

Assignments

Day 3: Assignments: Part a) & b) S3:

```
*Untitled - Notepad
File Edit Format View Help

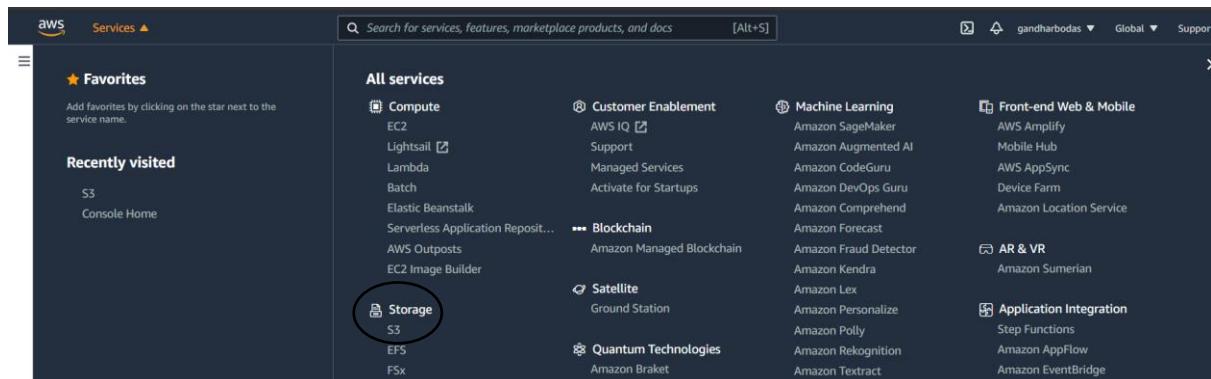
Assignment 1 Day3:S3
Task1:Create an S3 bucket
Task2:Upload an object
Task3:edit public access settings
Task4:Make object public
acess using url

Assignment2 ELB:
Create 2 ec2 instances with nginx webserver installed
Create Elastic load balancer
Add these two instances in to the ELB's target group
```

Answer:

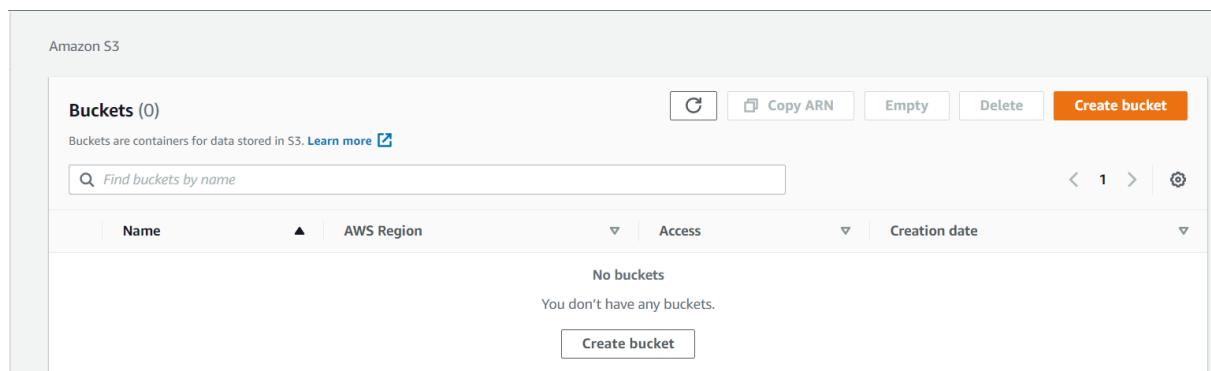
Part a):

Step 1: Go to the Service→Storage→S3



The screenshot shows the AWS Services dashboard. On the left, there's a sidebar with 'Favorites' and 'Recently visited' sections. Under 'Storage', the S3 service is highlighted with a circular selection. The main area is titled 'All services' and lists various AWS services in categories: Compute (EC2, Lightsail, Lambda, Batch, Elastic Beanstalk, Serverless Application Repository, AWS Outposts, EC2 Image Builder), Customer Enablement (AWS IQ, Support, Managed Services, Activate for Startups), Blockchain (Amazon Managed Blockchain), Satellite (Ground Station), Quantum Technologies (Amazon Braket), Machine Learning (Amazon SageMaker, Amazon Augmented AI, Amazon CodeGuru, Amazon DevOps Guru, Amazon Comprehend, Amazon Forecast, Amazon Fraud Detector, Amazon Kendra, Amazon Lex, Amazon Personalize, Amazon Polly, Amazon Rekognition, Amazon Texttract), Front-end Web & Mobile (AWS Amplify, Mobile Hub, AWS AppSync, Device Farm, Amazon Location Service), AR & VR (Amazon Sumerian), and Application Integration (Step Functions, Amazon AppFlow, Amazon EventBridge). A search bar at the top is empty.

Step 2: *Create an S3 bucket*



The screenshot shows the 'Amazon S3' service page. At the top, it says 'Buckets (0)' and 'No buckets'. Below that, it says 'You don't have any buckets.' There is a large 'Create bucket' button at the bottom. The page includes a search bar, a 'Copy ARN' button, and buttons for 'Empty' and 'Delete'. A table header with columns 'Name', 'AWS Region', 'Access', and 'Creation date' is visible, though no data rows are present.

Click on “Create Bucket” button and specify the “Bucket name: day3ass2”, keep “AWS Region as it is”, “Block Public Access settings for this bucket : keep as it is “, “Bucket Versioning: Disable” and “Default encryption: Disable”.

The screenshot shows the "Create bucket" wizard. In the "General configuration" step, the bucket name is set to "day3ass2" and the AWS Region is set to "US East (Ohio) us-east-2". Under "Copy settings from existing bucket - optional", there is a "Choose bucket" button. In the "Block Public Access settings for this bucket" step, the "Block all public access" checkbox is checked, and four sub-options are listed: "Block public access to buckets and objects granted through new access control lists (ACLs)", "Block public access to buckets and objects granted through any access control lists (ACLs)", "Block public access to buckets and objects granted through new public bucket or access point policies", and "Block public and cross-account access to buckets and objects through any public bucket or access point policies".

Amazon S3 > Create bucket

Create bucket

Buckets are containers for data stored in S3. [Learn more](#)

General configuration

Bucket name

day3ass2

Bucket name must be unique and must not contain spaces or uppercase letters. [See rules for bucket naming](#)

AWS Region

US East (Ohio) us-east-2

Copy settings from existing bucket - *optional*
Only the bucket settings in the following configuration are copied.

[Choose bucket](#)

Block Public Access settings for this bucket

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

Block all public access

Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

- Block public access to buckets and objects granted through new access control lists (ACLs)**
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
- Block public access to buckets and objects granted through any access control lists (ACLs)**
S3 will ignore all ACLs that grant public access to buckets and objects.
- Block public access to buckets and objects granted through new public bucket or access point policies**
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
- Block public and cross-account access to buckets and objects through any public bucket or access point policies**
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

Bucket Versioning

Disable
 Enable

Tags (0) - optional

Track storage cost or other criteria by tagging your bucket. [Learn more](#)

No tags associated with this bucket.

[Add tag](#)

Default encryption

Automatically encrypt new objects stored in this bucket. [Learn more](#)

Server-side encryption

Disable
 Enable

► Advanced settings

ⓘ After creating the bucket you can upload files and folders to the bucket, and configure additional bucket settings.

[Cancel](#) [Create bucket](#)

Now click on “Create bucket” button.

ⓘ Successfully created bucket "day3ass2"
To upload files and folders, or to configure additional bucket settings choose [View details](#).

[View details](#) [X](#)

Amazon S3

Buckets (1)

Buckets are containers for data stored in S3. [Learn more](#)

Find buckets by name < 1 > [?](#)

Name	AWS Region	Access	Creation date
day3ass2	US East (Ohio) us-east-2	Bucket and objects not public	March 19, 2021, 15:58:03 (UTC+05:30)

Step 3: *Upload an object*

Click on bucket name: [day3ass2](#)

Amazon S3 > day3ass2

day3ass2

Objects (0)

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

C Delete Actions ▾ Create folder Upload

Find objects by prefix

No objects

You don't have any objects in this bucket.

Upload

Here, uploads an object so for that click on “upload button” and then

Amazon S3 > day3ass2 > Upload

Upload

Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. [Learn more](#)

Drag and drop files and folders you want to upload here, or choose Add files, or Add folders.

Files and folders (0)

All files and folders in this table will be uploaded.

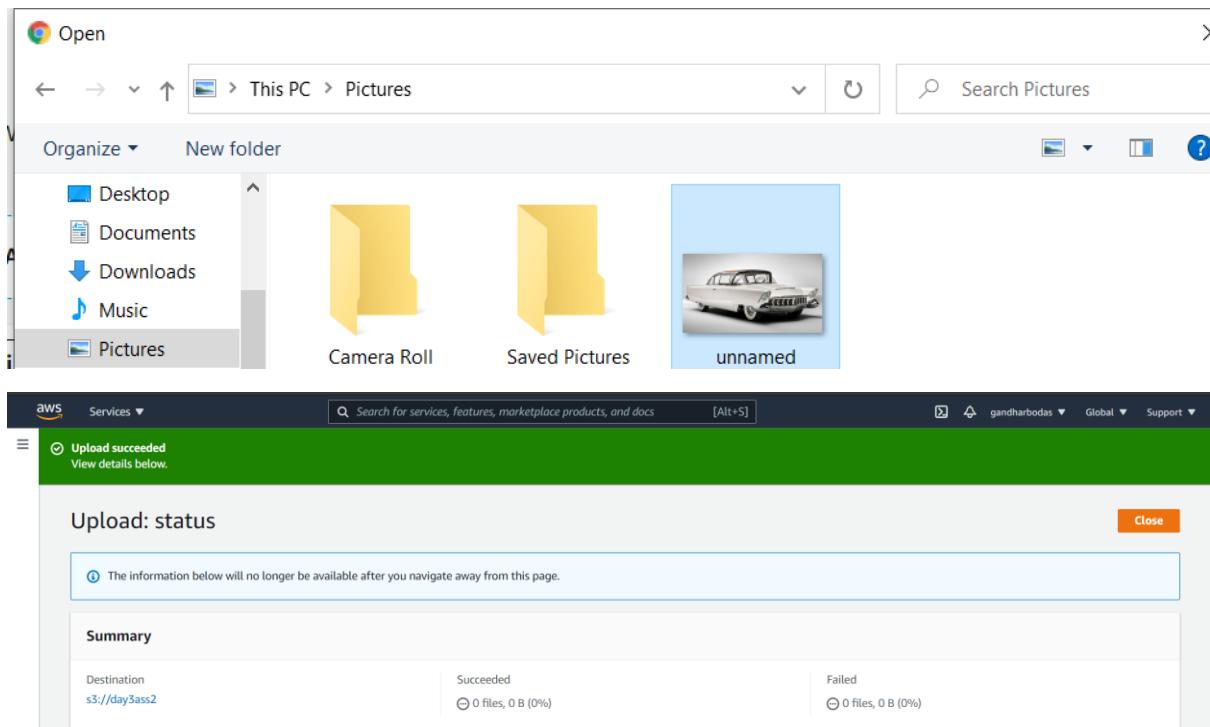
Remove Add files Add folder

Find by name

No files or folders

You have not chosen any files or folders to upload.

Click on “Add files” and then again click on “Upload button”



Uploaded successfully now click on Close button.

The screenshot shows the AWS S3 console with the path 'Amazon S3 > day3ass2'. The 'Objects' tab is selected, showing a single object named 'unnamed.jpg'. The object details are: Name: unnamed.jpg, Type: jpg, Last modified: March 19, 2021, 16:02:56 (UTC+05:30), Size: 28.7 KB, Storage class: Standard. There are buttons for Actions (Delete, Create folder, Upload) and a search bar.

Step 4: *Edit public access settings*

Select object and click on it and you will be able to see the below page.

Now copy Object URL: <https://day3ass2.s3.us-east-2.amazonaws.com/unnamed.jpg> and paste it on a new tab you will be able to see the XML file page where **Access Denied**.

Object overview

Owner	S3 URI
AWS Region	s3://day3ass2/unnamed.jpg
US East (Ohio) us-east-2	Amazon Resource Name (ARN)
Last modified	arn:aws:s3:::day3ass2/unnamed.jpg
March 19, 2021, 16:09:55 (UTC+05:30)	Entity tag (Etag)
Size	d891328a808d7391900f7c2516a43b2d
28.7 KB	Object URL
Type	https://day3ass2.s3.us-east-2.amazonaws.com/unnamed.jpg
jpg	
Key	
unnamed.jpg	

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
▼<Error>
  <Code>AccessDenied</Code>
  <Message>Access Denied</Message>
  <RequestId>BJ3RJ32H01GEV2K3</RequestId>
  <HostId>kGXUbGa5AQoljM02xWyxZYF93+6oE25tQLSGbbQ1GeJZJbD29DPY3t48Az8xNsJVzD+c6YVuEdE=</HostId>
</Error>
```

On this page to towards right hand side--→Object Section→Click on Make public option.

Amazon S3

unnamed.jpg

Properties Permissions Versions

Object overview

Owner	S3 URI
AWS Region	s3://day3ass2/unnamed.jpg
US East (Ohio) us-east-2	Amazon Resource Name (ARN)
Last modified	arn:aws:s3:::day3ass2/unnamed.jpg
March 19, 2021, 16:02:56 (UTC+05:30)	Entity tag (Etag)
Size	d891328a808d7391900f7c2516a43b2d
28.7 KB	Object URL
Type	https://day3ass2.s3.us-east-2.amazonaws.com/
jpg	
Key	
unnamed.jpg	

Copy S3 URI Object actions ▾

- Open
- Calculate total size
- Copy
- Move
- Initiate restore
- Query with S3 Select
- Download actions
- Download
- Download as
- Edit actions
- Rename object
- Edit storage class
- Edit server-side encryption
- Edit metadata
- Edit tags
- Make public

Make public

The make public action enables public read access in the object access control list (ACL) settings. [Learn more](#).



Public access is blocked because Block Public Access settings are turned on for this bucket.

To determine which settings are turned on, check your [Block Public Access settings for this bucket](#). Learn more about [using Amazon S3 Block Public Access](#).



When public read access is enabled and not blocked by Block Public Access settings, anyone in the world can access the specified objects.

Specified objects

Find objects by name

< 1 >

Name	Type	Last modified	Size
unnamed.jpg	jpg	March 19, 2021, 16:02:56 (UTC+05:30)	28.7 KB

Cancel

Make public

Now click on this “ [Block Public Access settings for this bucket](#).” You will get below page

Make public

The make public action enables public read access in the object access control list (ACL) settings. [Learn more](#).



Public access is blocked because Block Public Access settings are turned on for this bucket.

To determine which settings are turned on, check your [Block Public Access settings for this bucket](#). Learn more about [using Amazon S3 Block Public Access](#).

Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#).

Edit

Block all public access

On

On Block public access to buckets and objects granted through *new* access control lists (ACLs)

On Block public access to buckets and objects granted through *any* access control lists (ACLs)

On Block public access to buckets and objects granted through *new* public bucket or access point policies

On Block public and cross-account access to buckets and objects through *any* public bucket or access point policies

Now click on “Edit button” and uncheck “Block all public access” and then save changes and confirmed.

Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

Block all public access
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

- Block public access to buckets and objects granted through new access control lists (ACLs)**
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
- Block public access to buckets and objects granted through any access control lists (ACLs)**
S3 will ignore all ACLs that grant public access to buckets and objects.
- Block public access to buckets and objects granted through new public bucket or access point policies**
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
- Block public and cross-account access to buckets and objects through any public bucket or access point policies**
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

[Cancel](#) [Save changes](#)

If you require some level of public access to your buckets or objects

Edit Block public access (bucket settings) [X](#)

⚠️ Updating the Block Public Access settings for this bucket will affect this bucket and all objects within. This may result in some objects becoming public.

To confirm the settings, enter *confirm* in the field.

confirm

[Cancel](#) [Confirm](#)

Successfully edited Block Public Access settings.

The screenshot shows the AWS S3 console with the bucket 'day3ass2'. The 'Permissions' tab is selected. A green banner at the top indicates 'Successfully edited Block Public Access settings for this bucket.' Below this, the 'Permissions overview' section shows 'Access' and 'Objects can be public'. Under 'Block public access (bucket settings)', it states that public access is granted through ACLs, policies, or all. It recommends turning on 'Block all public access'. A link to 'Learn more' is provided, and an 'Edit' button is visible. The navigation bar at the top includes 'Services', a search bar, and user information 'gandharbodas'.

Step 5: *Now click on “Permission” and later on click on “Edit button” and under “Access control list (ACL)” give read and write permissions to an object as such*:

The screenshot shows the 'Access control list (ACL)' settings for objects. It lists three entries: 'Object owner (your AWS account)', 'Everyone (public access)', and 'Authenticated users group (anyone with an AWS account)'. For each entry, it shows the grantee, the objects they have permission to, and the specific permissions (Read or Write). The 'Object owner' has both Read and Write permissions. 'Everyone' has Read permission and Write is listed as pending. 'Authenticated users group' has both Read and Write permissions.

Grantee	Objects	Object ACL
Object owner (your AWS account)	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write
Everyone (public access)	<input checked="" type="checkbox"/> Δ Read Group: <input type="checkbox"/> http://acs.amazonaws.com/groups/global/AllUsers	<input checked="" type="checkbox"/> Δ Read <input type="checkbox"/> Write
Authenticated users group (anyone with an AWS account)	<input checked="" type="checkbox"/> Δ Read Group: <input type="checkbox"/> http://acs.amazonaws.com/groups/global/AuthenticatedUsers	<input checked="" type="checkbox"/> Δ Read <input type="checkbox"/> Write

Then save changes.

Successfully edited access control list for object "unnamed.jpg".

Amazon S3 > day3ass2 > unnamed.jpg

unnamed.jpg

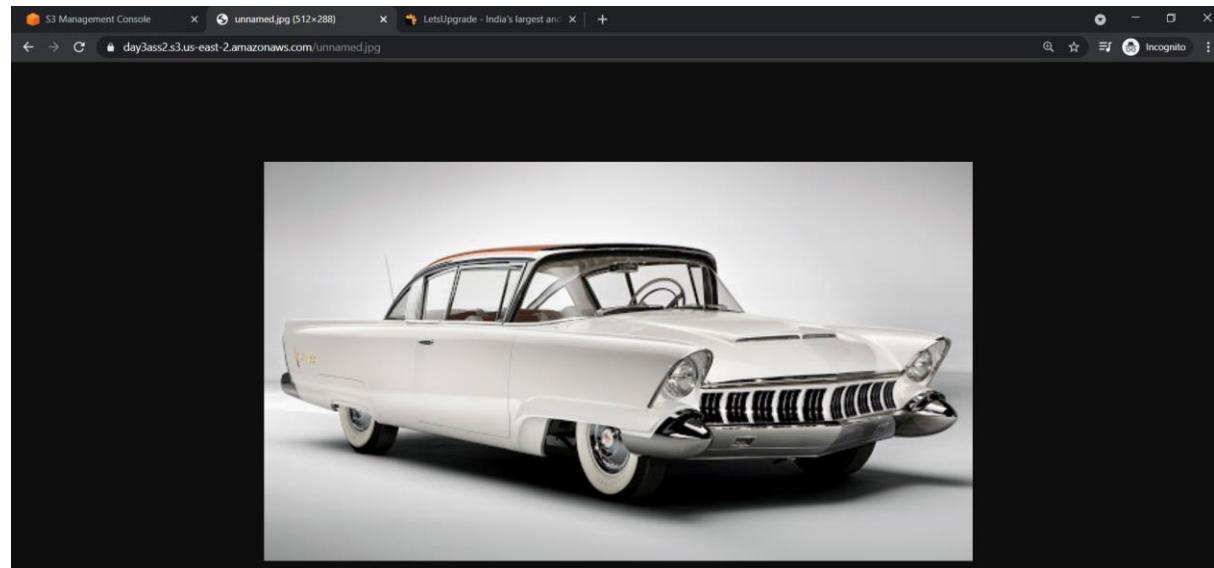
Properties Permissions Versions

Object overview

Owner	S3 URI
AWS Region	s3://day3ass2/unnamed.jpg
US East (Ohio) us-east-2	Amazon Resource Name (ARN)
Last modified	arn:aws:s3:::day3ass2/unnamed.jpg
March 19, 2021, 16:09:55 (UTC+05:30)	Entity tag (Etag)
Size	d891328a808d7391900f7c2516a43b2d
28.7 KB	Object URL
Type	https://day3ass2.s3.us-east-2.amazonaws.com/unnamed.jpg
jpg	

Step 6: Again, copy the same Object URL: <https://day3ass2.s3.us-east-2.amazonaws.com/unnamed.jpg> and open on a new tab then output is as below:

OUTPUT:



END

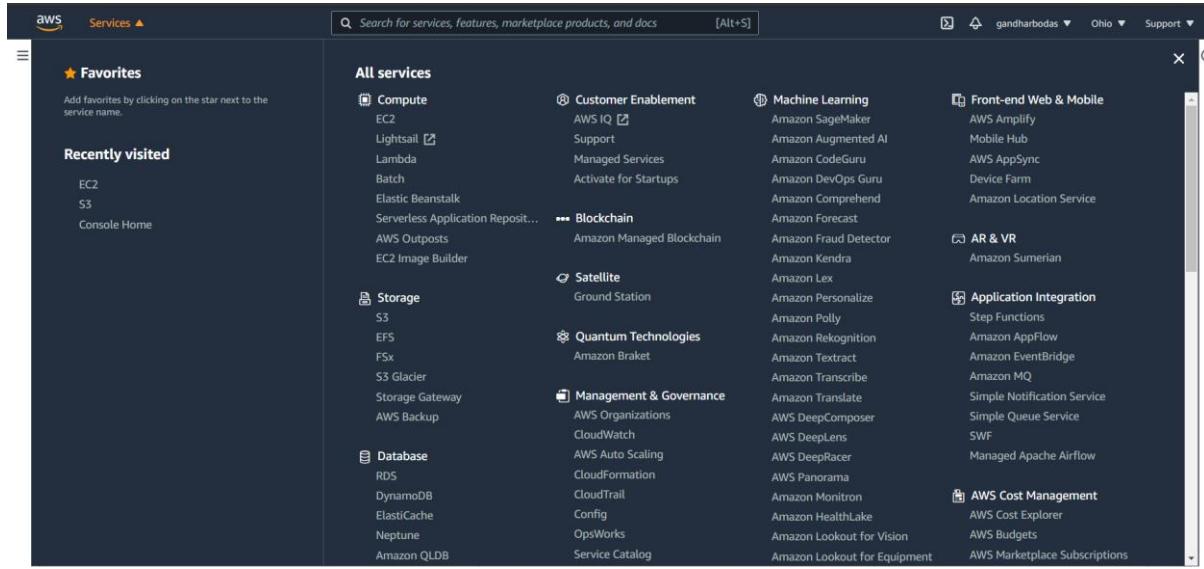
Answer:

Part b):

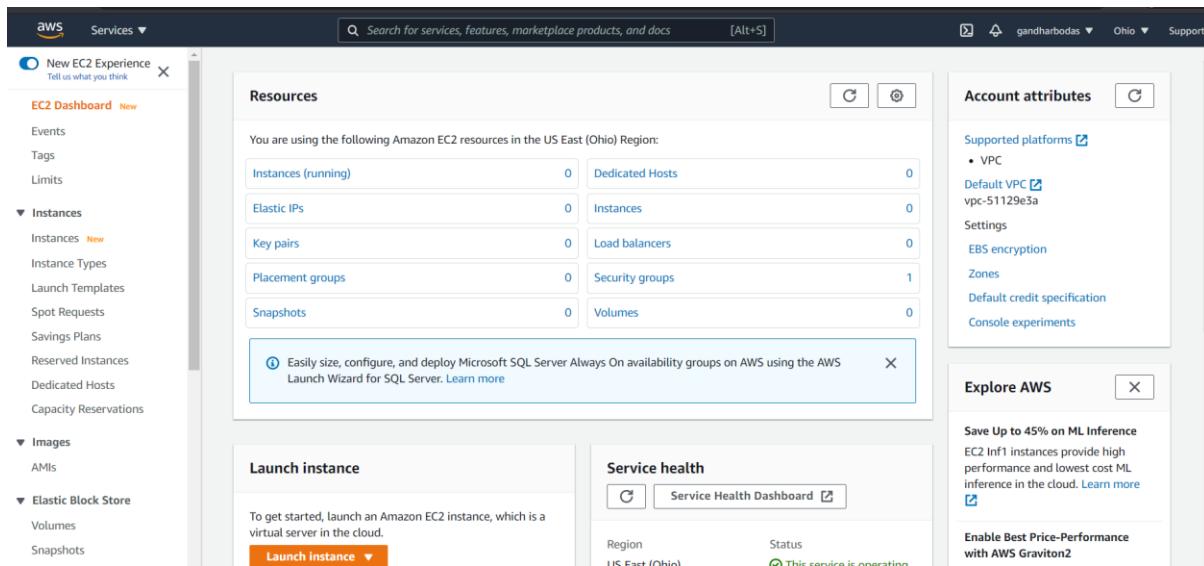
Step 1: *Create 2 EC2 Instances with ngnix web server installed*

Instance 1:

Go to the services --> click on EC2->



you will be able to see the below page



Click on instances option which is on left hand side panel:

Click on “Launch Instances” and you will get the new page i.e., AMI page.

Click on check box: “Free the only” and select “Ubuntu Server 20.04 LTS (HVM), SSD Volume Type - ami-08962a4068733a2b6 (64-bit x86) / ami-064446ad1d755489e (64-bit Arm)” and click on “Select button”.

Select Instance type: t2. micro (Free tier eligible) and then click 1 “Next: Configure instance Detail’s button”.

Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
t2	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
<input checked="" type="checkbox"/> t2	<input checked="" type="checkbox"/> t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate	Yes
	t2.small	1	2	EBS only	-	Low to Moderate	Yes
	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
	t2.large	2	8	EBS only	-	Low to Moderate	Yes
	t2.xlarge	4	16	EBS only	-	Moderate	Yes
	t2.2xlarge	8	32	EBS only	-	Moderate	Yes
	t3.nano	2	0.5	EBS only	Yes	Up to 5 Gigabit	Yes

Configure Instance Details as Auto-assign Public IP: Enable, enable termination protection: tick check box as “Protect against accidental termination” and later on click on Next: Add Storage.

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot Instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances	<input type="text" value="1"/>	Launch into Auto Scaling Group
Purchasing option	<input type="checkbox"/> Request Spot Instances	
Network	vpc-51129e3a (default)	<input type="checkbox"/> Create new VPC
Subnet	No preference (default subnet in any Availability Zone)	<input type="checkbox"/> Create new subnet
Auto-assign Public IP	Enable	
Placement group	<input type="checkbox"/> Add instance to placement group	
Capacity Reservation	Open	
Domain join directory	No directory	<input type="checkbox"/> Create new directory
IAM role	None	<input type="checkbox"/> Create new IAM role
CPU options <input type="checkbox"/> Specify CPU options		
Shutdown behavior	Stop	
Stop - Hibernate behavior	<input type="checkbox"/> Enable hibernation as an additional stop behavior	
Enable termination protection	<input checked="" type="checkbox"/> Protect against accidental termination	
Monitoring	<input type="checkbox"/> Enable CloudWatch detailed monitoring Additional charges apply.	
Tenancy	Shared - Run a shared hardware instance	Additional charges will apply for dedicated tenancy.
Elastic Inference	<input type="checkbox"/> Add an Elastic Inference accelerator Additional charges apply.	
Credit specification	<input type="checkbox"/> Unlimited Additional charges may apply	
File systems	<input type="button" value="Add file system"/>	<input type="button" value="Create new file system"/>

▼ Advanced Details

Enclave	<input type="checkbox"/> Enable
Metadata accessible	Enabled
Metadata version	V1 and V2 (token optional)
Metadata token response hop limit	1
User data	<input checked="" type="radio"/> As text <input type="radio"/> As file <input type="checkbox"/> Input is already base64 encoded (Optional)

Cancel Previous **Review and Launch** Next: Add Storage

Add Storage: Keep as it is. Later on, click on Next: Add Tags

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more](#) about storage options in Amazon EC2.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encryption
Root	/dev/sda1	snapshot-08d55512ce962b5e5	8	General Purpose SSD (gp2)	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted

Add New Volume

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. [Learn more](#) about free usage tier eligibility and usage restrictions.

Cancel Previous **Review and Launch** Next: Add Tags

Add Tags: Key – Name1 and Value: Ins1 and click on Next: Configure Security Group button

Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. A copy of a tag can be applied to volumes, instances or both. Tags will be applied to all instances and volumes. [Learn more](#) about tagging your Amazon EC2 resources.

Key	(128 characters maximum)	Value	(256 characters maximum)	Instances	Volumes	Network Interfaces
Name1		Ins1		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Add another tag (Up to 50 tags maximum)

Cancel **Previous** **Review and Launch** **Next: Configure Security Group**

Configure Security Group: Security group name: - Group1, Type: All Traffic, Source: Anywhere and click on Review and Launch button.

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: Create a new security group Select an existing security group

Security group name:	Group1			
Description:	launch-wizard-1 created 2021-03-19T17:04:35.100+05:30			
Type	Protocol	Port Range	Source	Description
All traffic	All	0 - 65535	Anywhere	0.0.0.0/:/0 e.g. SSH for Admin Desktop

Add Rule

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

Cancel **Previous** **Review and Launch**

Review Instance Launch and keep as it is and later on Launch button:

Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

AMI Details

Ubuntu Server 20.04 LTS (HVM), SSD Volume Type - ami-08962a4068733a2b6

Instance Type

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t2.micro	-	1	1	EBS only	-	Low to Moderate

Security Groups

Instance Details

Storage

Edit AMI **Edit instance type** **Edit security groups** **Edit instance details** **Edit storage**

Creating a new key pair, name as: day3 and download key pair and click on “Launch Instances” button”

Launch Status

Your instances are now launching
The following instance launches have been initiated: i-0f6a907c7966292ca [View launch log](#)

Click on View Instances button:

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
-	i-0f6a907c7966292ca	Running	t2.micro	2/2 checks passed	No alarms	us-east-2b	ec2-3-141-16-10.

Now click on “Connect button and you will be able to see this page:

EC2 > Instances > i-0f6a907c7966292ca > Connect to instance

Connect to instance [Info](#)

Connect to your instance i-0f6a907c7966292ca using any of these options

EC2 Instance Connect [Session Manager](#) [SSH client](#)

Instance ID: [i-0f6a907c7966292ca](#)

Public IP address: [3.141.16.10](#)

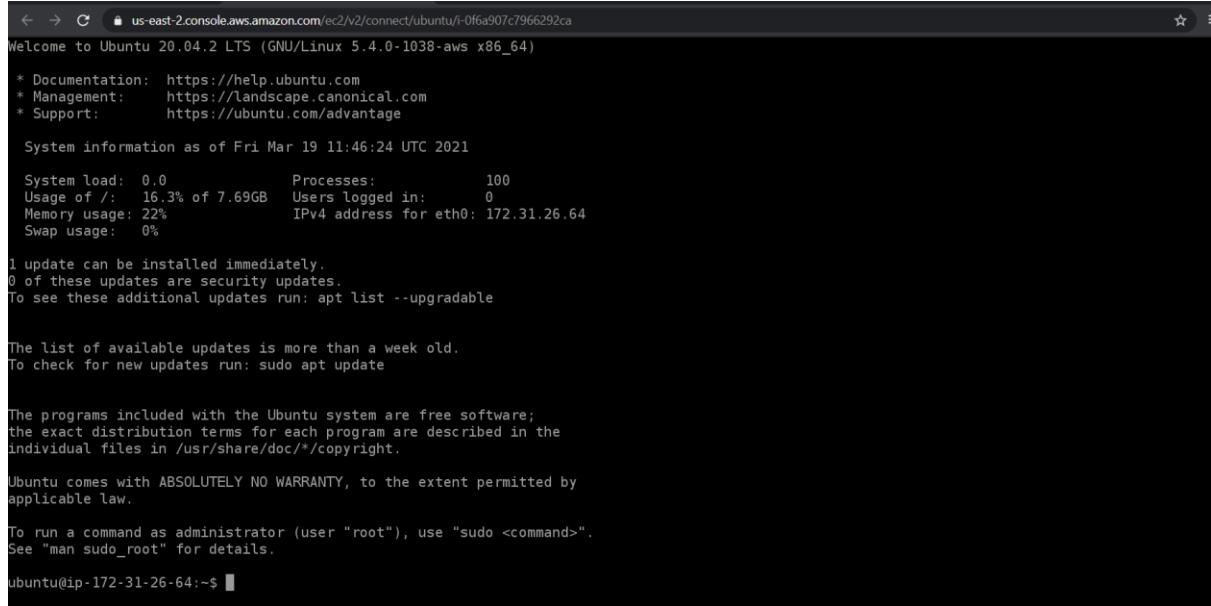
User name:

Connect using a custom user name, or use the default user name ubuntu for the AMI used to launch the instance.

Note: In most cases, the guessed user name is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI user name.

[Cancel](#) [Connect](#)

Click on “Connect” button and you will be able to see the black screen on new tab:



```
← → C us-east-2.console.aws.amazon.com/ec2/v2/connect/ubuntu/i-0f6a907c7966292ca
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-1038-aws x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

 System information as of Fri Mar 19 11:46:24 UTC 2021

 System load: 0.0      Processes:          100
 Usage of /: 16.3% of 7.69GB  Users logged in:    0
 Memory usage: 22%      IPv4 address for eth0: 172.31.26.64
 Swap usage:  0%

1 update can be installed immediately.
0 of these updates are security updates.
To see these additional updates run: apt list --upgradable

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

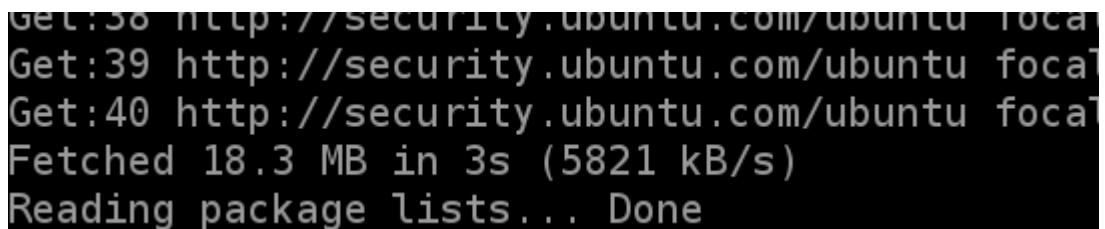
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-172-31-26-64:~$
```

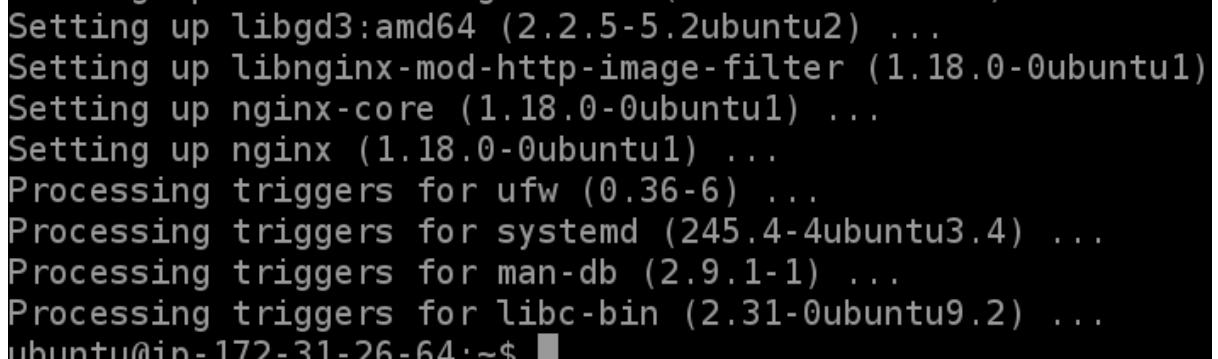
Now fire the below commands on the above screen:

Sudo apt-get -y update

Sudo apt-get -y install nginx



```
Get:58 http://security.ubuntu.com/ubuntu focal
Get:39 http://security.ubuntu.com/ubuntu focal
Get:40 http://security.ubuntu.com/ubuntu focal
Fetched 18.3 MB in 3s (5821 kB/s)
Reading package lists... Done
```

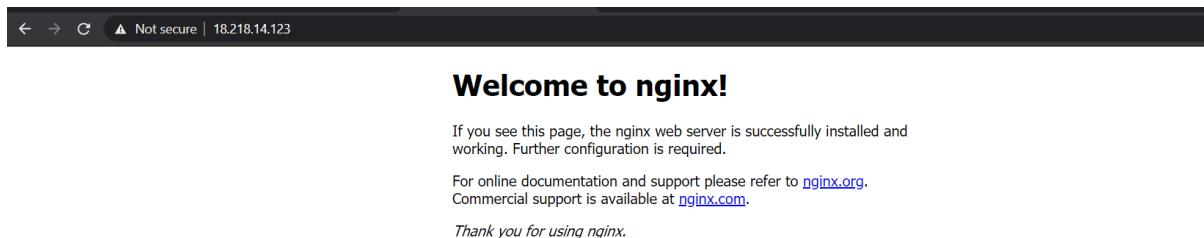


```
Setting up libgd3:amd64 (2.2.5-5.2ubuntu2) ...
Setting up libnginx-mod-http-image-filter (1.18.0-0ubuntu1)
Setting up nginx-core (1.18.0-0ubuntu1) ...
Setting up nginx (1.18.0-0ubuntu1) ...
Processing triggers for ufw (0.36-6) ...
Processing triggers for systemd (245.4-4ubuntu3.4) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for libc-bin (2.31-0ubuntu9.2) ...
ubuntu@ip-172-31-26-64:~$
```

Once update and installed nginx web server then copy the public ip : 3.141.16.10 and paste it on a new tab and you will be able to see the output:

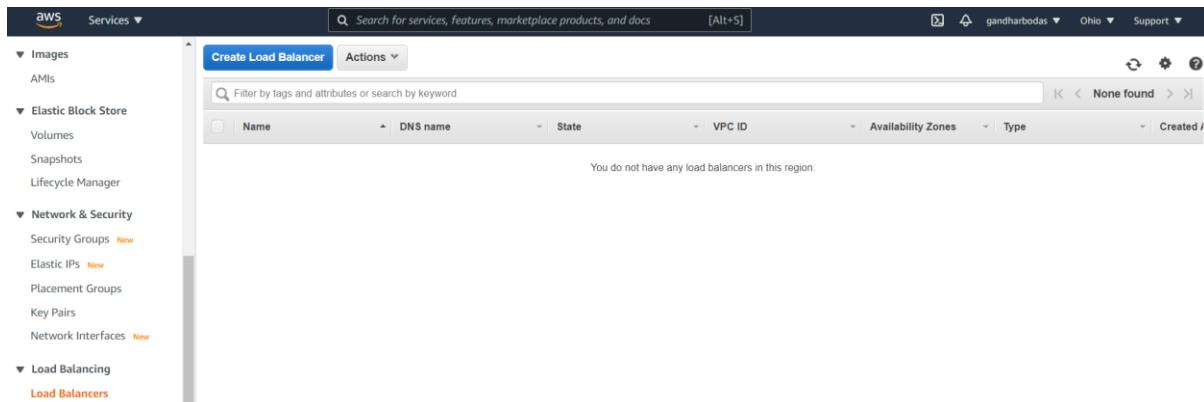


Instance 2: Follow the above same procedure to create another Instance

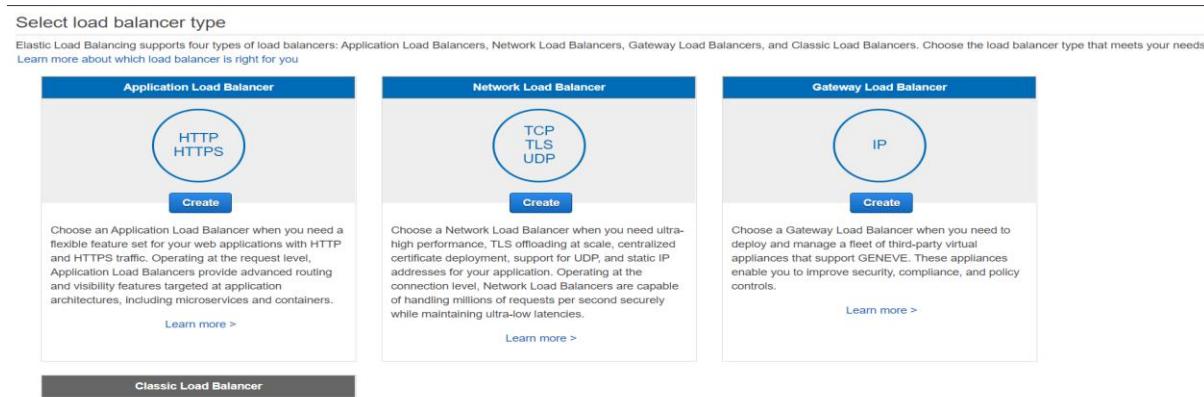


Step 2: Create Elastic Load Balancer:

Click on “Load Balancer” option which is on Left Hand Side.



Now click on “Application Load Balancer button”



Select “Application Load Balancer” and click on Create button. Now Basic configuration: Load Balancer Name- Demo, Load Balancer Protocols – HTTP, Port: 80, Availability Zones: tick on all check boxes, and now click on “Next: Assign Security Groups button” and you we be able to see the below screen:

Step 1: Define Load Balancer

Basic Configuration

This wizard will walk you through setting up a new load balancer. Begin by giving your new load balancer a unique name so that you can identify it from other load balancers you might create. You will also need to configure ports and protocols for your load balancer. Traffic from your clients can be routed from any load balancer port to any port on your EC2 instances. By default, we've configured your load balancer with a standard web server on port 80.

Load Balancer name:	Only a-z, A-Z, 0-9 and hyphens are allowed		
Create LB Inside:	My Default VPC (172.31.0.0/16)		
Create an internal load balancer:	<input type="checkbox"/> (what's this?)		
Enable advanced VPC configuration:	<input type="checkbox"/>		
Listener Configuration:			
Load Balancer Protocol	Load Balancer Port	Instance Protocol	Instance Port
HTTP	80	HTTP	80

Add

1. Define Load Balancer 2. Assign Security Groups 3. Configure Security Settings 4. Configure Health Check 5. Add EC2 Instances 6. Add Tags 7. Review

Step 2: Configure Security Settings

Warning: Improve your load balancer's security. Your load balancer is not using any secure listener.
If your traffic to the load balancer needs to be secure, use the HTTPS protocol for your front-end connection. You can go back to the first step to add/configure secure listeners under [Basic Configuration](#) section. You can also continue with current settings.

Click on “Next: Configure Security Groups” then Configure Security Groups page will be appearing.

Assign a security group: Create a new security group.

Security group name: group4.

Type: HTTP, Protocol: TCP, Port Range: 80, Source: Anywhere.

Once selected these all click on “Next: Configure Routing” button.

Step 3: Configure Security Groups

A security group is a set of firewall rules that control the traffic to your load balancer. On this page, you can add rules to allow specific traffic to reach your load balancer. First, decide whether to create a new security group or select an existing one.

Assign a security group	<input checked="" type="radio"/> Create a new security group <input type="radio"/> Select an existing security group		
Security group name	group4		
Description	load-balancer-wizard-1 created on 2021-03-19T20:45:38.309+05:30		
Type	Protocol	Port Range	Source
HTTP	TCP	80	Anywhere

Add Rule

Cancel Previous Next: Configure Routing

Once clicked on “Next: Configure Routing” button you will be able to see the below page:

Here, you will select Target group: New target group, Name: Group3, Target Type: Instance, Protocol: HTTP, Port: 80, Protocol version: HTTP1, and rest of the details keep as it is.

Step 4: Configure Routing

Your load balancer routes requests to the targets in this target group using the protocol and port that you specify, and performs health checks on the targets using these health check settings. The target group you specify in this step will apply to all of the listeners configured on this load balancer; you can edit the listeners and add listeners after the load balancer is created.

Target group

Target group	<input type="text" value="New target group"/>
Name	<input type="text" value="Group3"/>
Target type	<input checked="" type="radio"/> Instance <input type="radio"/> IP <input type="radio"/> Lambda function
Protocol	<input type="text" value="HTTP"/>
Port	<input type="text" value="80"/>

Protocol version

- HTTP1**
Send requests to targets using HTTP/1.1. Supported when the request protocol is HTTP/1.1 or HTTP/2.
- HTTP2**
Send requests to targets using HTTP/2. Supported when the request protocol is HTTP/2 or gRPC, but gRPC-specific features are not available.
- gRPC**
Send requests to targets using gRPC. Supported when the request protocol is gRPC.

Health checks

Protocol	<input type="text" value="HTTP"/>
Path	<input type="text" value="/"/>

[Advanced health check settings](#)

And later on, click on “Next: Register Targets button”. After clicking you will be able to see the Instances which we have created previously as such:

Step 5: Register Targets

Register targets with your target group. If you register a target in an enabled Availability Zone, the load balancer starts routing requests to the targets as soon as the registration process completes and the target passes the initial health checks.

Registered targets

To deregister instances, select one or more registered instances and then click Remove.

Remove	Instance	Name	Port	State	Security groups	Zone
No instances available.						

Instances

To register additional instances, select one or more running instances, specify a port, and then click Add. The default port is the port specified for the target group. If the instance is already registered on the specified port, you must specify a different port.

Add to registered on port

Search Instances

Instance	Name	State	Security groups	Zone	Subnet ID	Subnet CIDR
i-0fd3e6a910b3dbde1		running	Group3	us-east-2a	subnet-57f84f3c	172.31.0.0/20
i-0f6a907c7966292ca		running	Group1	us-east-2b	subnet-57fc112a	172.31.16.0/20

[Cancel](#) [Previous](#) [Next: Review](#)

Step 3: Add these two instances into the ELB's target group:

So, now click on two check boxes instance 1 and instance 2 and then click on “Add to registered”.

The screenshot shows the 'Registered targets' section of the Step 5: Register Targets page. It includes a 'Remove' button and a table with columns: Instance, Name, Port, State, Security groups, Zone, Subnet ID, and Subnet CIDR. Two instances are listed: i-0fd3e8a910b3dbde1 (running, Group3, us-east-2a, subnet-57fb4f3c, 172.31.0.0/20) and i-0f6a907c7966292ca (running, Group1, us-east-2b, subnet-57fc112a, 172.31.16.0/20). Below the table is an 'Instances' section with an 'Add to registered' button and a search bar. The search results show the same two instances listed again.

The moment I clicked on “Add to registered” button it will appear under “Registered targets”

The screenshot shows the 'Registered targets' section of the Step 5: Register Targets page after adding instances. The table now includes the two instances from the previous step, with their status set to 'running'. The 'Instances' section below also shows the same two instances.

Now, appeared under “Registered targets” click on Next: Review button” and you will able to see the below Review page:

The screenshot shows the Step 6: Review page. It displays the configuration details for the load balancer, including its name (Demo), scheme (internet-facing), listeners (Port:80 - Protocol:HTTP), IP address type (IPv4), VPC (vpc-51129e3a), subnets (subnet-57fb4f3c, subnet-57fc112a, subnet-1eaffa52), and tags. It also shows the security groups assigned to the load balancer, which are group3 and group4.

Routing

Target group New target group
Target group name Group3
Port 80
Target type instance
Protocol HTTP
Protocol version HTTP1
Health check protocol HTTP
Path /
Health check port traffic port
Healthy threshold 5
Unhealthy threshold 2
Timeout 5
Interval 30
Success codes 200

Targets

Instances i-0fd3e8a910b3dbde1:80, i-0f6a907c7966292ca:80

Add-on services

AWS Global Accelerator Disabled

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

[Cancel](#) [Previous](#) [Create](#)

Once reviewed then click on “Create button”. Once done you will be able to see the below page:

Load Balancer Creation Status

Successfully created load balancer
Load balancer [Demo](#) was successfully created.
Note: It might take a few minutes for your load balancer to be fully set up and ready to route traffic, and for the targets to complete the registration process and pass the initial health checks.

Suggested next steps

- Discover other services that you can integrate with your load balancer. Visit the [Integrated services](#) tab within [Demo](#)
- Consider using AWS Global Accelerator to further improve the availability and performance of your applications. [AWS Global Accelerator console](#)

[Close](#)

Once done then click on “Demo link” and it will take you to the home page as below:

Create Load Balancer Actions ▾

Filter by tags and attributes or search by keyword

Name	DNS name	State	VPC ID	Availability Zones	Type	Created /
Demo	Demo-1734106094.us-east-2...	active	vpc-51129e3a	us-east-2c, us-east-2a, ...	application	March 19,

Load balancer: [Demo](#)

Description [Listeners](#) [Monitoring](#) [Integrated services](#) [Tags](#)

Basic Configuration

Name	Demo
ARN	arn:aws:elasticloadbalancing:us-east-2:631052621391:loadbalancer/app/Demo/c9093932b6d9e454
DNS name	Demo-1734106094.us-east-2.elb.amazonaws.com (A Record)
State	active
Type	application
Scheme	internet-facing
IP address type	ipv4

[Edit IP address type](#)

VPC vpc-51129e3a [Edit](#)

Availability Zones

- subnet-1eaffa52 - us-east-2c [Edit](#)
IPv4 address: Assigned by AWS
- subnet-57f84f3c - us-east-2a [Edit](#)
IPv4 address: Assigned by AWS
- subnet-57fc112a - us-east-2b [Edit](#)
IPv4 address: Assigned by AWS

[Edit subnets](#)

Hosted zone Z3AADJGX6KTTL2

Creation time March 19, 2021 at 9:04:15 PM UTC+5:30

Security

Security groups sg-08f16589883aa1c57, group4
• load-balancer-wizard-1 created on 2021-03-19T20:45:38.309+05:30

[Edit security groups](#)

Attributes

Deletion protection	Disabled
Idle timeout	60 seconds
HTTP/2	Enabled
Desync mitigation mode	Defensive
Drop invalid header fields	Disabled
Access logs	Disabled
WAF fail open	Disabled

[Edit attributes](#)

Now, as part of the Load Balancer creation we created a Target Group as below:

EC2 > Target groups

Target groups (1) [info](#)

[Create target group](#)

<input type="checkbox"/>	Name	ARN	Port	Protocol	Target type	Load balancer
<input type="checkbox"/>	Group3	arn:aws:elasticloadbalancing:us-east-2:631052621391:targetgroup/Group3/05f500b332931096	80	HTTP	Instance	Demo

Now, go the home page of Name: Group3:

EC2 > Target groups > Group3

Group3

[Delete](#)

arn:aws:elasticloadbalancing:us-east-2:631052621391:targetgroup/Group3/05f500b332931096

Basic configuration

Target type Instance	Protocol : Port HTTP: 80 Protocol version HTTP1	VPC vpc-51129e3a Edit	Load balancer Demo Edit
-------------------------	--	--	--

Group details Targets Monitoring Tags

Health check settings

Protocol	Path
HTTP	/
Port	Healthy threshold
traffic-port	5 consecutive health check successes
Unhealthy threshold	Timeout
2 consecutive health check failures	5 seconds
Interval	Success codes
30 seconds	200

Attributes

Attributes for an Application Load Balancer target group are not editable.

Stickiness	Deregistration delay
Disabled	300 seconds
Slow start duration	Load balancing algorithm

Attributes

Attributes for an Application Load Balancer target group are not editable.

Stickiness	Deregistration delay
Disabled	300 seconds
Slow start duration	Load balancing algorithm
0 seconds	Round robin

These are the 2 EC2 Instances

Targets

Instance ID	Name	Port	Zone	Status	Status details
i-0fd3e8a910b3dbde1		80	us-east-2a	healthy	
i-0f6a907c7966292ca		80	us-east-2b	healthy	

Now again to the “Load Balancer” and you can able to see the State: active”.

Copy “DNS name: Demo-1734106094.us-east-2.elb.amazonaws.com” and paste it on a new tab. Once pasted then you will be able to see the below output:

OUTPUT:

← → ⌂ Not secure | demo-1734106094.us-east-2.elb.amazonaws.com

Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.

Thank you for using nginx.

END