

Purpose:

This lab was an introduction to Amazon IAM (Identity and Access Management), Amazon VPC and Amazon EC2. In the IAM lab we were introduced to IAM where to find users and group and how we can put users into user groups in order to give them access to different services. VPC was to create our own custom network and launch an EC2 instance from it in order to start a web server. In the EC2 lab we create, edit, monitor and manage an EC2 instance in order to grasp a general understanding of the utility of EC2 instances.

Background Information:

Amazon IAM(Identity and Access Management) is a free AWS service which allows customers to manage employee access to AWS resources and services within the customers AWS cloud. IAM uses Users, Groups, and roles in order to determine which employees have permissions to interact with what AWS resources. This is done by the owners of the cloud adding roles and users to user groups resulting in the users added to the user group gaining the access to whatever the role defines. Anything the role does not define however is implicitly denied by AWS automatically in order to prevent employees from having access to resources they weren't given by the customer.

Amazon EC2 (Elastic Compute Cloud) is a cloud computing service which allows users to rent out virtual servers in the AWS cloud. This virtualization allows for scalability based off the users needs. Users can run various configurations on their EC2 instance such as different instance types, operating systems and storage.

AWS S3 (Simple Storage Service) cloud storage service offered by AWS which offers both scalability and security. S3 allows clients to store and retrieve data stored in the cloud from anywhere and anytime on the web. S3 allows clients to store as much data as they wish while offering redundancy to prevent data loss, this makes S3 a great option for users to store backups and other data they deem important.

Amazon VPC (Virtual Private Cloud) gives users a logically isolated piece of the AWS cloud. Users can use this virtual network in order to

launch their AWS resources such as S3 and EC2. In a VPC, users have control over the network's IP address range, subnets, routing tables, and default gateways. This allows for a high customizable network for users which can be connected to already existing on premise infrastructure owned by the client.

All three of these services are part of the AWS (Amazon Web Services) infrastructure, a cloud service offered on a pay-as-you-go basis.

Lab Summary:

In the first lab we use IAM to add users to user groups. The usage of user groups allows us to control which users have access to which resources and services on our AWS network by added users to a user group with the assigned role. Given 3 users and 3 user groups, each user has to be assigned to a user group which will allow the user to do their "job". Support groups have roles which allow them to view at AWS configurations which admin groups have the permissions to change the configurations and shut down services.

The second lab is about the understanding of VPCs. This lab will guide us though creating a VPC, creating subnets for this VPC, and configuring a security group for this VPC. We will then launch a web server via an EC2 instance on this newly created VPC and test if we can connect to our new web server.

The third lab is the creation, editing, and monitoring of Ec2 instances. In this lab we start by using Amazon EC2 to start a web server then use the Amazon EC2 GUI to monitor the EC2 instance. We will then modify many things about the EC2 instance such as the security group, memory and storage. We will end the lab by testing out termination protection, turning off termination protection, and finally terminating the instance.

Lab Commands:

Lab 1: Introduction to AWS IAM

Users (4) Info									
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.									
Search (1)									
User name	Path	Group:	Last activity	MFA	Password age	Console last sign-in	Access key ID	Active key	
awsstudent	/	✖ Access denied	-	✖ Access denied	✖ Access denied	Create user			
user-1	/spl66/	0	-	-	6 minutes	-	Active - AKIAYAJOU4M...	✓ 6 minut	Edit
user-2	/spl66/	0	-	-	6 minutes	-	Active - AKIAYAJOU4M...	✓ 6 minut	Edit
user-3	/spl66/	0	-	-	6 minutes	-	Active - AKIAYAJOU4M...	✓ 6 minut	Edit

1: Use the navigation panel on the left to navigate to the users menu, click on user-1 and notice how user-1 has no permissions.

user-1 [info](#)

Summary		
ARN arn:aws:iam::550390522644:user/spl66/user-1	Console access ⚠ Enabled without MFA	Access key 1 AKIAYAJOU4MKEHWJ5AFE - Active ⓘ Never used. Created today.
Created December 08, 2023, 06:10 (UTC-08:00)	Last console sign-in ⓘ Never	Access key 2 Create access key

Permissions	Groups	Tags (1)	Security credentials	Access Advisor
Permissions policies (0)				
Permissions are defined by policies attached to the user directly or through groups.				
Filter by Type <input type="text" value="Search"/> <input type="button" value="All types"/> (1)				
Policy name	Type			Attached via
No resources to display				

This will be the same with all other users, you will need to assign users to each user group to gain permissions.

Identity and Access Management (IAM)

IAM > User groups

User groups (3) Info			
A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.			
Search (1)			
Group name	Users	Permissions	Creation time
EC2-Admin	-	0 Defined	8 minutes ago
EC2-Support	-	0 Defined	8 minutes ago
S3-Support	-	0 Defined	8 minutes ago

2: Use the navigation panel on the left to navigate to the user groups menu. Select S3-Support.

S3-Support [Info](#)

User group name	Creation time	ARN
S3-Support	December 08, 2023, 06:10 (UTC-08:00)	arn:aws:iam::550390522644:group/spl66/S3-Support

[Edit](#)

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

No resources to display

[C](#) [Remove](#) [Add users](#)

[Groups](#) [Last activity](#) [Creation time](#)

3: in order to add users to the user group, select users and Add users.

Other users in this account (3)

Search

User name	Groups	Last activity	Creation time
awsstudent	0	None	14 minutes ago
user-1	1	None	15 minutes ago
user-2	1	None	15 minutes ago

[Cancel](#) [Add](#)

4: Select user-1 via the check box and click Add users.

IAM > User groups

User groups (3) Info

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

Search

Group name	Users	Permissions	Creation time
EC2-Admin	0	Defined	8 minutes ago
EC2-Support	0	Defined	8 minutes ago
S3-Support	0	Defined	8 minutes ago

[C](#) [Delete](#) [Create group](#)

5: To add user-2 to EC2-Support, head back to user groups and click on EC2-Support

Summary

User group name EC2-Support	Creation time December 13, 2023, 09:38 (UTC-08:00)	ARN arn:aws:iam::550390522644: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.

< 1 >

<input type="checkbox"/> User name	▲ Groups	Last activity	▼ Creation time
No resources to display			

6: Add users

Add users to EC2-Support Info

Other users in this account (4)

< 1 >

<input type="checkbox"/> User name	▲ Groups	Last activity	▼ Creation time
<input type="checkbox"/> awsstudent		None	8 minutes ago
<input type="checkbox"/> user-1		None	9 minutes ago
<input type="checkbox"/> user-2		None	9 minutes ago
<input type="checkbox"/> user-3		None	9 minutes ago

7: select user-2 via the check box and click add users.

Identity and Access Management (IAM)

IAM > User groups

User groups (3) Info

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

< 1 >

<input type="checkbox"/> Group name	▲ Users	▼ Permissions	▼ Creation time
<input type="checkbox"/> EC2-Admin	0	Defined	8 minutes ago
<input type="checkbox"/> EC2-Support	0	Defined	8 minutes ago
<input type="checkbox"/> S3-Support	0	Defined	8 minutes ago

8: Finally we are going to add user-3 to EC2-admin, navigate to user groups and select EC2-admin

The screenshot shows the AWS IAM Groups page. At the top, there's a summary card for the 'EC2-Admin' group. Below it, tabs for 'Users', 'Permissions', and 'Access Advisor' are visible, with 'Users' being the active tab. Under the 'Users' tab, the heading 'Users in this group (0)' is shown, followed by a note: 'An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.' A search bar and pagination controls (1) are present. A table below lists users, with columns for 'User name' (sorted by creation time), 'Groups', 'Last activity', and 'Creation time'. The table displays the message 'No resources to display'.

9: Add users

The screenshot shows the AWS IAM Users page. The heading 'Other users in this account (4)' is displayed. A search bar and pagination controls (1) are at the top. A table lists four users: 'awsstudent', 'user-1', 'user-2', and 'user-3'. Red arrows point from the left towards the 'user-3' row and from the right towards the 'Add user' button. The table has columns for 'User name', 'Groups', 'Last activity', and 'Creation time'. The 'Add user' button is located at the bottom right of the table.

10: Select user-3 and add user.

EC2-Admin [Info](#)

Summary		Edit												
User group name EC2-Admin	Creation time December 08, 2023, 06:10 (UTC-08:00)	ARN arn:aws:iam::550390522644:group/spl66/EC2-Admin												
Users (1) Permissions Access Advisor														
Users in this group (1) <p>An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.</p> <table border="1"> <thead> <tr> <th>Search</th> <th>Groups</th> <th>Last activity</th> <th>Creation time</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/> User name</td> <td>1</td> <td>None</td> <td>15 minutes ago</td> </tr> <tr> <td><input type="checkbox"/> user-3</td> <td></td> <td></td> <td></td> </tr> </tbody> </table>			Search	Groups	Last activity	Creation time	<input type="checkbox"/> User name	1	None	15 minutes ago	<input type="checkbox"/> user-3			
Search	Groups	Last activity	Creation time											
<input type="checkbox"/> User name	1	None	15 minutes ago											
<input type="checkbox"/> user-3														

We should now have users in the respective user groups as shown above.

Note: there is a difference between the permissions between admin and permission groups

Failed to stop the instance i-0635fb6b184eb5e4

You are not authorized to perform the operation. User: arn:aws:iam::550390522644:user/spl66/user-2 is not authorized to perform: ec2:StopInstances on resource: arn:aws:ec2:us-east-1:550390522644:instance/i-0635fb6b184eb5e4 because no identity-based policy allows the ec2:StopInstances action. Encoded authorization failure message: MIG6ObCWS52l6w0Pzp_kxS9yGgrVkkIYrWmW2Jsd0aBsjQ4-S1BQTKWbloucQ-kodcvPhba_6EWkbh0b55s359OEcdh9wfyXbyTawg3y27Hdz0CO_X6gZ8Kxx18r-NYKUJhnduFQET5uZB8ldNk5o0nWUxrmf-IKbksu5oU73VCKnxMeMyJ7h2v9pkk5SHmsq0UBa_0KJGGprAjqWQDwch0LsJuEPqkJEPrPsw0bNgb8e9VZFrPs8koAu_elhuxzdF8f6pRjXGAXEBhrJiglqbzZvd5mqbdM4_EoR7-yqZMwl-aw0O0tgYg8L2w7CSImOwXx_m4ToPKKHx4eDalEEmpoIMxLp_lUFXCySheseqCp73klyVucKzGywKTUy26HO6NObscCg20XFHo_um5sgfTD_UbzT9-jnQzhGhqQLS8s5A4w1yf2_IHGp3hp15Xs-uJyOAypbz-TTaD0Gh7782kjwD2eY5dhe59VtYDbnrgfWkzGtyv8GwCr6KKLo_Slu_pKUD1808_Xzzppvh4FetT93b701NqtlPhg9gc5fEGoSgqUNd8cmZ4eo80OW0i4kzykT5tCluchPfa__TR60108hgSPfntlRQAoQsnNFJFV91N8Q8o9skfjf5QRRIHoSz2t:z3pQ8Jrmvg8l1343F1qkBY_QvnR0gPWWbj1HmWvY1VsukrLdMePpqkDlQotbJh-a1ElM3W4ms5xRIMjupowhoym3fIKNqQGSwsrSVyAwpelJ23iP-yqkfrDQ0QavIDSJa2zTlQlJ24q-ReK-F9KZC20SY2-tc6GMZMmJUJ57otoByuoR5ipZ1f4qXglr1aBxmrx271dTWTSPW55mrhblMPBLG1_w-LXL4l6JhwqEmmqJpTQzJx18EyovRAb55M2Rdfqvqwg3nPiPj0CpJ7s6Ygy5RNNUQynpJ1MqjU9JPy00J_BCHQ

Instances (1/2) Info		C	Connect	Instance state	Actions	Launch instances
<input type="checkbox"/> Find Instance by attribute or tag (case-sensitive)				Stop instance		
<input type="checkbox"/>	Name A D	Instance ID	Instance state A D	Instance type A D	Status check A D	Alarm status A D
<input type="checkbox"/>	Bastion Host	i-05154beaba8596991	Running Q Q	t2.micro	2/2 checks passed	No alarms +
<input checked="" type="checkbox"/>	LabHost	i-0635fb6b184eb5e4	Running Q Q	t2.micro	2/2 checks passed	No alarms +
				Start instance	Public IPv4 ...	Elastic IP
				Reboot instance	54.167.127.200	-
				Hibernate instance	54.196.148.39	-
				Terminate instance		

As you can see, user-2 which is under the EC2-support user group cannot stop EC-2 instances unlike user-3 which is under EC2-admin

Successfully stopped i-0635fb6b184eb5e4

Instances (1/2) Info		C	Connect	Instance state	Actions	Launch instances
<input type="checkbox"/> Find Instance by attribute or tag (case-sensitive)				Stop instance		
<input type="checkbox"/>	Name A D	Instance ID	Instance state A D	Instance type A D	Status check A D	Availability Zone A D
<input type="checkbox"/>	Bastion Host	i-05154beaba8596991	Running Q Q	t2.micro	2/2 checks passed	us-east-1a
<input checked="" type="checkbox"/>	LabHost	i-0635fb6b184eb5e4	Stopping Q Q	t2.micro	2/2 checks passed	us-east-1a
				Start instance	Public IPv4 ...	Elastic IP
				Reboot instance	54.167.127.200	-
				Hibernate instance	54.196.148.39	-
				Terminate instance		

Storage

Amazon S3

Store and retrieve any amount of data from anywhere

Amazon S3 is an object storage service that offers industry-leading scalability, data availability, security, and performance.

Create a bucket

How it works

Introduction to Amazon S3

Copy link

aws.amazon.com/S3

Pricing

With S3, there are no minimum fees. You only pay for what you use. Prices are based on the location of your S3 buckets.

Estimate your monthly bill using the [AWS Simple Monthly Calculator](#).

[View pricing details](#)

Resources

User guide

API reference

FAQs

If either user-2 or user-3 try to access S3 like user-1, they will be presented with the screen above instead of a GUI as they don't have access to AWS S3.

Lab 2: Build your VPC and Launch a Web Server

Search results for 'vpc'
Try searching with longer queries for more relevant results

See all 12 results

Services

- VPC ☆ Isolated Cloud Resources
- AWS Firewall Manager ☆ Central management of firewall rules
- Detective ☆ Investigate and Analyze potential security issues
- Managed Services ☆ IT operations management for AWS

Features

- Dashboard ☆ VPC feature
- Route 53 VPCs ☆ Route 53 feature

See all 57 results

VPC dashboard

EC2 Global View

Filter by VPC:

Select a VPC

Virtual private cloud

Your VPCs

Subnets

Route tables

Internet gateways

Egress-only internet gateways

Carrier gateways

DHCP option sets

Elastic IPs

Managed prefix lists

Endpoints

Endpoint services

NAT gateways

Peering connections

Security

Network ACLs

Security groups

1: Use the search bar in the top left to search for the Amazon VPC service.

The screenshot shows the AWS VPC dashboard. On the left, there's a sidebar with options like 'VPC dashboard', 'EC2 Global View', 'Filter by VPC' (with a dropdown menu), and 'Virtual private cloud' (with sub-options: 'Your VPCs', 'Subnets', and 'Route tables'). The main area has a title 'Resources by Region' with a 'Refresh Resources' button. Below it, a note says 'You are using the following Amazon VPC resources'. There are two boxes: one for 'VPCs' (with 'See all regions' link) and one for 'NAT Gateways' (with 'See all regions' link). At the top right, there are 'Create VPC' and 'Launch EC2 Instances' buttons, with a note below stating 'Note: Your Instances will launch in the US East region.'

2: On the VPC dashboard, select Create VPC.

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

- 3: Ensure these settings are correct:
 Select VPC and more
 check Auto-generate name tag but type in “lab”
 keep the Ipv6 CIDR block as 10.0.0.0/16

keep the number of Availability zones as 1.

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
---	---	---

▼ 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 (\$) [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](#) [Create VPC](#)

4: make sure these configurations are correct:

Number of public subnets: 1

Number of private subnets: 1

Public subnet CIDR: 10.0.0.0/24

Private subnet CIDR: 10.0.1.0/24

NAT gateways: In 1 AZ

VPC endpoints: None

And keep both DNS hotnames and DNS resolutions as enabled

5: Click create VPC



5: Ensure the preview panel has the same setting as this, and click Create VPC.

The screenshot shows the AWS VPC dashboard. On the left, a sidebar lists various VPC components like Subnets, Route tables, Internet gateways, etc. The main area displays a VPC named 'vpc-Odc5826763c703336 / lab-vpc'. The 'Details' tab is active, showing the VPC ID as 'vpc-Odc5826763c703336', state as 'Available', and other settings. The 'Resource map' tab shows the VPC structure with subnets, route tables, and network connections.

6: Select Subnets under Virtual private cloud

Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR
Work Public Subnet	subnet-0099de7ae01119ab	Available	vpc-046e386e187d0c3ea	172.51.10.0/20	-
lab-subnet-public1-us-east-1a	subnet-00703f16a8990998	Available	vpc-04fc5926763c703336e1ubb...	10.0.0.0/24	-
-	subnet-0f65fe1a510c5754	Available	vpc-036fb538ec187d0c3ea	172.51.48.0/20	-
-	subnet-040c285773170725	Available	vpc-036fb538ec187d0c3ea	172.31.16.0/20	-
lab-subnet-private1-us-east-1a	subnet-09f20b26085b577a7	Available	vpc-036fb538ec187d0c3ea	172.31.99.0/20	-
-	subnet-08029e1d8cc0cf5	Available	vpc-036fb538ec187d0c3ea	172.31.64.0/20	-
-	subnet-041dfbbbf6acd496cb	Available	vpc-036fb538ec187d0c3ea	172.31.82.0/20	-

7: Select Create subnet

VPC

VPC ID: lab-vpc
Create subnets in this VPC
Subnet CIDR: 10.0.0.0/16

Associated VPC CIDRs:
IPV4 CIDRs: 10.0.0.0/16

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

Subnet 1 of 1

Subnet Name: lab-subnet-public1
The name can be up to 256 characters long.

Availability Zone: us-east-1a
The zone where your subnet will reside, or let Amazon choose one for you.
Use last (N. Virginia) / us-east-1a

IPv4 CIDR: Use this VPC CIDR block to create a subnet in:
10.0.0.0/16

IPv4 subnet CIDR block: 10.0.2.0/24 (256 IPs)

Tags (optional):
Key: Name Value: lab-subnet-public1
Add new tag
Remove

Add new subnet

Cancel Create subnet

This screenshot shows the 'Create subnet' dialog box within the AWS VPC service. At the top, it displays the VPC ID 'lab-vpc' and its CIDR block '10.0.0.0/16'. Below this, the 'Subnet settings' section is visible, specifically for 'Subnet 1 of 1'. It includes fields for the subnet name ('lab-subnet-public1'), availability zone ('us-east-1a'), and the IPv4 CIDR block ('10.0.2.0/24'). A 'Tags' section is present, showing a single tag 'Name' with the value 'lab-subnet-public1'. At the bottom right, there are 'Cancel' and 'Create subnet' buttons.

8: Configure the VPC ID with the lab-vpc

VPC

VPC ID

Create subnets in this VPC.

vpc-0dc5826763c703336 (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-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 IPv4 VPC CIDR block to create a subnet in.

10.0.0.0/16 ▾

IPv4 subnet CIDR block

10.0.2.0/24

256 IPs

< > ^ ▾

▼ Tags - optional

Key

Q Name

Value - optional

Q lab-subnet-public2

Remove

Add new tag

You can add 49 more tags.

Remove

Add new subnet

Cancel

Create su

9: Configure:

Subnet name: lab-subnet-public2

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

Ipv4 subnet CIDR block: 10.0.2.0/24

Create subnet

10: Repeat and configure:

VPC ID: lab-vpc

Subnet name: lab-subnet-private2

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

IPv4 subnet CIDR block: 10.0.3.0/24

Create subnet

The screenshot shows the AWS VPC dashboard with the 'Route tables' section selected. On the left, there's a sidebar with various VPC-related options like Your VPCs, Subnets, Route tables, Internet gateways, etc. The main area displays a list of route tables with their names: lab-rtb-public, lab-rtb-private1-us-east-1a, Work Public Route Table, and three unnamed entries. Below the list is a large button labeled 'Select a route table'.

11: Navigate to Route tables and select lab-rtb-private1-us-east-1a

This screenshot shows the detailed view of the 'lab-rtb-private1-us-east-1a' route table. The top navigation bar includes tabs for Details, Routes (which is selected), Subnet associations, Edge associations, Route propagation, and Tags. The 'Routes' tab shows two routes: one for 0.0.0.0/0 targeting the nat-0b9bd295a89ef389c instance, and another for 10.0.0.0/16 targeting 'local'. A filter bar at the top of the route table list allows filtering by route name.

12: Select the Routes tab and note the 0.0.0.0/0 subnet is set with the nat Target

13: Select the Subnet associations tab and under Explicit subnet associations, click Edit subnet associations.

14: Keep lab-subnet-private1-us-east-1a but also select lab-subnet-public2 and Save associations

15: Select the lab-rtb-public route table

16: In the lower panel, Destination o.o.o/o is set to target igw

rtb-002e8856bb5159afe / lab-rtb-public

Details	Routes	Subnet associations	Edge associations	Route propagation	Tags
Explicit subnet associations (1)					
<input type="text" value="Find subnet association"/> Edit subr					
Name	▼	Subnet ID	▼	IPv4 CIDR	▼
lab-subnet-public1-us-east-1a		subnet-0070361f6a889d998		10.0.0.0/24	-
Subnets without explicit associations (0)					
The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:					
<input type="text" value="Find subnet association"/> Edit subr					
Name	▼	Subnet ID	▼	IPv4 CIDR	▼
No subnets without explicit associations					
All your subnets are associated with a route table.					

17: Select the Subnet associations tab and under Explicit subnet associations, click Edit subnet associations

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (2/3)					
<input type="text" value="Filter subnet associations"/>					
Name	▼	Subnet ID	▼	IPv4 CIDR	▼
lab-subnet-public1-us-east-1a		subnet-0070361f6a889d998		10.0.0.0/24	-
<input checked="" type="checkbox"/> lab-subnet-public2		subnet-e23fd0465e8a1751		10.0.2.0/24	-
<input checked="" type="checkbox"/> lab-subnet-private1-us-east-1a		subnet-047d81723a2db144d		10.0.1.0/24	-
Selected subnets					
<input style="width: 200px; margin-right: 10px;" type="text" value="subnet-047d81723a2db144d / lab-subnet-private1-us-east-1a"/> <input style="width: 200px; margin-right: 10px;" type="text" value="subnet-e23fd0465e8a1751 / lab-subnet-public2"/> Cancel					

18: Keep lab-subnet-private1-us-east-1a and select lab-subnet-public2. Save associations

NOTE: *image above is NOT accurate to instructions*

You have successfully updated subnet associations for rtb-002e8856bb5159afe / lab-rtb-public.

Route tables (5) Info									
<input type="text" value="Find resources by attribute or tag"/> Actions ▾ Create									
Name	▼	Route table ID	▼	Explicit subnet associati...	Edge associations	Main	▼	VPC	▼
lab-rtb-public		rtb-002e8856bb5159afe		2 subnets	-	No		vpc-0dc5826763c703336 lab-...	413066348106
-		rtb-039e6b894552e1aaaf		-	-	Yes		vpc-05bdd615739698994 Wo...	413066348106
lab-rtb-private1-us-east-1a		rtb-08c2b932ced99d40		subnet-047d81723a2db1...	-	No		vpc-0dc5826763c703336 lab-...	413066348106
-		rtb-0375057c2eae02a9b		-	-	Yes		vpc-0dc5826763c703336 lab-...	413066348106
Work Public Route Table		rtb-0802ff69f069839a		subnet-0695dea7ece111...	-	No		vpc-05bdd615739698994 Wo...	413066348106

You now have updated route tables with additional subnets

The screenshot shows the AWS VPC dashboard. On the left, there is a navigation panel with the following structure:

- VPC dashboard
- EC2 Global View
- Filter by VPC:
 - Select a VPC
- ▼ Virtual private cloud
 - Your VPCs
 - Subnets
 - Route tables
 - Internet gateways
 - Egress-only internet gateways
 - Carrier gateways
 - DHCP option sets
 - Elastic IPs
 - Managed prefix lists
 - Endpoints
 - Endpoint services
 - NAT gateways
 - Peering connections
- ▼ Security
 - Network ACLs
 - Security groups**
- ▼ DNS firewall
 - Rule groups
 - Domain lists

Security Groups (4) Info

Find resources by attribute or tag

<input type="checkbox"/>	Name	▼	Security group ID
<input type="checkbox"/>	-		sg-0ca1e44eddf591
<input type="checkbox"/>	-		sg-0f5802b4072ee1
<input type="checkbox"/>	-		sg-04cf78a30cacb4
<input type="checkbox"/>	-		sg-04c34aabeb040

19: In the navigation panel, select Security groups

Security Groups (4) Info						
<input type="checkbox"/>	Name	Security group ID	Security group name	VPC ID	Description	Owner
<input type="checkbox"/>	-	sg-0ca1e44eddff593954	default	vpc-0dc5826763c703336	default VPC security group	413i
<input type="checkbox"/>	-	sg-0f5802b4072ee0e5a	default	vpc-05bdd615739698994	default VPC security group	413i
<input type="checkbox"/>	-	sg-04cf78a30cacb4aaef	default	vpc-036fb38ea1870c5ca	default VPC security group	413i
<input type="checkbox"/>	-	sg-04c34aabeb0405940	Ec2SecurityGroup	vpc-05bdd615739698994	VPC Security Group	413i

20: Click Create security group

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

21: Configure:

Security group name: Web Security Group

Description: Enable HTTP access

VPC: lab-vpc

Inbound rules [Info](#)

Type Info	Protocol Info	Port range Info	Source Info	Description - optional Info
HTTP	TCP	80	Anywhere... <input type="button" value="▼"/>	<input type="text" value="permit web requests"/> <input type="button" value="X"/>

22: Click add rule and configure:

Type: HTTP

Source: Anywhere-IPv4

Description: Permit web requests

Tags - optional

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

No tags associated with the resource.

You can add up to 50 more tags

23: Click Create security group at the bottom of the page

Security group (sg-07094bb6761a9c7c1) was created successfully

sg-07094bb6761a9c7c1 - Web Security Group

Details

Security group name Web Security Group	Security group ID sg-07094bb6761a9c7c1	Description Enable HTTPS Access	VPC ID vpc-0dc5826763c703336
Owner 413066348106	Inbound rules count 1 Permission entry	Outbound rules count 1 Permission entry	

Inbound rules | Outbound rules | Tags

Inbound rules (1)

Name	Security group rule...	IP version	Type	Protocol	Port range	Source
sgr-070a54e50bb2fa536	IPv4	HTTP	TCP	80	0.0.0.0/0	

You have now created a new security group for your web server in order to be accessed via the internet.

aws Services Search [Alt+S]

Recently visited

Favorites

All services

- Analytics
- Application Integration
- Blockchain
- Business Applications
- Cloud Financial Management
- Compute
- Containers
- Customer Enablement
- Database
- Developer Tools
- End User Computing

Compute

- AWS App Runner**
Build and run production web applications at scale
- Batch**
Fully managed batch processing at any scale
- EC2**
Virtual Servers in the Cloud
- EC2 Image Builder**
A managed service to automate build, customize and deploy OS images
- Elastic Beanstalk**
Run and Manage Web Apps
- Lambda**
Run code without thinking about servers
- Lightsail**
Launch and Manage Virtual Private Servers

24: Select the services menu and go to EC2. You may have to search EC2 in the search bar

The screenshot shows the AWS EC2 Dashboard. On the left, a sidebar lists navigation options: EC2 Global View, Events, Console-to-Code Preview, Instances (with sub-options Instances, Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations), Images (AMIs, AMI Catalog), and Elastic Block Store (Volumes, Snapshots, Lifecycle Manager). The main content area is titled 'Resources' and displays a summary of Amazon EC2 resources in the US East (N. Virginia) Region. It includes tables for Instances (running: 1), Auto Scaling Groups (1, API Error), Dedicated Hosts, Key pairs, and Security groups. Below this is a 'Launch instance' section with a 'Launch instance' button and a note about launching in the US East (N. Virginia) Region. To the right is a 'Service health' section with a link to the AWS Health Dashboard, showing the region as US East (N. Virginia). A 'Zones' table lists three availability zones: us-east-1a (Zone ID: use1-az4), us-east-1b (Zone ID: use1-az6), and us-east-1c (Zone ID: use1-az1).

25: Launch a new instance

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.

This screenshot shows the 'Name and tags' step of the instance launch wizard. It features a 'Name' input field containing 'Web Server 1' and a 'Add additional tags' link.

26: Give the instance the name Web Server 1

▼ 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.

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

Recents Quick Start

Amazon Linux macOS Ubuntu Windows Red Hat SUSE Li  [Browse more AMIs](#)
Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Amazon Linux 2023 AMI Free tier eligible ▾
ami-0759f51a90924c166 (64-bit (x86), uefi-preferred) / ami-0f8faf5bcc2ac44e5 (64-bit (Arm), uefi)
Virtualization: hvm ENA enabled: true Root device type: ebs

Description
Amazon Linux 2023 AMI 2023.3.20231211.4 x86_64 HVM kernel-6.1

Architecture Boot mode AMI ID
64-bit (x86) ▾ uefi-preferred ami-0759f51a90924c166 Verified provider

27: Configure Quick start to Amazon Linux and ensure Amazon Linux 2023 AMI

The screenshot shows the AWS Lambda 'Create Function' configuration interface. The 'Instance type' section is expanded, showing the 't2.micro' option selected. The 'Key pair (login)' section is also expanded, showing 'vokey' as the selected key pair name.

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

Instance type

t2.micro Free tier eligible

Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Windows base pricing: 0.0162 USD per Hour
On-Demand SUSE base pricing: 0.0116 USD per Hour
On-Demand RHEL base pricing: 0.0716 USD per Hour
On-Demand Linux base pricing: 0.0116 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*

[Create new key pair](#)

28: Configure the instance type to t2.micro and the Key pair name to vokey

The screenshot shows the 'Network settings' section of the AWS EC2 instance configuration. It includes fields for VPC (set to 'lab-vpc'), Subnet ('lab-subnet-public2'), Auto-assign public IP (set to 'Enable'), and Firewall (set to 'Select existing security group'). A common security group 'Web Security Group' is selected.

VPC - required [Info](#)
vpc-0dc5826763c703336 (lab-vpc)
10.0.0.0/16

Subnet [Info](#)
subnet-0e23fd0465e8a1751 lab-subnet-public2
VPC: vpc-0dc5826763c703336 Owner: 413066348106
Availability Zone: us-east-1b IP addresses available: 251 CIDR: 10.0.2.0/24

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

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-07094bb6761a9c7c1 [X](#)

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

Advanced network configuration

29: Click Edit in Network settings then configure:

VPC: lab-vpc

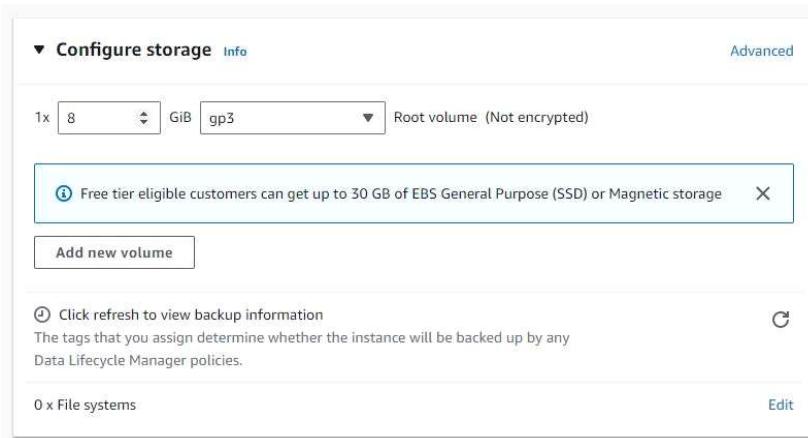
Subnet: lab-subnet-public2

Auto-assign public IP: Enable

Firewall: Select existing security group

Common security groups: Web Security Group

This will allow HTTP access to the EC2 web sever



30: Keep the default storage settings

User data - *optional* | [Info](#)
Upload a file with your user data or enter it in the field.

[Choose file](#)

```
#!/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
```

User data has already been base64 encoded

31: At the bottom of the page, paste this script into the User data box:

```
#!/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
```

At the bottom, click Launch instance

Success
Successfully initiated launch of instance (i-0796be240a7b76ec4)

▶ Launch log

Next Steps

Q. What would you like to do next with this instance, for example "create alarm" or "create backup"

< 1 2

Create billing and free tier usage alerts To manage costs and avoid surprise bills, set up email notifications for billing and free tier usage thresholds. Create billing alerts	Connect to your instance Once your instance is running, log into it from your local computer. Connect to instance Learn more	Connect an RDS database Configure the connection between an EC2 instance and a database to allow traffic flow between them. Connect an RDS database Create a new RDS database Learn more	Create EBS snapshot policy Create a policy that automates the creation and deletion of EBS snapshots. Create EBS snapshot policy
Manage detailed monitoring Enable or disable detailed monitoring for the instance. If you enable detailed monitoring, the Amazon EC2 console displays monitoring graphs with a 1-minute period. Manage detailed monitoring	Create Load Balancer Create a application, network gateway or classic Elastic Load Balancer. Create Load Balancer	Create AWS budget AWS Budgets allows you to create budgets, forecast spend, and take action on your costs and usage from a single location. Create AWS budget	Manage CloudWatch alarms Create or update Amazon CloudWatch alarms. Manage CloudWatch alarms

You now have launched a web server via EC2, click [View all instances](#)

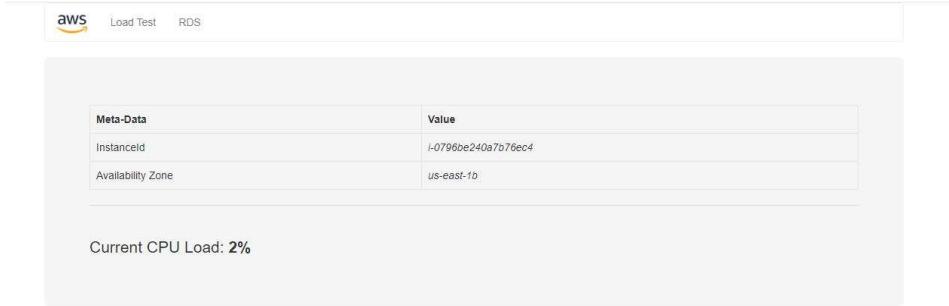
Instances (1/2) Info										
Find Instance by attribute or tag (case-sensitive) Connect Instance state ▾ Actions ▾ Launch										
Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Public IPv4 ...	Public IPv4 ...
<input checked="" type="checkbox"/> Web Server 1	i-0796be240a7b76ec4	Running	t2.micro	2/2 checks passed	No alarms	+ us-east-1b	ec2-174-129-107-42.co...	174.129.107.42		
<input type="checkbox"/> Bastion Host	i-0ee2c8d0dfb1c6623	Running	t2.micro	2/2 checks passed	No alarms	+ us-east-1a	ec2-18-205-18-207.co...	18.205.18.207		

32: Once Web Server 1 have shows 2/2 checks passed in the Status check column. Select Web Sever 1

Instance: i-0796be240a7b76ec4 (Web Server 1)

Instance ID i-0796be240a7b76ec4 (Web Server 1)	Public IPv4 address 174.129.107.42 [open address]	Private IPv4 addresses 10.0.2.130
IPv6 address -	Instance state Running	Public IPv4 DNS ec2-174-129-107-42.compute-1.amazonaws.com [open]
Hostname type IP name: ip-10-0-2-130.ec2.internal	Private IP DNS name (IPv4 only) ip-10-0-2-130.ec2.internal	Elastic IP addresses -
Answer private resource DNS name -	Instance type t2.micro	AWS Compute Optimizer finding X User: arn:aws:sts::413066348106:assumed-role/voclabs/us-huk is not authorized to perform: compute-optimizer:GetEligibleStatus action source: * because no identity-based policy allows the compute-optimizer:GetEligibleStatus action Retry
Auto-assigned IP address 174.129.107.42 [Public IP]	VPC ID vpc-0dc5826763c703336 (lab-vpc)	Auto Scaling Group name -
IAM Role -	Subnet ID subnet-0e23fd0465e8a1751 (lab-subnet-public2)	
IMDVCu?		

33: Copy the Public IPv4 DNS address into a web browser. (Chrome, Firefox, Edge)



You now can access your web server.

LAB 3: Introduction to Amazon EC2

The screenshot shows the AWS Management Console Services menu. Under the 'Compute' section, it lists 'AWS App Runner', 'Batch', 'EC2', 'EC2 Image Builder', and 'Elastic Beanstalk'. On the right, there is a summary for EC2: '0 Dedicated Hosts', '1 Key pairs', '4 Security groups', and a link to 'AWS Health Dashboard'. A note indicates '0 EC2 free tier offers in use'.

1: In the AWS Management Console, choose Services> Compute > EC2

The screenshot shows the 'Launch instance' page. It has a heading 'Launch instance' and a note: 'To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.' Below this are two buttons: 'Launch instance' (highlighted in orange) and 'Migrate a server'. A note at the bottom states: 'Note: Your instances will launch in the US East (N. Virginia) Region'.

Name and tags [Info](#)

Name
Web Server [Add additional tags](#)

▼ 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

[Search our full catalog including 1000s of application and OS images](#)

[Recents](#) [Quick Start](#)

[Amazon Linux](#) [macOS](#) [Ubuntu](#) [Windows](#) [Red Hat](#) [SUSE Li](#)

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

Amazon Machine Image (AMI)

Amazon Linux 2023 AMI ami-079db87dc4c10ac91 (64-bit (x86), uefi-preferred) / ami-02cd6549baea35b55 (64-bit (Arm), uefi) Virtualization: hvm ENA enabled: true Root device type: ebs	Free tier eligible ▼
---	--------------------------------------

Description
Amazon Linux 2023 AMI 2023.3.20231218.0 x86_64 HVM kernel-6.1

2: Click

Launch instance

3: Name the instance Web Server and Select Amazon Linux under AMI. Keep the default Amazon Linux 2023 AMI

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

t2.micro [Free tier eligible](#)

Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Windows base pricing: 0.0162 USD per Hour
On-Demand RHEL base pricing: 0.0162 USD per Hour
On-Demand RHEL Linux base pricing: 0.0116 USD per Hour
On-Demand Linux base pricing: 0.0116 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 [Create new key pair](#)

3: Select the Instance type as t2.micro and Key pair as vokey

Network settings [Info](#)

VPC - required [Info](#)

vpc-000fef1e4d8905350 (Lab VPC)
10.0.0.0/16

Subnet [Info](#)

subnet-0d87f5048b33b8de6 Public Subnet 2
VPC: vpc-000fef1e4d8905350 Owner: 775815040940 Availability Zone: us-east-1b
IP addresses available: 251 CIDR: 10.0.2.0/24

[Create new subnet](#)

Auto-assign public IP [Info](#)

Enable

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 Sever 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	Protocol	Port range
ssh	TCP	22

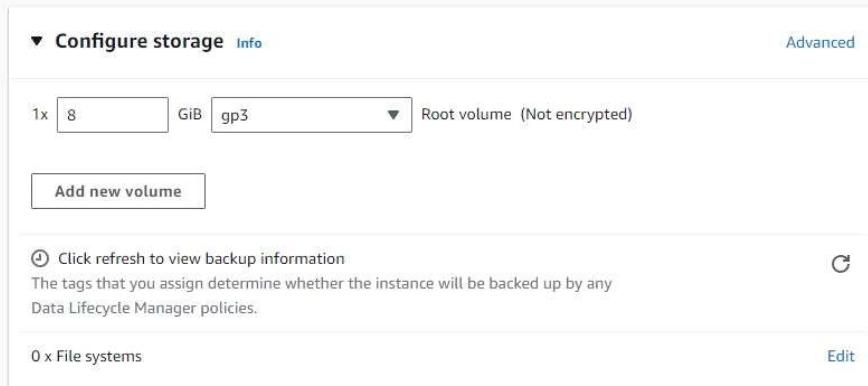
Source type	Source	Description - optional
Anywhere	Add CIDR, prefix list or security	e.g. SSH for admin desktop

4: Under Network settings configure:

VPC: Lab VPC

Subnets: Public Subnet 2

Auto-assign public IP: Enable
Firewall: Create security group
Name: Web Server security group
Description: Security Group for my Web Server
Remove the default Inbound Security Group Rule



The screenshot shows the 'Configure storage' section of the AWS Lambda console. It displays a single root volume configuration: 1x 8 GiB gp3. The volume is labeled as 'Root volume (Not encrypted)'. There is a link to 'Add new volume'. A note at the bottom says 'Click refresh to view backup information' and 'The tags that you assign determine whether the instance will be backed up by any Data Lifecycle Manager policies.' There is also a note about '0 x File systems' and an 'Edit' button.

5: Keep the default storage settings

▼ 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

6: Expand the Advanced details tab and enable Termination Protection

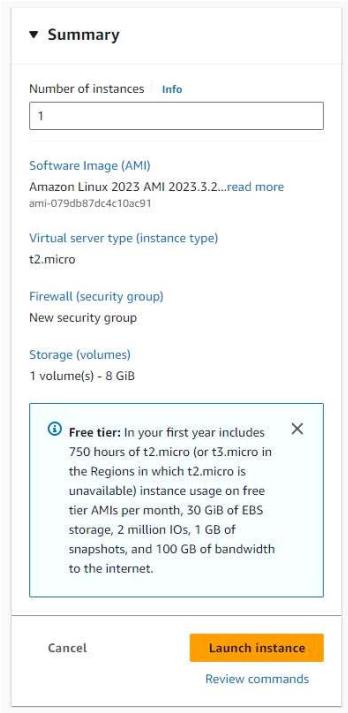
User data - *optional* [Info](#)
Upload a file with your user data or enter it in the field.

```
#!/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 has already been base64 encoded

7: Scroll all the way down to User data and paste this code into the box:

```
#!/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
```



8: Click Launch instance under summary

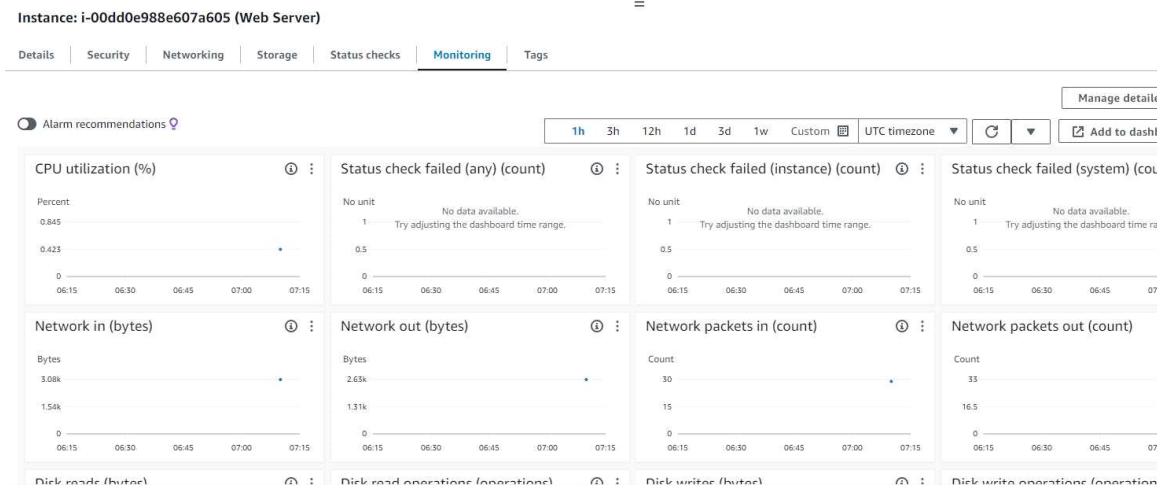
Instances (2) <small>Info</small>									
<input type="text"/> Find Instance by attribute or tag (case-sensitive)									
	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4...
<input type="checkbox"/>	Web Server	i-00dd0e988e607a605	Running	t2.micro	2/2 checks passed	No alarms	+ us-east-1b	ec2-44-203-40-142.co...	44.203.40.1...
<input type="checkbox"/>	Bastion Host	i-0826bac3fb3915f5	Running	t2.micro	2/2 checks passed	No alarms	+ us-east-1a	ec2-34-234-234-148.co...	34.234.234...

9: Wait for 2/2 checks passed for Web Server

Instance: i-00dd0e988e607a605 (Web Server)

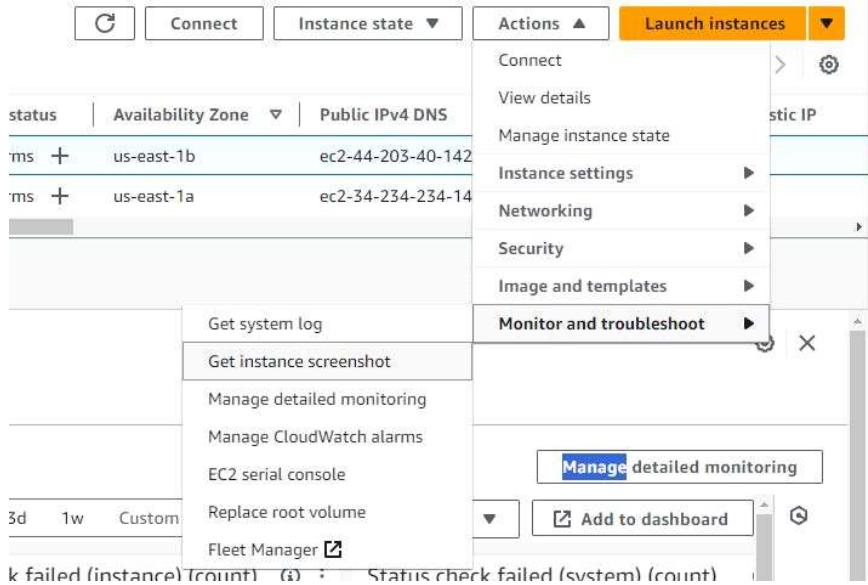
Details	Security	Networking	Storage	Status checks	Monitoring	Tags
Status checks: Info <small>Status checks detect problems that may impair i-00dd0e988e607a605 (Web Server) from running your applications.</small>						
System status checks (✓) System reachability check passed				Instance status checks (✓) Instance reachability check passed		

10: Click your Web Server Instance and then in the lower panel, select the Status checks tab



11: Now select the Monitoring tab

Note here that you can expand the charts by clicking the 3 dots icon at the top right of each chart.



12: Near the top of the screen select the Actions menu > Monitor and troubleshoot>Get instance log

Get system log [Info](#)

When you experience issues with your EC2 instance, reviewing system logs can help you pinpoint the cause.

System log

Review system log for instance i-00dd0e988e607a605 as of Tue Jan 02 2024 23:23:09 GMT-0800 (Pacific Standard Time)

```

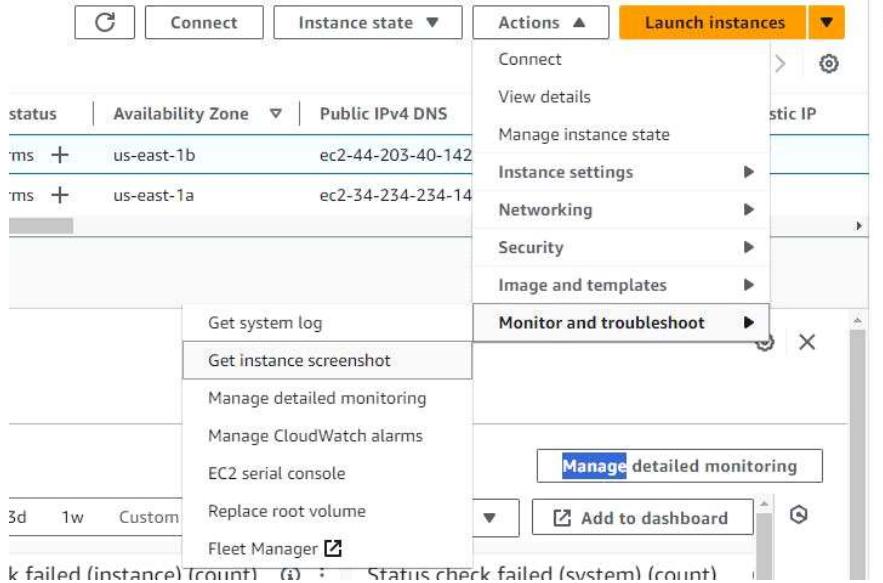
[ 28.971254] cloud-init[2284]: Running transaction test
[ 29.440076] cloud-init[2284]: Transaction test succeeded.
[ 29.447439] cloud-init[2284]: Running transaction
[ 29.755379] cloud-init[2284]: Preparing : 1/1
[ 29.789644] cloud-init[2284]: Installing : apr-1.7.2-2.amzn2023.0.2.x86_64 1/12
[ 29.810180] cloud-init[2284]: Installing : apr-util-openssl-1.6.3-1.amzn2023.0.1.x86_64 2/12
[ 29.843418] cloud-init[2284]: Installing : apr-util-1.6.3-1.amzn2023.0.1.x86_64 3/12
[ 29.879436] cloud-init[2284]: Installing : mailcap-2.1.49-3.amzn2023.0.noarch 4/12
[ 29.902813] cloud-init[2284]: Installing : httpd-tools-2.4.58-1.amzn2023.noarch 5/12
[ 31.296310] cloud-init[2284]: Running scriptlet: httpd-filesystem-2.4.58-1.amzn2023.noarch 6/12
[ 31.931451] cloud-init[2284]: Installing : httpd-filesystem-2.4.58-1.amzn2023.noarch 6/12
[ 31.980400] cloud-init[2284]: Installing : httpd-core-2.4.58-1.amzn2023.x86_64 7/12
[ 32.005830] cloud-init[2284]: Installing : mod_lua-2.4.58-1.amzn2023.x86_64 8/12
[ 32.016699] cloud-init[2284]: Installing : mod_http2-2.0.11-2.amzn2023.x86_64 9/12
[ 32.037702] cloud-init[2284]: Installing : generic-logos-htpd-18.0.0-12.amzn2023.0.3.noarch 10/12
[ 32.058468] cloud-init[2284]: Installing : libbrotli-1.0.9-4.amzn2023.0.2.x86_64 11/12
[ 32.076638] cloud-init[2284]: Installing : httpd-2.4.58-1.amzn2023.x86_64 12/12
[ 32.679836] systemd-sysv-generator[2387]: SysV service '/etc/rc.d/init.d/cfn-hup' lacks a native systemd unit file. Automatically generating a unit file for compatibility. Please see /etc/systemd/system/cfn-hup.service.
[ 32.700954] zram_generator::config[2507]: zram0: system has too much memory (949MB), limit is 800MB, ignoring.
[ 33.461192] cloud-init[2284]: Running scriptlet: httpd-2.4.58-1.amzn2023.x86_64 12/12

```

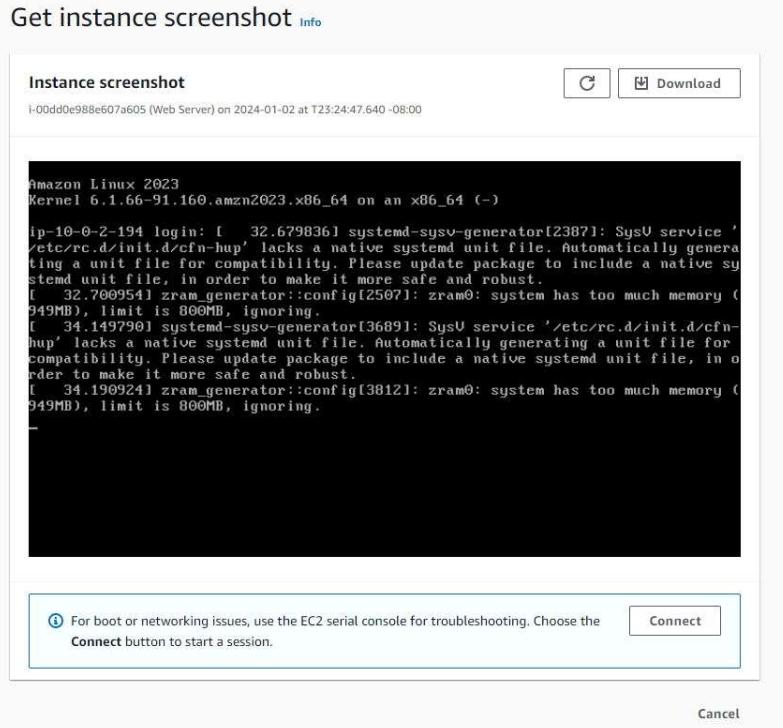
For boot or networking issues, use the EC2 serial console for troubleshooting. Choose the **Connect** button to start a session.

13: This will show everything happening on the instance including the HTTP packets that were installed via the user data code when creating the instance

Click cancel at the bottom once done.



14: Now select Actions > Monitor and troubleshoot > Get instance log



This will display a screenshot of how the EC2 instance would look like if it had a screen.

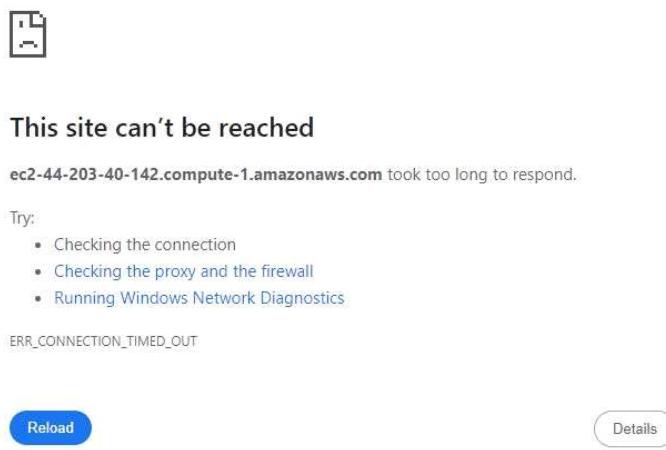
15: Click Cancel when done

Instances (2) Info											Connect	Instance state ▾	Actions ▾	Edit
Find Instance by attribute or tag (case-sensitive)														
Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4						
Web Server	i-00dd0e988e607a605	Running Details Logs	t2.micro	2/2 checks passed	No alarms	+ us-east-1b	ec2-44-203-40-142.co...	44.203.40.1						
Bastion Host	i-0826bac3bfb3915f5	Running Details Logs	t2.micro	2/2 checks passed	No alarms	+ us-east-1a	ec2-34-234-234-148.co...	34.234.234						

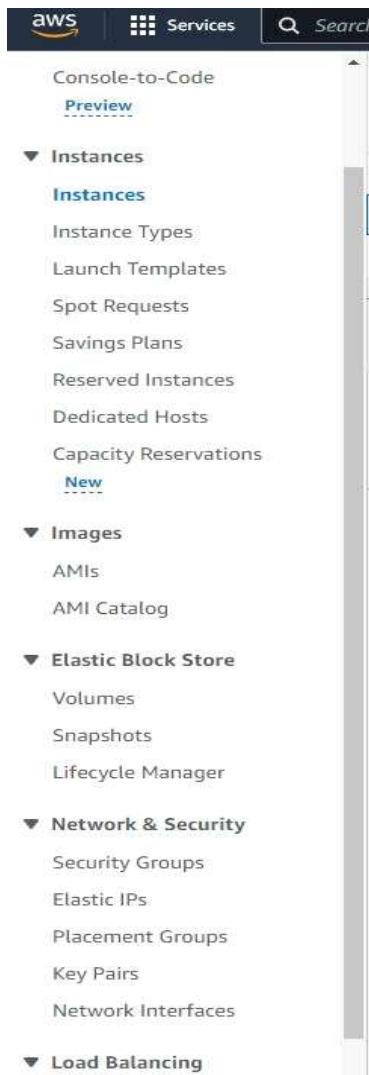
16: Select Web Sever

Instance: i-00dd0e988e607a605 (Web Server)		
Details	Security	Networking
Storage	Status checks	Monitoring
▼ Instance summary Info		
Instance ID i-00dd0e988e607a605 (Web Server)	Public IPv4 address 44.203.40.142 [Open address]	Private IPv4 addresses 10.0.2.194
IPv6 address -	Instance state Running	Public IPv4 DNS ec2-44-203-40-142.compute-1.amazonaws.com [Open address]
Hostname type IP name: ip-10-0-2-194.ec2.internal	Private IP DNS name (IPv4 only) ip-10-0-2-194.ec2.internal	Elastic IP addresses -
Answer private resource DNS name -	Instance type t2.micro	AWS Compute Optimizer finding Opt-in to AWS Compute Optimizer for recommendations.
Auto-assigned IP address 44.203.40.142 [Public IP]	VPC ID vpc-000fef1e4d8905350 (Lab VPC)	Auto Scaling Group name -
IAM Role -	Subnet ID subnet-0d87f5048b33b8de6 (Public Subnet 2)	
IMDSv2 Required		
▼ Instance details Info		
Platform	AMI ID	Monitoring

17: Under the Details tab, copy the Public IPv4 DNS address



18: Paste this address into any web browser, it would be unreachable. This is because of the EC2 security group not allowing port 80/HTTP traffic.



19: Back to the EC2 Console, select Security Groups

Security Groups (1/5) Info						
Actions ▾		Export security groups to CSV ▾			Create	
Find resources by attribute or tag						
Name	Security group ID	Security group name	VPC ID	Description	Own	
sg-0a765ddc6d3ac311b	default	vpc-00a642038d461cb2d	default VPC security group	7758		
sg-013d6c460d34101c1	default	vpc-000fef1e4d8905350	default VPC security group	7758		
sg-0752a7d073936947a	default	vpc-01614f0b48a386808	default VPC security group	7758		
sg-031d163446332bc72	Ec2SecurityGroup	vpc-00a642038d461cb2d	VPC Security Group	7758		
<input checked="" type="checkbox"/> sg-097813aad831c97ed	Web Sever Security Group	vpc-000fef1e4d8905350	Security Group for my Web Server	7758		

20: Select the Web Server Security Group

sg-097813aad831c97ed - Web Sever Security Group

Details	Inbound rules	Outbound rules	Tags
Edit			
Inbound rules (1)			
Name	Security group rule...	IP version	Type
sgr-0cd1225a501429b0e...	IPv4	SSH	TCP
		22	0.0.0.0/0

21: In the lower panel, select the inbound rules tab and click Edit inbound riles

Edit inbound rules [Info](#)

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

Security group rule ID	Type	Protocol	Port range	Source	Description - optional
sgr-0cd1225a501429b0e	HTTP	TCP	80	Anywhere... 0.0.0.0/0	

[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.

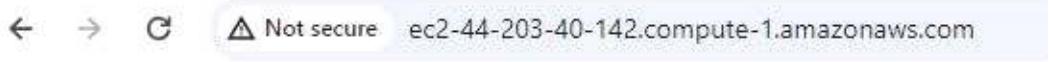
[Cancel](#) [Preview changes](#)

22: Configure:

Type: HTTP

Source: Anywhere IPv4

Save rules



Hello From Your Web Server!

23: Reload your web browser page, you should now be able to access your web server

Instances (1/2) Info						
	Name	Instance ID	Instance state	Instance type	Status check	Alarm status
<input checked="" type="checkbox"/>	Web Server	i-00dd0e988e607a605	Running	t2.micro	2/2 checks passed	No alarms +
<input type="checkbox"/>	Bastion Host	i-0826bac3fbf3915f5	Running	t2.micro	2/2 checks passed	No alarms +

Connect Instance state ▲ Actions ▾ Launch

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

[Public IPv4 ...](#) [... 44.203.40.142](#) [... 34.234.234.148](#)

24: In order to change your instance type or resize your EBS volume, you must first stop your EC2 instance. Select your Web Server instance then in the top right, Instance state > Stop Instance

Instances (2) Info									
	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...
<input type="checkbox"/>	Web Server	i-00dd0e988e607a605	Stopping	t2.micro	-	No alarms +	us-east-1b	ec2-44-203-40-142.co...	44.203.40.142
<input type="checkbox"/>	Bastion Host	i-0826bac3fbf3915f5	Running	t2.micro	2/2 checks passed	No alarms +	us-east-1a	ec2-34-234-234-148.co...	34.234.234.148

Your Instance should be stopped now.

Instances (1/2) Info						
	Name	Instance ID	Instance state	Instance type	Status check	Alarm status
<input checked="" type="checkbox"/>	Web Server	i-00dd0e988e607a605	Stopping	t2.micro	-	No alarms +
<input type="checkbox"/>	Bastion Host	i-0826bac3fbf3915f5	Running	t2.micro	2/2 checks passed	No alarms +

Connect Instance state ▾ Actions ▾ Launch

[View details](#) [Manage instance state](#)

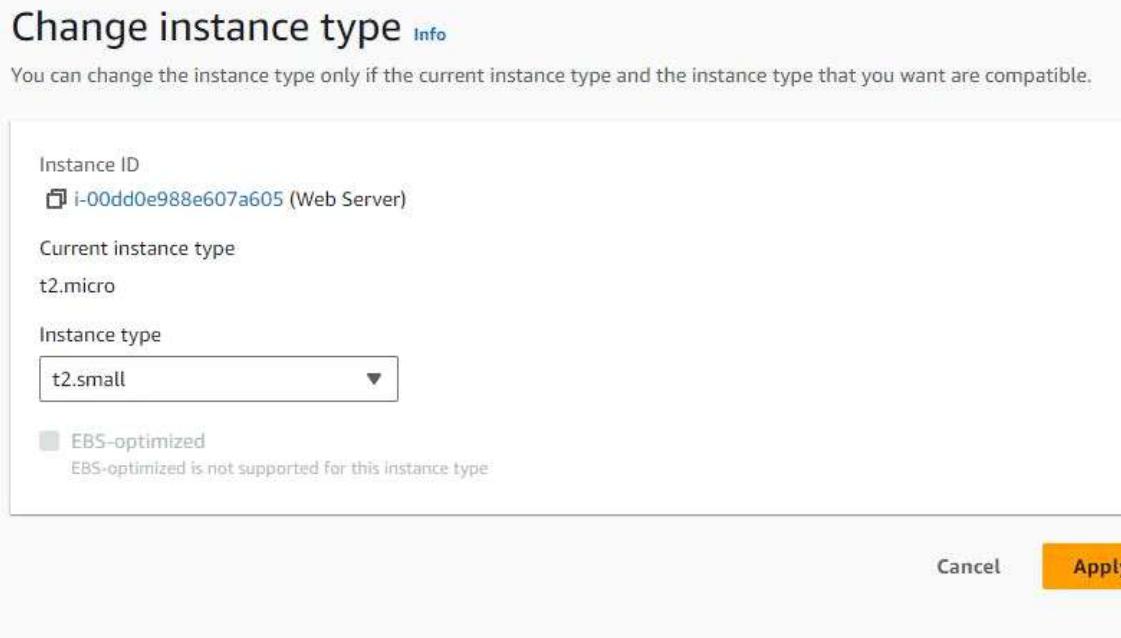
Instance settings

- [Networking](#)
- [Security](#)
- [Image and templates](#)
- [Monitor and troubleshooting](#)

Instance: i-00dd0e988e607a605 (Web Server)

Details	Security	Networking	Storage	Status checks	Monitoring	Tags
<div style="border-bottom: 1px solid #ccc; padding-bottom: 5px;"> ▶ Instance summary Info </div> <div> ▼ Instance details Info <div style="display: flex; justify-content: space-between;"> <div style="flex: 1;"> <p>Platform</p> <p>Amazon Linux (Inferred)</p> <p>Platform details</p> <p>Linux/UNIX</p> <p>Stop protection</p> <p>Disabled</p> </div> <div style="flex: 1;"> <p>AMI ID</p> <p>ami-079db87dc4c10ac91</p> <p>AMI name</p> <p>al2023-ami-2023.3.20231218.0-kernel-6.1-x86_64</p> <p>Launch time</p> <p>Tue Jan 02 2024 22:17:11 GMT-0800 (Pacific Standard Time) (28 minutes ago)</p> </div> </div> </div>						

25: In order to change your instance type, first make sure your Web Server is selected. Select Actions > Instance settings > Change instance type.



26: Change the instance type from t2.micro to t2.small. Click Apply.

Instance: i-00dd0e988e607a605 (Web Server) =

Details	Security	Networking	Storage	Status checks	Monitoring	Tags																										
Root device details <p>Root device name: /dev/xvda Root device type: EBS EBS optimization: disabled</p> Block devices <table border="1"> <thead> <tr> <th>Volume ID</th> <th>Device name</th> <th>Volume size (GiB)</th> <th>Attachment status</th> <th>Attachment time</th> <th>Encrypted</th> <th>KMS key ID</th> <th>Delete on termi</th> </tr> </thead> <tbody> <tr> <td>vol-0913852da3f5f352b</td> <td>/dev/xvda</td> <td>8</td> <td>Attached</td> <td>2024/01/02 23:12 GMT-8</td> <td>No</td> <td>-</td> <td>Yes</td> </tr> </tbody> </table> Recent root volume replacement tasks <table border="1"> <thead> <tr> <th>Task ID</th> <th>Task state</th> <th>Start time</th> <th>Completion time</th> <th>Tags</th> </tr> </thead> <tbody> <tr> <td colspan="5">No recent replace root volume tasks</td> </tr> </tbody> </table>							Volume ID	Device name	Volume size (GiB)	Attachment status	Attachment time	Encrypted	KMS key ID	Delete on termi	vol-0913852da3f5f352b	/dev/xvda	8	Attached	2024/01/02 23:12 GMT-8	No	-	Yes	Task ID	Task state	Start time	Completion time	Tags	No recent replace root volume tasks				
Volume ID	Device name	Volume size (GiB)	Attachment status	Attachment time	Encrypted	KMS key ID	Delete on termi																									
vol-0913852da3f5f352b	/dev/xvda	8	Attached	2024/01/02 23:12 GMT-8	No	-	Yes																									
Task ID	Task state	Start time	Completion time	Tags																												
No recent replace root volume tasks																																

27: Now to resize your EBS Volume, in the lower panel select the Storage tab and click on the Volume ID

Volumes (1/1) Info											
<input type="button" value="Search"/> <input type="button" value="Clear filters"/>											
<input checked="" type="checkbox"/>	Name	Volume ID	Type	Size	IOPS	Throughput	Snapshot	Created	Availability Zone	Actions	
<input checked="" type="checkbox"/>	-	vol-0913852da3f5f352b	gp3	8 GiB	3000	125	snap-0ced1c8...	2024/01/02 23:12 GMT-8	us-east-1b	<input type="button" value="Modify volume"/> <input type="button" value="Create snapshot"/> <input type="button" value="Delete volume"/> <input type="button" value="Attach volume"/> <input type="button" value="Detach volume"/> <input type="button" value="Force detach voli"/> <input type="button" value="Manage auto-en"/> <input type="button" value="Manage tags"/> <input type="button" value="Fault injection"/>	

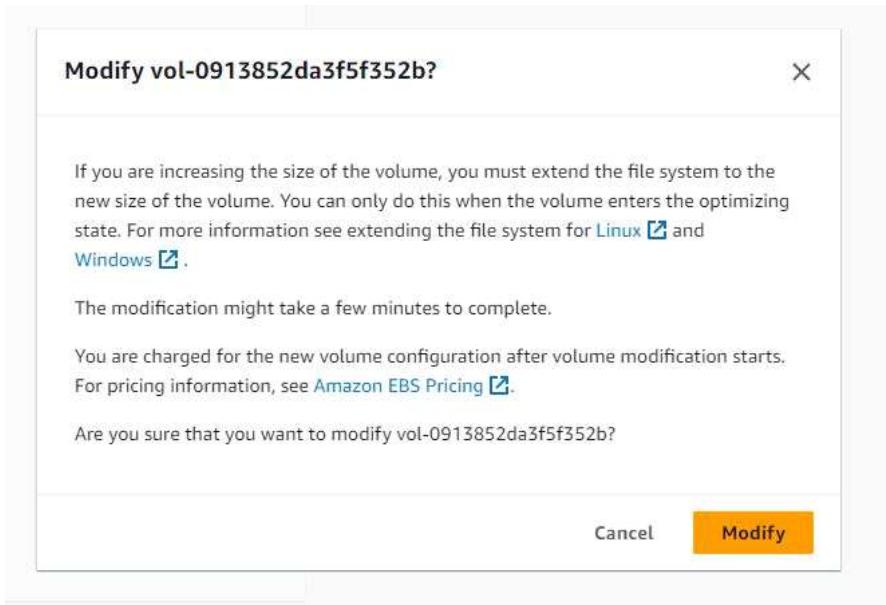
28: Ensure the Volume is selected and under Actions > Modify volume.

Modify volume [Info](#)

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

Volume details	
Volume ID	<input type="text" value="vol-0913852da3f5f352b"/>
Volume type Info	<input type="text" value="General Purpose SSD (gp3)"/>
Size (GiB) Info	<input type="text" value="10"/>
Min: 1 GiB, Max: 16384 GiB. The value must be an integer.	
IOPS Info	<input type="text" value="3000"/>
Min: 3000 IOPS, Max: 16000 IOPS. The value must be an integer.	
Throughput (MiB/s) Info	<input type="text" value="125"/>
Min: 125 MiB, Max: 1000 MiB. Baseline: 125 MiB/s.	
<input type="button" value="Cancel"/> <input type="button" value="Modify"/>	

29: Change the Size from 8 to 10 and click Modify



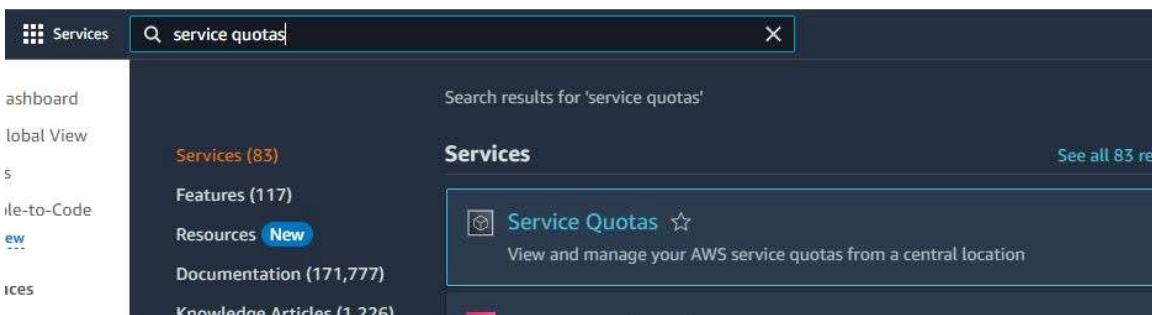
30: Confirm your modification

Volumes (2) Info											
<input type="checkbox"/>	Name	Volume ID	Type	Size	IOPS	Throughput	Snapshot	Created	Availability Zone	Volume	
<input type="checkbox"/>	-	vol-0913852da3f5f352b	gp3	10 GiB	3000	125	snap-0ced1c8...	2024/01/02 23:12 GMT-8	us-east-1b		
<input type="checkbox"/>	-	vol-040308071fe58b2fc	gp3	8 GiB	3000	125	snap-0ced1c8...	2024/01/02 23:01 GMT-8	us-east-1a		

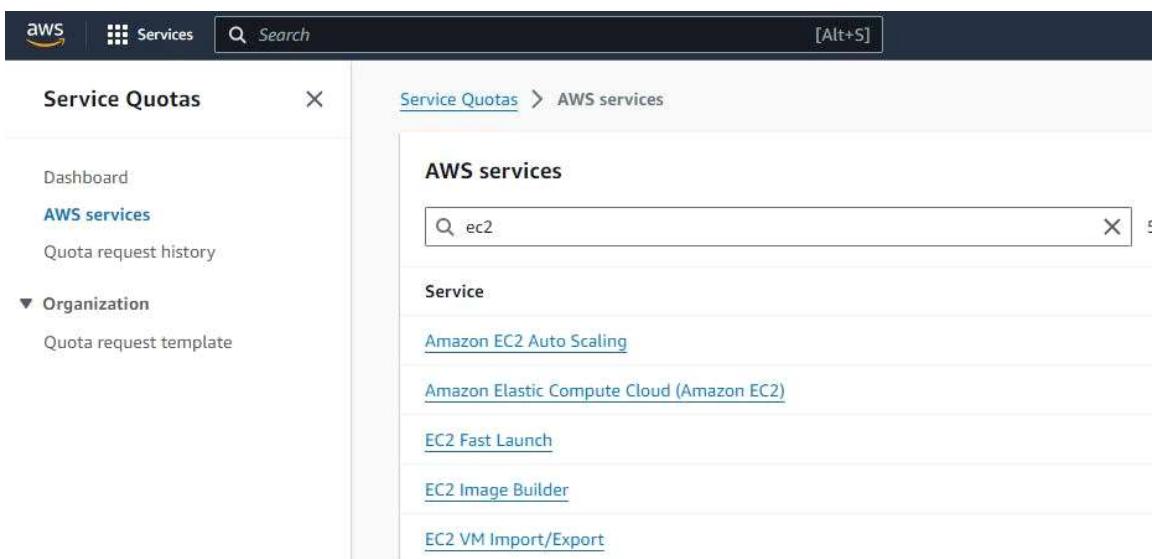
31: You can now see your volume has 10 GiB instead of the previous 8

Instances (1/2) Info							
<input type="button" value="Create"/> <input type="button" value="Connect"/> <input type="button" value="Actions ▾"/> <input type="button" value="Launch"/>							
<input type="text"/> Find Instance by attribute or tag (case-sensitive)							
<input type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
<input checked="" type="checkbox"/>	Web Server	i-00dd0e980e607a605		t2.small	-	No alarms	us-east-1b
<input type="checkbox"/>	Bastion Host	i-0826bac3fb3915f5		t2.micro		No alarms	us-east-1a

32: In order to restart your EC2 instance, Select the instance then under Instance state > Start instance.



33: In the Management Console search for Service Quotas and click.



34: Choose AWS services and search EC2 in the search bar. Choose Amazon Elastic Compute Cloud (Amazon EC2)

Service Quotas > AWS services > Amazon Elastic Compute Cloud (Amazon EC2)

Amazon Elastic Compute Cloud (Amazon EC2)

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

Service quotas [Request increase at account level](#)

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

10 matches

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

35: In the Service quotas search bar, search for running on-demand. Don't select anything, instead observe the quota limits set here. These are soft limits which can be increased on request.

Services [Alt+S] N. Virginia

- Recently visited
- Favorites
- All services
- Analytics
- Application Integration
- Blockchain
- Business Applications
- Cloud Financial Management
- Compute
- Containers

Compute

- AWS App Runner** Build and run production web applications at scale
- Batch** Fully managed batch processing at any scale
- EC2** Virtual Servers in the Cloud
- EC2 Image Builder** A managed service to automate build, customize and deploy OS images
- Elastic Beanstalk** Run and Manage Web Apps

EC2 Free Tier Offers for all AWS Regions.

0 EC2 free tier offers in use

End of month forecast:

(@ User: arn:aws:sts::775815040941 1-Kevin_Chuk is not authorized to perform resource: arn:aws:free-tier:us-east-1 because no identity-based policy allows it)

Exceeds free tier

(@ User: arn:aws:sts::775815040941 1-Kevin_Chuk is not authorized to perform resource: arn:aws:free-tier:us-east-1 because no identity-based policy allows it)

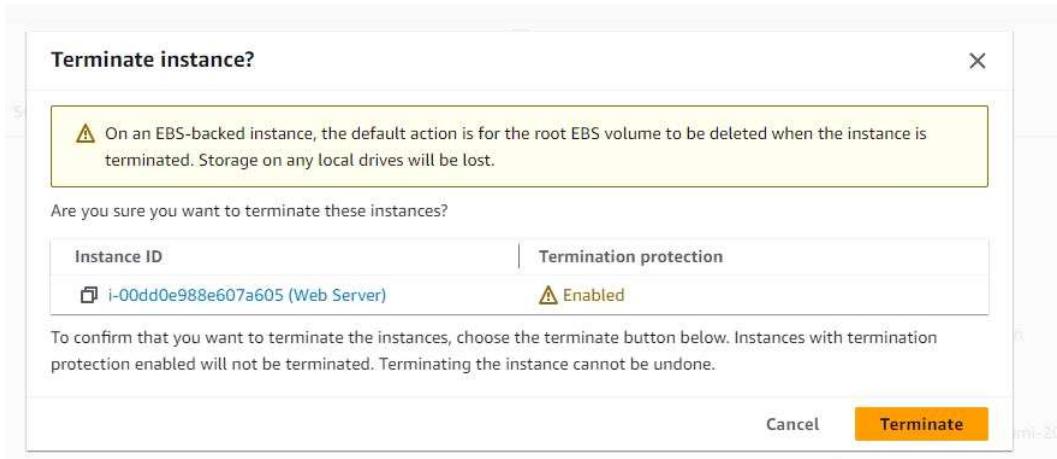
36: Head back to Amazon EC2 and go to instances

Instances (1/2)

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
<input checked="" type="checkbox"/> Web Server	i-00dd0e988e607a605	Running	t2.small	2/2 checks passed	No alarms +	us-east-1b
<input type="checkbox"/> Bastion Host	i-0826bac3fb3915f5	Running	t2.micro	2/2 checks passed	No alarms +	us-east-1a

Instance state	Actions	Last modified
Stop instance		2023-09-12 10:45:00
Start instance		2023-09-12 10:45:00
Reboot instance		2023-09-12 10:45:00
Hibernate instance		2023-09-12 10:45:00
Terminate instance		2023-09-12 10:45:00

36: We will now test our termination protection. Select the Web Server then under Instance state > Terminate instance.



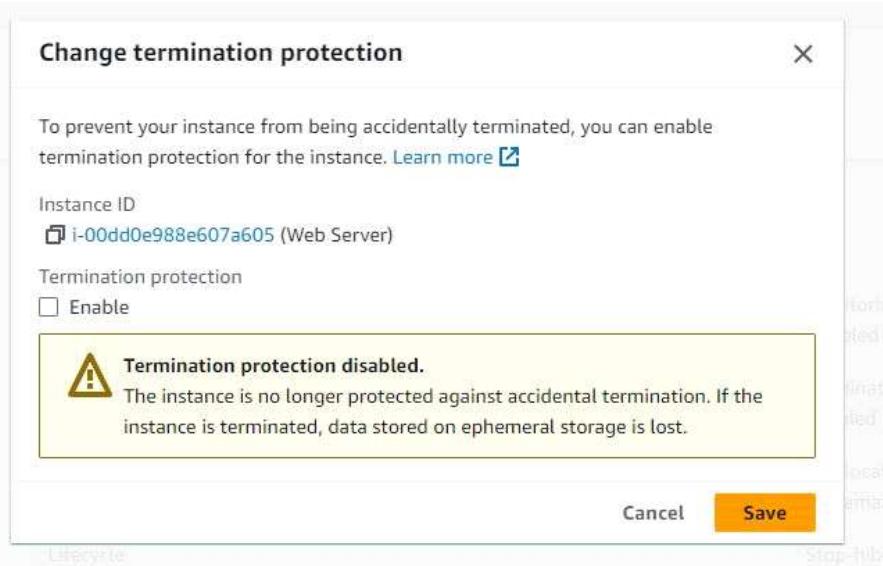
37: Confirm you want to Terminate this EC2 instance

Failed to terminate an instance: The instance 'i-00dd0e988e607a605' may not be terminated. Modify its 'disableApiTermination' instance attribute

38: This error message will appear at the top of your screen. This is Termination Protection at work. We will have to disable this feature in order to terminate our EC2 instance.



39: Under Actions > Instance settings > Change termination protection



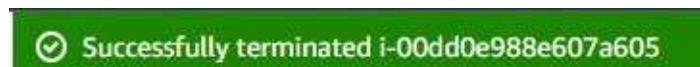
40: Uncheck the Enable box and click Save

Instances (1/2) Info						
Find Instance by attribute or tag (case-sensitive)						
Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
<input checked="" type="checkbox"/> Web Server	i-00dd0e988e607a605	Running	t2.small	2/2 checks passed	No alarms	us-east-1b
<input type="checkbox"/> Bastion Host	i-0826bac3fb3915f5	Running	t2.micro	2/2 checks passed	No alarms	us-east-1a

[Create](#) [Connect](#) [Launch](#)

Instance state	Actions
Stop instance	Start instance
Reboot instance	Public IPv4 ...
Hibernate instance	54.173.159.102
Terminate instance	34.234.234.148

41: Try terminating the instance again. Select the instance, then Instance state > Terminate instance.



42: This time the instance should terminate because Termination Protection was turned off.

Problems:

Being such a simple lab there were not many issues encountered. The only potential issue I faced was regions in lab 1. My region got changed to Ohio instead of N. Virginia when I logged into the user-2 account which made it so that I could not see my EC2 instances. A very simple fix to change the regions under the Region Menu located in the top-right corner of the screen back to N. Virginia.

In lab 2 I did miss steps when creating subnets for my VPC which required me to restart the lab. This was purely human error due to not following the instructions provided by Amazon properly.

Conclusion:

These 3 labs were introductory labs into Amazon IAM, VPC, and EC2 showing some of their basic and more widely used features.

The IAM lab showed Users, User groups, and Roles and how to assign User and Roles to User groups.

Lab 2 was about VPCs and how to create a VPC via VPC wizard, creating subnets for the VPC, configuring a security group, and using EC2 on the VPC to launch a Web Server.

Lab 3 was all about EC2. While we did use EC2 in lab 2, lab 3 went into more detail and showed off termination protection, EC2 instance monitoring, modification of a security group, editing your EC2 type, editing EBS volume and EC2 termination.