

CLOUD COMPUTING LABS SECTION I

Daniel Ge

Period 678



CISCO

CCNP LAB REPORT

Purpose

To practice the AWS concepts covered in the AWS Cloud Foundations course and train to use the AWS system in our companies, we must go through mock scenarios where we implement AWS Cloud solutions to address business goals our company may have. Through these three labs, we practice using the AWS Management Console accessed through a web browser to achieve setting up many services or networks, such as virtual machines, virtual networks, and security policies for a hypothetical company. At the end of these exercises, we are better prepared to replicate these steps to real-life business scenarios.

Background Information

Under the AWS Shared Responsibility Model, although AWS will protect the security of the cloud, including the computing resources and servers, it is the user's responsibility to ensure security in the cloud by protecting elements like their own data and configuring firewalls. The AWS IAM (Identity and Access Management) Service provides a framework to achieve this for AWS users. AWS IAM is split into two halves corresponding to the two pillars of web security: authorization and authentication.

With AWS IAM authentication, we may verify that users accessing their AWS account are who they claim to be. To achieve this, IAM allows us to configure which login credentials employees are required to set, from passwords to access keys. We additionally have the ability to apply MFA (multi-factor authentication) to combine multiple authentication methods during login.

Through AWS IAM authorization, we may configure users, groups, and roles. Users and groups of users are usually static, but roles can be applied to users or applications temporarily. After these are defined, we may then configure policies to be applied to these subjects. The policies will rule what the users, groups, and roles may complete.

Using AWS IAM, administrators can configure access permissions to the company's web resources. Additional tools may be applied to encrypt data at rest and in transit. Given that Amazon continues to properly secure the AWS cloud itself, with the correct security settings, intruders and malicious actors will be prevented from accessing, viewing, or altering company resources.

Just as breakthroughs in communications allowed for the construction of networks, where devices with 32-bit IPv4 or 128-bit IPv6 addresses may communicate with each other, we may build networks on AWS as well using Amazon VPC (Virtual Private Cloud). VPCs are networks run on AWS logically isolated from VPCs of other accounts and dedicated to one AWS account. Unlike traditional networks, however, AWS allows us to deploy VPCs in one region but multiple availability zones within the region.

Within each availability zone, we may deploy subnets. Subnets are divided into public and private types. Public subnets may communicate with the public internet through an IGW (internet gateway) while private subnets can be accessed through a NAT gateway. AWS allows us to construct routes between the networks and IP addresses of applications within the networks. There also exist additional services such as VPC sharing, VPC peering, or VPC site-to-site VPNs to better connect VPC subnets or VPCs themselves, but they are beyond the scope of this lab.

One of the most common uses of Amazon VPCs is using them to launch Amazon EC2 instances. Since VPCs provides the networking environment and security configurations beyond that of what EC2 itself can provide, we isolate EC2 instances in the VPCs and assign them with IP addresses to use them. Just as we cannot use a real-life computer to provide a service to customers without connecting it to a network, we cannot use virtual EC2 machines without having a VPC network.

To handle the IT load of running a large organization including businesses or research institutes, we often need to employ the use of large data servers. However, given the difficulty and cost in maintaining, scaling, and running these servers independently, Amazon AWS offers the opportunity to migrate away from traditional company data centers to virtual machines on the cloud. Using Amazon EC2 (Elastic Compute Cloud), we may use AWS virtual machines' computing power to run services like web servers, gaming servers, or file servers for our users.

Amazon EC2 instances are launched from AMIs (Amazon Machine Images) based on operating systems like Linux or Windows and packages them in such a way they can be used for AWS. Users then have the option to configure instance size, with various levels of memory, CPU processing power, disk space, and network performance. To optimize costs, users should consider their priorities and select appropriately sized instances.

Additional configurations that users will set when creating and using an Amazon EC2 instance includes network settings (selecting the VPC), IAM role, user data (what the virtual machine contains), storage options (storage volume size), tags, security groups, and key pair.

Lab Summary

In Lab 1, the Introduction to IAM lab, we will open a sample AWS account with 3 pre-existing IAM Users and Groups set with pre-existing policies: EC2-Admin, EC2-Support, and S3-Support. These groups are respectively configured with permissions to modify EC2 instances, view EC2 instances, and view S3 information. We will then configure three users with the correct permissions, then log in through their usernames and passwords to verify that each user is configured to be able to do precisely what they are meant to do.

In Lab 2, we practice building and using a VPC (Virtual Private Cloud) on AWS. We follow steps to configure public and private subnets in the VPC across multiple Availability Zones, including NAT Gateways and Internet Gateways to allow for communication with the VPC. We will additionally configure the VPC with other necessary components including

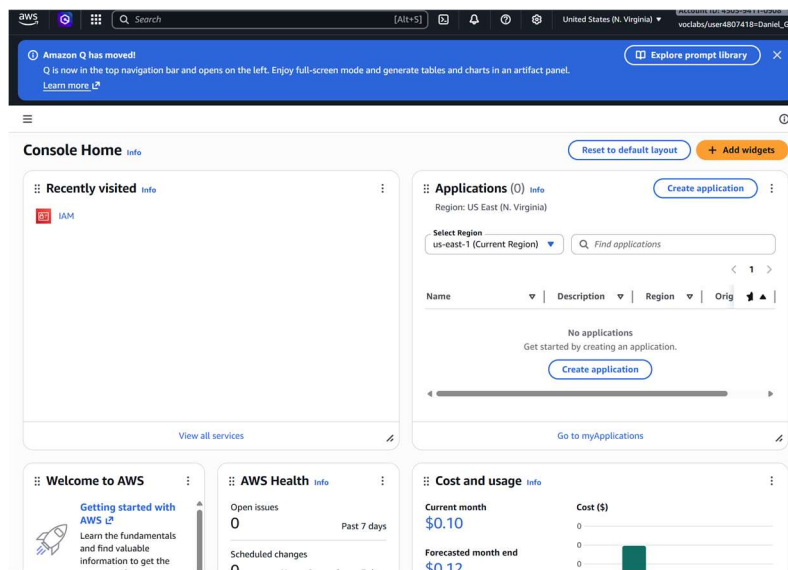
security groups. In the end, we will practice using the VPC by launching an EC2 instance into the VPC.

Lab 3 focuses on launching an EC2 instance. We will launch the instance with the appropriate configurations in security to allow for HTTP traffic and practice monitoring the instance. Afterwards, we will experiment with features such as stopping the EC2 instance to adjust its size or stop protection, which prevents the instance from getting stopped on accident.

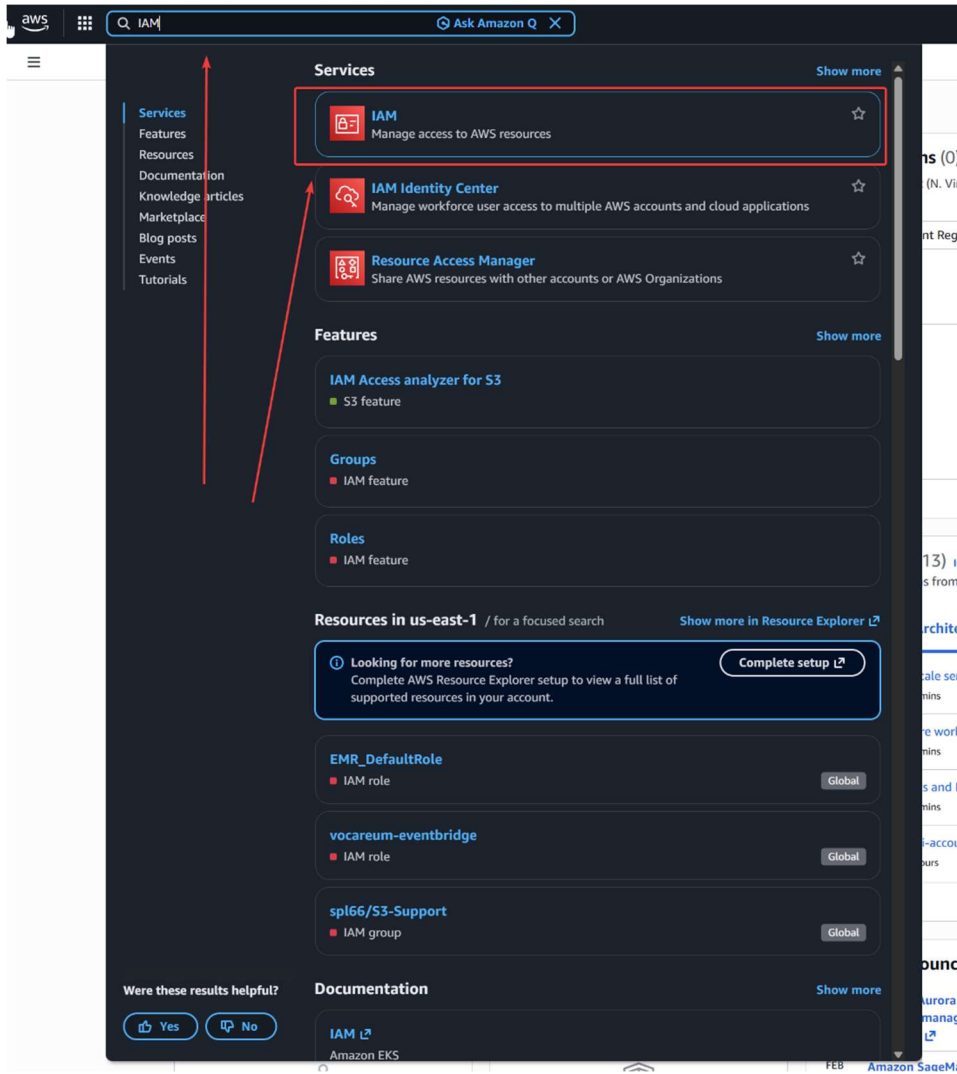
Lab Procedure

Introduction to IAM (Lab 1)

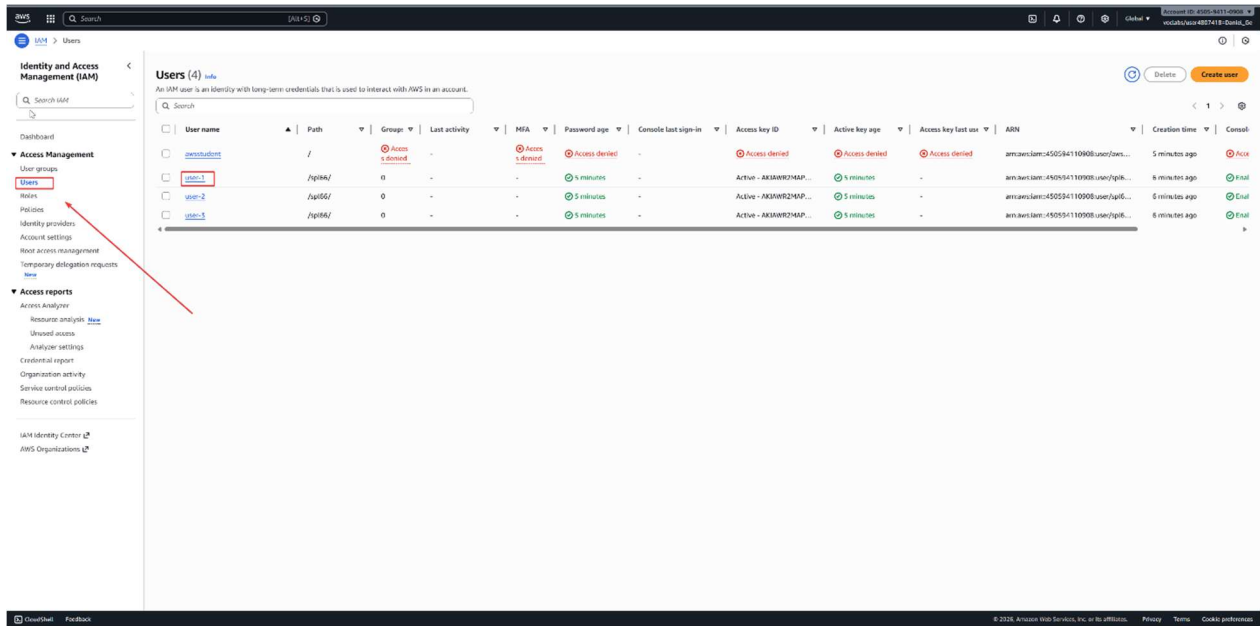
Start the lab and enter the main menu



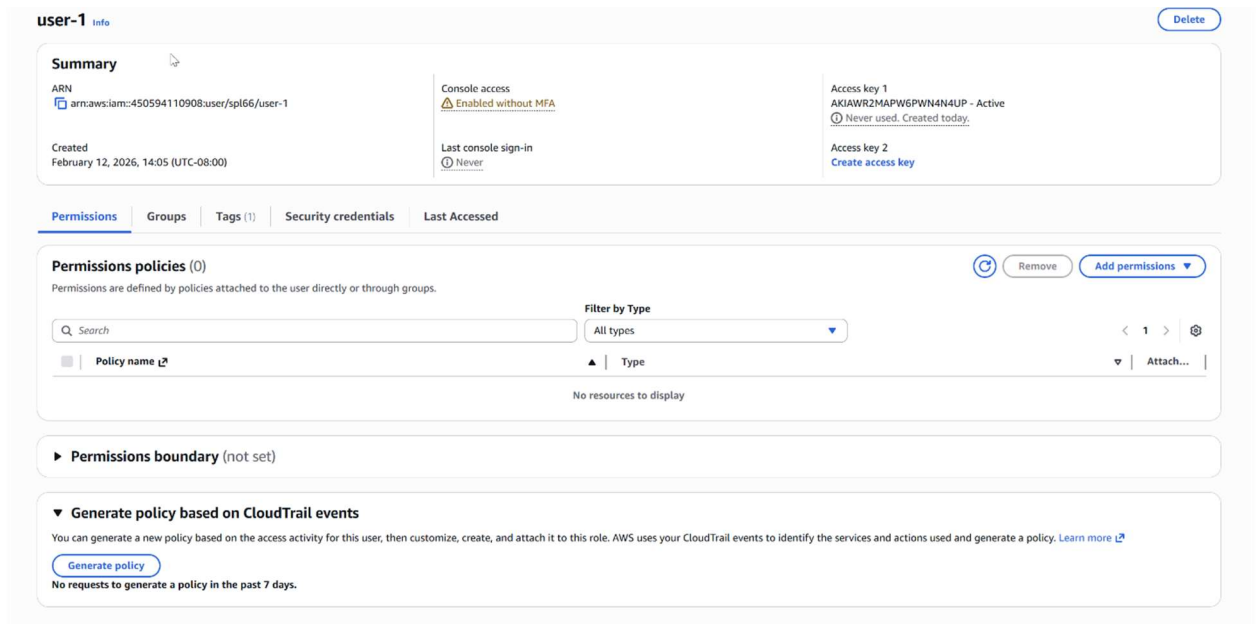
Search “IAM” in the search bar and click the IAM option to open the IAM menu



Click “Users” on the left menu and observe how there are three existing users currently. Click “user-1” the first option



Observe that user-1 does not have any permissions



Click the “Groups” tab to observe that user-1 is not a member of any group

user-1 [Info](#) [Delete](#)

Summary

<p>ARN arn:aws:iam::450594110908:user/spl66/user-1</p> <p>Created February 12, 2026, 14:05 (UTC-08:00)</p>	<p>Console access Enabled without MFA</p> <p>Last console sign-in Never</p>	<p>Access key 1 AKIAWR2MAPW6PWN4N4UP - Active Never used. Created today.</p> <p>Access key 2 Create access key</p>
--	---	--

Permissions | **Groups** | Tags (1) | Security credentials | Last Accessed

User groups membership [Remove](#) [Add user to groups](#)

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users. A user can be a member of up to 10 groups at a time.

Group name	Attached policies
No resources This user does not belong to any groups.	

Click the “Security credentials” tab to observe that user-1 has a console password

user-1 [Info](#) [Delete](#)

Summary

<p>ARN arn:aws:iam::450594110908:user/spl66/user-1</p> <p>Created February 12, 2026, 14:05 (UTC-08:00)</p>	<p>Console access Enabled without MFA</p> <p>Last console sign-in Never</p>	<p>Access key 1 AKIAWR2MAPW6PWN4N4UP - Active Never used. Created today.</p> <p>Access key 2 Create access key</p>
--	---	--

Permissions | Groups | Tags (1) | **Security credentials** | Last Accessed

Console sign-in [Manage console access](#)

<p>Console sign-in link https://450594110908.signin.aws.amazon.com/console</p>	<p>Console password Updated 8 minutes ago (2026-02-12 14:06 PST)</p> <p>Last console sign-in Never</p>
---	--

Multi-factor authentication (MFA) (0) [Remove](#) [Resync](#) [Assign MFA device](#)

Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. [Learn more](#)

Type	Identifier	Certifications	Created on
No MFA devices. Assign an MFA device to improve the security of your AWS environment.			

[Assign MFA device](#)

Access keys (1) [Create access key](#)

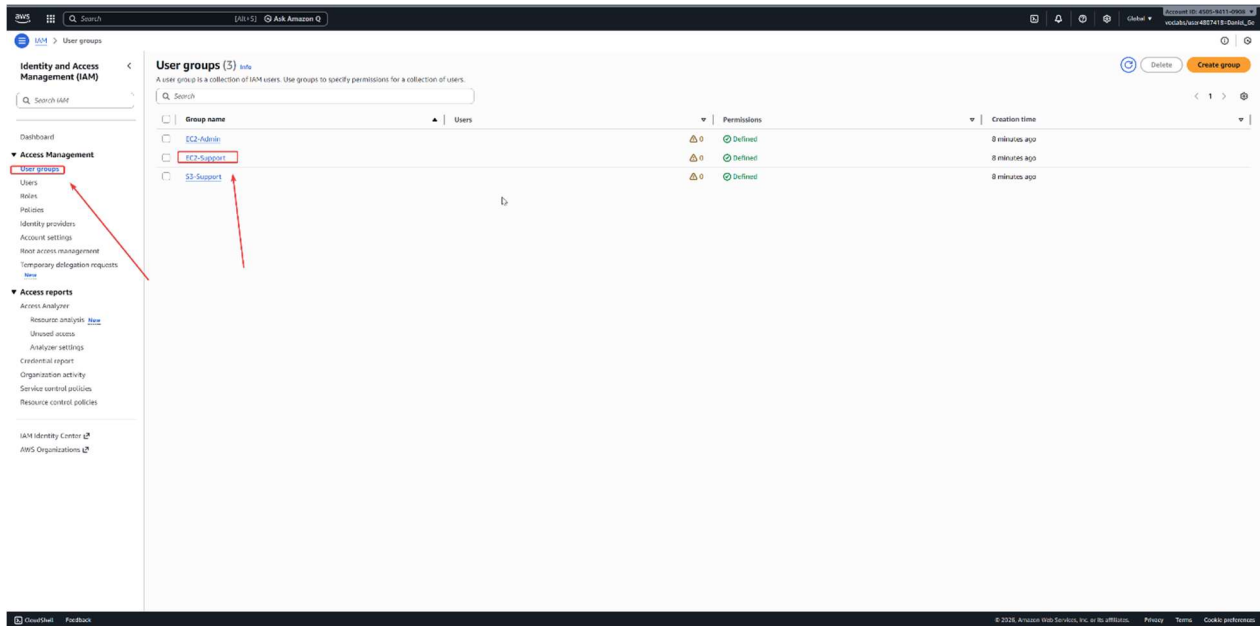
Use access keys to send programmatic calls to AWS from the AWS CLI, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time. [Learn more](#)

Access key ID	Status
AKIAWR2MAPW6PWN4N4UP	Active

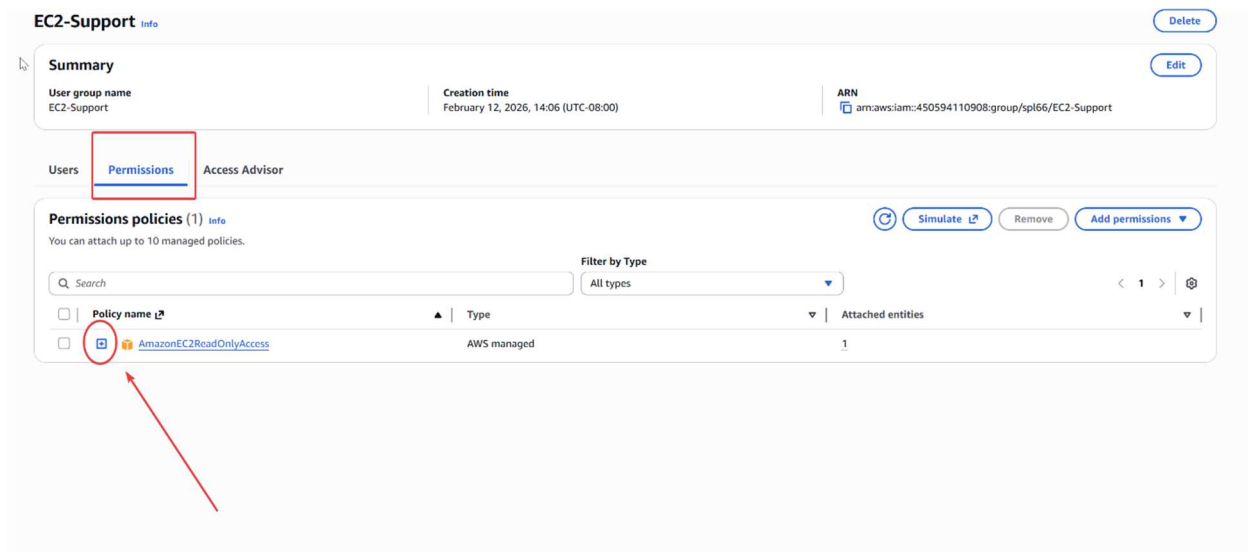
<p>Description -</p> <p>Last used None</p> <p>Last used region N/A</p>	<p>Created 8 minutes ago</p> <p>Last used service N/A</p>
--	---

[Actions](#)

Click the User Groups option on the left menu to find the three pre-made groups



Click EC2-Support group, then the tab Permissions. Click the blue plus next to “AmazonEC2ReadOnlyAccess”



The AmazonEC2ReadOnlyAccess policy has been configured with multiple Allow and Deny statements which allow the user to read EC2 information, but denies them the ability to affect the operation

EC2-Support Info Delete

Summary Edit

User group name EC2-Support	Creation time February 12, 2026, 14:06 (UTC-08:00)	ARN arn:aws:iam:450594110908:group/spl66/EC2-Support
---------------------------------------	--	--

Users **Permissions** Access Advisor

Permissions policies (1) Info Simulate Remove Add permissions

You can attach up to 10 managed policies.

Filter by Type: All types

Policy name	Type	Attached entities
<input checked="" type="checkbox"/> AmazonEC2ReadOnlyAccess	AWS managed	1

AmazonEC2ReadOnlyAccess Copy JSON

```

1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": [
7         "ec2:Describe*",
8         "ec2:GetSecurityGroupsForVpc"
9       ],
10      "Resource": "*"
11    },
12    {
13      "Effect": "Allow",
14      "Action": "elasticloadbalancing:Describe*",
15      "Resource": "*"
16    },
17    {
18      "Effect": "Allow",
19      "Action": [
20        "cloudwatch:ListMetrics",

```

Return to the User Groups tab, and now click S3-Support

The screenshot shows the AWS IAM console interface. On the left sidebar, under 'Access Management', the 'User groups' link is highlighted with a red box. The main content area displays a table of user groups:

Group name	Users	Permissions	Creation time
<input type="checkbox"/> EC2-Admin		✔ Defined	10 minutes ago
<input type="checkbox"/> EC2-Support		✔ Defined	10 minutes ago
<input checked="" type="checkbox"/> S3-Support		✔ Defined	10 minutes ago

Click Permissions then the blue square to expand and view the configuration for “AmazonS3ReadOnlyAccess”

Users **Permissions** Access Advisor

Permissions policies (1) info Simulate Remove Add permissions

You can attach up to 10 managed policies.

Search Filter by Type All types

Policy name	Type	Attached entities
AmazonS3ReadOnlyAccess	AWS managed	1

AmazonS3ReadOnlyAccess Copy JSON

```

1- {
2-   "Version": "2012-10-17",
3-   "Statement": [
4-     {
5-       "Effect": "Allow",
6-       "Action": [
7-         "s3:Get*",
8-         "s3:List*",
9-         "s3:Describe*",
10-        "s3-object-lambda:Get*",
11-        "s3-object-lambda:List*"
12-       ],
13-       "Resource": "*"
14-     }
15-   ]
16- }

```

Return to the User Groups tab, and now click EC2-Admin

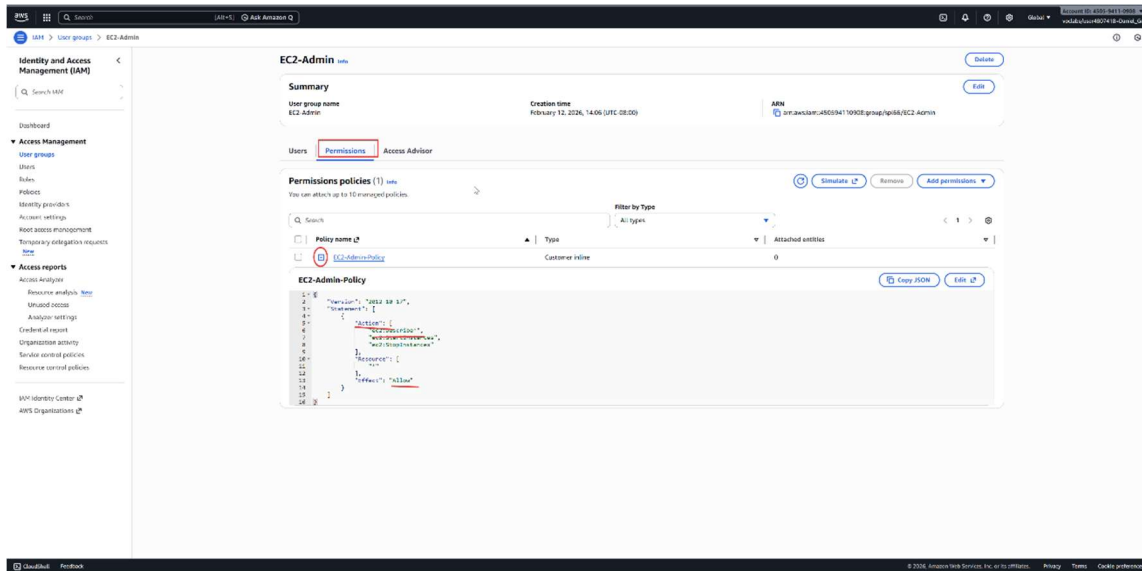
User groups (3) info Delete Create group

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

Search

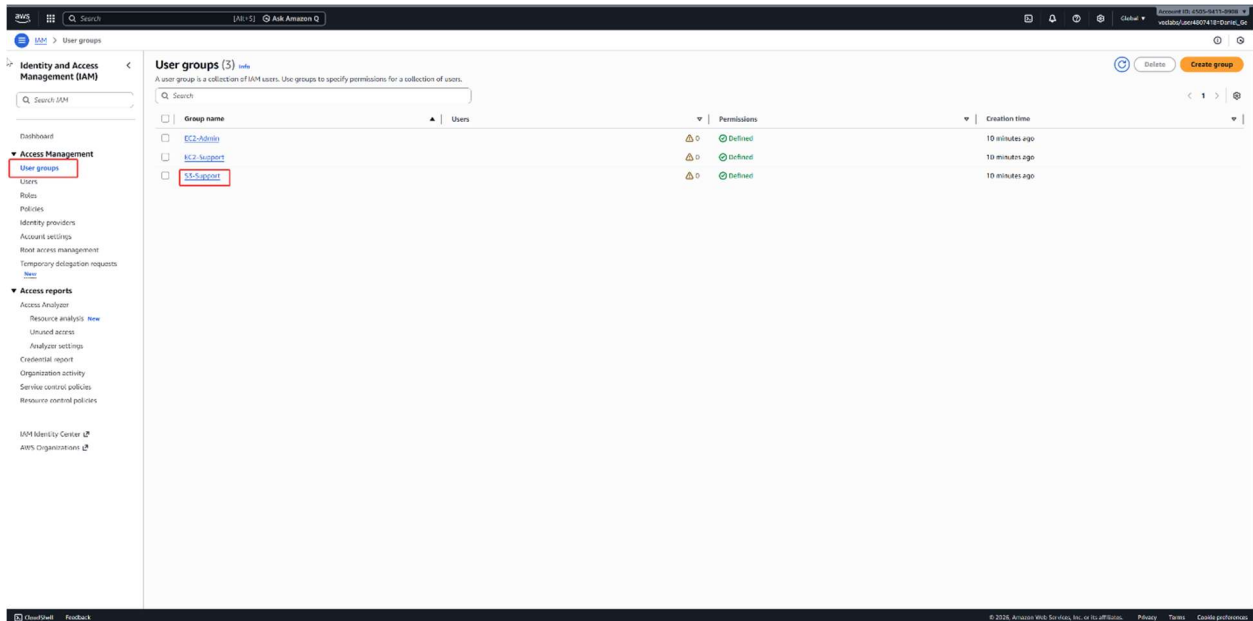
Group name	Permissions	Creation time
EC2-Admin	Defined	12 minutes ago
EC2-Support	Defined	12 minutes ago
S3-Support	Defined	12 minutes ago

Click Permissions then the blue square to expand and view the configuration for “EC2-Admin-Policy”. This group is configured with an Inline Policy which allows the user to stop and start the EC2 instances.

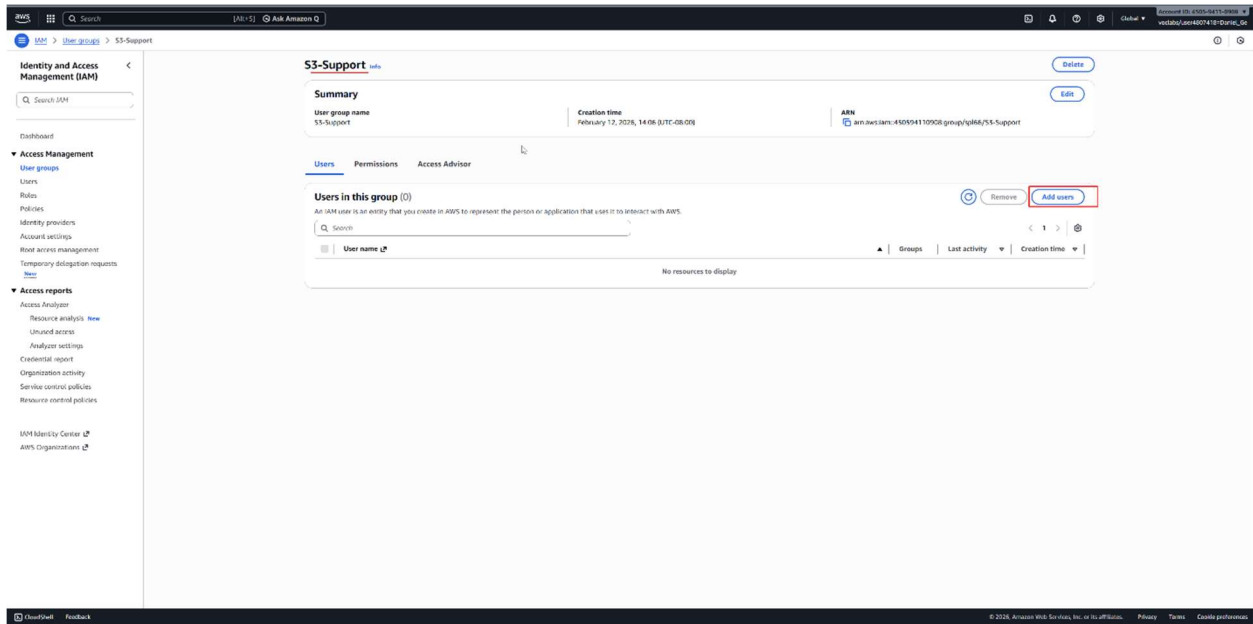


Configuring User Permissions through IAM (Lab 1 continued)

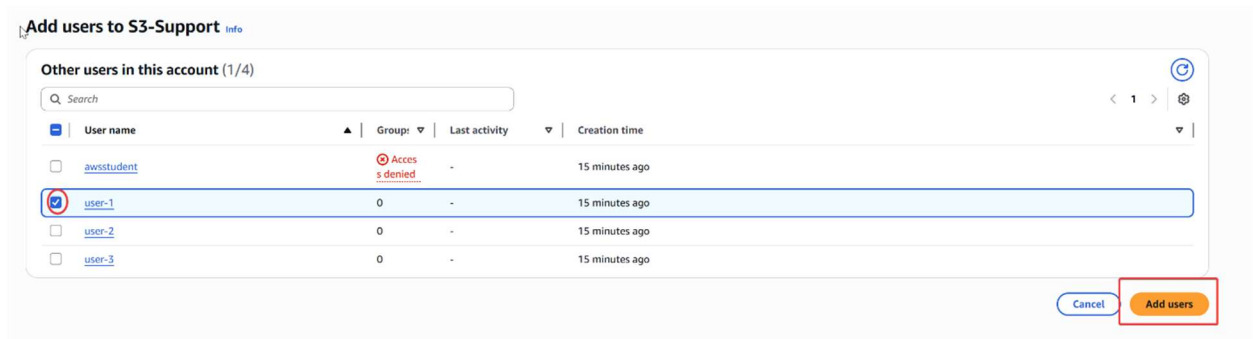
Click “User Groups” on the left menu to return to S3-Support group menu



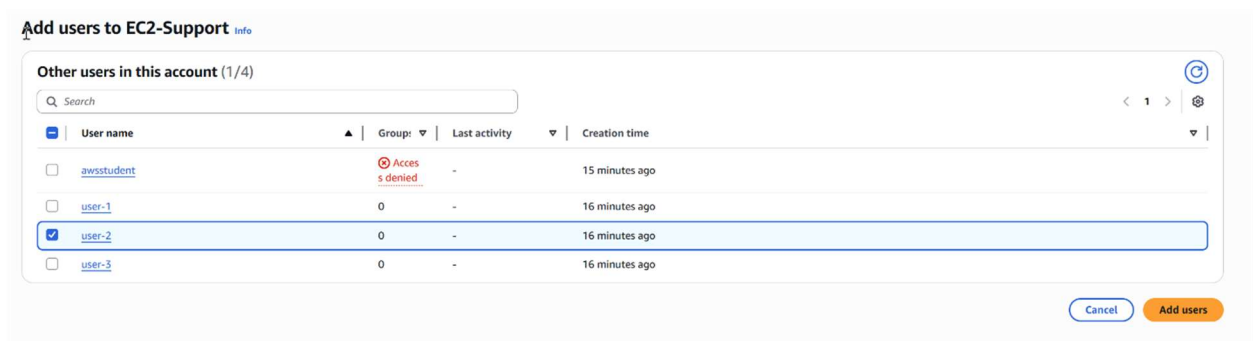
Click “Add users”



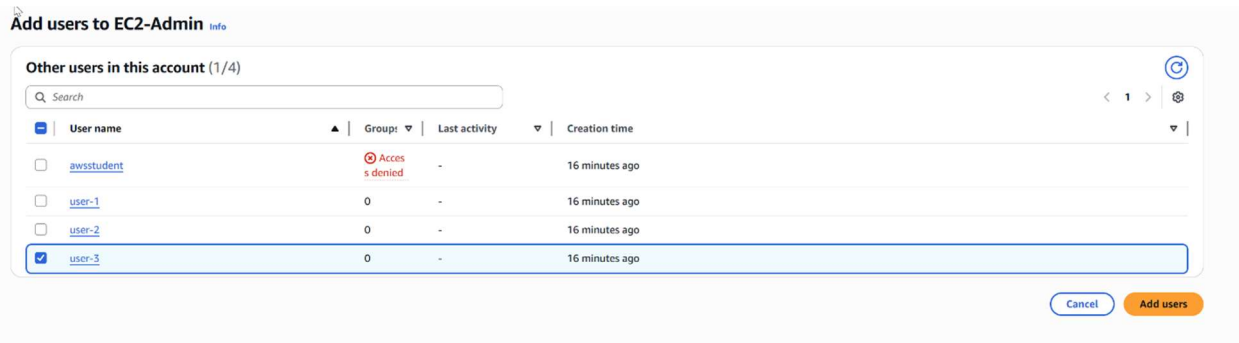
Check the box next to “user-1”, then click the orange “Add users” button to add user-1 to S3-Support



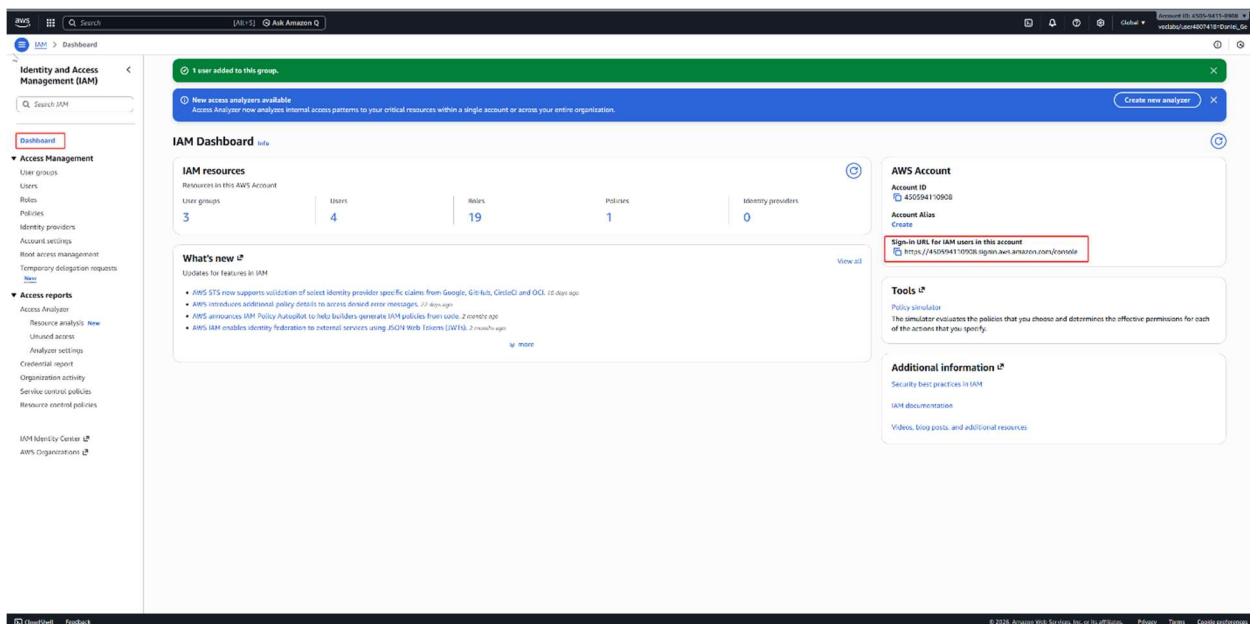
Follow the analogous steps to add “user-2” to EC2-Support



Follow the analogous steps to add “user-3” to EC2-Admin

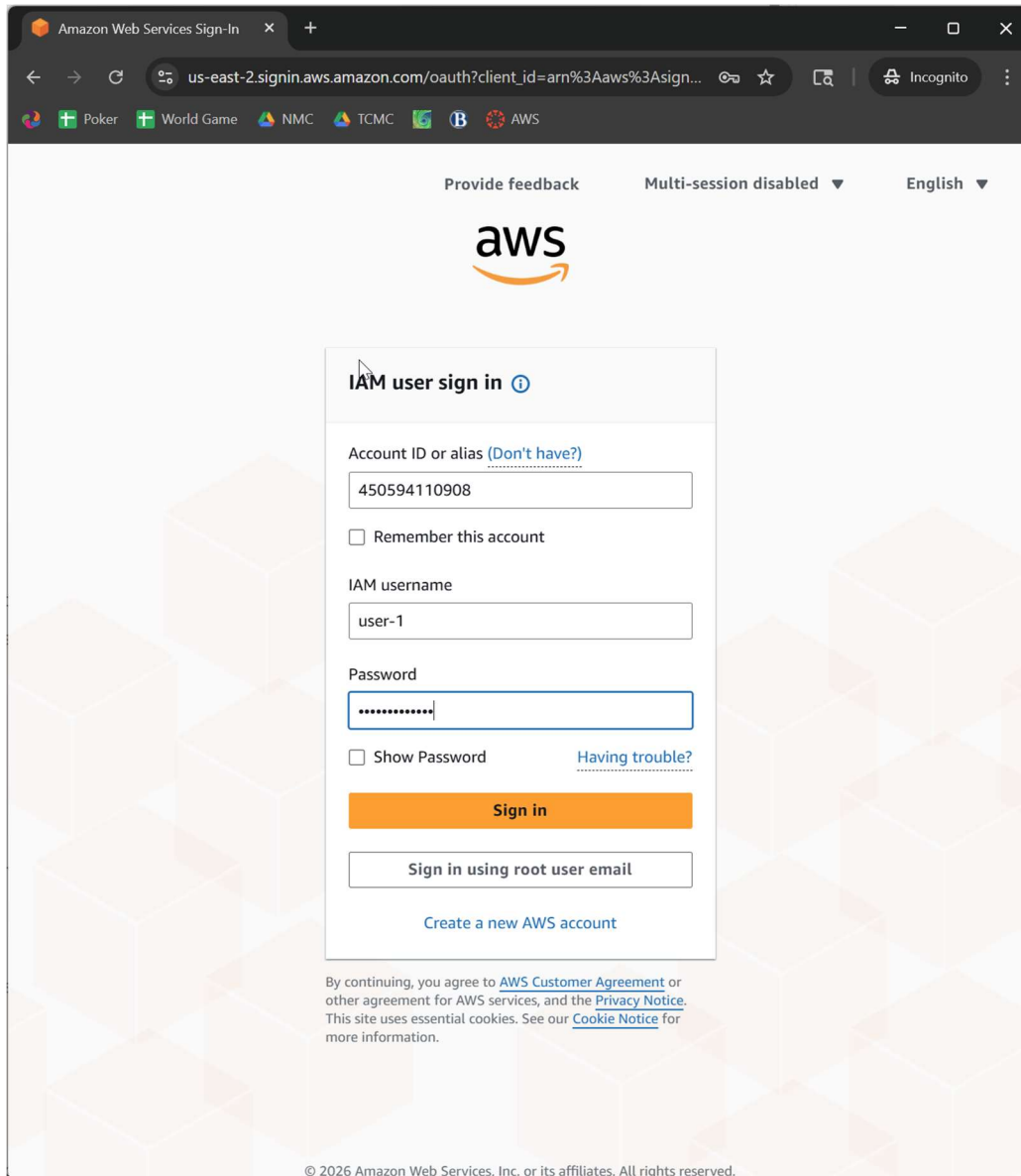


Click “Dashboard” on the left menu, then find the Sign-in URL for IAM users under AWS Account

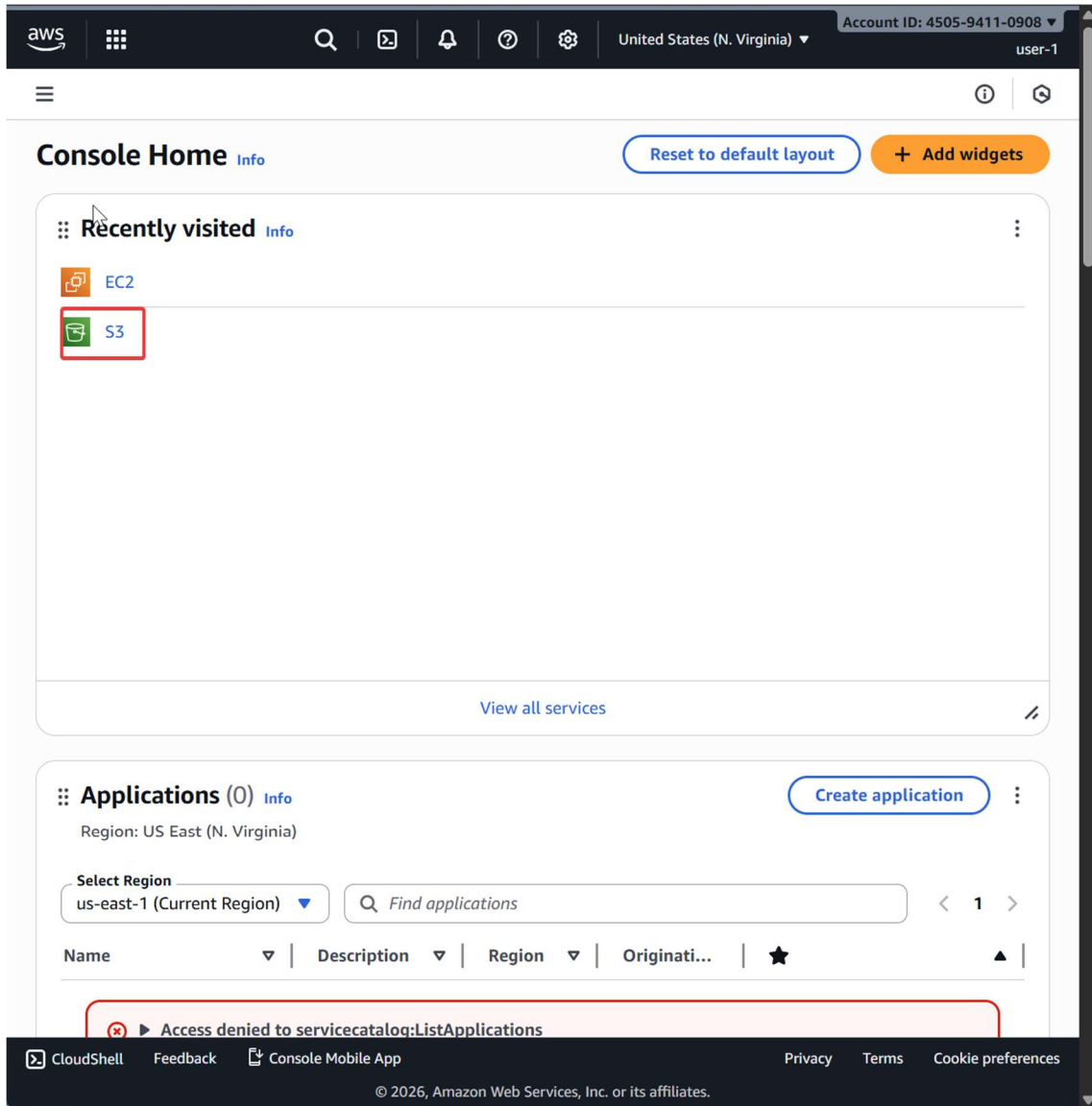


Open an Incognito tab using Ctrl+Shift+N, then paste the above sign-in URL into the search bar. Sign in through user-1’s credentials

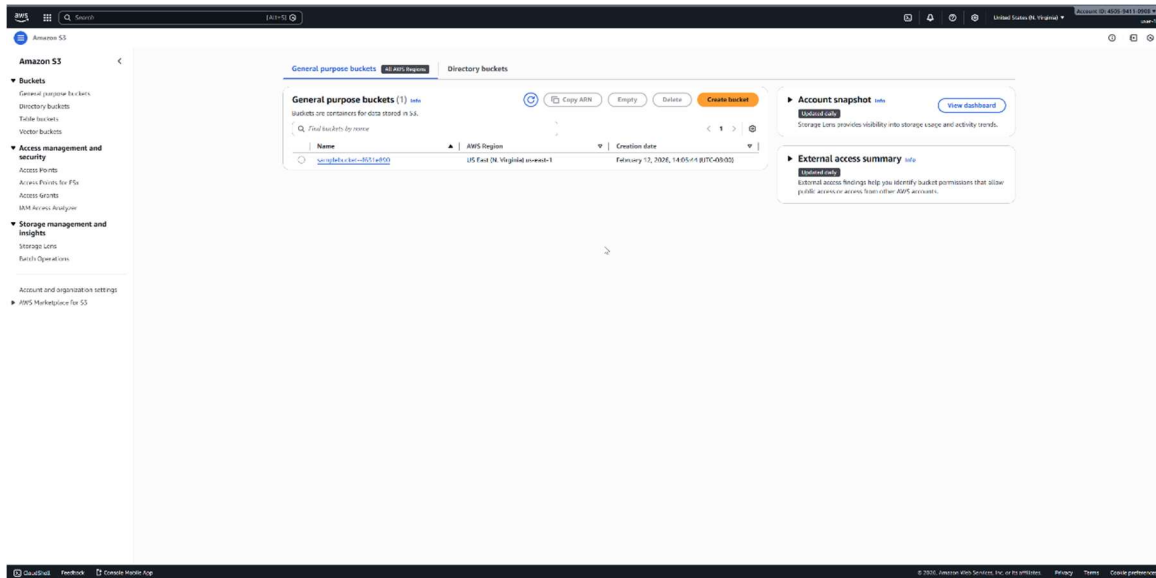
- Username: user-1
- Password: Lab-Password1



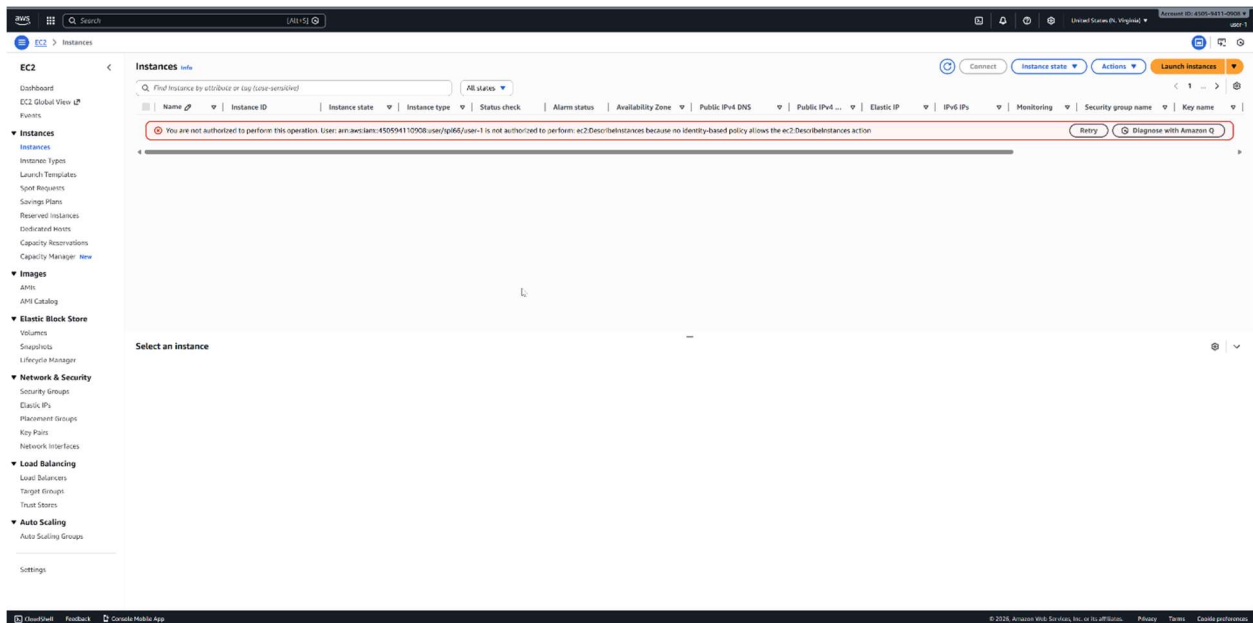
Once signed in, click S3 to enter the Simple Storage System console



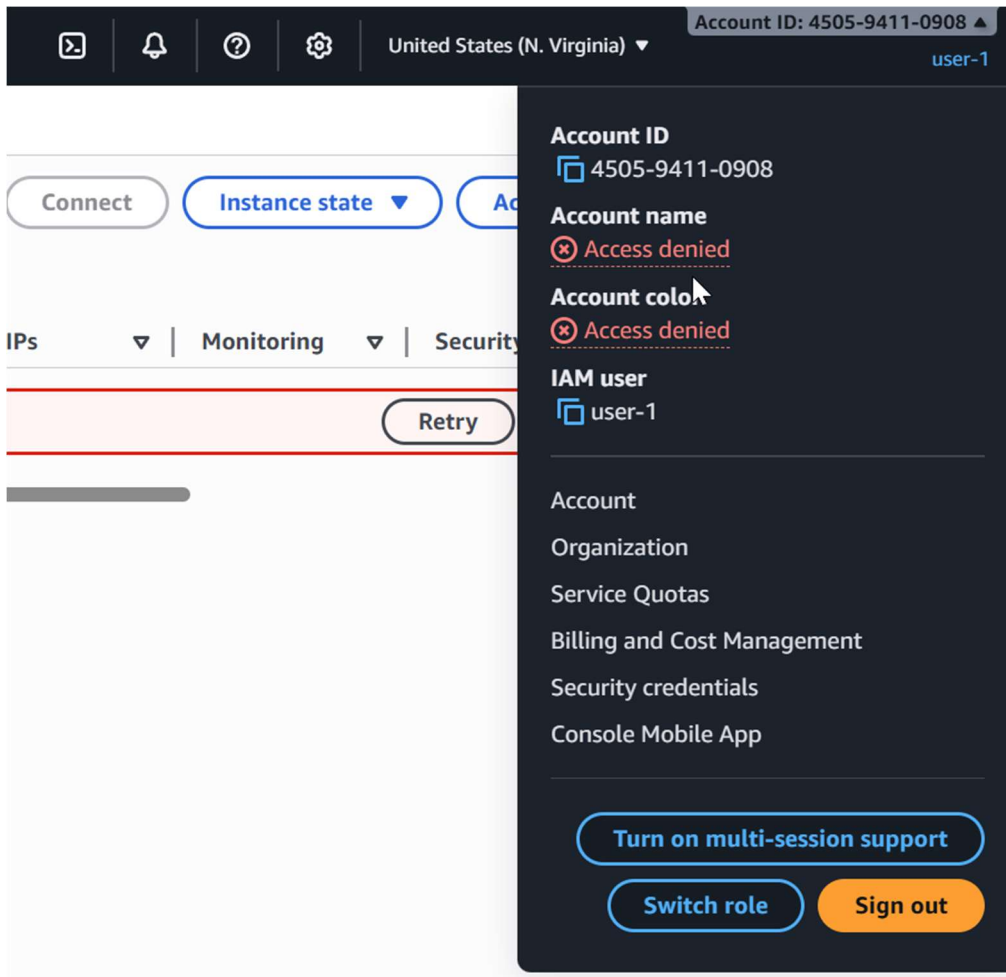
Since User-1 has been configured with the permissions to view S3 configurations, observe that they can see the Amazon S3 buckets associated with the company account



Navigate to EC2 through Services, and observe that User-1 cannot see the EC2 instances since they do not have permissions to do so



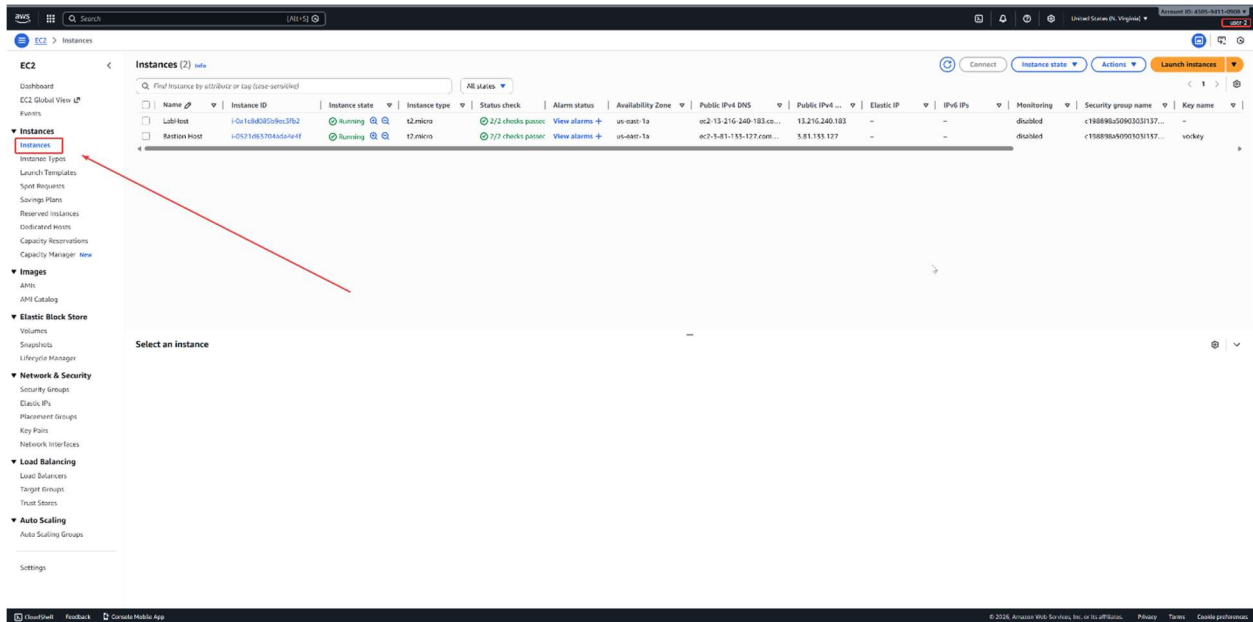
Click “user-1” on the top-right and “sign out”



Follow the same steps to sign in with User-2

- Username: user-2
- Password: Lab-Password2

Enter the EC2 console, then click “Instances” on the left menu.

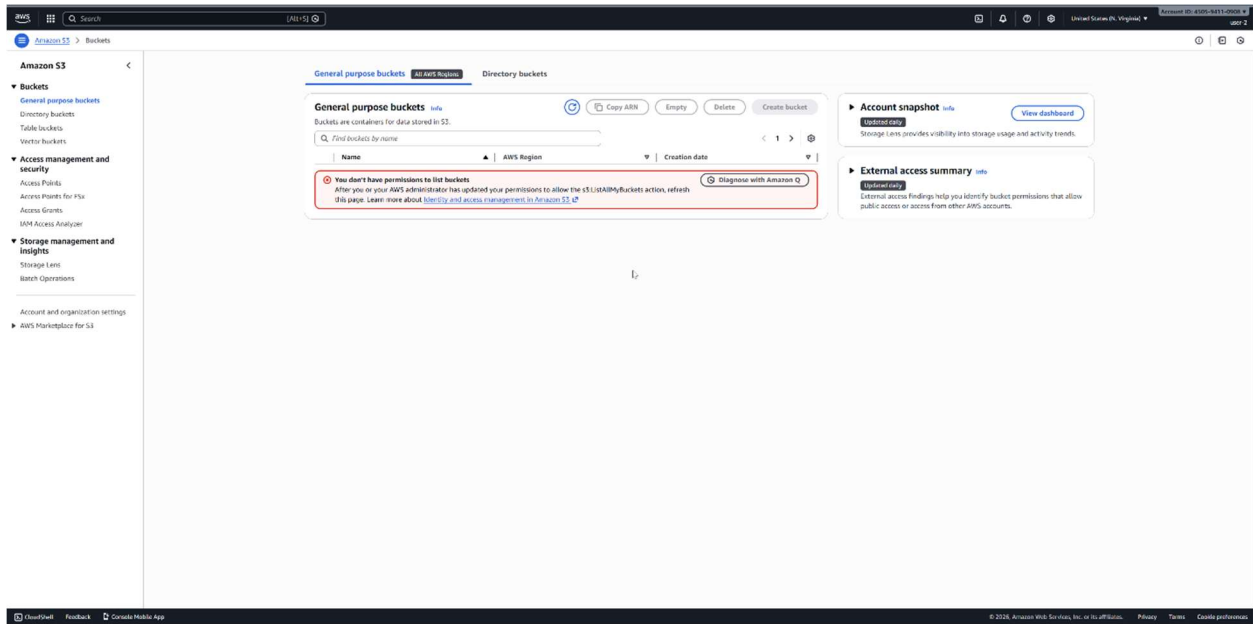


Click Instance-state in the top-right, then “Stop instance”



Observe the failure message. Although user-2 does have permissions to view EC2 instances, they do not have permissions to stop or start those instances

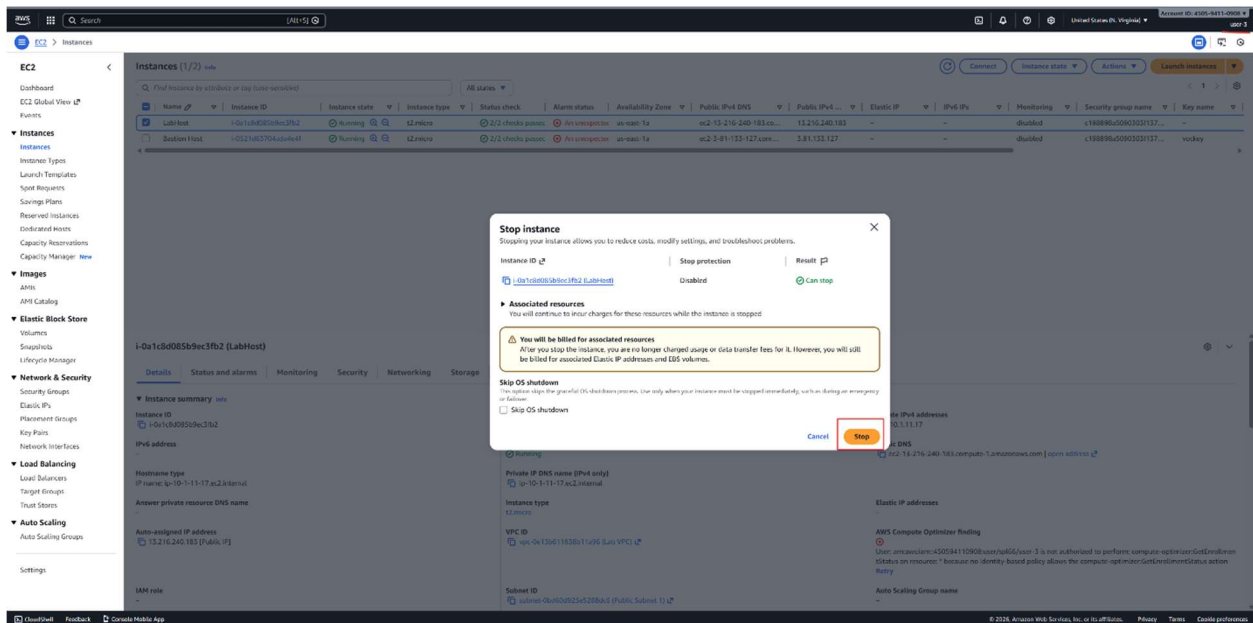




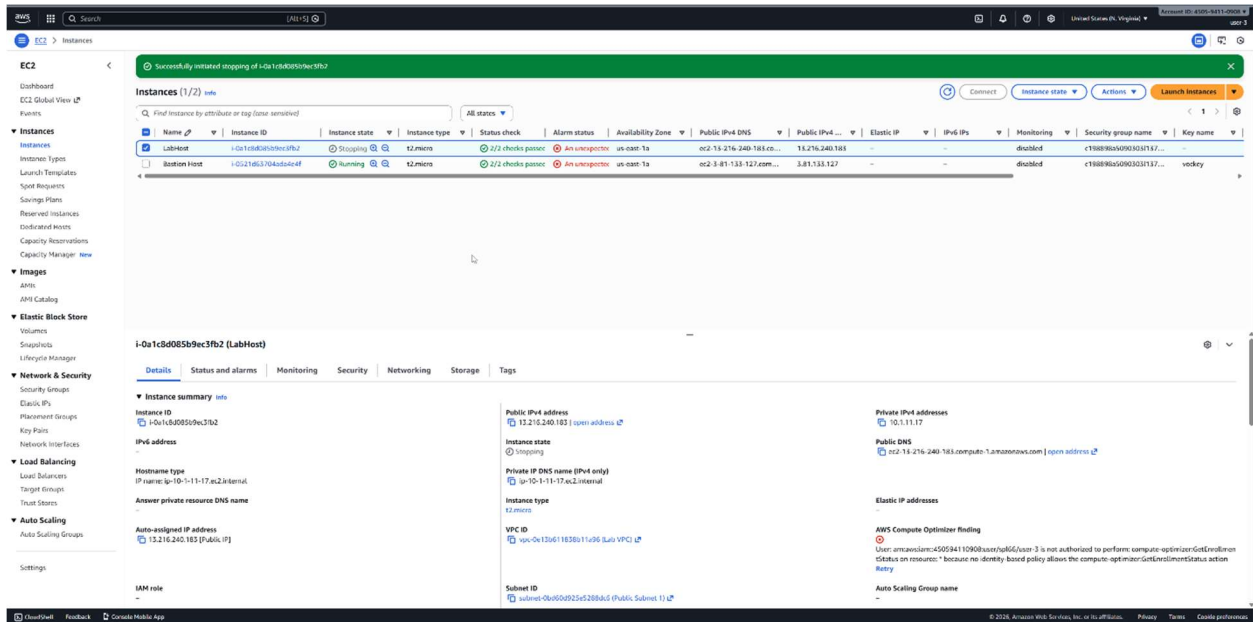
Sign out and log in to User-3's account

- Username: User-3
- Password: Lab-Password3

Follow the same steps as before to attempt to stop the instance

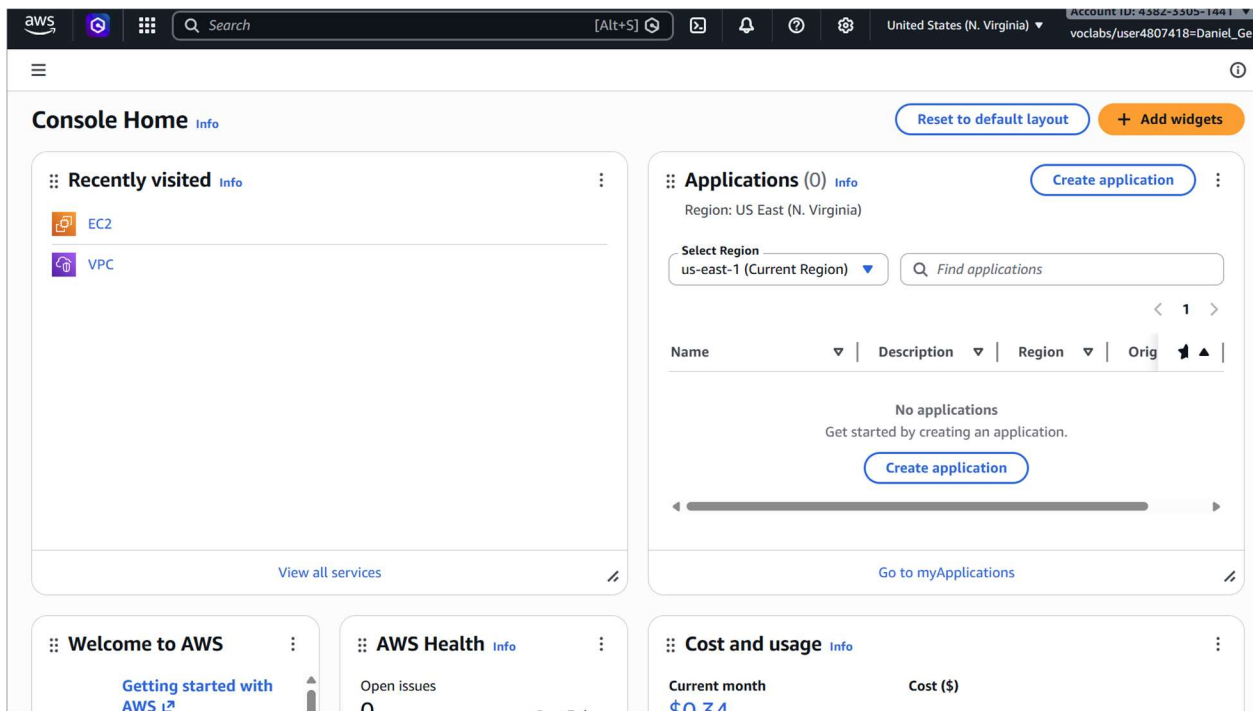


This time, the stop should be successful, since User-3 has been configured with permissions to stop the EC2 instance

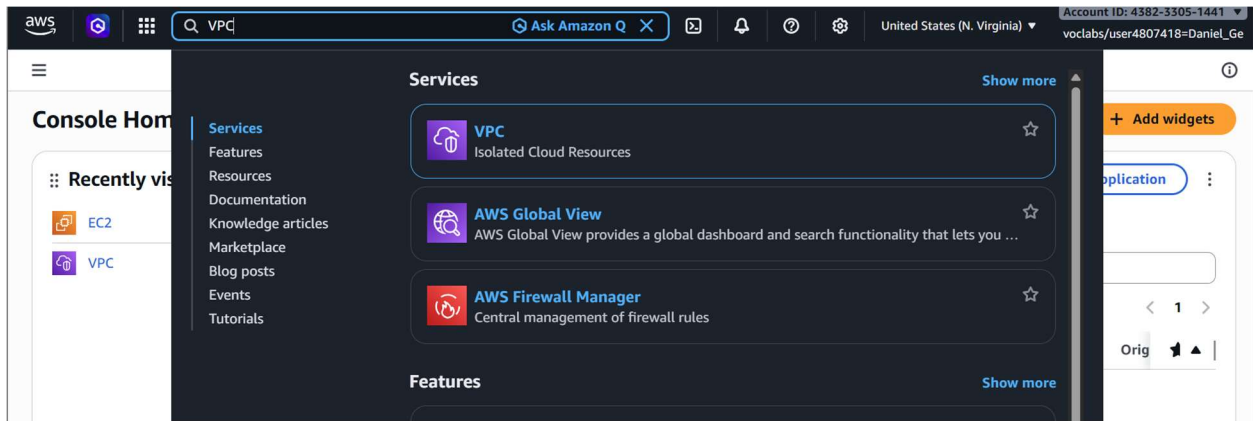


Building a Virtual Private Cloud and Launching a Web Server (Lab 2)

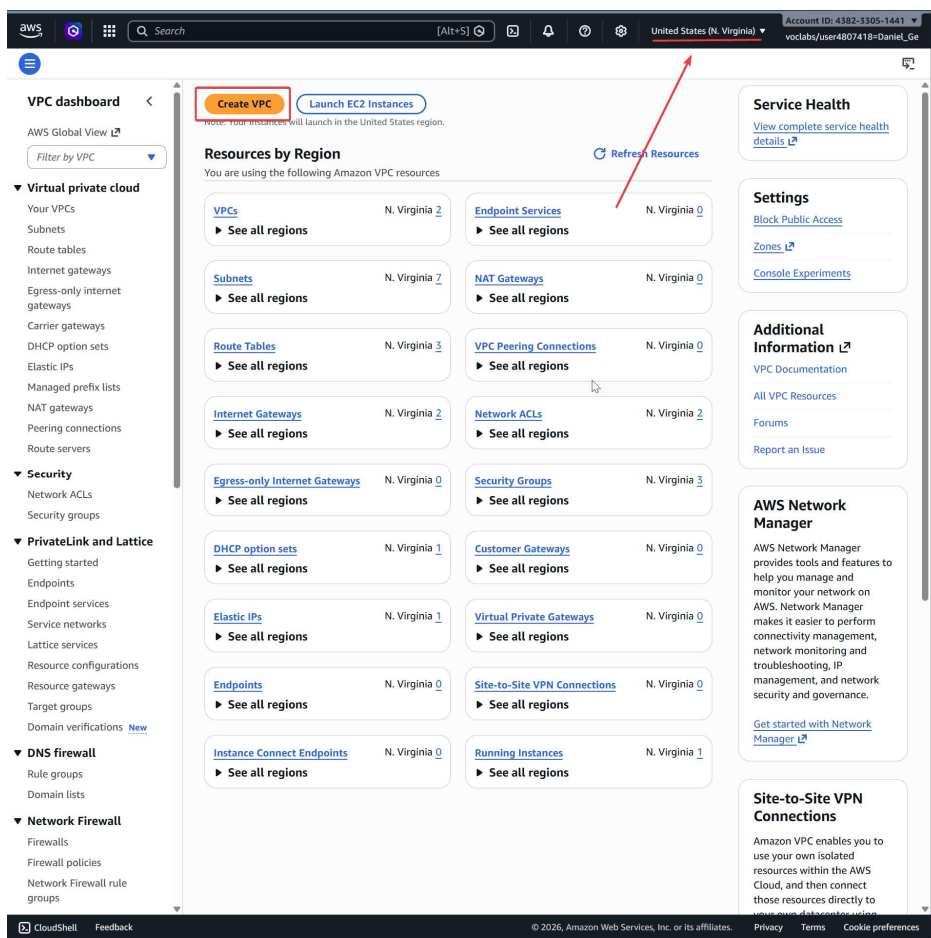
Start the lab and enter the main menu



Search “VPC” in the search bar and click the VPC option to open the VPC menu



Read the top right to verify that the server is N. Virginia, then click “Create VPC”



Under VPC Settings, change the Name tag to “lab” and Number of Availability Zones 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

► **Encryption settings - optional**

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

Edit the Public and Private subnet CIDRs as follows, change NAT gateways to Zonal, and set VPC endpoints to None. After verifying the configuration, click “Create VPC”

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

▼ **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

NAT gateways (\$) - updated [Info](#)

NAT gateway allows private resources to access the internet from any availability zone within a VPC, providing a single managed internet exit point for the entire region. Additional charges apply.

None | Regional - new | Zonal

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

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

Wait for everything to activate and complete

Create VPC workflow

↶ Wait for NAT Gateways to activate 72%

▼ Details

- ✔ Create VPC: [vpc-0d0f2116588df031a](#)
- ✔ Enable DNS hostnames
- ✔ Enable DNS resolution
- ✔ Verifying VPC creation: [vpc-0d0f2116588df031a](#)
- ✔ Create subnet: [subnet-03d6a295787746faa](#)
- ✔ Create subnet: [subnet-0369cbac0afd5becc](#)
- ✔ Create internet gateway: [igw-073a31aaa23f64515](#)
- ✔ Attach internet gateway to the VPC
- ✔ Create route table: [rtb-0167035c2580d802a](#)
- ✔ Create route
- ✔ Associate route table
- ✔ Allocate elastic IP: [eipalloc-023b39c2d9bc7f9a2](#)
- ✔ Create NAT gateway: [nat-0d585dd26b62ccdad](#)
- ⌚ Wait for NAT Gateways to activate
- ⌚ Create route table
- ⌚ Create route
- ⌚ Associate route table
- ⌚ Verifying route table creation

Click “View VPC”. The VPC contains all the addresses in the network 10.0.0.0/16. We have further configured the Lab subnets 10.0.0.0/24 and 10.0.1.0/24

vpc-0d0f2116588df031a / lab-vpc Actions ▼

Details Info

VPC ID vpc-0d0f2116588df031a	State Available	Block Public Access Off	DNS hostnames Enabled
DNS resolution Enabled	Tenancy default	DHCP option set dopt-011e576a6ea437fd5	Main route table rtb-09bf08fe3ecb3cb2d
Main network ACL acl-0fd15d2e0f9a98ebf	Default VPC No	IPv4 CIDR 10.0.0.0/16	IPv6 pool -
IPv6 CIDR (Network border group) -	Network Address Usage metrics Disabled	Route 53 Resolver DNS Firewall rule groups -	Owner ID 438233051441
Encryption control ID -	Encryption control mode -		

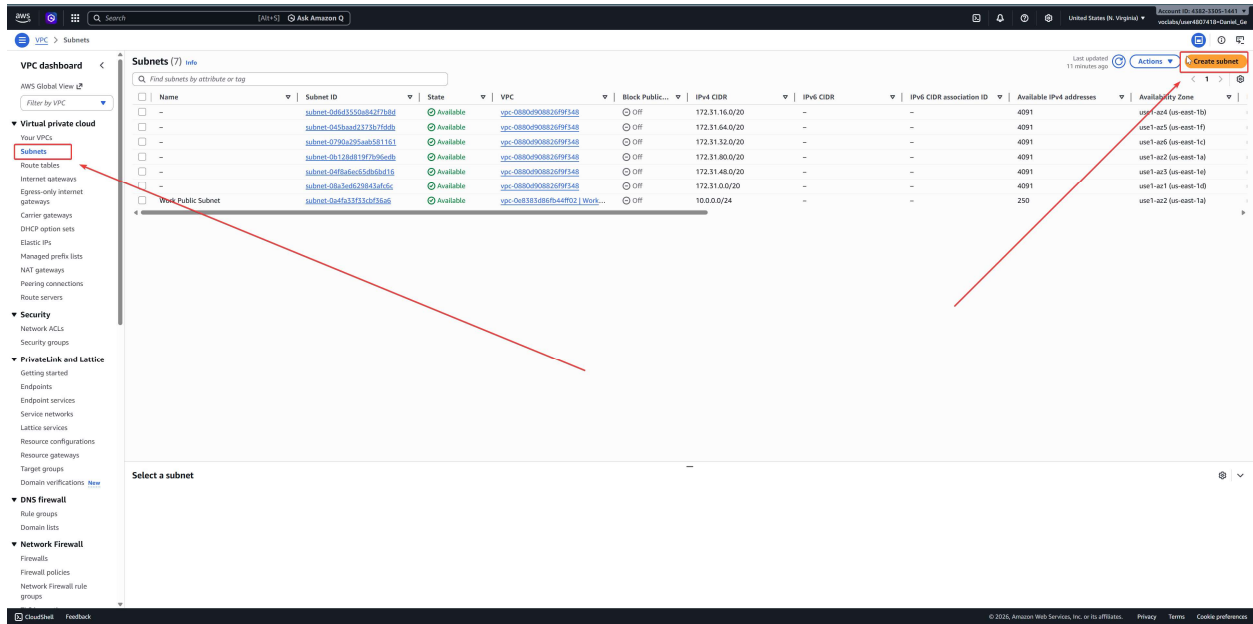
[Resource map](#) | [CIDRs](#) | [Flow logs](#) | [Tags](#) | [Integrations](#)

Resource map Info Show all details

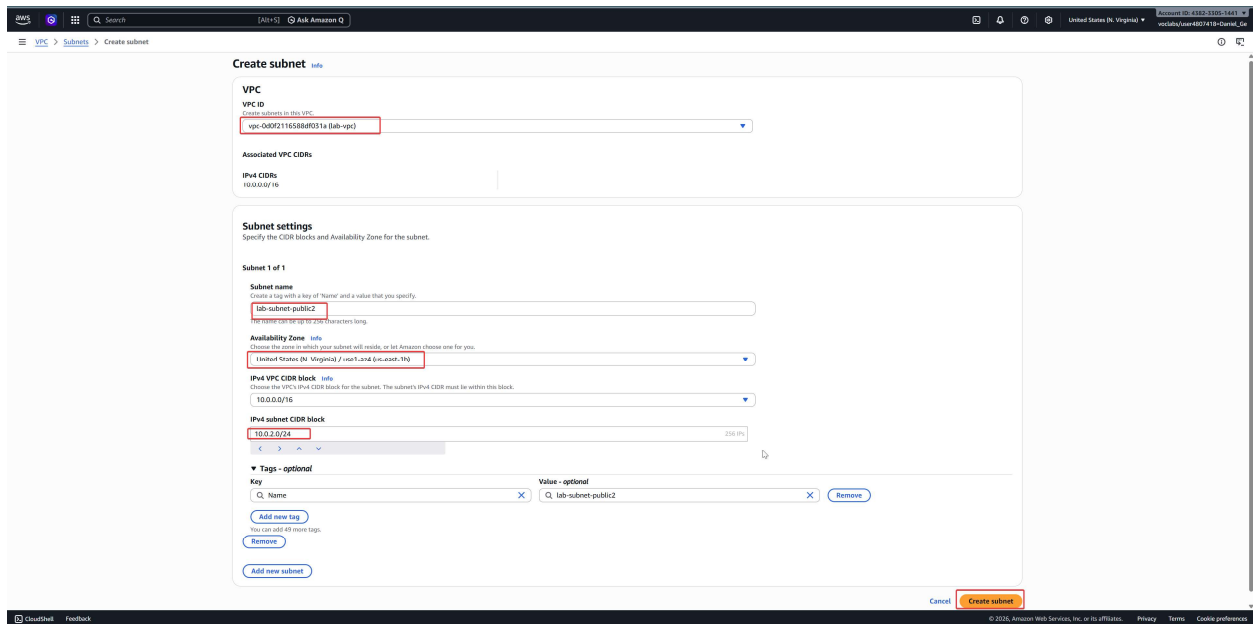
The resource map shows the following components and their connections:

- VPC** (lab-vpc) is connected to **Subnets (2)**.
- Subnets (2)** (lab-subnet-public1-us-east-1 and lab-subnet-private1-us-east-1) are connected to **Route tables (3)** (rtb-09bf08fe3ecb3cb2d, lab-rtb-public, and lab-rtb-private1-us-east-1).
- Route tables (3)** are connected to **Network Connections (2)** (lab-igw and lab-nat-public1-us-east-1).

Click “Subnets” and “Create Subnets” to create more subnets



Set the VPC ID to “lab-vpc”, the Subnet name, and the IPv4 subnet CIDR block as follows:



Create the corresponding private subnet using the following configurations

Create subnet Info

VPC

VPC ID
Create subnets in this VPC.

vpc-0d0f2116588df031a (lab-vpc)

Associated VPC CIDRs

IPv4 CIDRs
10.0.0.0/16

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-private2
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.

United States (N. Virginia) / us-east-1a (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
10.0.3.0/24 256 IPs

Tags - optional

Key	Value - optional
Name	lab-subnet-private2

[Add new tag](#)
You can add 49 more tags.

[Remove](#)

[Add new subnet](#)

[Cancel](#) [Create subnet](#)

To begin configuring the routes, click “Route Table” on the left menu, and select the lab-rtb-private1-us-east-1a route table

Route tables (1/6)

Name	Route table ID	Explicit subnet associ...	Edge associations	Main	VPC	Owner ID
lab-rtb-public	rtb-0767031c3450d802a	subnet-03d6a2957977d5...	-	No	vpc-0d0f2116588df031a lab-y...	438233051441
lab-rtb-private1-us-east-1a	rtb-076c327ce33da1690	subnet-0369b2af5bacc / lab-subnet-private1-us-east-1a	-	Yes	vpc-0d0f2116588df031a lab-y...	438233051441

rtb-076c327ce33da1690 / lab-rtb-private1-us-east-1a

Details

Route table ID rtb-076c327ce33da1690	Main No	Explicit subnet associations subnet-0369b2af5bacc / lab-subnet-private1-us-east-1a
VPC vpc-0d0f2116588df031a lab-vpc	Owner ID 438233051441	Edge associations -

Click “Routes” on the bottom menu, and observe how traffic to the internet (0.0.0.0/0) is sent through the nat gateway

rtb-07c6327ce33da1690 / lab-rtb-private1-us-east-1a

Details Routes Subnet associations Edge associations Route propagation Tags

Routes (2)

Destination	Target	Status	Propagated	Route Origin
0.0.0.0/0	nat-0d585d42b642ccdbab	Active	No	Create Route
10.0.0.0/16	local	Active	No	Create Route Table

Click “Subnet associations”, then “Edit subnet associations” under Explicit subnet associations

rtb-07c6327ce33da1690 / lab-rtb-private1-us-east-1a

Details Routes Subnet associations Edge associations Route propagation Tags

Explicit subnet associations (1)

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
lab-subnet-private1-us-east-1a	subnet-0369cbac0afd5becc	10.0.1.0/24	-

Subnets without explicit associations (2)

The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
lab-subnet-private2	subnet-069ac7d5f29593e9e	10.0.3.0/24	-

Select both lab-subnet-private1-us-east-1a and lab-subnet-private2, then “Save Associations” such that both subnets receive this Route Table

Edit subnet associations
Change which subnets are associated with this route table.

Available subnets (2/4)

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
<input checked="" type="checkbox"/> lab-subnet-private2	subnet-069ac7d5f29593e9e	10.0.3.0/24	-
<input checked="" type="checkbox"/> lab-subnet-private1-us-east-1a	subnet-0369cbac0afd5becc	10.0.1.0/24	-
<input type="checkbox"/> lab-subnet-public1-us-east-1a	subnet-03d6a295787746faa	10.0.0.0/24	-
<input type="checkbox"/> lab-subnet-public2	subnet-08c269c9e3e32b01c	10.0.2.0/24	-

Selected subnets

subnet-0369cbac0afd5becc / lab-subnet-private1-us-east-1a subnet-069ac7d5f29593e9e / lab-subnet-private2

Cancel **Save associations**

Return to the Route Table and select lab-rtb-public, then the “Routes” tab. Observe that for the public subnet, traffic to the internet have a direct route through the IGW (internet gateway)

Route tables (1/6)

Name	Route table ID	Explicit subnet associ...	Edge associations	Main	VPC	Owner ID
lab-rtb-public	rtb-0167035c2580d802a	subnet-03d6a295787746...	-	No	vpc-0a0f2116588d031a lab-v...	438233051441

rtb-0167035c2580d802a / lab-rtb-public

Details Routes Subnet associations Edge associations Route propagation Tags

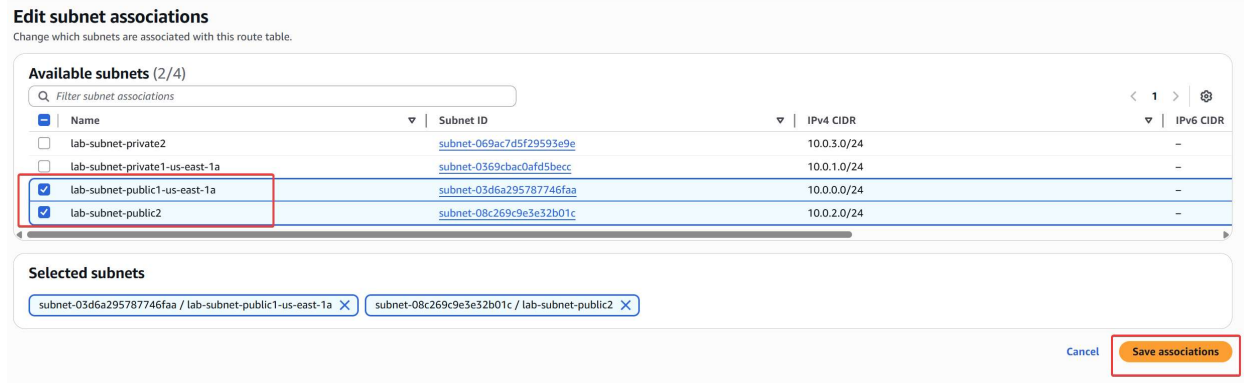
Routes (2)

Destination	Target	Status	Propagated	Route Origin
0.0.0.0/0	igw-073a31aa23f64515	Active	No	Create Route
10.0.0.0/16	local	Active	No	Create Route Table

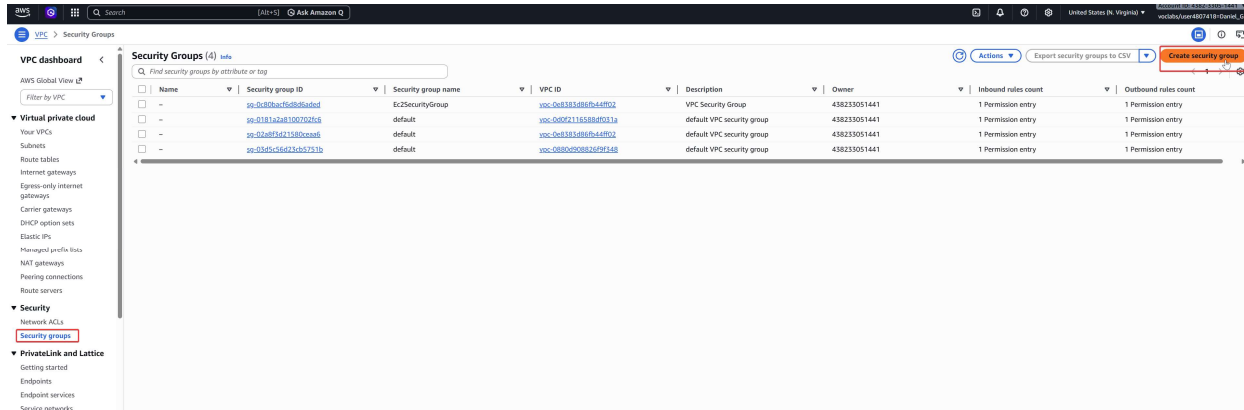
Click “Subnet associations”, then “Edit subnet associations” under Explicit subnet associations



Select both public subnets, then “Save Associations”



Click “Security Groups” on the left menu, then “Create Security Group”



Configure the name, description and VPC of the group as follows:

Create security group Info

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name Info

Name cannot be edited after creation.

Description Info

VPC Info

Click “Add rule” under Inbound rules to add an inbound rule. Set the Type to HTTP, configure Source as “Anywhere IPv4”, and configure the description

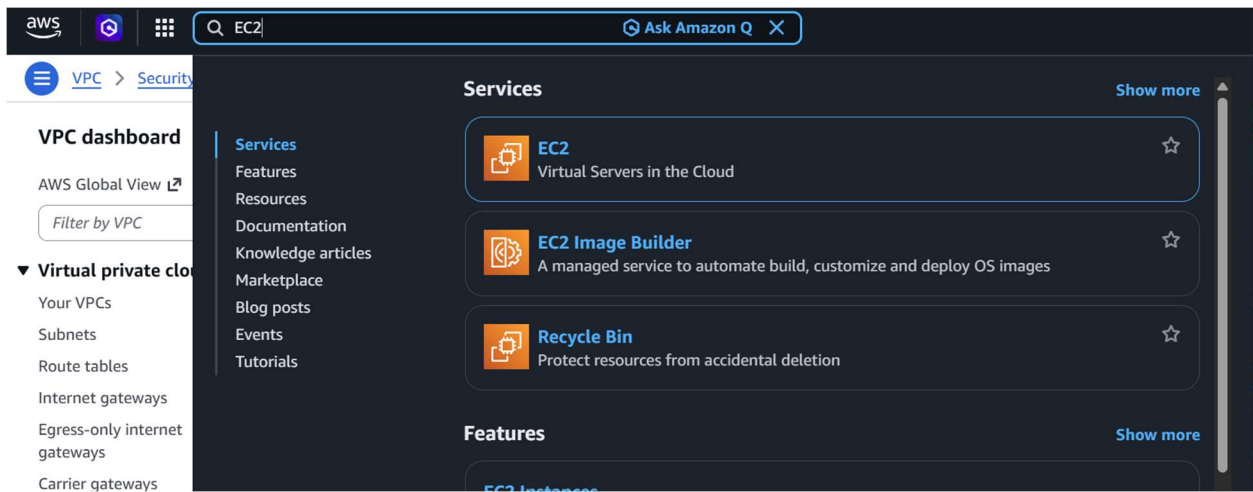
Inbound rules Info

Type Info Protocol Info Port range Info Source Info Description - optional Info

HTTP TCP 80 Anywh... 0.0.0.0/0

Click Create Security Group

Search EC2 in the top search bar and open the EC2 console



Click "Launch Instance"

EC2

- Dashboard
- AWS Global View
- Events
- ▼ **Instances**
 - Instances
 - Instance Types
 - Launch Templates
 - Spot Requests
 - Savings Plans
 - Reserved Instances
 - Dedicated Hosts
 - Capacity Reservations
 - Capacity Manager
- ▼ **Images**
 - AMIs
 - AMI Catalog
- ▼ **Elastic Block Store**
 - Volumes
 - Snapshots
 - Lifecycle Manager
- ▼ **Network & Security**
 - Security Groups
 - Elastic IPs
 - Placement Groups

Resources

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

Instances (running)	1	Auto Scaling Groups	0	Capacity Reservations	0
Elastic IPs	2	Instances	1	Key pairs	1
Placement groups	0	Security groups	5	Snapshots	0

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 United States (N. Virginia) Region

Instance alarms

0 in alarm 0 OK 0 insufficient data

[View in CloudWatch](#)

[Instances in alarm](#)

Scheduled events

United States (N. Virginia)

No scheduled events

Service he

Region

United States (

Zones

Zone name

- us-east-1a
- us-east-1b
- us-east-1c
- us-east-1d
- us-east-1e
- us-east-1f

[Enable addition](#)

Name the instance “Web Server 1” and the Instance type to t2.micro

Launch an instance [Info](#)

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags [Info](#)

Name

Web Server 1

[Add additional tags](#)

▼ Application and OS Images (Amazon Machine Image) [Info](#)

An AMI contains the operating system, application server, and applications for your instance. If you don't see a suitable AMI below, use the search field or choose [Browse more AMIs](#).

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

Recents

Quick Start



[Browse more AMIs](#)
Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Amazon Linux 2023 kernel-6.1 AMI
ami-0f3caa1cf4417e51b (64-bit (x86), uefi-preferred) / ami-0bea3ccc607167c10 (64-bit (Arm), uefi)
Virtualization: hvm ENA enabled: true Root device type: ebs

Free tier eligible

Description

Amazon Linux 2023 (kernel-6.1) 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 2023.10.20260216.1 x86_64 HVM kernel-6.1

Architecture	Boot mode	AMI ID	Publish Date	Username
64-bit (x86)	uefi-preferred	ami-0f3caa1cf4417e51b	2026-02-16	ec2-user

Verified provider

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

Instance type

t2.micro
Family: t2 1 vCPU 1 GiB Memory Current generation: true On-Demand Linux base pricing: 0.0116 USD per Hour
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

All generations

[Compare instance types](#)

Additional costs apply for AMIs with pre-installed software

Set the Key pair name 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](#)

Click the “Edit” button next to Network settings, and add the instance to the subnet and VPC network we created by


- selecting “lab-vpc” under VPC
- selecting “lab-subnet-public2” under Subnet
- enabling auto-assigning public IP
- Set Firewall to security group “Web Security Group”

▼ **Network settings** [Info](#)


VPC - required | [Info](#)

vpc-0d0f2116588df031a (lab-vpc)
10.0.0.0/16 

Subnet | [Info](#)

subnet-08c269c9e3e32b01c **lab-subnet-public2**
VPC: vpc-0d0f2116588df031a Owner: 438233051441 Availability Zone: us-east-1b (use1-az4)
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-04044b85d2c7d0b02 
VPC: vpc-0d0f2116588df031a  [Compare security group rules](#)

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

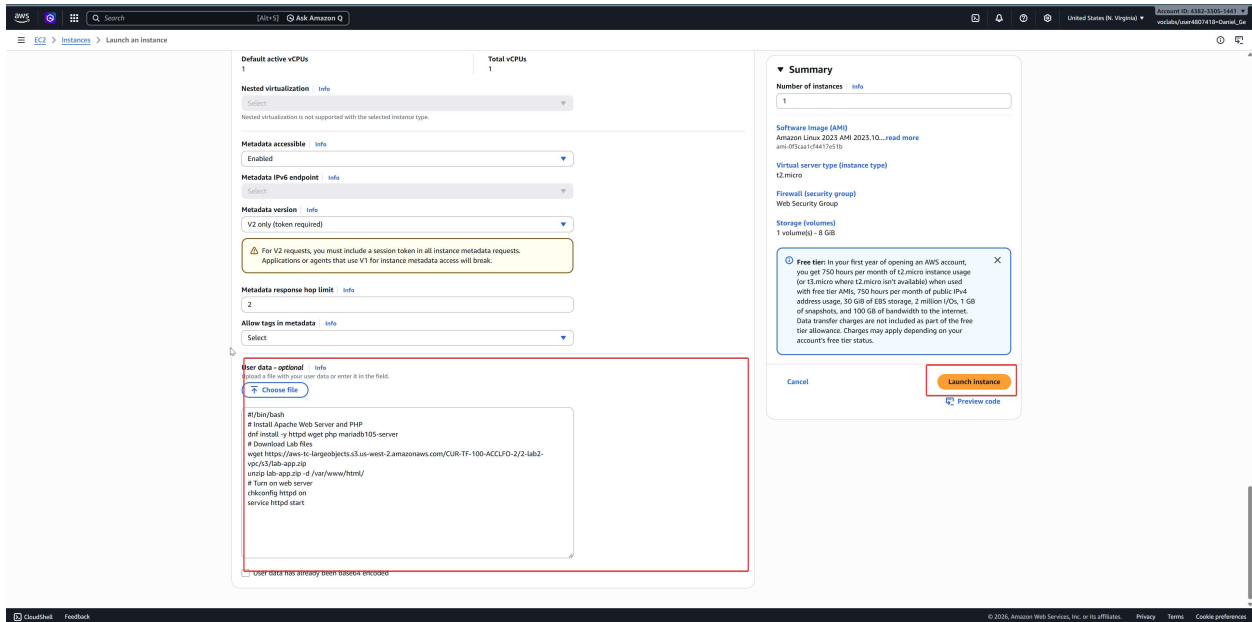
► **Advanced network configuration**

Open “Advanced details”, scroll all the way to the bottom, and paste the following code

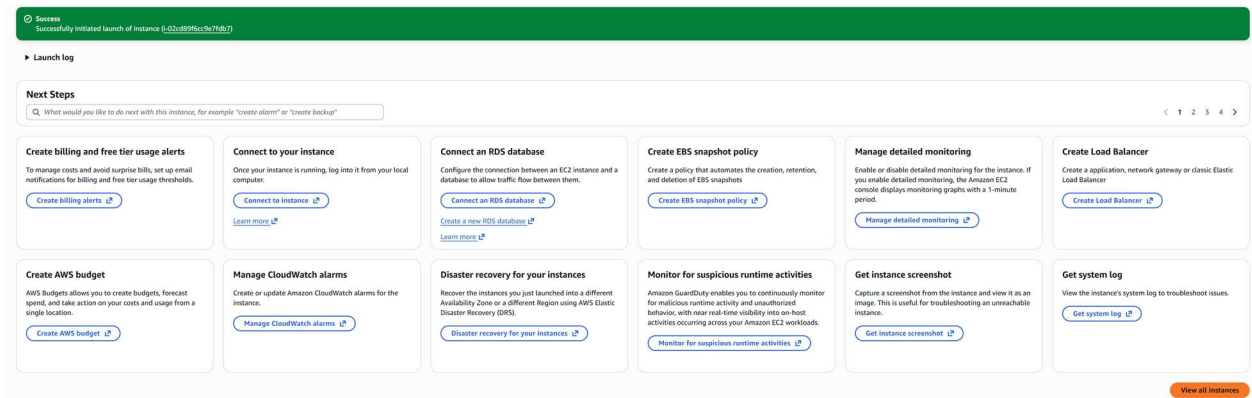
```
#!/bin/bash
# Install Apache Web Server and PHP
dnf install -y httpd wget php mariadb105-server
# Download Lab files
wget https://aws-tc-largeobjects.s3.us-west-2.amazonaws.com/CUR-TF-100-ACCLFO-2/2-lab2-vpc/s3/lab-app.zip
unzip lab-app.zip -d /var/www/html/
# Turn on web server
chkconfig httpd on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

Into the “User data” box

Click “Launch Instance”



Upon seeing the Success message, click “View all instances” at the bottom of the screen



After the status displays 2/2 checks passed next to Web Server 1, check the Web Server 1 box

The screenshot shows the AWS Management Console interface. At the top, there's a navigation bar with the AWS logo, search bar, and user information. Below that, the 'Instances' page is displayed, showing a table of EC2 instances. The table has columns for Name, Instance ID, Instance state, Instance type, Status check, Alarm status, Availability Zone, Public IPv4 DNS, Public IPv4, Elastic IP, IPv6 IPs, Monitoring, Security group name, and Key name. One instance, 'Web Server 1', is highlighted with a red box around its Public IPv4 DNS address: 'ec2-34-228-54-95.compute-1.amazonaws.com'. Below the table, the 'Details' tab for the selected instance is shown, with a red box around the 'Public DNS' field, which contains the same address: 'ec2-34-228-54-95.compute-1.amazonaws.com | open address'. The left sidebar contains various navigation options like Dashboard, Events, Instances, Images, Elastic Block Store, Network & Security, Load Balancing, and Auto Scaling.

Check the details tab to find the Public IPv4 DNS address, and paste the address into the browser

The screenshot shows a web browser window with a dark theme. The address bar contains the URL 'ec2-34-228-54-95.compute-1.amazonaws.com'. The page is currently loading, as indicated by the 'Loading...' text in the top left corner of the browser window.

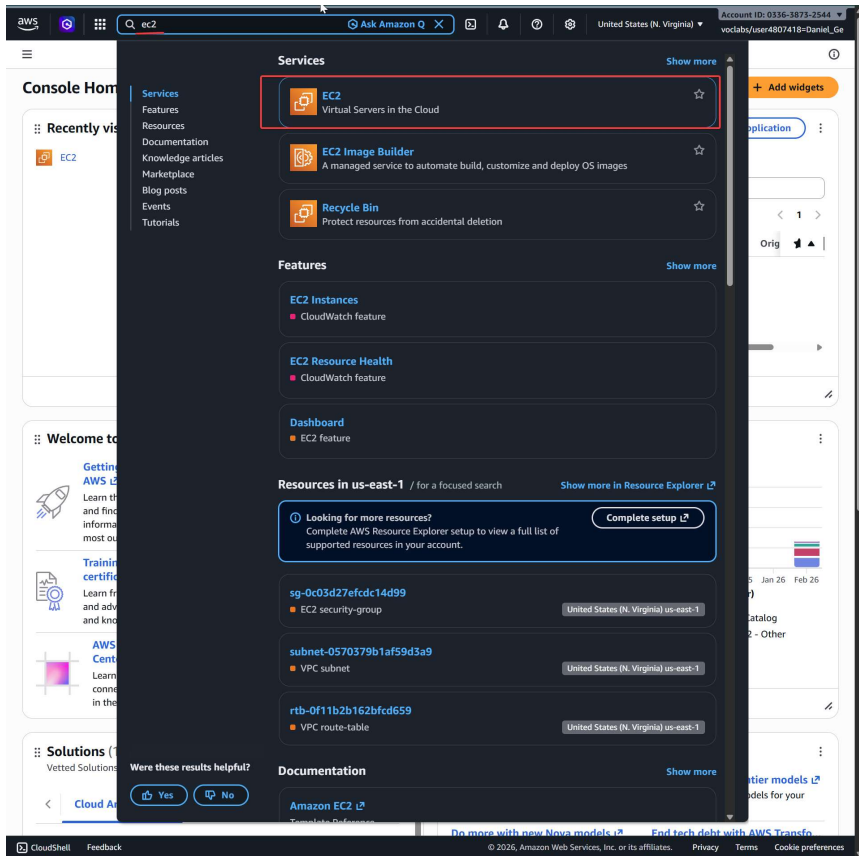
Introduction to Amazon EC2 (Lab 3)

Start the lab and enter the main menu

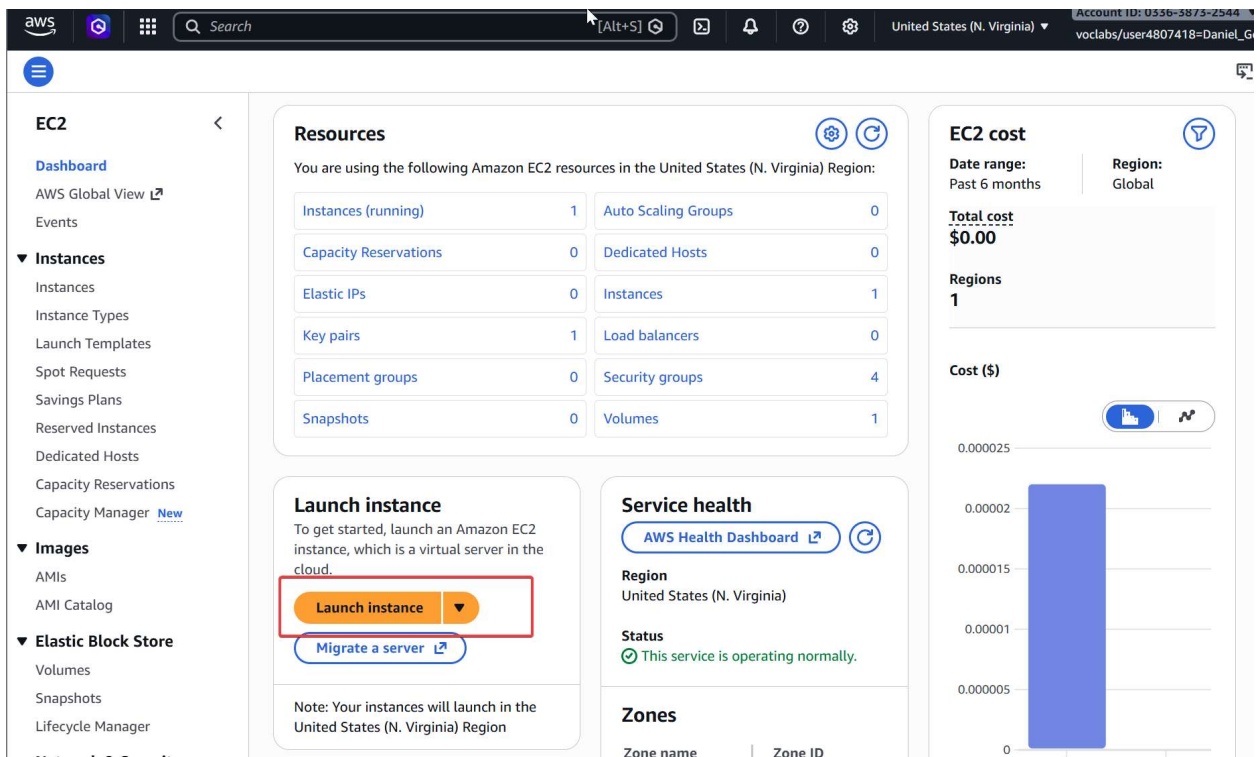
The screenshot displays the AWS Management Console Home page. At the top, the search bar contains the text "EC2". The page is divided into several sections:

- Recently visited:** A list showing "EC2" as the only recently visited service.
- Applications:** A section titled "Applications (0)" with a "Create application" button. It shows "Region: US East (N. Virginia)" and a "Select Region" dropdown menu set to "us-east-1 (Current Region)". Below this, there is a search bar for "Find applications" and a table header with columns: Name, Description, Region, and Orig. The table is currently empty, displaying "No applications" and a "Create application" button.
- Welcome to AWS:** A section with a rocket icon and links for "Getting started with AWS" and "Training and certification".
- AWS Health:** A section showing "Open issues: 0 Past 7 days", "Scheduled changes: 0 Upcoming and past 7 days", and "Other notifications: 0".
- Cost and usage:** A section showing "Current month: \$0.07" and "Forecasted month end: \$0.07". It includes a bar chart titled "Cost (\$)" with a y-axis from 0 to 0 and an x-axis with dates: Sep 25, Oct 25, Nov 25, Dec 25, Jan 26, Feb 26. The chart shows a purple bar for Oct 25 and a red bar for Jan 26.

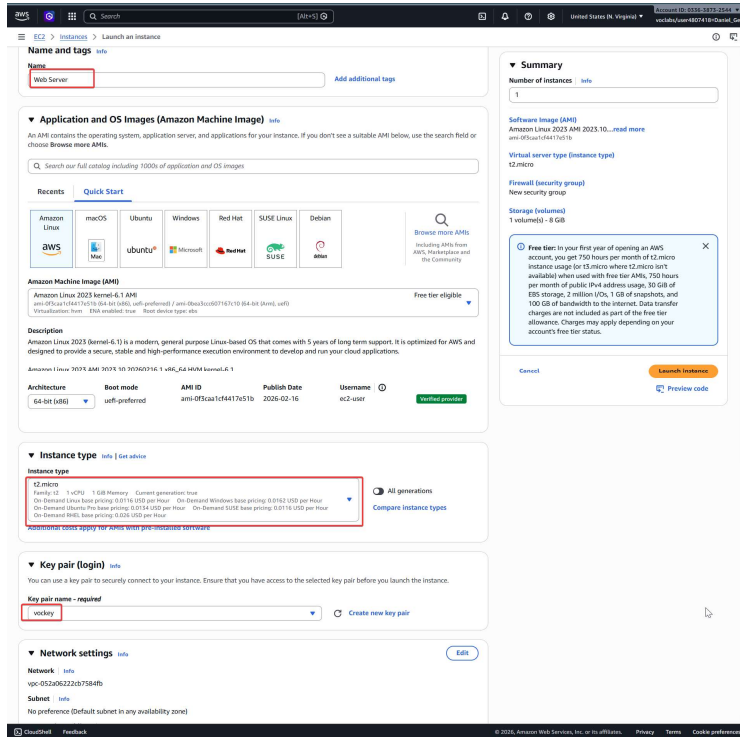
Search “EC2” in the search bar and click the EC2 option to open the EC2 menu



Click "Launch Instance"



Name the server “Web Server”, set the instance type to t2.micro, and the key pair to “vockey”. Click the blue “edit” button to the right of network settings



Configure the VPC to “Lab VPC”, fill out the security group name and description as follows, and click “Remove” to remove the current inbound security group rule

EC2 > Instances > Launch an instance

Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Linux base pricing: 0.0116 USD per Hour 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

All generations
Compare instance types

Additional costs apply for AMIs with pre-installed software

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](#)

Network settings [Info](#)

VPC - *required* [Info](#)
vpc-0ee5d22d0d1599d8d (Lab VPC) [10.0.0.0/16](#) [Create new VPC](#)

Subnet [Info](#)
subnet-07d58525776fa808c PublicSubnet1
VPC: vpc-0ee5d22d0d1599d8d Owner: 033638732544 Availability Zone: us-east-1a (us-east-1a) [Create new subnet](#)
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](#)
Web Server security group

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

Type	Protocol	Port range	Source type	Source	Description - optional
ssh	TCP	22	Anywhere	0.0.0.0/0	e.g. SSH for admin desktop

Under Advanced details, enable Termination protection

▼ **Advanced details** [Info](#)

Domain join directory | [Info](#)
Select [Create new directory](#)

IAM instance profile | [Info](#)
Select [Create new IAM profile](#)

Hostname type | [Info](#)
IP name

DNS Hostname | [Info](#)
 Enable IP name IPv4 (A record) DNS requests
 Enable resource-based IPv4 (A record) DNS requests
 Enable resource-based IPv6 (AAAA record) DNS requests

Instance auto-recovery | [Info](#)
Select

Shutdown behavior | [Info](#)
Stop

Stop - Hibernate behavior | [Info](#)
Select

Termination protection | [Info](#)
Enable

Stop protection | [Info](#)
Select

Detailed CloudWatch monitoring | [Info](#)
Select

Credit specification | [Info](#)
Standard

Placement group | [Info](#)
Select [Create new placement group](#)

EBS-optimized instance | [Info](#)
Disable

Paste the following code into the User data box, then click Launch instance.

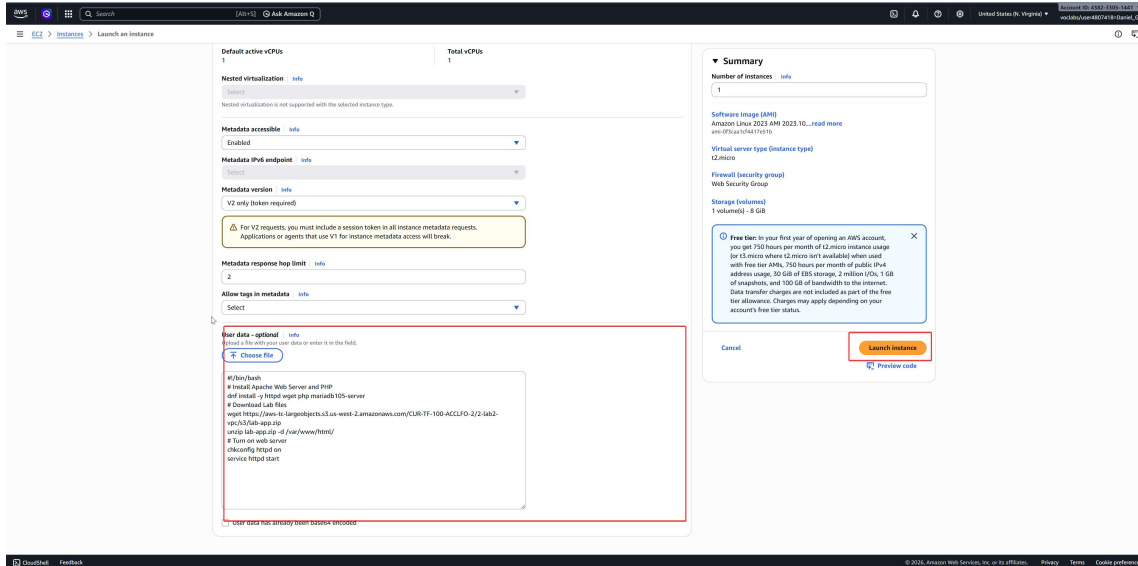
```
#!/bin/bash
```

```
dnf install -y httpd
```

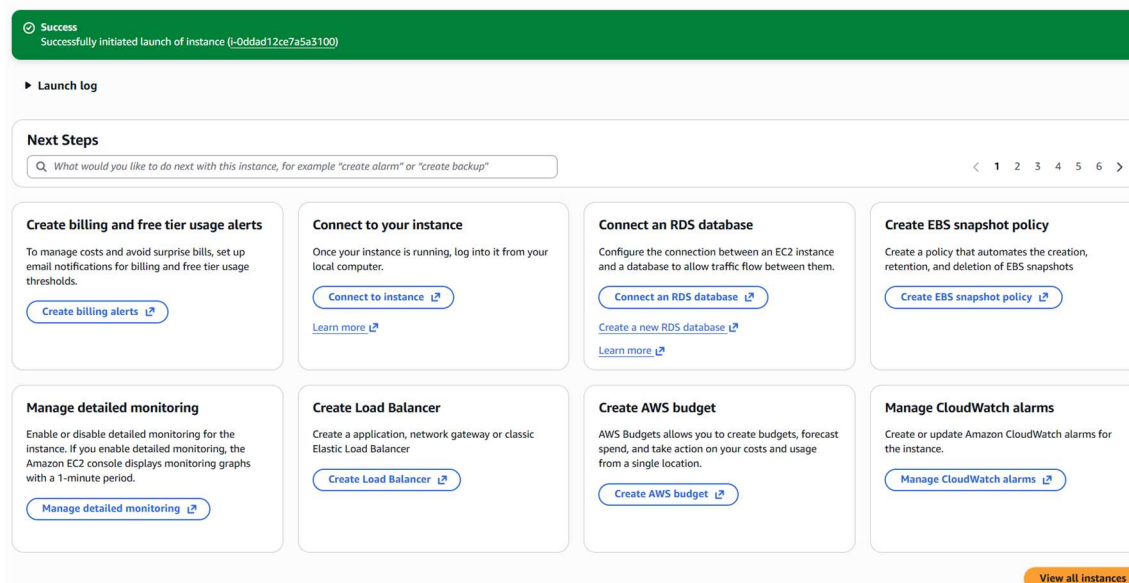
```
systemctl enable httpd
```

```
systemctl start httpd
```

```
echo '<html><h1>Hello From Your Web Server!</h1></html>' > /var/www/html/index.html
```



Click “View all Instances”



After the status check displays 2/2 checks passed, click the checkbox next to “Web Server”, then the “Status and alarms” tab to observe that both status checks have passed

Instances (1/2) Info Connect Instance state Actions Launch instances

Find Instance by attribute or tag (case-sensitive) All states < 1 >

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
<input checked="" type="checkbox"/> Web Server	i-0ddad12ce7a5a3100	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1a	ec2-34-229-216-29.x
<input type="checkbox"/> Bastion Host	i-0252b1d4e9280f2da	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1a	ec2-44-220-163-95.x

i-0ddad12ce7a5a3100 (Web Server)

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

Status checks Info Actions

Status checks detect problems that may impair i-0ddad12ce7a5a3100 (Web Server) from running your applications.

System status check Check passed **Instance status check** Check passed

▶ Metrics

▼ Alarms

Find alarms by name < 1 >

Name	State	Description	Metric name	State reason
Instance has no associated alarms				

Click “Monitoring” to go to the monitoring tab, then, to enlarge one of the graphs, click the three dots then “Enlarge”

i-0ddad12ce7a5a3100 (Web Server)

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

Include metrics in the CWAgent namespace Configure CloudWatch agent Manage detailed monitoring

Alarm recommendations Investigate with AI - new 1h 3h 12h 1d 3d 1w Custom UTC timezone Explore related

CPU utilization (%) **Network in (bytes)** **Network out (bytes)** **Network packets in (count)**

Percent **Bytes** **Count**

2.68 42.17K 21.09K 3.02K

1.34 0 1.51K

21:00 21:30

Network packets out (count) **CPU credit usage (count)** **CPU credit balance (count)**

Count **Count** **Count**

462 1 30

231 0.5 15

0 21:00 21:30

0 21:00 21:30

0 21:00 21:30

Enlarge Refresh Apply time range Explore related Investigate View in metrics View logs View in EC2 Resource Health

Instances (1/2) Info

Find Instance by attribute or tag (case-sensitive) All states

Name	Instance ID	Instance state	Instance type	Status check	Alarm status
Web Server	i-0ddad12ce7a5a3100	Running	t2.micro	2/2 checks passed	View alarms +
Bastion Host	i-0252b1d4e9280f2da	Running	t2.micro	2/2 checks passed	View alarms +

Actions

- Instance diagnostics
- Instance settings
- Networking
- Security
- Image and templates
- Storage
- Monitor and troubleshoot

Monitor

- Manage detailed monitoring
- Manage CloudWatch alarms
- Configure CloudWatch agent

Troubleshoot

- Get system log
- Get instance screenshot
- Connect to serial port
- Replace root volume
- Visit SSM Fleet Manager

i-0ddad12ce7a5a3100 (Web Server)

Details Status and alarms Monitoring Security Networking Storage

Instance summary Info

Instance ID Public IPv4 address Private IPv4 address

After reading the screenshot and checking for errors, click cancel at the bottom of the page to exit out

CloudTrail events Systems Manager Reachability Analyzer - new Instance events Instance screenshot System log

Instance screenshot Last updated February 24, 2026, 14:07 (UTC-08:00) Download

Retrieve console screenshots from your EC2 instance.

```

Amazon Linux 2023.10.20260216
Kernel 6.1.161-183.298.amzn2023.x86_64 on an x86_64 (-)

ip-10-0-1-10 login: [ 26.256653] zram_generator::config[2315]: zram0: system has too much memory (961MB), limit is 800MB, ignoring.
[ 27.456257] zram_generator::config[3502]: zram0: system has too much memory (961MB), limit is 800MB, ignoring.

```

For boot or networking issues, use the EC2 serial console for troubleshooting. Choose the Connect button to start a session.

Connect

Cancel

Click “Details” then click “open address” under “Public DNS” to attempt to access the website right now

The screenshot shows the AWS Management Console interface. At the top, there's a header for "Instances (1/2)" with a search bar and filters. Below this is a table of instances:

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
Web Server	i-0ddad12ce7a5a3100	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1a	ec2-34-229-216-29
Bastion Host	i-0252b1d4e9280f2da	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1a	ec2-44-220-163-95

Below the table, the details for the "Web Server" instance (i-0ddad12ce7a5a3100) are shown. The "Details" tab is selected and highlighted with a red box. The "Public DNS" field is also highlighted with a red box, showing the address "ec2-34-229-216-29.compute-1.amazonaws.com".

Observe that the website is currently inaccessible since we have not created any inbound security rule allowing traffic to visit the website

The screenshot shows a web browser window with the address bar displaying "ec2-34-229-216-29.compute-1.amazonaws.com". The page content is a dark-themed error message:

This site can't be reached
ec2-34-229-216-29.compute-1.amazonaws.com took too long to respond.

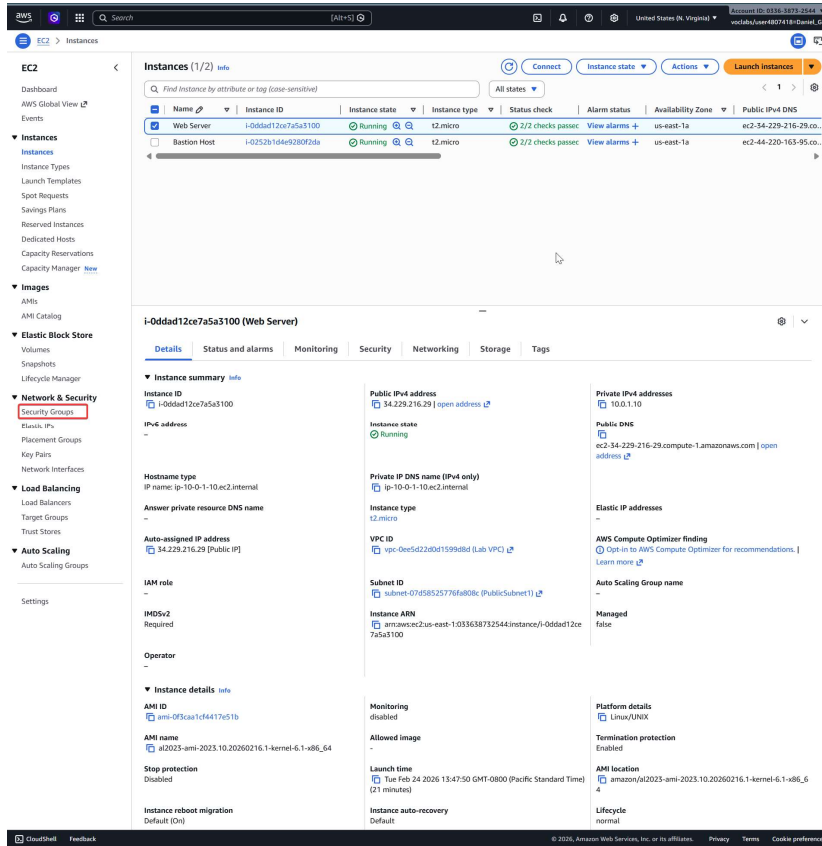
Try:

- Checking the connection
- Checking the proxy and the firewall
- Running Windows Network Diagnostics

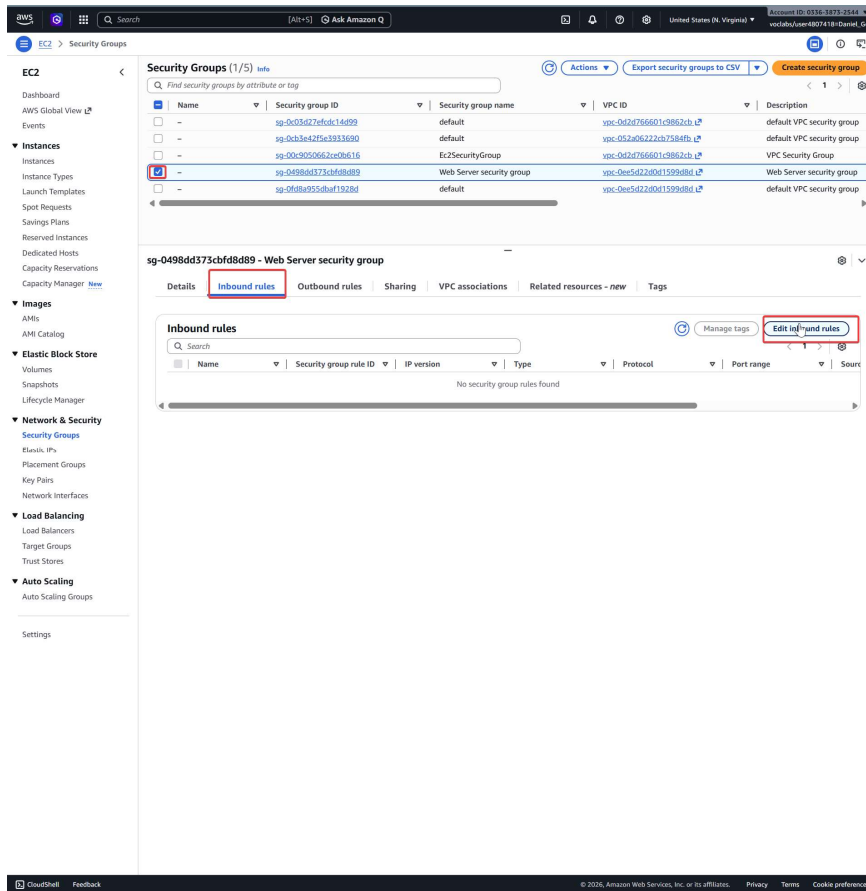
ERR_CONNECTION_TIMED_OUT

Buttons for "Reload" and "Details" are visible at the bottom of the error message.

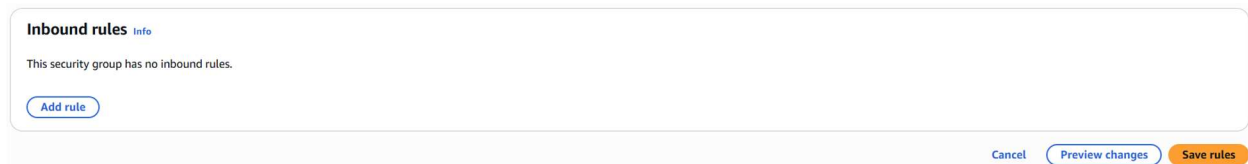
With the browser tab still open, return to the previous EC2 Console tab and click “Security Groups” on the left menu



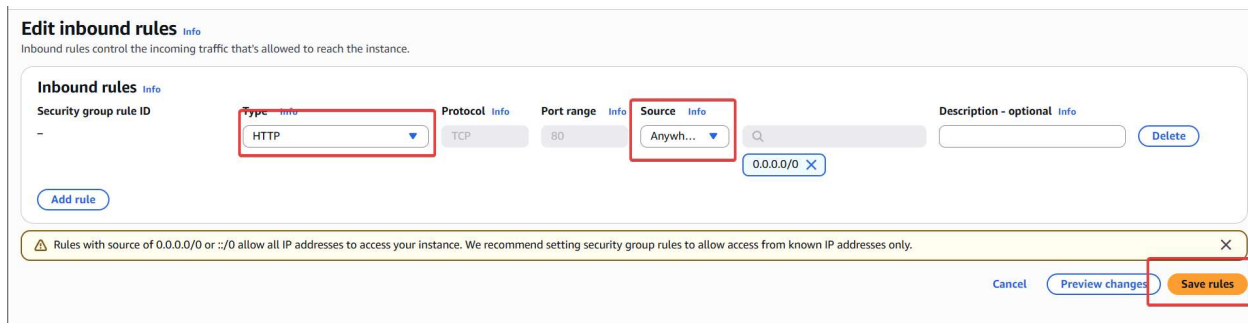
Check the box for “Web Server security group”, click the “Inbound rules” tab, then “Edit inbound rules”



Click “Add rule”



Set the Type to HTTP, Source to “Anywhere IPV4”, then Save rules

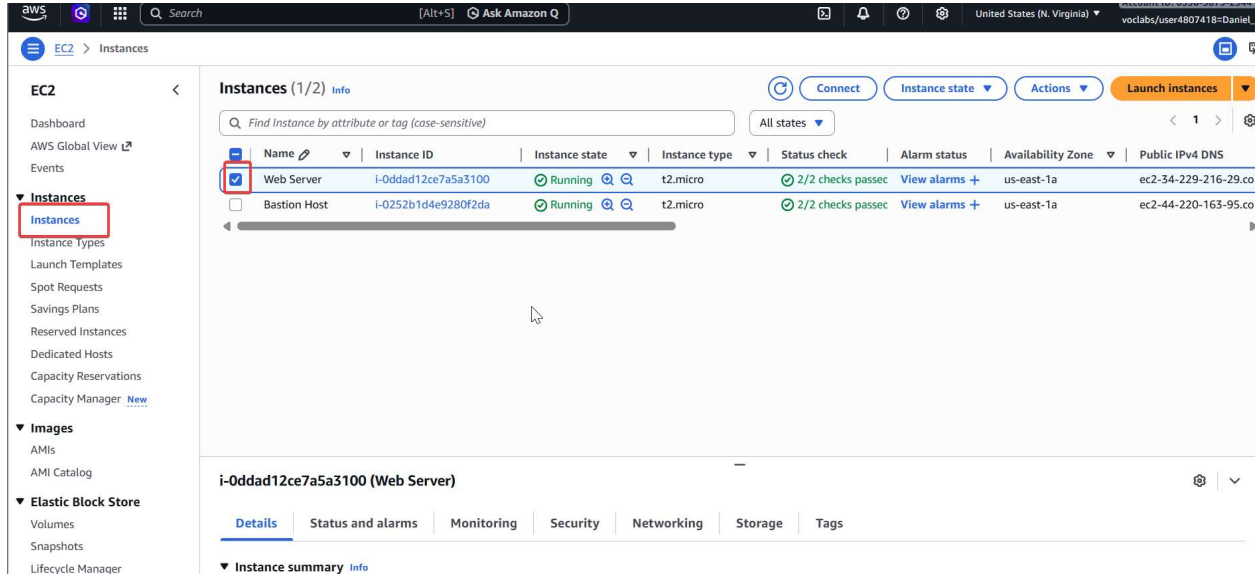


Returning to the tab with the web server, we are now able to access it and see the message

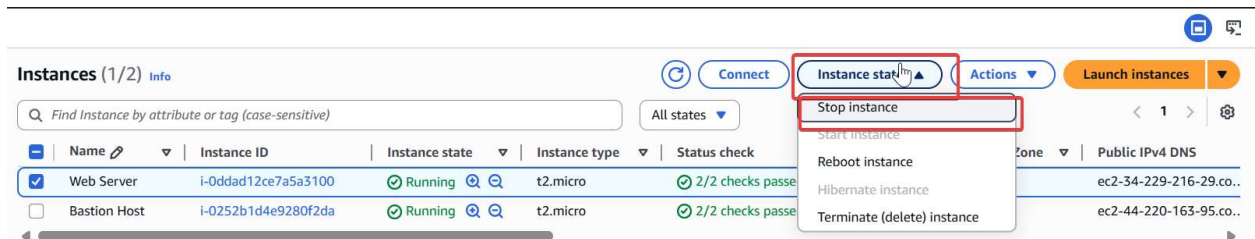


Hello From Your Web Server!

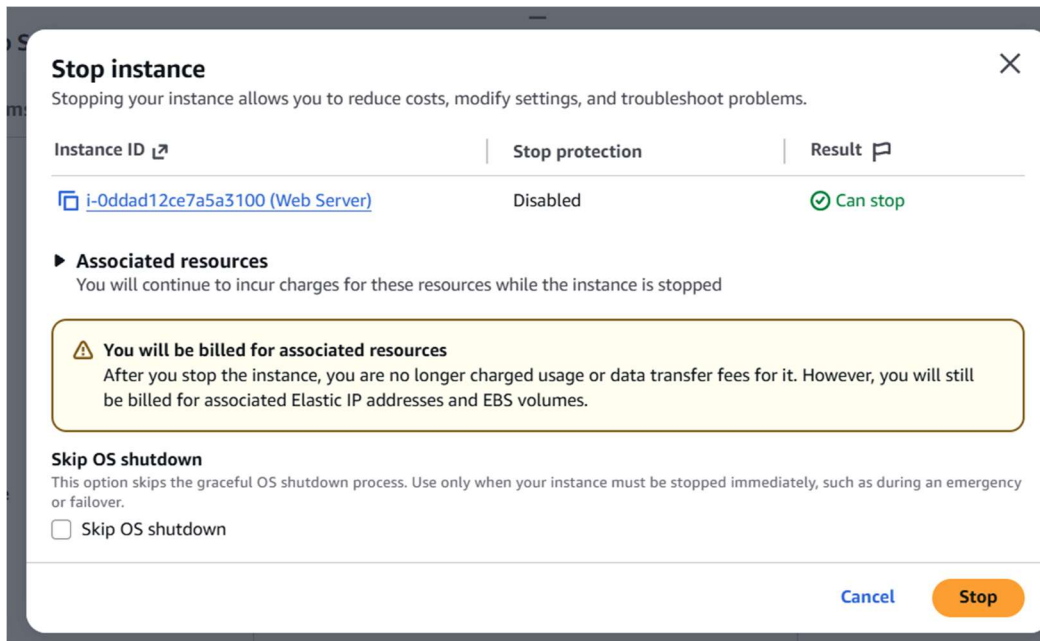
To change the size of the instance, we first must stop the instance. Begin by clicking “Instances” on the left menu, then checkbox the Web Server



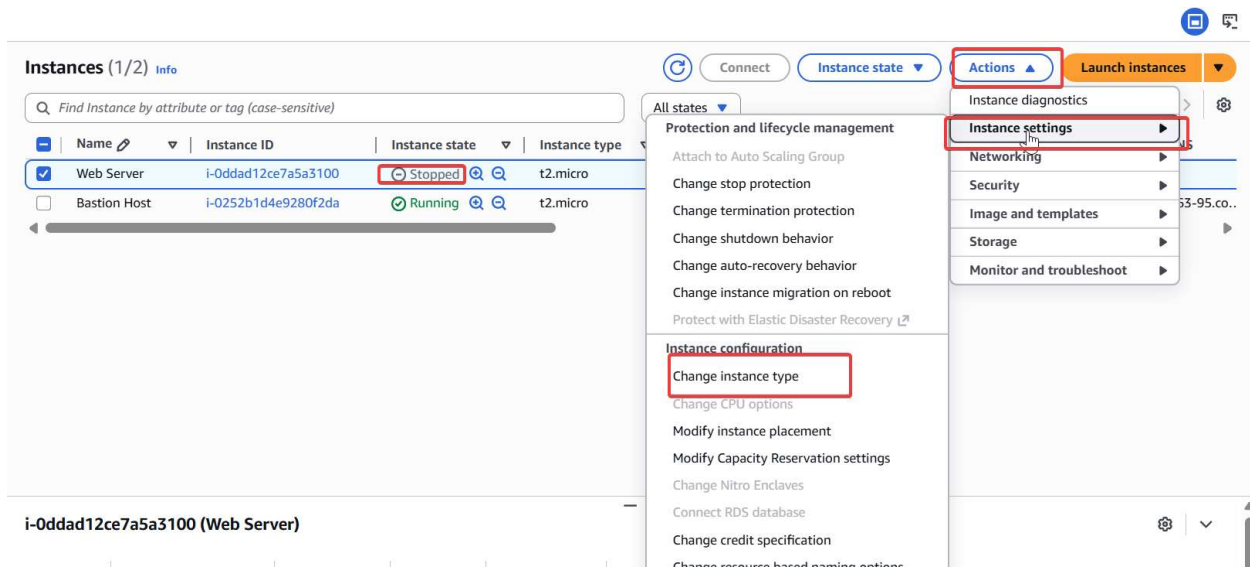
Click “Instance state” then “Stop instance” on the top



Click “Stop”



After the Instance state displays “Stopped”, click “Actions” then “Instance settings” then “Change instance type”



Change the instance type to “t2.small”, then click “Change instance type”

Instance ID
i-0ddad12ce7a5a3100 (Web Server)

Current instance type
t2.micro

New instance type
t2.small

▼ 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 (MiB)	1024	2048
Storage (GiB)	-	-
Supported root device types	ebs	ebs
Network performance	Low to Moderate	Low to Moderate
Architecture	i386	i386
Burstable	true	true
Free-tier eligible	false	false
Current generation	true	true

Advanced details

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

Cancel **Change instance type**

Click “Actions” then “Instance settings” then “Change stop protection”

Instance type changed successfully

Instances (1/2) Info

Find Instance by attribute or tag (case-sensitive)

Name	Instance ID	Instance state	Instance type
Web Server	i-0ddad12ce7a5a3100	Stopped	t2.micro
Bastion Host	i-0252b1d4e9280f2da	Running	t2.micro

Connect Instance state Actions Launch instances

Instance diagnostics

Instance settings

Networking

Security

Image and templates

Storage

Monitor and troubleshoot

Change stop protection

Change termination protection

Change shutdown behavior

Change auto-recovery behavior

Change instance migration on reboot

Protect with Elastic Disaster Recovery

Instance configuration

Click “Enable” then “Save”

Change stop protection

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

[Learn more](#)

Instance ID

i-Oddad12ce7a5a3100 (Web Server)

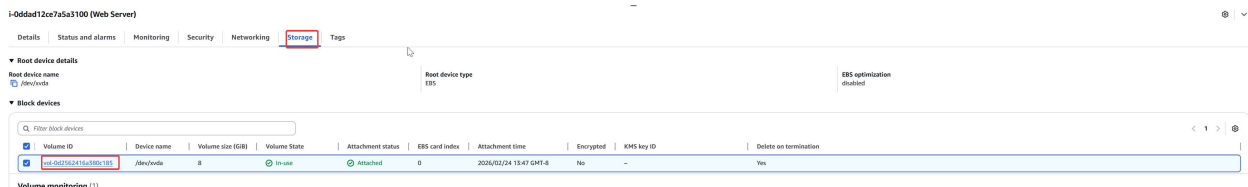
Stop protection

Enable

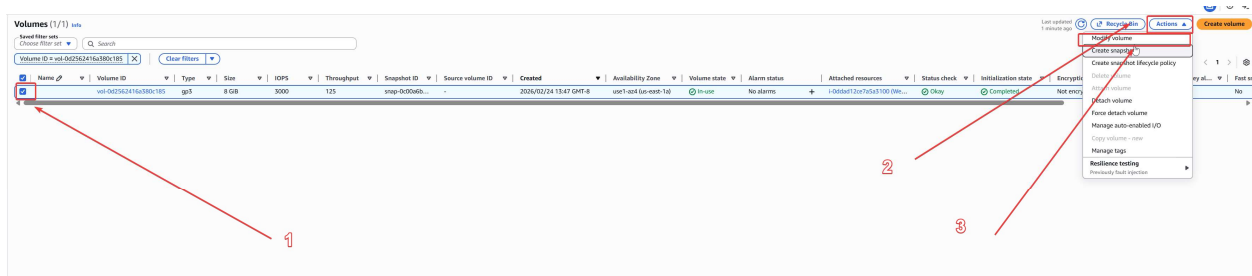
Cancel

Save

Next, to resize the EBS Volume, click the Storage tab, then select the Volume ID name



Click the checkbox next to the first volume displayed, then “Actions” and “Modify Volume”



Set the Size to 10 GiB, and click “Modify”

Modify volume

Modify the type, size, and performance of an EBS volume.

Volume details

Volume ID

vol-0d2562416a380c185

Volume type

General Purpose SSD (gp3)

Size (GiB)

10

Min: 1 GiB, Max: 65536 GiB.

IOPS

3000

Min: 3000 IOPS, Max: 80000 IOPS.

Throughput (MiB/s)

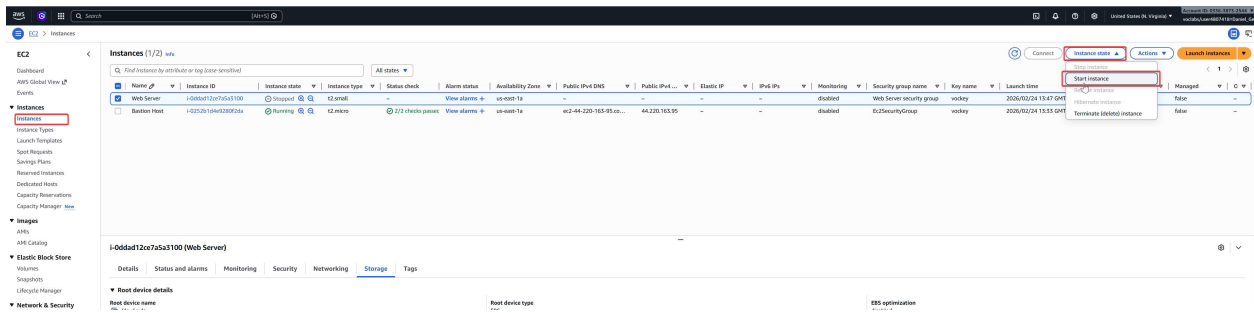
125

Min: 125 MiB, Max: 2000 MiB. Baseline: 125 MiB/s.

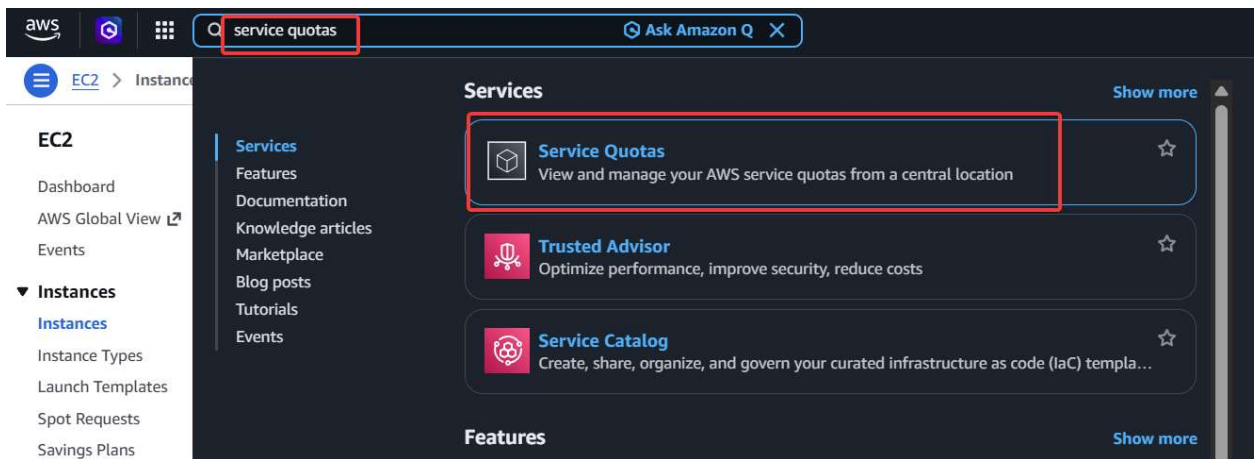
Cancel

Modify

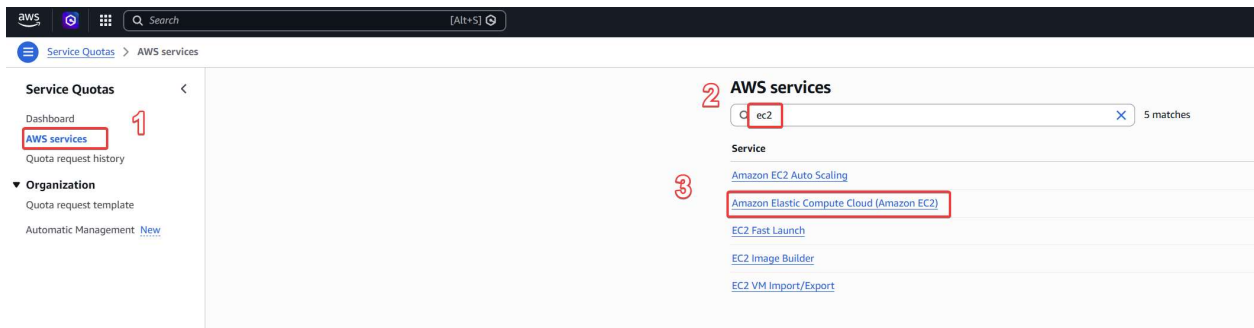
Return to the Instances tab using the left menu, then click “Instance state” and “Start instance”



To find information on quotas, search “service quotas” in the search bar



Click “AWS Services” in the left menu, then search for EC2



As the EC2 account owner, you can search and modify the Service quotas. For example, to modify the running on-demand quotas, simply search running on-demand in the search bar

Amazon Elastic Compute Cloud (Amazon EC2)

Amazon Elastic Compute Cloud (EC2) provides resizable compute capacity through virtual machines (VMs or instances) in the cloud.

For Amazon Elastic Compute Cloud (Amazon EC2) quotas with Adjustability at the Resource-level, you can now request a quota increase at the resource level by clicking the quota name to navigate to the quota details page and choosing the resource for which you want to request a quota increase. [Learn more](#)

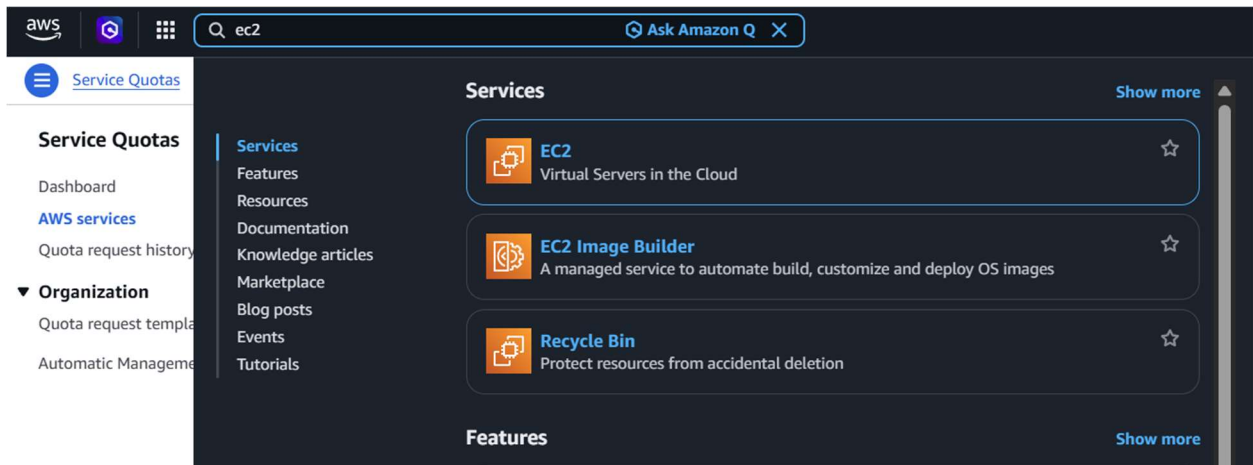
Service quotas info Request increase at account level

View your applied quota values, default quota values, and request quota increases for quotas. [Learn more](#)

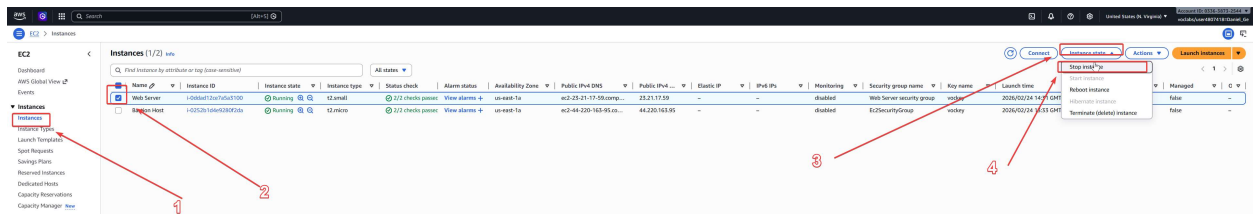
Q: running on-demand X 10 matches < 1 > ⚙

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

To test the stop protection, return to the EC2 menu



Return to the instances tab, check the checkbox next to Web server, and click “Instance state” then Stop instance



Click “Stop”. Observe that the instance cannot be stopped since stop protection is enabled

Stop instance ✕

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

Instance ID ↗	Stop protection	Result 🚩
i-0ddad12ce7a5a3100 (Web Server)	Enabled	⚠️ Can't stop

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

⚠️ **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.

Skip OS shutdown
This option skips the graceful OS shutdown process. Use only when your instance must be stopped immediately, such as during an emergency or failover.

Skip OS shutdown

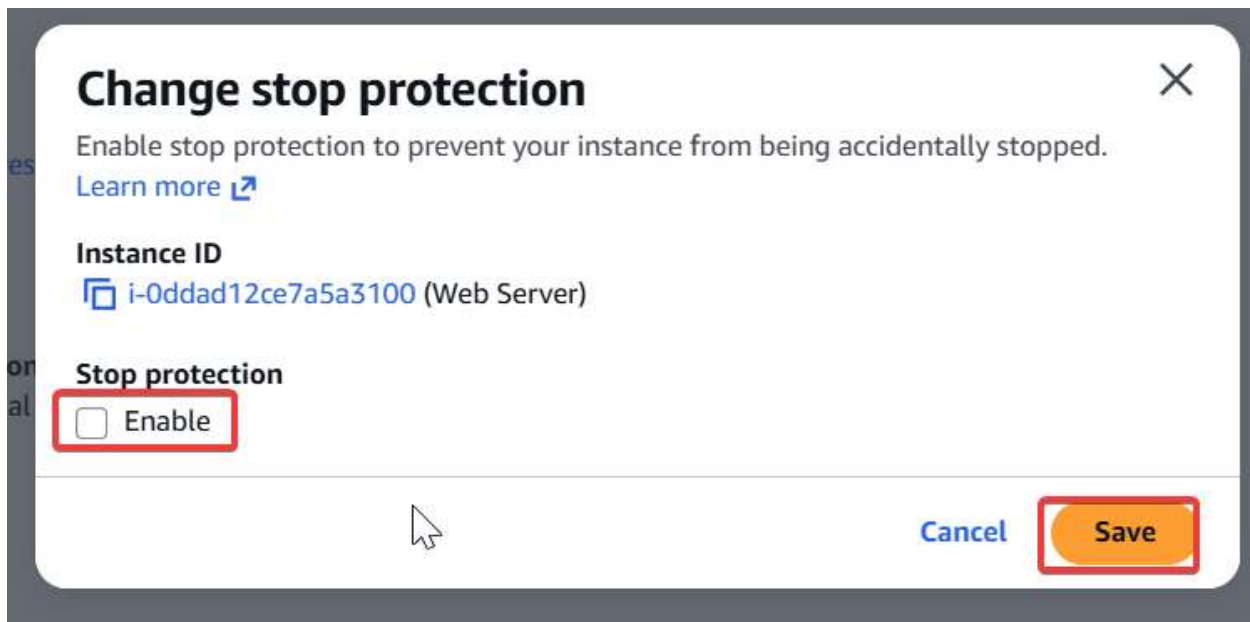
Cancel Stop

⚠️ Failed to stop the instance i-0ddad12ce7a5a3100. The instance i-0ddad12ce7a5a3100 may not be stopped. Modify its 'UserData'/'Stop' instance attribute and try again. 🔍 Diagnose with Amazon Q

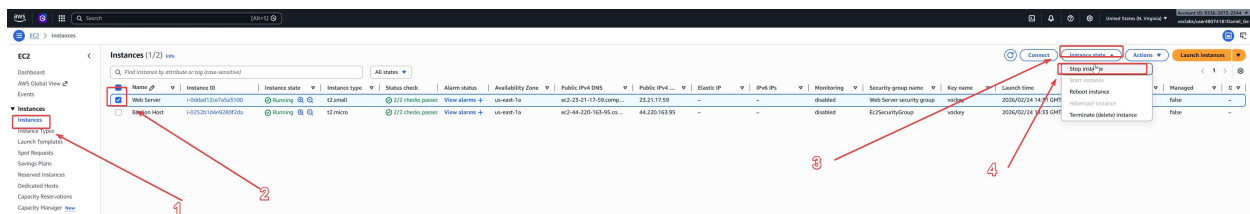
Click “Actions” then “Instance settings” then “Change stop protection”

The screenshot shows the AWS Management Console interface. At the top, a green notification bar states "Instance type changed successfully". Below this, the "Instances (1/2) info" section displays a table with two instances: "Web Server" (ID: i-0ddad12ce7a5a3100, state: Stopped, type: t2.micro) and "Bastion Host" (ID: i-0252b1d4e9280f2da, state: Running, type: t2.micro). The "Web Server" instance is selected. To the right of the table, the "Actions" menu is open, showing options like "Change stop protection", "Change termination protection", and "Change shutdown behavior". The "Change stop protection" option is highlighted with a red box. The "Instance settings" sub-menu is also visible, with "Instance settings" highlighted.

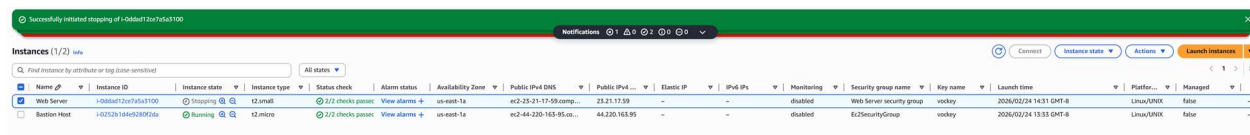
Uncheck the “Enable” box for stop protection, then click “Save”



Follow the same steps to stop the instance

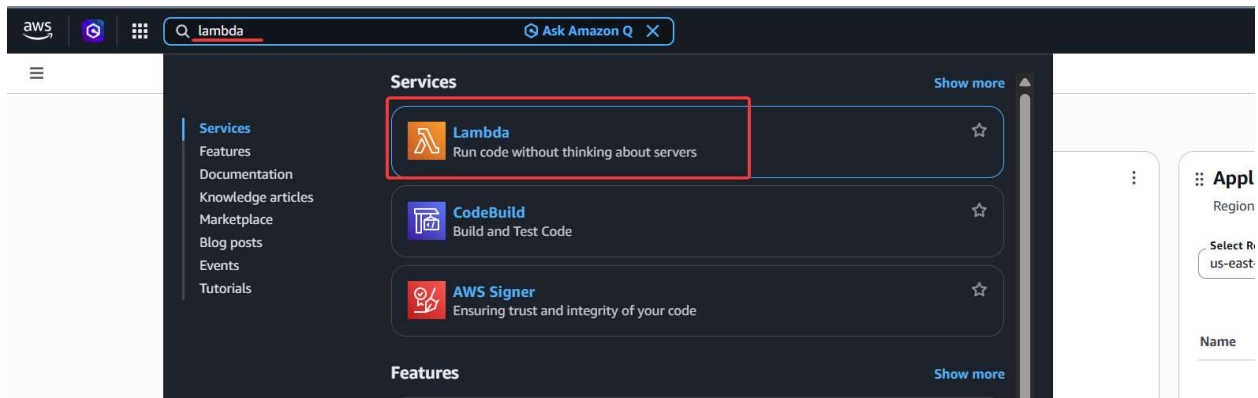


This time, the stop should be successful since stop protection is disabled

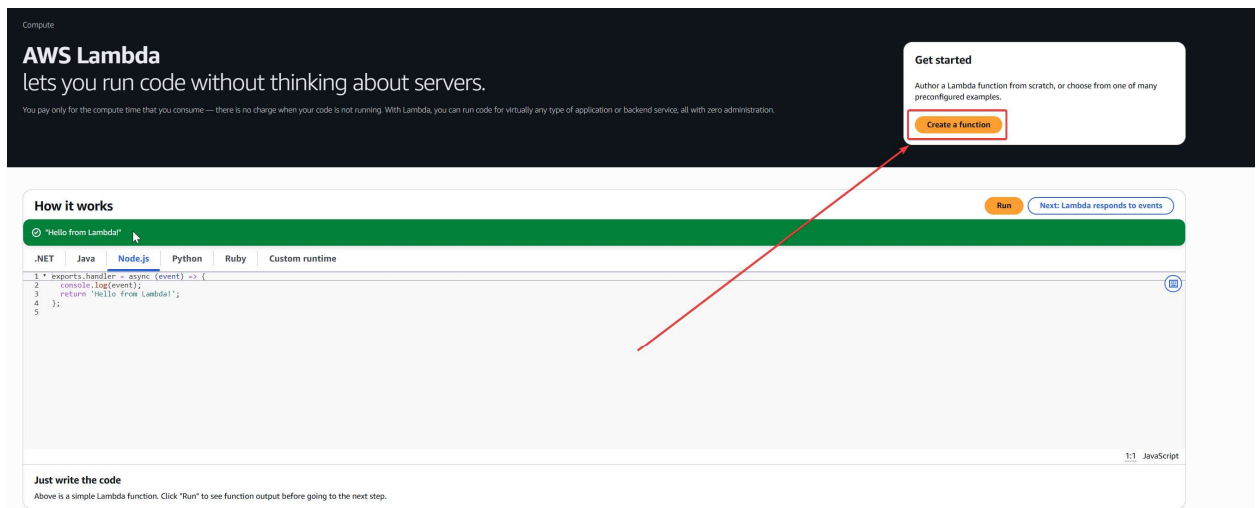


AWS Lambda

Using the search bar next to services, search for “Lambda” and open to AWS Lambda console



Click “Create a Function”



Configure the Python function with the following settings and permissions

Create function [Info](#)

Choose one of the following options to create your function.

Author from scratch

Start with a simple Hello World example.

Use a blueprint

Build a Lambda application from sample code and configuration presets for common use cases.

Container image

Select a container image to deploy for your function.

Basic information

Function name

Enter a name that describes the purpose of your function.

myStopinator

Function name must be 1 to 64 characters, must be unique to the Region, and can't include spaces. Valid characters are a-z, A-Z, 0-9, hyphens (-), and underscores (_).

Runtime

Choose the language to use to write your function. Note that the console code editor supports only Node.js, Python, and Ruby.

Python 3.11

Durable execution - new

Enable durable execution to simplify building resilient multi-step applications that checkpoint progress and resume after interruptions. Supports Python and Node.js runtimes. [View pricing](#)

Enable

Architecture

Choose the instruction set architecture you want for your function code.

arm64

x86_64

Permissions

By default, Lambda will create an execution role with permissions to upload logs to Amazon CloudWatch Logs. You can customize this default role later when adding triggers.

Change default execution role

Execution role

To access other AWS services and resources your function needs an IAM role. Choose a role with the right permissions for your function.

Create default role

Use another role

myStopinatorRole



Create new role

[View role details in IAM](#)

Additional configurations

Use additional configurations to set up networking, security, and governance for your function. These settings help secure and customize your Lambda function deployment.

Cancel

Create function

To create a trigger which automatically activates the function, click “Add trigger”

Successfully created the function **myStopinator**. You can now change its code and configuration. To invoke your function with a test event, choose “Test”.

myStopinator

Throttle Copy ARN Actions

Export to Infrastructure Composer Download

Function overview

Diagram Template

myStopinator

Layers (0)

+ Add trigger + Add destination

Description

Last modified 33 seconds ago

Function ARN arn:aws:lambda:us-east-1:675453665734:function:myStopinator

Function URL

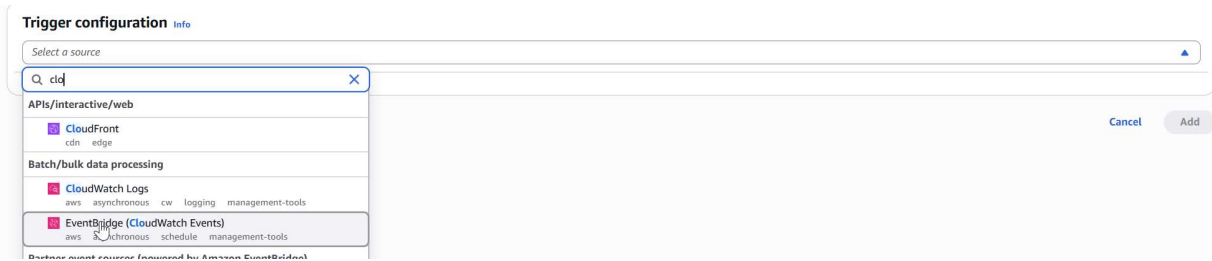
Code Test Monitor Configuration Aliases Versions

Code source

Open in Visual Studio Code Upload from

```
1 import json
2
3 def lambda_handler(event, context):
4     # TODO implement
5     return {
6         'statusCode': 200,
7         'body': json.dumps('Hello from Lambda!')}
8
9
```

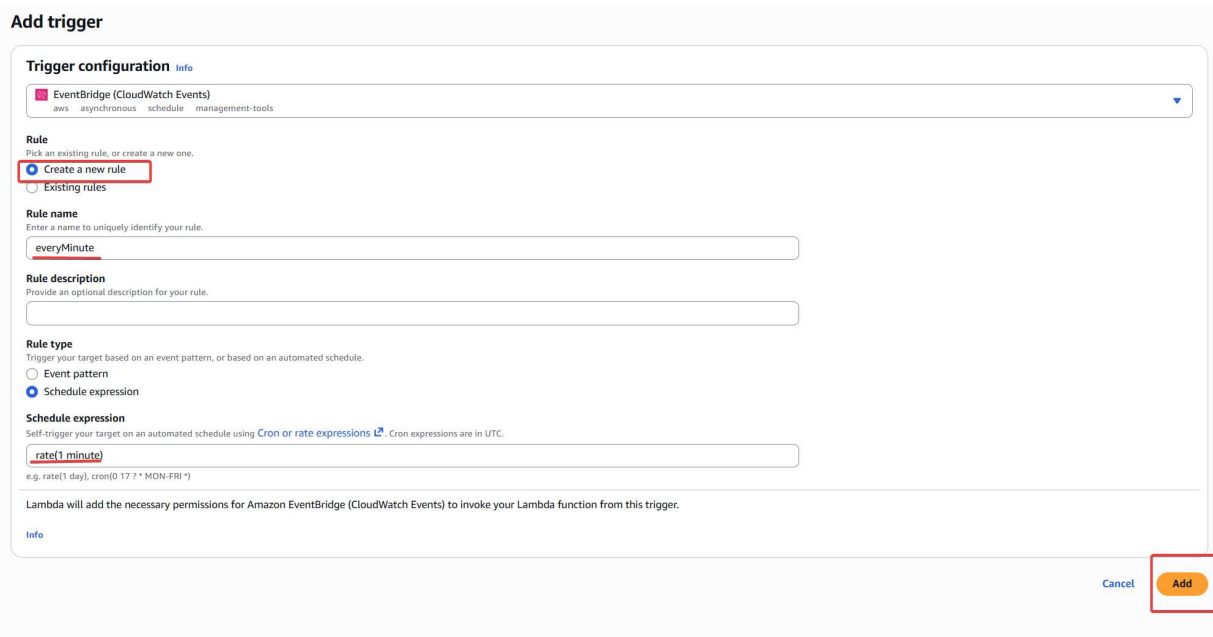
Link the trigger to CloudWatch by selecting “**EventBridge (CloudWatch Events)**” from the source options



Click “Create a new rule” to create a rule with,

- Name: everyMinute
- Schedule expression: rate(1 minute)

Click Add to add the rule



Click the “Code” tab and replace the current content of the text editor with the following code

```
import boto3

region = '<REPLACE_WITH_REGION>'
instances = ['<REPLACE_WITH_INSTANCE_ID>']
ec2 = boto3.client('ec2', region_name=region)

def lambda_handler(event, context):
    ec2.stop_instances(InstanceIds=instances)
    print('stopped your instances: ' + str(instances))
```

Function overview Info

Export to Infrastructure Composer Download

Diagram Template

myStopinator

Layers (0)

EventBridge (CloudWatch Events)

+ Add trigger

+ Add destination

Description

Last modified 4 minutes ago

Function ARN [arn:aws:lambda:us-east-1:675453665734:function:myStopinator](#)

Function URL [Info](#)

Code Test Monitor Configuration Aliases Versions

Code source Info

Open in Visual Studio Code Upload from

EXPLORER

MYSTOPINATOR

lambda_function.py

DEPLOY Undeployed

Deploy (Ctrl+Shift+U)

Test (Ctrl+Shift+T)

TEST EVENTS (NONE SELECTED)

Create new test event

ENVIRONMENT VARIABLES

Undeployed Changes

```

1 import boto3
2 region = '<REPLACE_WITH_REGION>'
3 instances = ['<REPLACE_WITH_INSTANCE_ID>']
4 ec2 = boto3.client('ec2', region_name=region)
5
6 def lambda_handler(event, context):
7     ec2.stop_instances(InstanceIds=instances)
8     print("Stopped your instances: " + str(instances))
9

```

Amazon Q Tip 1/3: Start typing to get suggestions ([ESC] to exit)

See what's new in the code editor

Source: Explore new features

OK Not now

Ln 9, Col 1 Spaces: 4 UTF-8 LF Python Lambda Layout: US

Click the tab on the top right displaying the user's current region to find the region name, then replace "<REPLACE_WITH_REGION>" with this name

myStopinator

The trigger eventbridge was successfully added to function myStopinator.

Function overview

Export to Infrastructure Composer Download

Diagram Template

myStopinator

Layers (0)

EventBridge (CloudWatch Events)

+ Add trigger

+ Add destination

Description

Last modified 7 minutes ago

Function ARN [arn:aws:lambda:us-east-1:675453665734:function:myStopinator](#)

Function URL [Info](#)

Code Test Monitor Configuration Aliases Versions

Code source Info

Open in Visual Studio Code Upload from

EXPLORER

MYSTOPINATOR

lambda_function.py

DEPLOY Undeployed

Deploy (Ctrl+Shift+U)

Test (Ctrl+Shift+T)

TEST EVENTS (NONE SELECTED)

Create new test event

ENVIRONMENT VARIABLES

Undeployed Changes

```

1 import boto3
2 region = 'us-east-1'
3 instances = ['i-201402c100']
4 ec2 = boto3.client('ec2', region_name=region)
5
6 def lambda_handler(event, context):
7     ec2.stop_instances(InstanceIds=instances)
8     print("Stopped your instances: " + str(instances))
9

```

Amazon Q Tip 1/3: Start typing to get suggestions ([ESC] to exit)

United States

- us-east-1
- us-east-2
- us-west-1
- us-west-2
- Canada
- ap-south-1
- ap-south-2
- ap-south-3
- ap-south-4
- ap-south-5
- ap-south-6
- ap-south-7
- ap-south-8
- ap-south-9
- ap-south-10
- ap-south-11
- ap-south-12
- ap-south-13
- ap-south-14
- ap-south-15
- ap-south-16
- ap-south-17
- ap-south-18
- ap-south-19
- ap-south-20
- ap-south-21
- ap-south-22
- ap-south-23
- ap-south-24
- ap-south-25
- ap-south-26
- ap-south-27
- ap-south-28
- ap-south-29
- ap-south-30
- ap-south-31
- ap-south-32
- ap-south-33
- ap-south-34
- ap-south-35
- ap-south-36
- ap-south-37
- ap-south-38
- ap-south-39
- ap-south-40
- ap-south-41
- ap-south-42
- ap-south-43
- ap-south-44
- ap-south-45
- ap-south-46
- ap-south-47
- ap-south-48
- ap-south-49
- ap-south-50
- ap-south-51
- ap-south-52
- ap-south-53
- ap-south-54
- ap-south-55
- ap-south-56
- ap-south-57
- ap-south-58
- ap-south-59
- ap-south-60
- ap-south-61
- ap-south-62
- ap-south-63
- ap-south-64
- ap-south-65
- ap-south-66
- ap-south-67
- ap-south-68
- ap-south-69
- ap-south-70
- ap-south-71
- ap-south-72
- ap-south-73
- ap-south-74
- ap-south-75
- ap-south-76
- ap-south-77
- ap-south-78
- ap-south-79
- ap-south-80
- ap-south-81
- ap-south-82
- ap-south-83
- ap-south-84
- ap-south-85
- ap-south-86
- ap-south-87
- ap-south-88
- ap-south-89
- ap-south-90
- ap-south-91
- ap-south-92
- ap-south-93
- ap-south-94
- ap-south-95
- ap-south-96
- ap-south-97
- ap-south-98
- ap-south-99
- ap-south-100

There are 17 regions that are not enabled for this account

Manage Regions Manage Local Zones

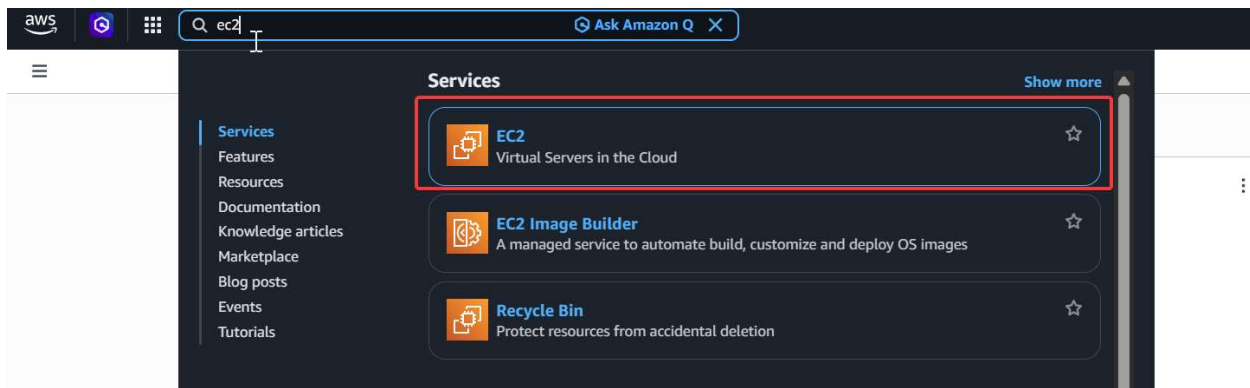
Code properties

Package size 209 bytes

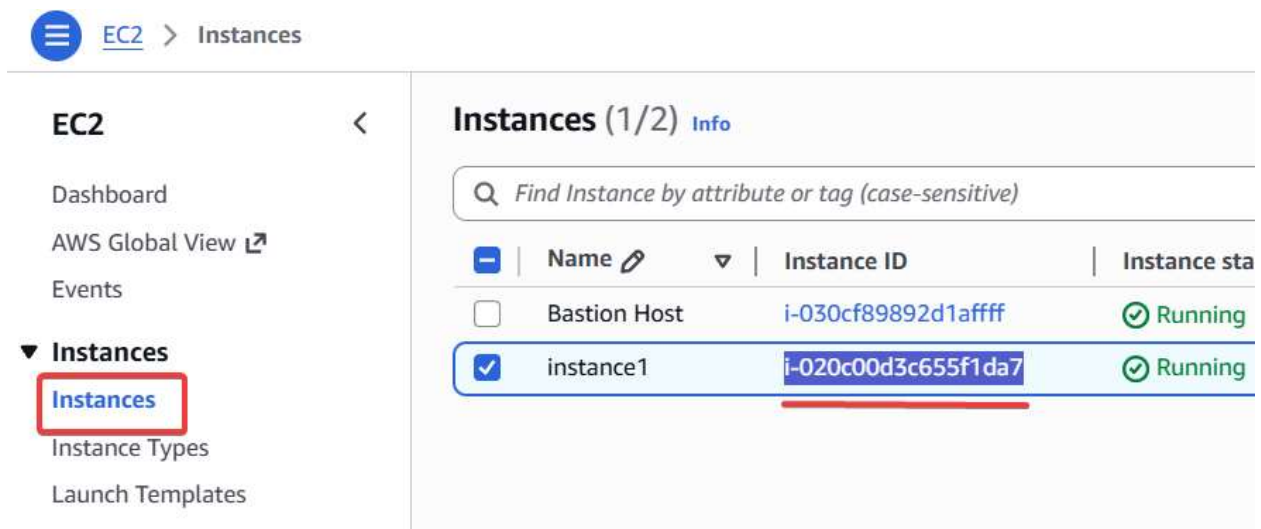
SHA256 hash [View on S3](#)

Last modified 6 minutes ago

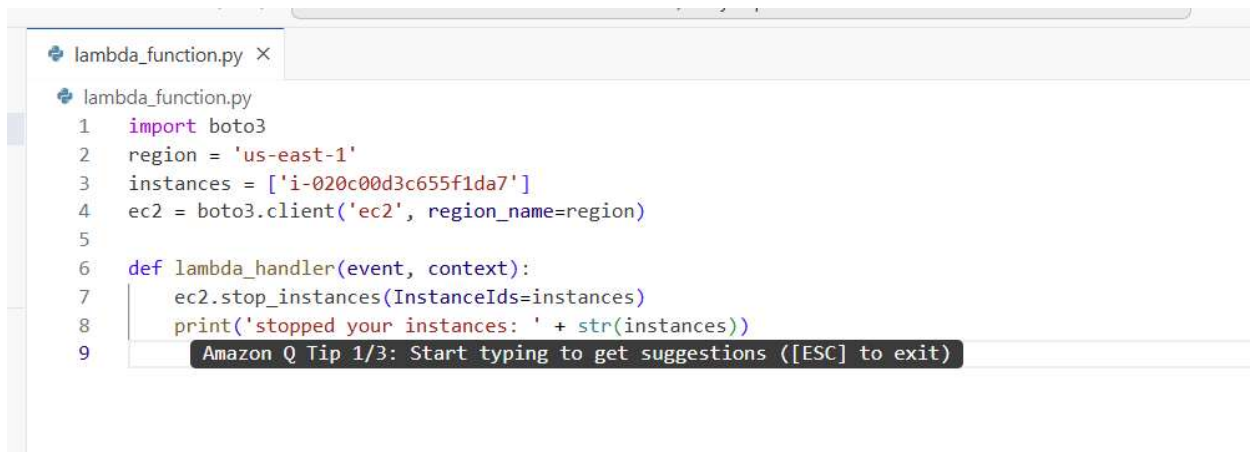
Open the EC2 menu in a new tab



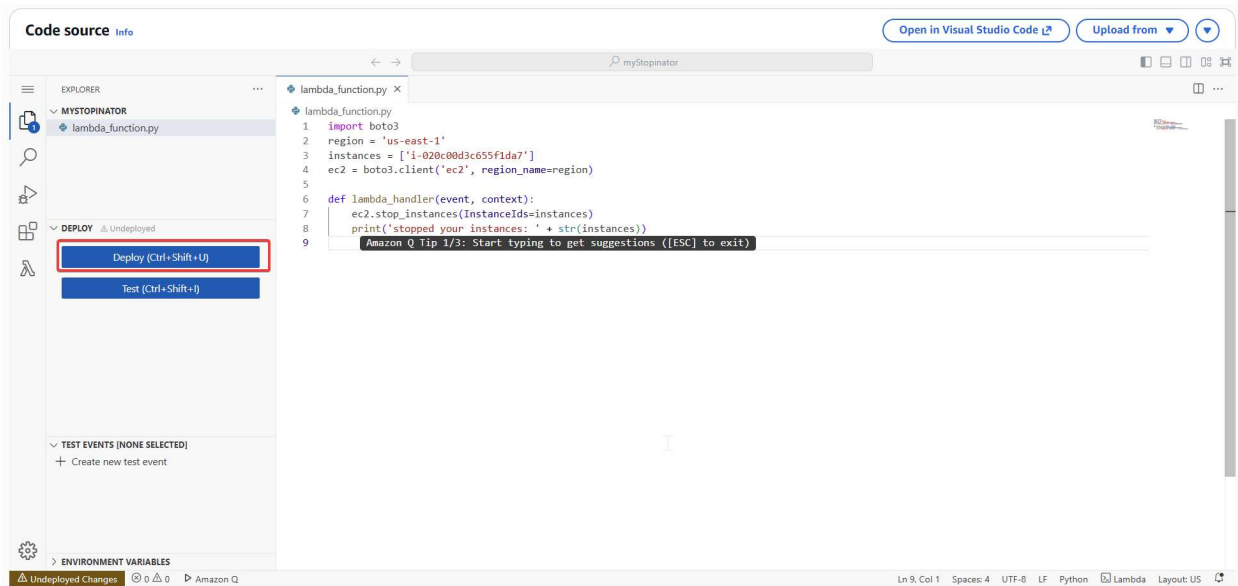
Click “Instances” on the left menu, then copy the Instance ID of “instance1”



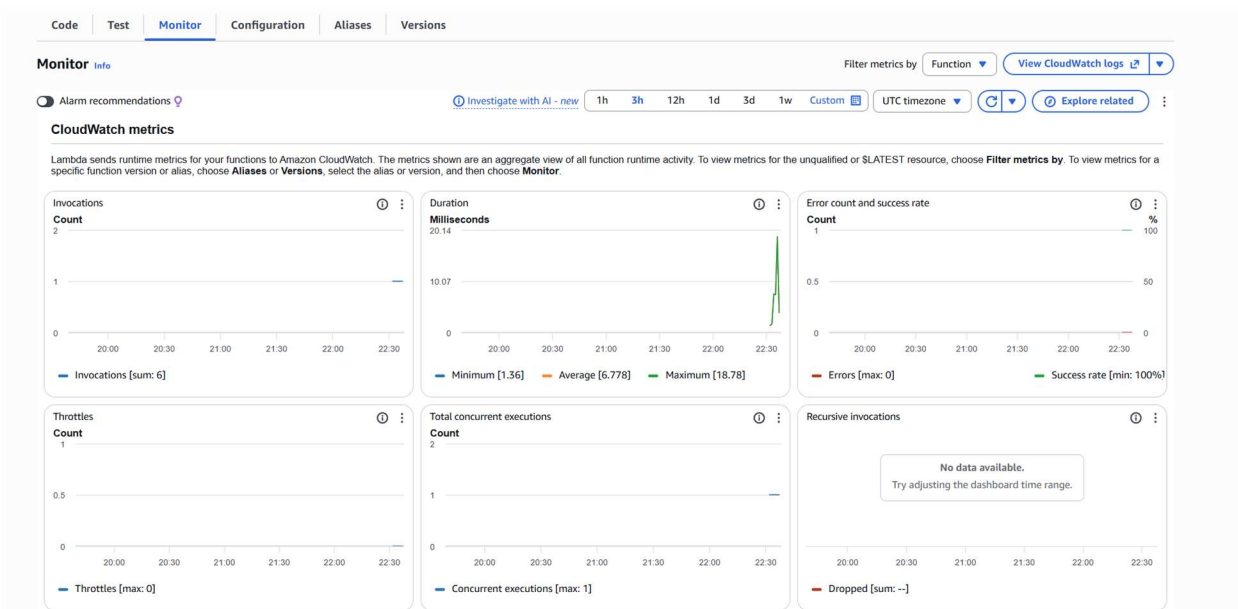
Copy this instance ID to the code



Click “Deploy”

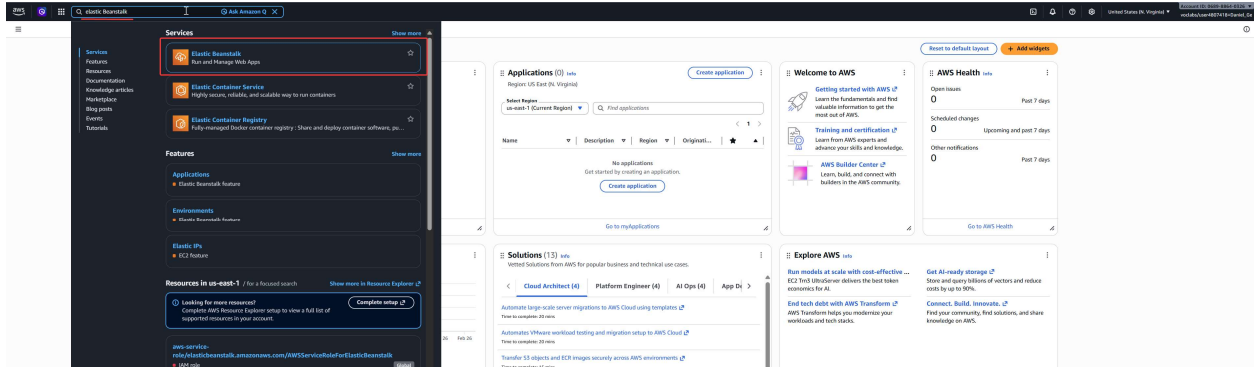


Click the Monitor tab to see if there are any issues reported, as well as other telemetry about how the code is running

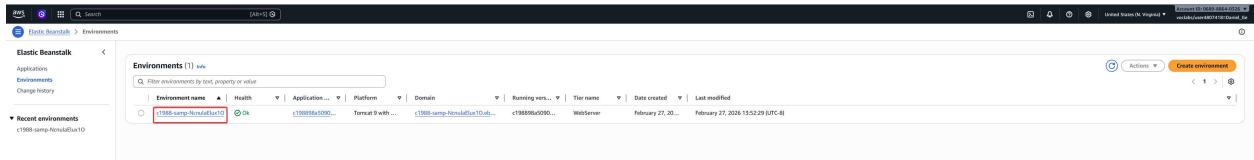


AWS Elastic Beanstalk Activity

In the top-left search bar, search for “Elastic Beanstalk” and click its option to open up the AWS Elastic Beanstalk console



Click the environment name to open the environment menu



Open the Domain link

c1988-samp-ncnulaelux10 Info Actions Upload and deploy

Environment overview

Health
Ok

Domain
c1988-samp-ncnulaelux10.eba-t3aigznm.us-east-1.elasticbeanstalk.com

Environment ID
e-ff692burmh

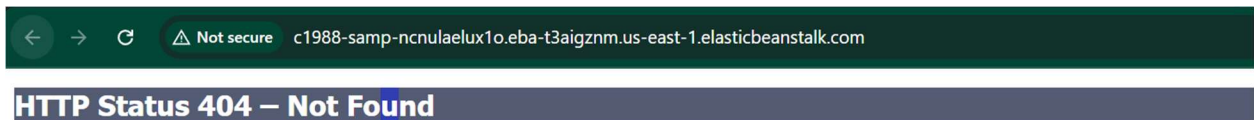
Application name
c198898a5090322113984528t1w068988640326-sampleApplication-MXTJAMNLJ4OT

Platform
Tomcat 9 with Corretto 11 running on 64bit Amazon Linux 2023/5.11.0

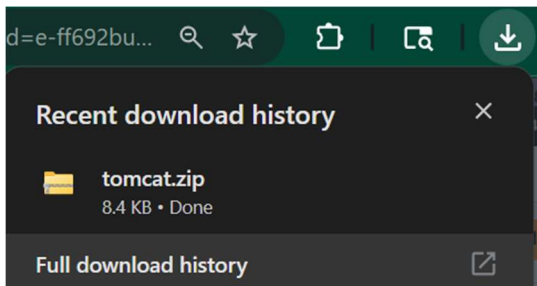
Running version
c198898a5090322113984528t1w068988640326-sampleapplicationversion-yxvpcnrrqdk

Platform state
Supported

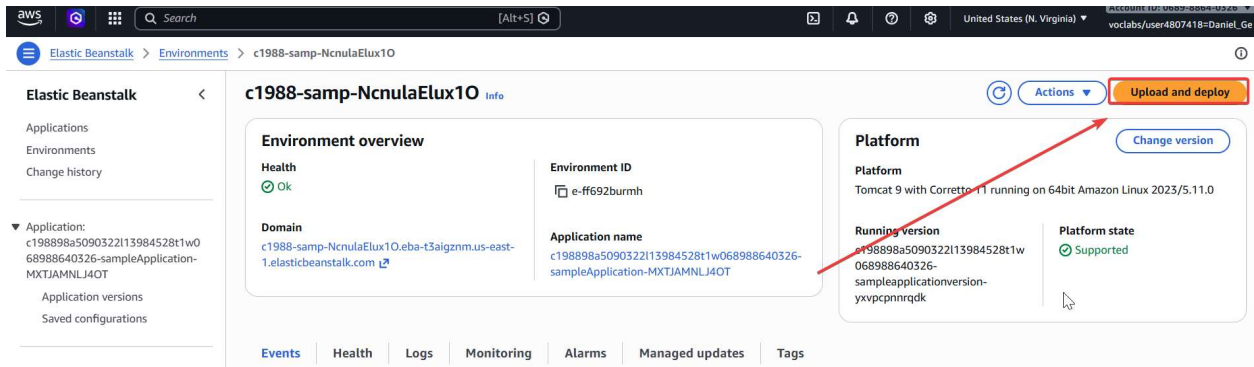
Since the server doesn't have any application yet, the webpage should display Error 404



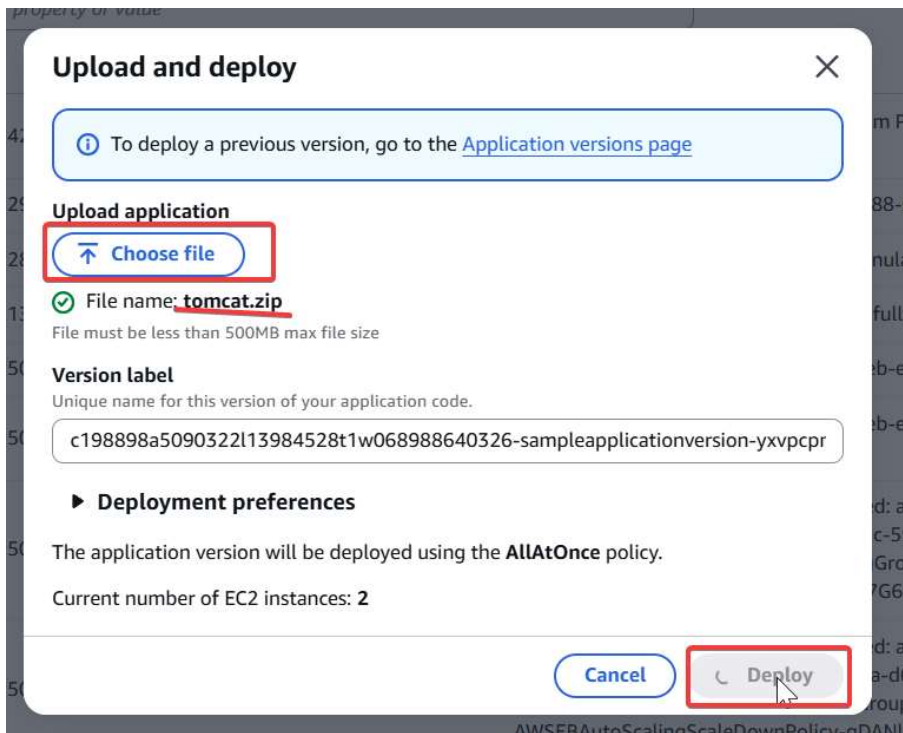
To practice deploying application on AWS Elastic Beanstalk, download a sample application from docs.aws.amazon.com/elasticbeanstalk/latest/dg/samples/tomcat.zip



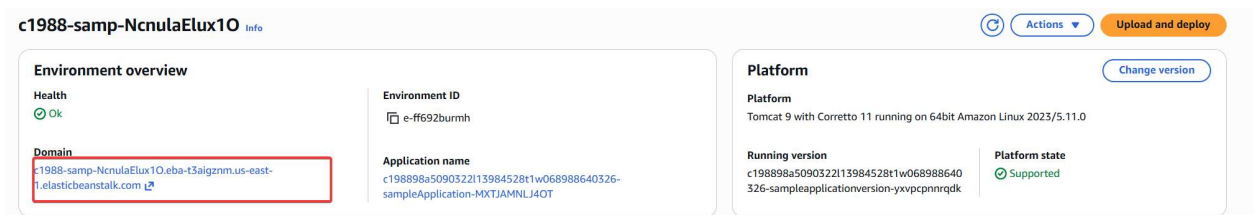
Click "Upload and Deploy"

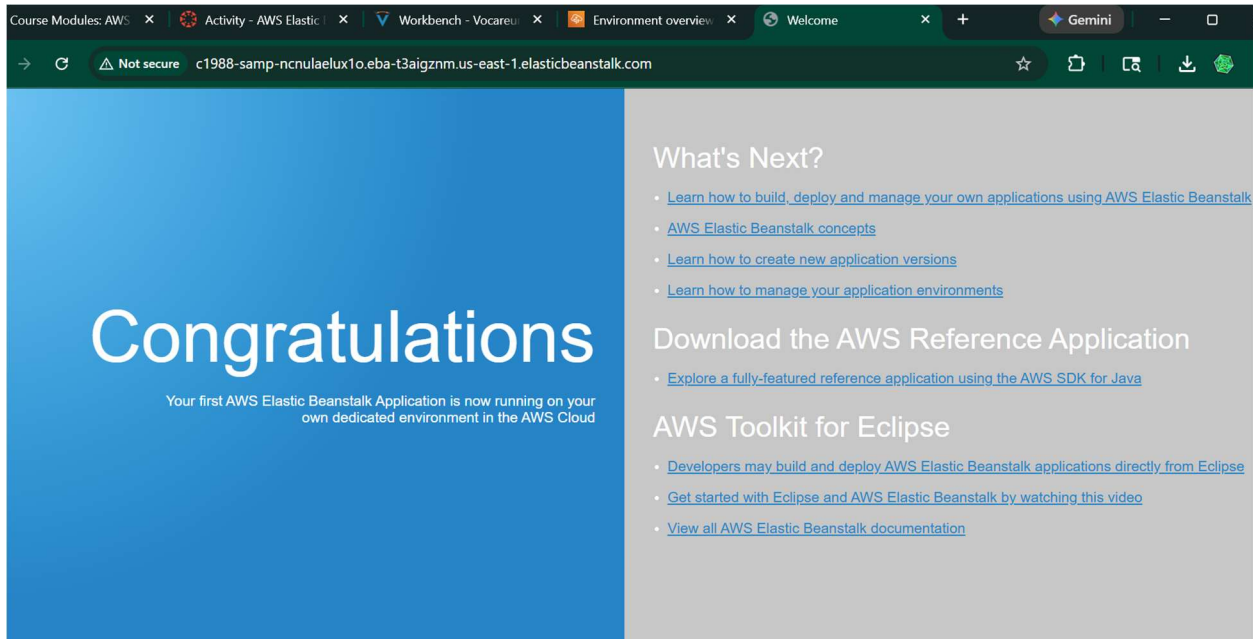


Click “Choose file” and select the recently downloaded tomcat.zip file, then click “Deploy”

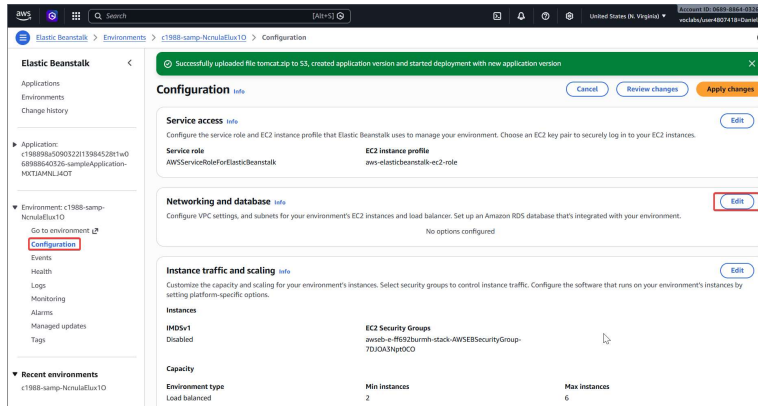


Reopen the domain link and verify that the website now shows a successful page





Go to the Configuration tag menu, then click “Edit”



We may configure the Instance setting in this tab. Click “Cancel” to return to the menu.

Configure networking and database [Info](#)

Instance settings

Choose a subnet in each AZ for the instances that run your application. To avoid exposing your instances to the Internet, run your instances in private subnets and load balancer in public subnets. To run your load balancer and instances in the same public subnets, assign public IP addresses to the instances. [Learn more](#)

VPC

Launch your environment in a custom VPC instead of the default VPC. You can create a VPC and subnets in the VPC management console. [Learn more](#)

[Create VPC](#)

Public IP address

Assign a public IP address to the Amazon EC2 instances in your environment.

Enable

Instance subnets

Availability Zone	Subnet	CIDR	Name
-------------------	--------	------	------

No instance subnets
No instance subnets to display

Database [Info](#)

Integrate an RDS SQL database with your environment. [Learn more](#)

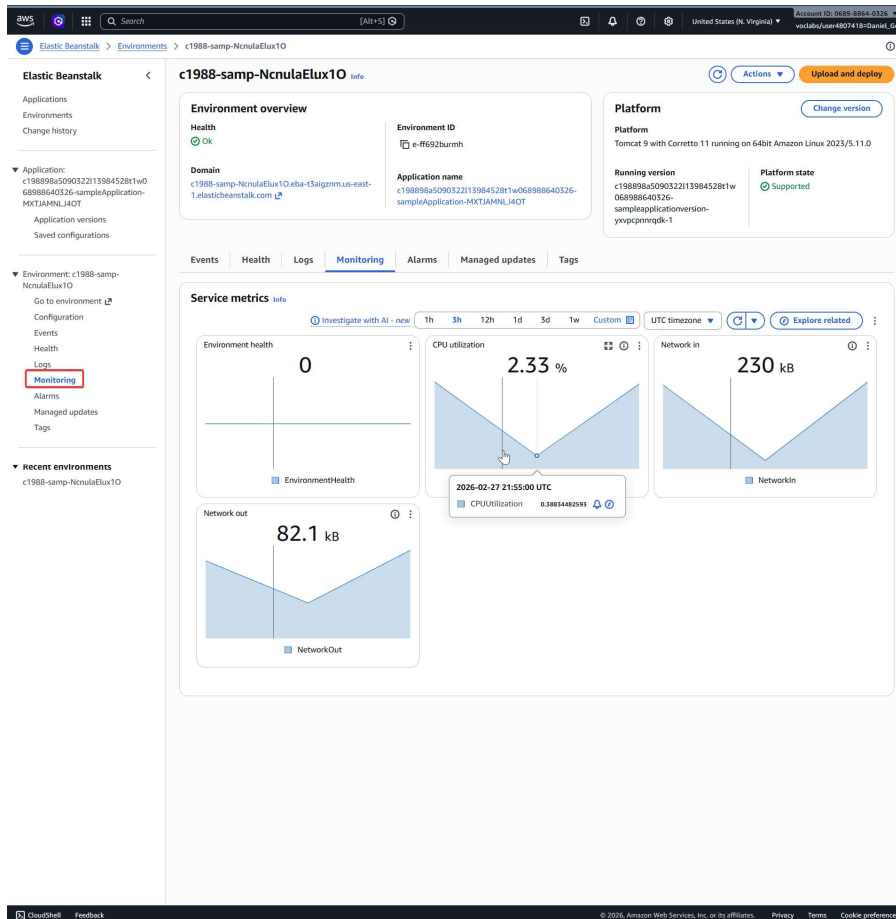
Enable database

Cancel

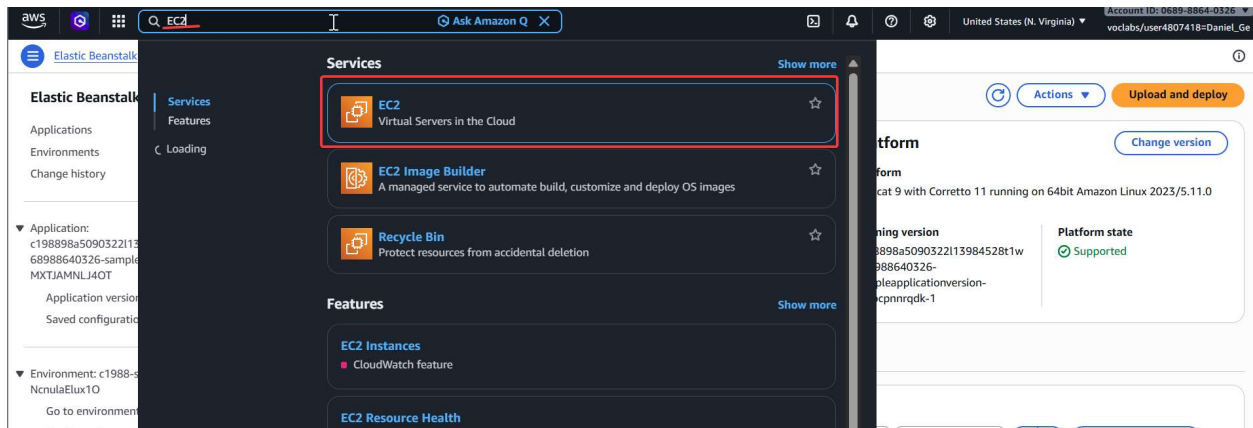
Continue

Apply

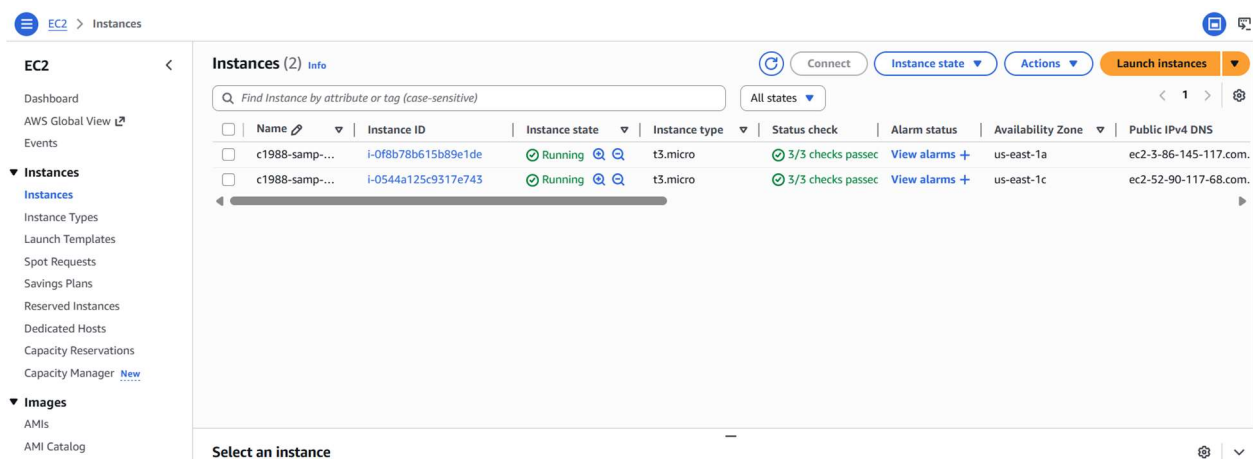
To view telemetry about the application, click the Monitoring tab



Using the search bar, navigate to the EC2 dashboard



Here, we may find more information about the instances launched



Problems

At the end of lab 2, I observed that I could not access the website we launched, receiving a request timeout error. This was due to the permissions being set up in such a way that requests from HTTPS were not permitted, hence an expected failure. In a later lab, this was addressed and I was able to access the desired website.

When attempting to complete multiple labs on the same day, I encountered an error when trying to open the second lab. This problem was due to AWS refusing to open multiple test accounts in rapid succession. The problem was fixed once I moved to a different browser application.

Conclusion

Through the experience of completing Labs 1, 2, and 3, including the encounter of occasional errors which needed troubleshooting, we gain a better understanding of how web services and cloud services operating on AWS are run. We are better prepared to apply the tools we learned about through the AWS instruction videos in AWS IAM, VPC, and EC2 to real-life applications.