



AWS Academy Cloud Foundations: Configuring Identity and Access Management, Virtual Private Cloud, and Elastic Compute Cloud

Colin J. Faletto, CCNA

Purpose

This write-up is intended to document and explain the first three labs in the AWS Academy Cloud Foundations course. These labs are intended to provide an introduction to very basic AWS concepts, such as basic security, cloud networking, and virtual machines. These concepts are essential for new cloud engineers to provide parallels to the core skills of traditional IT. These labs also provide a strong foundation of knowledge for the AWS management console, as they all take place primarily inside this console.

Background

Amazon is a company based in Seattle that runs the biggest e-commerce platform in the world. They were started in 1994 by former CEO Jeff Bezos and have grown from a small online bookstore to a giant online store offering a wide variety of products. Amazon also has a strong physical retail presence in the grocery space with their Amazon Fresh and Whole Foods chains, and has a strong online media presence through Twitch, Prime Video, and Amazon Music, which provide entertainment in the form of livestreams, movies and television shows, and music respectively. Amazon also has a popular line of e-readers and tablets with their Kindle brand and has a successful brand of artificial intelligence assistants with their Amazon Alexa A.I. and their Amazon Echo line of smart speakers.

Amazon Web Services, or AWS, is Amazon's cloud computing division. It was created in 2002 to provide simple web services to customers and expanded to cloud storage and computing in 2006. It is the leading cloud service provider and is popular for its pay-as-you-go service model. AWS provides services to everyone from small businesses to massive companies like Coca-Cola and Apple, and even provides web infrastructure to government branches. AWS takes the responsibility and cost of managing a data center out of the hands of businesses and maintains a massive global network of Amazon data centers that split customer traffic among them. AWS currently has 34 geographic regions, each of which have multiple availability zones which themselves contain multiple data centers. These data centers are in undisclosed locations for security reasons, though their general position is published. AWS offers services for virtual machines, cloud storage, database management, machine learning, IoT services, cloud networking, and much more.

Amazon Elastic Compute Cloud, or EC2, is an AWS service that allows customers to create virtual machines in the AWS cloud. These machines are very versatile, as they can be allocated as many or as few resources (CPU, RAM, GPU) as needed and can run nearly any operating system. By default, EC2 instances will run Amazon Linux, which is a version of Linux optimized for AWS servers. Amazon's e-commerce platform, its primary source of revenue, has been running on EC2 instances for over a decade. EC2 instances have a variety of different types, which are optimized for different purposes such as memory (R series, X series), compute (C series), and storage (H series, I series, D series).

Amazon Virtual Private Cloud, or VPC, is an AWS service that provides a virtual network inside the AWS cloud. This service allows AWS objects, such as EC2 instances, to communicate with each other. In a VPC, each EC2 machine is assigned a

unique private IPv4 address, which is then connected via NAT to a public address on an internet gateway. Using this gateway, machines in the VPC can communicate with other AWS VPCs and other Internet-connected machines. Amazon VPC is provided at no additional charge to customers using EC2 instances.

Amazon Identity and Access Management, or IAM, is an AWS service that provides a layer of security to customers by limiting the resources different users can access. IAM follows the principle of least privilege, meaning that by default, all AWS controls are blocked for users unless they have been explicitly granted permissions. IAM represents a portion of the customer responsibilities in the AWS shared responsibility model, which is a model outlining that AWS is responsible for the physical security of data centers and networks while the customer is responsible for keeping their customer data and configurations safe. One of IAM's unique features is its role feature, which creates identities with elevated permissions that can be temporarily assigned to users. This feature works similarly to the "sudo" command in unix-based operating systems.

Lab Summary

This write-up covers three different AWS labs. The first lab covers AWS IAM. The lab entails assigning permissions to three different users to allow them to interact with S3 and EC2 services. Two of these users are support users, who are assigned read-only permissions to EC2 and S3 respectively. The other user is an administrator with start and stop access to EC2 instances. The second lab covers AWS VPC, and entails creating a VPC with four different subnets, two public and two private, spread across two different availability zones. The lab also involves creating a security group to allow HTTP access to machines in the second public subnet. The third lab involves creating a web server EC2 instance, allowing HTTP access through a security group, then resizing the instance and testing the stop protection feature.

Lab Commands (Lab 1 IAM)

Log into the AWS management console.

The screenshot shows the AWS Console Home dashboard. On the left, there's a sidebar with 'Recently visited' services (EC2, S3, RDS, Lambda), 'Welcome to AWS' (Getting started with AWS, Training and certification), and 'AWS Health' (Open issues: 0, Scheduled changes: 0, Other notifications: 0). The main area has sections for 'Applications (0)', 'Cost and usage' (Current month costs: \$0.00, Forecasted month end costs: \$0.00, Savings opportunities: Enable Cost Optimization Hub), and a 'View all services' link.

In the search bar, search for "IAM" and open the first result.

The screenshot shows the IAM service page. A red arrow points to the 'IAM' icon in the 'Services' section of the navigation bar. Below it, the text 'Manage access to AWS resources' is visible.

In the IAM dashboard, open the "User Groups" tab from the sidebar.

▼ Access management

User groups

Users

Roles

Open the "S3-Support" group.

<input type="checkbox"/> Group name	▲ Users	▼ Permissions	▼ Creation time
<input type="checkbox"/> EC2-Admin	⚠ 0	✓ Defined	7 minutes ago
<input type="checkbox"/> EC2-Support	⚠ 0	✓ Defined	7 minutes ago
<input type="checkbox"/> S3-Support	⚠ 0	✓ Defined	7 minutes ago

Click "Add Users".

S3-Support [Info](#)

[Delete](#) [Edit](#)

Summary

User group name	S3-Support	Creation time	December 13, 2024, 12:09 (UTC-08:00)	ARN	arn:aws:iam::858935888409:group/spl66/S3-Support
-----------------	------------	---------------	--------------------------------------	-----	--

[Users](#) [Permissions](#) [Access Advisor](#)

Users in this group (0)

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

[Search](#)

[User name](#)

No resources to display

[Add users](#)

Check the box next to “user-1”.

[user-1](#)

0 None 13 minutes ago

Click “Add Users”.

[Add users](#)

Return to the “User Groups” section and select “EC2-Support”.

<input type="checkbox"/>	Group name	▲ Users	▼ Permissions	▼ Creation time
<input type="checkbox"/>	EC2-Admin	⚠ 0	✓ Defined	7 minutes ago
<input type="checkbox"/>	EC2-Support	⚠ 0	✓ Defined	7 minutes ago
<input type="checkbox"/>	S3-Support	⚠ 0	✓ Defined	7 minutes ago

Click “Add Users”.

EC2-Support [Info](#)

[Delete](#) [Edit](#)

Summary

User group name	EC2-Support	Creation time	December 13, 2024, 12:09 (UTC-08:00)	ARN	arn:aws:iam::858935888409:group/spl66/EC2-Support
-----------------	-------------	---------------	--------------------------------------	-----	---

[Users](#) [Permissions](#) [Access Advisor](#)

Users in this group (0)

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

[Search](#)

[User name](#)

No resources to display

[Add users](#)

Select “user-2” and click “Add Users”.

The screenshot shows the 'User Groups' section of the AWS IAM console. It lists two groups: 'EC2-Admin' and 'EC2-Support'. Both groups have 0 users and were created 15 minutes ago. At the bottom right, there is a blue 'Edit' button and an orange 'Add users' button, with a red arrow pointing to the 'Add users' button.

Return to the “User Groups” section and click on “EC2-Admin”.

The screenshot shows the 'EC2-Admin' user group details page. It displays the group name 'EC2-Admin', creation time (December 13, 2024, 12:09 (UTC-08:00)), ARN, and a summary table with columns for Group name, Users, Permissions, and Creation time. The 'EC2-Admin' row is highlighted with a red arrow. At the bottom right, there is a blue 'Delete' button and an orange 'Edit' button.

Group name	Users	Permissions	Creation time
EC2-Admin	0	Defined	7 minutes ago
EC2-Support	0	Defined	7 minutes ago
S3-Support	0	Defined	7 minutes ago

Click “Add Users”.

The screenshot shows the 'Users' tab for the 'EC2-Admin' group. It displays a table with 0 users. At the bottom right, there is a blue 'Edit' button and an orange 'Add users' button, with a red arrow pointing to the 'Add users' button.

Click the checkbox next to “user-3” and click “Add Users”.

The screenshot shows the 'Users' tab for the 'EC2-Admin' group after adding user-3. It displays a table with 1 user. At the bottom right, there is a blue 'Edit' button and an orange 'Add users' button, with a red arrow pointing to the 'Add users' button.

If done correctly, each user group should have a “1” next to it.

The screenshot shows the 'User groups' page. It lists three groups: 'EC2-Admin', 'EC2-Support', and 'S3-Support'. Each group has 1 user assigned. At the bottom right, there is a blue 'Edit' button, an orange 'Create group' button, and a search bar.

Return to the dashboard.

Identity and Access Management (IAM)

Search IAM

Dashboard



On the dashboard page, find and copy the sign-in URL for IAM users. This URL will be used to test the permissions that have just been set up.

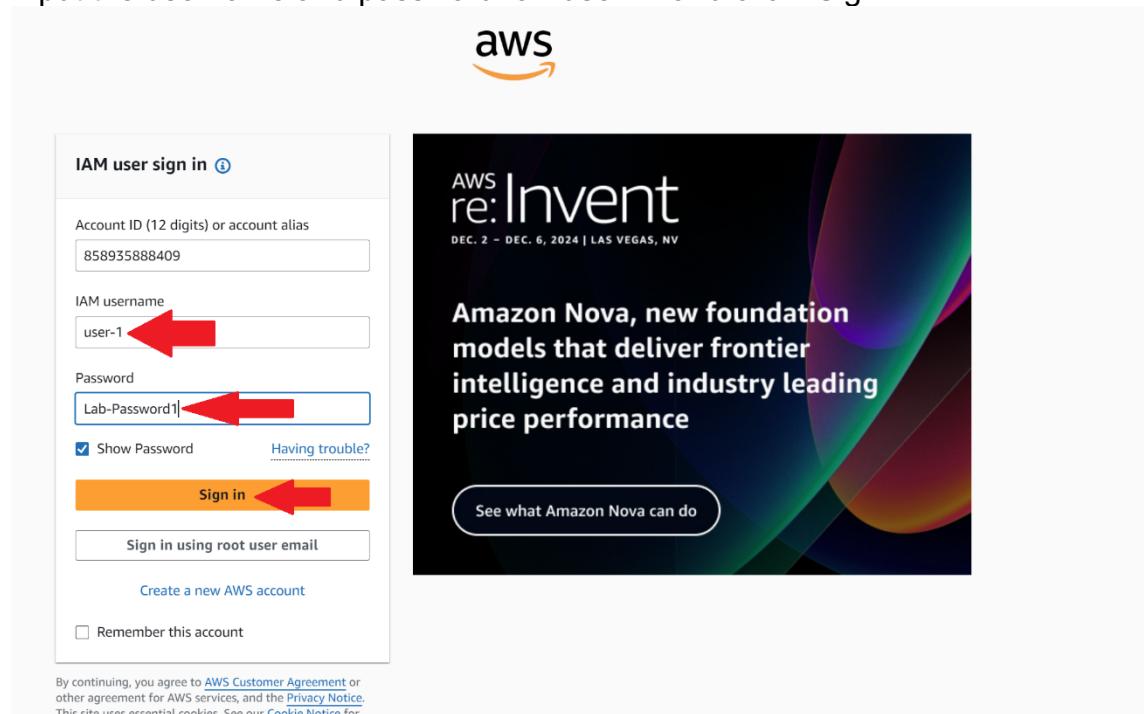
Sign-in URL for IAM users in this account

https://858935888409.signin.aws.amazon.com/console

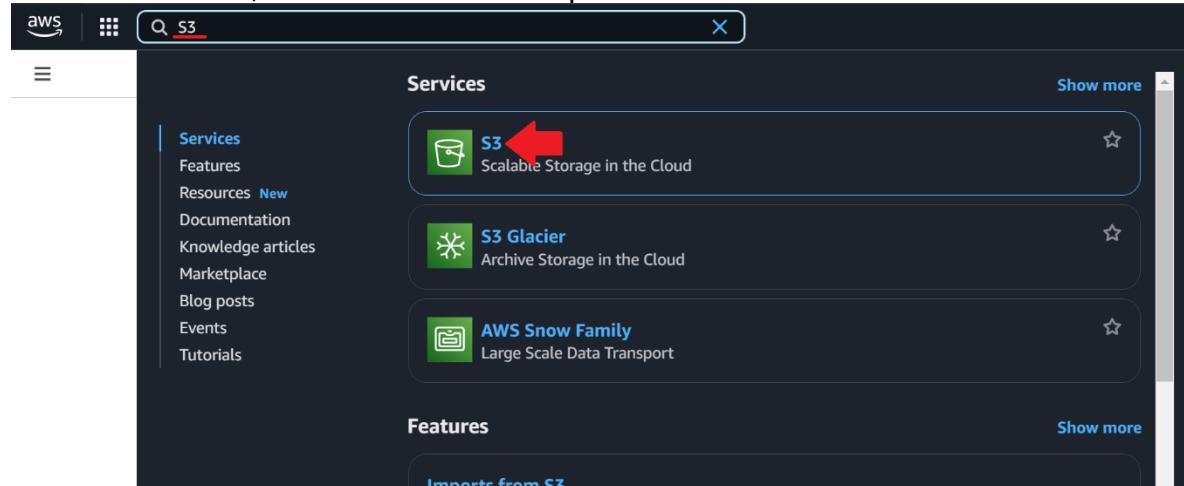
Open a new private browser window and input the URL.



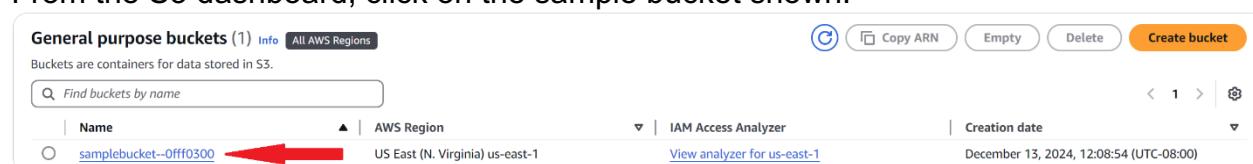
Input the username and password for “user-1” and click “Sign In”.



In the search bar, search for “S3” and open the S3 dashboard.



From the S3 dashboard, click on the sample bucket shown.



If permissions have been set correctly, user-1 should be able to see the objects in the bucket. In this case, there are no objects in the bucket, which should be evident in a message displayed to the user.

samplebucket--0fff0300 [Info](#)

[Objects](#) [Metadata - Preview](#) [Properties](#) [Permissions](#) [Metrics](#) [Management](#) [Access Points](#)

Objects (0) [Info](#)

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions.

[Learn more](#)

[Copy S3 URI](#) [Copy URL](#) [Download](#) [Open](#) [Delete](#) [Actions](#) [Create folder](#) [Upload](#)

No objects

You don't have any objects in this bucket.

[Upload](#)

In the search bar, search for “EC2” and open the EC2 dashboard.

aws | [Amazon](#) [X](#)

Services

[Amazon S3](#) [Services](#) [Features](#) [Resources New](#) [Documentation](#)

[General purpose](#) [Directory buckets](#) [Table buckets](#)

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access

EC2 Virtual Servers in the Cloud

[EC2 Image Builder](#)

Show more

Resources

You are using the following Amazon EC2 resources in the US East (N. Virginia) Region:

Instances (running)	0	Auto Scaling Groups	API Error	Capacity Reservations	API Error
Dedicated Hosts	API Error	Elastic IPs	API Error	Instances	API Error
Key pairs	API Error	Load balancers	API Error	Placement groups	API Error
Security groups	API Error	Snapshots	API Error	Volumes	API Error

[EC2 Global View](#)

Launch instance

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

[Launch instance](#) [Migrate a server](#)

Note: Your instances will launch in the US East (N. Virginia) Region

Service health

[An error occurred](#)
An error occurred retrieving service health information

[Diagnose with Amazon Q](#)

[AWS Health Dashboard](#)

If permissions are set up correctly, the following error will occur:

Instances [Info](#)

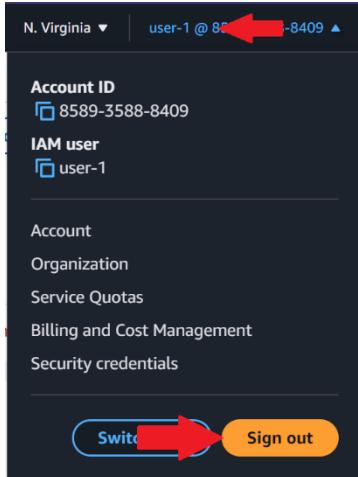
[All states](#)

[Instances state = running](#)

[Name](#) [Instance ID](#) [Instance state](#) [Instance type](#) [Status check](#) [Alarm status](#) [Availability Zone](#) [Public IPv4 DNS](#) [Public IPv4 ...](#) [Elastic IP](#) [IPv6 IPs](#) [Monitoring](#)

You are not authorized to perform this operation. User: arn:aws:iam:858935888409:user:spl66/user-1 is not authorized to perform: ec2:DescribeInstances because no identity-based policy allows the ec2:DescribeInstances action

This is intended behavior, as user-1 is only authorized to access S3 services. Click the “user-1” button in the top right corner and click “Sign Out”.



In the resulting window, click "Sign In".

The AWS Management Console sign-in page. At the top, there are links for "Overview", "Features", "Mobile Application", and "FAQs". Below that, a breadcrumb trail shows "Products > Management and Governance > Management Console". The main heading is "AWS Management Console" with the subtext "Everything you need to access and manage the AWS Cloud — in one web interface". A large "Sign in" button is at the bottom left, with a large red arrow pointing to it.

Enter the username and password for user-2 and click "Sign In". Your AWS account ID should be automatically filled, but if it isn't, you can paste the same sign-in URL from before.

The IAM user sign-in form. It includes fields for "Account ID (12 digits) or account alias" (858935888409), "IAM username" (user2), and "Password" (Lab-Password2). A red arrow points to the "user2" field. Another red arrow points to the "Lab-Password2" field. A third red arrow points to the orange "Sign in" button. Other visible buttons include "Show Password" and "Having trouble?". Links for "Create a new AWS account" and "Sign in using root user email" are also present.

Return to the EC2 dashboard.

Click on “Instances (running)”. You’ll notice a distinct lack of “API Error” messages, unlike the page for user-1.

Resources	Value
Instances (running)	2
Auto Scaling Groups	0
Capacity Reservations	0
Dedicated Hosts	0
Elastic IPs	0
Instances	2
Key pairs	1
Load balancers	0
Placement groups	0
Security groups	3
Snapshots	0
Volumes	2

You’ll notice that the instances will properly display this time. Select the “LabHost” instance.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP	IPv6 IPs	Monitoring
<input checked="" type="checkbox"/> LabHost	i-02157c36a0a841d1c	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1a	ec2-44-195-46-204.co...	44.195.46.204	-	-	disabled
<input type="checkbox"/> Bastion Host	i-0caf67c66b8993fc	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1a	ec2-34-234-208-187.co...	34.234.208.187	-	-	disabled

Click on “Instance state” > “Stop Instance”.

Actions

- Stop instance
- Start instance

Click “Stop”.

Stop instance

Stopping your instance allows you to reduce costs, modify settings, and troubleshoot problems.

Instance ID	Stop protection
i-02157c36a0a841d1c (LabHost)	<input checked="" type="checkbox"/> Off (Can stop instance)

⚠️ You will be billed for associated resources
After you stop the instance, you are no longer charged usage or data transfer fees for it. However, you will still be billed for associated Elastic IP addresses and EBS volumes.

Associated resources
You will continue to incur charges for these resources while the instance is stopped

Stop

Since user-2 doesn’t have the appropriate permissions, you should get the following error message:



To confirm that user-2 doesn't have access to S3, access the S3 dashboard from the search bar.

The screenshot shows the AWS Services dashboard. The S3 icon is highlighted with a red arrow. Other services listed include S3 Glacier and AWS Snow Family.

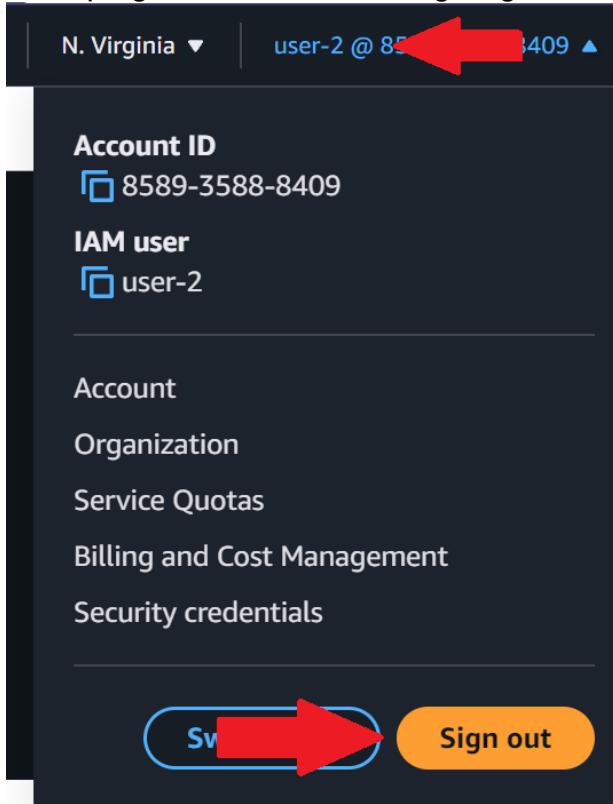
You should see the following page, where it appears that no S3 buckets have been set up (user-2 is unable to see these buckets, so AWS treats them as if they don't exist here).

The screenshot shows the Amazon S3 landing page. It features a large 'Create a bucket' button and a 'How it works' video player.

Attempting to create a bucket as user-2 will result in the following error message:

The screenshot shows an error message indicating that user-2 lacks the s3:CreateBucket permission. It also links to the IAM console for viewing permissions and provides an API response link.

Now, switch to user-3. Sign out of the user-2 account by clicking the “user-2” button in the top right corner and clicking “Sign Out”.



Enter the username and password for user-3 and click “Sign In”.

The screenshot shows the AWS IAM sign-in page. It has fields for 'Account ID (12 digits) or account alias' (858935888409), 'IAM username' (user-3), and 'Password' (Lab-Password3). There are checkboxes for 'Show Password' and 'Remember this account'. A red arrow points to the 'Sign in' button. To the right, there is a promotional banner for 're:Invent' with the text 'Explore how to prepare, respond, and recover from security events with AWS Security Incident Response' and a 'Sign in using root user email' link.

Return to the EC2 dashboard.

Return to the “Instances (running)” tab.

Resources

You are using the following Amazon EC2 resources in the US East (N. Virginia) Region:

Instances (running)	2	Auto Scaling Groups	0 API Error	Capacity Reservations	0
Dedicated Hosts	0	Elastic IPs	0	Instances	2
Key pairs	1	Load balancers	0 API Error	Placement groups	0
Security groups	3	Snapshots	0	Volumes	2

Select “LabHost” again, and try to stop the instance again.

Instances (1/2) Info

Last updated less than a minute ago

Find Instance by attribute or tag (case-sensitive)

Instance state = running

Clear filters

Instance state ▾ Actions ▾

LabHost

Bastion Host

Stop instance

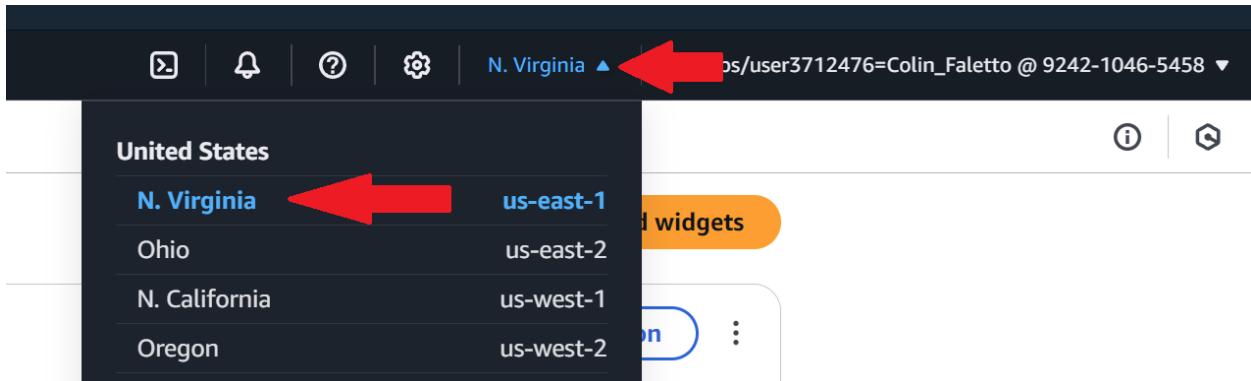
Start instance

If user-3's permissions are correctly set up, you should see the following success message:

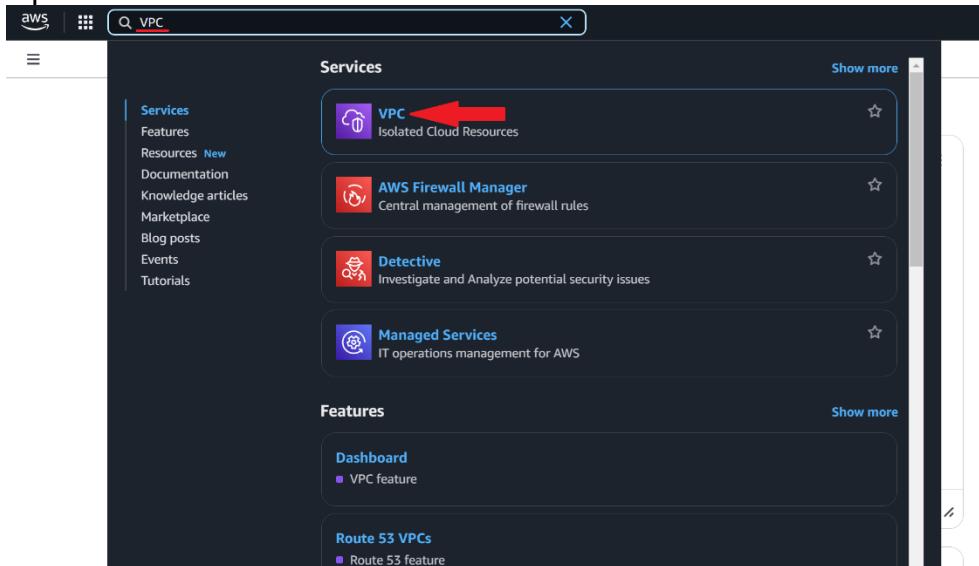
Successfully initiated stopping of i-02157c36a0a841d1c

Lab Commands (Lab 2 VPC)

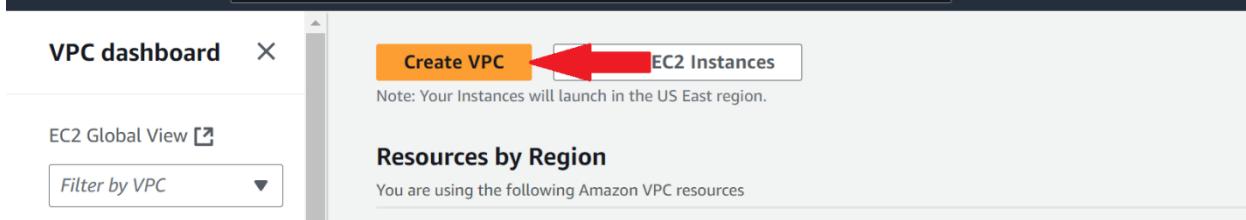
In the AWS management console, ensure that you have the “N. Virginia (us-east-1)” region selected.



Open the VPC dashboard from the search bar.



Click "Create VPC".



Keep all settings on their default values (ensure they match with the screenshot below) besides the following:

- Set "Resources to create" to "VPC and more"
- Set "Name tag auto-generation" to "lab"
- Set "Number of Availability Zones (AZs)" to "1"

VPC settings

Resources to create [Info](#)

Create only the VPC resource or the VPC and other networking resources.

VPC only

VPC and more

Name tag auto-generation [Info](#)

Enter a value for the Name tag. This value will be used to auto-generate Name tags for all resources in the VPC.

Auto-generate

lab

IPv4 CIDR block [Info](#)

Determine the starting IP and the size of your VPC using CIDR notation.

10.0.0.0/16

65,536 IPs

CIDR block size must be between /16 and /28.

IPv6 CIDR block [Info](#)

No IPv6 CIDR block

Amazon-provided IPv6 CIDR block

Tenancy [Info](#)

Default

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

[► Customize AZs](#)

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

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

Open the “Customize subnets CIDR blocks” section and ensure that the public and private subnet CIDR blocks are set to 10.0.0.0/24 and 10.0.1.0/24 respectively.

[▼ Customize subnets CIDR blocks](#)



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

Set “NAT gateways” to “In 1 AZ”, set “VPC Endpoints” to “None”, and ensure that both boxes under “DNS options” are checked. Verify that the Subnets, Route Tables, and Network connections in the “Preview” section match the screenshot below, then click “Create VPC”.

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

Cancel **Preview code** **Create VPC**

Click after verifying information in "Preview"

Preview

VPC [Show details](#)
Your AWS virtual network
lab-vpc

Subnets (2)
Subnets within this VPC
us-east-1a
A lab-subnet-public1-us-east-1a
A lab-subnet-private1-us-east-1a

Route tables (2)
Route network traffic to resources
lab-rtb-public
lab-rtb-private1-us-east-1a

Network connections (2)
Connections to other networks
lab-igw
lab-nat-public1-us-east-1a

You should see a window like this while the VPC is being created:

Create VPC workflow

>Create subnet

22%

▼ Details

- ✓ Create VPC: vpc-0b119727c01eb831d []
- ✓ Enable DNS hostnames
- ✓ Enable DNS resolution
- ✓ Verifying VPC creation: vpc-0b119727c01eb831d []
- ... Create subnet
- ⌚ Create subnet
- ⌚ Create internet gateway
- ⌚ Attach internet gateway to the VPC
- ⌚ Create route table
- ⌚ Create route
- ⌚ Associate route table
- ⌚ Allocate elastic IP
- ⌚ Create NAT gateway
- ⌚ Wait for NAT Gateways to activate
- ⌚ Create route table
- ⌚ Create route
- ⌚ Associate route table
- ⌚ Verifying route table creation

You should see a screen like this when the VPC has finished being created:

VPC > Your VPCs > vpc-0b119727c01eb831d / lab-vpc

Actions ▾

Details	Info
VPC ID vpc-0b119727c01eb831d	State Available
DNS resolution Enabled	Tenancy default
Main network ACL acl-0766d6c0ef345680e	Default VPC No
IPv6 CIDR (Network border group) -	Network Address Usage metrics Disabled
	Block Public Access Off
	DHCP option set dopt-0803267abe9d2ea4e
	IPv4 CIDR 10.0.0.0/16
	Route 53 Resolver DNS Firewall rule groups -
	DNS hostnames Enabled
	Main route table rtb-073694f2c5b876a0f
	IPv6 pool -
	Owner ID 924210465458

Resource map Info

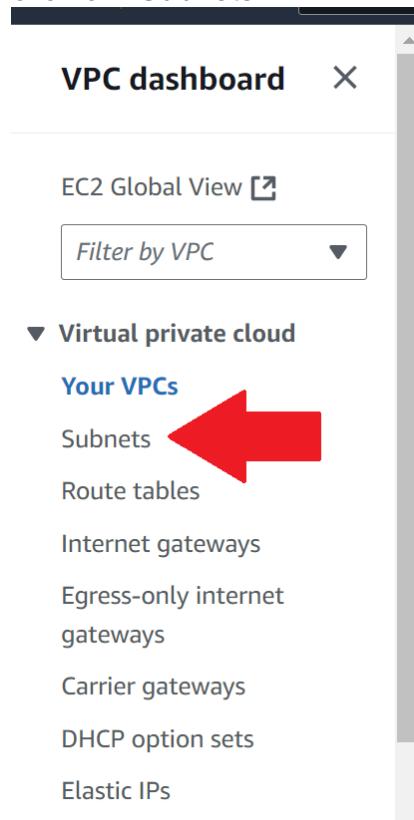
VPC Show details Your AWS virtual network lab-vpc

Subnets (2) Subnets within this VPC us-east-1a lab-subnet-public1-us-east-1a lab-subnet-private1-us-east-1a

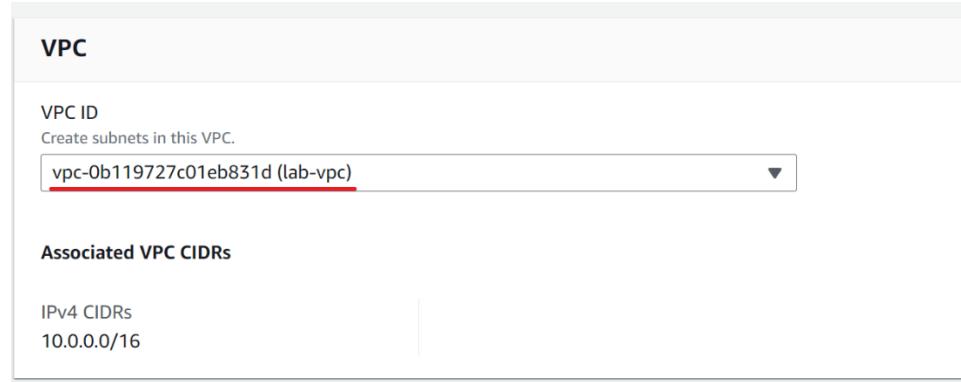
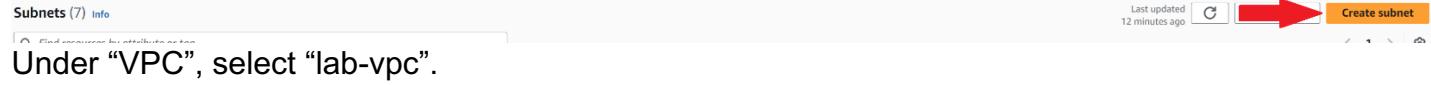
Route tables (3) Route network traffic to resources rtb-073694f2c5b876a0f lab-rtb-private1-us-east-1a lab-rtb-public

Network connections (2) Connections to other networks lab-igw lab-nat-public1-us-east-1a

You will now create additional subnets in a second availability zone. From the sidebar, click on “Subnets”.



Click “Create Subnet”.



Under “Subnet settings”, set the name to “lab-subnet-public2”, the availability zone to “us-east-1b”, and the IPv4 subnet CIDR block to 10.0.2.0/24. Click “Create Subnet”.

Subnet settings
Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.
lab-subnet-public2
The 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-1b

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
<input type="text" value="Name"/> X	<input type="text" value="lab-subnet-public2"/> X
Add new tag	

You can add 49 more tags.
[Remove](#)

[Add new subnet](#)

 **Create subnet**

From the subnet dashboard again, select “Create Subnet” and set the VPC to “lab-vpc” again.

Subnets (7) [Info](#)

Last updated  12 minutes ago  **Create subnet**

VPC

VPC ID
Create subnets in this VPC.
vpc-0b119727c01eb831d (lab-vpc)

Associated VPC CIDRs

IPv4 CIDRs
10.0.0.0/16

Under “Subnet settings” this time, set the name to “lab-subnet-private2”, the Availability Zone to “us-east-1b”, and the IPv4 Subnet CIDR block to 10.0.3.0/24. Click “Create Subnet”.

Subnet settings
Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.

The 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.

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.

IPv4 subnet CIDR block
 256 IPs

Tags - optional

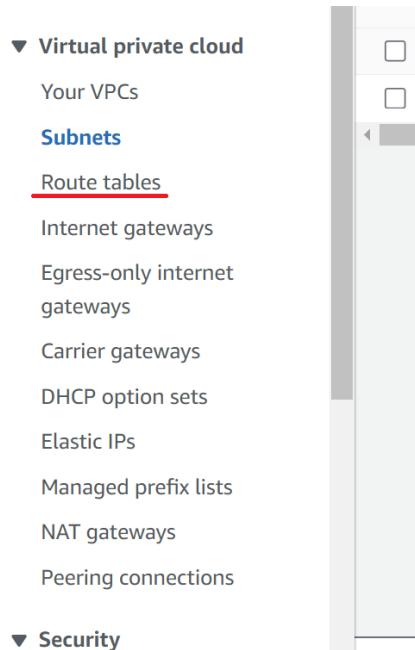
Key	Value - optional
<input type="text" value="Name"/>	<input type="text" value="lab-subnet-private2"/>

Add new tag
You can add 49 more tags.
Remove

Add new subnet

 **Create subnet**

Next, set the second private subnet to share a routing table with the first private subnet. Go to the “Route tables” section from the sidebar.



Click on the “Route table ID” hyperlink associated with “lab-rtp-private1-us-east-1a”.

Route tables (6) [Info](#)

Last updated less than a minute ago [Actions](#) [Create route table](#)

Find resources by attribute or tag

Name	Route table ID	Explicit subnet associations	Edge associations	Main	VPC	Owner ID
-	rtb-073694f2c5b876a0f	-	-	Yes	vpc-0b119727c01eb831d lab...	924210465458
-	rtb-0a1558d65466896a5	-	-	Yes	vpc-09ec9f5893e09458 Wor...	924210465458
lab-rtb-private1-us-east-1a	rtb-0ac581ded2cd7ba2d	subnet-09f084179558fc...	-	No	vpc-0b119727c01eb831d lab...	924210465458
-	rtb-04a73cd2ad287f1c1	-	-	Yes	vpc-072bfefaa0f069148	924210465458
Work Public Route Table	rtb-0be92c5b756f2604	subnet-08cc5bc299a44...	-	No	vpc-09ec9f5893e09458 Wor...	924210465458
lab-rtb-public	rtb-0fa868d8374751624	subnet-04eeff38a38c12...	-	No	vpc-0b119727c01eb831d lab...	924210465458

Click “Subnet associations”.

[rtb-0ac581ded2cd7ba2d / lab-rtb-private1-us-east-1a](#)

[Details](#) [Routes](#) [Subnet associations](#) [Route propagation](#) [Tags](#)

Details

Route table ID rtb-0ac581ded2cd7ba2d VPC vpc-0b119727c01eb831d lab-vpc	Main No Owner ID 924210465458	Explicit subnet associations subnet-09f084179558fc24 / lab-subnet-private1-us-east-1a	Edge associations
---	--	--	-------------------

Click “Edit subnet associations”.

[Explicit subnet associations \(1\)](#)

[Edit subnet associations](#)

Name lab-subnet-private1-us-east-1a	Subnet ID subnet-09f084179558fc24	IPv4 CIDR 10.0.1.0/24	IPv6 CIDR -
--	--	--------------------------	----------------

Select both private subnets, then click “Save associations”.

[Available subnets \(2/4\)](#)

[Selected subnets](#)

[Save associations](#)

Available subnets (2/4)	Selected subnets
<input checked="" type="checkbox"/> Name lab-subnet-public2	subnet-09f084179558fc24 / lab-subnet-private1-us-east-1a
<input checked="" type="checkbox"/> Name lab-subnet-private1-us-east-1a	subnet-09f084179558fc24
<input type="checkbox"/> Name lab-subnet-public1-us-east-1a	subnet-04eeff38a38c1227901
<input checked="" type="checkbox"/> Name lab-subnet-private2	subnet-03c1c5e984e277901

Return to the “Route tables” page. Click on the “Route table ID” hyperlink of the “lab-rtp-public” table.

Route tables (6) [Info](#)

Last updated less than a minute ago [Actions](#) [Create route table](#)

Find resources by attribute or tag

Name	Route table ID	Explicit subnet associations	Edge associations	Main	VPC	Owner ID
-	rtb-073694f2c5b876a0f	-	-	Yes	vpc-0b119727c01eb831d lab...	924210465458
-	rtb-0a1558d65466896a5	-	-	Yes	vpc-09ec9f5893e09458 Wor...	924210465458
lab-rtb-private1-us-east-1a	rtb-0ac581ded2cd7ba2d	subnet-09f084179558fc...	-	No	vpc-0b119727c01eb831d lab...	924210465458
-	rtb-04a73cd2ad287f1c1	-	-	Yes	vpc-072bfefaa0f069148	924210465458
Work Public Route Table	rtb-0be92c5b756f2604	subnet-08cc5bc299a44...	-	No	vpc-09ec9f5893e09458 Wor...	924210465458
lab-rtb-public	rtb-0fa868d8374751624	subnet-04eeff38a38c12...	-	No	vpc-0b119727c01eb831d lab...	924210465458

Click “Subnet associations”.

rtb-0fa868d8374751624 / lab-rtb-public

Details Routes Subnet associations **Associations** Route propagation Tags

Details

Route table ID rtb-0fa868d8374751624	Main No	Explicit subnet associations subnet-04eef38a38c122297 / lab-subnet-public1-us-east-1a	Edge -
VPC vpc-0b119727c01eb851d lab-vpc	Owner ID 924210465458		

Click “Edit subnet associations”.

Explicit subnet associations (1)

Edit subnet associations

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
lab-subnet-public1-us-east-1a	subnet-04eef38a38c122297	10.0.0.0/24	-

Select both public subnets, then click “Save associations”.

Available subnets (2/4)

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
lab-subnet-public2	subnet-0b7125fb16f8716ba	10.0.2.0/24	-	Main (rtb-073694f2c5b476a0f)
lab-subnet-private1-us-east-1a	subnet-09f0841795588f24	10.0.1.0/24	-	rtb-0ac581ded2cd7ba2d / lab-rtb-private1-us-east-1a
lab-subnet-public1-us-east-1a	subnet-04eef38a38c122297	10.0.0.0/24	-	rtb-0fa868d8374751624 / lab-rtb-public
lab-subnet-private2	subnet-05c13e984c277901	10.0.3.0/24	-	rtb-0ac581ded2cd7ba2d / lab-rtb-private1-us-east-1a

Selected subnets

Save associations

Next, you will configure a security group to permit HTTP access to a web server. Go to the “Security groups” page from the sidebar.

- Filter by 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
 - NAT gateways
 - Peering connections
- ▼ Security
 - Network ACLs
 - Security groups**

Click “Create security group”.

Security Groups (4) Info

Create security group

Under “Basic details”, set the name to “Web Security Group”, the description to “Enable HTTP Access”, and the VPC to “lab-vpc”.

The screenshot shows the 'Basic details' section of the AWS Security Groups creation wizard. It includes fields for 'Security group name' (Web Security Group), 'Description' (Enable HTTP access), and 'VPC' (vpc-0b119727c01eb831d (lab-vpc)). The 'VPC' field has a red underline.

Under “Inbound rules”, click “Add rule”.

The screenshot shows the 'Inbound rules' section with the message "This security group has no inbound rules." A large red arrow points to the 'Add rule' button.

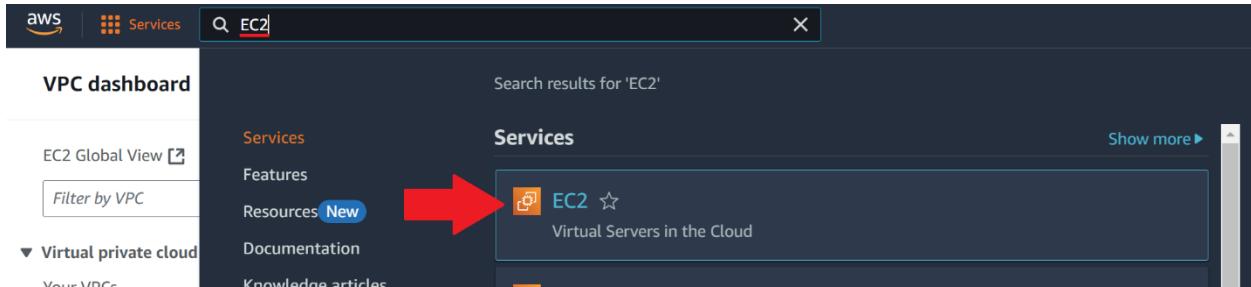
Set the rule type to “HTTP”, the source to “Anywhere-IPv4”, and the description to “Permit web requests”. Click “Add rule”.

The screenshot shows the 'Inbound rules' configuration page. The 'Type' dropdown is set to 'HTTP' (with a red arrow), 'Protocol' is 'TCP', 'Port range' is '80', 'Source' is 'Anywhere-IPv4' (with a red arrow), and 'Description - optional' is 'Permit web requests' (with a red arrow). A red arrow also points to the 'Add rule' button at the bottom left.

Click “Create security group”.

The screenshot shows the final step of creating the security group. A large red arrow points to the 'Create security group' button, which is highlighted in orange.

Next, we will create a web server with this security group applied. Open the EC2 dashboard from the search bar.



Click “Launch instance”.

A screenshot of the "Launch instance" page. The title is "Launch instance" and the sub-instruction is "To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud." There are two buttons: "Launch instance" (highlighted with a red border) and "Migrate a server". A note below states: "Note: Your instances will launch in the US East (N. Virginia) Region".

Set the name to “Web Server 1” and set the Amazon Machine Image to “Amazon Linux 2023 AMI”.

A screenshot of the "Launch an instance" configuration page. The "Name and tags" section has "Name" set to "Web Server 1". The "Application and OS Images (Amazon Machine Image)" section shows a search bar and a grid of OS icons. The "Amazon Machine Image (AMI)" section highlights the "Amazon Linux 2023 AMI" (ami-045sec754f44f9a4a). The "Description" section provides details about Amazon Linux 2023. The bottom section shows configuration for "Architecture" (64-bit (x86)), "Boot mode" (uefi-preferred), "AMI ID" (ami-045sec754f44f9a4a), "Username" (ec2-user), and "Verified provider".

Set the instance type to “t2.micro”.

▼ Instance type [Info](#) | [Get advice](#)

Instance type

t2.micro

Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Windows base pricing: 0.0162 USD per Hour
On-Demand Ubuntu Pro base pricing: 0.0134 USD per Hour
On-Demand SUSE base pricing: 0.0116 USD per Hour On-Demand RHEL base pricing: 0.026 USD per Hour
On-Demand Linux base pricing: 0.0116 USD per Hour

Free tier eligible

All generations

[Compare instance types](#)

[Additional costs apply for AMIs with pre-installed software](#)

Set the Key pair to “vockey”.

▼ Key pair (login) [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - required

vockey

[Create new key pair](#)

Under “Network settings”, set the VPC to “lab-vpc”, the subnet to “lab-subnet-public2”, and “Auto-assign public IP” to “Enable”. Set the “Firewall (security groups)” to “Select existing security groups” and add the “Web Security Group” created earlier.

▼ Network settings [Info](#)

VPC - required [Info](#)

vpc-0b119727c01eb831d (lab-vpc)
10.0.0.0/16

[Create new VPC](#)

Subnet [Info](#)

subnet-0b7125fb16f87168a lab-subnet-public2
VPC: vpc-0b119727c01eb831d Owner: 924210465458 Availability Zone: us-east-1b
Zone type: Availability Zone IP addresses available: 251 CIDR: 10.0.2.0/24

[Create new subnet](#)

Auto-assign public IP [Info](#)

Enable

Additional charges apply when outside of free tier allowance

Firewall (security groups) [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group

Select existing security group

Common security groups [Info](#)

Select security groups

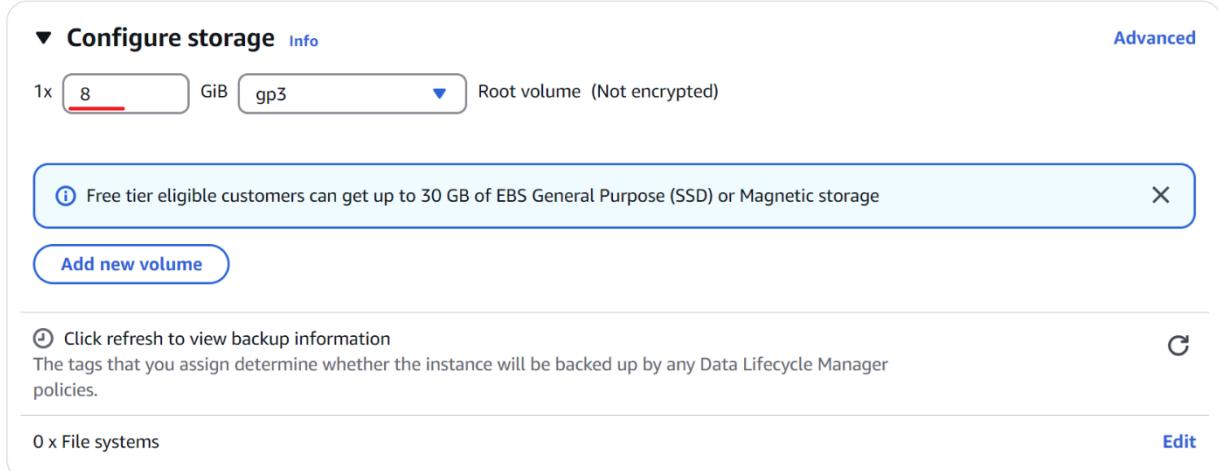
Web Security Group sg-0380efff0878eebab X
VPC: vpc-0b119727c01eb831d

[Compare security group rules](#)

Security groups that you add or remove here will be added to or removed from all your network interfaces.

► Advanced network configuration

Under “Configure storage”, set the storage to 8 Gibibytes.



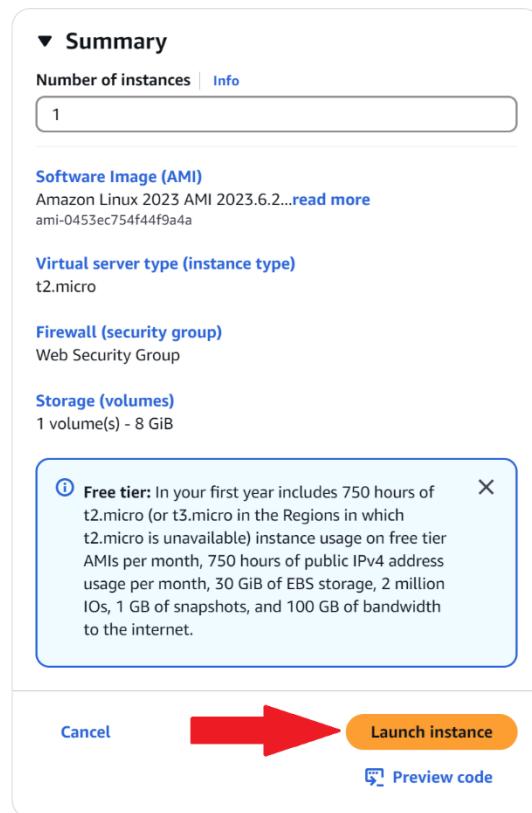
Open the “Advanced details” tab.

▼ Advanced details [Info](#)

Scroll down to the “User data” section.

Add the following script:

```
#!/bin/bash
# Install Apache Web Server and PHP
dnf install -y httpd wget php mariadb105-server
# Download Lab files
wget https://aws-tc-largeobjects.s3.us-west-2.amazonaws.com/CUR-
TF-100-ACCLFO-2/2-lab2-vpc/s3/lab-app.zip
unzip lab-app.zip -d /var/www/html/
# Turn on web server
chkconfig httpd on
service httpd start
Click “Launch Instance”.
```



Click “View All Instances”.



Click the checkbox next to “Web Server 1”.

After the “Status Check” section says “2/2 checks passed”, look for the public IPv4 address of the server and click the button to open the URL in a new tab:

i-0f8cef3e324f29f82 (Web Server 1)

Details Status and alarms | Monitoring | Security | Networking | Storage | Tags

Instance summary [Info](#)

Instance ID [i-0f8cef3e324f29f82](#)

IPv6 address —

Hostname type IP name: ip-10-0-2-165.ec2.internal

Answer private resource DNS name —

Auto-assigned IP address [3.237.181.14 \[Public IP\]](#)

Public IPv4 address [3.237.181.14 | open address](#)

Instance state [Running](#)

Private IP DNS name (IPv4 only) [ip-10-0-2-165.ec2.internal](#)

Instance type t2.micro

VPC ID [vpc-0b119727c01eb831d \(lab-vpc\)](#)

Private IPv4 addresses [10.0.2.165](#)

Public IPv4 DNS [ec2-3-237-181-14.compute-1.amazonaws.com | open address](#)

Elastic IP addresses —

AWS Compute Optimizer finding [Opt-in to AWS Compute Optimizer for recommendations.](#) | Learn more

If done correctly, a page like this should open:

Instances | EC2 | us-east-1 | Welcome to AWS Technical +

← → Q ⓘ Not Secure ec2-3-237-181-14.compute-1.amazonaws.com

[Home](#) [Shopping](#) [Travel](#) [Bookmarks](#) [AWS Canvas](#)

[aws](#) Load Test RDS

Meta-Data	Value
InstanceId	i-0f8cef3e324f29f82
Availability Zone	us-east-1b

Current CPU Load: 7%

Lab Commands (Lab 3 EC2)

Open the EC2 console from the search bar.

aws | EC2

Services

EC2 Virtual Servers in the Cloud

EC2 Image Builder A managed service to automate build, customize and deploy OS images

Show more

Ensure you have the North Virginia region selected.

N. Virginia ▲

Region	Region Name
United States	
N. Virginia	us-east-1
Ohio	us-east-2
N. California	us-west-1
S. California	us-west-2

From the EC2 homepage, select “Launch Instance”.

Launch instance

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

Launch instance



Note: Your instances will launch in the US East (N. Virginia) Region

Name this instance “Web Server”.

Name and tags Info

Name

Web Server

[Add additional tags](#)

Set the AMI to “Amazon Linux 2023 AMI” and set the instance type to “t2.micro”.

▼ Application and OS Images (Amazon Machine Image) Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below.

Q Search our full catalog including 1000s of application and OS images

Recent [Quick Start](#)

Amazon Linux macOS Ubuntu Windows Red Hat SUSE Linux Debian

Amazon Machine Image (AMI)

Amazon Linux 2023 AMI ami-04d3e754f4495a4a (64-bit x86, uefi preferred) / ami-0fb53e778a23014a (64-bit UEFI, uefi) Free tier eligible

Description

Amazon Linux 2023 is a modern, general purpose Linux-based OS that comes with 5 years of long term support. It is optimized for AWS and designed to provide a secure, stable and high-performance execution environment to develop and run your cloud applications.

Amazon Linux 2023 AMI 2023.6.20241121.0.x86_64 HVM kernel-6.1

Architecture Boot mode AMI ID Username

64-bit (x86) uefi-preferred ami-0453ec754f4495a4a ec2-user Verified provider

▼ Instance type Info | Get advice

Instance type t2.micro

t2.micro 1 vCPU 1 GB Memory Current generation: true

On-Demand Windows base pricing: 0.0162 USD per Hour

On-Demand Ubuntu Pro base pricing: 0.0134 USD per Hour

On-Demand SUSE base pricing: 0.0116 USD per Hour On-Demand RHEL base pricing: 0.0216 USD per Hour

All generations Compare instance types

Set the key pair to “vockey”.

▼ Key pair (login) Info

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - **required**

vockey

[Create new key pair](#)

Under “Network Settings”, click “Edit”.

▼ Network settings Info



Edit

Set the VPC to “Lab VPC”, the subnet to “Public Subnet 1”, and the “Auto-Assign Public IP” setting to “enable”. Create a new security group with the name “Web Server security group” and the description “Security group for my web server”.

▼ Network settings [Info](#)

VPC - required [Info](#)
vpc-0880e90346060a779 (Lab VPC)
10.0.0.0/16

Subnet [Info](#)
subnet-03978ef8e7d5c0fa7
VPC: vpc-0880e90346060a779 Owner: 938883298313 Availability Zone: us-east-1a
Zone type: Availability Zone IP addresses available: 1 CIDR: 10.0.1.0/28

Auto-assign public IP [Info](#)
Enable

Additional charges apply when outside of free tier allowance

Firewall (security groups) [Info](#)
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

[Create security group](#) [Select existing security group](#)

Security group name - required
Web Server security group

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and _-:/()#,@[]+=&;!\$^*

Description - required [Info](#)
Security group for my web server

Inbound Security Group Rules

▼ Security group rule 1 (TCP, 22, 0.0.0.0/0) [Remove](#)

Type Info	Protocol Info	Port range Info
ssh	TCP	22
Source type Info	Source Info	Description - optional Info
Anywhere	Add CIDR, prefix list or security group 0.0.0.0/0 X	e.g. SSH for admin desktop

Make sure to remove “Security group rule 1”.

Inbound Security Group Rules

▼ Security group rule 1 (TCP, 22, 0.0.0.0/0) 

Type Info	Protocol Info	Port range Info
ssh	TCP	22
Source type Info	Source Info	Description - optional Info
Anywhere	Add CIDR, prefix list or security group 0.0.0.0/0 X	e.g. SSH for admin desktop

⚠ Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only. X

[Add security group rule](#)

Under “Configure storage”, select 8 GiB of gp3.

Configure storage [Info](#)

1x GiB Root volume (Not encrypted)

ⓘ Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage

[Add new volume](#)

ⓘ Click refresh to view backup information
The tags that you assign determine whether the instance will be backed up by any Data Lifecycle Manager policies.

0 x File systems [Edit](#)

Go to the Advanced Details section.

Advanced details [Info](#)

Termination protection [Info](#)

Enter the following into the “User Data” section:

```
#!/bin/bash
dnf install -y httpd
systemctl enable httpd
systemctl start httpd
echo '<html><h1>Hello From Your Web Server!</h1></html>' >
/var/www/html/index.html
```

User data - optional | [Info](#)

Upload a file with your user data or enter it in the field.

[Choose file](#)

```
#!/bin/bash
dnf install -y httpd
systemctl enable httpd
systemctl start httpd
echo <html><h1>Hello From Your Web Server!</h1></html> >
/var/www/html/index.html
```

Under the “Summary” section, click “Launch Instance”.

▼ **Summary**

Number of instances | [Info](#)

1

Software image (AMI)

Amazon Linux 2023 AMI 2023.6.2... [read more](#)

ami-0452cc754f44f9a4a

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

[Cancel](#)  [Launch instance](#) [Preview code](#)

After launching the EC2 instance, click “View all instances”.

View all instances

Wait for your web server to have the instance state of “Running”, then click the checkbox next to it.

<input type="checkbox"/>  Web Server	i-010cc7662e674e509	 Running  	t2.micro	 2/2 checks passed	
---	---------------------	---	----------	---	---

Under the “Status and Alarms” tab, ensure that both reachability checks have passed.

Click “Actions > Monitor and troubleshoot > Get system log”.

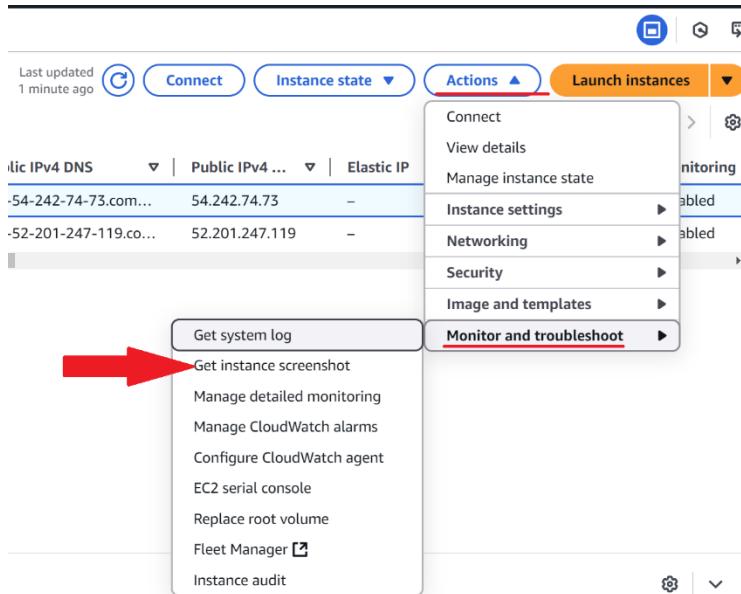
If done correctly, you should see a reference to the “httpd” service started in the User Data section.

```

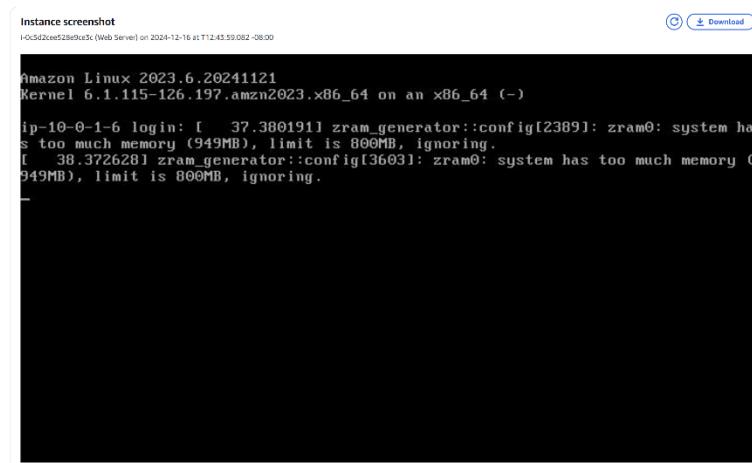
[ 38.935061] cloud-init[2221]: mod_lua-2.4.62-1.amzn2023.x86_64
[ 38.937650] cloud-init[2221]: Complete!
[ 39.045738] cloud-init[2221]: Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/lib/systemd/system/httpd.service.
[ 38.372628] zram_generator::config[3603]: zram0: system has too much memory (949MB), limit is 800MB, ignoring.
ci-info: +-----+-----+-----+-----+
ci-info: | Keypair | Fingerprint (sha256) | Options | Comment |
ci-info: +-----+-----+-----+-----+
ci-info: | ssh-rsa | e6:7b:08:96:5e:49:f2:5a:1c:c0:35:50:60:64:57:60:66:aa:ac:4a:07:51:83:14:b2:fd:80:47:a1:a0:19:15 | - | vockey |
ci-info: +-----+-----+-----+-----+
<14>Dec 16 20:38:32 cloud-init: #####
<14>Dec 16 20:38:32 cloud-init: #####
<14>Dec 16 20:38:32 cloud-init: BEGIN SSH HOST KEY FINGERPRINTS-----
<14>Dec 16 20:38:32 cloud-init: 256 SHA256:R8/o3wyXrKCFjeB/xH4XTCarGv1tx8FfdNl13ZaONQ root@ip-10-0-1-6.ec2.internal (EDDSA)
<14>Dec 16 20:38:32 cloud-init: 256 SHA256:9mpjPVLFvEfuQosx2rt8mjZv6cc2iZNzSj1l002AA root@ip-10-0-1-6.ec2.internal (ED25519)
<14>Dec 16 20:38:32 cloud-init: ----END SSH HOST KEY FINGERPRINTS-----
<14>Dec 16 20:38:32 cloud-init: #####
----BEGIN SSH HOST KEY KEYS-----
ecdsa-sha2-nistp256 AAAEAV2Vj7HNnLXn0YITtbm1zdHJhdAhyITYAAABBLw1A0AOw964nDAw9TYFmV1vsg0Q0U3gtfBQjyOT/q+QbBGF2Gy5m8pkSGtngcmJB8c7DbaN7td4Hgq= root@ip-10-0-1-6
ssh-ed25519 AACAC3nzaC11zDIINTE5AAAII5BPfhqnjdXkajb6+H0Woy1SVi+HTgdFnMzdimEK root@ip-10-0-1-6.ec2.internal
----END SSH HOST KEY KEYS-----
[ 39.695104] cloud-init[2221]: Cloud-init v. 22.2.2 finished at Mon, 16 Dec 2024 20:38:32 +0000. Datasource DataSourceEc2. Up 39.68 seconds

```

Return to the instances page and click Actions > Monitor and troubleshoot > Get instance screenshot.



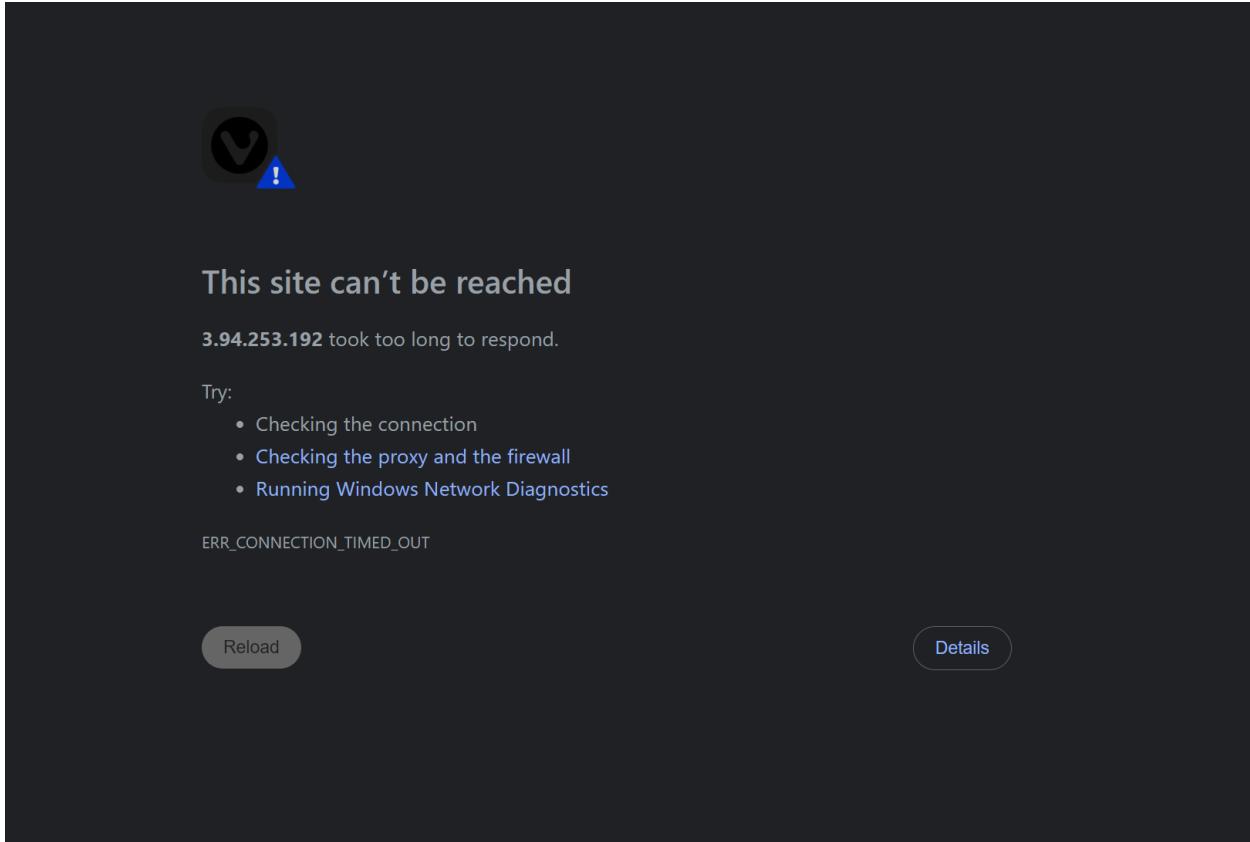
You should see a screenshot similar to this:



On the instances page, select Web Server and click open address under the Public IPv4 address field.

The screenshot shows the AWS Instances page. It lists several instances, with one instance named 'Web Server' selected. A red arrow points to the checkbox next to 'Web Server'. Another red arrow points to the 'open address' link next to the 'Public IPv4 address' field for the selected instance. The instance details page for 'i-0c7554ed44d4e1603 (Web Server)' is shown below, with the 'Details' tab selected. The 'Public IPv4 address' field contains '3.94.253.192' and the 'open address' link is highlighted with a red arrow.

You should see an error message. This is because the security group for the instance has not yet been configured to permit HTTP access.



Next, you will configure a security group for the EC2 instance. Go to Security Groups > Select Web server security group > Inbound rules > Edit inbound rules.

A screenshot of the AWS Management Console showing the "Security Groups (1/5) - Info" page. The left sidebar shows various AWS services like Instances, Images, Elastic Block Store, Network & Security, Load Balancing, and Auto Scaling. A red arrow points to the "sg-0695acd804598b6cf" entry in the list, which is labeled "Web Server security group". The main pane shows a table with columns: Name, Security group ID, Security group name, VPC ID, Description, Owner, and Inbound rules count. The "Inbound rules" tab is selected for the "sg-0695acd804598b6cf - Web Server security group" details page. A red arrow points to the "Edit inbound rules" button at the bottom right of this pane.

Click Add rule, set the type to HTTP, the source to Anywhere-IPv4, then click Save rules.

Edit inbound rules Info

Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules Info

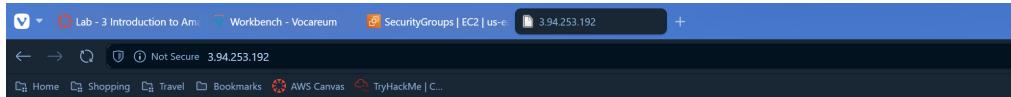
Security group rule ID	Type	Protocol	Port range	Source	Description - optional	Delete
-	HTTP	TCP	80	Anywhere... <small>Anywhere-IPv4</small>	0.0.0.0/0	Delete

[Add rule](#)

⚠ 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.

[Cancel](#) [Save rules](#)

Refresh the web server page. You should see the following message:



Hello From Your Web Server!

Next, you will resize the instance. Go to Instances > Select Web Server > Instance state > Stop instance.

Instances (1/2) Info

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4
Bastion Host	i-09928d430b55929	Running	t2.micro	2/2 checks passed	View alarms	us-east-1a	ec2-3-82-56-112.comp...	3.82.56.112
Web Server	i-0c7554ed44d4e1603	Running	t2.micro	Initializing	View alarms	us-east-1a	ec2-3-94-253-192.com...	3.94.253.19

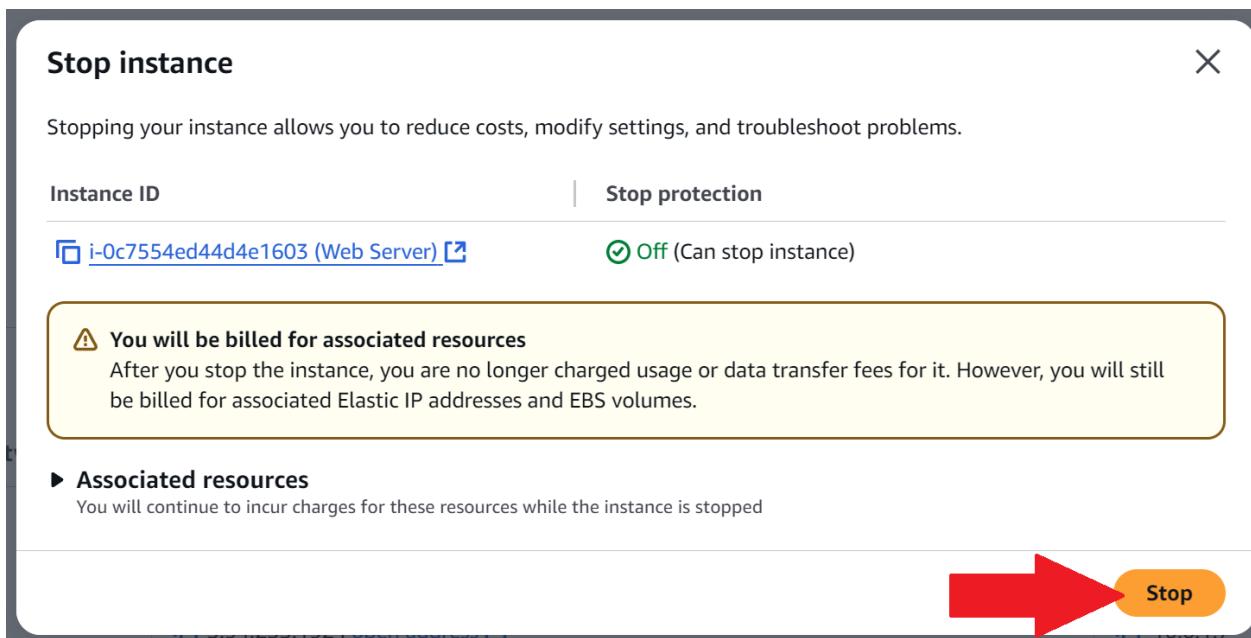
Last updated 9 minutes ago

[Connect](#) [Actions](#) [Launch instances](#)

[Stop instance](#) [Start instance](#) [Reboot instance](#) [Hibernate instance](#) [Terminate \(delete\) instance](#)

[IPv6 IPs](#) [Monitoring](#)

Click Stop.



Click the refresh icon until the instance state shows Stopped, then go to Actions > Instance settings > Change instance type.

Set the instance type to t2.small, then click Change.

Change instance type [Info](#) | [Get advice](#)

You can change the instance type only if the current instance type and the instance type that you want are compatible.

Instance ID	i-0755e4d44de1603 (Web Server)	
Current instance type	t2.micro	
New instance type	<input type="text" value="t2.small"/> X	
EBR-optimized		
EBR-optimized is not supported for this instance type.		
Instance type comparison		
Attribute	t2.micro	t2.small
On-Demand Linux pricing	0.0116 USD per Hour	0.0230 USD per Hour
On-Demand Windows pricing	0.0162 USD per Hour	0.0320 USD per Hour
vCPUs	1 (1 core)	1 (1 core)
Memory (MB)	1024	2048
Storage (GB)	-	-
Supported root device types	ebs	ebs
Network performance	Low to Moderate	Low to Moderate
Architecture	32-bit	32-bit
Bundlable	true	true
Free-tier eligible	true	false
Current generation	true	true

[Compare more instance type attributes](#)

Advanced details

The t2.small instance type does not support changing CPU options.

[Change](#)



Go to Actions > Instance settings > Change stop protection.

Instance type changed successfully

Instances (1/2) [Info](#)

Last updated 1 minute ago [Connect](#) [Instance state](#) [Actions](#) [Launch instances](#)

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 IP	Elastic IP	IPv6 IPs	Monitoring	Security group name
Bastion Host	i-0923661506c55029	Running View Logs	t2.micro	2/2 checks passed	View alarms +	us-east-1a	ec2-5-82-56-112.compute-1.amazonaws.com	58.256.112	-	-	Edit	Attach to Auto Scaling Group
Web Server	i-0755e4d44de1603	Stopped View Logs	t2.small	-	View alarms +	us-east-1a	-	-	-	-	Edit	Change termination protection

[Change stop protection](#)

- [Change shutdown behavior](#)
- [Change auto-recovery behavior](#)
- [Change instance type](#)
- [Change CPU options](#)
- [Change Nitro features](#)
- [Change credit specification](#)
- [Change resource based naming options](#)
- [Modify instance placement](#)
- [Modify Capacity Reservation settings](#)
- [Edit user data](#)
- [Allow tags in instance metadata](#)



Click Enable, then click save.

Change stop protection [Info](#)

Enable stop protection to prevent your instance from being accidentally stopped.

Instance ID	i-0c5d2cee528e9ce3c (Web Server)
Stop protection	<input checked="" type="checkbox"/> Enable

[Save](#)




Next, go to the web server's Storage tab..

i-0c5d2cee528e9ce3c (Web Server)

[Details](#) [Status and alarms](#) [Monitoring](#) [Security](#) [Networking](#) [Storage](#) [Tags](#)

Select the volume created earlier, then click Actions > Modify volume.

Volumes (1/1) [Info](#)

Saved filter sets [Choose filter set](#)

<input checked="" type="checkbox"/>	Name	Volume ID	Type	Size	IOPS	Throughput	Snapshot ID	Created	Availability Zone	Volume state	Actions
<input checked="" type="checkbox"/>	vol-090fbf8a754c4cf2a	gp3	8 GiB	3000	125		snap-0938e31...	2024/12/16 12:37 GMT-8	us-east-1a	In-use	<input type="button" value="Actions"/> <input type="button" value="Create volume"/>

Attached resources
5d2ce528e9ce5c (W)

Change the size to 10 GiB.

Volume type | [Info](#)

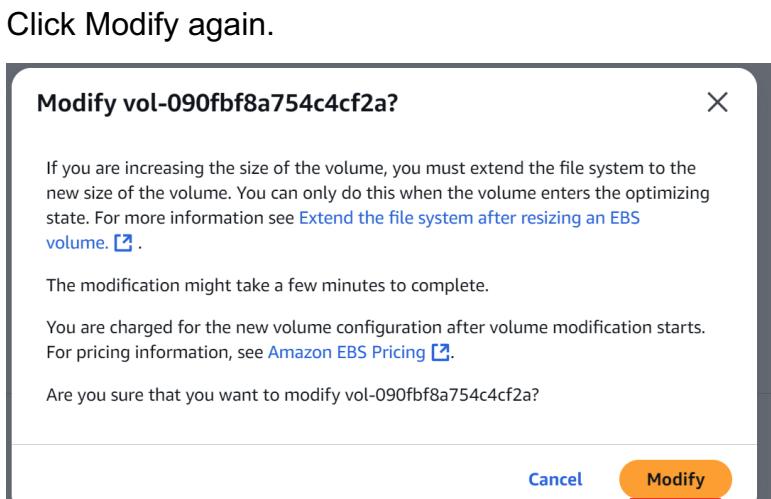
General Purpose SSD (gp3)

Size (GiB) | [Info](#)

Min: 1 GiB, Max: 16384 GiB.

Click Modify.

[Cancel](#) [Modify](#)



Return to the Instances section of the EC2 dashboard.

▼ Instances

Instances

Instance Types

Launch Templates

Spot Requests

Select Web Server and click Instance state > Start instance.

The screenshot shows the AWS EC2 Instances page. There are two instances listed:

Name	Instance ID	Instance state	Instance type	Status check t	Alarm status	Availability Zone	Public IPv4 DNS	Public IP
Web Server	i-0c5d2cee528e9ce3c	Stopped	t2.small	-	View alarms	us-east-1a	-	-
Bastion Host	i-09e4cc6b7f5fee95c	Running	t2.micro	...	View alarms	us-east-1a	ec2-52-201-247-119.co...	52.201.247.119

Actions dropdown menu (for the Web Server):

- Stop instance
- Start instance** (highlighted)
- Reboot instance
- Hibernate instance
- Terminate (delete) instance

While the EC2 instance is starting, go to the Service Quotas dashboard from the search bar.

The screenshot shows the AWS Service Quotas dashboard. The sidebar has 'Instances' selected, and 'Instances' is also highlighted in the main content area. The main content shows the 'Service Quotas' card:

Service Quotas
View and manage your AWS service quotas from a central location

Trusted Advisor
Optimize performance, improve security, reduce costs

Select AWS services from the sidebar.

Service Quotas

Dashboard

AWS services

Quota request history

Organization

Quota request template

Search for and select Amazon Elastic Compute Cloud (Amazon EC2).

AWS services

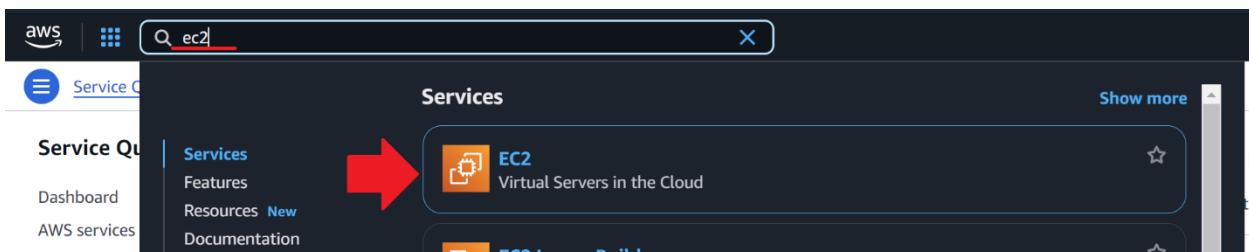
The screenshot shows the AWS search interface. A search bar at the top contains the text "ec2". To the right of the search bar, it says "5 matches". Below the search bar is a list titled "Service" containing several links: "Amazon EC2 Auto Scaling", "Amazon Elastic Compute Cloud (Amazon EC2)" (which is underlined in red), "EC2 Fast Launch", "EC2 Image Builder", and "EC2 VM Import/Export".

Search for running on-demand. Note the limits applied to how many concurrent EC2 instances can be run based on the instance type. Ensure that you do not surpass these limits while working with EC2.

The screenshot shows the "Service quotas" page. A search bar at the top contains the text "running on-demand". To the right of the search bar, it says "10 matches". Below the search bar is a table with columns: "Quota name", "Applied account-level quota value", "AWS default quota value", "Utilization", and "Adjustability". The table lists various EC2 instance types with their respective quota values. A red box highlights the "Applied account-level quota value" column.

Quota name	Applied account-level quota value	AWS default quota value	Utilization	Adjustability
Running On-Demand DL instances	96	0	0	Account level
Running On-Demand F instances	64	0	0	Account level
Running On-Demand G and VT instances	0	0	0	Account level
Running On-Demand High Memory instances	0	0	0	Account level
Running On-Demand HPC instances	192	0	0	Account level
Running On-Demand Inf instances	8	0	0	Account level
Running On-Demand P instances	0	0	0	Account level
Running On-Demand Standard (A, C, D, H, I, M, R, T, Z) instances	256	5	1	Account level
Running On-Demand Trn instances	8	0	0	Account level
Running On-Demand X instances	0	0	0	Account level

Return to the EC2 dashboard from the search bar.



From the homepage, click Instances (running) under the Resources tab.

The screenshot shows the "Resources" page for Amazon EC2. A red arrow points to the "Instances (running)" link, which is underlined in blue. To the right of the link, the number "2" indicates the count of running instances.

Select Web Server.

Instances (1/2) [Info](#)

Find Instance by attribute or tag (case-sensitive)

Name	Instance ID
<input checked="" type="checkbox"/> Web Server	i-0c5d2cee528e9ce3c
<input type="checkbox"/> Bastion Host	i-09e4cc6b7f5fee95c

Select Instance state > Stop instance.

Instance state ▲ Actions ▼

Stop instance 

Start instance
Reboot instance
Hibernate instance
Terminate (delete) instance

IPv4 IP IPv6 IP

Click stop. Note the warning that stop protection is on.

Stop instance 

Stopping your instance allows you to reduce costs, modify settings, and troubleshoot problems.

Instance ID	Stop protection
i-0c5d2cee528e9ce3c (Web Server)	 On (Can't stop instance)

⚠ You will be billed for associated resources
After you stop the instance, you are no longer charged usage or data transfer fees for it. However, you will still be billed for associated Elastic IP addresses and EBS volumes.

▶ Associated resources
You will continue to incur charges for these resources while the instance is stopped

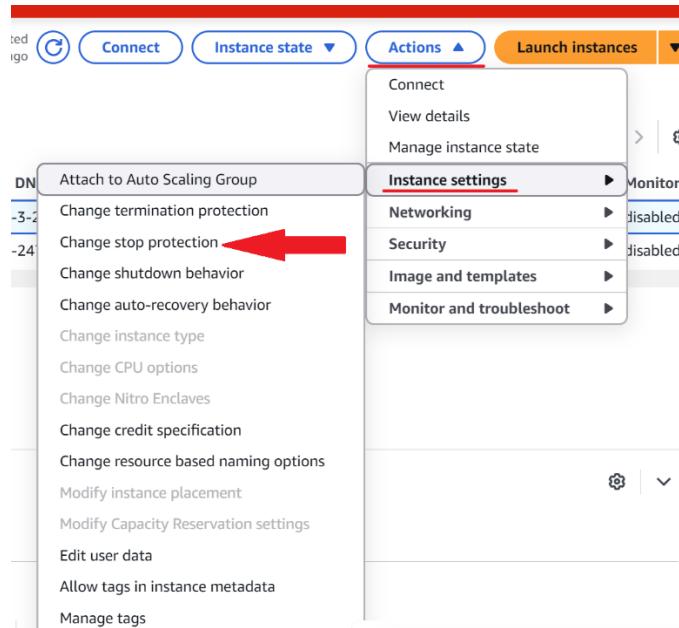
Stop

You will see the following error message.

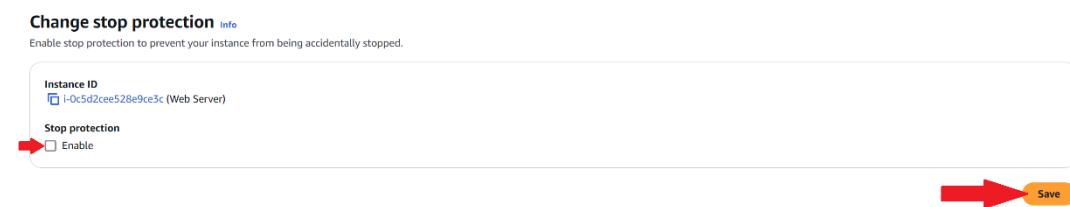
Failed to stop the instance i-0c5d2cee528e9ce3c
The instance 'i-0c5d2cee528e9ce3c' may not be stopped. Modify its 'disableApiStop' instance attribute and try again.

[Diagnose with Amazon Q](#)

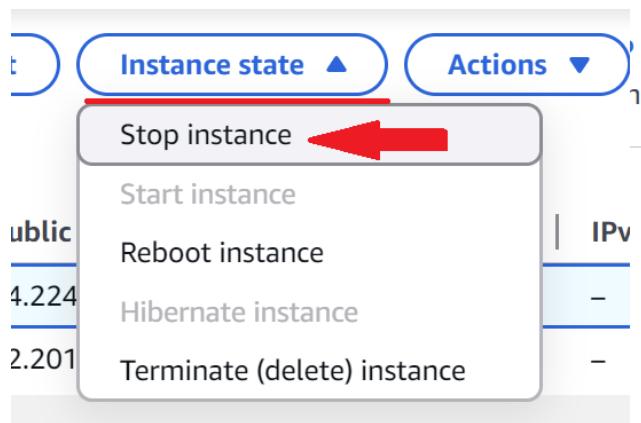
Next, you will disable stop protection. Go to Actions > Instance settings and click Change stop protection.



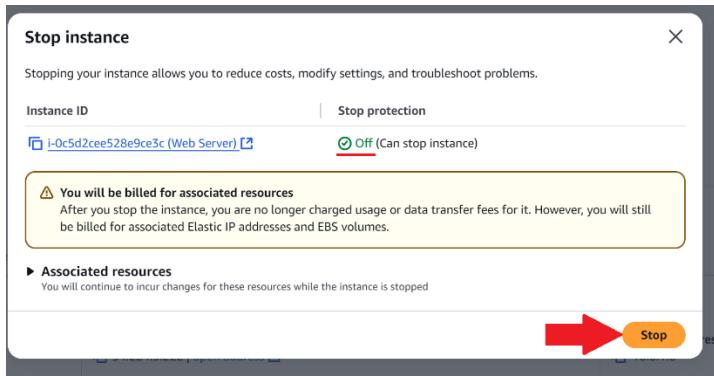
Uncheck Enable and click Save.



Now, click Instance state > Stop instance.



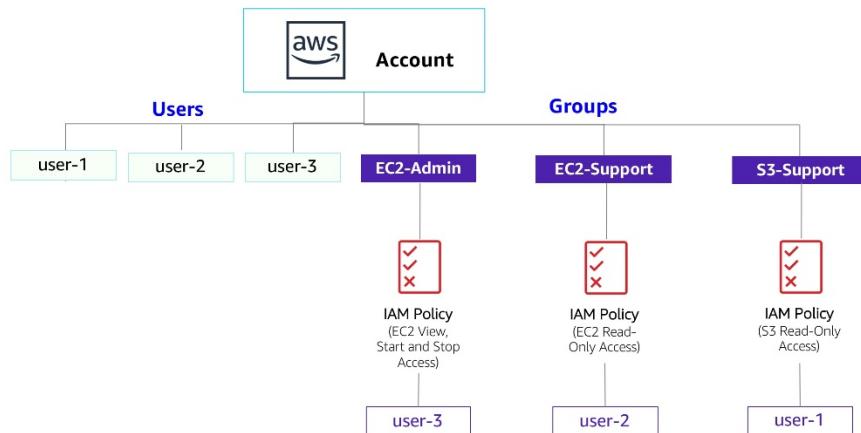
Click Stop. Note the confirmation that stop protection is now off.



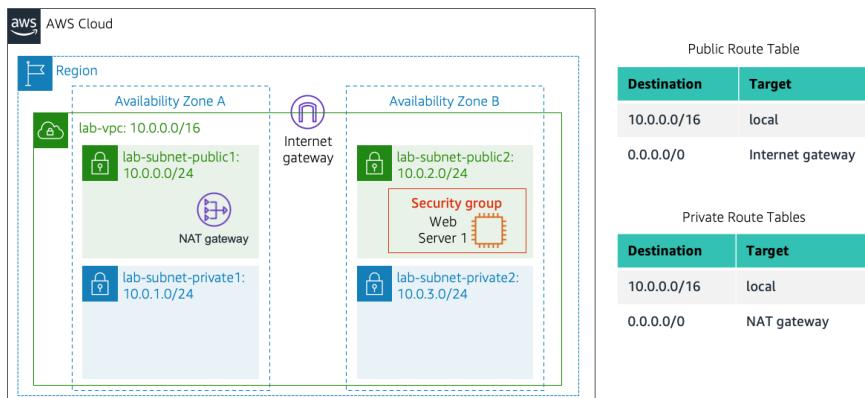
Wait a few minutes and refresh the Instances page. The web server's instance state should now show as Stopped.



Network Diagram (Lab 1 IAM)



Network Diagram (Lab 2 VPC)



Network Diagram (Lab 3 EC2)



Problems

One problem I encountered was in Lab 3 (the EC2 lab), where even after correctly updating the Web server security group, the server's webpage refused to connect. This is because my web browser attempted to connect with HTTPS instead of HTTP. This was fixed simply by modifying the protocol in the URL to connect over HTTP.

Conclusion

To wrap up, this lab was a very useful introduction to the world of cloud computing. I'm grateful to have learned about exciting new cloud computing concepts such as complex security mechanisms, virtual routing through a private cloud, and easily scalable virtual machines. I'm now confident that I could help a company migrate basic services from traditional IT to the cloud, I'm hopeful that these foundational skills will help me secure a career in cloud services in the future.