, Dashboard, Courses, Calendar, Inbox, History, and Help. The main content area displays a confirmation dialog box with the message "Are you sure you want to end the lab?". Below the dialog, there are "Yes" and "No" buttons. At the top of the main content area, there are buttons for "Start Lab", "End Lab", "AWS Details", "Readme", and "Reset". To the right of the main content area, there is a sidebar titled "Learner Lab" containing links to various resources: Environment Overview, Environment Navigation, Access the AWS Management Console, Region restriction, Service usage and other restrictions, Using the terminal in the browser, Running AWS CLI commands, Using the AWS SDK for Python, Preserving your budget, Accessing EC2 instances, SSH Access to EC2 instances, SSH Access from Windows, and SSH Access from a Mac.