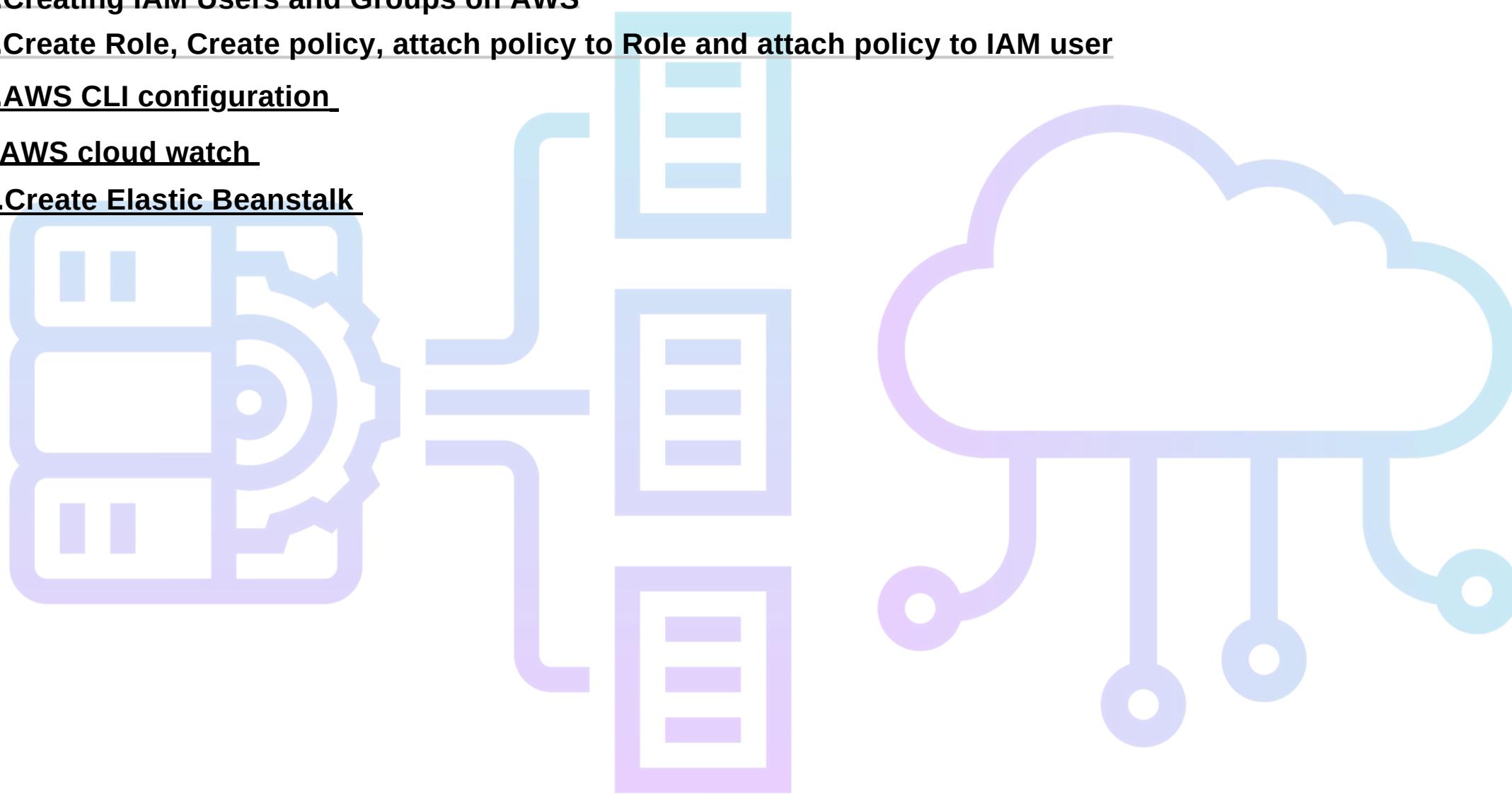


AWS

- 1.Create keypair
- 2.Create Security group
- 3. Create linux EC2 instance in AWS
- 4. Create EC2 windows instance in AWS
- 5. Create an elastic IP Address on AWS using AWS Elastic IP
- 6. Create EBS volume and attach(mount) to Ec2
- 7.How to Use a Snapshot to Restore an AWS EC2 Instance
- 8.Introduction to AWS Elastic Load Balancing
- 9.Monolith and Microservice in AWS
- 10.RDS and connect MySQL
- 11. Create bucket and host static website
- 12.Multi-Factor Authentication for IAM User
- 13.Create IAM User with Multi-Factor Authentication
- 14.Creating IAM Users and Groups on AWS
- 15.Create Role, Create policy, attach policy to Role and attach policy to IAM user
- 16.AWS CLI configuration
- 17.AWS cloud watch
- 18.Create Elastic Beanstalk



Create keypair

The screenshot shows the AWS EC2 Dashboard in the US East (Ohio) Region. The left sidebar navigation bar has 'Key Pairs' highlighted with a red box. The main content area displays various resources and features:

- Resources:** A summary of Amazon EC2 resources in the region, including Instances (running), Auto Scaling Groups, Dedicated Hosts, Elastic IPs, Instances, Key pairs, Load balancers, Placement groups, Security groups, Snapshots, and Volumes.
- Launch instance:** A section to start an Amazon EC2 instance, featuring a prominent "Launch instance" button.
- Scheduled events:** A section showing "US East (Ohio)" with "No scheduled events".
- Migrate a server:** A section about AWS Application Migration Service.
- Service health:** Information about the region being "US East (Ohio)".
- Zones:** A table listing three availability zones: us-east-2a (Zone ID: use2-az1), us-east-2b (Zone ID: use2-az2), and us-east-2c (Zone ID: use2-az3).
- Account attributes:** Details about the Default VPC (vpc-0b94752dea0bc251c) and Settings (Data protection and security, Zones, EC2 Serial Console, Default credit specification, Console experiments).
- Explore AWS:** A section with links to "10 Things You Can Do Today to Reduce AWS Costs", "Amazon GuardDuty Malware Protection", "Save up to 90% on EC2 with Spot Instances", and "Additional information".
- Additional information:** Links to Getting started guide, Documentation, All EC2 resources, Forums, and Pricing.

At the bottom, there are links for CloudShell, Feedback, and a footer with copyright information: © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms

The screenshot shows the AWS Management Console interface for the EC2 service, specifically the Key Pairs section. The URL in the address bar is <https://us-east-2.console.aws.amazon.com/ec2/home?region=us-east-2#KeyPairs>. The top navigation bar includes links for IAM, EC2, S3, API Gateway, Lambda, Simple Notification Service, Simple Queue Service, CloudWatch, Amazon EventBridge, AWS Chatbot, and Billing and Cost Management. The AWS logo and a search bar are also present.

The left sidebar contains a navigation menu with the following items:

- EC2 Dashboard
- EC2 Global View
- Events
- Instances
 - Instances
 - Instance Types
 - Launch Templates
 - Spot Requests
 - Savings Plans
 - Reserved Instances
 - Dedicated Hosts
 - Capacity Reservations
- Images
 - AMIs
 - AMI Catalog
- Elastic Block Store
 - Volumes
 - Snapshots
 - Lifecycle Manager
- Network & Security
 - Security Groups
 - Elastic IPs
 - Placement Groups
 - Key Pairs** (highlighted in blue)
 - Network Interfaces
- Load Balancing
 - Load Balancers
 - Target Groups

The main content area displays a table titled "Key pairs (1) Info". The table has columns for Name, Type, Created, Fingerprint, and ID. One row is shown, representing the key pair "thinkpad_keypair" which was created on "2024/01/08 18:37 GMT-6" and has a specific "Fingerprint" value. A red box highlights the "Create key pair" button at the top right of the table header.

Name	Type	Created	Fingerprint	ID
thinkpad_keypair	rsa	2024/01/08 18:37 GMT-6	f6:ed:d8:5f:ef:1d:2e:b0:9a:e3:7f:9a:d5:86:76:79:18:39:de:c9	key-0cecbca75f7d2b58

Create key pair Info

Key pair

A key pair, consisting of a private key and a public key, is a set of security credentials that you use to prove your identity when connecting to an instance.

Name

JJ-Demo-TodaysDate

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type Info

RSA

ED25519

Private key file format

.pem

For use with OpenSSH

.ppk

For use with PuTTY

Tags - optional

No tags associated with the resource.

[Add new tag](#)

You can add up to 50 more tags.

Cancel

Create key pair

File Edit View History Bookmarks Tools Help

Key pairs | EC2 | us-east-2 X + https://us-east-2.console.aws.amazon.com/ec2/home?region=us-east-2#KeyPairs:

aws Services Search [Alt+S]

IAM EC2 S3 API Gateway Lambda Simple Notification Service Simple Queue Service CloudWatch Amazon EventBridge AWS Chatbot Billing and Cost Management

EC2 Dashboard X Successfully created key pair

Key pairs (2) Info

Find Key Pair by attribute or tag

Name	Type	Created	Fingerprint	ID
thinkpad_keypair	rsa	2024/01/08 18:37 GMT-6	f6:ed:d8:5f:ef:1d:2e:b0:9a:e3:7f:9a:d5:86:76:79:18:39:de:c9	key-0cecbca75f7d2b58
JJ-Demo-TodaysDate	rsa	2024/01/09 09:44 GMT-6	6b:9d:3d:13:e6:f3:41:09:ef:cd:be:9a:4a:6a:8a:cb:31:1a:36:b1	key-05a6dc37a536339a8

Actions Create <

Instances Instances Instance Types Launch Templates Spot Requests Savings Plans Reserved Instances Dedicated Hosts Capacity Reservations New

Images AMIs AMI Catalog

Elastic Block Store Volumes Snapshots Lifecycle Manager

Network & Security Security Groups Elastic IPs Placement Groups Key Pairs Network Interfaces

Load Balancing Load Balancers Target Groups Trust Stores New

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

Keypair is created

Now create security group

The screenshot shows the AWS Management Console interface for the EC2 service. The left sidebar navigation bar is visible, with the 'Key Pairs' section highlighted by a red box. The main content area displays a table titled 'Key pairs (2) Info' containing the following data:

Name	Type	Created	Fingerprint	ID
thinkpad_keypair	rsa	2024/01/08 18:37 GMT-6	f6:ed:d8:5f:ef:1d:2e:b0:9a:e3:7f:9a:d5:86:76:79:18:39:de:c9	key-0ceccbbca75f7d2b58
JJ-Demo-TodaysDate	rsa	2024/01/09 09:44 GMT-6	6b:9d:3d:13:e6:f3:41:09:ef:cd:be:9a:4a:6a:8ac:cb:31:1a:36:b1	key-05a6dc37a536339a8

The browser address bar shows the URL: <https://us-east-2.console.aws.amazon.com/ec2/home?region=us-east-2#KeyPairs>.

EC2 Dashboard X Security Groups (3) Info

EC2 Global View Export security groups to CSV Create security group

Find resources by attribute or tag

Instances Actions < 1 > @

Name	Security group ID	Security group name	VPC ID	Description	Owner	Inbound
-	sg-086de69c963ef4de2	default	vpc-0b94752dea0bc251c	default VPC security group	112074902077	1 Perm
-	sg-0e14c9e99133a0ea0	launch-wizard-1	vpc-0b94752dea0bc251c	launch-wizard-1 created 2023-12-20T...	112074902077	1 Perm
-	sg-04be4eca5b2d42cb9	JJ_SG_useast2	vpc-0b94752dea0bc251c	test security group for ec2f	112074902077	3 Perm

Instances Images Elastic Block Store Network & Security Load Balancing

AMIs AMI Catalog

Volumes Snapshots Lifecycle Manager

Security Groups Elastic IPs Placement Groups Key Pairs Network Interfaces

Load Balancers Target Groups Trust Stores New

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

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

JJ_SG_demo_useast2

Name cannot be edited after creation.

Description Info

Security Group Tutorial Demo

VPC Info

vpc-0b94752dea0bc251c

Inbound rules Info

This security group has no inbound rules.

Add rule

Outbound rules Info

Type Info

Protocol Info

Port range Info

Destination Info

Description - optional Info

All traffic

All

All

Custom

Q

0.0.0.0/0 X

Add rule

Inbound rules [Info](#)

Type Info	Protocol Info	Port range Info	Source Info	Description - optional Info	Delete
RDP	TCP	3389	My IP	<input type="text"/> Edit	Delete

[Add rule](#)

Outbound rules [Info](#)

Type Info	Protocol Info	Port range Info	Destination Info	Description - optional Info	Delete
All traffic	All	All	Custom	<input type="text"/> Edit 0.0.0.0/0 X	Delete

[Add rule](#)

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

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.

[Add new tag](#)

You can add up to 50 more tags

[Cancel](#) Create security group

IAM EC2 S3 API Gateway Lambda Simple Notification Service Simple Queue Service CloudWatch Amazon EventBridge AWS Chatbot Billing and Cost Management

EC2 Dashboard EC2 Global View Events Instances Instances Instance Types Launch Templates Spot Requests Savings Plans Reserved Instances Dedicated Hosts Capacity Reservations New

Images AMIs AMI Catalog

Elastic Block Store Volumes Snapshots Lifecycle Manager

Network & Security Security Groups Elastic IPs Placement Groups Key Pairs Network Interfaces

Load Balancing Load Balancers Target Groups Trust Stores New

CloudShell Feedback

Security group (sg-03005b0b4de40c034 - JJ_SG_demo_useast2) was created successfully

Details

EC2 > Security Groups > sg-03005b0b4de40c034 - JJ_SG_demo_useast2

sg-03005b0b4de40c034 - JJ_SG_demo_useast2

Actions

Details

Security group name	JJ_SG_demo_useast2	Security group ID	sg-03005b0b4de40c034	Description	Security Group Tutorial Demo	VPC ID	vpc-0b94752dea0bc251c
Owner	112074902077	Inbound rules count	1 Permission entry	Outbound rules count	1 Permission entry		

Inbound rules Outbound rules Tags

Inbound rules (1)

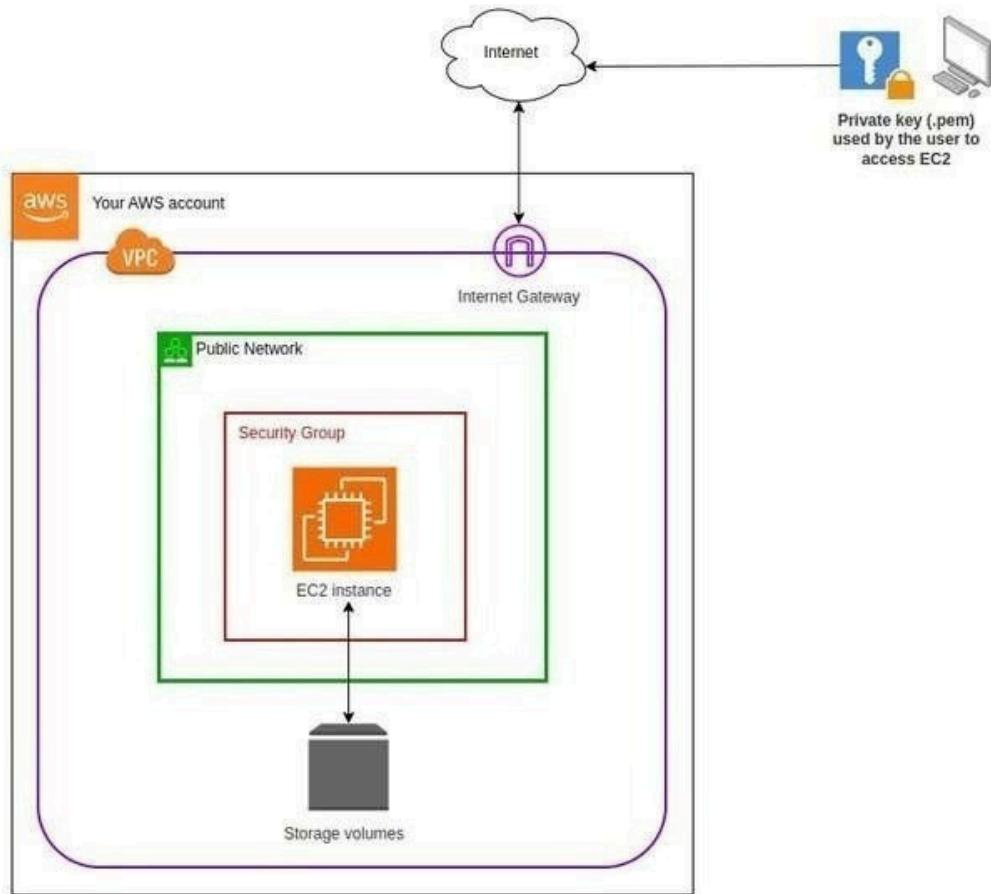
Name	Security group rule...	IP version	Type	Protocol	Port range	Source	Description
-	sgr-00ff395e80eb44388	IPv4	RDP	TCP	3389		-

Manage tags Edit inbound rules

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

Shortcuts 10:19 AM

Create linux EC2 instance in AWS



So, let's get started with the fundamentals and gradually explore advanced configurations to unlock the full potential of AWS EC2!

Step 1: Sign In to AWS

Log in to your AWS Management Console (<https://aws.amazon.com/console/>) using your AWS account credentials.

From the AWS Management Console, locate the "Services" dropdown and select "EC2" under the "Compute" section.

Step 2: Launch an Instance

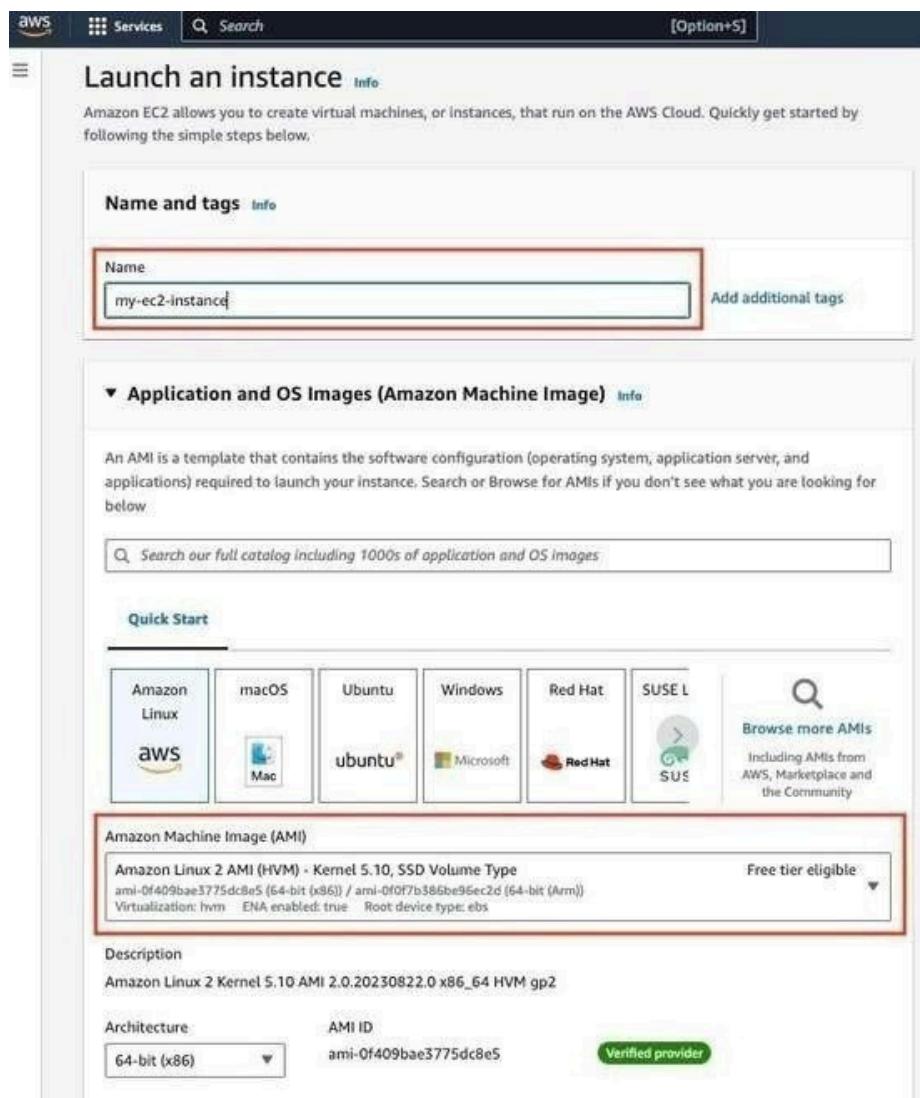
In the EC2 Dashboard, click the "Instances" link in the left navigation pane, then click the orange "Launch Instance" button.



Step 3: Choose an Amazon Machine Image (AMI)

Give a name to your instance.

- Choose an AMI that matches your requirements.
- AMIs are pre-configured templates that include an operating system and other software. Most of the world's servers use Linux because it's open-source, reliable, and efficient. It's commonly used for web servers, databases, and more. For this guide, we'll choose a Linux AMI.



Step 4: Choose an Instance Type

Give a name to your instance.

- Choose an AMI that matches your requirements.
- AMIs are pre-configured templates that include an operating system and other software. Most of the world's servers use Linux because it's open-source, reliable, and efficient. It's commonly used for web servers, databases, and more. For this guide, we'll choose a Linux AMI.

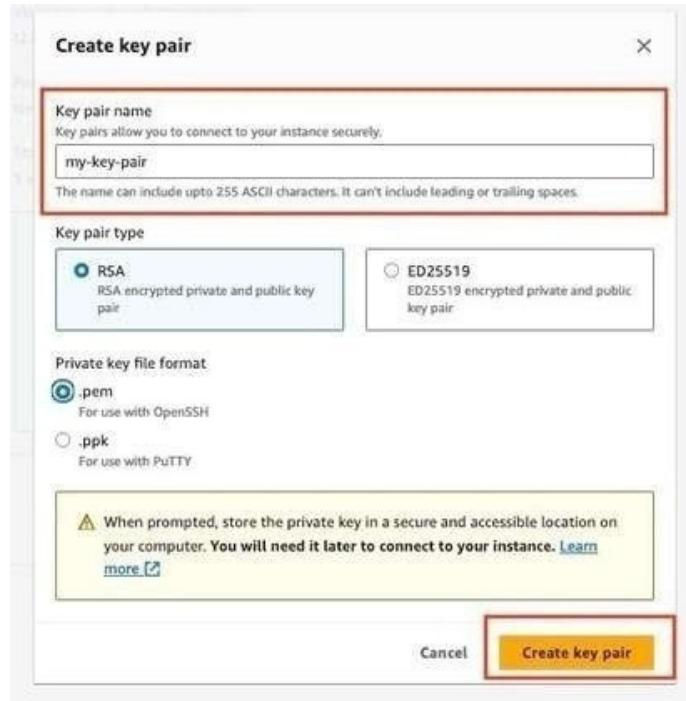


Step 5: Create or Select a Key Pair

You need a key pair to securely connect to your instance using SSH. Create a new key pair or select an existing one. Make sure to safely store the private key file, as it's the key to accessing your server. If you lose it, you won't be able to access the instance. You can add other key pairs later if needed.

Select create a new key pair and give a name to your `.pem` key.

- Click on the “Create key pair” orange button.
- A `.pem` key will get downloaded into your local computer.



Step 6: Configure Network Details

Here, you can choose the network settings (like the VPC and subnet), and more. For now, we'll use

the default VPC and subnet. Think of VPC as a private network, and we'll dive deeper into it later.



Step 7: Configure Security Group

Security groups act as virtual firewalls for your instance. Define inbound and outbound rules to control network traffic. For now, use the default security group. We can delve deeper into it later on how we use security groups for security.



Step 8: Add Storage

Configure the amount and type of storage for your instance. You can add additional storage volumes if needed.



Step 9: Review and Launch

Review your instance configuration settings. If everything looks good, click the "Launch" button.

Step 10: Launch Status

As you delve deeper into the EC2 service, you will gradually grasp and gain insights into additional settings, expanding your understanding and knowledge over time.

Once you click "Launch," your instance will start launching. You'll see its status change to

- "running" in the EC2 Dashboard.

Name	Instance ID	Instance state	Instance type
my-ec2-instance	i-03b2cf8cd1cc7448c	Running	t2.micro

Step 11: Access Your Instance using "ssh"

Once your instance is running, go to the EC2 Dashboard, select your instance, and click the "Connect" button. You'll find instructions for both Linux and Windows connections below:

Connecting from Mac and Linux:

Open a terminal on your local machine.

- Navigate to the directory where you saved your private key file (.pem).
- Use the "`chmod`" command to set the appropriate permissions on the key file:
 -
- `chmod 400 <your-key-file>.pem`

Copy the SSH command from the EC2 instance connect page.

- Paste the command into your terminal and press Enter
 -

Connecting from Windows:

Download and install an SSH client such as PuTTY.

- Convert your .pem key file to a .ppk key file using PuTTYgen.
- Open PuTTY and enter the public IP address of your instance in the "Host Name" field.
- Load your .ppk key file in the "Connection > SSH > Auth" settings.
- Click "Open" to start the SSH session.
-

Step 13: Access Your Instance using "AWS Session Manager"

You can access now the instance through the AWS console using Session Manager.

This provides a browser-based session similar to EC2 Instance Connect, eliminating the need to open port 22.

Step 1: Right click keypair file and open gitbash

Step 2 copy 2 commands
and paste
in gitbash as shown step 3

EC2 Instance Connect Session Manager SSH client EC2 serial console

Instance ID
i-07df547babb8834c0 (VM_1)

1. Open an SSH client.

Command copied: vate key file. The key used to launch this instance is psa_keys_details.pem. You can use the chmod command, if necessary, to ensure your key is not publicly viewable.
chmod 400 "psa_keys_details.pem"

4. Connect to your instance using its Public DNS:
ec2-15-207-109-118.ap-south-1.compute.amazonaws.com

Example:
ssh -i "psa_keys_details.pem" ec2-user@ec2-15-207-109-118.ap-south-1.compute.amazonaws.com

Note: In most cases, Ch mode command everything later file permissions also we are going to talk about in our series of lecture but correct. However, read your AMI usage in

Step 3

```
Admin@DESKTOP-9DFQ51N MINGW64 /g/key_pair
$ chmod 400 "psa_keys_details.pem"

Admin@DESKTOP-9DFQ51N MINGW64 /g/key_pairs_aws
$ ssh -i "psa_keys_details.pem" ec2-user@ec2-15-207-109-118.ap-south-1.compute.amazonaws.com
```

```
Warning: Permanently added 'ec2-15-207-109-118.ap-south-1.compute.amazonaws.com' (ED25519) to the list of known hosts.
, #_
~\_\####_
~~\####\#
~~\###|
~~\#/ __
x/amazon-linux-2023 ~ V~' '-->
~~\~/,-/ \
~~\~/,-/ \
[ec2-user@ip-172-31-52-92 ~]$
```

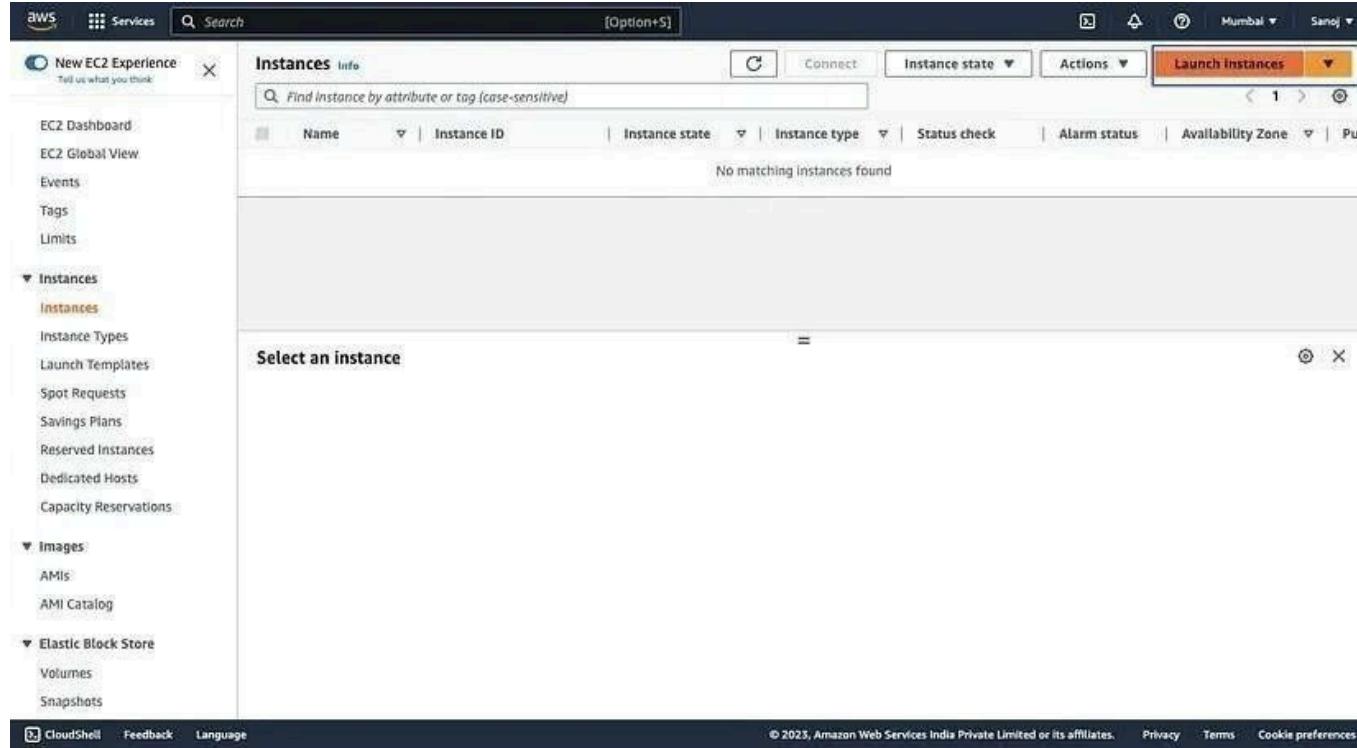
Amazon Linux 2023
<https://aws.amazon.com/linux>

-----> Done

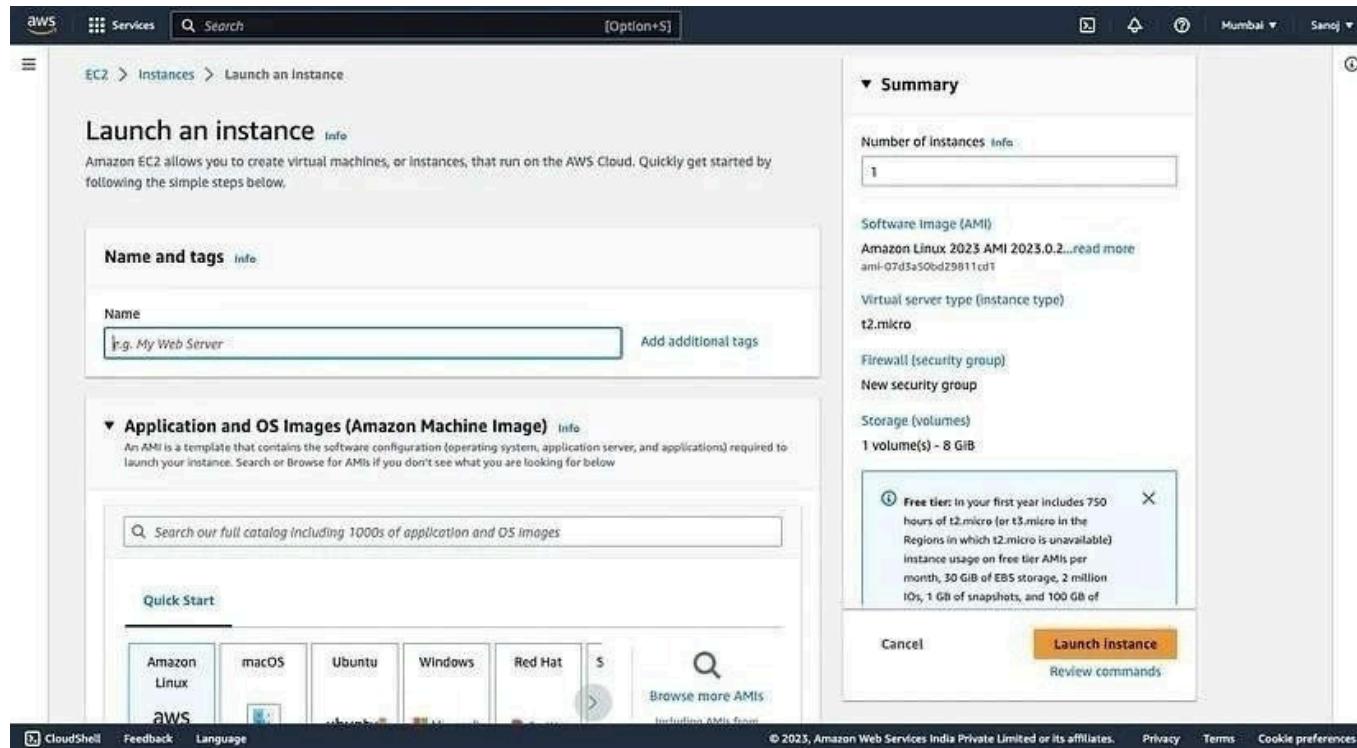
How to create a Windows Ec2 instance in AWS?



Step 1: Sign in to the AWS Management Console and click on the “Launch Instances”



After clicking on the “Launch Instances” the following interface will appear.



Step 2: Now give the Instance name, I gave the name “Windows-Server”

The screenshot shows the 'Launch an instance' wizard in the AWS EC2 console. The 'Name and tags' step is active, with the instance name 'Windows-Server' entered in the 'Name' field. The 'Summary' section on the right shows the configuration: 1 instance, Amazon Linux 2023 AMI 2023.0.2, t2.micro instance type, and a new security group. A tooltip for the t2.micro instance type indicates it's included in the free tier. The 'Launch Instance' button is highlighted.

Step 3: Select the AMI (Amazon Machine Image) or OS.

The screenshot shows the 'Application and OS Images (Amazon Machine Image)' step in the AWS EC2 console. The 'Windows' tab is selected in the 'Quick Start' menu. The 'Microsoft Windows Server 2022 Base' AMI is selected, showing its details: ami-09461328af8fbcb9c (64-bit (x86)), Virtualization: hvm, ENA enabled: true, Root device type: ebs. The 'Free tier eligible' status is also indicated. The 'Summary' section on the right remains the same as in the previous step, showing 1 instance of Amazon Linux 2023 AMI 2023.0.2, t2.micro instance type, and a new security group. A tooltip for the t2.micro instance type is visible. The 'Launch Instance' button is highlighted.

Step 4: Select the Instance Type or Hardware Type, I selected t2.micro.

The screenshot shows the AWS CloudShell interface with the following details:

- Services**: Services menu is open, showing options like Amazon Linux, macOS, Ubuntu, Windows, Red Hat, and S. A search bar and [Option+S] button are also present.
- Browse more AMIs**: A callout box indicates that the list includes AMIs from AWS, Marketplace, and the Community.
- Number of Instances**: Set to 1.
- Software Image (AMI)**: Microsoft Windows Server 2022 Base (ami-09461328af8fbcb9c).
- Virtual server type (instance type)**: t2.micro.
- Firewall (security group)**: New security group.
- Storage (volumes)**: 1 volume(s) - 30 GiB.
- Free tier eligible**: Information about the free tier is displayed, stating it covers 750 hours of t2.micro usage per month.
- Launch Instance**: The primary action button at the bottom right.

Step 5: Select your “Key pair” by clicking on the Drop down menu, if you don’t have , create new “key pair”.

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

Select

Proceed without a key pair (Not recommended) Default value

my-key Type: rsa

Network Info

vpc-0188f5a0c77bec16d

Subnet Info

No preference (Default subnet in any availability zone)

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

We'll create a new security group called 'launch-wizard-1' with the following rules:

Allow RDP traffic from Anywhere Helps you connect to your instance

Summary

Number of instances Info

1

Software Image (AMI)

Microsoft Windows Server 2022 ...read more
ami-09461328af8fbcb9c

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

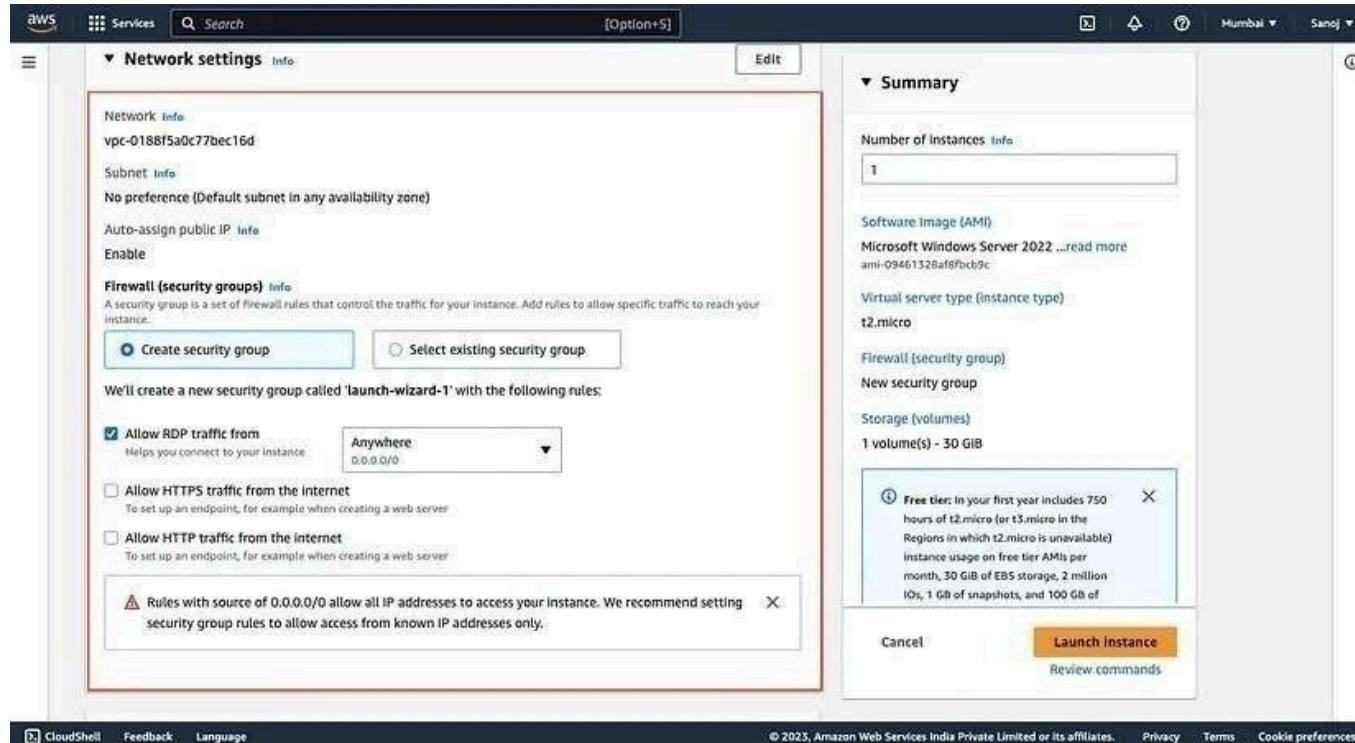
Storage (volumes)

1 volume(s) - 30 GB

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

Step 6: Select your security group if you have already if you don't have a, create a new security group.

Note: If you keep it as it is, AWS will create a new security group for you.



Step 7: Click on the “Launch Instance”.

The screenshot shows the 'Configure storage' section of the EC2 instance creation wizard. It specifies a root volume of 30 GiB using an gp2 SSD type. A note indicates that free-tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. Below this, it notes that the selected AMI contains more instance store volumes than the instance allows, and only the first 0 instance store volumes from the AMI will be accessible from the instance. The 'File systems' section is currently empty. The 'Advanced details' section is also visible.

Configure storage

Root volume (Not encrypted)

30 GiB gp2

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

Add new volume

The selected AMI contains more instance store volumes than the instance allows. Only the first 0 instance store volumes from the AMI will be accessible from the instance.

File systems

Advanced details

Summary

Number of instances: 1

Software Image (AMI): Microsoft Windows Server 2022 ...read more ami-09461328af8fbcb9c

Virtual server type (instance type): t2.micro

Firewall (security group): New security group

Storage (volumes): 1 volume(s) - 30 GiB

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

Cancel Launch instance Review commands

After clicking on the “launch Instance” the following interface will appear, just click on the “View all instances”

The screenshot shows the 'Success' page after launching an instance. It displays a success message: "Successfully initiated launch of instance i-0642a220c4322e36r". Below this, there's a 'Launch log' link and a 'Next Steps' section with various options:

- Create billing and free tier usage alerts
- Connect to your instance
- Connect an RDS database
- Create EBS snapshot policy
- Manage detailed monitoring
- Create Load Balancer
- Create AWS budget
- Manage CloudWatch alarms

A navigation bar at the bottom includes 'View all instances' (which is highlighted in orange), 'CloudShell', 'Feedback', 'Language', and links to 'Privacy', 'Terms', and 'Cookie preferences'.

Success

Successfully initiated launch of instance i-0642a220c4322e36r

Launch log

Next Steps

View all instances

The screenshot shows the AWS EC2 Instances page. On the left, there's a navigation sidebar with sections like EC2 Dashboard, EC2 Global View, Events, Tags, Limits, Instances (selected), Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, Images (AMIs, AMI Catalog), and Elastic Block Store (Volumes, Snapshots). The main content area displays a table of instances. One instance, named "Windows-Server" with the ID i-0642a22bc4322e36e, is listed and is currently running. The "Actions" dropdown menu is open, showing options like "Launch instances", "Stop", "Start", "Reboot", "Shutdown", "Delete", "Copy tags", "Edit tags", and "Connect".

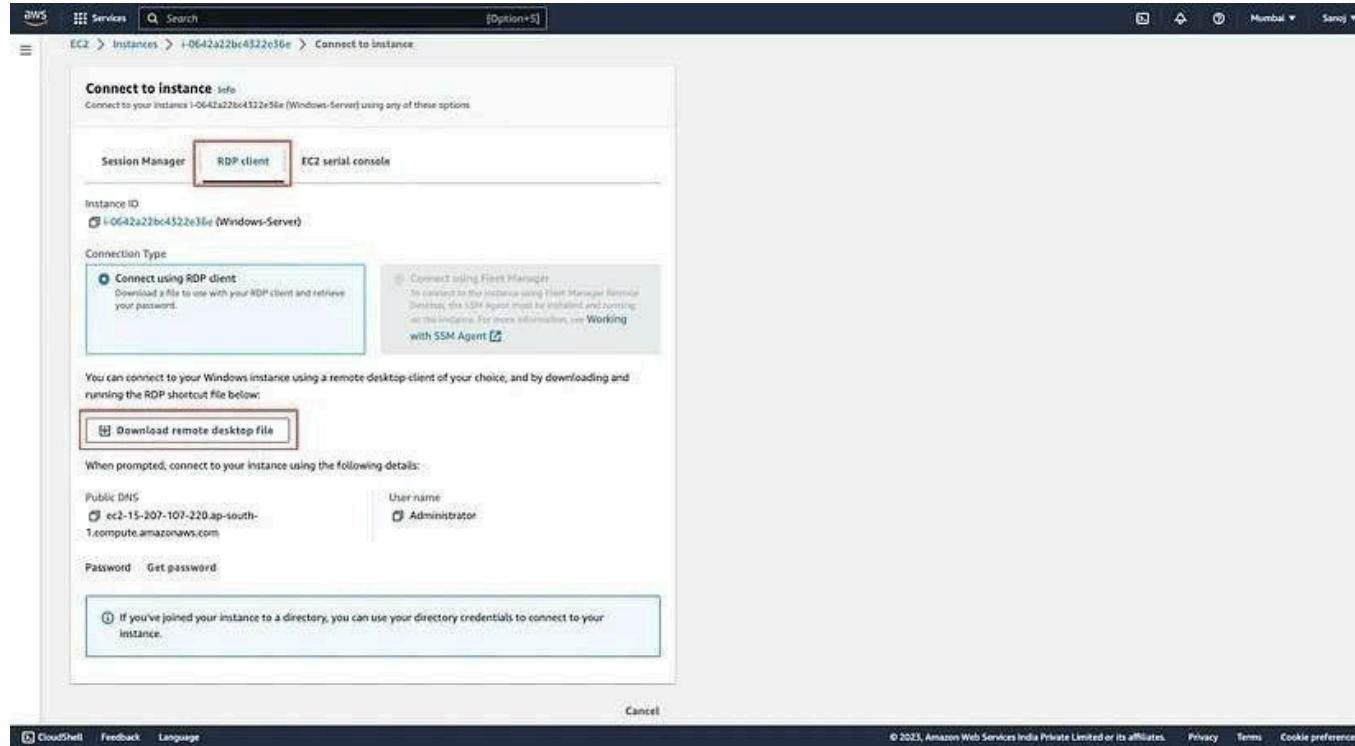
Now it's time to connect our Ec2 instance that we have recently launched.

Step 8: Select your Windows Instance and Click on the “Connect”.

This screenshot shows the same EC2 Instances page as before, but with a specific action taken. The "Windows-Server" instance has been selected, as indicated by a checked checkbox in the first column of the table. The "Actions" dropdown menu is still open, and the "Connect" button is now highlighted in yellow, indicating it is the next step to be performed.

Step 9: After Clicking on “Connect” the following interface will appear. just select the “RDP Client” Tab and download the “Remote desktop file”.

Note: In the case of Windows only, Linux and mac have different mechanisms to connect RDP Connection.



Step 10: Now click on the “Get password”, select your “key pair” and decrypt the password.

Get Windows password [Info](#)

Use your private key to retrieve and decrypt the initial Windows administrator password for this instance.

Instance ID: i-0642a22bc4322e36e (Windows-Server)

Key pair associated with this instance: my-key

Private key
Either upload your private key file or copy and paste its contents into the field below.

[Upload private key file](#)

my-key.cer
1.674KB

Private key contents - optional

```
-----BEGIN RSA PRIVATE KEY-----  
MIIEowIBAAKCAQEAjazyET8ShlqMjoaRrRoYIDcN4O4ONUID5qn5A4L1alnS//  
b+qNW+XS+Dcy6zOzyd/xYFl5hf21oppOFvUloNQjh8012R4b6b55XKGASZ/xN  
MZW1+Hw2gtlQ+i7ALE9B+E39osYFU1KRh7nCtfDa8qgwn9hdJBm8Jr?PtvFdzoB  
tt2QAOaEalllaXx9K+n08jh7pscUBL32b842h55p0kO+6Y2QSwhBC55jRvKKoJ  
VYNyj6oi1L1ekG4ppNAfeD17AYZBy/Eml3xKwtdCOg9ImHQNdjUSMEv14HzAH2v  
sjdNS5ilovCuSRbrROvl6BXna/giRZltB1pNtQIDAQABaoIBAHjNBpK9GknhF1E  
wdnp4oFGYPtgt25Y0yh/NwYQxKoyvd55Mfvrl6VVH466CMgWAGcSA6svl+Nbm6NbZ
```

[Cancel](#) [Decrypt password](#)

CloudShell Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

Step 11: After clicking on the “Decrypt password” the following interface will appear to copy the password and use that password to connect your Windows EC2 instance

Connection Type

Connect using RDP client
Download a file to use with your RDP client and retrieve your password.

Connect using Fleet Manager
To connect to the instance using Fleet Manager Remote Desktop, the SSH Agent must be installed and running on the instance. For more information, see [Working with SSM Agent](#).

You can connect to your Windows instance using a remote desktop client of your choice, and by downloading and running the RDP shortcut file below:

[Download remote desktop file](#)

When prompted, connect to your instance using the following details:

Public DNS: ec2-15-207-107-220.ap-south-1.compute.amazonaws.com

User name: Administrator

Password: BUhc*tOK?gN-4Dd-ErujtETr4&ba2L

If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.

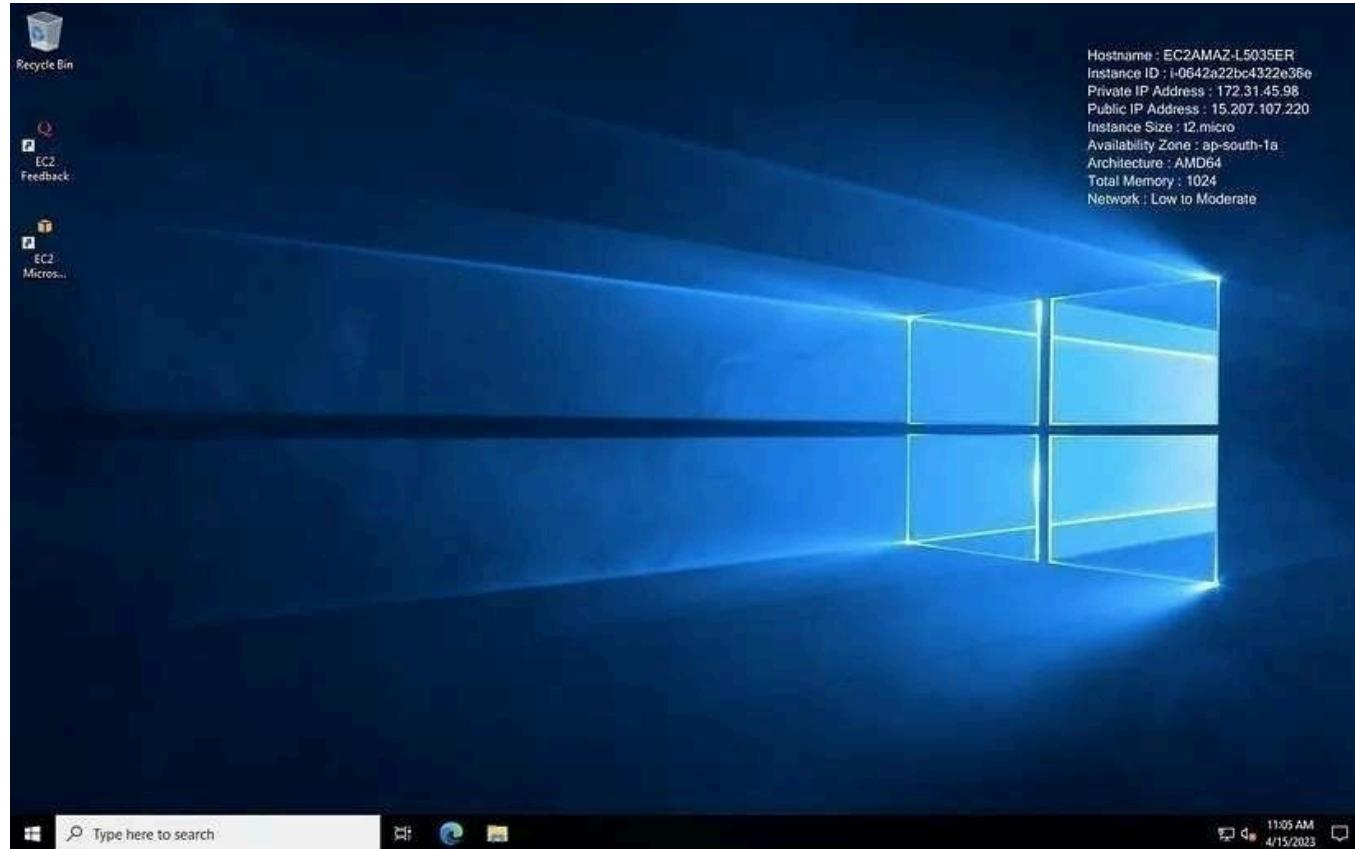
[Cancel](#)

CloudShell Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

Step 12: Open your Downloaded file “RDP file” and put, the password that you decrypted.

The default user name will be “Administrator” and the password is that you have decrypted and shown in the above screenshot.

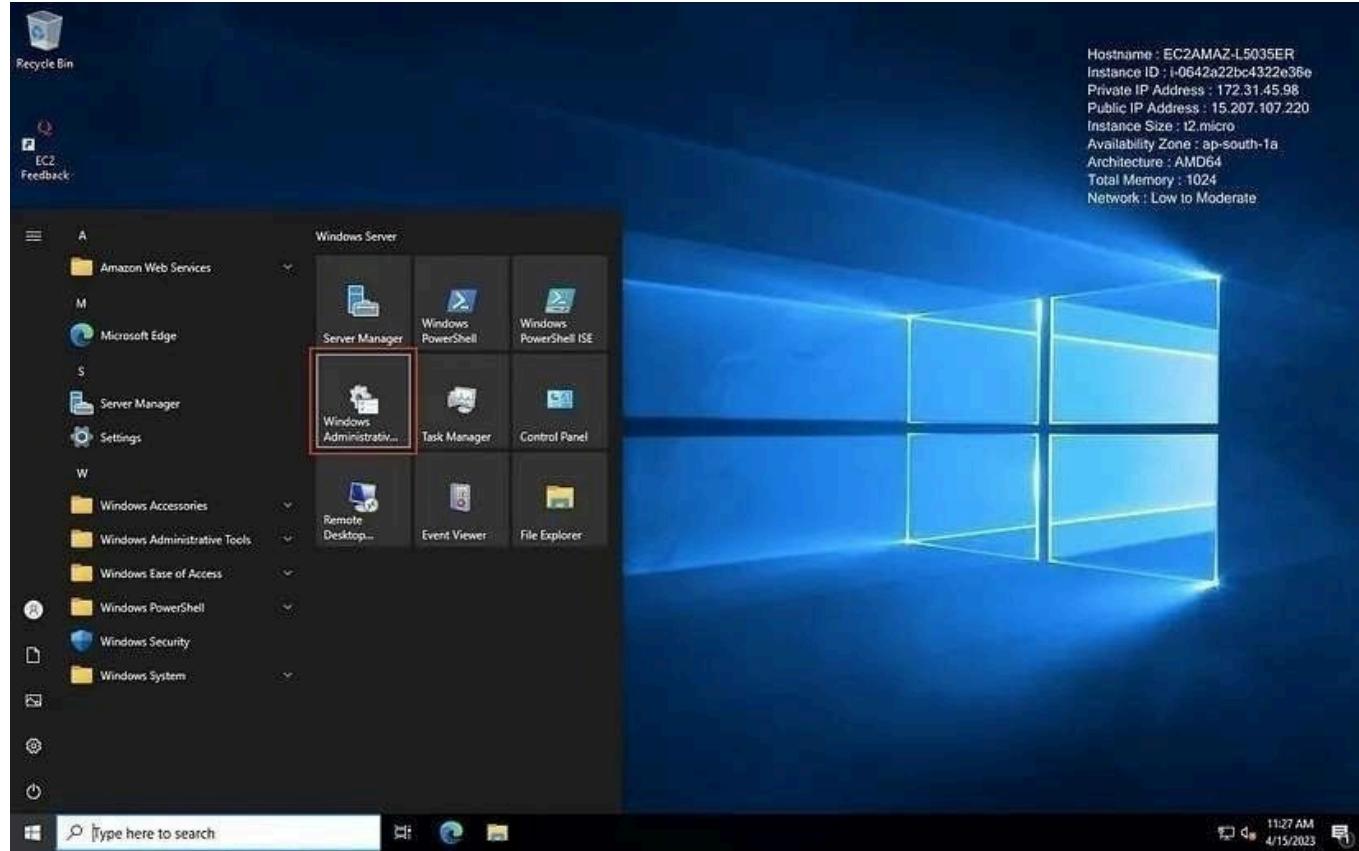
Note: Every time whenever you want to connect after closing the session you need to regenerate the password or decrypt the using “Key pair”



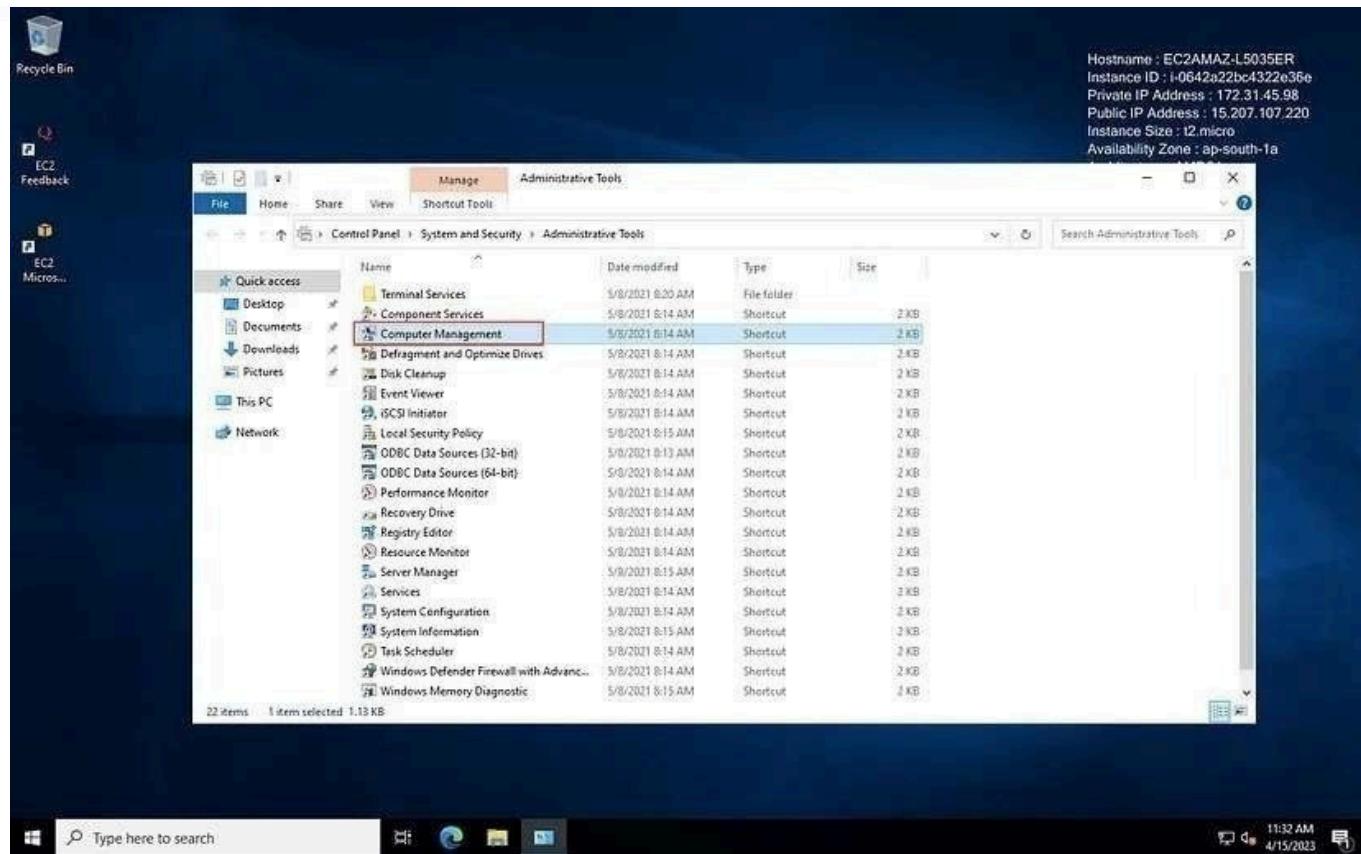
Now we don't want to decrypt the password every time to connect the Windows EC2 instance for that just change the Windows Password.

Now the question is how we can do that.

Step 13: Press Windows Button or Click on the “Windows Icon”, then click on “Windows Administrative tool”.

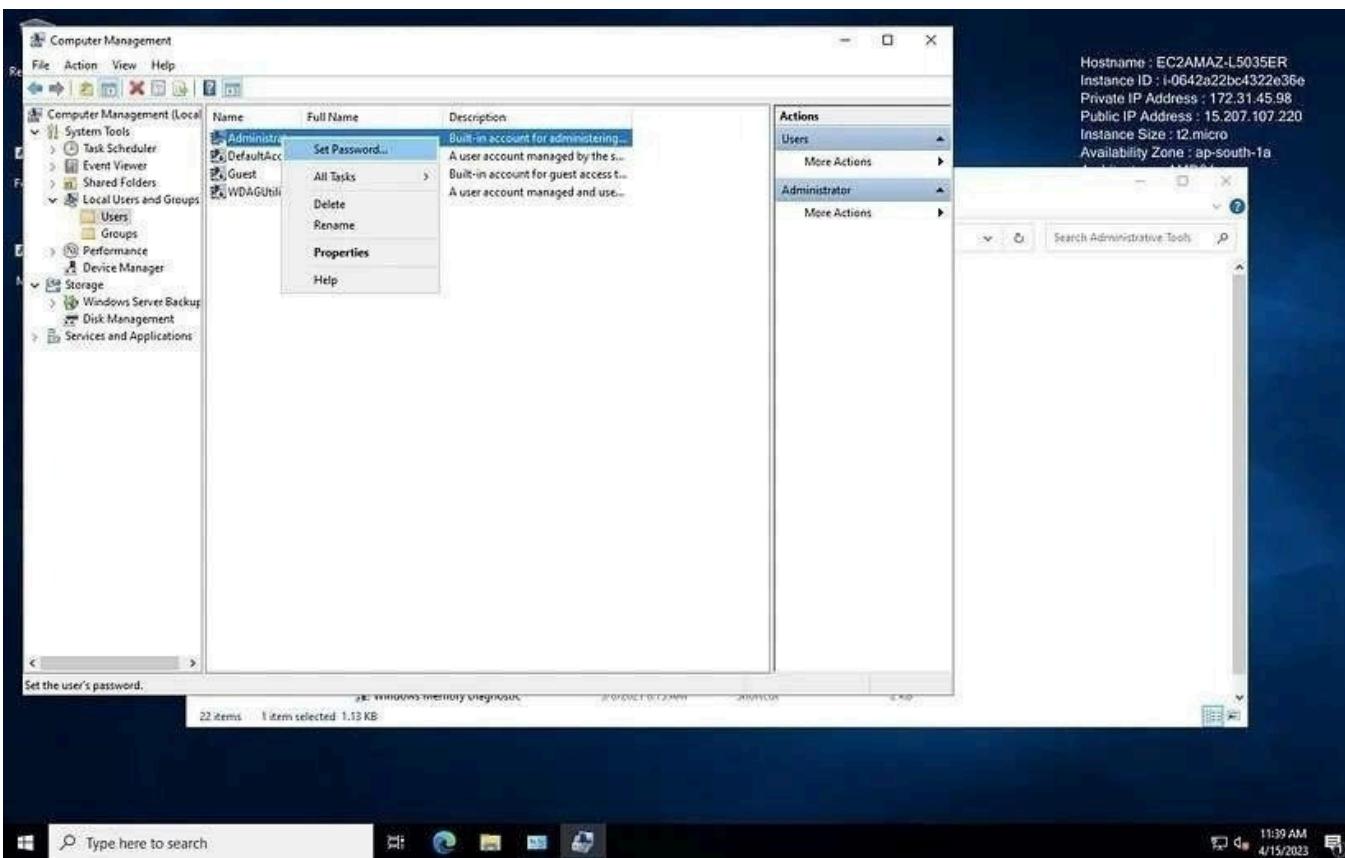
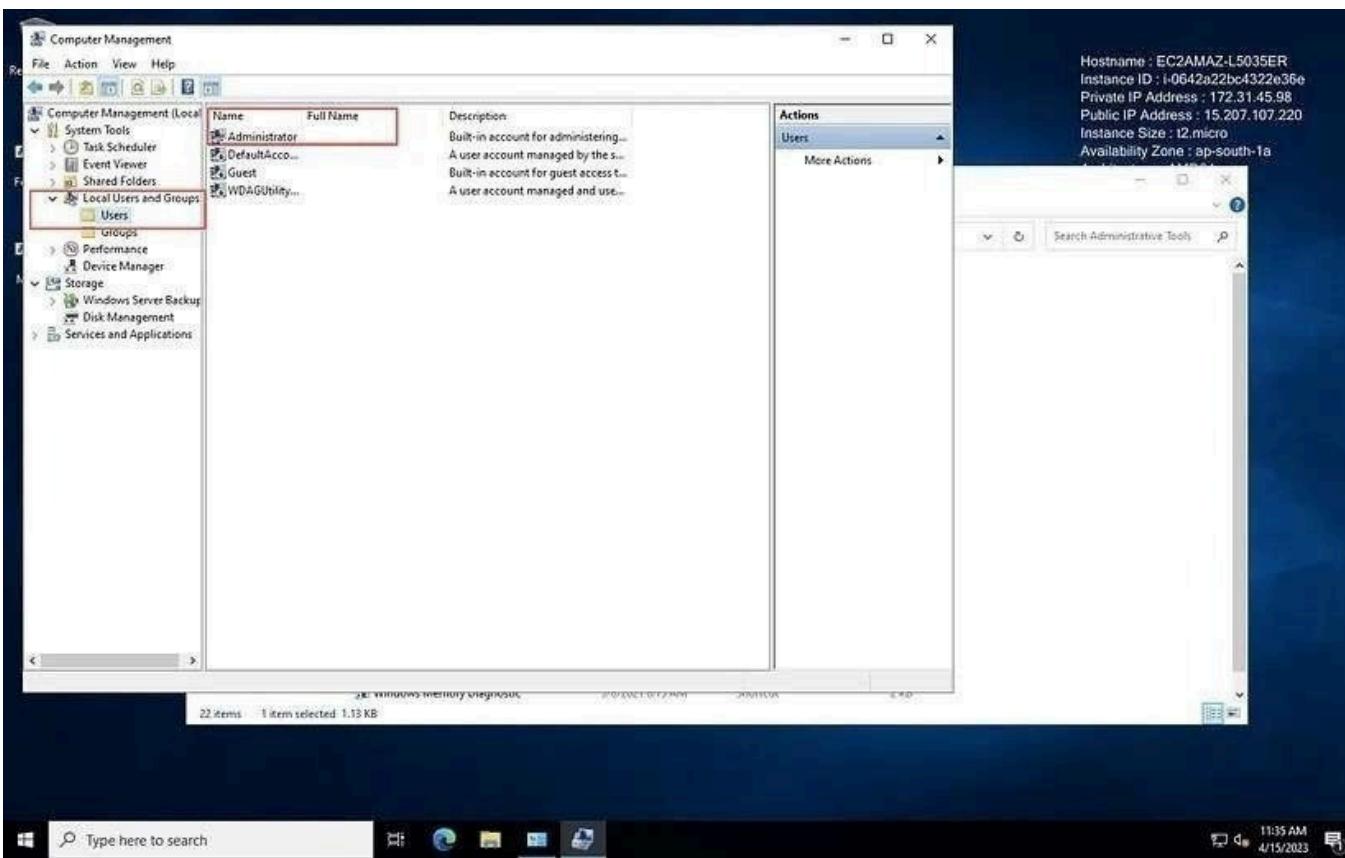


After clicking the “Windows Administrative tool” the following interface will appear, just click on “Computer Management”

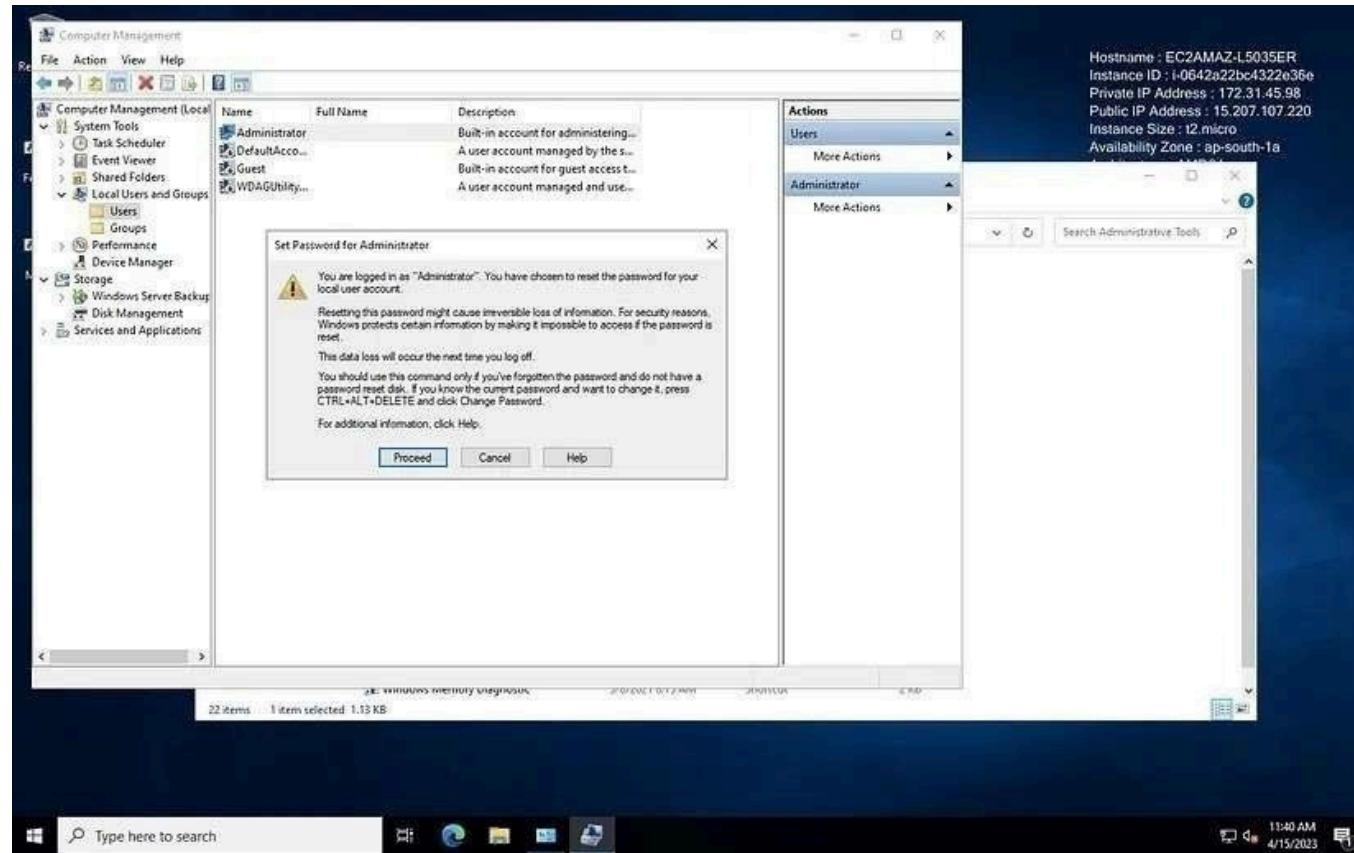


Step 14: After clicking on “Computer Management” the following interface will appear. Just click on “Local Users and Groups” then click on “Users”.

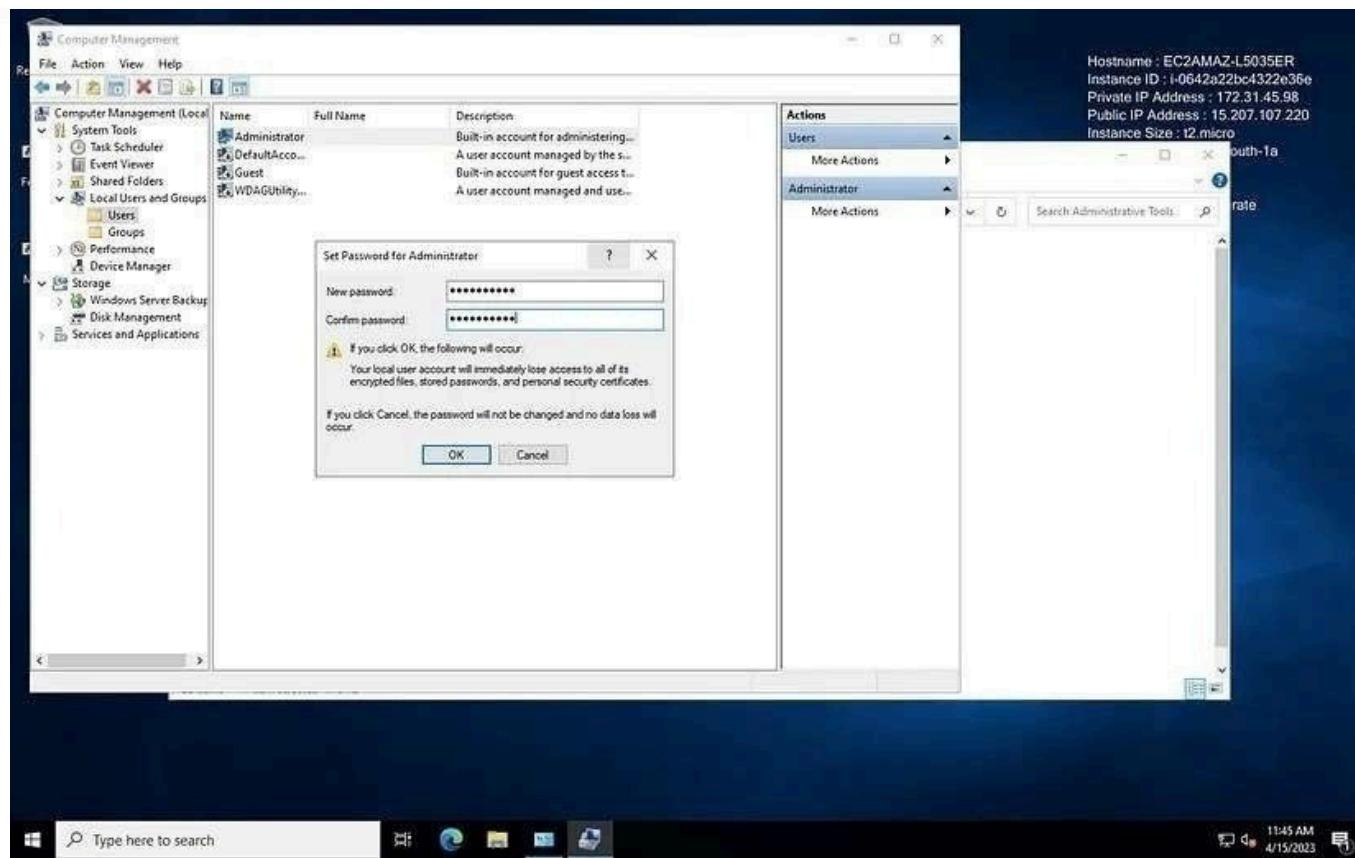
Then right-click on the “Administrator” and set your password



Click on the “Proceed”



After setting a new password just click on “ok”



Congratulations, you have successfully created your own Windows EC2 instance in AWS! By following these step-by-step instructions, you can now leverage the power of the cloud to run your Windows-based applications and workloads with ease. Happy computing!

[Ec2 Instance](#)

[Ec2 Instance Connect](#)

[Windows](#)

[Launch Ec2 Instance](#)

Written by Sanoj



85 Followers · 50 Following

AWS/DevOps Engineer

Follow

Create an elastic IP Address on AWS

The screenshot shows the AWS EC2 Instances page. On the left, there's a sidebar with various navigation options like EC2 Dashboard, Events, Tags, Limits, and Instances. Under Instances, 'Instances' is selected. The main area displays a table of instances:

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Available
flask-dev	i-065ee05912856710b	Stopped	t2.micro	-	No alarms	+ us-east
flask-staging	i-0fd80e5c945669987	Stopped	t2.micro	-	No alarms	+ us-east
flask-prod	i-07a1d67fc99f6bf37	Stopped	t2.micro	-	No alarms	+ us-east
EC2	i-049a2956e7b38612a	Running	t2.micro	2/2 checks passed	No alarms	+ us-east

Below the table, a modal window titled "Instance: i-049a2956e7b38612a (EC2)" is open. The "Details" tab is selected in the top navigation bar of the modal. The "Instance summary" section contains the following information:

Instance ID	Public IPv4 address	Private IPv4 addresses
i-049a2956e7b38612a (EC2)	100.26.137.231 open address	172.31.16.211
IPv6 address	-	Public IPv4 DNS
		ec2-100-26-137-231.compute-1.amazonaws.com open address
Instance state	Running	

Select the Details tab:

This screenshot is identical to the one above it, showing the AWS EC2 Instances page with the 'EC2' instance selected. The "Details" tab is now selected in the instance details panel, as indicated by the red box around it. The "Instance summary" section remains the same.

Then Under the Instance summary, scroll down to the Elastic IP addresses section; it should be empty:

The screenshot shows the AWS EC2 Instances page. On the left, there's a navigation panel with 'Instances' selected. The main area displays a table of instances. One instance, 'EC2' (i-049a2956e7b38612a), is highlighted with a checkmark. The instance details panel below it shows various attributes: Instance ID (i-049a2956e7b38612a), Instance state (Running), Instance type (t2.micro), and Public IPv4 DNS (ec2-100-26-137-231.compute-1.amazonaws.com). A red box highlights the 'Elastic IP addresses' section, which currently shows a value of '-'.

In the same tab in the navigation panel to the left:

This screenshot shows the same AWS EC2 Instances page as above, but with the navigation panel expanded. The 'Instances' section is highlighted with a red box. The main content area shows the same instance details for 'EC2' (i-049a2956e7b38612a), including its state, type, and public DNS name. The 'Elastic IP addresses' section still shows a value of '-'.

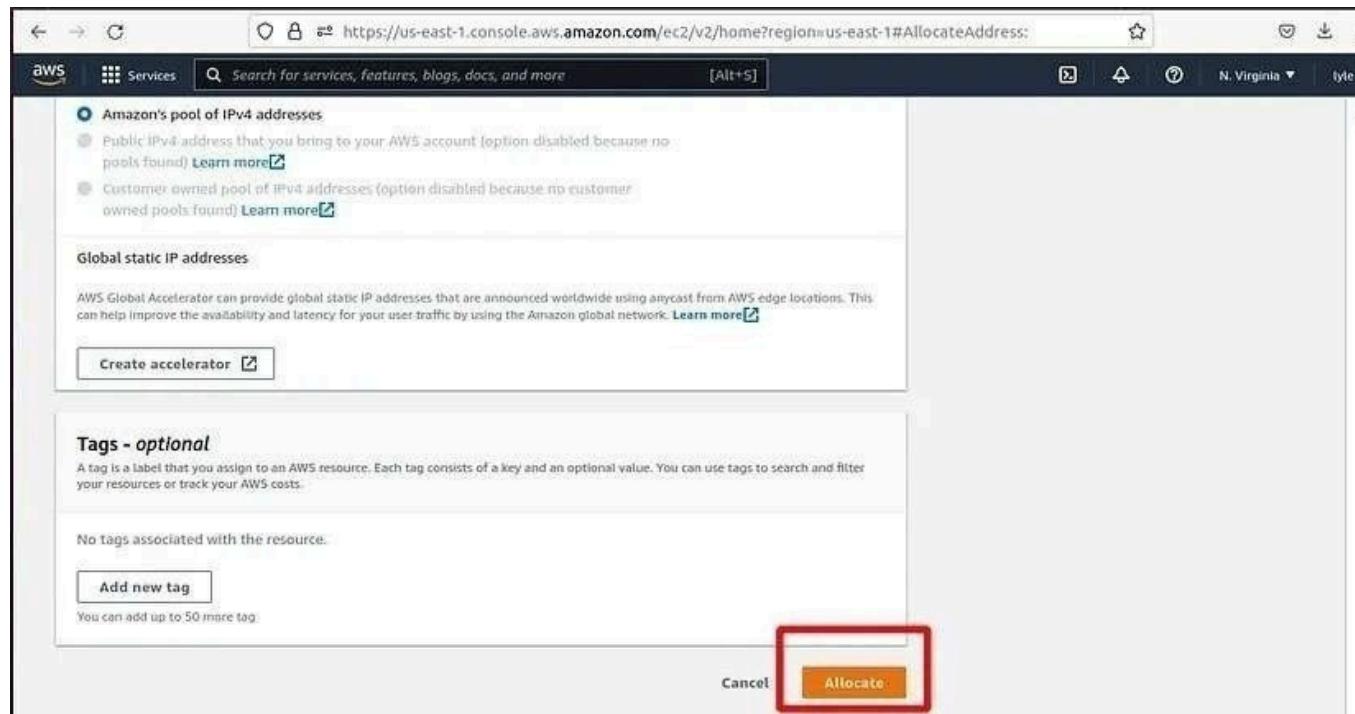
Scroll down to the Network and Security section; within the drop-down, select Elastic IPs:

The screenshot shows the AWS EC2 Instances page. On the left sidebar, under the Network & Security section, the 'Elastic IPs' link is highlighted with a red box. The main table lists four instances: 'flask-dev', 'flask-staging', 'flask-prod', and 'EC2'. The 'EC2' instance is currently selected, indicated by a checked checkbox in the first column. The details pane for the selected instance shows its public IPv4 address (100.26.137.231), instance state (Running), private IP DNS name (ip-172-31-16-211.ec2.internal), and instance type (t2.micro). The public IPv4 DNS is listed as ec2-100-26-137-231.compute-1.amazonaws.com.

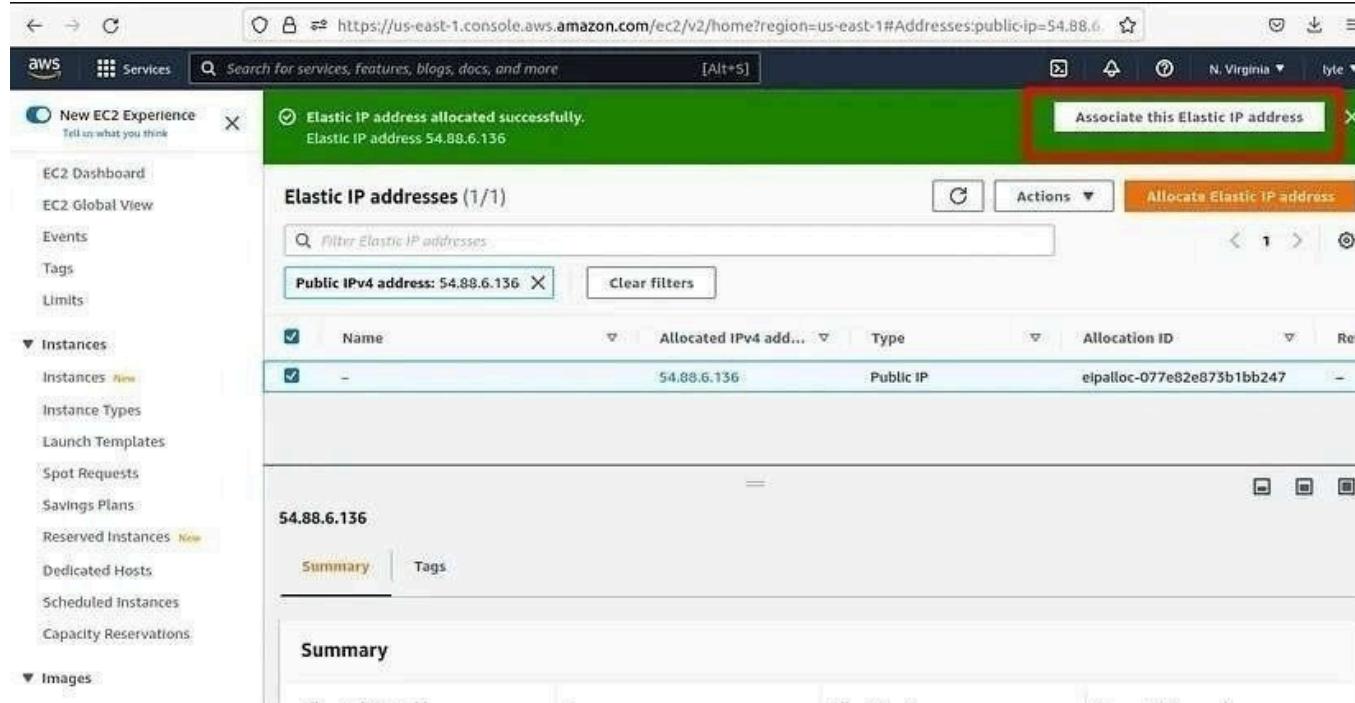
Click on the Allocate Elastic IP address button:

The screenshot shows the AWS Elastic IP addresses page. Under the Network & Security section, the 'Elastic IPs' link is highlighted with a red box. The main table shows one allocated IP address: 3.212.197.205, which is a Public IP with an allocation ID of elpalloc-062d4cf1a79e95f6c. A red box highlights the 'Allocate Elastic IP address' button in the top right corner of the table header. Below the table, a detailed view of the IP address 3.212.197.205 is shown, including tabs for Summary and Tags, and a summary table with columns for Allocated IPv4 address, Type, Allocation ID, and Reverse DNS record.

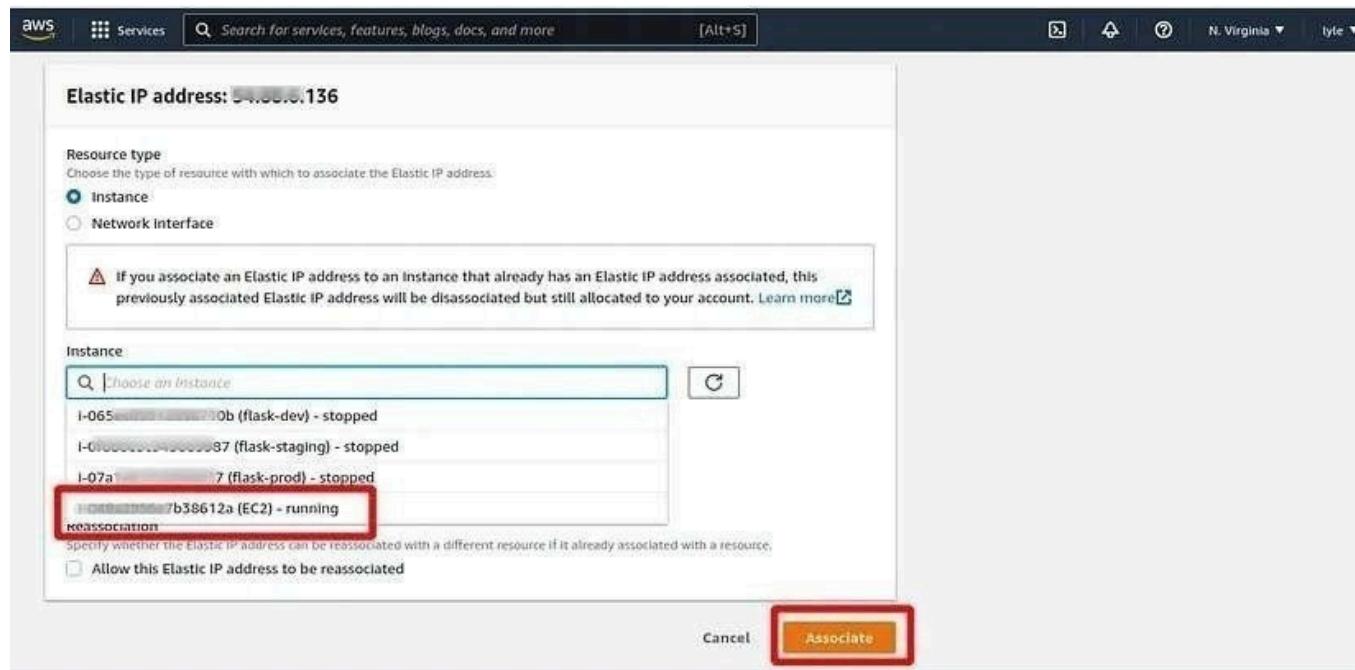
Leave the defaults and click on Allocate:



Then select the Associate this Elastic IP address prompt:



Select the instance to associate it with in the Instance drop-down, then in the Private IP address drop-down, select the instance's private IP address. then click the Associate button:



And with that, we have successfully allocated an Elastic IP address to our EC2 server:

Create EBS volume and attach(mount) to Ec2

Back to the topic, Click on “Create Volume” as you can see in the upper right corner.

2. I selected the Volume type as gp2 and gave 4 GB size. And the same region “ap-south-1a” as our instance. Then click on “Create Volume” on the bottom.

Create volume Info

Create an Amazon EBS volume to attach to any EC2 instance in the same Availability Zone.

Volume settings

Volume type Info
General Purpose SSD (gp2)

Size (GiB) Info
4
Min: 1 GiB, Max: 16384 GiB. The value must be an integer.

IOPS Info
100 / 3000
Baseline of 3 IOPS per GiB with a minimum of 100 IOPS, burstable to 3000 IOPS.

Throughput (MiB/s) Info
Not applicable

Availability Zone Info
ap-south-1a

Snapshot ID - optional Info
Don't create volume from a snapshot

Encryption Info
Use Amazon EBS encryption as an encryption solution for your EBS resources associated with your EC2 instances.
 Encrypt this volume

Tags - optional Info
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 50 more tags.

Snapshot summary Info

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

3. Just gave the name “my-ebs-volume” to our newly created EBS Volume for simplicity and understanding.

The screenshot shows the AWS EC2 Dashboard with the 'Volumes' section selected. A success message at the top says 'Successfully created volume vol-0d2b547e8d6dad5d0.' Below it, a table lists two volumes. The second volume, 'my-ebs-volume', has its 'Name' field populated with the value 'my-ebs-volume'. The 'Actions' button is highlighted in orange.

Name	Volume ID	Type	Size	IOPS	Throughput	Snapshot ID	Created
-	vol-0c21cb481513f8975	gp3	9 GiB	3000	125	snap-02f0663...	2024/08/13 06:40 GMT+5:...
<input checked="" type="checkbox"/> my-ebs-volume	vol-0d2b547e8d6dad5d0	gp2	4 GiB	100	-	-	2024/08/13 07:21 GMT+5:...

Clicked on the blank space of name and given the name

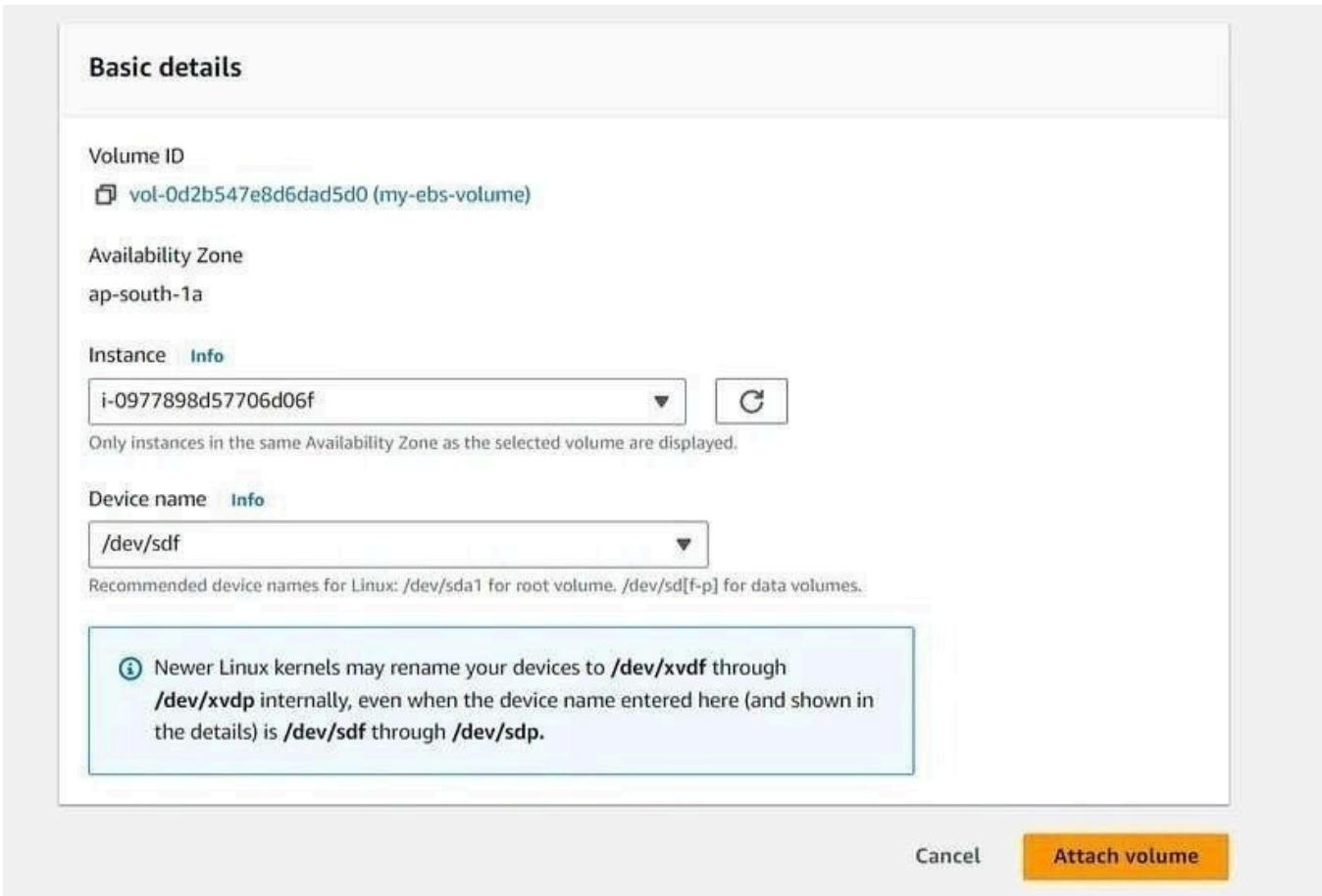
4. Select “my-ebs-volume” checkbox then Click on “Actions” then click on “Attach volume” to attach it to our ec2 instance.

The screenshot shows the same EC2 Volumes page. The 'Actions' menu is open over the 'my-ebs-volume' row. The 'Attach volume' option is highlighted in blue.

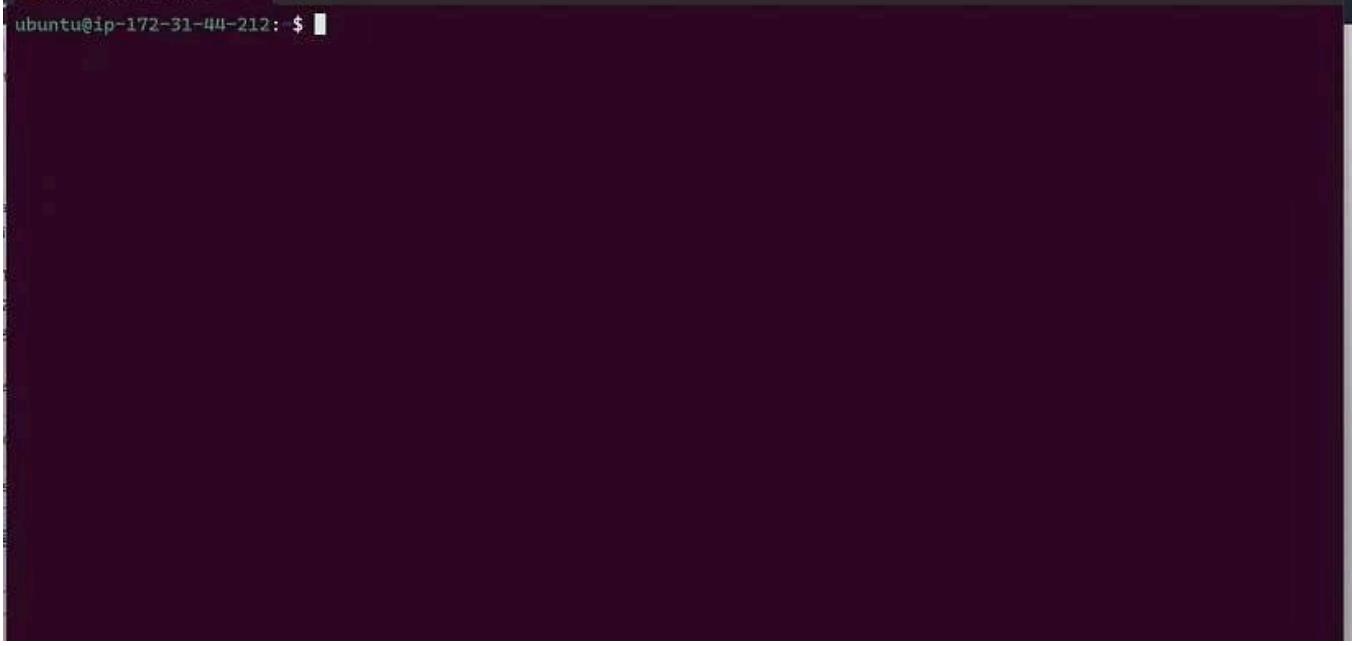
- Modify volume
- Create snapshot
- Create snapshot lifecycle policy
- Delete volume
- Attach volume**
- Detach volume
- Force detach volume
- Manage auto-enabled I/O
- Manage tags
- Fault injection

5. Select the instance (in the same availability zone) for which you want to attach this Volume. I have selected the same instance “shivam-ebs-tutorial” as I launched above.

You can select any device type, it won't matter. Then click on “Attach Volume” button.



6. Now, volume “my-ebs-volume” is attached to the instance “shivam-ebs-tutorial”. We have reached till image 2 of our visualization tutorial.
SSH to my EC2 machine to download code on “my-ebs-volume” to reach image 3.



A screenshot of a terminal window on an Ubuntu system. The title bar shows the session name 'ubuntu@ip-172-31-44-212: ~' and a small icon. The main area of the terminal is completely black, indicating no output or a blank screen.

```
ubuntu@ip-172-31-44-212: ~
```

7. Everything we will do on this EC2 instance, we have to do in the terminal because there is no GUI available here.

We have to check, what block devices (hard disk, EBS Volumes) etc attached to this machine. The below command is for this:

```
lsblk
```

```
ubuntu@ip-172-31-44-212: $ lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
loop0    7:0    0 25.2M  1 loop /snap/amazon-ssm-agent/7993
loop1    7:1    0 55.7M  1 loop /snap/core18/2829
loop2    7:2    0 38.8M  1 loop /snap/snapd/21759
xvda   202:0    0   9G  0 disk
└─xvda1 202:1    0   8G  0 part /
  ├─xvda14 202:14   0   4M  0 part
  ├─xvda15 202:15   0 106M 0 part /boot/efi
  └─xvda16 259:0    0 913M 0 part /boot
xvdf   202:80   0   4G  0 disk
ubuntu@ip-172-31-44-212: $
```

You can see, there are two volumes: one is “xvda” of 9 GB (this is the default root volume that we gave during the launch instance) and the second is “xvdf” of 4 GB (this is “my-ebs-volume” we created. Here we will download our code).

If it is your first time and you don’t know all the below steps that I am doing with Linux commands then just cram it here. If you know Linux then these are very common for you.

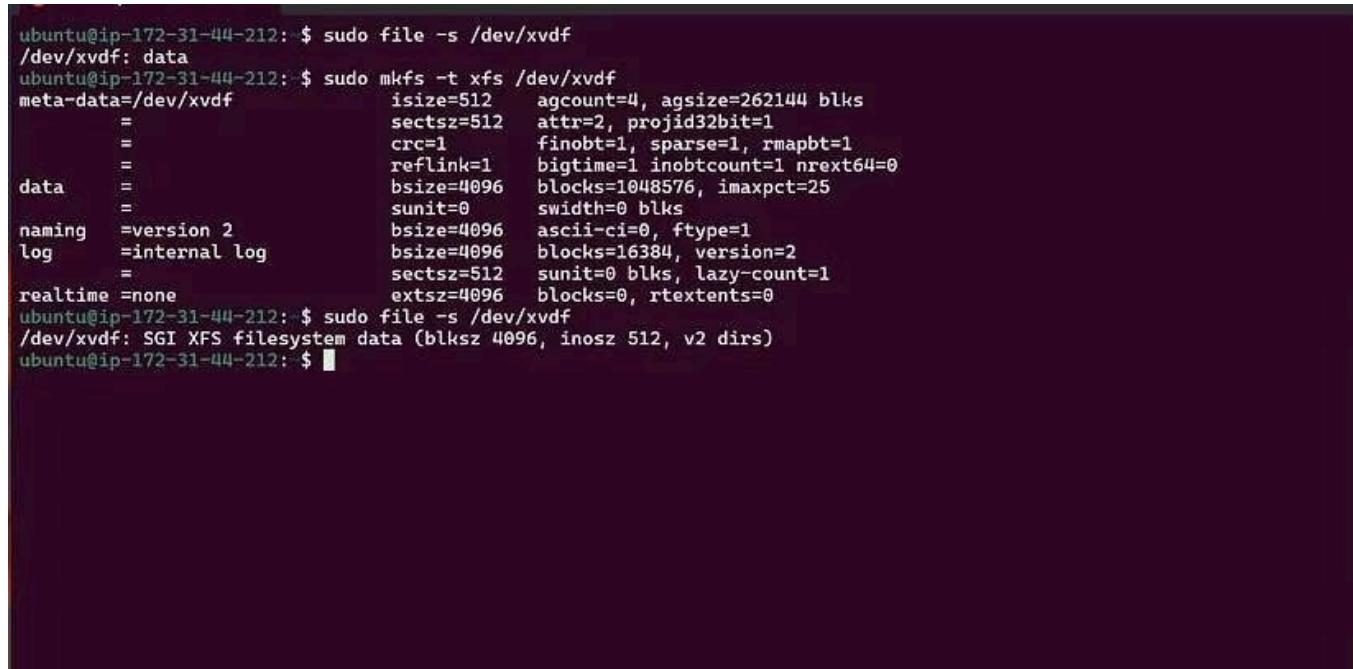
- First, we have to enable the File System for newly created xvdf storage. If you are attaching any existing EBS volume then you don’t need to do this. But, since we created this EBS Volume fresh and haven’t enabled the file system till now, we have to do it. To check file system is enabled or not, type the below command

```
sudo file -s /dev/xvdf
```

If the response comes as “/dev/xvdf: data”, then it is not enabled.

- Enable File System, type the below command

```
sudo mkfs -t xfs /dev/xvdf
```



A terminal window showing the configuration and creation of an XFS file system. The session starts with a check of the device status using `sudo file -s /dev/xvdf`, which returns "data". Then, the command `sudo mkfs -t xfs /dev/xvdf` is run, followed by a detailed output of the XFS file system parameters. The parameters listed include: meta-data=/dev/xvdf, isize=512, agcount=4, agsize=262144 blks, sectsz=512, attr=2, projid32bit=1, crc=1, finobt=1, sparse=1, rmapbt=1, reflink=1, bigtime=1, inobtcount=1, nrext64=0, data, bsize=4096, blocks=1048576, imaxpct=25, sunit=0, swidth=0 blks, naming, version 2, log, internal log, bsize=4096, blocks=16384, version=2, sectsz=512, sunit=0 blks, lazy-count=1, realtime, none, extsz=4096, blocks=0, rtextents=0. The session concludes with another `sudo file -s /dev/xvdf` command, which now correctly identifies the device as "SGI XFS filesystem data (blksz 4096, inosz 512, v2 dirs)".

```
ubuntu@ip-172-31-44-212: $ sudo file -s /dev/xvdf
/dev/xvdf: data
ubuntu@ip-172-31-44-212: $ sudo mkfs -t xfs /dev/xvdf
meta-data=/dev/xvdf          isize=512    agcount=4, agsize=262144 blks
                           =         sectsz=512  attr=2, projid32bit=1
                           =         crc=1    finobt=1, sparse=1, rmapbt=1
data                      =         reflink=1  bigtime=1 inobtcount=1 nrext64=0
                           =         bsize=4096   blocks=1048576, imaxpct=25
                           =         sunit=0    swidth=0 blks
naming        =version 2   bsize=4096   ascii-ci=0, ftype=1
log           =internal log  bsize=4096   blocks=16384, version=2
                           =         sectsz=512  sunit=0 blks, lazy-count=1
realtime      =none        extsz=4096   blocks=0, rtextents=0
ubuntu@ip-172-31-44-212: $ sudo file -s /dev/xvdf
/dev/xvdf: SGI XFS filesystem data (blksz 4096, inosz 512, v2 dirs)
ubuntu@ip-172-31-44-212: $
```

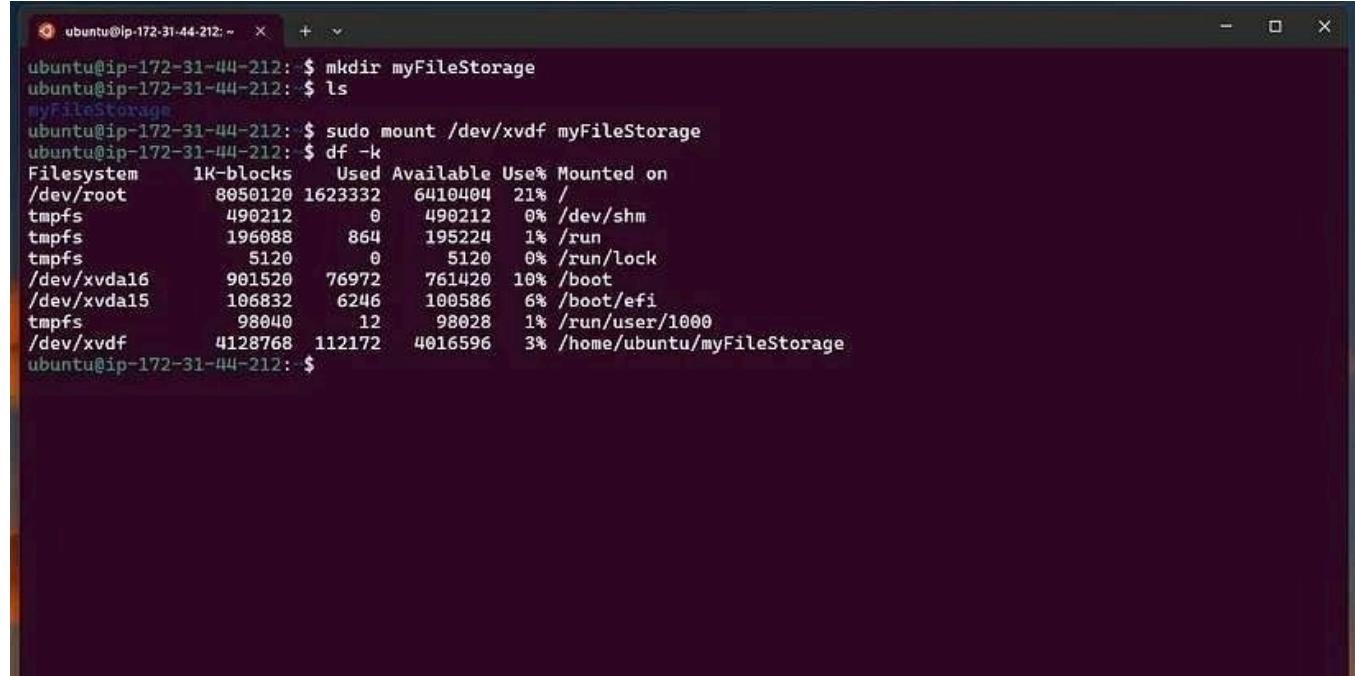
- Make a folder and mount that file system into this folder. Now all the things that you download or make in this folder will be created in the file system of EBS Volume.

Make a folder with the name “myFileStorage” from the below command:

```
mkdir myFileStorage
```

Mount the file system of “xvdf” into this folder from below command:

```
sudo mount /dev/xvdf myFileStorage
```



The screenshot shows a terminal window with a dark background and light-colored text. The user is performing the following steps:

- Creating a directory named "myFileStorage": `mkdir myFileStorage`
- Listing the contents of the current directory: `ls`
- Moving to the "myFileStorage" directory: `cd myFileStorage`
- Mounting the EBS volume at this location: `sudo mount /dev/xvdf myFileStorage`
- Checking the disk usage with the `df -h` command to verify the mount point.

The output of the `df -h` command shows the following disk usage:

Filesystem	1K-blocks	Used	Available	Use%	Mounted on
/dev/root	8050120	1623332	6410404	21%	/
tmpfs	490212	0	490212	0%	/dev/shm
tmpfs	196088	864	195224	1%	/run
tmpfs	5120	0	5120	0%	/run/lock
/dev/xvda16	901520	76972	761420	10%	/boot
/dev/xvda15	106832	6246	100586	6%	/boot/efi
tmpfs	98040	12	98028	1%	/run/user/1000
/dev/xvdf	4128768	112172	4016596	3%	/home/ubuntu/myFileStorage

Now, our EBS volume is mounted to folder “myFileStorage”. Whatever we make inside this folder will be kept inside our EBS Volume.

8. Terminate the instance “shivam-ebs-tutorial”.

The screenshot shows the AWS EC2 Instances page. On the left, there's a sidebar with various navigation options like EC2 Dashboard, Events, Instances, Instance Types, Launch Templates, etc. The main area displays a table of instances. One instance, named "shivam-ebs-tutorial" with the ID "i-0977898d57706d06f", is selected. In the top right corner of the instance row, there's a dropdown menu with options: Stop instance, Start instance, Reboot instance, and a long menu item "Terminate instance". The "Terminate instance" option is highlighted with a blue border. Below the table, a detailed view of the selected instance is shown, including its summary, network information (Public IPv4 address: 13.201.115.192, Private IP4 address: 172.31.44.212), and security details.

Completed till image 4 of the visualization tutorial.

[Open in app](#)

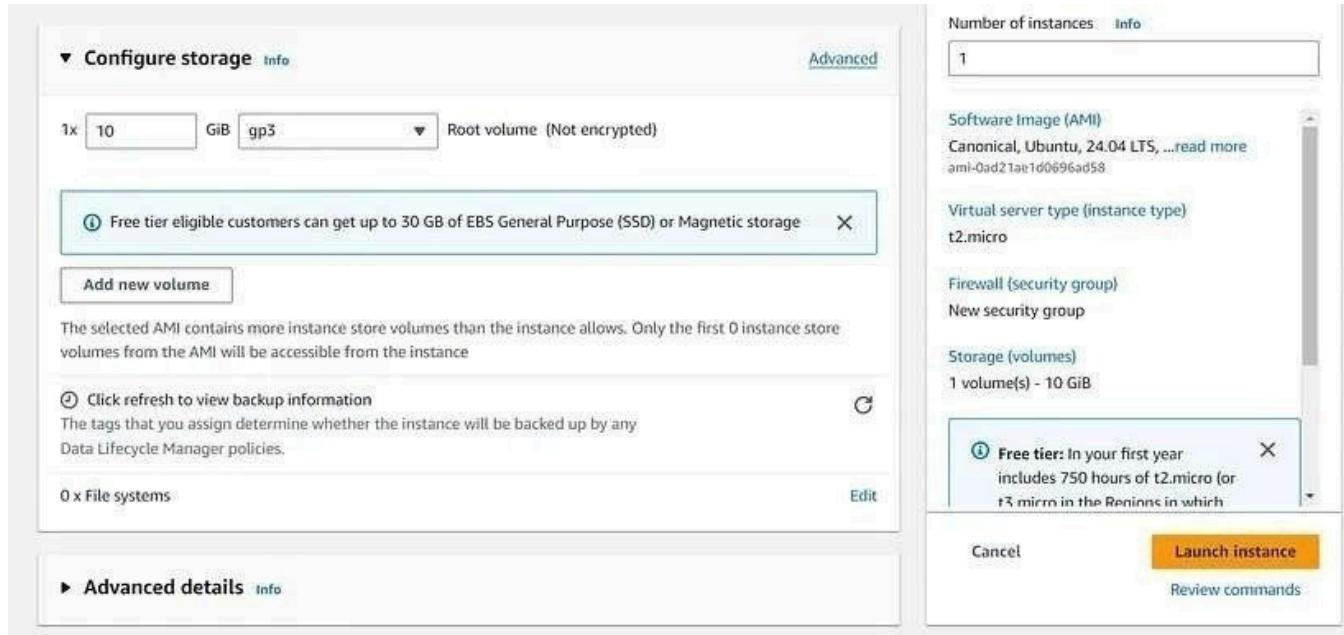
[Sign up](#) [Sign in](#)

Search

Write



9. Launch a new EC2 Instance with name “2-shivam-ec2-tutorial” with default root EBS Volume 10 GB.



While launching EC2 Instance, go to the network setting and select a subnet of “ap-south-1a”. It will launch our instance in ap-south-1a. We are doing it because our EBS Volume is in ap-south-1a. Don’t worry, if you don’t know about the subnet. We will study it in detail in upcoming blogs just like we are studying EBS Volume now.

The screenshot shows the AWS EC2 Launch Instance wizard. On the left, under 'Network settings', there's a VPC dropdown set to 'vpc-0e28c412ef07e0e34 (default)', a Subnet dropdown set to 'subnet-02a12bd6f2dbe8f88', and an 'Auto-assign public IP' dropdown set to 'Enable'. Below these are 'Firewall (security groups)' options with 'Create security group' selected. On the right, the 'Summary' section shows 'Number of instances: 1', 'Software Image (AMI): Canonical, Ubuntu, 24.04 LTS', 'Virtual server type (instance type): t2.micro', 'Firewall (security group): New security group', and 'Storage (volumes): 1 volume(s) - 8 GiB'. A tooltip for the 'Free tier' is visible, stating 'Free tier: In your first year includes 750 hours of t2.micro (or 15 mics in the Regions in which you launch the instance)'. At the bottom are 'Cancel', 'Launch instance' (highlighted in orange), and 'Review commands'.

Click on “Launch Instance” and our instance named “2-shivam-ebs-tutorial” launched in ap-south-1a.

The screenshot shows the AWS EC2 Instances page. The sidebar has 'Instances' selected. The main table shows two instances: one terminated and one running. The running instance is selected. The details pane below shows the instance ID 'i-0cb6559c3626a2eec', name '2-shivam-ebs-tutorial', state 'Running', and public IP '13.200.252.70'. It also lists private IP '172.31.38.188', public DNS 'ec2-13-200-252-70.ap-south-1.compute.amazonaws.com', and private IP DNS 'ip-172-31-38-188.ap-south-1.compute.internal'.

10. Now, go to Volumes and select the same EBS Volume “my-ebs-volume” to attach it to our new EC2 instance.

Volumes (1/2) info

Name	Volume ID	Type	Size	IOPS	Throughput	Snapshot
vol-08013d57adb2f4281	gp3	10 GiB	3000	125	-	snap-02f0
my-ebs-volume	vol-0d2b547e8d6dad5d0	gp2	4 GiB	100	-	-

Actions ▾ Create volume

- Modify volume
- Create snapshot
- Create snapshot lifecycle policy
- Delete volume
- Attach volume
- Detach volume
- Force detach volume
- Manage auto-enabled I/O
- Manage tags
- Fault injection

Volume ID: vol-0d2b547e8d6dad5d0 (my-ebs-volume)

Details Status checks Monitoring Tags

Volume ID vol-0d2b547e8d6dad5d0 (my-ebs-volume)	Size 4 GiB	Type gp2	Volume status Okay
AWS Compute Optimizer finding Opt-in to AWS Compute Optimizer for recommendations. Learn more	Volume state Available	IOPS 100	Throughput -

Select the newly created EC2 Instance and any device type.

Basic details

Volume ID
vol-0d2b547e8d6dad5d0 (my-ebs-volume)

Availability Zone
ap-south-1a

Instance Info
i-0cb6559c3626a2eec

Only instances in the same Availability Zone as the selected volume are displayed.

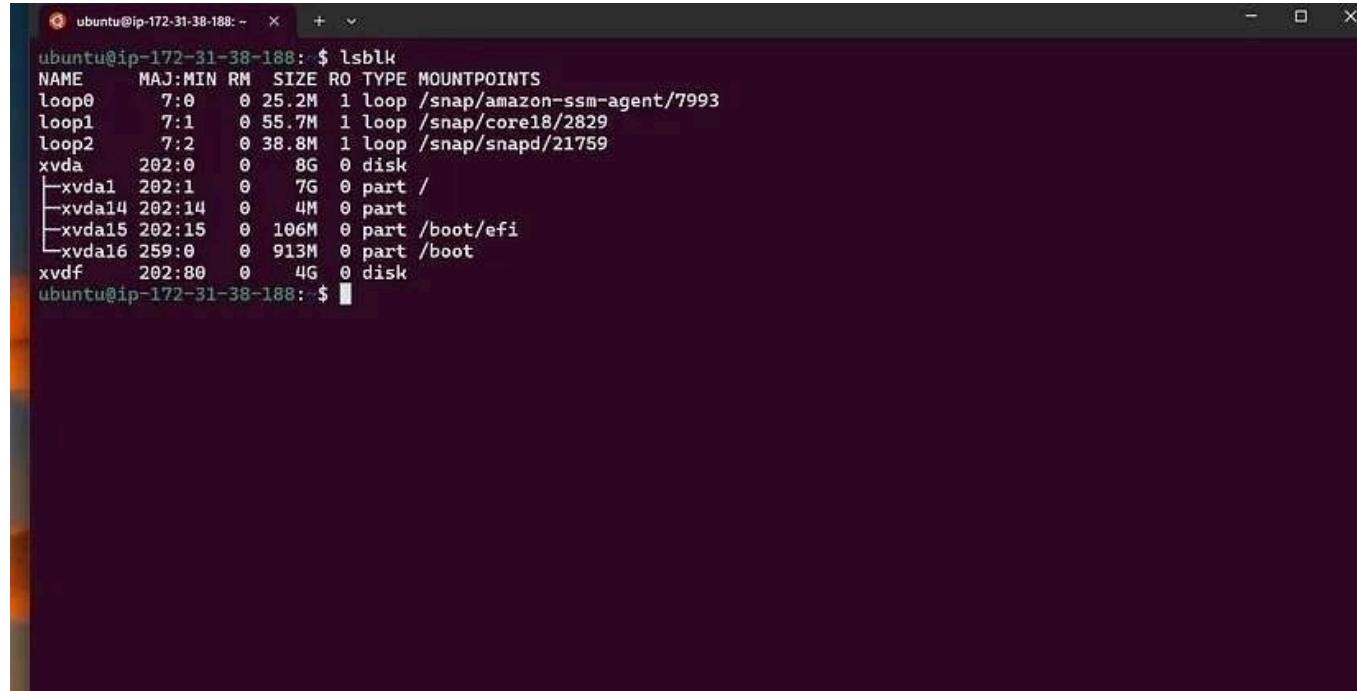
Device name Info
/dev/sdf

Recommended device names for Linux: /dev/sda1 for root volume. /dev/sd[f-p] for data volumes.

Note: Newer Linux kernels may rename your devices to /dev/xvdf through /dev/xvdः internally, even when the device name entered here (and shown in the details) is /dev/sdf through /dev/sdः.

Cancel Attach volume

11. Do SSH in the new EC2 instance “2-shivam-ebs-tutorial” and run `lsblk` to check if the volume is correctly attached or not.



```
ubuntu@ip-172-31-38-188: ~ + - X
ubuntu@ip-172-31-38-188: ~ $ lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
loop0    7:0    0 25.2M  1 loop /snap/amazon-ssm-agent/7993
loop1    7:1    0 55.7M  1 loop /snap/core18/2829
loop2    7:2    0 38.8M  1 loop /snap/snapd/21759
xvda   202:0    0   8G  0 disk
└─xvda1  202:1    0   7G  0 part /
  ├─xvda14 202:14  0   4M  0 part
  ├─xvda15 202:15  0 106M 0 part /boot/efi
  └─xvda16 202:16  0 913M 0 part /boot
xvdf   202:80   0   4G  0 disk
ubuntu@ip-172-31-38-188: ~ $
```

Since we already created the file system of this EBS Volume so we don't need to do it now. Just make any folder in this EC2 instance and attach this file system to that folder. Then check if the code that we installed previously persists or not.

The screenshot shows a terminal window with the following command history:

```
ubuntu@ip-172-31-38-188: ~ / + - x
ubuntu@ip-172-31-38-188: $ sudo file -s /dev/xvdf
/dev/xvdf: SGI XFS filesystem data (blksz 4096, inosz 512, v2 dirs)
ubuntu@ip-172-31-38-188: $ mkdir mySecondInstanceFileStorage
ubuntu@ip-172-31-38-188: $ ls
mySecondInstanceFileStorage
ubuntu@ip-172-31-38-188: $ sudo mount /dev/xvdf mySecondInstanceFileStorage
ubuntu@ip-172-31-38-188: $ df -k
Filesystem      1K-blocks    Used Available Use% Mounted on
/dev/root        7034376  1607624   5410368  23% /
tmpfs            490212       0    490212   0% /dev/shm
tmpfs            196088     872    195216   1% /run
tmpfs             5120       0     5120   0% /run/lock
/dev/xvda16      901520    76972   761420  10% /boot
/dev/xvda15      106832    6246   100586   6% /boot/efi
tmpfs            98040       12    98028   1% /run/user/1000
/dev/xvdf        4128768  112924   4015844   3% /home/ubuntu/mySecondInstanceFileStorage
ubuntu@ip-172-31-38-188: $ cd mySecondInstanceFileStorage/
ubuntu@ip-172-31-38-188: ~/mySecondInstanceFileStorage $ ls
SmartSkill-Studio-Frontend
ubuntu@ip-172-31-38-188: ~/mySecondInstanceFileStorage $
```

df -k command is to check the mount folder.

You can see in the above image that when we do “ls”, we get the same data that we downloaded previously. This shows data persists.

And finally, we complete image 5 of the Visualization Tutorial.

This was a little boring but if you read carefully till now, then I hope you understood everything.

Changing the size of existing EBS volume without downtime

1. Select the EBS Volume by clicking the checkbox
2. Click to “Action” button on the top right corner
3. Click on resize volume then give the new volume size.

Note: You can only increase the size, which means if you have initially given 4 GB then you can only give a size which is greater than 4GB.

How to Use a Snapshot to Restore an AWS EC2 Instance



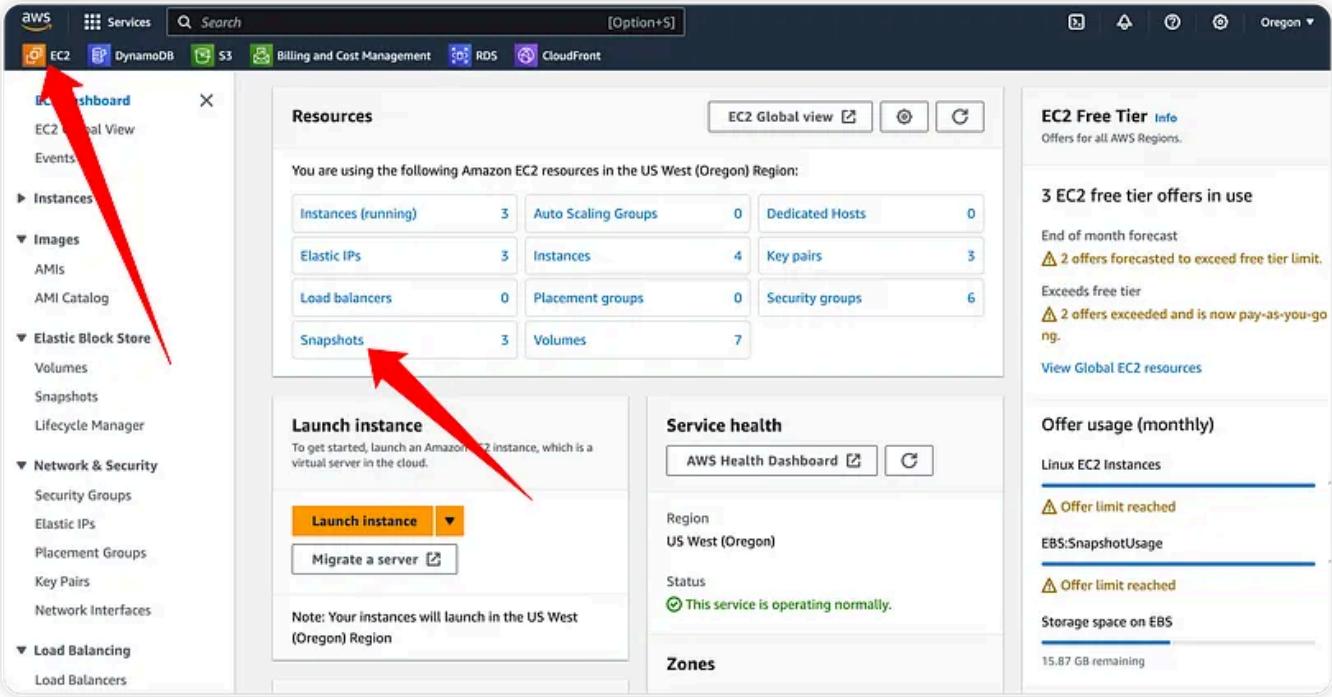
Step 1: Create a Snapshot

If you don't already have a snapshot, you'll need to create one from your existing EBS volume.

Navigate to the EC2 Dashboard:

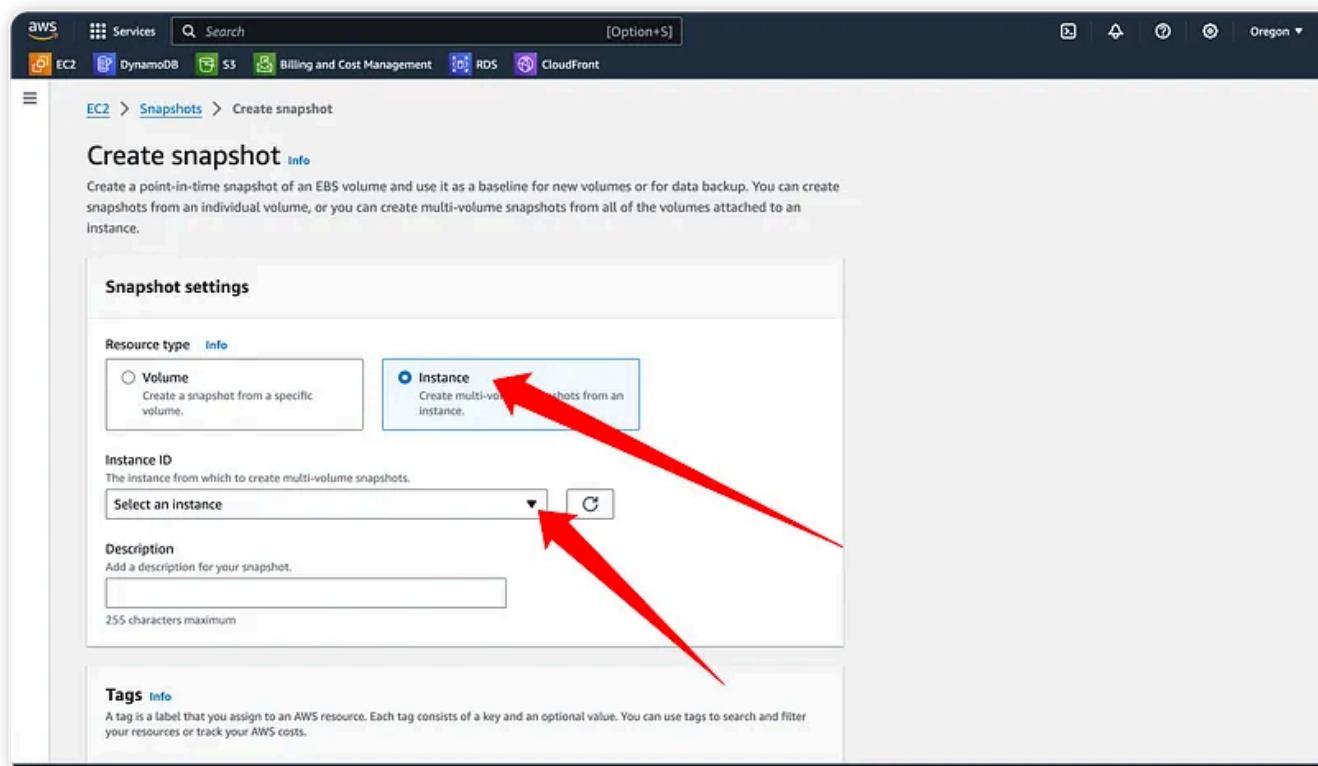
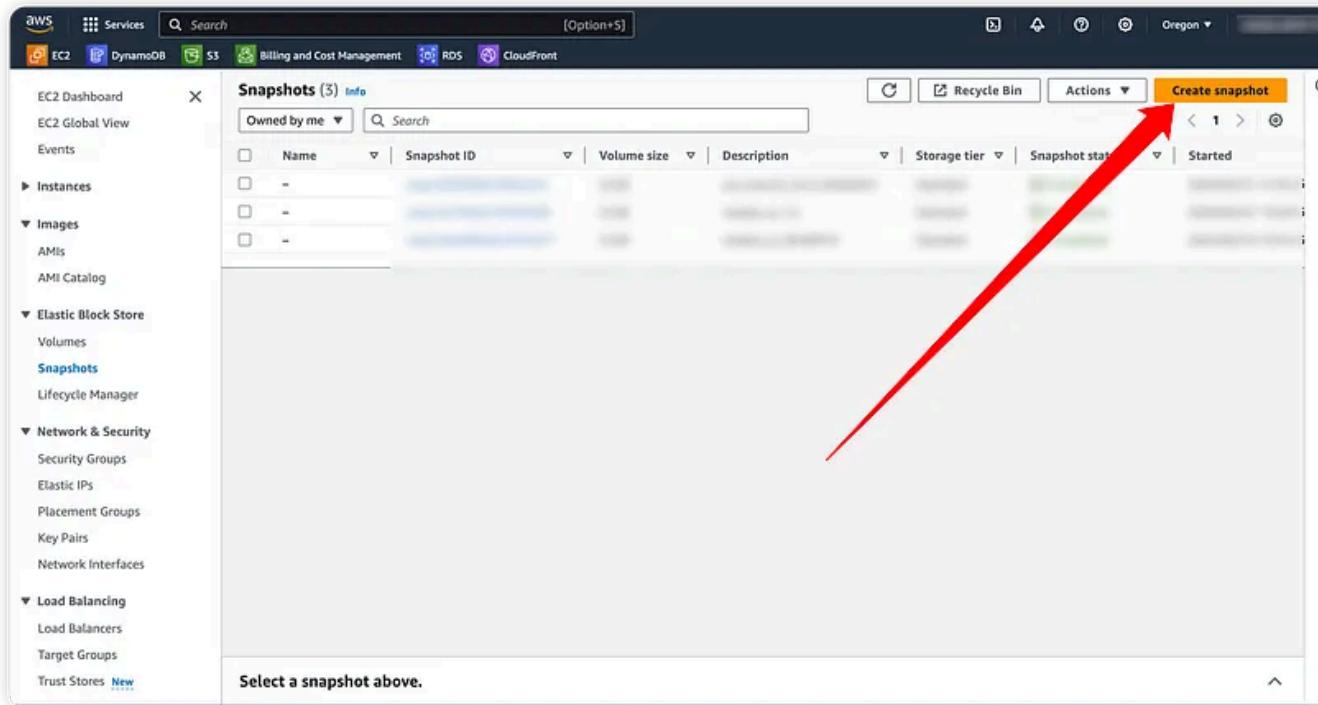
Go to the AWS Management Console.

Select EC2 from the Services menu.



Create a Snapshot:

- In the left-hand navigation pane, click on Snapshots under the Elastic Block Store section.
- Click on the Create Snapshot button.
- Select the volume you want to create a snapshot of and provide a description.
- Click Create Snapshot.



Step 2: Create a Volume from the Snapshot

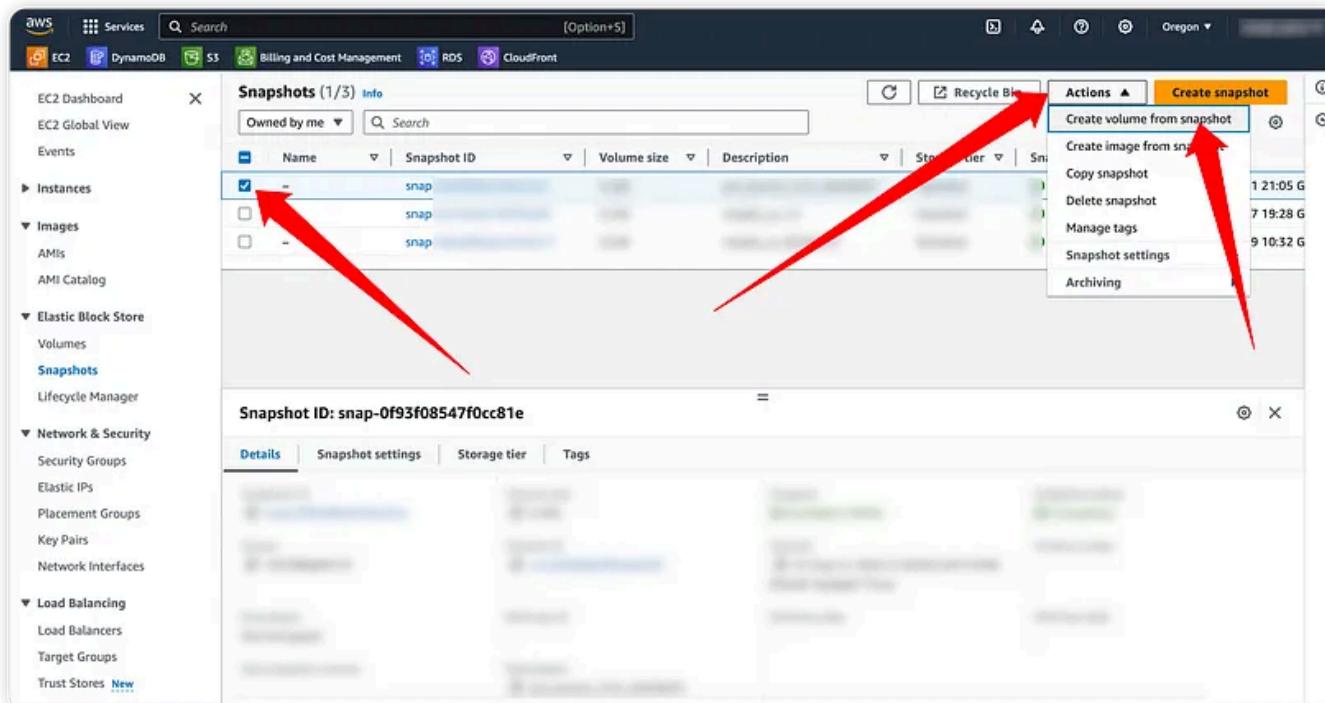
Once you have the snapshot, the next step is to create a new EBS volume from the snapshot.

Navigate to Snapshots:

- In the EC2 Dashboard, select Snapshots .

Create Volume:

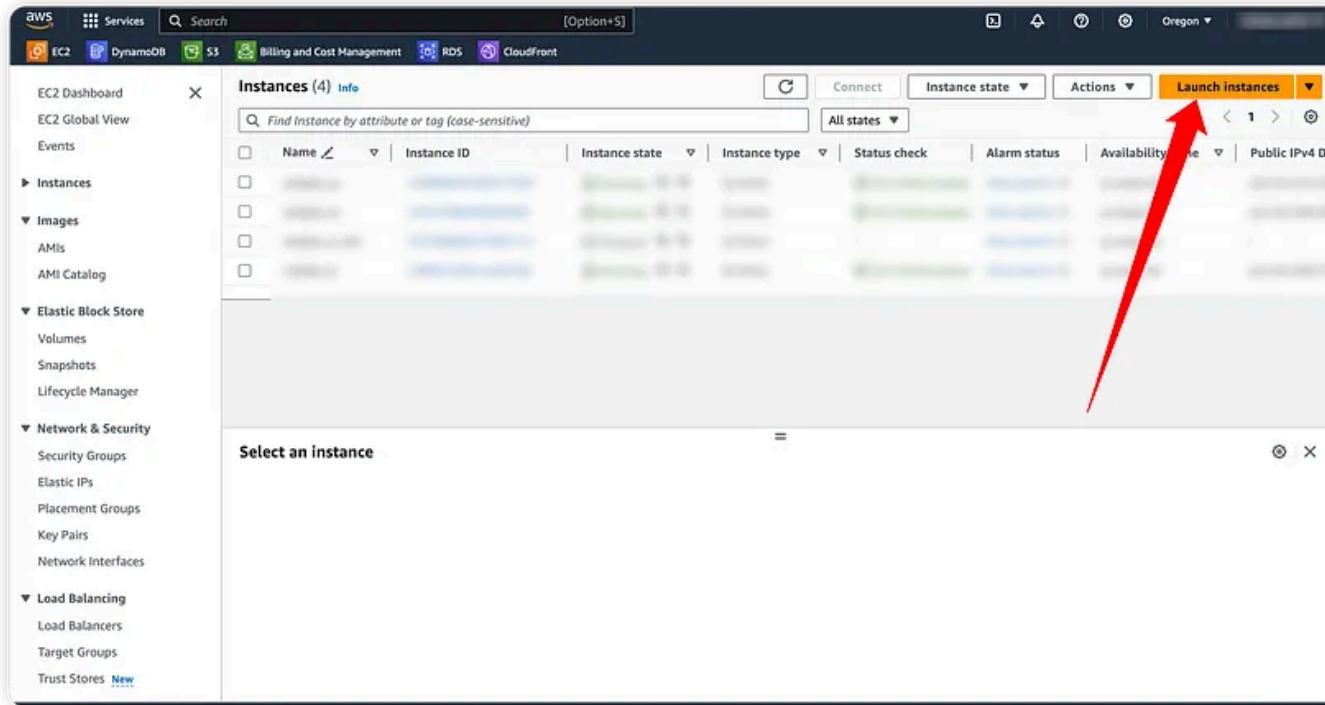
- Select the snapshot you created.
- Click Actions and choose Create Volume.
- In the Create Volume dialog:
 - Ensure the Availability Zone matches where you want to launch the new instance.
 - Click Create Volume.



Step 3: Launch a New EC2 Instance

Launch an Instance:

- Go to the Instances section in the EC2 Dashboard.
- Click Launch Instance .



Select an AMI:

- Choose an Amazon Machine Image (AMI) that matches your application's requirements.

Choose an Instance Type:

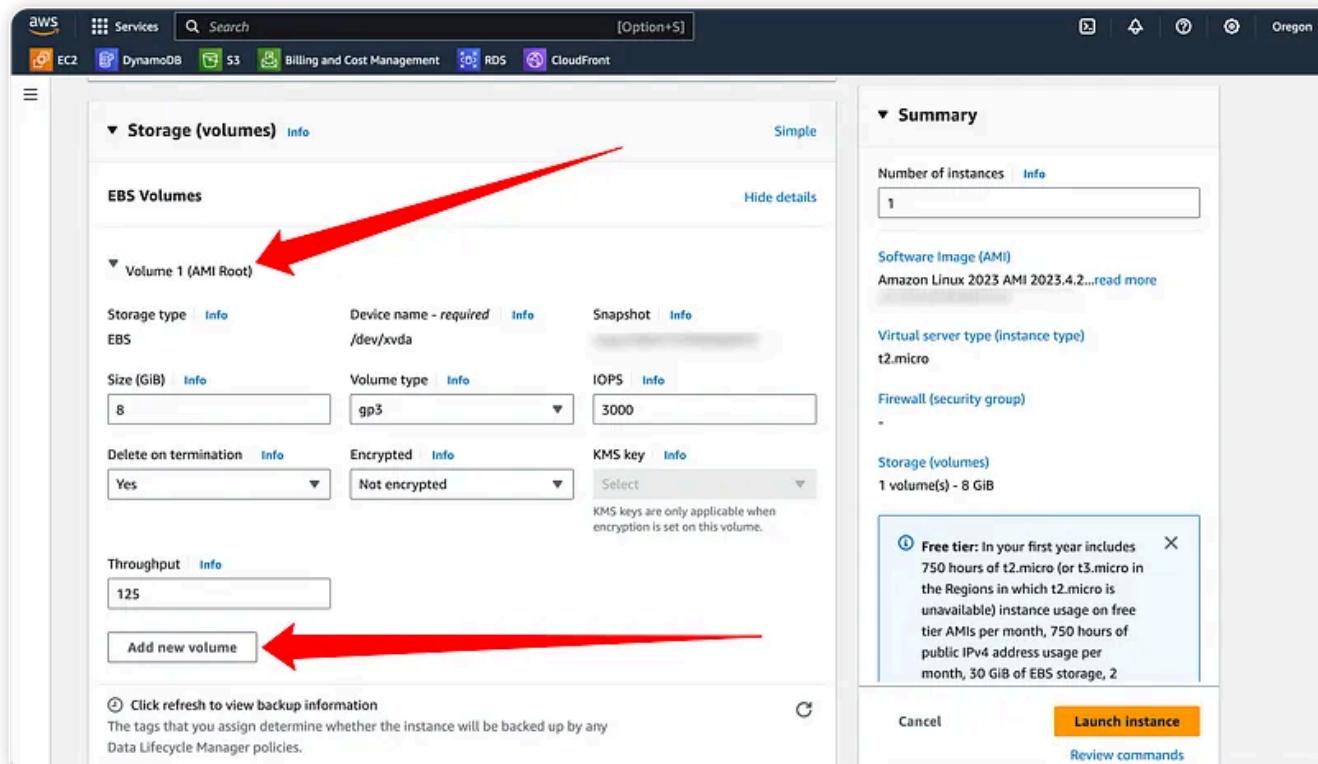
- Select the instance type that best suits your needs.

Configure Instance Details:

- Ensure the instance is in the same Availability Zone as the volume created from the snapshot.
- Complete the configuration and click Next: Add Storage.

Add Storage:

- Remove the default root volume (if possible. not possible in my case).



can't delete the root volume, we will handle it later

Configure Security Group:

- Select the existing security group

Network settings

No preference (Default subnet in any availability zone)

Auto-assign public IP

Enable

Additional charges apply when outside of free tier allowance

Firewall (security groups)

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

Select security groups

Compare security group rules

Advanced

Number of instances: 1

Software Image (AMI): Amazon Linux 2023 AMI 2023.4.2...read more

Virtual server type (instance type): t2.micro

Firewall (security group):

Storage (volumes): 1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2

Cancel Launch instance Review commands

Key pair

- Select the old key pair

Key pair (login)

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

Select

Create new key pair

Proceed without a key pair (Not recommended)

Default value

key_pair_1

Type: rsa

key_pair_2

Type: rsa

key_pair_3

Type: rsa

No preference (Default subnet in any availability zone)

Auto-assign public IP

Enable

Additional charges apply when outside of free tier allowance

Firewall (security groups)

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

We'll create a new security group called 'launch-wizard-4' with the following rules:

Number of instances: 1

Software Image (AMI): Amazon Linux 2023 AMI 2023.4.2...read more

Virtual server type (instance type): t2.micro

Firewall (security group): New security group

Storage (volumes): 1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2

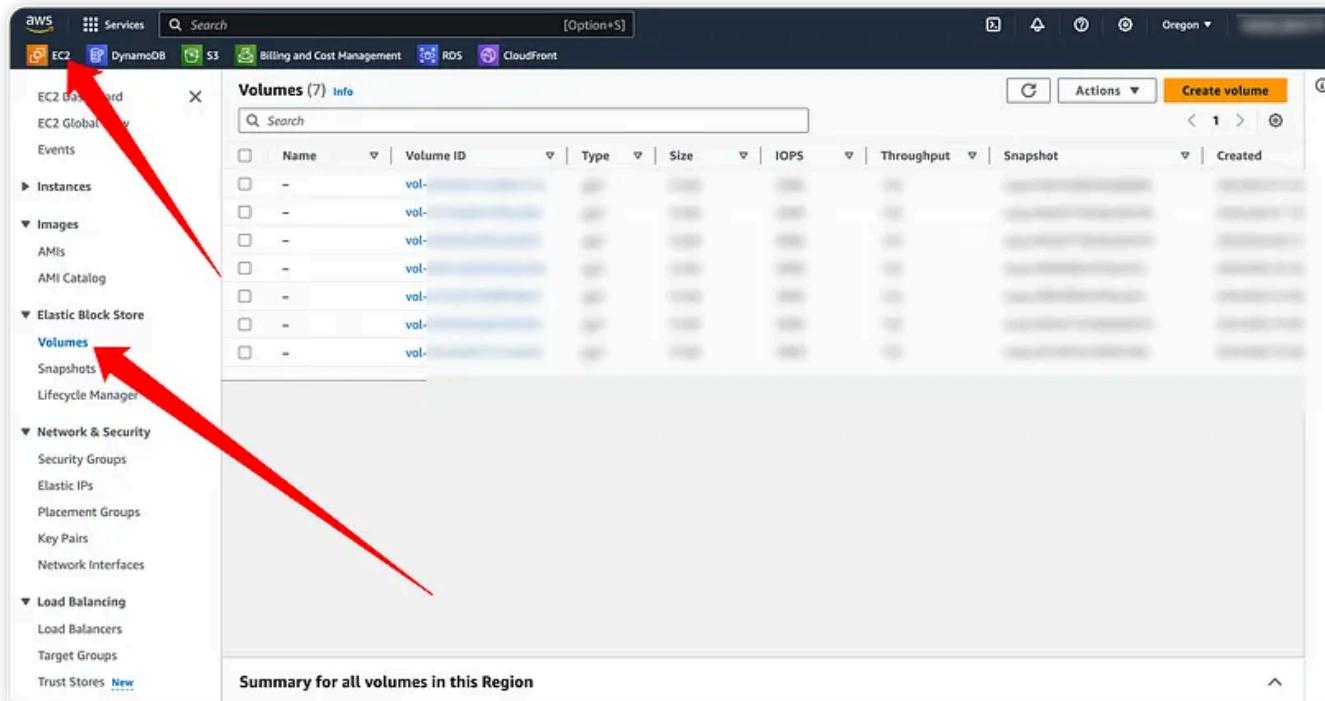
Cancel Launch instance Review commands

Review and Launch:

- Review your configuration and click Launch.
 - Select or create a key pair and acknowledge that you have access to the selected key pair.
- Click Launch Instances.
-

Step 4: Connect the snapshot volume to Instance

Stop the Instance and Detach the Default Root Volume



Screenshot of the AWS EC2 Volumes page. The left sidebar shows navigation options like EC2 Dashboard, Instances, Images, and Network & Security. The main table lists 7 volumes across various availability zones. The 'Attached resources' column for the first volume shows the path '/dev/xvda (attached)'. A red arrow points to this path.

	availability Zone	Volume state	Alarm status	Attached resources	Volume state	Encryption
1	s-west-2a	In-use	No alarms	/dev/xvda (attached)	Okay	Not encrypted
2	s-west-2a	In-use	No alarms	/dev/xvda (attached)	Okay	Not encrypted
3	s-west-2a	In-use	No alarms	/dev/xvda (attached)	Okay	Not encrypted
4	s-west-2a	Available	No alarms	/dev/xvda (attached)	Okay	Not encrypted
5	s-west-2a	Available	No alarms	/dev/xvda (attached)	Okay	Not encrypted
6	s-west-2a	In-use	No alarms	/dev/xvda (attached)	Okay	Not encrypted

Screenshot of the AWS EC2 Volumes page. The left sidebar shows navigation options like EC2 Dashboard, Instances, Images, and Network & Security. The main table lists 7 volumes. A red arrow points to the 'Actions' button for the first volume. A second red arrow points to the 'Detach volume' option in the context menu that appears when the 'Actions' button is clicked.

	Name	Volume ID	Type	Size	IOPS	Throughput	Snapshot
1	-	vol-	gp3	8 GiB	3000	125	snap-03b
2	-	vol-	gp3	8 GiB	3000	125	snap-002
3	-	vol-	gp3	8 GiB	3000	125	snap-002
4	-	vol-	gp3	8 GiB	3000	125	snap-002
5	-	vol-	gp3	8 GiB	3000	125	snap-0d5
6	-	vol-	gp3	8 GiB	3000	125	snap-0a7

Attach the New Volume Created from the Snapshot

The screenshot shows the AWS EC2 Volumes page. On the left, there's a navigation sidebar with various services like EC2 Dashboard, Instances, Images, etc. The main area is titled "Volumes (1/7) Info" and lists a single volume named "vol". The volume details are: Name: vol, Volume ID: vol-06f1cd6295454238e, Type: gp3, Size: 8 GiB, IOPS: 3000, Throughput: 125, and Snapshot: snap-03b7. A red arrow points from the top-left towards the volume row. Another red arrow points from the top-right towards the "Actions" dropdown menu. The "Actions" menu is open, showing options like Modify volume, Create snapshot, Create snapshot lifecycle policy, Delete volume, Attach volume (which is highlighted), Detach volume, Force detach volume, Manage auto-enabled I/O, Manage tags, and Fault injection.

The screenshot shows the "Attach volume" dialog. At the top, it says "Attach volume" and "Info". Below that, it says "Attach a volume to an instance to use it as you would a regular physical hard disk drive." The "Basic details" section includes a "Volume ID" field with "vol-06f1cd6295454238e" selected, and an "Availability Zone" field set to "us-west-2a". The "Instance" section has a "Search instance ID or name tag" input field with "Q |" and a dropdown list below it containing several instance names starting with "i-". A red arrow points from the top-left towards the instance search field. Another red arrow points from the bottom-right towards the "Attach volume" button. At the bottom of the dialog are "Cancel" and "Attach volume" buttons.

Start the instance again.

Step 5: Steps to Unassociate and Reassociate an Elastic IP

Introduction to AWS Elastic Load Balancing

Open in app ↗

Sign up

Sign in

Medium



Search



Write



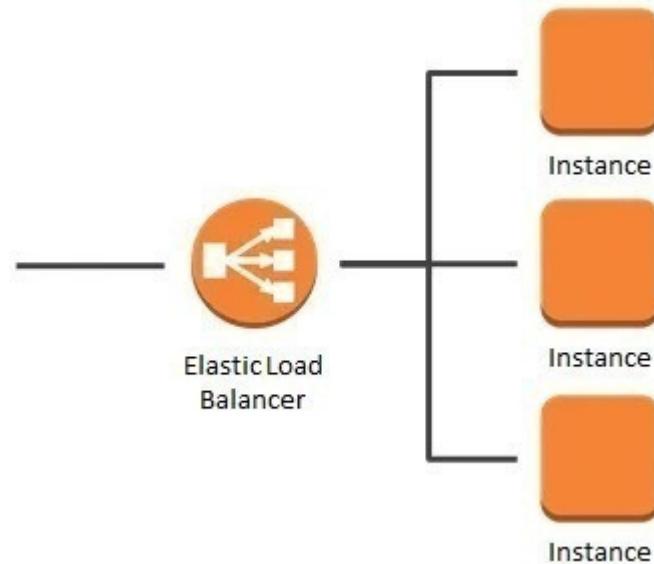
Introduction to AWS Load Balancing



Meriem Terki · [Follow](#)

Published in [AWS Tip](#) · 10 min read · Jan 18, 2024

5



Looking to learn and practice about Elastic Load Balancing ?

incoming application traffic across multiple Amazon EC2 instances in the cloud. We will demonstrate elastic load balancing with 2 EC2 Instances.

Introduction

What is Elastic Load Balancing?

- ELB is a service that automatically distributes incoming application traffic and scale resources to meet traffic demands.
- ELB helps in adjusting capacity according to incoming application and network traffic.
- ELB can be enabled within a single availability zone or across multiple availability zones to maintain consistent application performance.

What are ELB features?

- Detection of unhealthy EC2 instances.
- Spreading EC2 instances across healthy channels only.
- Centralized management of SSL certificates.
- Optional public key authentication.
- Support for both IPv4 and IPv6.
- ELB accepts incoming traffic from clients and routes requests to its registered targets.
 - When an unhealthy target or instance is detected, ELB stops routing traffic to it and resumes only when the instance is healthy again.
- ELB monitors the health of its registered targets and ensures that the traffic is routed only to healthy instances.
-

- ELB's are configured to accept incoming traffic by specifying one or more listeners. A listener is a process that checks for connection requests.
- Listeners are configured with a protocol and port number from the client to the ELB and vice-versa i.e., back from ELB to the client.

What are ELB types of load balancers ?

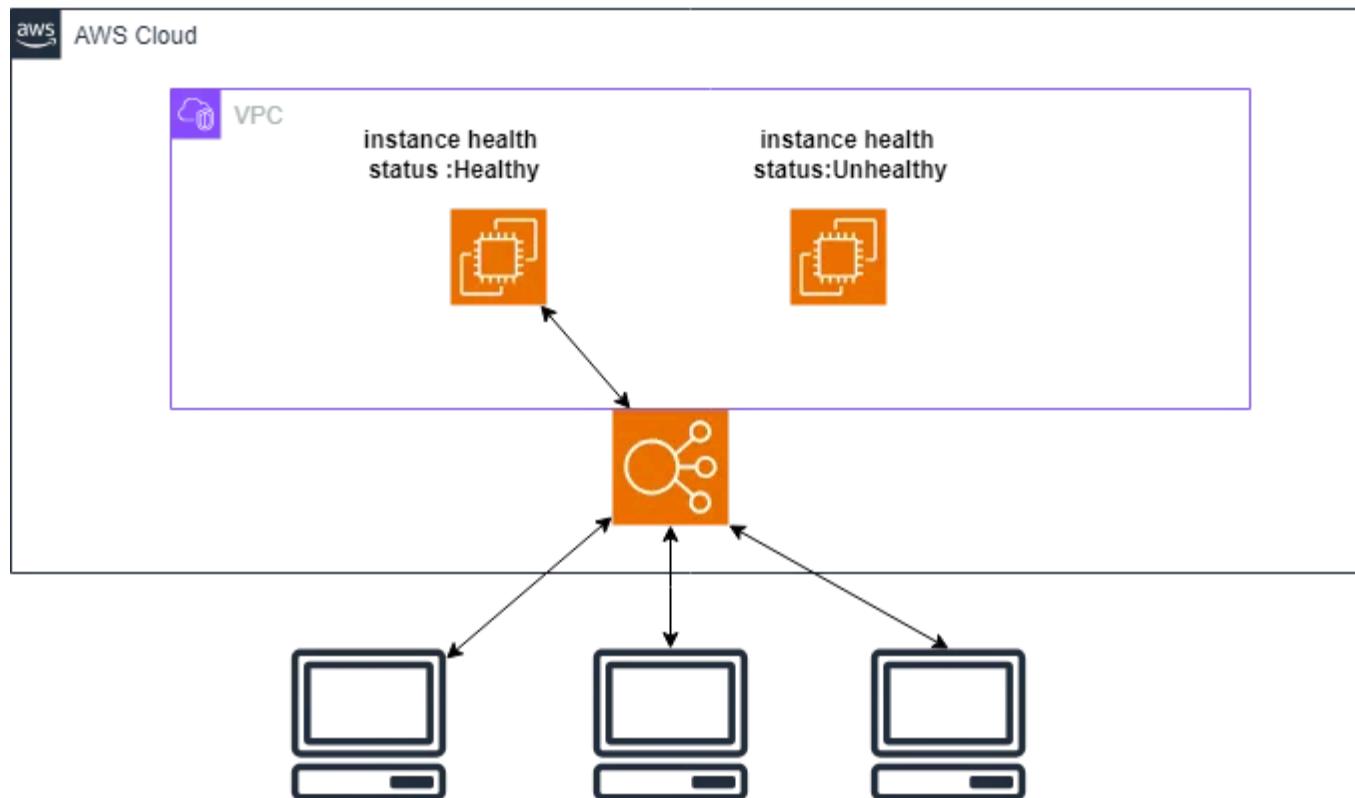
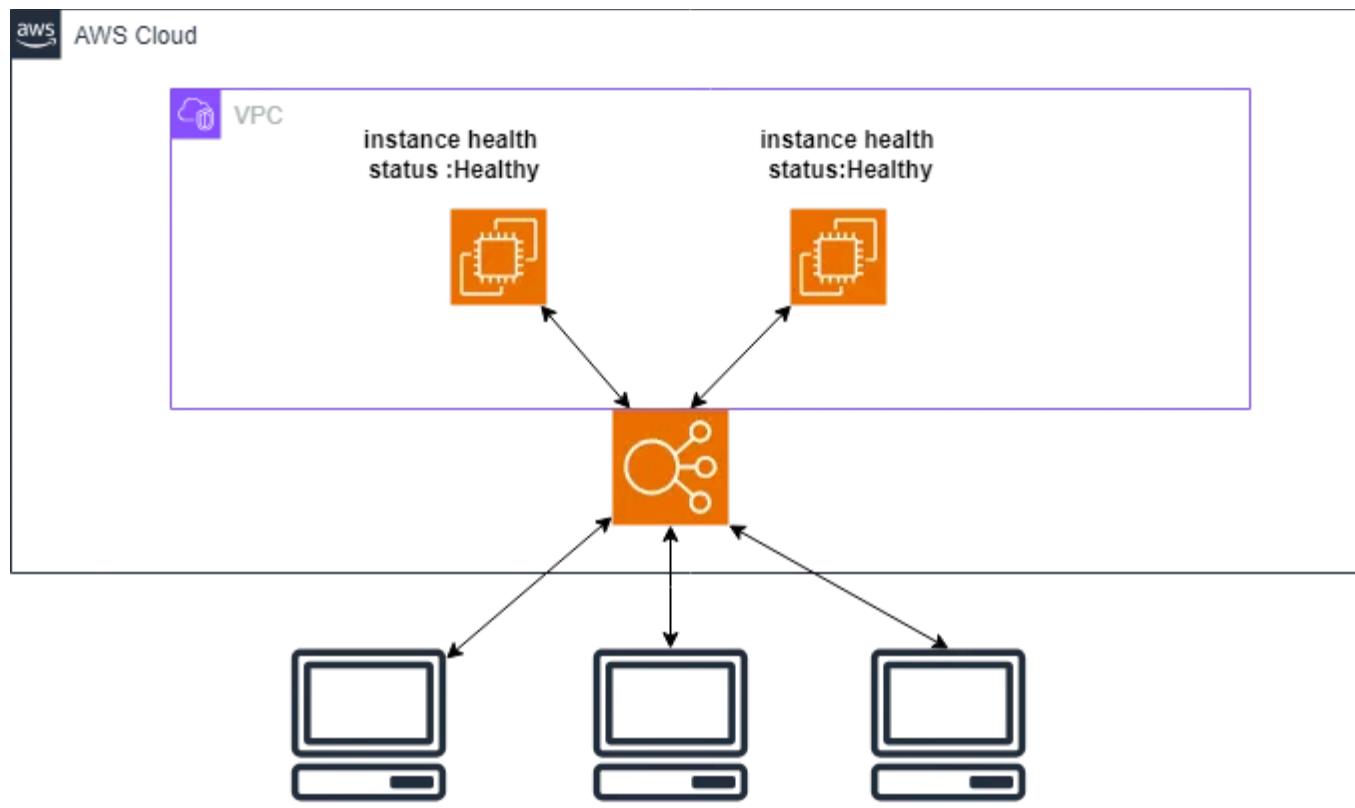
- Application Load Balancers
- Network Load Balancers
- Classic Load Balancers
- Each load balancer is configured differently.
- For Application and Network Load Balancers, you register targets in target groups and route traffic to target groups.
For Classic Load Balancers, you register instances with the load balancer.
- AWS recommends users to work with Application Load Balancer to use multiple Availability Zones because if one availability zone fails, the load balancer can continue to route traffic to the next available one.

Some more features

- We can have our load balancer be either internal or internet-facing.
The nodes of an internet-facing load balancer have Public IP addresses,
- and the DNS name is publicly resolvable to the Public IP addresses of the nodes.

- Due to the point above, internet-facing load balancers can route requests from clients over the Internet.
 - The nodes of an internal load balancer have only Private IP addresses, and the DNS name is publicly resolvable to the Private IP addresses of the nodes.
 - Due to the point above, internal load balancers can only route requests from clients with access to the VPC for the load balancer.
- Both internet-facing and internal load balancers route requests to your
- targets using Private IP addresses.
- Your targets do not need Public IP addresses to receive requests from an
- internal or an internet-facing load balancer.

Architecture Diagram



Task Steps

Step 1: Sign in to AWS Management Console

1. On the AWS sign-in page ,enter your credentials to log in to your AWS account and click on the Sign in button.

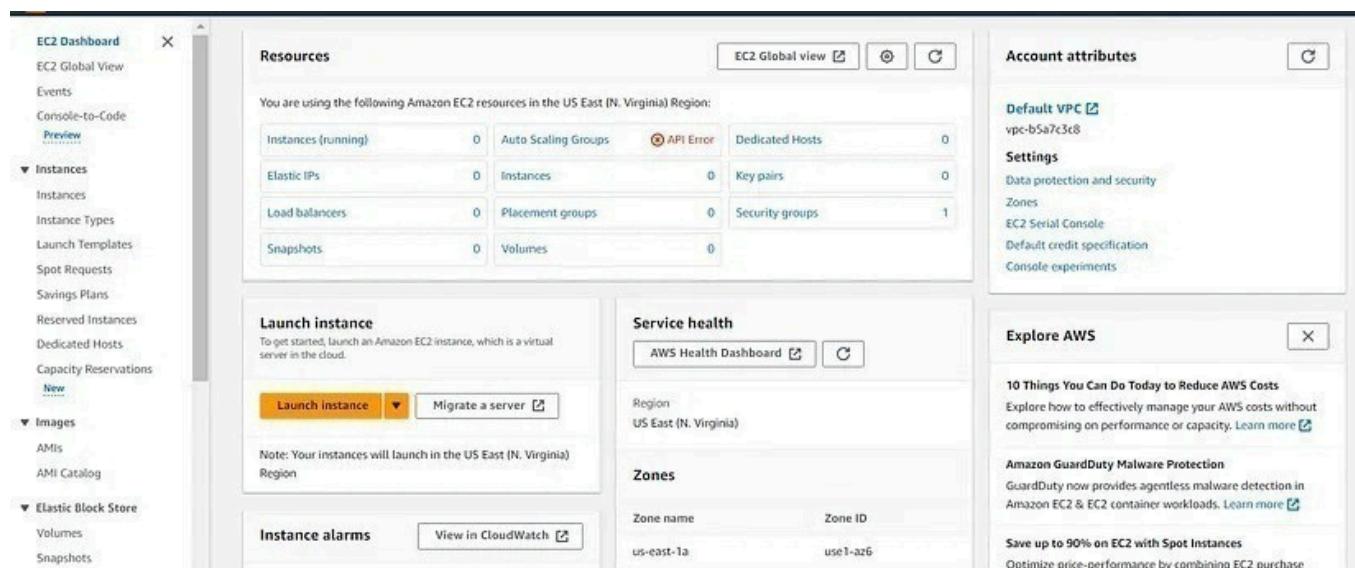
2. Once Signed In to the AWS Management Console, Make the default AWS Region as US East (N. Virginia) us-east-1

Step 2: Launching First EC2 Instance

1. Make sure you are in the US East (N. Virginia) us-east-1 Region.
2. Navigate to EC2 by clicking on the Services menu in the top, then click on EC2 in the Compute section.



3. Navigate to Instances on the left panel and click on Launch Instances button.



3. Name: Enter MyEC2Server

EC2 > Instances > Launch an 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.

Name and tags Info

Name

MyEC2Server Add additional tags

4. For Amazon Machine Image (AMI): Search for Amazon Linux 2 AMI in the search box and click on the Select button.

▼ 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

Quick Start

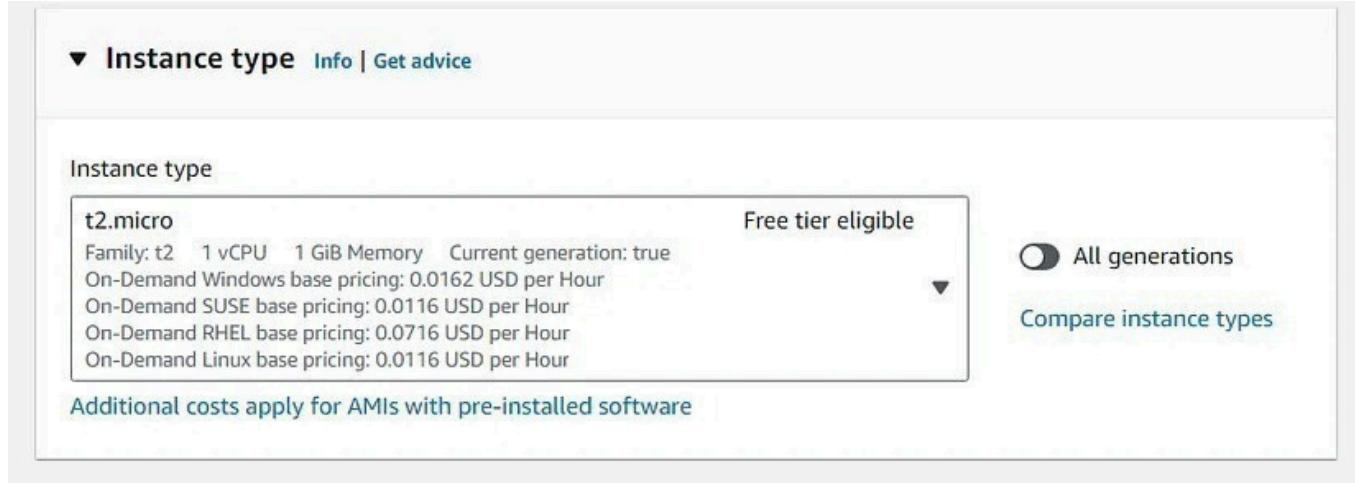
Amazon Linux 	macOS 	Ubuntu 	Windows 	Red Hat 	SUSE Li 
--	---	--	---	---	---

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

Amazon Machine Image (AMI)

Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type ami-0c0b74d29acd0cd97 (64-bit (x86)) / ami-095889fa7a7b9da4e (64-bit (Arm)) Virtualization: hvm ENA enabled: true Root device type: ebs	Free tier eligible 
---	--

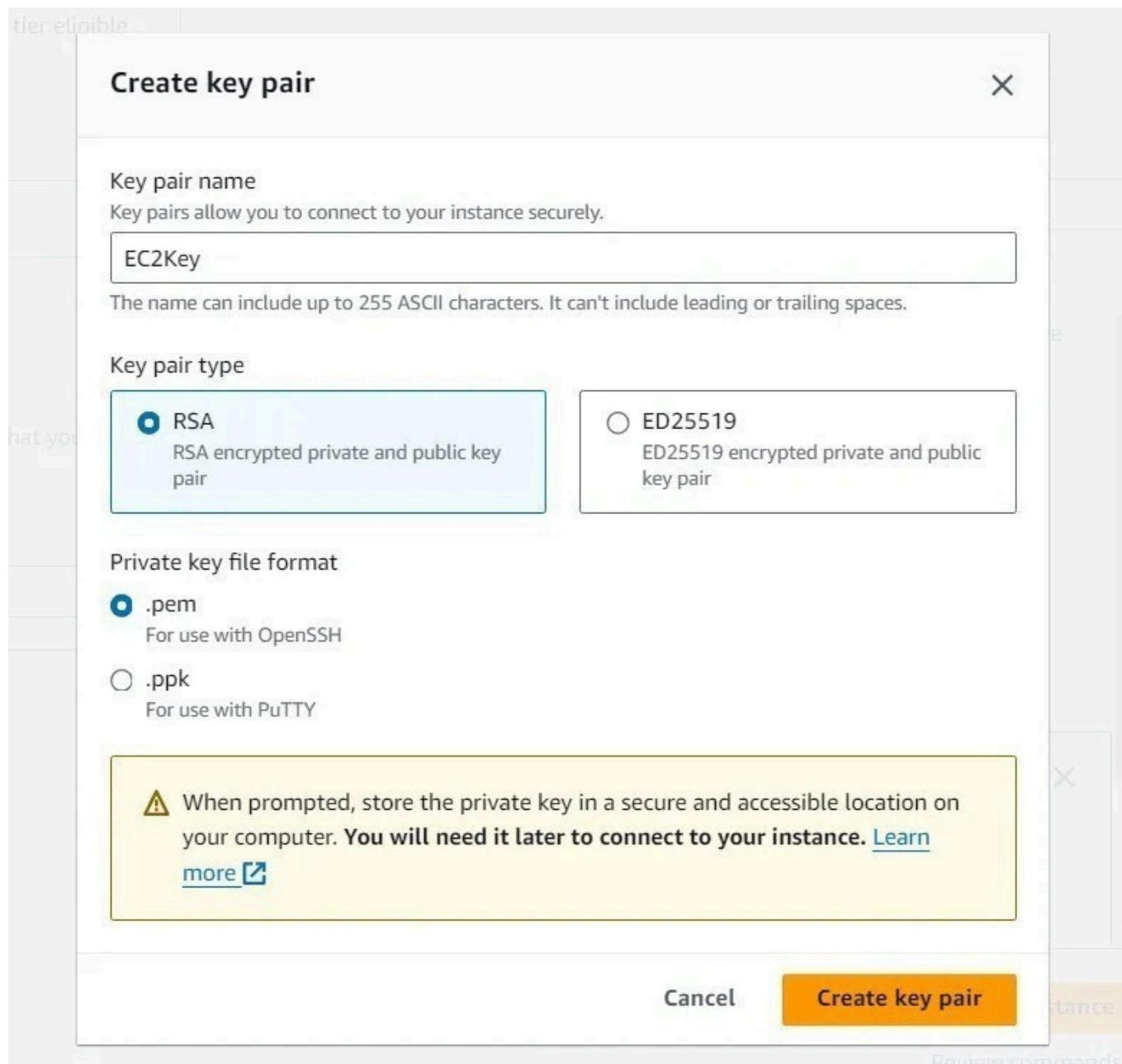
6. For Instance Type: Select t2.micro



7. For Key pair: Select Create a new key pair Button

- Key pair name: EC2Key
- Key pair type: RSA
- Private key file format: .pem

8. Select Create key pair Button.



9. In Network Settings Click on Edit button:

- Auto-assign public IP: Enable
- Select Create new Security group
- Security group name : Enter MyEC2Server_SG
- Description : Enter Security Group to allow traffic to EC2

▼ Network settings [Info](#)

VPC - required [Info](#)

vpc-b5a7c3c8 (Default VPC) (default) [Edit](#)

Subnet [Info](#)

No preference [Edit](#) [Create new subnet](#)

Auto-assign public IP [Info](#)

Enable [Edit](#)

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

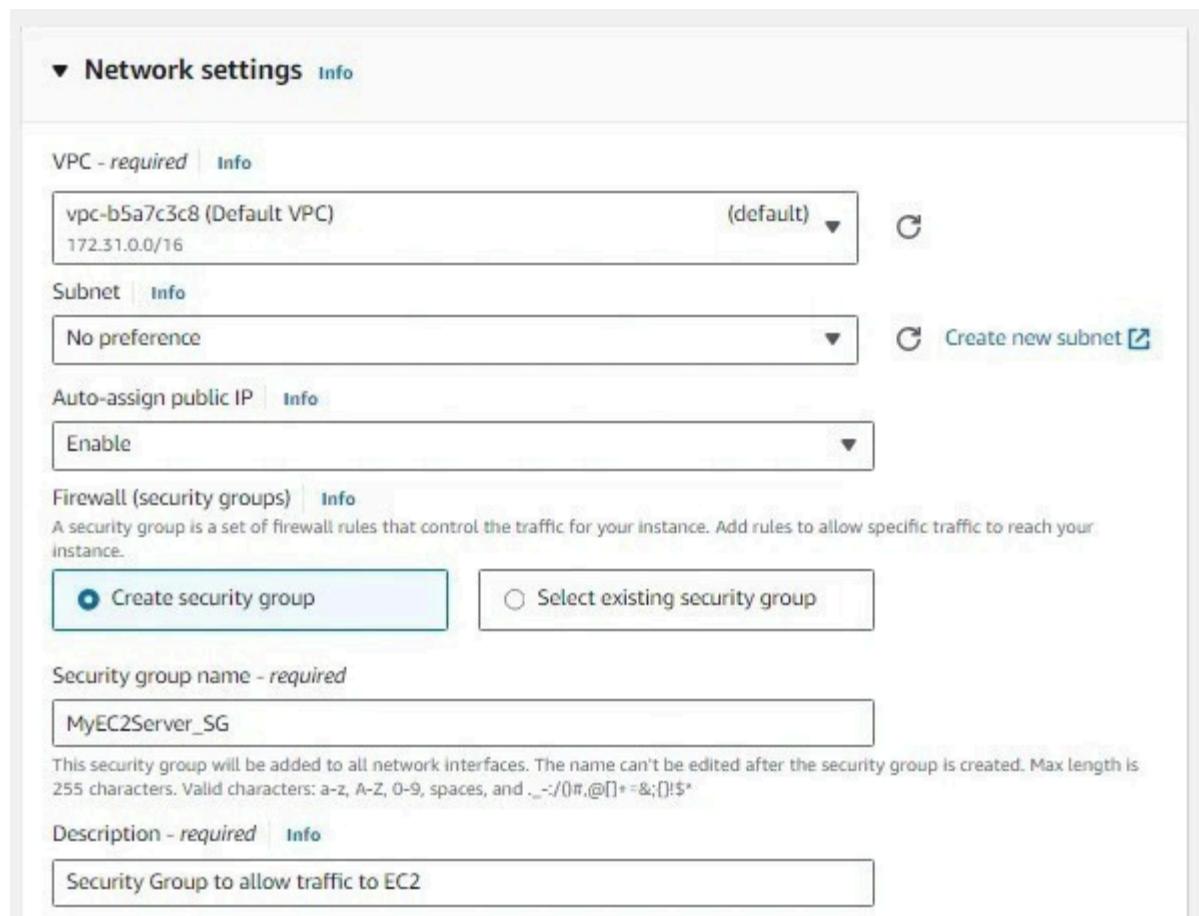
Security group name - required

MyEC2Server_SG

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 to allow traffic to EC2



10. Check Allow SSH from and Select Anywhere from dropdown

- To add SSH,
- Choose Type: SSH
- Source: Select Anywhere
- For HTTP, Click on Add security group rule
- Choose Type: HTTP
- Source: Select Anywhere
- For HTTPS, Click on Add security group rule
- Choose Type: HTTPS
- Source: Select Anywhere

Inbound Security Group Rules

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

Type | Info Protocol | Info Port range | Info

ssh TCP 22

Remove

Source type | Info Source | Info Description - optional | Info

Anywhere Add CIDR, prefix list or security e.g. SSH for admin desktop

0.0.0.0/0 X

▼ Security group rule 2 (TCP, 80, 0.0.0.0/0)

Type | Info Protocol | Info Port range | Info

HTTP TCP 80

Remove

Source type | Info Source | Info Description - optional | Info

Anywhere Add CIDR, prefix list or security e.g. SSH for admin desktop

0.0.0.0/0 X

▼ Security group rule 3 (TCP, 443, 0.0.0.0/0)

Type | Info Protocol | Info Port range | Info

HTTPS TCP 443

Remove

Source type | Info Source | Info Description - optional | Info

Anywhere Add CIDR, prefix list or security e.g. SSH for admin desktop

0.0.0.0/0 X

11. Click on Advanced details and under the User data: section, Enter the following script to create an HTML page served by an Apache httpd web server.

```
#!/bin/bash
sudo su
yum update -y
yum install httpd -y
echo "<html><h1>Welcome to Server 1 </h1></html>" > /var/www/html/index.html
systemctl start httpd
systemctl enable httpd
```

12. Keep Rest thing Default and Click on Launch Instance Button.



13. Select View all Instances to View Instance you Created.

14. Launch Status: Your instance is now launching, Click on the instance ID and wait for complete initialization of the instance till status changes to Running.

Step3 : Launching Second EC2 Instance

1. Make sure you are in the US East (N. Virginia) us-east-1 Region.
2. Navigate to EC2 by clicking on the Services menu in the top, then click on EC2 in the Compute section.
3. Navigate to Instances on the left panel and click on Launch Instances button.
4. Name : Enter MyEC2Server2

Launch an instance [Info](#)

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

Name and tags [Info](#)

Name

 [Add additional tags](#)

- 5.. For Amazon Machine Image (AMI): Search for Amazon Linux 2 AMI in the search box and click on the Select button.

▼ 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

6. For Instance Type: select t2.micro

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

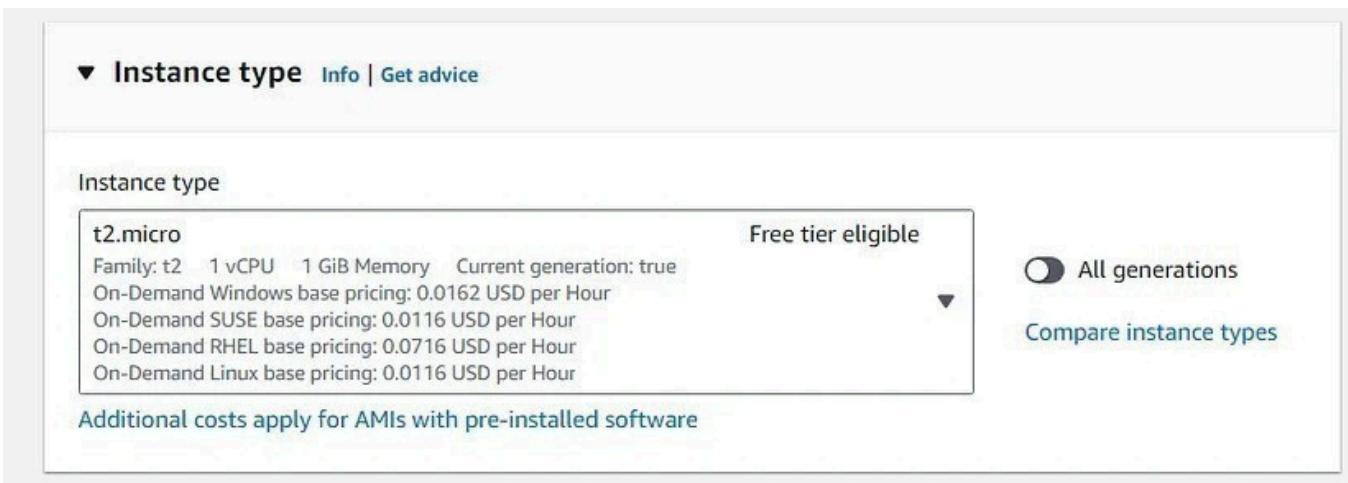
Instance type

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	

Additional costs apply for AMIs with pre-installed software

All generations

[Compare instance types](#)



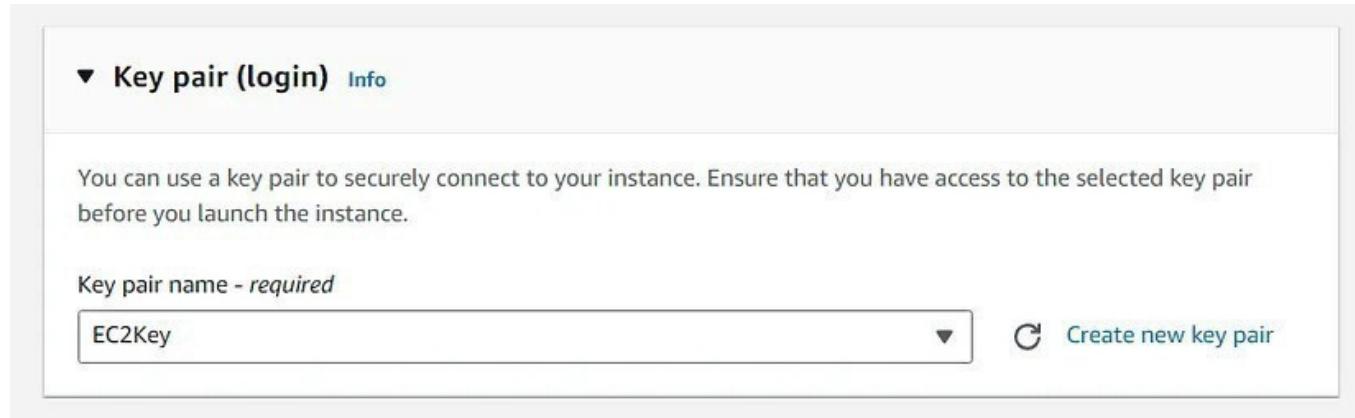
7. For Key pair: Select the key you created previously.

▼ 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.

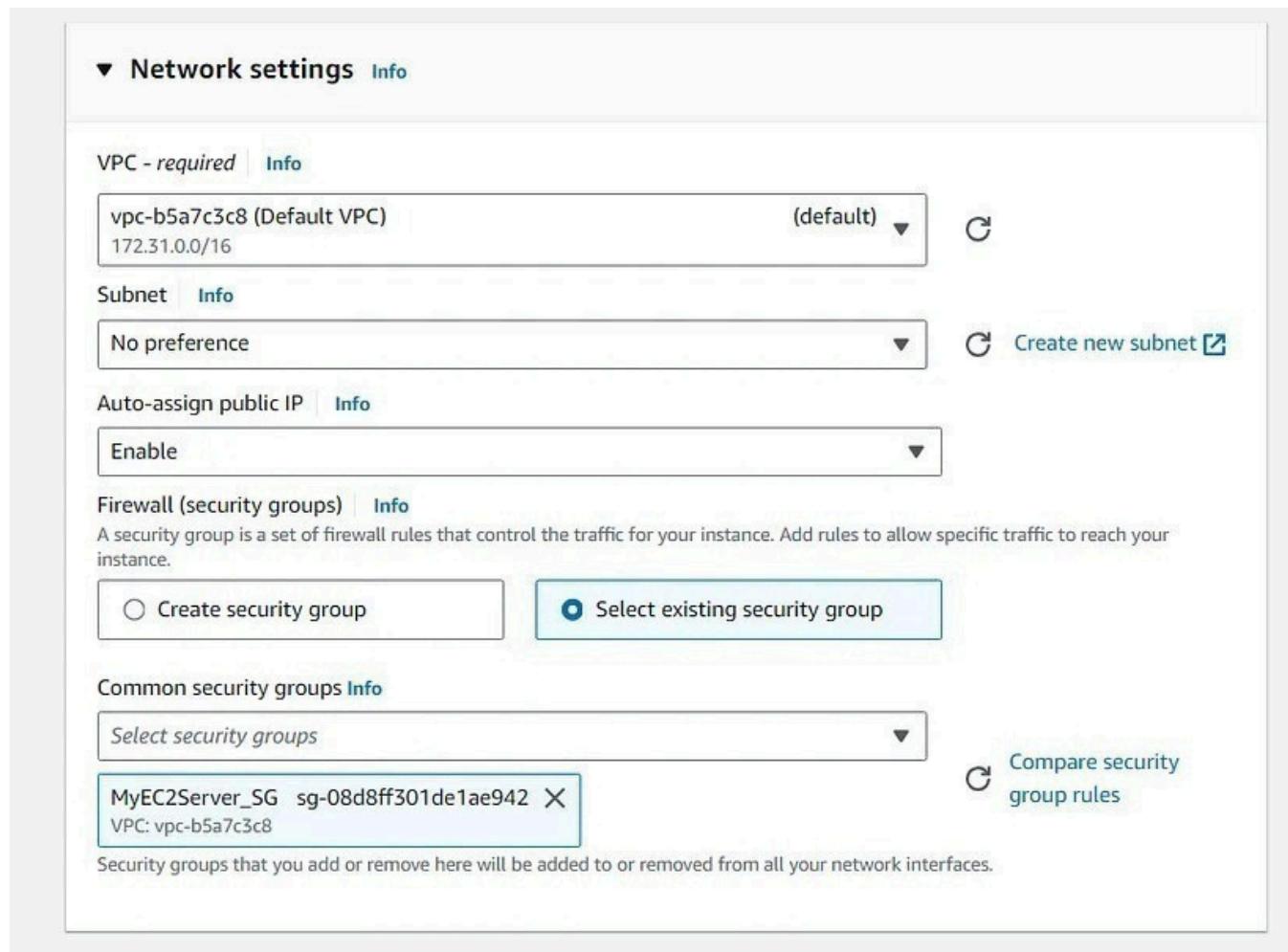
Key pair name - *required*

[!\[\]\(aa9b36e8b875671c3bd80877dcf5daf3_img.jpg\) Create new key pair](#)



8. In Network Settings Click on Edit:

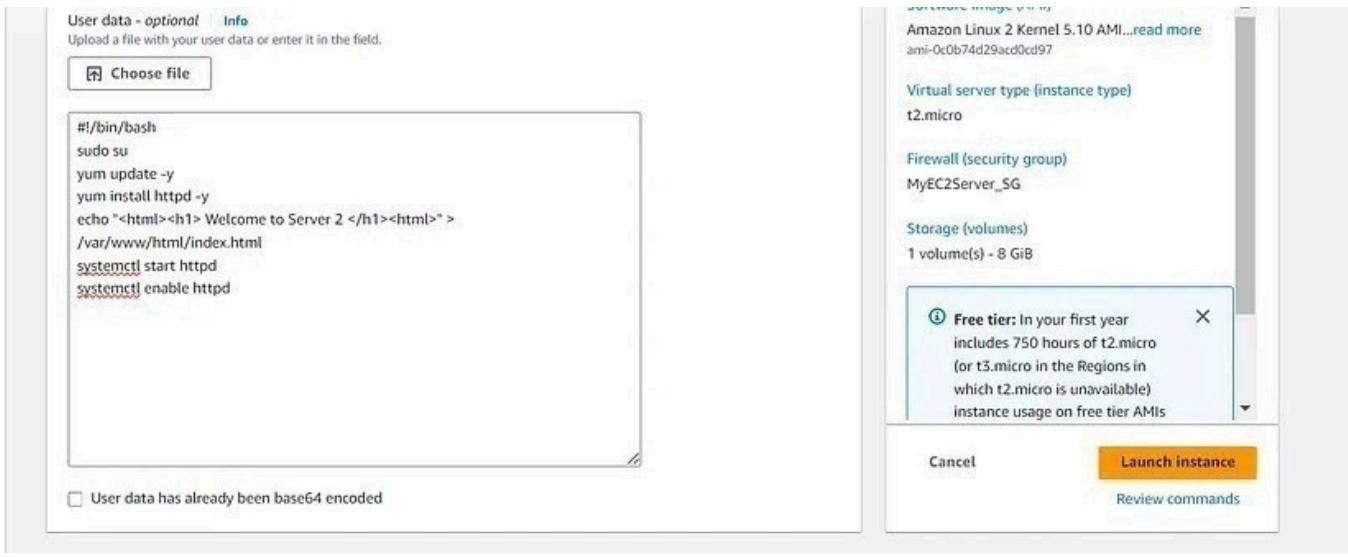
- Auto-assign public IP: Enable
- Select Select existing security group and Select the group created earlier.



9. Click on Advanced details and under the User data: section, Enter the following script to create an HTML page served by Apache httpd web server:

```
#!/bin/bash sudo su yum update -y yum install httpd -y echo "<html><h1> Welcome to Server 2 </h1><html>" > /var/www/html/index.html systemctl start httpd systemctl enable httpd
```

10. Keep Rest thing Default and Click on Launch Instance Button.



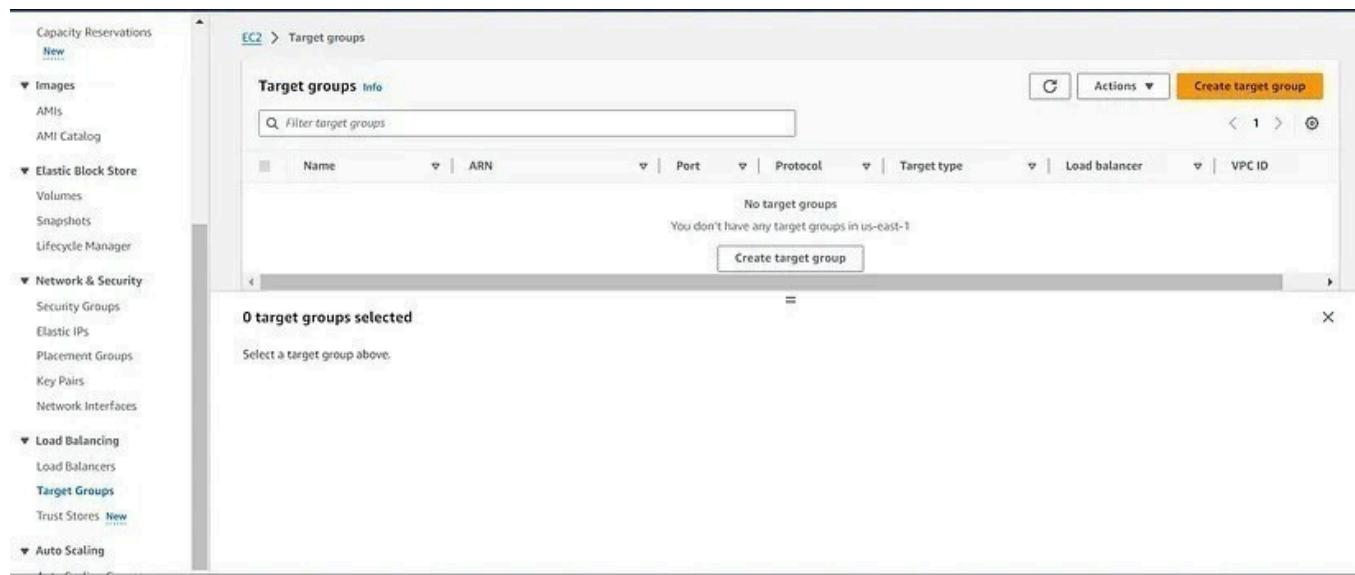
11. Select View all Instances to View Instance you Created

12. Launch Status: Your instance is now launching. Click on View Instances. In the dashboard find your instance and wait for complete initialization of the instance until the instance state changes to running.

Instances (2) Info		Connect		Instance state ▼		Actions ▼		Launch instances ▼	
<input type="checkbox"/>	Name ▼	Instance ID	Instance state ▼	Instance type ▼	Status check ▼	Alarm status	Availability Zone ▼	Public IPv4 DNS	Public IPv4
<input type="checkbox"/>	MyEC2Server	i-01c19759dc52a899a	Running View Logs	t2.micro	2/2 checks passed View alarms +	us-east-1a	ec2-18-209-105-234.co...	18.209.105...	
<input type="checkbox"/>	MyEC2Server2	i-0a7b0ac6aa4f24acb	Running View Logs	t2.micro	2/2 checks passed View alarms +	us-east-1a	ec2-54-175-240-156.co...	54.175.240...	

Step 4: Creating the Target Group and Load Balancer

1. In the EC2 Console, Navigate to Target Groups, present in the left panel under Load Balancing.
2. Click on the Create target group button.



3. For Step 1, Specify group details

- Under Basic configurations,
- Choose a target group: Choose Instances
- Target group name: Enter MyTargetGroup

Basic configuration

Settings in this section can't be changed after the target group is created.

Choose a target type

Instances

- Supports load balancing to instances within a specific VPC.
- Facilitates the use of [Amazon EC2 Auto Scaling](#) to manage and scale your EC2 capacity.

IP addresses

- Supports load balancing to VPC and on-premises resources.
- Facilitates routing to multiple IP addresses and network interfaces on the same instance.
- Offers flexibility with microservice based architectures, simplifying inter-application communication.
- Supports IPv6 targets, enabling end-to-end IPv6 communication, and IPv4-to-IPv6 NAT.

Lambda function

- Facilitates routing to a single Lambda function.
- Accessible to Application Load Balancers only.

Application Load Balancer

- Offers the flexibility for a Network Load Balancer to accept and route TCP requests within a specific VPC.
- Facilitates using static IP addresses and PrivateLink with an Application Load Balancer.

Target group name

MyTargetGroup

A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

- Keep all the settings as default.
- Scroll to the end of the page and click on the Next button.

4. For Step 2, Register targets

- Select both instances and click on the Include as pending below button.

- Instances will be present in the Review targets part, having health status as Pending.

- Click on the Create target group button.
- The Target group is now created.
 - In the EC2 console, navigate to Load balancers in the left-side panel.
 - Click on Create Load Balancer button at the top-left to create a new load balancer for our web servers.

The screenshot shows the AWS EC2 Load Balancers page. The left sidebar includes links for EC2 Dashboard, EC2 Global View, Events, Console-to-Code, Instances, Images, Elastic Block Store, and Network & Security. The main content area is titled "Load balancers" and contains a message: "Elastic Load Balancing scales your load balancer capacity automatically in response to changes in incoming traffic." A search bar labeled "Filter load balancers" is present. Below it is a table header with columns: Name, DNS name, State, VPC ID, Availability Zones, Type, and Date created. A message "No load balancers" and "You don't have any load balancers in us-east-1" is displayed. A prominent orange "Create load balancer" button is at the bottom.

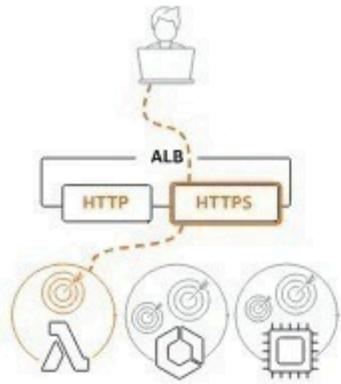
8. Select Load Balancer Type: Under the Application load balancer, click on Create button

Compare and select load balancer type

A complete feature-by-feature comparison along with detailed highlights is also available. [Learn more](#)

Load balancer types

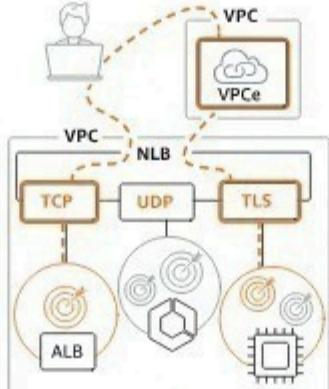
Application Load Balancer [Info](#)



Choose an Application Load Balancer when you need a flexible feature set for your applications with HTTP and HTTPS traffic. Operating at the request level, Application Load Balancers provide advanced routing and visibility features targeted at application architectures, including microservices and containers.

[Create](#)

Network Load Balancer [Info](#)



Choose a Network Load Balancer when you need ultra-high performance, TLS offloading at scale, centralized certificate deployment, support for UDP, and static IP addresses for your applications. Operating at the connection level, Network Load Balancers are capable of handling millions of requests per second securely while maintaining ultra-low latencies.

[Create](#)

Gateway Load Balancer [Info](#)



Choose a Gateway Load Balancer when you need to deploy and manage a fleet of third-party virtual appliances that support GENEVE. These appliances enable you to improve security, compliance, and policy controls.

[Create](#)

▶ [Classic Load Balancer - previous generation](#)

[Close](#)

9. To create an Application load balancer, configuring the load balancer as below

- For the Basic configuration section,

- Name: Enter MyLoadBalancer
- Scheme: Select Internet-facing
- IP address type: Choose IPv4

Basic configuration

Load balancer name
Name must be unique within your AWS account and can't be changed after the load balancer is created.
 MyLoadBalancer
A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

Scheme [Info](#)
Scheme can't be changed after the load balancer is created.

Internet-facing
An internet-facing load balancer routes requests from clients over the internet to targets. Requires a public subnet. [Learn more](#)

Internal
An internal load balancer routes requests from clients to targets using private IP addresses.

IP address type [Info](#)
Select the type of IP addresses that your subnets use.

IPv4
Recommended for internal load balancers.

Dualstack
Includes IPv4 and IPv6 addresses.

- For the Network mapping section:
- VPC: Select Default
- Mappings: Select all the Availability zone present

Network mapping [Info](#)

The load balancer routes traffic to targets in the selected subnets, and in accordance with your IP address settings.

VPC [Info](#)

Select the virtual private cloud (VPC) for your targets or you can create a new VPC [Create](#). Only VPCs with an internet gateway are enabled for selection. The selected VPC can't be changed after the load balancer is created. To confirm the VPC for your targets, view your [target groups](#) [Edit](#)

Default VPC
vpc-b5a7cfb
IPv4: 172.51.0.0/16

Mappings [Info](#)

Select at least two Availability Zones and one subnet per zone. The load balancer routes traffic to targets in these Availability Zones only. Availability Zones that are not supported by the load balancer or the VPC are not available for selection.

us-east-1a (use1-az6)
Subnet
subnet-1b134744

IPv4 address
Assigned by AWS

us-east-1b (use1-az1)
Subnet
subnet-3bf0b85d

IPv4 address
Assigned by AWS

us-east-1c (use1-az2)
Subnet
subnet-7b97c15a

IPv4 address
Assigned by AWS

us-east-1d (use1-az4)
Subnet
subnet-62445f2f

IPv4 address
Assigned by AWS

us-east-1e (use1-az3)
Subnet
subnet-7e851a4f

IPv4 address
Assigned by AWS

us-east-1f (use1-az5)
Subnet
subnet-13bfbd1d

IPv4 address
Assigned by AWS

- For the Security groups section,
- Select the MyEC2Server_SG Security group from the dropdown and remove the default security group.

Security groups [Info](#)
A security group is a set of firewall rules that control the traffic to your load balancer. Select an existing security group, or you can create a new security group [Create new](#).

Security groups

Select up to 5 security groups [▼](#) [C](#)

MyEC2Server_SG [X](#)
sg-08d8ff301de1ae942 VPC: vpc-b5a7e3c8

- For the Listeners and routing section,
- The listener is already present with Protocol HTTP and Port 80.
- Select the target group MyTargetGroup for the Default action forwards to option.

Listeners and routing [Info](#)
A listener is a process that checks for connection requests using the port and protocol you configure. The rules that you define for a listener determine how the load balancer routes requests to its registered targets.

▼ Listener HTTP:80 [Remove](#)

Protocol Port Default action [Info](#)

HTTP : 80 Forward to [MyTargetGroup](#) Target type: Instance, IPv4 [HTTP](#) [C](#)

[Create target group](#)

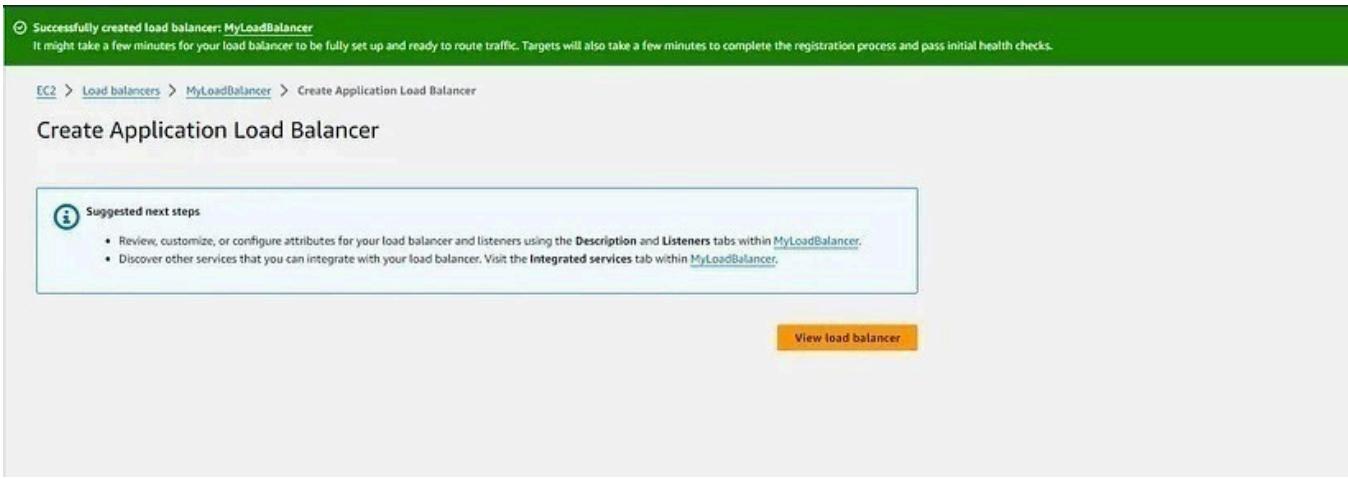
Listener tags - optional
Consider adding tags to your listener. Tags enable you to categorize your AWS resources so you can more easily manage them.

[Add listener tag](#)
You can add up to 50 more tags.

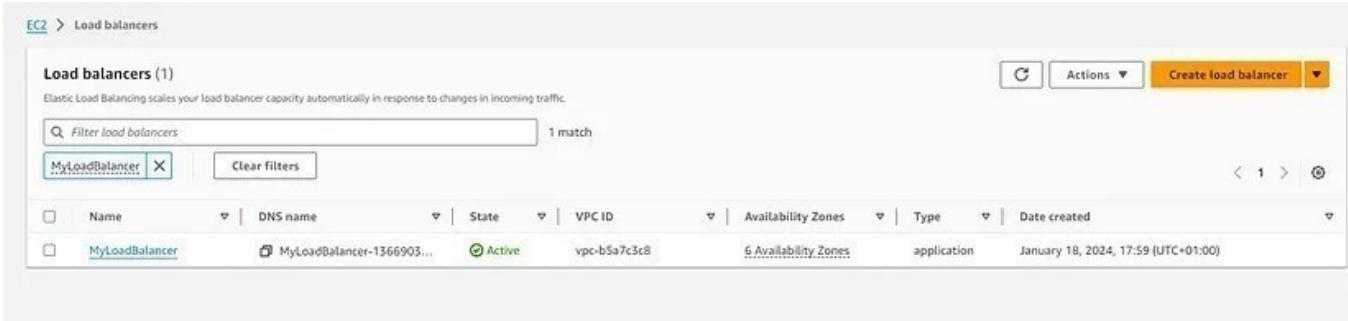
[Add listener](#)

10. Keep the tags as default and click on the Create load balancer button.

11. You have successfully created the Application Load balancer. Click on the View load balancers button.



12. Wait for 2 to 3 minutes for the load balancer to become Active.



Step 5: Testing the Elastic Load Balancer

1. Click on Target groups from the left menu section.
2. Select MyTargetGroup and navigate to the Targets tab below.
3. Wait until the status column of the instances changes to healthy (this means both web servers have passed ELB health check)

The screenshot shows the 'Target groups' section of the AWS EC2 console. A single target group named 'MyTargetGroup' is listed. The details are as follows:

Name	ARN	Port	Protocol	Target type	Load balancer	VPC ID
MyTargetGroup	arn:aws:elasticloadbalancing:us-east-1:990629140213:targetgroup/MyTargetGroup/01d1d7a3f11b3d7	80	HTTP	Instance	MyLoadBalancer	vpc-b5a7c3c8

The screenshot shows the 'Registered targets' section for the 'MyTargetGroup'. There are two registered targets, both labeled as 'Healthy' and 'Normal':

Instance ID	Name	Port	Zone	Health status	Anomaly detection result
i-01c19759dc52a899a	MyEC2Server	80	us-east-1a	Healthy	Normal
i-0a7b0ac6aa4f24acb	MyEC2Server2	80	us-east-1a	Healthy	Normal

4. Next, navigate to Load Balancers and notice the state of ELB is active.

5. Copy the DNS name of the ELB and enter the address in the browser.

- DNS Example: myloadbalancer-1366903611.us-east-1.elb.amazonaws.com

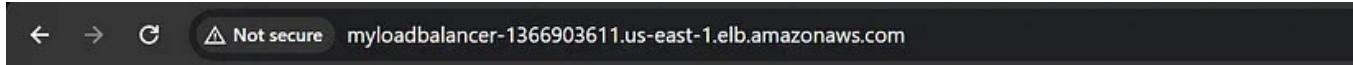
The screenshot shows the 'Load balancers' section of the AWS EC2 console. A single load balancer named 'MyLoadBalancer' is listed as active. The details are as follows:

Name	DNS name	State	VPC ID	Availability Zones	Type	Date created
MyLoadBalancer	MyLoadBalancer-1366903...	Active	vpc-b5a7c3c8	6 Availability Zones	application	January 18, 2024, 17:59 (UTC+01:00)

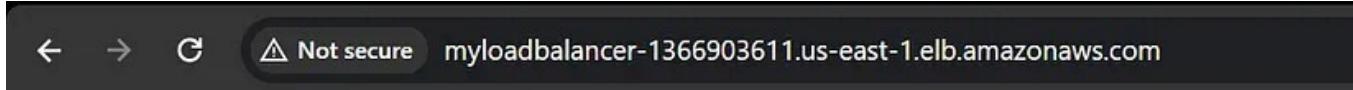
The screenshot shows the detailed configuration of the 'MyLoadBalancer'. Key details include:

- Scheme:** Internet-facing
- Hosted zone:** Z355XDOTRQ7XK
- Availability Zones:**
 - subnet-7e851a4f (us-east-1e)
 - subnet-7b97c15a (us-east-1c)
 - subnet-1b134744 (us-east-1a)
 - subnet-13bfbd1d (us-east-1f)
 - subnet-3bf0b885d (us-east-1b)
 - subnet-62445f2f (us-east-1d)
- Date created:** January 18, 2024, 17:59 (UTC+01:00)
- Load balancer ARN:** arn:aws:elasticloadbalancing:us-east-1:990629140213:loadbalancer/app/MyLoadBalancer/01d1d7a3f11b3d7
- DNS name:** MyLoadBalancer-1366903611.us-east-1.elb.amazonaws.com (A Record)

6. You should see the index.html page content of Web Server 1 or Web Server 2



Welcome to Server 1



Welcome to Server 2

7. Now Refresh the page a few times. You will observe that the index pages change each time you refresh.

Note: The ELB is equally dividing the incoming traffic to both servers in a Round Robin manner.

8. For testing, if ELB is working properly,

- In the left side menu, scroll up and navigate back to the Instances page. Select MyEC2Server1, click on Instance State and click on Stop instance to stop the EC2 instance.

Instances (1/2) Info								
Name		Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Actions
<input checked="" type="checkbox"/>	MyEC2Server1	i-01c19759dc52a899a	Running	t2.micro	2/2 checks passed	View alarms	us-east-1a	Stop instance Start instance Reboot instance Hibernate instance Terminate instance
<input type="checkbox"/>	MyEC2Server2	i-0a7b0ac6aa4f24acb	Running	t2.micro	2/2 checks passed	View alarms	us-east-1a	Public IPv4 ... Elastic IP 18.209.105.234 - 54.175.240.156 -

- Once MyEC2Server1 is stopped, navigate to Target Groups. Select the MyTargetGroup, Click on the Targets.

Successfully stopped i-01c19759dc52a899a								
Instances (1/2) Info								
<input type="checkbox"/> Find Instance by attribute or tag (case-sensitive)								
Name		Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
<input checked="" type="checkbox"/>	MyEC2Server1	i-01c19759dc52a899a	Stopped	t2.micro	-	View alarms	us-east-1a	-
<input type="checkbox"/>	MyEC2Server2	i-0a7b0ac6aa4f24acb	Running	t2.micro	2/2 checks passed	View alarms	us-east-1a	ec2-54-175-240-156.co... 54.175.240.156 -

- It will say that the stopped instance MyEC2Server1 is unused.

Registered targets (2) Info								
Anomaly mitigation: Not applicable C Deregister Register targets								
<input type="checkbox"/> Filter targets								
<input type="checkbox"/> Instance ID								
<input type="checkbox"/>	Instance ID	Name	Port	Zone	Health status	Health status details	Anomaly detection result	
<input type="checkbox"/>	i-01c19759dc52a899a	MyEC2Server1	80	us-east-1a	Unused	Target is in the stoppe...	Normal	
<input type="checkbox"/>	i-0a7b0ac6aa4f24acb	MyEC2Server2	80	us-east-1a	Healthy	-	Normal	

- Refresh the ELB domain name URL in Browser, and notice the HTML webpage remains visible. The ELB is only rendering the HTML page from the MyEC2Server2 instance.

Step 7: Delete AWS Resources

Deleting Load balancer

- In the EC2 console, navigate to Load Balancers in the left-side panel.

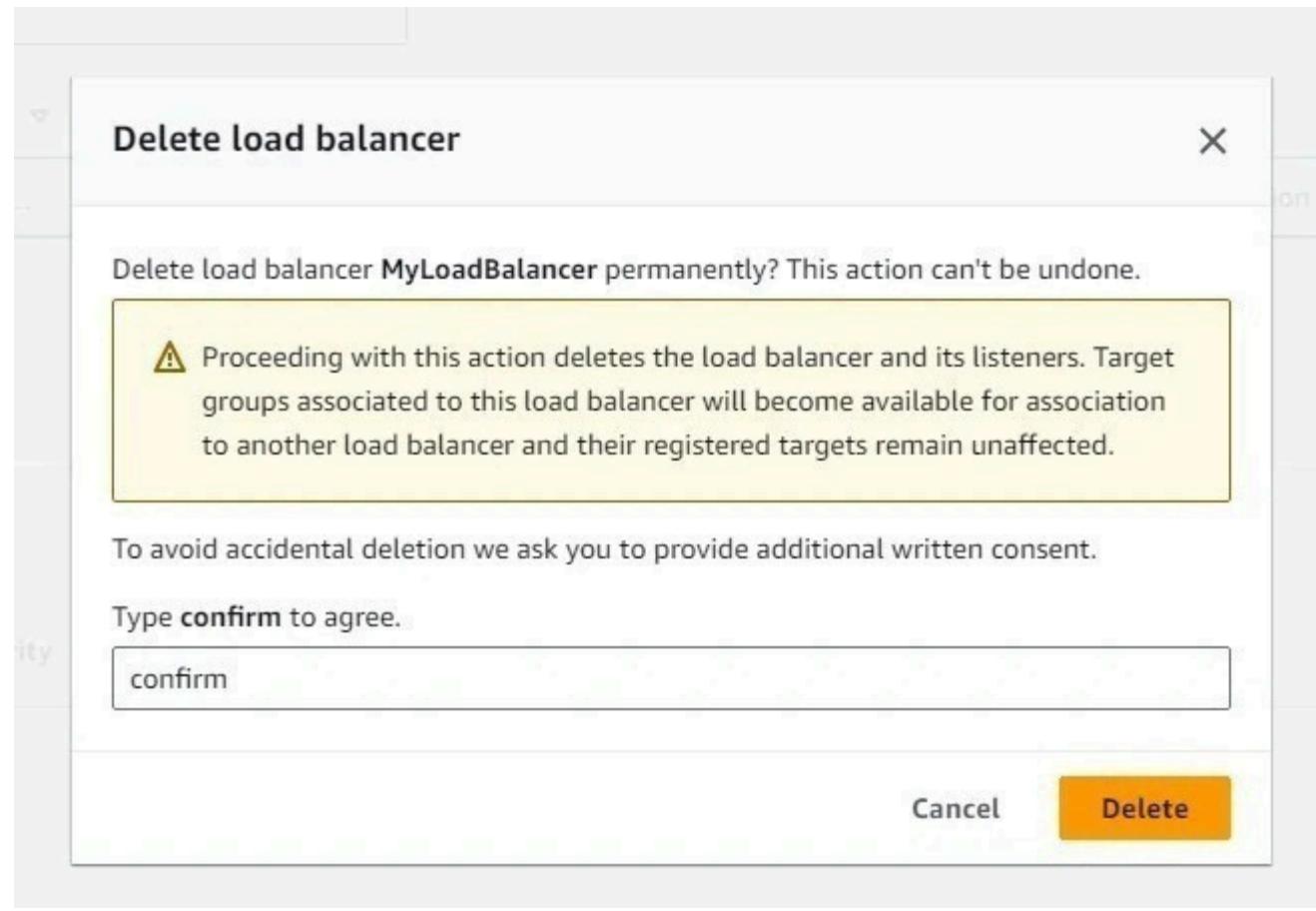
2. MyLoadBalancer will be listed here.

3. To delete the load balancer, you need to perform the following actions:

- Select the load balancer,
- Click on the Actions button,
- Select the Delete option.

The screenshot shows the AWS EC2 Load Balancers console. On the left, there's a navigation sidebar with various services like Spot Requests, Savings Plans, Reserved Instances, etc. The main area shows a table titled 'Load balancers (1/1)'. It lists one item: 'MyLoadBalancer' with a status of 'Active', VPC ID 'vpc-b5a7c3c8', and 6 Availability Zones. An 'Actions' dropdown menu is open over this row, with 'Delete load balancer' highlighted. Below this, a detailed view of 'MyLoadBalancer' is shown under 'Load balancer: MyLoadBalancer'. The 'Details' tab is selected, displaying information such as Load balancer type (Application), Status (Active), Scheme (Internet-facing), VPC (vpc-b5a7c3c8), IP address type (IPv4), and Availability Zones (subnet-7e851a4f, subnet-7b97c152, subnet-1b134744). The 'Date created' is January 18, 2024, 17:59 (UTC+01:00).

4. Confirm by typing confirm when a pop-up is shown. Click on Delete button.



5. Web-server-LG will be deleted immediately.

Deleting Target groups

1. In the EC2 console, navigate to Target groups in the left-side panel.
2. MyTargetGroup will be listed here.

3. To delete the target group, you need to perform the following actions:
 - Select the target group
 - Click on the Actions button,
 - Select the Delete option.

The screenshot shows the AWS EC2 Target groups page. On the left sidebar, under the 'EC2' section, there are links for Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, New, Images, AMIs, AMI Catalog, and Elastic Block Store. The main content area is titled 'Target groups (1/1) info'. It displays a table with one row for 'MyTargetGroup'. The columns include Name, ARN, Port, Protocol, Target type, Load balancer, and VPC ID. The 'Actions' menu for this target group includes options for Delete, Register targets, Edit health check settings, Edit target group attributes, and Manage tags. A 'Create target group' button is also visible.

4. Confirm by clicking on the Yes, delete button when a pop-up is shown.

The screenshot shows a modal dialog box titled 'Delete target group?'. It contains the message 'You can't undo this action.' followed by 'Deleting a target group deletes the group; the individual resources registered to the target group don't get deleted as a result of this action.' Below this, a question 'Are you sure you want to delete this target group?' is asked, with a radio button selected next to 'MyTargetGroup'. At the bottom of the dialog are two buttons: 'Cancel' and 'Yes, delete', with 'Yes, delete' highlighted in orange.

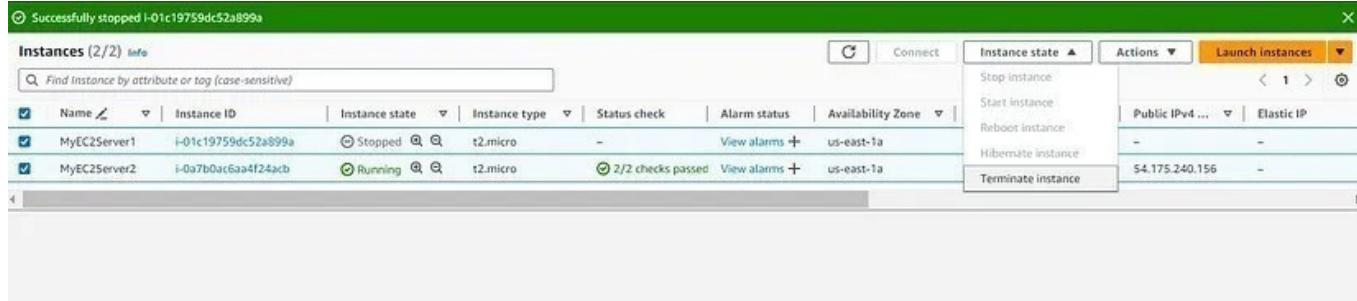
5. MyTargetGroup will be deleted immediately.

Deleting EC2 Instances

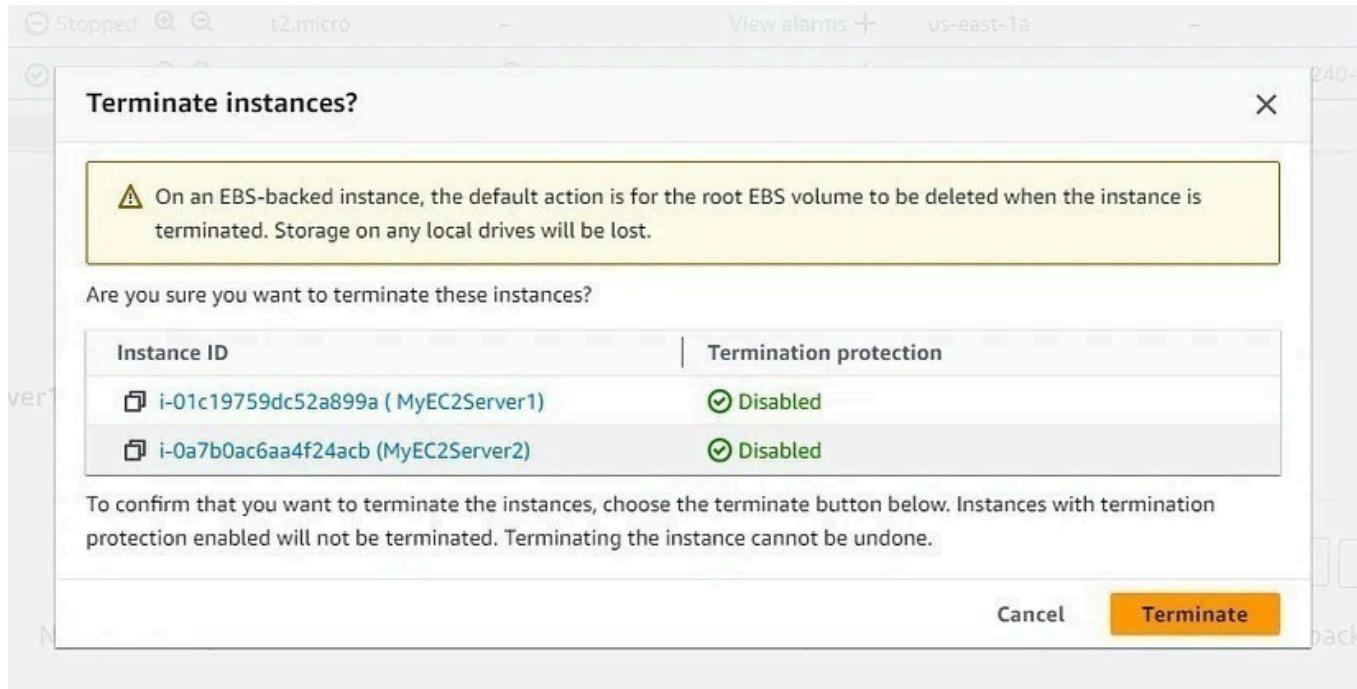
1. In the EC2 console, navigate to Instances in the left-side panel.
2. Two EC2 Instances MyEC2Server1 and MyEC2Server2 will be listed here.

3. To terminate the EC2 Instances, need to perform the following actions:
 - Select the EC2 instance

- Click on the Instance state button,
- Select the Terminate instance option



4. Confirm by clicking on the Terminate button when a pop-up is shown.



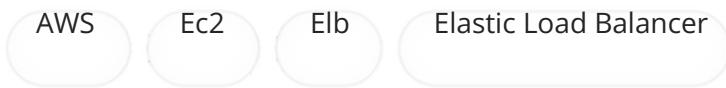
5. EC2 Instances will be terminated immediately.

Successfully terminated i-01c19759dc52a899a,i-0a7b0ac6aa4f24acb	Notifications	0	Δ 0	0	2	0	0	0	X
Instances (2/2) Info									
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 ...	Elastic IP
MyEC2Server1	i-01c19759dc52a899a	Terminated	t2.micro	-	View alarms	us-east-1a	-	-	-
MyEC2Server2	i-0a7b0ac6aa4f24acb	Terminated	t2.micro	-	View alarms	us-east-1a	-	-	-

You're all done! Congratulations!

That's all I have for today folks. Thank you for reading and/or following along! I hope this project was helpful and worth your while. Stay tuned for my next project on this journey into the cloud.

Let's connect on LinkedIn! <https://www.linkedin.com/in/meriemterki/>



Published in AWS Tip



7.7K Followers · Last published 2 days ago

Follow

Best AWS, DevOps, Serverless, and more from top Medium writers .

Written by Meriem Terki

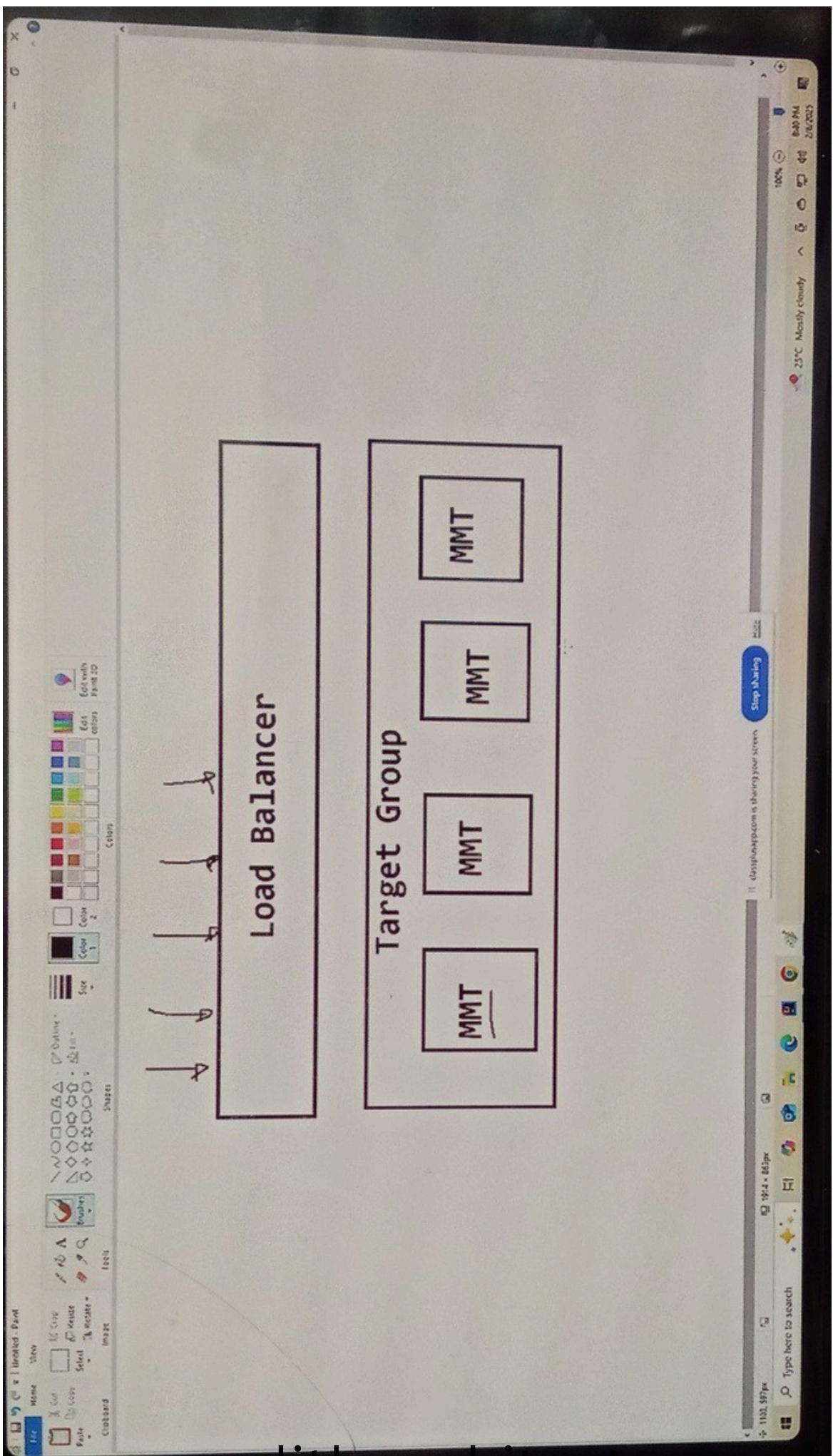


445 Followers · 1.1K Following

Follow

Data, Cloud & AI enthusiast | Follow me on my journey

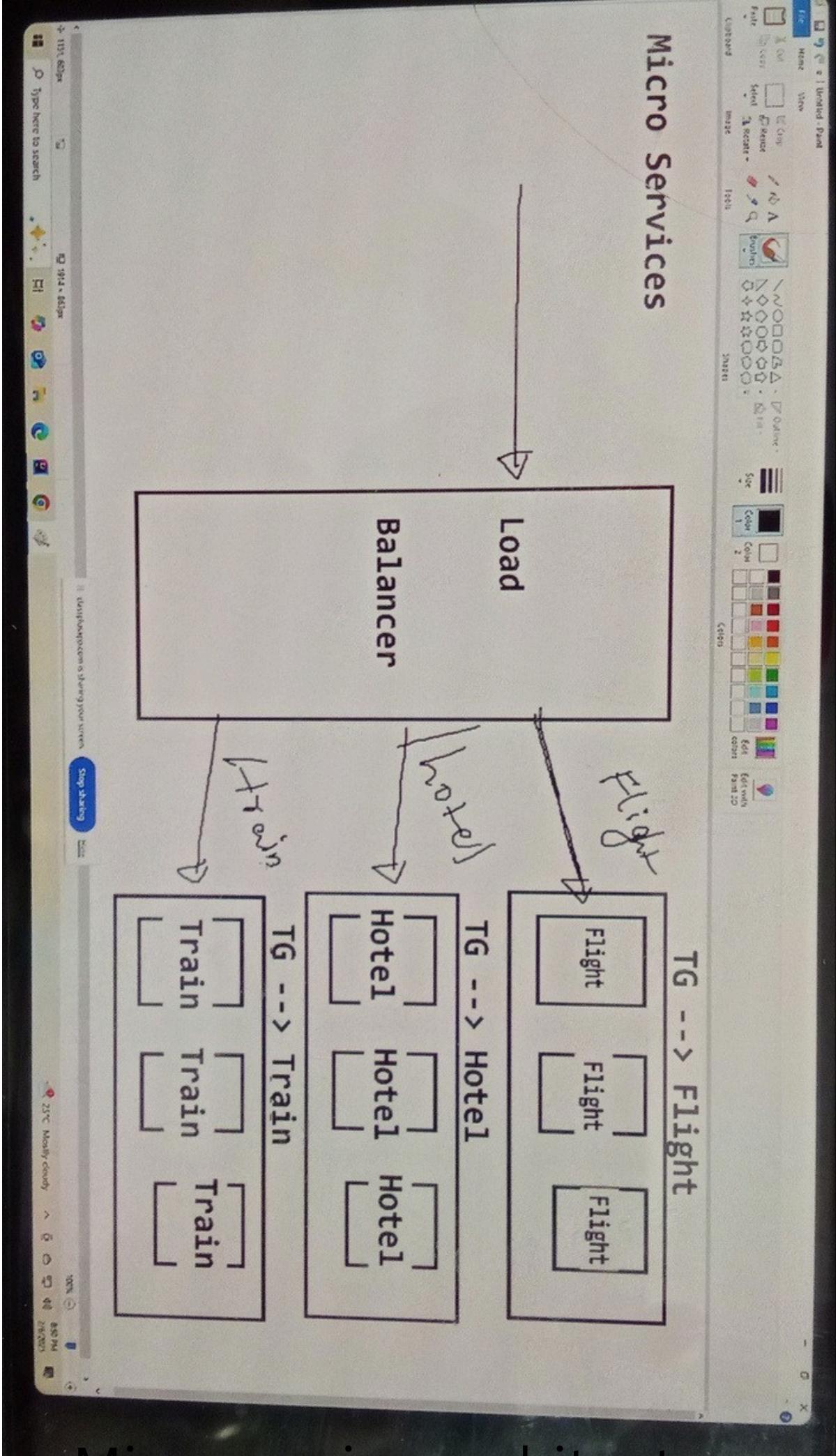
Monolith and Microservice in AWS



monolith architecture



AnyScanner



Microservice architecture

The screenshot shows the AWS EC2 'Launch an instance' wizard. In the 'Name and tags' step, a new instance is being named 'Flight_server_1'. The 'Software Image (AMI)' section is selected, showing the 'Amazon Linux 2023 AMI' (ami-0c50b6f7dc3701ddd) as the chosen AMI. Other AMI options like macOS, Ubuntu, Windows, Red Hat, SUSE Linux, and Debian are also listed. The 'Virtual server type (instance type)' is set to 't2.micro'. The 'Storage (volumes)' section indicates 1 volume(s) - 8 GiB. A summary box on the right shows 1 instance and provides a link to the 'Amazon Linux 2023 AMI' details. A tooltip for the 'Free tier' explains it includes 750 hours of t2.micro usage per month, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, and 2 million IOPS. The bottom of the screen shows the Windows taskbar with various pinned icons.

step 1: create Flight_server_2ec2 instance

Spring Initializer Live Session G monolithic vs microservices Monolithic App Problems Troubleshooting Manage AWS Resources Launch an instance (EC2) Download history

aws Search [Alt+S]

EC2 Instances Launch an instance

t2.micro

Family: t2 1 vCPU 1 GB Memory Current generation: true
On-Demand Linux base pricing: 0.0124 USD per Hour On-Demand Windows base pricing: 0.017 USD per Hour
On-Demand RHEL base pricing: 0.0268 USD per Hour
On-Demand Ubuntu Pro base pricing: 0.0142 USD per Hour
On-Demand SUSE base pricing: 0.0124 USD per Hour

Additional costs apply for AMIs with pre-installed software

Free tier eligible

All generations Compare instance types

▼ Summary

Number of instances Info 1

Software Image (AMI)
Amazon Linux 2023 AMI 2023.6.2...read more
ami-0c50b6f7dc3701ddd

Virtual server type (instance type)
t2.micro

Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 8 GiB

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

Cancel Launch instance Preview code

CloudShell Feedback

Type here to search

classplusapp.com is sharing your screen Stop sharing Help

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Breaking news

255 MiB 06:2025

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

Select Create new key pair

Q

Proceed without a key pair (Not recommended)

devops_session_1 Default value

Type: rsa

Subnet Info

No preference (Default subnet in any availability zone)

Auto-assign public IP Info

Enable

Additional charges apply when outside of free tier allowance

Firewall (security groups) Info

String Validator X Live Session X monolithic vs microservices X Monolithic App Problems X TripMoney Insurance X Manage AWS Resources X Launch an instance [EC2] X Download history X

aws X Search [Alt+S]

EC2 Instances Launch an instance

Network Info
vpc-01341020aca0d3c0d

Subnet Info
No preference (Default subnet in any availability zone)

Auto-assign public IP Info
Enable
Additional charges apply when outside of free tier allowance

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

Create security group Info Select existing security group Info

Common security groups Info
Select security groups ▾

Q

<input type="checkbox"/> security_group_1 VPC: vpc-01341020aca0d3c0d	sg-01cd7975a59a7c419
<input type="checkbox"/> default VPC: vpc-01341020aca0d3c0d	sg-079afe067df7c696b

Add new volume

Compare security group rules Advanced

Storage (volumes)
1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2 million

Cancel Launch instance Preview code

CloudShell Feedback

classplusapp.com is sharing your screen. Stop sharing Hide

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

8:56 PM 2/6/2025

This screenshot shows the 'Launch an instance' wizard in the AWS Management Console. The user is configuring a new instance with the following details:

- Network:** Using VPC `vpc-01341020aca0d3c0d`.
- Subnet:** No preference (Default subnet in any availability zone).
- Auto-assign public IP:** Enabled.
- Firewall (security groups):** A security group is being selected from existing ones.
- Storage:** 1 volume(s) - 8 GiB (EBS storage).
- Software Image (AMI):** Amazon Linux 2023.6.2...read more (`ami-0c50b6f7dc3701ddd`).
- Virtual server type (instance type):** t2.micro.
- Summary:** Number of instances: 1.

A tooltip for the 'Free tier' information is displayed, stating: "Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2 million".

The screenshot shows the AWS EC2 'Launch an instance' wizard. In the 'User data - optional' section, the following command is entered:

```
#!/bin/bash  
sudo yum install -y httpd  
sudo systemctl enable httpd  
sudo systemctl start httpd  
  
echo "<html><body><h1>Flight App 1</h1></body></html>" | sudo tee  
/var/www/html/index.html > /dev/null
```

A tooltip for the 'Free tier' is visible, stating: "Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2 million".

step 2 : add below command in User data

Spring Initializer Live Session Monolithic vs microservices Monolithic App Problems Tripmoney Insurance Manage AWS Resources Launch an instance EC2 Instances Launch an instance

aws Search [Alt+S] Asia Pacific (Mumbai) pirthvi

Success Successfully initiated launch of instance (i-098c7d370c9747cc8)

Launch log

Next Steps

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

1 2 3 4 5 6 >

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, retention, and deletion of EBS snapshots. Create EBS snapshot policy

Manage detailed monitoring Enable or disable detailed monitoring for the instance. Create Load Balancer Create a application, network

Create AWS budget Stop sharing Help you to create budgets. Create AWS budget

Manage CloudWatch alarms Create or update Amazon CloudWatch alarms for the instance. Manage CloudWatch alarms

CloudShell Feedback Type here to search Breaking news 8:56 PM 2/19/2025 © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

The screenshot shows the AWS EC2 'Launch an instance' success page. A green success message at the top states 'Successfully initiated launch of instance (i-098c7d370c9747cc8)'. Below this, a 'Next Steps' section lists several options: 'Create billing and free tier usage alerts', 'Connect to your instance', 'Connect an RDS database', 'Create EBS snapshot policy', 'Manage detailed monitoring', 'Create Load Balancer', 'Create AWS budget', and 'Manage CloudWatch alarms'. Each option has a brief description and a corresponding button or link. The browser's address bar shows the URL 'ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#LaunchInstances;'. The bottom of the screen shows the Windows taskbar with icons for File Explorer, Task View, Task Manager, and others.

The screenshot shows the AWS EC2 Instances page. On the left, there's a navigation sidebar with options like Dashboard, EC2 Global View, Events, Instances (with sub-options like Instances, Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations), Images (AMIs, AMI Catalog), Elastic Block Store (Volumes, Snapshots, Lifecycle Manager), and Network & Security. The main content area is titled "Instances (1) Info". It displays a table with one row for "Flight_server_1". The columns in the table are Name, Instance ID, Instance state, Instance type, Status check, Alarm status, and Availability Zone. The "Name" column has a dropdown menu open, showing "Flight_server_1" selected. The "Instance state" column shows "Running". The "Instance type" column shows "t2.micro". The "Status check" column shows "Initializing". The "Alarm status" column has a "View alarms" button. The "Availability Zone" column shows "ap-south-1b". At the bottom of the page, there's a "Select an instance" section and a footer with links for CloudShell, Feedback, Stop sharing, and a copyright notice for 2025.

Flight_Server_1 instance is created

Similarly create Filight_Server 2 instance is crated

The screenshot shows the AWS EC2 'Launch an instance' wizard. The instance name is set to 'flight_server_2'. The software image selected is 'Amazon Linux 2023 AMI 2023.6.2...'. The virtual server type is 't2.micro'. A summary panel on the right indicates 1 instance will be launched. A tooltip for the free tier is visible, stating: 'Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2 million'. The bottom right corner shows the status '8:56 PM 2/2/2025'.

It seems like you may be new to launching instances in EC2. Take a walkthrough to learn about EC2, how to launch instances and about best practices

Do not show me this message again [Take a walkthrough](#)

Launch an instance Info

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

Name and tags Info

Name
flight_server_2 [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 Linux Debian

SUSE awsplusapp.com is sharing your screen Stop sharing By

Browse more AMIs
Including AMIs from AWS, Marketplace and

Summary

Number of instances Info
1

Software Image (AMI)
Amazon Linux 2023 AMI 2023.6.2...read more
ami-0c50b6f7dc3701ddd

Virtual server type (instance type)
t2.micro

Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2 million

Cancel [Launch instance](#)

© 2025, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

Spring initializer Live Session monolithic vs microservice Monolithic App Problems Tripmoney Insurance Manage AWS Resources Launch an instance | EC2 Download history

aws Search [Alt+S] Asia Pacific (Mumbai) prithvi

EC2 Instances Launch an instance

t2.micro Family: t2 1 vCPU 1 GiB Memory Current generation: true Free tier eligible On-Demand Linux base pricing: 0.0124 USD per Hour On-Demand Windows base pricing: 0.017 USD per Hour On-Demand RHEL base pricing: 0.0268 USD per Hour On-Demand Ubuntu Pro base pricing: 0.0147 USD per Hour On-Demand SUSE base pricing: 0.0124 USD per Hour Additional costs apply for AMIs with pre-installed software

All generations Compare instance types

▼ 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 devops_session Create new key pair

▼ Network settings Info Network Info vpc-01341020aca0fd3c0d Subnet Info No preference (Default subnet in any availability zone)

Auto-assign public IP Info Enable Additional charges apply when outside of free tier allowance Firewall (security groups) Info

Summary Number of instances 1 Software Image (AMI) Amazon Linux 2023 AMI 2023.6.2...read more ami-0c50b6f7dc3701ddd Virtual server type (instance type) t2.micro Firewall (security group) New security group Storage (volumes) 1 volume(s) - 8 GiB

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

Cancel Launch instance Preview code

CloudShell Feedback classplusapp.com is sharing your screen Stop sharing Help © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences Breaking news 8:51 PM 21/02/2025

Spring Initializer Live Session monolithic vs microservices Monolithic App Problems Trifecta Insurance Manage AWS Resources Launch an instance | EC2 Download history

aws Search [Alt+S]

EC2 Instances Launch an instance

Network info
vpc-01341020acaf3c0d

Subnet info
No preference (Default subnet in any availability zone)

Auto-assign public IP info
Enable
Additional charges apply when outside of free tier allowance

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

Create security group Select existing security group

Common security groups info
Select security groups

security_group_1 sg-01cd7975a59a7c419 X
VPC: vpc-01341020acaf3c0d

Compare security group rules

▼ Summary Number of instances 1

Software Image (AMI)
Amazon Linux 2023 AMI 2023.6.2...read more
ami-0c50b6f7dc3701ddd

Virtual server type (instance type)
t2.micro

Firewall (security group)
security_group_1

Storage (volumes)
1 volume(s) - 8 GiB

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

Cancel Launch instance Preview code

CloudShell Feedback

Type here to search

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Breaking news 9:54 PM 2/1/2025

This screenshot shows the 'Launch an instance' wizard in the AWS Management Console. The user is configuring a new EC2 instance. In the 'Network' section, they've selected a VPC and subnet. Under 'Firewall (security groups)', they've chosen an existing security group named 'security_group_1'. In the 'Configure storage' section, they've selected a 8 GiB gp3 root volume. A tooltip about the free tier is displayed, stating: 'Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage'. The right side of the screen shows a summary of the instance configuration, including the AMI (Amazon Linux 2023), instance type (t2.micro), and storage (1 volume - 8 GiB). At the bottom, there are 'Launch instance' and 'Preview code' buttons.

Spring initializer Live Session monolithic vs microservice Monolithic App Problems Tripmoney Insurance Manage AWS Resources Launch an instance | EC2 Download history

ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#LaunchInstances:

AWS Search [Alt+S]

EC2 Instances Launch an instance

2

Allow tags in metadata Info Select

User data - optional Info Upload a file with your user data or enter it in the field.

Choose file

```
#!/bin/bash
sudo yum install -y httpd
sudo systemctl enable httpd
sudo systemctl start httpd

echo "<html><body><h1>Flight App 2</h1></body>" | sudo tee /var/www/html/index.html > /dev/null
```

User data has already been base64 encoded

Summary

Number of instances Info 1

Software Image (AMI) Amazon Linux 2023 AMI 2023.6.2...read more ami-0c50b6f7dc3701ddd

Virtual server type (instance type) t2.micro

Firewall (security group) security_group_1

Storage (volumes) 1 volume(s) - 8 GiB

ⓘ Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2 million

Cancel Launch instance Preview code

CloudShell Feedback

classplusapp.com is sharing your screen Stop sharing Hide

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Type here to search

857 PM 2/6/2025

The screenshot shows the AWS EC2 'Launch an instance' wizard. On the left, there's a large text area containing a bash script to install and start an Apache HTTPD server. On the right, the 'Summary' section details the launch configuration: one instance of the Amazon Linux 2023 AMI (ami-0c50b6f7dc3701ddd), a t2.micro instance type, and a security group named 'security_group_1'. It also specifies 1 volume(s) with 8 GiB of storage. A tooltip for the 'Free tier' indicates usage limits for the first year. At the bottom right are 'Cancel', 'Launch instance' (in red), and 'Preview code' buttons.

The screenshot shows the AWS CloudWatch Logs interface with the URL <https://ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#LaunchInstances>. The page displays a green success message: "Successfully initiated launch of instance (i-0b3c42de7bab50f4b)". Below the message, there is a link to "Launch log".

Next Steps

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

< 1 2 3 4 5 6 >

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, retention, and deletion of EBS snapshots. Create EBS snapshot policy
Manage detailed monitoring Enable or disable detailed monitoring for the instance. CloudShell Feedback	Create Load Balancer Create a application, network, or API load balancer. Stop sharing	Create AWS budget AWS Budgets allows you to create budgets. Create budget	Manage CloudWatch alarms Create or update Amazon CloudWatch alarms for metrics. Create alarm

The screenshot shows the AWS EC2 Instances page. The left sidebar is collapsed. The main area displays a table of instances:

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
Flight_server_1	i-098c7d370c9747cc8	Running	t2.micro	Initializing	View alarms +	ap-south-1b
flight_server_2	i-0b3c42de7bab50f4b	Running	t2.micro	Initializing	View alarms +	ap-south-1b

Below the table, a message says "Select an instance". The browser's address bar shows the URL: ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#instances.

Now see Flight_server1 and Flight_server2 is created

Now see Similarly do Hotel_server1 and Hotel_server2 is created

The screenshot shows the AWS EC2 Instances page. A red circle highlights the list of instances in the main table. The table contains the following data:

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
Hotel_server_2	i-02f79b2f28eb7adec	Running	t2.micro	ap-south-1b
Hotel_server_1	i-0c4dda20fb2ea7ea7	Running	t2.micro	Initializing	...	ap-south-1b
Flight_server_1	i-098c7d370c9747cc8	Running	t2.micro	2/2 checks passed	...	ap-south-1b
Flight_server_2	i-0b3c42de7bab50f4b	Running	t2.micro	Initializing	...	ap-south-1b

Below the table, the details for the selected instance (Flight_server_2) are displayed:

i-0b3c42de7bab50f4b (Flight_server_2)

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

Instance summary

Instance ID	i-0b3c42de7bab50f4b	Public IPv4 address	13.203.76.194 open address
IPv6 address	-	Instance state	Running
		Private IPv4 addresses	172.31.2.229
		Public IPv4 DNS	ec2-13-203-76-194.ap-south-1.compute.amazonaws.com open address

Now see above 4 instance is created

Create Target group of flight

The screenshot shows the AWS Management Console interface for the EC2 service. On the left, a sidebar menu includes sections for Images, Elastic Block Store, Network & Security, Load Balancing, Auto Scaling, and Settings. The Load Balancing section is expanded, showing sub-options: Load Balancers, Target Groups (which is highlighted with a blue oval and a red callout), and Trust Stores. In the main content area, the 'Instances (4) Info' table lists four instances: Hotel_server_2, Hotel_server_1, Flight_server_1, and Flight_server_2, all in the 'Running' state. Below the table, a message says 'Select an instance' and 'Click on Target Groups'. The browser's address bar shows the URL: <https://ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#targetGroups>.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
Hotel_server_2	i-02f79b2f28eb7adec	Running	t2.micro	Initializing	View alarms +	ap-south-1b
Hotel_server_1	i-0c4dda20fb2ea7ea7	Running	t2.micro	Initializing	View alarms +	ap-south-1b
Flight_server_1	i-098c7d370c9747cc8	Running	t2.micro	2/2 checks passed	View alarms +	ap-south-1b
Flight_server_2	i-0b3c42de7bab50f4b	Running	t2.micro	Initializing	View alarms +	ap-south-1b

A screenshot of the AWS Management Console showing the EC2 Target groups page. The URL in the address bar is `ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#TargetGroups`. The left sidebar shows navigation options like Images, Elastic Block Store, Network & Security, Load Balancing, Auto Scaling, and Settings. The main content area is titled "Target groups" and displays a table with columns: Name, ARN, Port, Protocol, Target type, Load balancer, and VPC ID. A search bar at the top of the table says "Filter target groups". Below the table, a message says "No target groups" and "You don't have any target groups in ap-south-1". An orange "Create target group" button is located in the top right corner of the table area. A blue circle highlights this button, and a red arrow points from it to the text "Click on Create Target Group" located below the table. The status bar at the bottom indicates "daisplusapp.com is sharing your screen" and shows system information like battery level, signal strength, and date.

= Click on Create Target Group

The screenshot shows the 'Specify group details' step of creating a target group in the AWS EC2 console. The 'Instances' target type is selected and highlighted with a blue circle. The 'Basic configuration' section states: 'Your load balancer routes requests to the targets in a target group and performs health checks on the targets.' Below this, the 'Choose a target type' section lists four options:

- Instances** (selected):
 - Supports load balancing to Instances within a specific VPC.
 - Facilitates the use of Amazon EC2 Auto Scaling to manage and scale your EC2 capacity.
- IP addresses**:
 - Supports load balancing to VPC and on-premises resources.
 - Facilitates routing to multiple IP addresses and network interfaces on the same instance.
 - Offers flexibility with microservice based architectures, simplifying inter-application communication.
 - Supports IPv6 targets, enabling end-to-end IPv6 communication, and IPv4-to-IPv6 NAT.
- Lambda function**:
 - Facilitates routing to a single Lambda function.
 - Accessible to Application Load Balancers only.
- Application Load Balancer**:
 - Offers the flexibility for a Network Load Balancer to accept and route TCP requests within a specific VPC.
 - Facilitates using static IP addresses.

At the bottom of the screen, there are browser navigation icons and a status bar showing 'CloudShell Feedback' and 'Earnings Upcoming'.

choose instances

Give target group name

Target group name
flight

A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

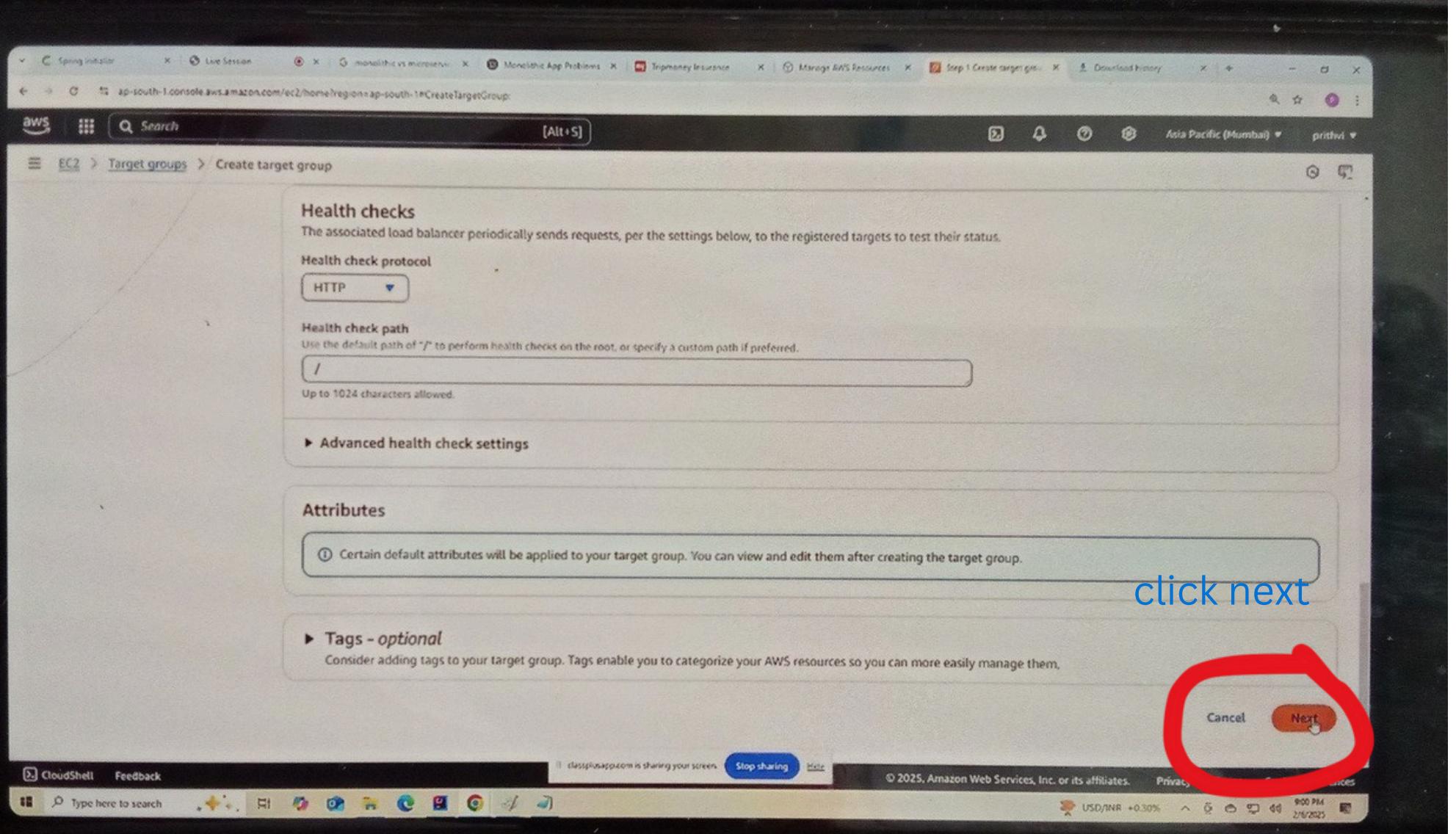
Protocol : Port
Choose a protocol for your target group that corresponds to the Load Balancer type that will route traffic to it. Some protocols now include anomaly detection for the targets and you can set mitigation options once your target group is created. This choice cannot be changed after creation.

HTTP 80 1-65535

IP address type
Only targets with the indicated IP address type can be registered to this target group.

IPv4
Each instance has a default network interface (eth0) that is assigned the primary private IPv4 address. The instance's primary private IPv4 address is the one that will be applied to the target.

IPv6
Each instance you register must have an assigned public IPv6 address. This must be a static IPv6 address assigned to the instance's default network interface.



create separate group of flight

The screenshot shows the AWS EC2 console with the URL ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1>CreateTargetGroup. The page is titled "Create target group" and is on "Step 2: Register targets".

Available instances (2/4)

Instance ID	Name	State	Security groups	Zone
i-02f79b2f28eb7adec	Hotel_server_2	Running	security_group_1	ap-south-1b
i-0c4dda20fb2ea7ea7	Hotel_server_1	Running	security_group_1	ap-south-1b
<input checked="" type="checkbox"/> i-0b3c42de7bab50f4b	Flight_server_2	Running	security_group_1	ap-south-1b
<input checked="" type="checkbox"/> i-098c7d370c9747cc8	Flight_server_1	Running	security_group_1	ap-south-1b

2 selected

Ports for the selected instances
Ports for routing traffic to the selected instances.
80
1-65535 (separate multiple ports with commas)

[Include as pending below](#)

CloudShell Feedback Type here to search Stop sharing 800 PM 2/6/2025 © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

click include page as pending below

EC2 > Target groups > Create target group

Instance ID	Name	State	Security groups	Region
i-0b3c42de7bab50f4b	Flight_server_2	Running	security_group_1	ap-south-1b
i-098c7d370c9747cc8	Flight_server_1	Running	security_group_1	ap-south-1b

2 selected

Ports for the selected instances
Ports for routing traffic to the selected instances.

80

1-65535 (separate multiple ports with commas)

Include as pending below

Review targets

Targets (0)

No instances added yet

Specify instances above, or leave the group empty if you prefer to add targets later.

CloudShell Feedback

Stop sharing

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

USD/INR +0.30% 9:00 PM 2/6/2025

now see your target group is flight 1 and flight 2

click create target group

The screenshot shows the 'Create target group' step in the AWS EC2 wizard. At the top, it says '0 selected'. Below that is a section for 'Ports for the selected instances' with a dropdown set to '80' and a note about comma-separated ports. A button 'Include as pending below' is present. A message at the bottom indicates '2 selections are now pending below. Include more or register targets when ready.' The 'Review targets' section shows a table with two entries:

Targets (2)						
Instance ID	Name	Port	State	Security groups	Zone	Private IPv4 address
i-0b3c42de7bab50f4b	Flight_server_2	80	<input checked="" type="radio"/> Running	security_group_1	ap-south-1b	172.31.2.229
i-098c7d370c9747cc8	Flight_server_1	80	<input checked="" type="radio"/> Running	security_group_1	ap-south-1b	172.31.14.152

At the bottom right of the review section are buttons for 'Cancel', 'Previous', and a large orange 'Create target group' button.

The screenshot shows the AWS CloudWatch Metrics interface. At the top, there are tabs for 'Metrics' and 'Logs'. Below the tabs, there's a search bar and a 'Metrics Insights' button. The main content area displays a table of metrics. The first row has columns for 'Metric Name', 'Dimensions', 'Unit', and 'Value'. The second row contains the values: 'AWS/CloudWatchMetrics/MetricName', 'awsRegion=ap-south-1', 'Count', and '1'. There are also 'Next' and 'Last' buttons at the bottom of the table.

Now click on register target

Spring Initializer Live Session monolithic vs microservices Monolithic App Problems TripMoneyInsurance Manage AWS Resources Register targets | EC2 | Register targets | Download history

aws Search [Alt+S] Asia Pacific (Mumbai) prithvi

EC2 > Target groups > flight > Register targets

Register targets

Select instances, specify ports, and add the instances to the list of pending targets. Repeat to add additional combinations of instances and ports to the list of pending targets. Once you are satisfied with your selections, click Register pending targets.

Available instances (4)

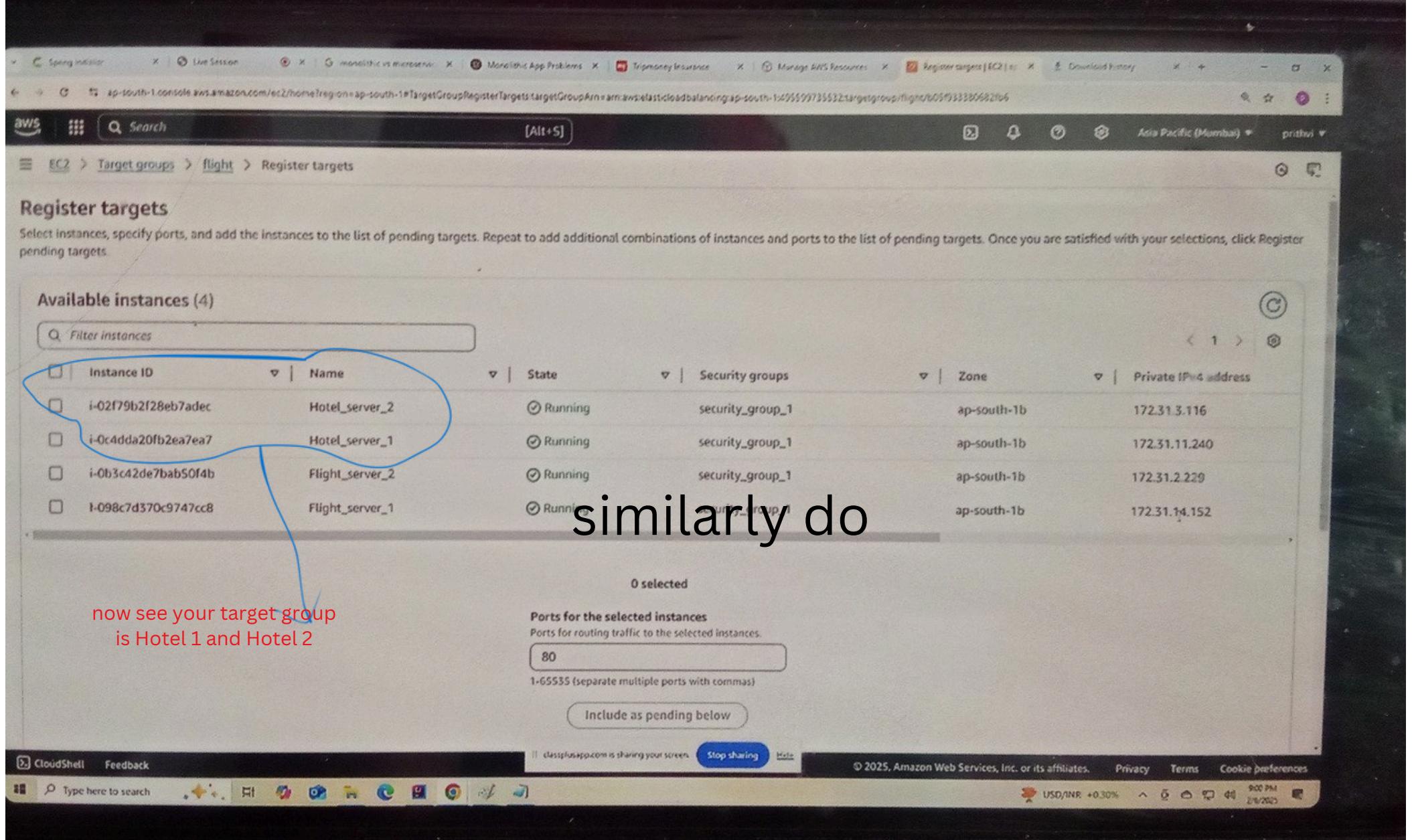
Instance ID	Name	State	Security groups	Zone	Private IPv4 address
i-02f79b2f28eb7adec	Hotel_server_2	Running	security_group_1	ap-south-1b	172.31.3.116
i-0c4dda20fb2ea7ea7	Hotel_server_1	Running	security_group_1	ap-south-1b	172.31.11.240
i-0b3c42de7bab50f4b	Flight_server_2	Running	security_group_1	ap-south-1b	172.31.2.229
i-098c7d370c9747cc8	Flight_server_1	Running	security_group_1	ap-south-1b	172.31.14.152

similarly do

now see your target group is Hotel 1 and Hotel 2

Ports for the selected instances
Ports for routing traffic to the selected instances.
80
1-65535 (separate multiple ports with commas)
Include as pending below

CloudShell Feedback classplusapp.com is sharing your screen Stop sharing Note © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences USD/INR +0.30% 8:00 PM 12/12/2025



The screenshot shows the AWS EC2 Target groups page. On the left, there's a navigation sidebar with sections like Images, Elastic Block Store, Network & Security, Load Balancing, and Auto Scaling. The main area is titled "Target groups (2) Info" and contains a table with two rows:

Name	ARN	Port	Protocol	Target type	Load balancer	VPC ID
hotels	arn:aws:elasticloadbalancing:... arn:aws:elasticloadbalancin...	80	HTTP	Instance	None associated	vpc-01341c
flight	arn:aws:elasticloadbalancin...	80	HTTP	Instance	None associated	vpc-01341c

Below the table, a message says "0 target groups selected" and "Select a target group above."

At the bottom of the page, there are links for CloudShell, Feedback, and a search bar. The status bar at the bottom right shows "classplusapp.com is sharing your screen", "Stop sharing", "USD/NRA +0.30%", "9:01 PM", "4G", and "2/8/2020".

now see 2 target group is created

The screenshot shows the AWS EC2 Load Balancers console. On the left, a sidebar menu is open under the 'Load Balancing' section, with 'Load Balancers' selected. A blue oval highlights this selection. A blue arrow points from the text 'click on load Balancers' to the 'Load Balancers' link in the sidebar. Another blue arrow points from the text 'create load Balancers' to the 'Create load balancer' button at the top right of the main content area. The main content area displays a table header for 'Load balancers' with columns: Name, DNS name, State, VPC ID, Availability Zones, Type, and Date created. Below the table, it says 'No load balancers' and 'You don't have any load balancers in ap-south-1'. A large 'Create load balancer' button is centered below this message.

Spring Initializer Live Session monolithic vs microservices Monolithic App Problems Tripmoney Insurance Manage AWS Resources Compare and select load balancer Download history

aws Search [Alt+S] Asia Pacific (Mumbai) prithvi

EC2 > Load balancers > Compare and select load balancer type

ALB

Choose an Application Load Balancer when you need a flexible feature set for your applications with HTTP and HTTPS traffic. Operating at the request level, Application Load Balancers provide advanced routing and visibility features targeted at application architectures, including microservices and containers.

NLB

Choose a Network Load Balancer when you need ultra-high performance, TLS offloading at scale, centralized certificate deployment, support for UDP, and static IP addresses for your applications. Operating at the connection level, Network Load Balancers are capable of handling millions of requests per second securely while maintaining ultra-low latencies.

GWLB

Choose a Gateway Load Balancer when you need to deploy and manage a fleet of third-party virtual appliances that support GENEVE. These appliances enable you to improve security, compliance, and policy controls.

Create

▶ Classic Load Balancer - previous generation

click on create

CloudShell Feedback

classplusapp.com is sharing your screen Stop sharing Help

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

USD/INR +0.30% 9:02 PM 2/6/2025

Spring Initializer Live Session monolithic vs microservice Monolithic App Problems TripMoney Insurance Manage AWS Resources Create application load balancer Download history

aws Search [Alt+S] EC2 > Load balancers > Create Application Load Balancer

▶ How Application Load Balancers work

Basic configuration

Load balancer name
Name must be unique within your AWS account and can't be changed after the load balancer is created.
 A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

Scheme Info
Scheme can't be changed after the load balancer is created.

Internet-facing
• Serves internet-facing traffic.
• Has public IP addresses.
• DNS name is publicly resolvable.
• Requires a public subnet.

Internal
• Serves internal traffic.
• Has private IP addresses.
• DNS name is publicly resolvable.
• Compatible with the IPv4 and Dualstack IP address types.

Load balancer IP address type Info
Select the front-end IP address type to assign to the load balancer. The VPC and subnets mapped to this load balancer must include the selected IP address types. Public IPv4 addresses have an additional cost.

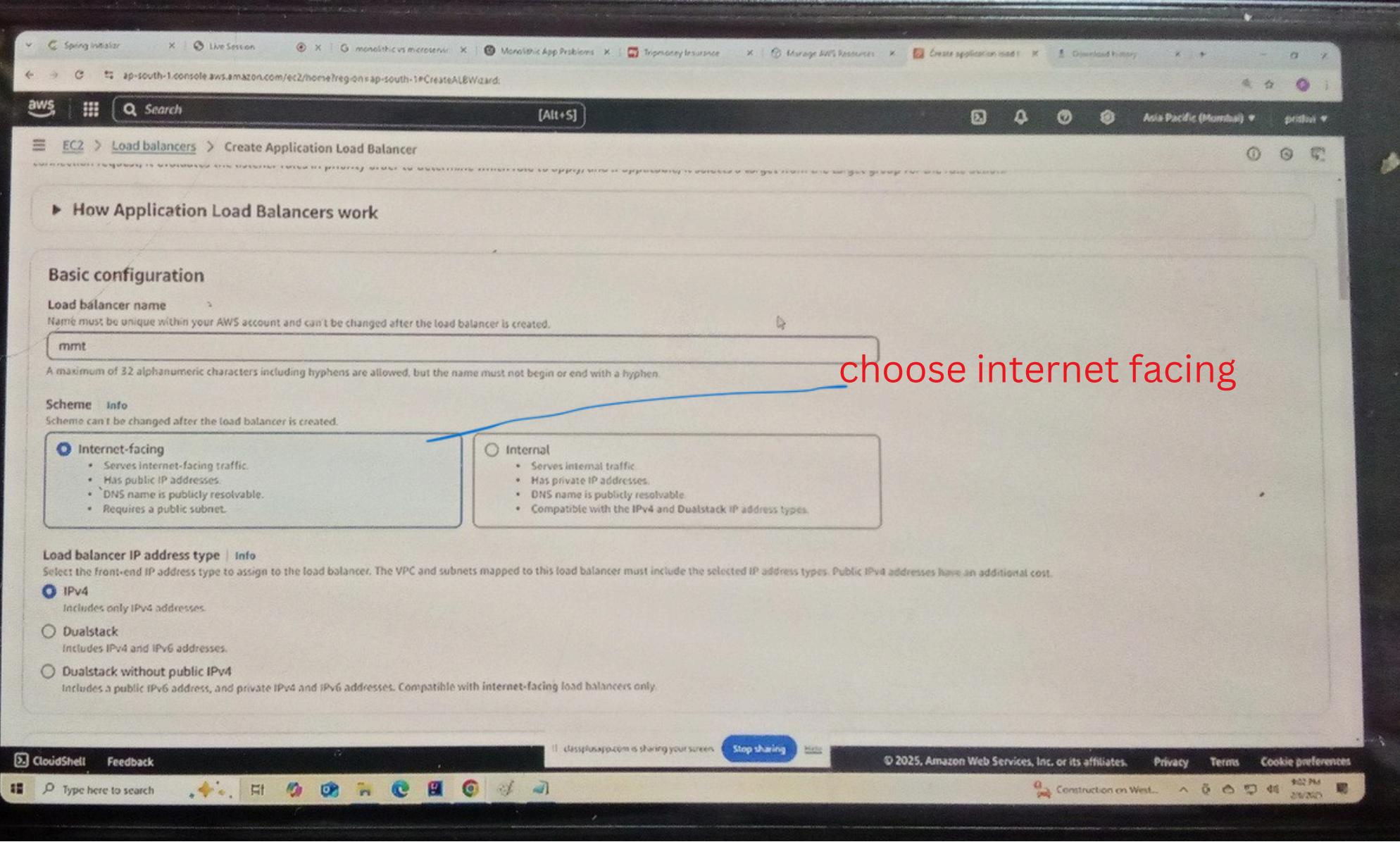
IPv4
Includes only IPv4 addresses.

Dualstack
Includes IPv4 and IPv6 addresses.

Dualstack without public IPv4
Includes a public IPv6 address, and private IPv4 and IPv6 addresses. Compatible with internet-facing load balancers only.

CloudShell Feedback Type here to search Stop sharing Help © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences Construction on West... 9:02 PM 20/2/2025

choose internet facing



Spring initial Live Session monolithic vs microserv... Monolithic App Problems TripMoney Insurance Manage AWS Resources Create application load l... Download history

aws Search [Alt+S]

EC2 > Load balancers > Create Application Load Balancer

Network mapping Info

The load balancer routes traffic to targets in the selected subnets, and in accordance with your IP address settings.

VPC Info

The load balancer will exist and scale within the selected VPC. The selected VPC is also where the load balancer targets must be hosted unless routing to Lambda or on-premises targets, or if using VPC peering. To confirm the VPC for your targets, view target groups. For a new VPC, create a VPC.

vpc-01341020acaf3c0d IPv4 VPC CIDR: 172.31.0.0/16

Mappings Info

Select at least two Availability Zones and one subnet per zone. The load balancer routes traffic to targets in these Availability Zones only. Availability Zones that are not supported by the load balancer or the VPC are not available for selection.

Availability Zones

ap-south-1a (aps1-az1)

Subnet

subnet-0e1dd98dfe26019d6 IPv4 subnet CIDR: 172.31.32.0/20

IPv4 address Assigned by AWS

ap-south-1b (aps1-az3)

Subnet

subnet-0b73d56438dfc3c31 IPv4 subnet CIDR: 172.31.0.0/20

IPv4 address Assigned by AWS

ap-south-1c (aps1-az2)

Subnet

CloudShell Feedback

Stop sharing

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Construction on West...

Type here to search

AnyScanner

A red annotation with a blue outline and a red arrow points from the text "select all availability zone" to the checkbox for "ap-south-1a (aps1-az1)".

Spring Initializer Live Session monolithic vs microservice Monolithic App Problems TripMoney Insurance Manage AWS Resources Create application load b... Download history

aws Search [Alt+S] Asia Pacific (Mumbai) prithvi

EC2 > Load balancers > Create Application Load Balancer

subnet-010cdc50c1178faa9
IPv4 subnet CIDR: 172.31.16.0/20

IPv4 address
Assigned by AWS

Security groups Info
A security group is a set of firewall rules that control the traffic to your load balancer. Select an existing security group, or you can create a new security group.

Security groups

Select up to 5 security groups

security_group_1
sg-01cd7975a59a7c419 VPC: vpc-01341020acaf3c0d

default
sg-079afe067df7c696b VPC: vpc-01341020acaf3c0d

Listeners and routing Info
A listener is a process that checks for connection requests using the port and protocol you configure. The rules that you define for a listener determine how the load balancer routes requests to its registered targets.

▼ Listener HTTP:80

Protocol: HTTP Port: 80

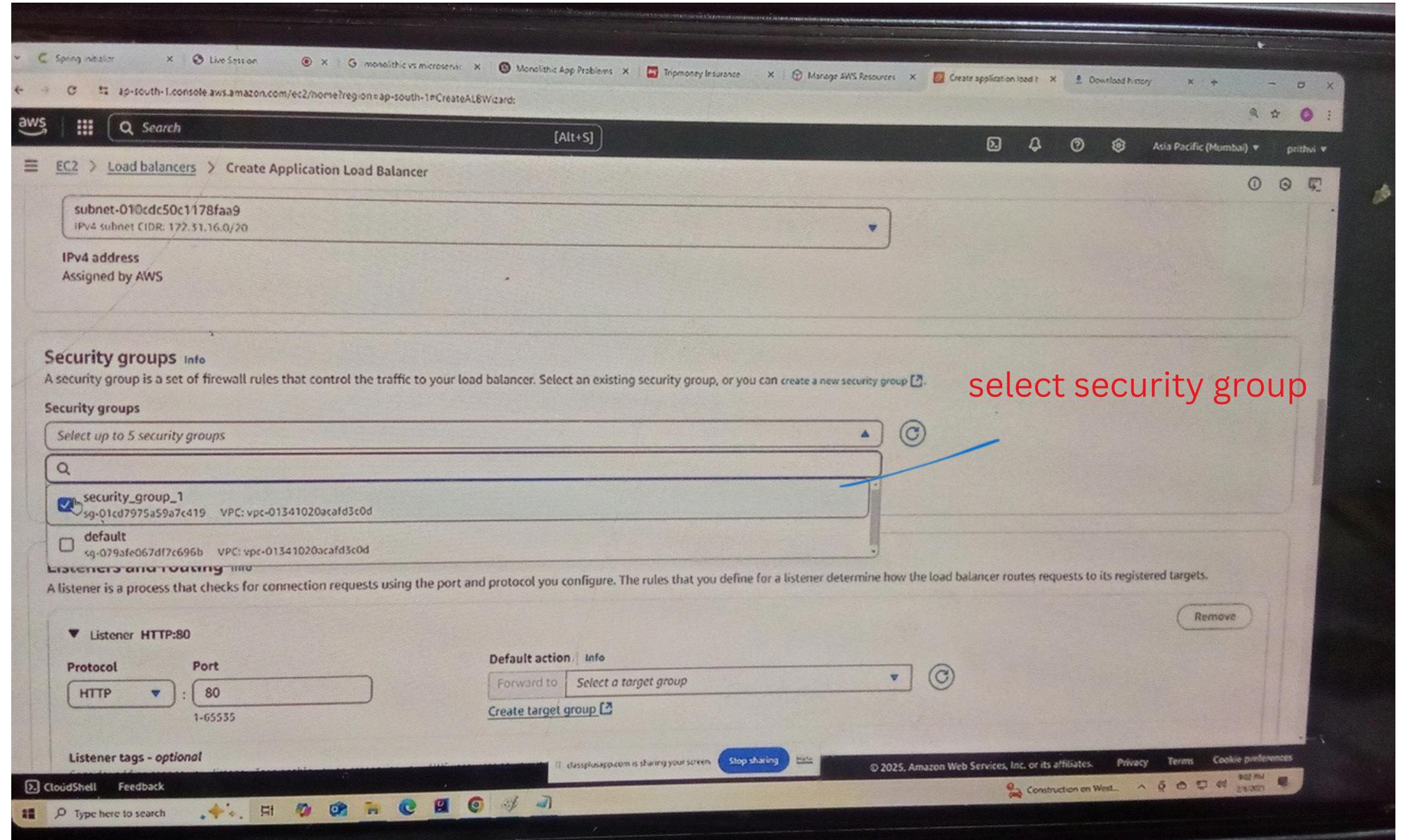
Default action: Info
Forward to: Select a target group
Create target group

Listener tags - optional

CloudShell Feedback Type here to search

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

A red annotation with the text "select security group" and a blue arrow points to the "security_group_1" entry in the dropdown menu.



Spring Metrics X Live Metrics X Monitoring in CloudWatch X Monolithic App Problems X Troubleshooting X Manage AWS Resources X Create application load balancer X Download history X

aws Search [All+S] Notifications Help Feedback Asia Pacific (Mumbai) prithvi

EC2 > Load balancers > Create Application Load Balancer

Listeners and routing Info

A listener is a process that checks for connection requests using the port and protocol you configure. The rules that you define for a listener determine how the load balancer routes requests to its registered targets.

Listener: HTTP:80

Protocol: **HTTP** Port: **80** Remove

Default action: **Select a target group** Info

Create target Q

flight Target type: instance, IPv4 **HTTP**

hotels Target type: instance, IPv4 **HTTP**

Listener tags - optional

Consider adding tags to your listener. Tags enable you to categorize your AWS resources so you can more easily manage them. You can add up to 50 tags.

Add listener tag Add listener tag

Add listener Add listener

Load balancer tags - optional

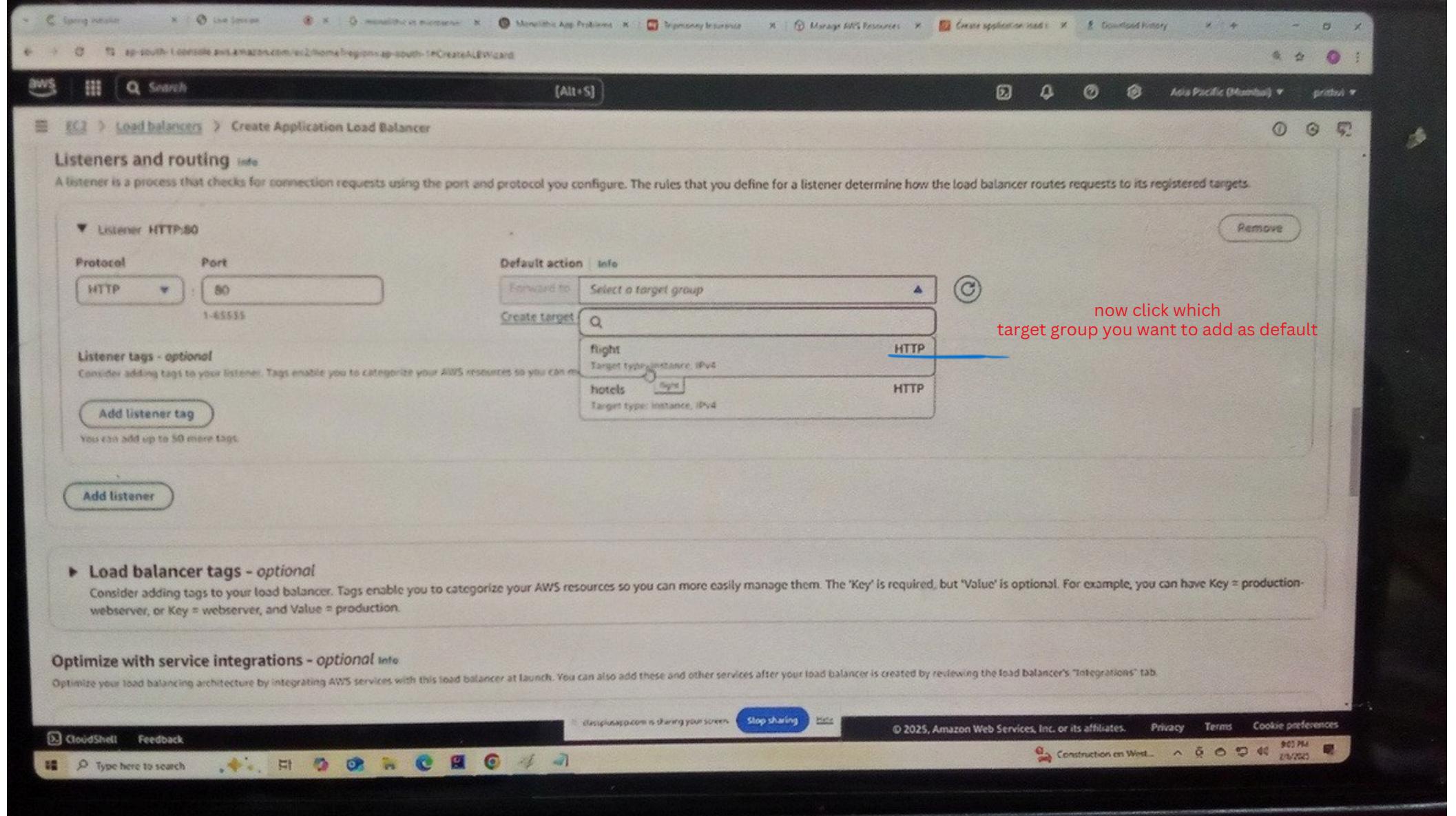
Consider adding tags to your load balancer. Tags enable you to categorize your AWS resources so you can more easily manage them. The 'Key' is required, but 'Value' is optional. For example, you can have Key = production-webserver, or Key = webserver, and Value = production.

Optimize with service integrations - optional Info

Optimize your load balancing architecture by integrating AWS services with this load balancer at launch. You can also add these and other services after your load balancer is created by reviewing the load balancer's "Integrations" tab.

CloudShell Feedback classplusapp.com is sharing your screen Stop sharing Help © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences Construction on... 9:05 PM 2/6/2025

now click which target group you want to add as default



Spring Initializer X Live Session G monolithic vs microservices Monolithic App Problems Tripmoney Insurance Manage AWS Resources Create application load balancer Download history

ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#CreateALBWizard:

Search [Alt+S]

EC2 > Load balancers > Create Application Load Balancer

Internet-facing IPv4 sg-01cd7975a59a7c419

ap-south-1a subnet-0e1dd98dfe26019d6 flight

ap-south-1b subnet-0b73d56438dfc3c31

ap-south-1c subnet-010dc50c1178faa9

Service integrations Edit

Amazon CloudFront + AWS Web Application Firewall (WAF): None

AWS WAF: None

AWS Global Accelerator: None

Tags Edit

None

create load balancer

Attributes

① Certain default attributes will be applied to your load balancer. You can view and edit them after creating the load balancer.

Creation workflow and status

► Server-side tasks and status

After completing and submitting the above steps, all server-side tasks and their statuses become available for monitoring.

Cancel Create load balancer

CloudShell Feedback classplusapp.com is sharing your screen Stop sharing © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences Construction on West... 8:03 PM 6/6/2025

Screenshot of the AWS Management Console showing the configuration of an Internet-facing Load Balancer named "mmt".

The Load Balancer ARN is: arn:aws:elasticloadbalancing:ap-south-1:495599735532:loadbalancer/app/mmt/c25dcfe0d806197

The DNS name is: mmt-1460234105.ap-south-1.elb.amazonaws.com (A Record)

The Listener configuration shows one rule for port 80:

- Protocol: Port: HTTP:80
- Default action:
 - Forward to target group
 - Weight: 1 (100%)
 - Target group stickiness: Off

A blue circle highlights the "Forward to target group" section.

Other tabs visible include: Network mapping, Resource map - new, Security, Monitoring, Integrations, Attributes, Capacity - new.

Bottom status bar: dasplusapp.com is sharing your screen, Stop sharing, 25°C Partly cloudy, 9:03 PM, 2/6/2025.

The screenshot shows the AWS EC2 Load Balancers console. On the left, a sidebar lists various services: Images, AMIs, AMI Catalog, Elastic Block Store (Volumes, Snapshots, Lifecycle Manager), Network & Security (Security Groups, Elastic IPs, Placement Groups, Key Pairs, Network Interfaces), Load Balancing (Load Balancers, Target Groups, Trust Stores), Auto Scaling (Auto Scaling Groups), and Settings. The main pane displays a load balancer named 'mmt' (ARN: am.aws.elasticloadbalancing.ap-south-1:495599735532:loadbalancer/app/mmt/c25ddcf0d806197). It shows three subnets: subnet-010cd50c1178faa9 (ap-south-1c), subnet-0e1dd98dfe26019d6 (ap-south-1a), and subnet-0b73d56438dfc3c31 (ap-south-1b). The DNS name is mmt-1460234105.ap-south-1.elb.amazonaws.com (A Record). The 'Listeners and rules' tab is active, showing one rule for port 80. This rule forwards traffic to a target group named 'flight' (1 rule) with 100% weight and target group stickiness off. A context menu is open over this rule, with 'Add rule' highlighted.

select default Flight and
after that select add rule

The screenshot shows the AWS Lambda Step Functions console. A state machine named 'HelloWorld' is displayed with two states: 'Hello World' and 'Lambda Function'. The 'Hello World' state has a 'Next' transition to the 'Lambda Function' state. The 'Lambda Function' state has a 'Next' transition back to the 'Hello World' state. The 'Hello World' state also has a 'Cancel' transition.

Step 1
Add rule

Step 2
Define rule conditions

Step 3
Define rule actions

Step 4
Set rule priority

Step 5
Review and create

Add rule Info

Define the rule and then review it in the context of the other rules on this listener.

▶ Listener details: HTTP:80

Name and tags Info

Tags can help you manage, identify, organize, search for and filter resources.

Name Add additional tags

Cancel Next

CloudShell Feedback

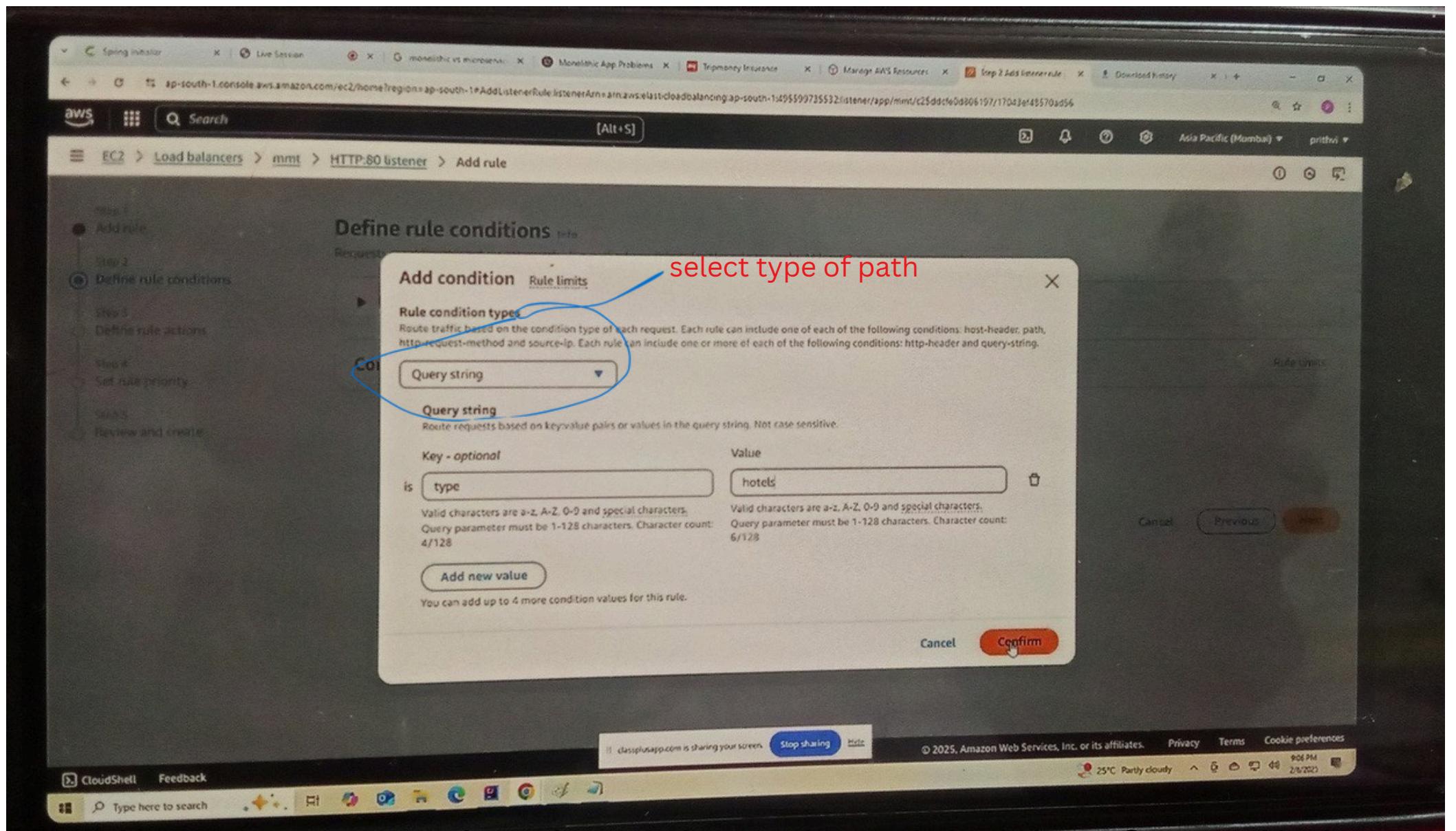
classplusapp.com is sharing your screen Stop sharing Help

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

25°C Partly cloudy 8:55 PM 2/6/2025

Type here to search

now give name and click next



key -type and value - hotels add this after click
confirm

now select hotels target group

click next

The screenshot shows the AWS Lambda function configuration interface. The 'Environment' tab is selected. In the 'Variables' section, several environment variables are listed:

- AWS_LAMBDA_FUNCTION_NAME: myapp
- AWS_LAMBDA_FUNCTION_MEMORY_SIZE: 128
- AWS_LAMBDA_FUNCTION_TIMEOUT: 3
- AWS_LAMBDA_LOG_GROUP_NAME: /aws/lambda/myapp
- AWS_LAMBDA_LOG_STREAM_NAME: 2025-01-12T10:43:07.000Z-000
- AWS_LAMBDA_SOURCE_CODE_HASH: 25ddcfe0d80619717043e48570ad56

The 'Tracing' section shows that tracing is disabled.

The screenshot shows the AWS CloudFront Listener Rule Priority configuration interface. The top navigation bar includes tabs for 'Live Session', 'monolithic vs microservice', 'ALB Listener Rule Priority', 'Tripmoney Insurance', 'Manage AWS Resources', 'Step 4 Add listener rule', and 'Download history'. The main title is 'Set rule priority' with an 'Info' link. A sidebar on the left lists steps: Step 1 (Add rule), Step 2 (Define rule conditions), Step 3 (Define rule actions), Step 4 (Set rule priority), and Step 5 (Review and create). The current step, 'Step 4 Set rule priority', is highlighted with a blue circle. The main content area shows 'Listener details: HTTP:80' and 'Listener rules (2)'. The table displays two rules:

Name tag	Priority	Conditions (If)	Actions (Then)	ARN
hotels	1	Query String is type=hotels	Forward to target group • hotels [1] (100%) • Target group stickiness: Off	Pending
Default	Last (default)	If no other rule applies	Forward to target group • flight [1] (100%) • Target group stickiness: Off	ARN

Buttons at the bottom include 'Cancel', 'Previous', and 'Next' (highlighted with a mouse cursor).

set priority and click next

The screenshot shows the AWS CloudFront console with the following details:

- Region:** ap-south-1
- Distribution Name:** monolithic vs microserver
- Protocol:** HTTPS
- Origin:** mmt (Amazon S3 bucket)
- SSL Certificate:** TripMoney Insurance
- Custom Headers:** Content-Type: application/javascript
- Cache Behavior:** Cache based on query string
- Behaviors:** One behavior named "Default" with a priority of 1.
- Default Cache Behavior:** Cache based on query string
- Logs:** Log to CloudWatch Logs with a log group name of /aws/lambda/mmt

The status bar at the bottom indicates the distribution is in the **Pending** state.

Review and submit

The screenshot shows the AWS CloudWatch Metrics Insights interface. A search bar at the top contains the query: `CloudWatch Metrics Insights metrics`. Below the search bar, the results are displayed in a table format:

Series	Dimensions	Metrics
CloudWatch Metrics Insights metrics	CloudWatch Metrics Insights metrics	CloudWatch Metrics Insights metrics

Below the table, there is a section titled "Metrics Insights metrics" with a table:

Series	Dimensions	Metric Name	Unit	Period	Value
CloudWatch Metrics Insights metrics					

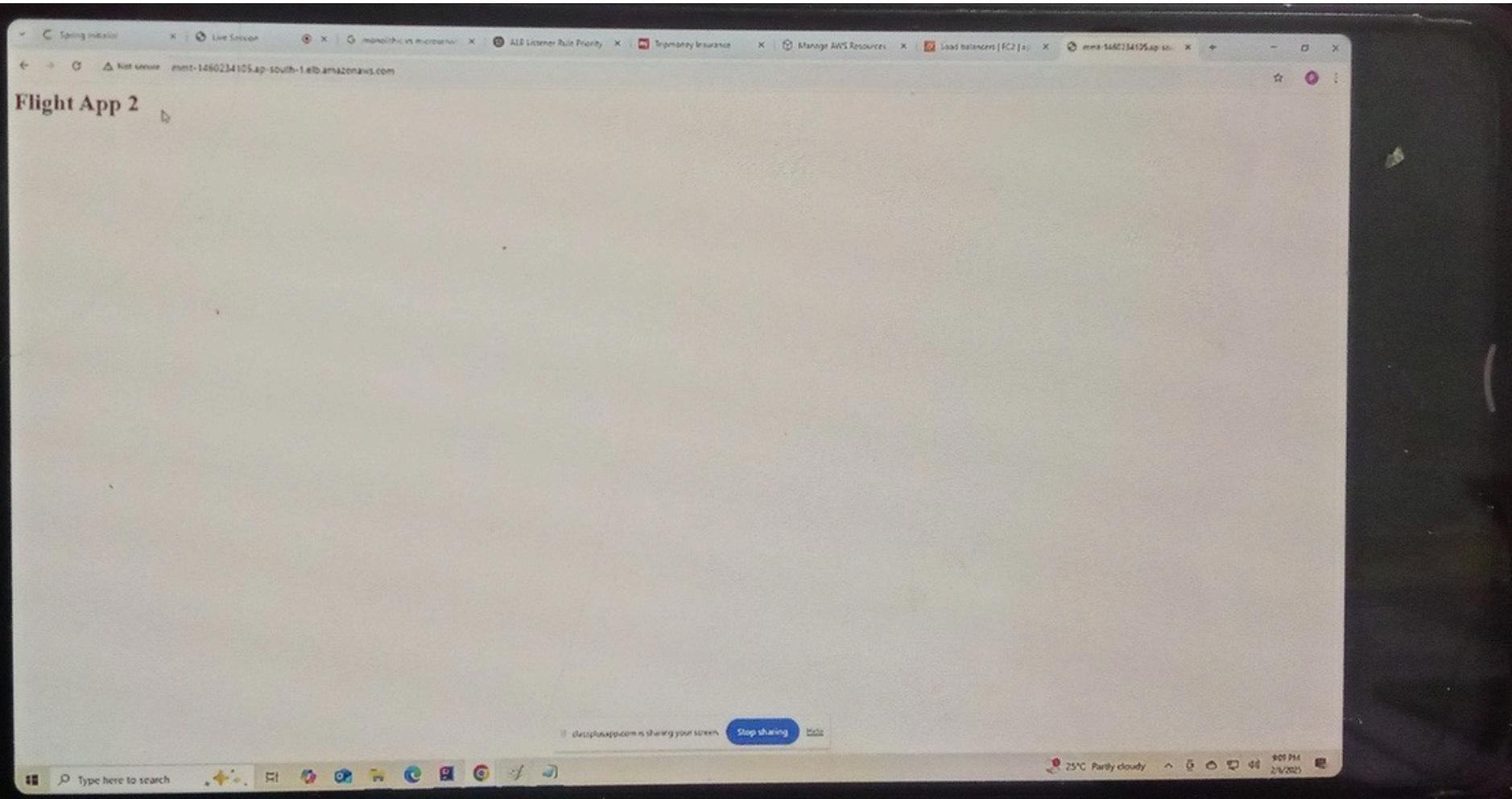
At the bottom of the interface, there are several buttons: `Run`, `Stop`, `Cancel`, `Clear`, and `Help`.

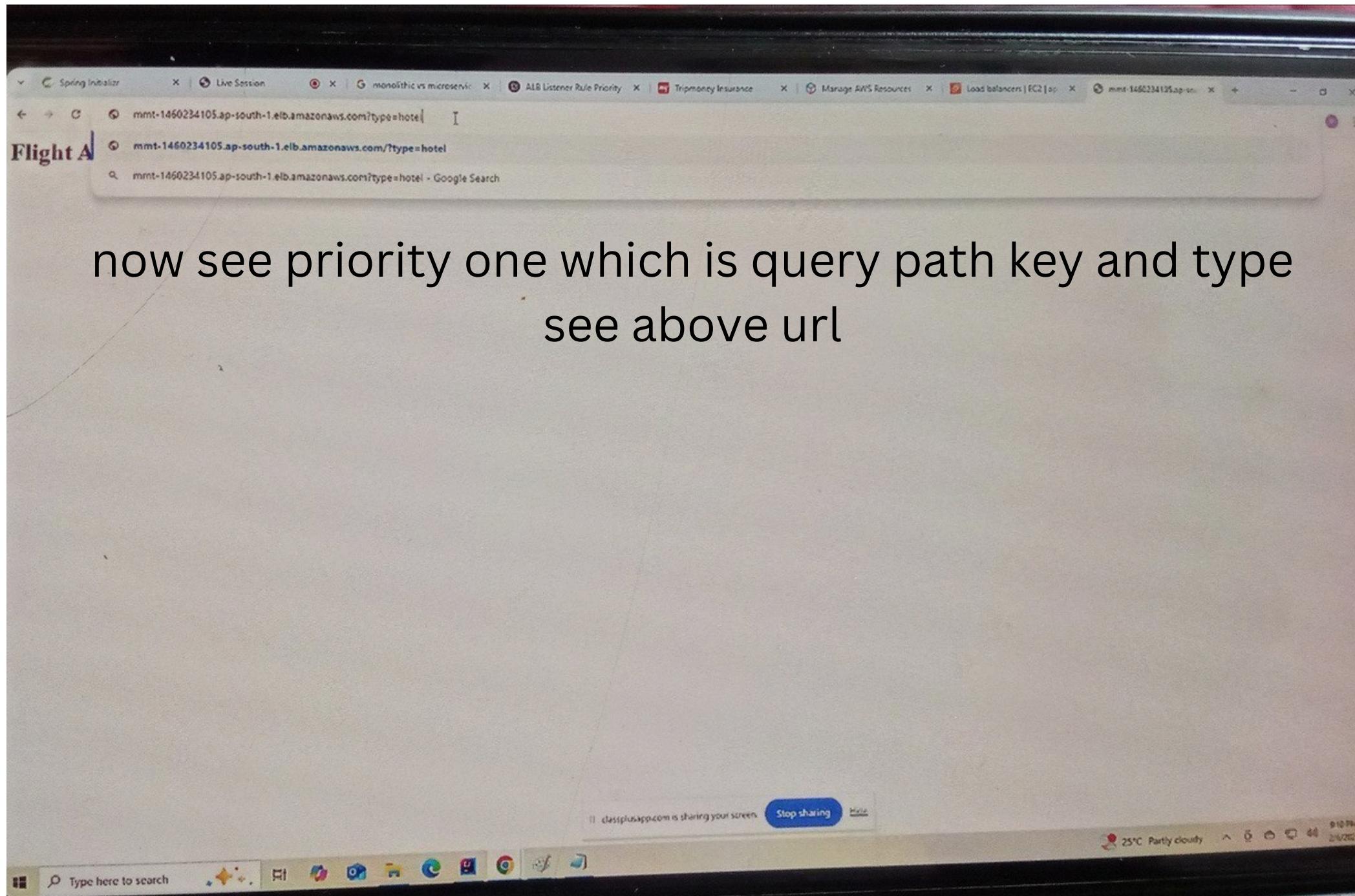
now see both present default and priority

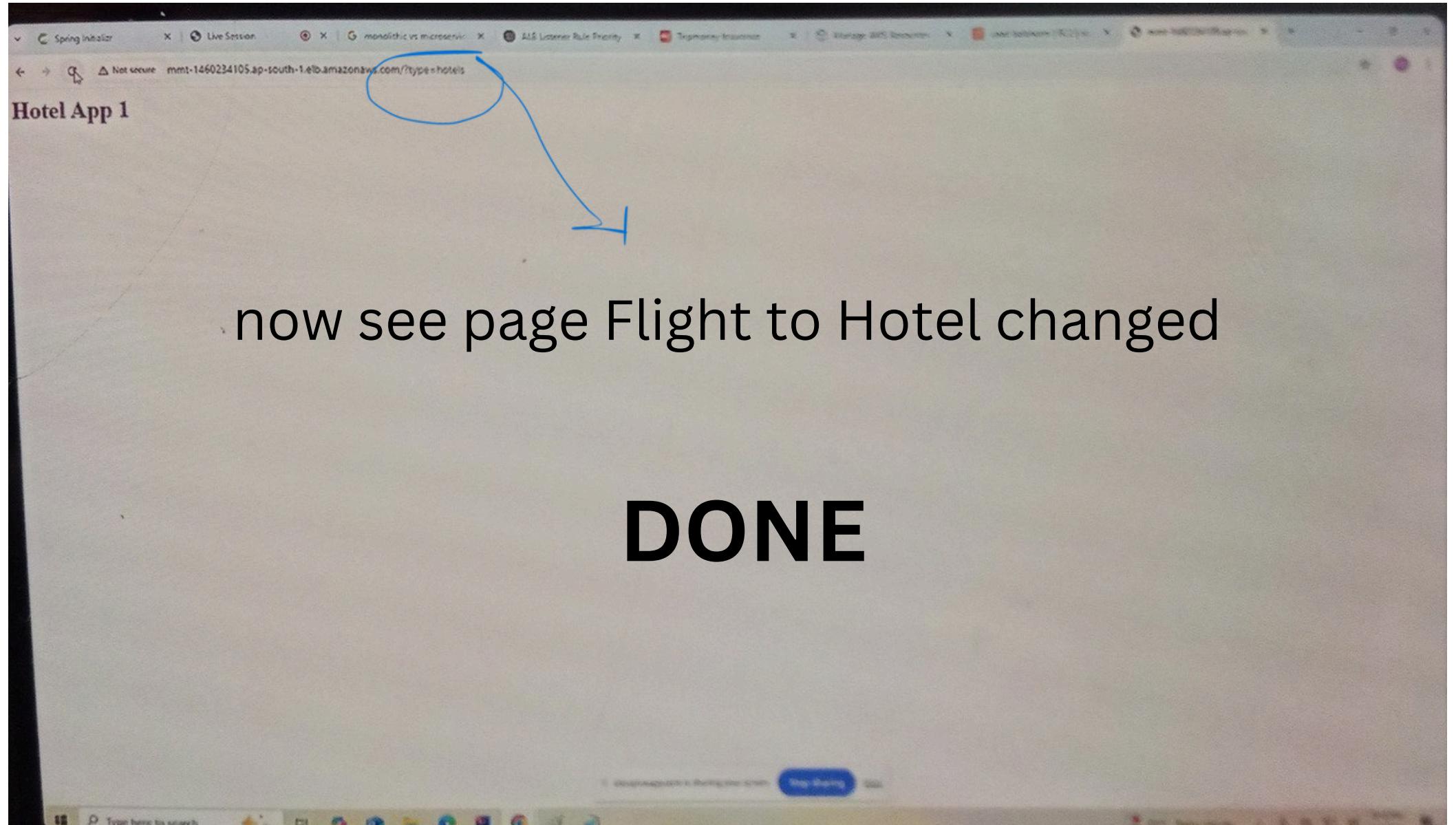
The screenshot shows the AWS CloudShell interface with the AWS Management Console open. The user is in the EC2 service, specifically viewing the Load balancers section. On the left, there's a sidebar with various AWS services like Images, Elastic Block Store, Network & Security, Load Balancing, Auto Scaling, and Settings. The main area displays a table of load balancers with one entry: 'mmt'. The 'DNS name' column for this entry shows 'mmt-1460234105.ap-south-1.elb.amazonaws.com'. A blue oval highlights the 'DNS name info' link next to this value. Below the table, there's a section for the 'Load balancer: mmt' with details like 'Internet-facing' and 'ZP97RAFLXTNZK'. At the bottom of the page, there's a footer with links for CloudShell, Feedback, and a search bar, along with standard browser navigation icons.

now go to load balancer and select DNS

default is flight







DONE

Create RDS and Connect MySQL

2. Prerequisites 3. Creating an AWS RDS

MySQL Database

3.1. Step 1: Accessing AWS Console and Navigating to RDS

3.2. Step 2: Creating a MySQL Database

3.3. Step 3: Modifying Database Configuration

3.4. Step 4: Configuring Security Group Rules

3.5. Step 5: Obtaining the Database Endpoint

4. Connecting to the AWS RDS MySQL Database

4.1. Step 1: Downloading MySQL Workbench

4.2. Step 2: Creating a New Connection

4.3. Step 3: Logging Into the Database

5. Conclusion

6. Resources

Introduction:

Amazon Web Services (AWS) provides a powerful and scalable cloud-based solution for managing databases through its Relational Database Service (RDS). In this tutorial, we will walk through the process of setting up an AWS RDS MySQL database, configuring its access, and connecting to it using MySQL Workbench. Whether you're new to AWS or looking to expand your knowledge, this guide will help you get started with RDS databases quickly and efficiently.

Prerequisites:

Before diving into the setup process, make sure you have the following prerequisites in place:

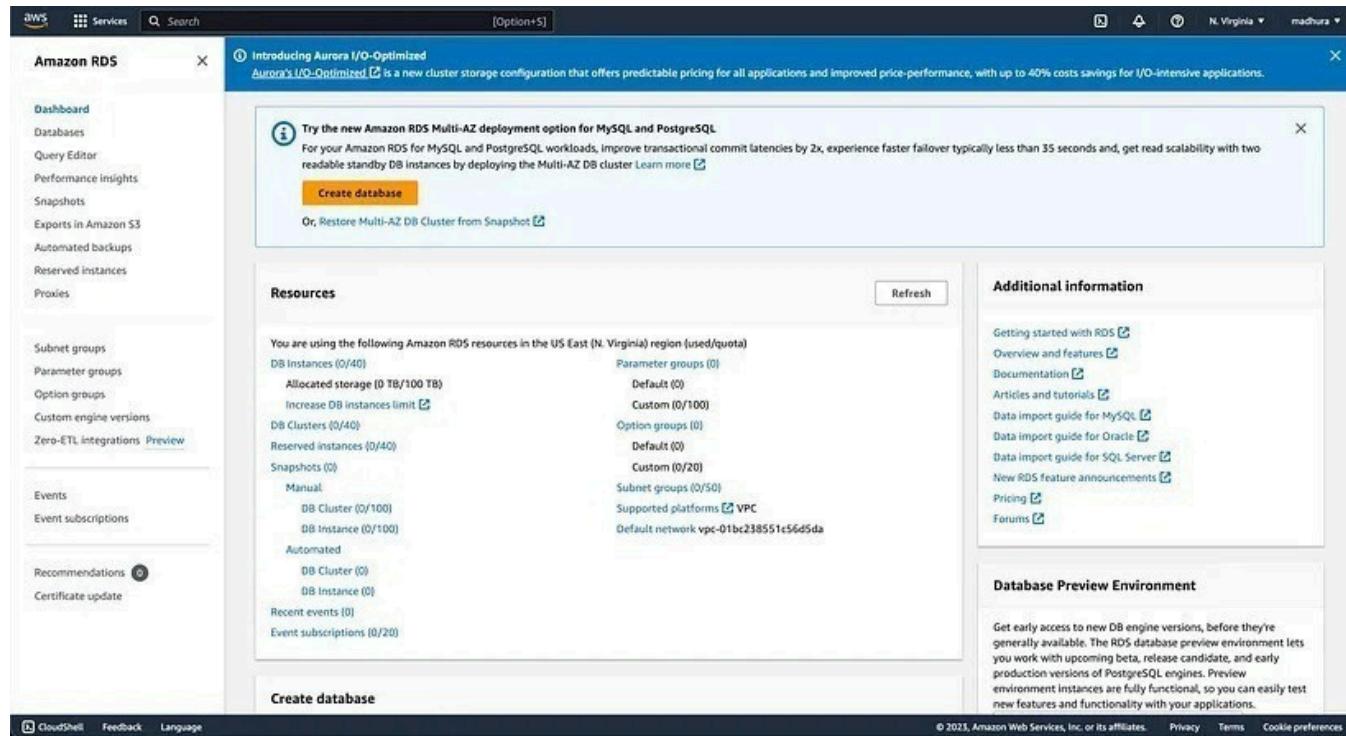
- An active AWS account with appropriate access permissions.
- Basic familiarity with AWS services and the AWS Management Console.
- A computer with an internet connection.

Creating an AWS RDS MySQL Database:

Step 1: Accessing AWS Console and Navigating to RDS

To begin, log in to your AWS Management Console and search for “RDS” in the service search bar. Click on the “RDS” service to open the RDS Dashboard.

Step 2: Creating a MySQL Database



Within the RDS Dashboard, click on the “Create database” button and select “MySQL” as the database engine.

AWS Services Search [Option+S]

RDS > Create database

Create database

Choose a database creation method [Info](#)

Standard create
You set all of the configuration options, including ones for availability, security, backups, and maintenance.

Easy create
Use recommended best-practice configurations. Some configuration options can be changed after the database is created.

Engine options

Engine type [Info](#)

Aurora (MySQL Compatible) 

Aurora (PostgreSQL Compatible) 

MySQL 

MariaDB 

PostgreSQL 

Oracle 

Microsoft SQL Server 

[CloudShell](#) [Feedback](#) [Language](#)

Provide a name for your database and choose the “Free tier” option.



Templates

Choose a sample template to meet your use case.

Production

Use defaults for high availability and fast, consistent performance.

Dev/Test

This instance is intended for development use outside of a production environment.

Free tier

Use RDS Free Tier to develop new applications, test existing applications, or gain hands-on experience with Amazon RDS.

[Info](#)

Availability and durability

Deployment options [Info](#)

The deployment options below are limited to those supported by the engine you selected above.

Multi-AZ DB Cluster - new

Creates a DB cluster with a primary DB instance and two readable standby DB instances, with each DB instance in a different Availability Zone (AZ). Provides high availability, data redundancy and increases capacity to serve read workloads.

Multi-AZ DB instance (not supported for Multi-AZ DB cluster snapshot)

Creates a primary DB instance and a standby DB instance in a different AZ. Provides high availability and data redundancy, but the standby DB instance doesn't support connections for read workloads.

Single DB instance (not supported for Multi-AZ DB cluster snapshot)

Creates a single DB instance with no standby DB instances.

Settings

DB instance identifier [Info](#)

Type a name for your DB instance. The name must be unique across all DB instances owned by your AWS account in the current AWS Region.

database-1

The DB instance identifier is case-insensitive, but is stored as all lowercase (as in "mydbinstance"). Constraints: 1 to 60 alphanumeric characters or hyphens. First character must be a letter. Can't contain two consecutive hyphens. Can't end with a hyphen.

▼ Credentials Settings

Set a password for accessing the database and proceed to create the database. Note that the creation process might take a few minutes.

The screenshot shows the AWS RDS Database Configuration page. At the top, there's a navigation bar with the AWS logo, a services menu, a search bar, and a keyboard shortcut [Option+S]. The main content area has a sidebar with a 'Settings' section. The 'DB instance identifier' field contains 'database-1'. Below it, a note says the identifier is case-insensitive and stored lowercase. The 'Master username' field contains 'admin'. A note says it must be a letter and between 1 and 16 characters. There are two checkboxes: one for managing credentials in AWS Secrets Manager (unchecked) and one for auto-generating a password (unchecked). A note states that managing credentials in Secrets Manager limits some RDS features. The 'Master password' field contains '....'. A note specifies at least 8 printable ASCII characters. The 'Confirm master password' field also contains '....'. At the bottom, the 'Instance configuration' section notes that options are limited to those supported by the selected engine. A footer bar includes CloudShell, Feedback, and Language links.

Step 3: Modifying Database Configuration

Once the database is created, go to the “Modify” option for your database. Expand the “Additional configuration” section and select the “Publicly accessible” option. Save the changes.

Security group
List of DB security groups to associate with this DB instance.

Certificate authority [Info](#)
Using a server certificate provides an extra layer of security by validating that the connection is being made to an Amazon database. It does so by checking the server certificate that is automatically installed on all databases that you provision.

Additional configuration

Public access

Publicly accessible
RDS assigns a public IP address to the database. Amazon EC2 instances and other resources outside of the VPC can connect to your database. Resources inside the VPC can also connect to the database. Choose one or more VPC security groups that specify which resources can connect to the database.

Not publicly accessible
No IP address is assigned to the DB instance. EC2 instances and devices outside the VPC can't connect.

Database port
Specify the TCP/IP port that the DB instance will use for application connections. The application connection string must specify the port number. The DB security group and your firewall must allow connections to the port. [Learn more](#)

Database authentication

Database authentication options [Info](#)

Password authentication
Authenticates using database passwords.

Password and IAM database authentication
Authenticates using the database password and user credentials through AWS IAM users and roles.

Password and Kerberos authentication
Choose a directory in which you want to allow authorized users to authenticate with this DB instance using Kerberos Authentication.

[CloudShell](#) [Feedback](#) [Language](#)

Step 4: Configuring Security Group Rules

Next, navigate to the “Security Group Rules” section for your database. In the “Inbound rules” tab, add a rule for MySQL. Specify the source as your IP address or any desired location. Save the changes.

Step 5: Obtaining the Database Endpoint

After saving the security group rules, allow some time for the changes to propagate. Once completed, you should see the “Publicly accessible” option set to “true” for your database. Copy the endpoint provided for your database. This endpoint will be used to connect to the database.

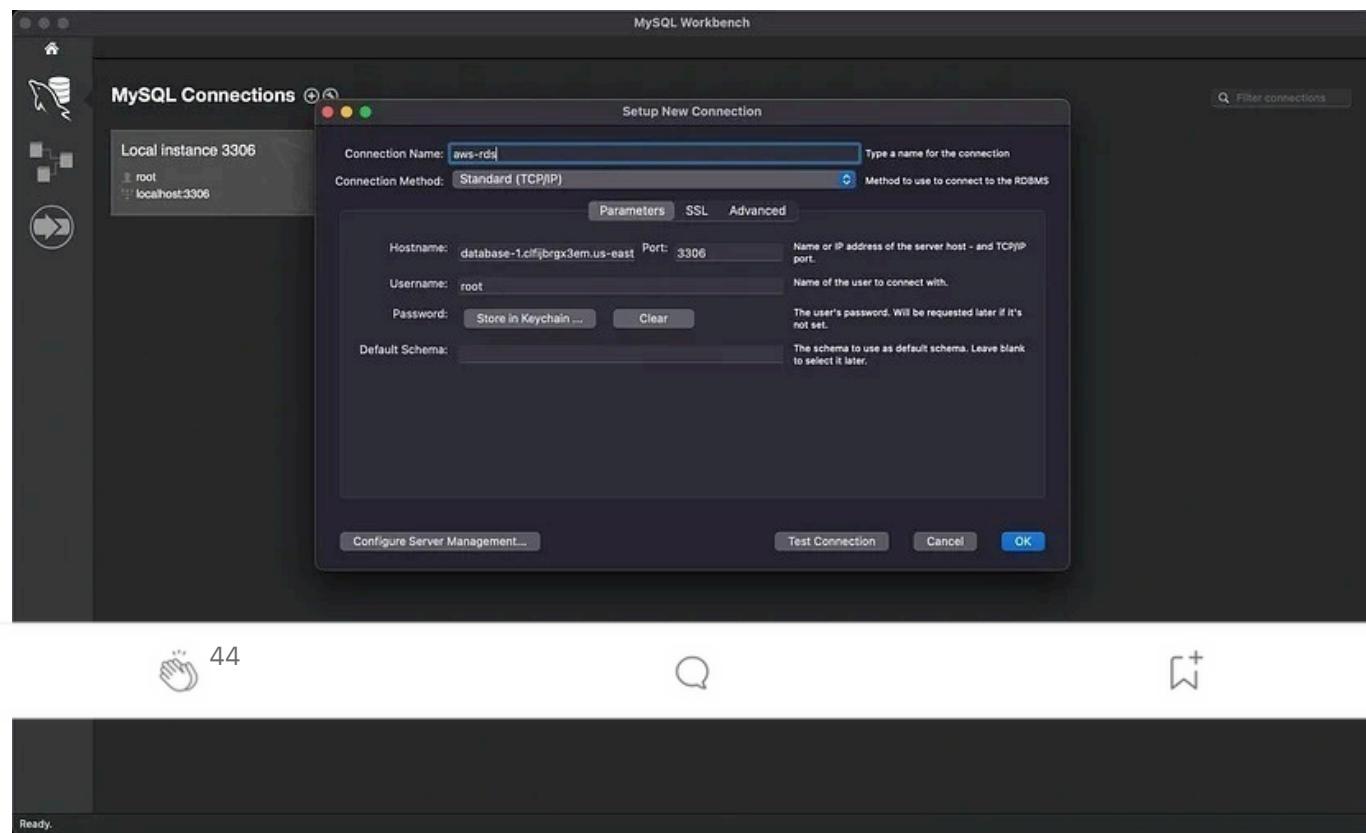
Connecting to the AWS RDS MySQL Database:

Step 1: Downloading MySQL Workbench

To connect to the RDS database, download and install MySQL Workbench on your local machine. MySQL Workbench is a popular tool for managing and interacting with MySQL databases.

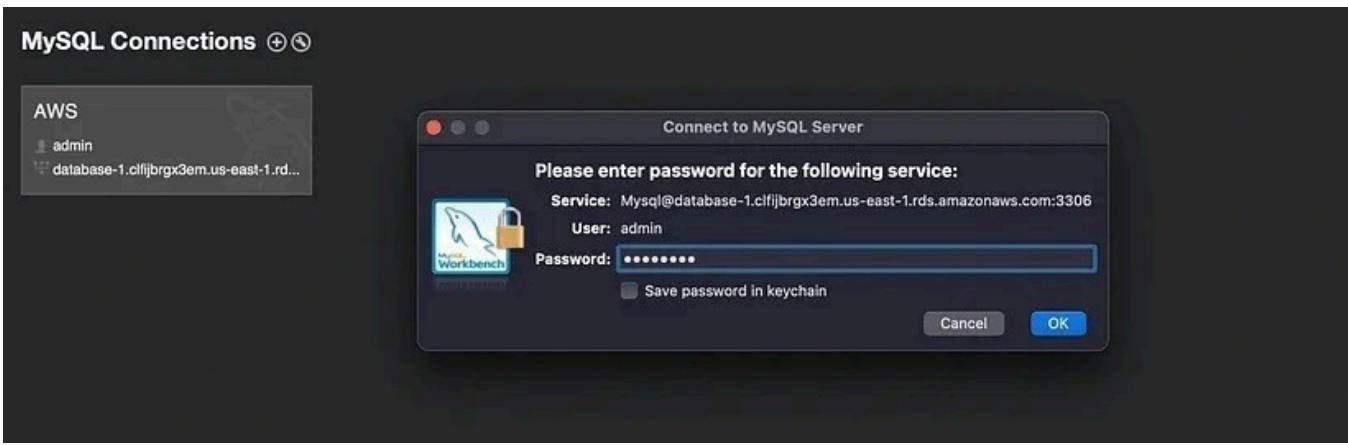
Step 2: Creating a New Connection

Launch MySQL Workbench and click on the “+” button next to “MySQL Connections” to create a new connection. Provide a name for the connection and enter the database endpoint copied earlier. Set the port to 3306 and leave the other settings as default.

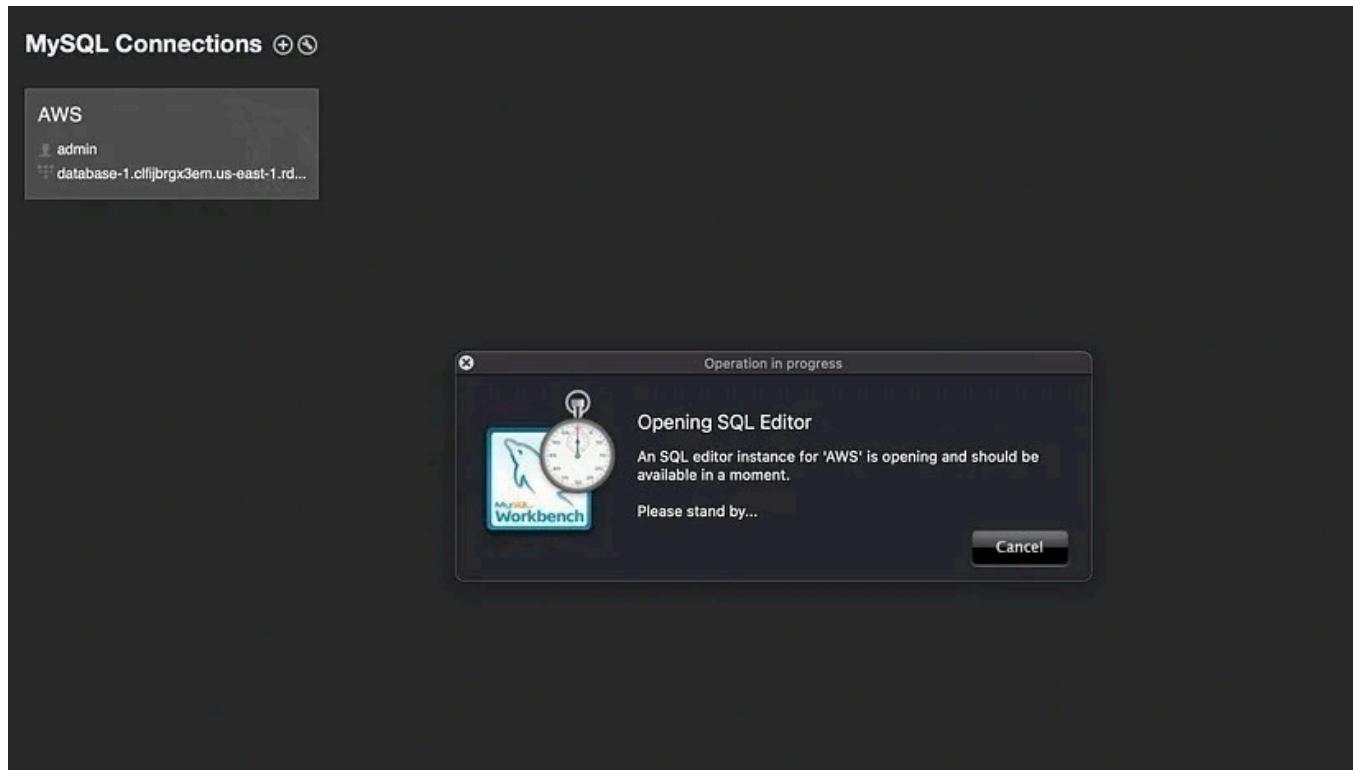


Step 3: Logging Into the Database

Click on the newly created connection and enter the password you set during the database creation process. Click “Test Connection” to verify the connection settings. If successful, click “OK” to establish the connection.



Now you can use MySQL like it's on your local machine!



MySQLWorkbench File Edit View Query Database Server Tools Scripting Help 38° 80% Mon 17 Jul 6:35 PM MySQL Workbench

AWS

Administration Schemas Query 1

MANAGEMENT

- Server Status
- Client Connections
- Users and Privileges
- Status and System Variables
- Data Export
- Data Import/Restore

INSTANCE

- Startup / Shutdown
- Server Logs
- Options File

PERFORMANCE

- Dashboard
- Performance Reports
- Performance Schema Setup

Object Info Session No object selected

100% 40:10

Action Output

Time	Action	Response	Duration / Fetch Time
18:35:32		Error: Canceled by user	

Executing Query...

```
1 CREATE DATABASE store;
2 use db;
3 CREATE TABLE customers (
4     id INT PRIMARY KEY AUTO_INCREMENT,
5     name VARCHAR(50),
6     age INT,
7     email VARCHAR(50)
8 );
9 INSERT INTO customer (name, age, email) VALUES
10 ('John Doe', 25, 'john@example.com'),
11 ('Jane Smith', 30, 'jane@example.com'),
12 ('Mike Johnson', 35, 'mike@example.com');
13
14 SELECT * FROM customers;
15
16
17
```

MySQLWorkbench File Edit View Query Database Server Tools Scripting Help 38° 80% Mon 17 Jul 6:39 PM MySQL Workbench

AWS

Administration Schemas Query 1

SCHEMAS

- SYS
- Tables
- Views
- Stored Procedures
- Functions

Filter objects

1 CREATE DATABASE IF NOT EXISTS store;
2 use store;
3 CREATE TABLE customers (
4 id INT PRIMARY KEY AUTO_INCREMENT,
5 name VARCHAR(50),
6 age INT,
7 email VARCHAR(50)
8);
9 INSERT INTO customers (name, age, email) VALUES
10 ('John Doe', 25, 'john@example.com'),
11 ('Jane Smith', 30, 'jane@example.com'),
12 ('Mike Johnson', 35, 'mike@example.com');
13
14 SELECT * FROM customers;
15

100% 27:14

Result Grid Filter Rows: Search Edit: Export/Import: Result Grid

	id	name	age	email
1	1	John Doe	25	john@example.com
2	2	Jane Smith	30	jane@example.com
3	3	Mike Johnson	35	mike@example.com

Object Info Session No object selected

customers 1

Action Output

Time	Action	Response	Duration / Fetch Time
18:39:00	CREATE DATABASE IF NOT EXISTS store	1 row(s) affected	0.315 sec
18:39:00	use store	0 row(s) affected	0.313 sec
18:39:01	CREATE TABLE customers (id INT PRIMARY KEY AUTO_INCREMENT, name VARCHAR(50), age INT, email VAR...)	0 row(s) affected	0.383 sec
18:39:01	INSERT INTO customers (name, age, email) VALUES ('John Doe', 25, 'john@example.com'), ('Jane Smith', 30, 'jan...')	3 row(s) affected Records: 3 Duplicates: 0 Warnings: 0	0.329 sec
18:39:01	SELECT * FROM customers LIMIT 0, 1000	3 row(s) returned	0.337 sec / 0.000062...

Query Completed

Conclusion:

Congratulations! You have successfully set up an AWS RDS MySQL database and connected to it using MySQL Workbench. AWS RDS provides a robust and scalable solution for managing databases in the cloud, and with the steps outlined in this tutorial, you can start building and deploying your applications with ease.

Create bucket in S3 and host static website

Select AWS S3 service in the management console.



General configuration

AWS Region

US East (N. Virginia) us-east-1

Bucket type [Info](#)

General purpose

Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.

Directory

Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.

Bucket name [Info](#)

aws-s3-demo

Bucket name must be unique within the global namespace and follow the bucket naming rules. [See rules for bucket naming](#) 

Copy settings from existing bucket - optional

Only the bucket settings in the following configuration are copied.

[Choose bucket](#)

Format: s3://bucket/prefix

General Configurations for Amazon S3

- After that, we have to define the ownership of bucket objects through the ACL options. Here, we have two options: we can either enable or disable ACLs. Let's see what Access Control Lists are.

Access Control Lists

- An Access Control List (ACL) is a set of rules determining who can access a resource. In this S3 setup, enabling ACLs lets you control who can access and manage the objects (e.g., website files) you upload to your bucket.
- ACLs enable different AWS accounts to own and control specific files(objects) within your bucket.

- However, a warning may suggest using “bucket policies” instead, as they simplify access control by applying permissions to the entire bucket (e.g., publishing the entire bucket and its objects). Unlike ACLs, bucket policies do not offer fine-grained control over individual objects.
- In summary, if your bucket contains no sensitive information, a bucket policy is sufficient. However, if even one object in the bucket needs to remain private, using ACLs is advisable.

So, I chose the “ACLs enabled” option and assigned the object ownership to the bucket owner.

Object Ownership Info

Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

ACLs disabled (recommended)
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

ACLs enabled
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

⚠️ We recommend disabling ACLs, unless you need to control access for each object individually or to have the object writer own the data they upload. Using a bucket policy instead of ACLs to share data with users outside of your account simplifies permissions management and auditing.

Object Ownership

Bucket owner preferred
If new objects written to this bucket specify the bucket-owner-full-control canned ACL, they are owned by the bucket owner. Otherwise, they are owned by the object writer.

Object writer
The object writer remains the object owner.

ℹ️ If you want to enforce object ownership for new objects only, your bucket policy must specify that the bucket-owner-full-control canned ACL is required for object uploads. [Learn more](#) 

Defining object ownership in S3 bucket

- Now, we need to decide whether this bucket will be public or not. Since this bucket will be used to deploy a static website, I made the bucket public by clearing all the checkboxes to enable access for everyone.

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.

⚠️ Turning off block all public access might result in this bucket and the objects within becoming public
AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.

I acknowledge that the current settings might result in this bucket and the objects within becoming public.

Defining public access setting for the S3 bucket

- Next, there is an option to manage bucket versions, which allows saving previous objects as a history when the bucket is updated with new ones. This feature helps track previous objects (backup copies), their URLs, and

last modified dates. It is helpful because it allows recovering a previous object if it is mistakenly deleted. Therefore, I chose to enable this option.

- After that, we can optionally add tags to manage cost allocations. I leave that field empty and keep the default settings for encryption.

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 - optional (0)

You can use bucket tags to track storage costs and organize buckets. [Learn more](#)

No tags associated with this bucket.

[Add tag](#)

Default encryption Info

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type [Info](#)

Server-side encryption with Amazon S3 managed keys (SSE-S3)
 Server-side encryption with AWS Key Management Service keys (SSE-KMS)
 Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)
Secure your objects with two separate layers of encryption. For details on pricing, see [DSSE-KMS pricing](#) on the Storage tab of the [Amazon S3 pricing page](#).

Bucket Key

Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. [Learn more](#)

Disable
 Enable

Versioning and encryption in S3 bucket

- Now, choose the Create Bucket option.

Excellent! You just created an S3 bucket. Now, let's upload your static website to it.

The screenshot shows the Amazon S3 Buckets page. At the top, a green banner displays a success message: "Successfully created bucket 'aws-s3-medium-article'" with a "View details" button and a close icon. Below the banner, the navigation bar shows "Amazon S3 > Buckets". A callout box titled "Account snapshot - updated every 24 hours" includes "All AWS Regions" and a "View Storage Lens dashboard" button. The main content area has tabs for "General purpose buckets" (selected) and "Directory buckets". Under "General purpose buckets", there is a table with one item:

Name	AWS Region	IAM Access Analyzer	Creation date
aws-s3-medium-article	US East (N. Virginia) us-east-1	View analyzer for us-east-1	August 31, 2024, 16:21:19 (UTC+05:30)

Actions for the bucket include "Copy ARN", "Empty", "Delete", and "Create bucket". A note states: "Buckets are containers for data stored in S3." A search bar "Find buckets by name" and a pagination indicator "1" are also present.

Amazon S3 bucket creation

🎯 Step 2: Upload Contents to the Amazon S3

- Now select the created bucket in the Buckets section.
- Then, choose and upload the files to the bucket.

Upload Info

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 folder**.

Files and folders (2 Total, 553.0 B)

[Remove](#) [Add files](#) [Add folder](#)

All files and folders in this table will be uploaded.

[Find by name](#)

< 1 >

<input type="checkbox"/>	Name	Folder	Type	Size
<input type="checkbox"/>	main.css	-	text/css	253.0 B
<input type="checkbox"/>	index.html	-	text/html	300.0 B

Destination Info

Destination

[s3://aws-s3-medium-article](#)

► Destination details

Bucket settings that impact new objects stored in the specified destination.

► Permissions

Grant public access and access to other AWS accounts.

► Properties

Specify storage class, encryption settings, tags, and more.

[Cancel](#)

[Upload](#)

Upload files to the S3 bucket.

🎯 Step 3: Configure a static web hosting on Amazon S3

- We have already uploaded our static website contents to the S3 bucket.
- However, we still need a URL to access our website. Now, let's set up the bucket for static website hosting.

- By configuring your S3 bucket for hosting, you're instructing it to create a URL that will take anyone to a page displaying the files you've uploaded.
- Once again, move to your bucket page and choose the properties tab. Then scroll down until you find the “Static Website Hosting” Panel and select the “Edit” option.
- Now, “Enable” the static website hosting option.
- Configure the following settings:
 - Hosting type: Host a static website
 - Index document: In my case, the default page/home page is an index.html file. This can be different in your case.Keep the optional settings as the default and save the changes.
-

Edit static website hosting Info

Static website hosting

Use this bucket to host a website or redirect requests. [Learn more](#)

Static website hosting

- Disable
 Enable

Hosting type

- Host a static website
Use the bucket endpoint as the web address. [Learn more](#)
 Redirect requests for an object
Redirect requests to another bucket or domain. [Learn more](#)

ⓘ For your customers to access content at the website endpoint, you must make all your content publicly readable. To do so, you can edit the S3 Block Public Access settings for the bucket. For more information, see [Using Amazon S3 Block Public Access](#)

Index document

Specify the home or default page of the website.

index.html

Error document - optional

This is returned when an error occurs.

error.html

Redirection rules – optional

Redirection rules, written in JSON, automatically redirect webpage requests for specific content. [Learn more](#)

1

Static hosting configurations

- Now, once again, navigate to the static website hosting section, which is located in the properties tab on your bucket page.
- Now, you will be able to see a bucket website endpoint. Please copy and paste it into any web browser to check whether it is accessible.

Static website hosting

Use this bucket to host a website or redirect requests. [Learn more](#) 

Static website hosting
Enabled

Hosting type
Bucket hosting

Bucket website endpoint
When you configure your bucket as a static website, the website is available at the AWS Region-specific website endpoint of the bucket. [Learn more](#) 
 <http://aws-s3-medium-article.s3-website-us-east-1.amazonaws.com> 

Static website hosting section

Oops!!! Forbidden

403 Forbidden

- Code: AccessDenied
- Message: Access Denied
- RequestId: ZTYDTGF0PB8Z1RY7
- HostId: GwOqOVLWQU8Vm2zJX1AH9h6V9i4dWYh81UbqPIvPwu5GVrT7D0jRblvcTgCdZtYMJ82Chz0wmkQ=

403 Forbidden error message: Our files are still private

Why did we get this error? 

Even if our bucket is public, objects in S3 are private by default to secure your data. The error you're seeing indicates that while your static website is hosted, the uploaded files are still private. It's like having a visible bucket with its contents hidden. We need to set the object permissions to public to fix this, which is why ACLs were enabled previously.

 Step 04: Configure ACLs to set your S3 bucket objects as public.

Now, let's make the objects publicly accessible through the ACLs.

- Once again, move into the bucket and select all the objects using checkboxes. Then, in the Actions tab, select the “Make public using ACL” option. Then, Choose Make Public.

Amazon S3 > Buckets > aws-s3-medium-article

aws-s3-medium-article [Info](#)

Objects (2) [Info](#)

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

Upload

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. You'll need to explicitly grant them permissions. [Learn more](#)

[Find objects by prefix](#)

<input checked="" type="checkbox"/>	Name	Type	Last modified	Size
<input checked="" type="checkbox"/>	index.html	html	August 31, 2024, 16:37:45 (UTC+05:30)	
<input checked="" type="checkbox"/>	main.css	css	August 31, 2024, 16:37:44 (UTC+05:30)	

Actions

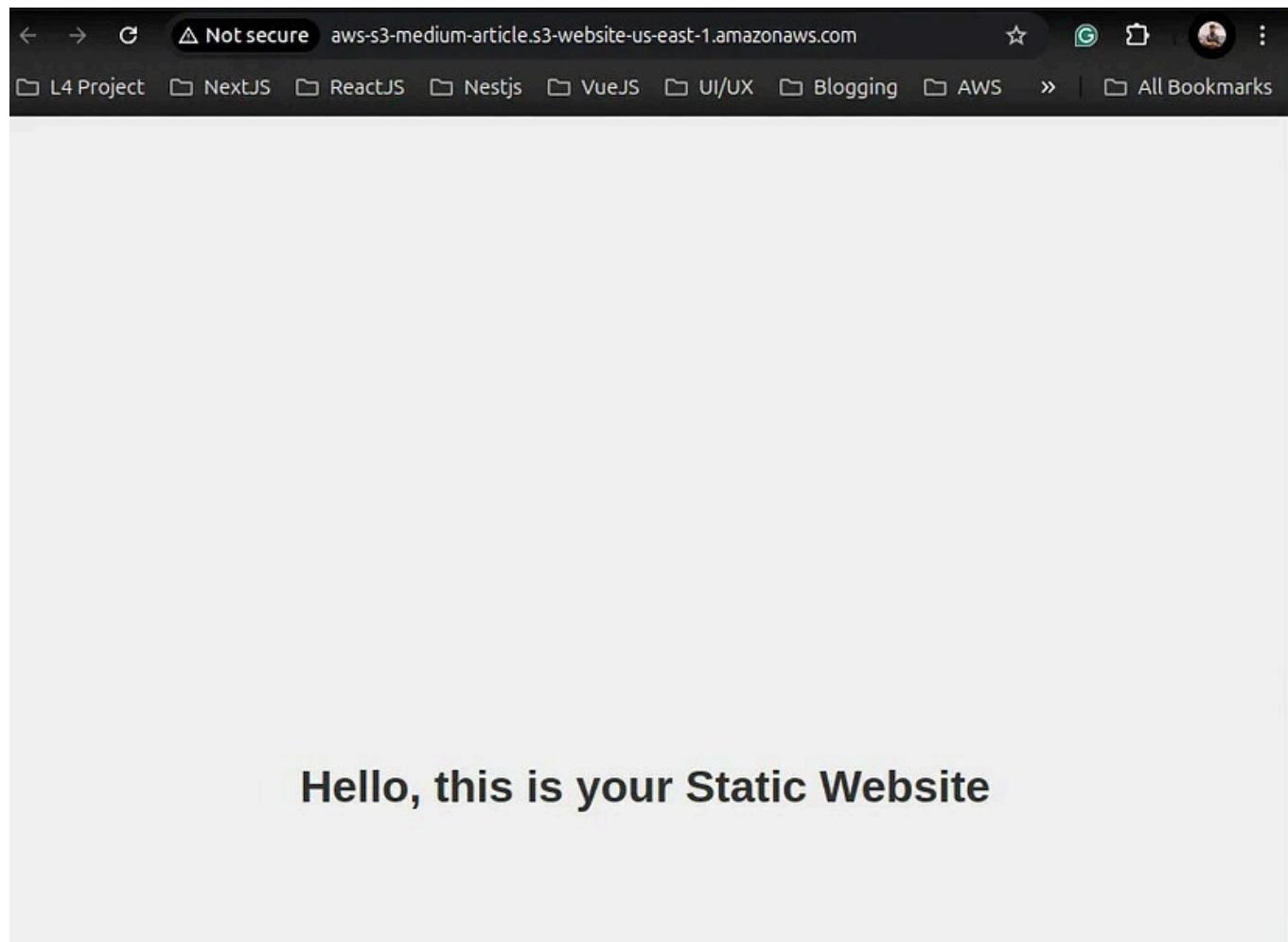
Download as
Share with a presigned URL
Calculate total size
Copy
Move
Initiate restore
Query with S3 Select

Edit actions

Rename object
Edit storage class
Edit server-side encryption
Edit metadata
Edit tags
Make public using ACL

Option to make public our files using ACL

Cool! We have set everything up, and your website should now be visible to everyone. Let's refresh it.



Website preview

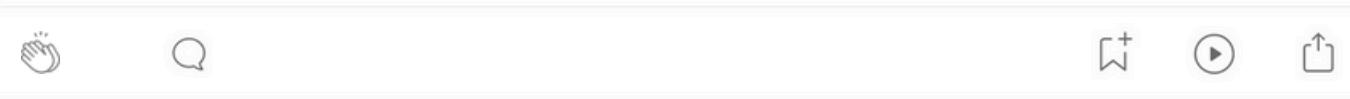
Boom!!! 🎉 Here it is — my website! 😊 Don't laugh too hard; it's just a simple demo I whipped up.

We've just wrapped up the main part of today's session and hosted our static website on Amazon S3. Time to celebrate, right? 🎉

Tip: If you're not using this bucket, be sure to delete it to avoid unnecessary charges.

Update the website

How to secure an AWS IAM User with Multi-Factor Authentication



To enhance security, it's recommended to activate multi-factor authentication to protect AWS resources. MFA can be enabled on the root user and IAM users. Enabling it on the root user only affects that user. It must be enabled separately on other IAM users since each has independent

MFA configurations. There are 3 ways to set up MFA depending on the device which includes:

Virtual MFA U2F

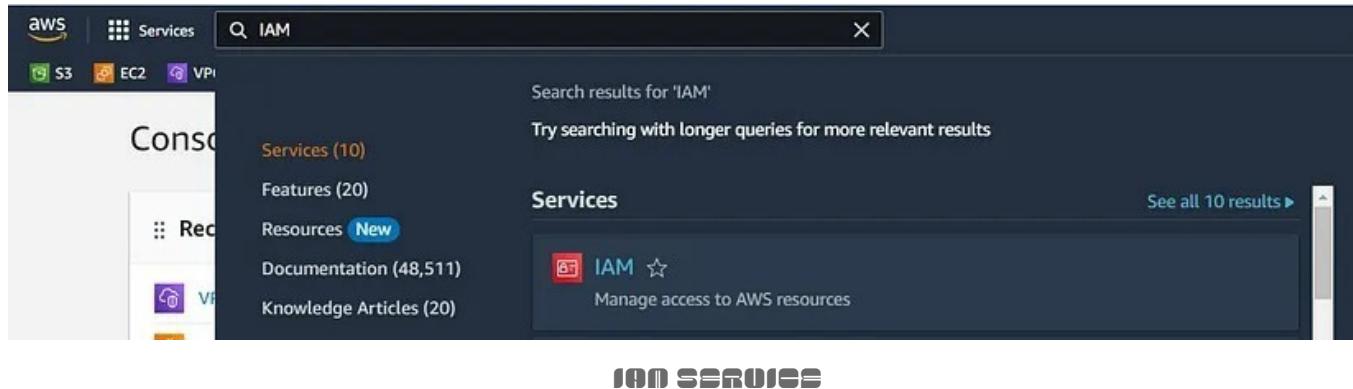
Security key

Hardware MFA

In this article, I showcase the setting up a virtual MFA device since it's the most common method used. It requires installing an authenticator app on your device which is compatible with AWS. You can find the list of authorized apps you can use on this page. We shall use the Google Authenticator for this purpose.

Enabling MFA device

1. Sign in to the IAM administrator user you created previously and open the IAM console.



2. Choose Users in the left navigation pane and select “Administrator”. Click the link to open it.

The screenshot shows the AWS IAM 'Access management' section. On the left, a sidebar lists 'User groups', 'Users' (which is circled in red), 'Roles', 'Policies', 'Identity providers', and 'Account settings'. The main area displays a list of users with checkboxes next to their names. The 'CostOp_Admin' user is highlighted with a red circle and selected, as indicated by the checked checkbox.

3. Click Enabled without MFA and click Enable MFA.

The screenshot shows the detailed view for the 'CostOp_Admin' user. It includes fields for ARN (arn:aws:iam::414501764934:user/CostOp_Admin), Created (April 11, 2023, 14:39 (UTC+05:30)), and three tabs: Permissions, Groups (1), and Tags. A tooltip for 'Console access' is displayed, stating 'As a best practice, enable MFA for users who have console access.' and contains a link to 'Enable MFA', which is also circled in red.

4. When the MFA wizard opens give your device a name such as MyMFADevice. Select Authenticator app and click Next.

MFA device name

Device name
Enter a meaningful name to identify this device.

Maximum 128 characters. Use alphanumeric and '+ = , . @ - _' characters.

MFA device

[OPEN IN APP](#) [SIGN UP](#) [SIGN IN](#)

Medium [SEARCH](#) [WRITE](#)

 **Authenticator app**
Authenticate using a code generated by an app installed on your mobile device or computer.

5. The console displays info for the virtual MFA device. This is when you'll add an account on the authenticator app on your device. By now you should've installed the Google Authenticator on your phone. From it you'll get a QR code for the next step. If you've not yet installed the app, please go ahead and do so. You can install apps for your smartphone from the app store that is specific to your type of smartphone. Some app providers also have web and desktop applications available. See the following table for examples:

Android	Twilio Authy Authenticator , Duo Mobile , Microsoft Authenticator , Google Authenticator , Symantec VIP
iOS	Twilio Authy Authenticator , Duo Mobile , Microsoft Authenticator , Google Authenticator , Symantec VIP

6. Open the Google Authenticator on your device. You can add an account and select the QR code option.

7. Click on Show QR Code on the MFA wizard and then use the app to scan the QR code.

Authenticator app

A virtual MFA device is an application running on your device that you can configure by scanning a QR code.

1

Install a compatible application such as Google Authenticator, Duo Mobile, or Authy app on your mobile device or computer.

[See a list of compatible applications](#)

2



Open your authenticator app, choose **Show QR code** on this page, then use the app to scan the code. Alternatively, you can type a secret key.
[Show secret key](#)

Fill in two consecutive codes from your MFA device.

MFA code 1

3

MFA code 2

8. Once you scan the QR code, the app will start generating one-time passcodes. Use these codes to fill in the MFA code 1 and code 2 boxes with two consecutive codes. Get the first one then wait for 30 seconds to get the next. Once that's done. Click "Add MFA."

You'll get the confirmation that MFA is enabled for the user

To test it, simply logout and log back in with this same "Administrator" user. After entering your credentials, you'll be prompted to enter a one-time passcode. Open the Google Authenticator and copy the code provided. The app generates codes every 30 seconds.

That's it for this article. I hope you were enriched. We learned how to create an IAM user with administrator privileges and further secure it by enabling MFA. Thank you for reading and see you at the next one.

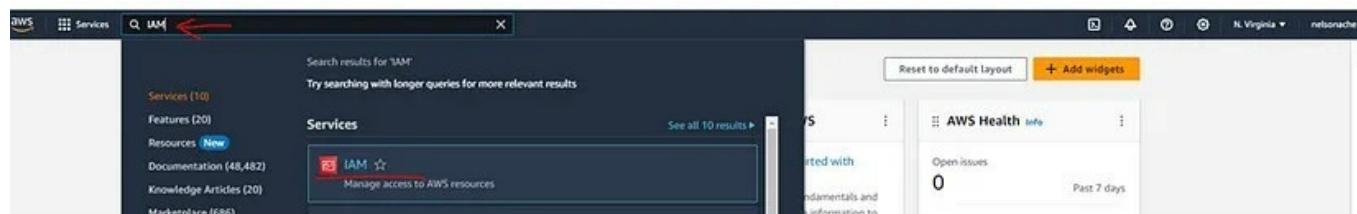


SOURCE: AWS.AMAZON.COM

How to Create an IAM User

We shall see how to create an IAM User with Administrator privileges in the following steps:

1. First we need to be logged into the AWS Management console. Search for IAM and select it to open the IAM Console



2. On the left navigation pane, click Users, then click “Create User” at the top right corner.

The screenshot shows the AWS Identity and Access Management (IAM) service. On the left, there's a navigation sidebar with options like 'Dashboard', 'Access management', 'User groups', 'Users' (which is selected and highlighted with a red box), 'Roles', and 'Policies'. The main content area is titled 'Users (1) Info' and contains a table with one row for 'nelson'. The table includes columns for 'User name', 'Path', 'Groups', 'Last activity', 'MFA', 'Password age', 'Console last sign-in', 'Access key ID', and 'Active key age'. A 'Delete' button and a 'Create user' button are at the top right of the table area, with the 'Create user' button also highlighted with a red box.

3. Specify “Administrator” as the user name which will be used to sign-in. Since this user should have administrator privileges, check the box “Provide user access to the AWS Management Console”. Check the option “I want to create an IAM user”.

The screenshot shows the 'Specify user details' step of the IAM User creation wizard. It has a 'User details' section with a 'User name' field containing 'Administrator' (highlighted with a red arrow). Below it is a note: 'The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = . @ _ - (hyphen)'. To the left of this note is a red arrow pointing to a checked checkbox: 'Provide user access to the AWS Management Console - optional'. Below this is another note: 'If you're providing console access to a person, it's a best practice to manage their access in IAM Identity Center.' At the bottom, there's a question 'Are you providing console access to a person?' with two radio button options: 'Specify a user in Identity Center - Recommended' (unchecked) and 'I want to create an IAM user' (checked, highlighted with a red arrow). There's also a note: 'We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AWS CodeCommit or Amazon Keyspaces, or a backup credential for emergency account access.'

4. It will open the section for us to set the password policy for this user. We can choose either Autogenerated or custom password. Let’s go with “Custom password” to give us control over it. Make sure you enter a password that respects the requirements indicated. Also, uncheck “Users must create a new password at next sign in” then click “Next”

Console password
 Autogenerated password
 You can view the password after you create the user.
 Custom password
 Enter a custom password for the user:

 Must be at least 8 characters long.
 Must include at least three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols ! @ # \$ % ^ & * { } _ + - [] ()) !
 Show password

→ Users must create a new password at next sign-in - Recommended
 Users automatically get the IAMUserChangePassword policy to allow them to change their own password.

If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keypairs, you can generate them after you create this IAM user. [Learn more](#)

Cancel **Next Step**

5. This takes us to set permissions for the user to select how we want to assign permission to this group of users. There are 3 options. Since we're creating an administrator user, and you'll likely be doing this for the first time, we shall go with "Attach policies directly". This will open a list of all existing policies. We shall select the "AdministratorAccess" policy to grant the necessary permissions and click "Next".

Set permissions
 Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

Permissions options

- Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.
- Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.
- Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

Permissions policies (1/1132)
 Choose one or more policies to attach to your new user.

Policy name	Type	Attached entities
<input type="checkbox"/> AccessAnalyzerServiceRolePolicy	AWS managed	0
<input checked="" type="checkbox"/> AdministratorAccess	AWS managed - job function	1
<input type="checkbox"/> AdministratorAccess-Amplify	AWS managed	0
<input type="checkbox"/> AdministratorAccess-AWSLambda	AWS managed	0

[Create policy](#)

A policy is essentially a JSON file that defines the permissions a user or group of users have.

6. Now review and take note of the credentials you created. Click "Create user."

Review and create

Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.

User details

User name: Administrator	Console password type: Custom password	Require password reset: No
-----------------------------	---	-------------------------------

Permissions summary

Name	Type	Used as
AdministratorAccess	AWS managed - job function	Permissions policy

Tags - optional
Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

No tags associated with the resource.

Add new tag
You can add up to 50 more tags.

Cancel Previous Create user

7. At this point download the sign-in details in the .csv and copy the sign-in URL. This is for your records. The URL helps to autofill your information. Then return to the users' list.

Retrieve password

You can view and download the user's password below or email users instructions for signing in to the AWS Management Console. This is the only time you can view and download this password.

Console sign-in details

Console sign-in URL https://[REDACTED].signin.aws.amazon.com/console	Email sign-in instructions
User name Administrator	
Console password [REDACTED] Show	

Cancel Download .csv file Return to users list

8. You can identify IAM users in the following ways:

- A friendly name used when creating the user “Administrator” in this case
- The Amazon Resource Name (ARN) that uniquely identifies the user across all of AWS.
- A unique identifier for this user.

You can find the ARN by selecting the user we just created in the IAM console.

Administrator Info

Summary

ARN
arn:aws:iam::123456789012:user/Administrator

Created
October 15, 2023, 09:26 (UTC-04:00)

Console access
Enabled without MFA

Last console sign-in
Never

Access key 1
Create access key

Permissions Groups Tags Security credentials Access Advisor

Permissions policies (1)
Permissions are defined by policies attached to the user directly or through groups.

Filter by Type
Search All types

Policy name	Type	Attached via
AdministratorAccess	AWS managed - job function	Directly

9. Finally, test the login by navigating to the URL you copied previously. Sign in and test the permissions.

Sign in as IAM user

Account ID (12 digits) or account alias

IAM user name

Administrator

>Password

Remember this account

Sign in

Sign in using root user email

Forgot password?

AWS re:Invent
NOV. 27 - DEC. 1, 2023 | LAS VEGAS, NV

Discover generative AI through keynotes, sessions, demos, and more.

Register now

That's it for the section. We shall dive next into setting up Multi-Factor Authentication for the admin user we just created.

How to Set up MFA on AWS

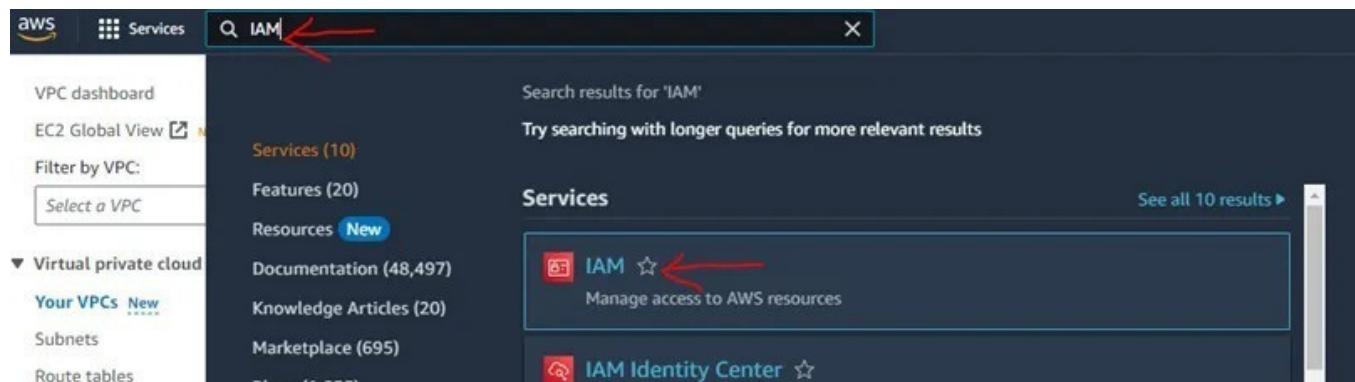
To enhance security, it's recommended to activate multi-factor authentication to protect AWS resources. MFA can be enabled on the root user and IAM users. Enabling it on the root user only affects that user. It must be enabled separately on other IAM users since each has independent MFA configurations. There are 3 ways to set up MFA depending on the device which includes:

- Virtual MFA U2F
- Security key
- Hardware MFA

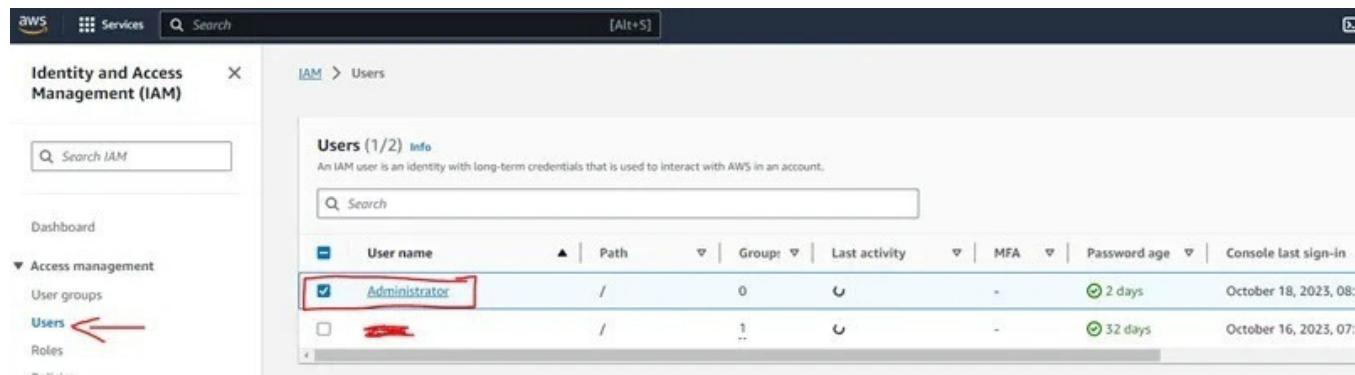
In this lab, we shall set up a virtual MFA device since it's the most common method used. It requires installing an authenticator app on your device which is compatible with AWS. You can find the list of authorized apps you can use on this page. We shall use the Authy app for this purpose.

Enabling MFA device

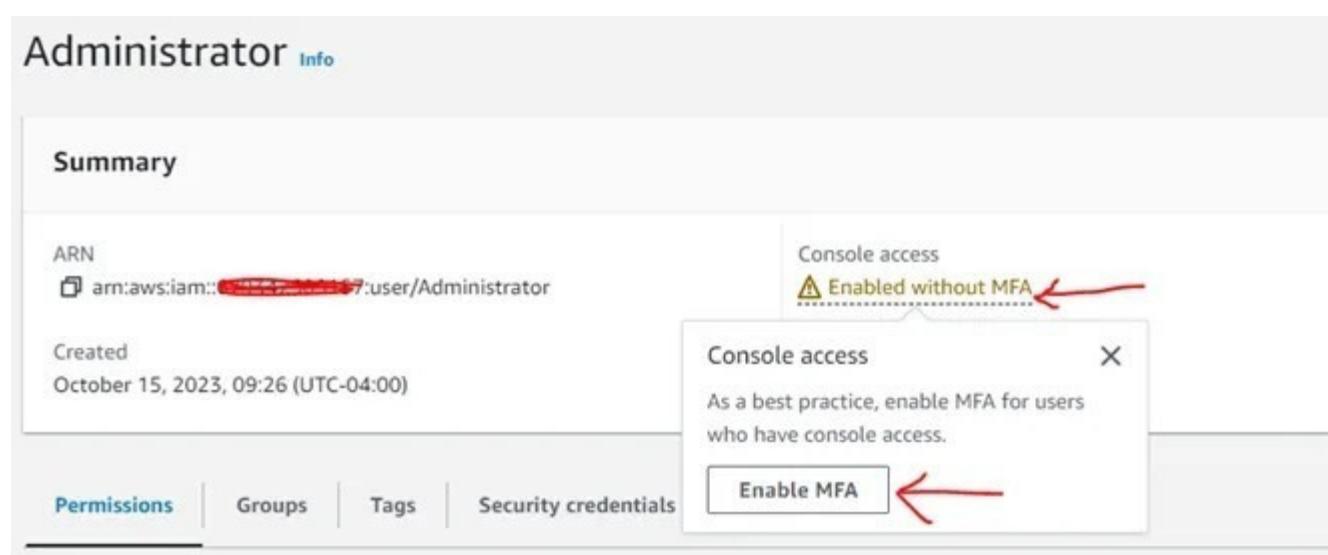
1. Sign in to the IAM administrator user you created previously and open the IAM console.



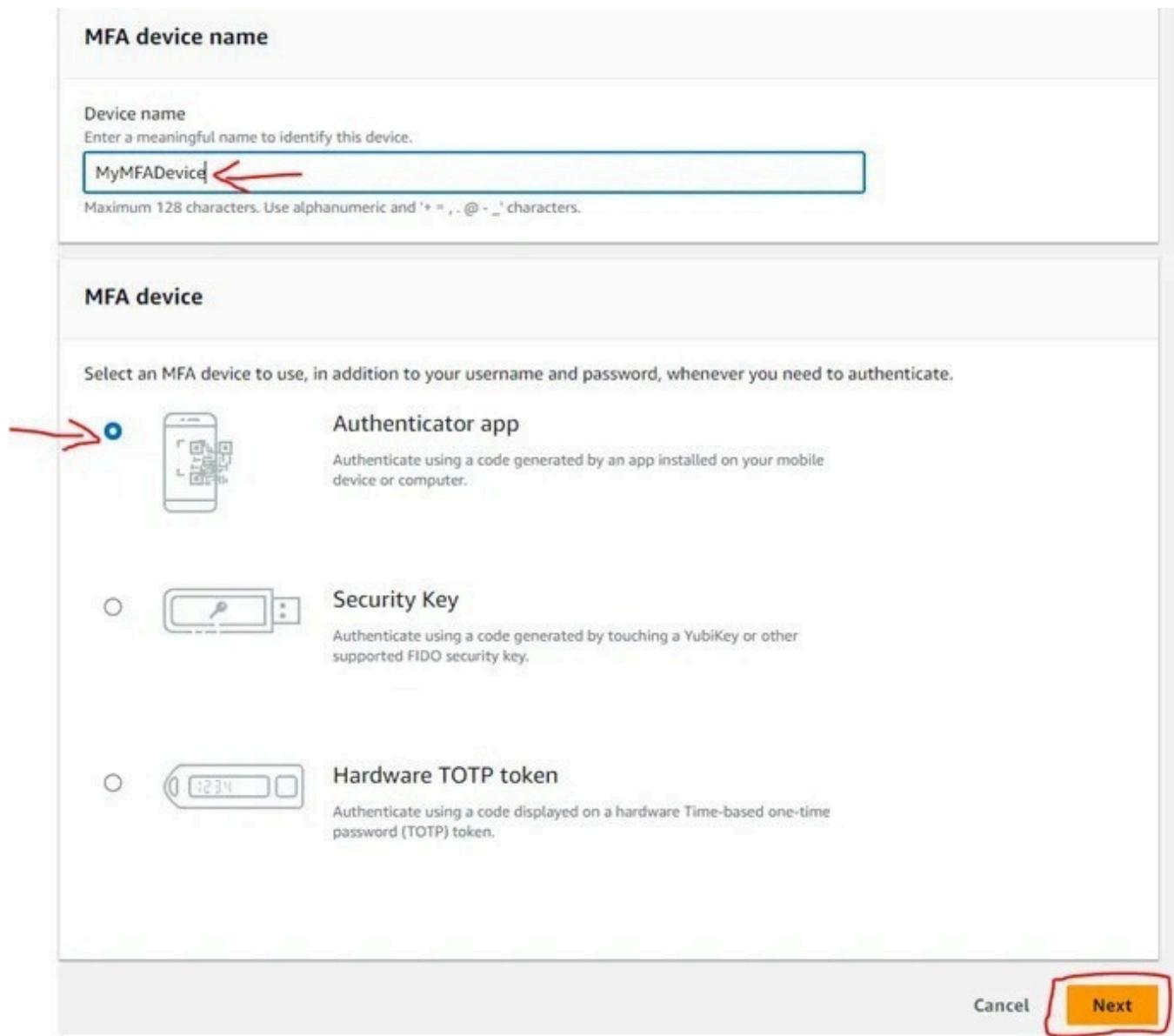
2. Choose Users in the left navigation pane and select “Administrator”.
Click the link to open it.



3. Click Enabled without MFA and click Enable MFA.



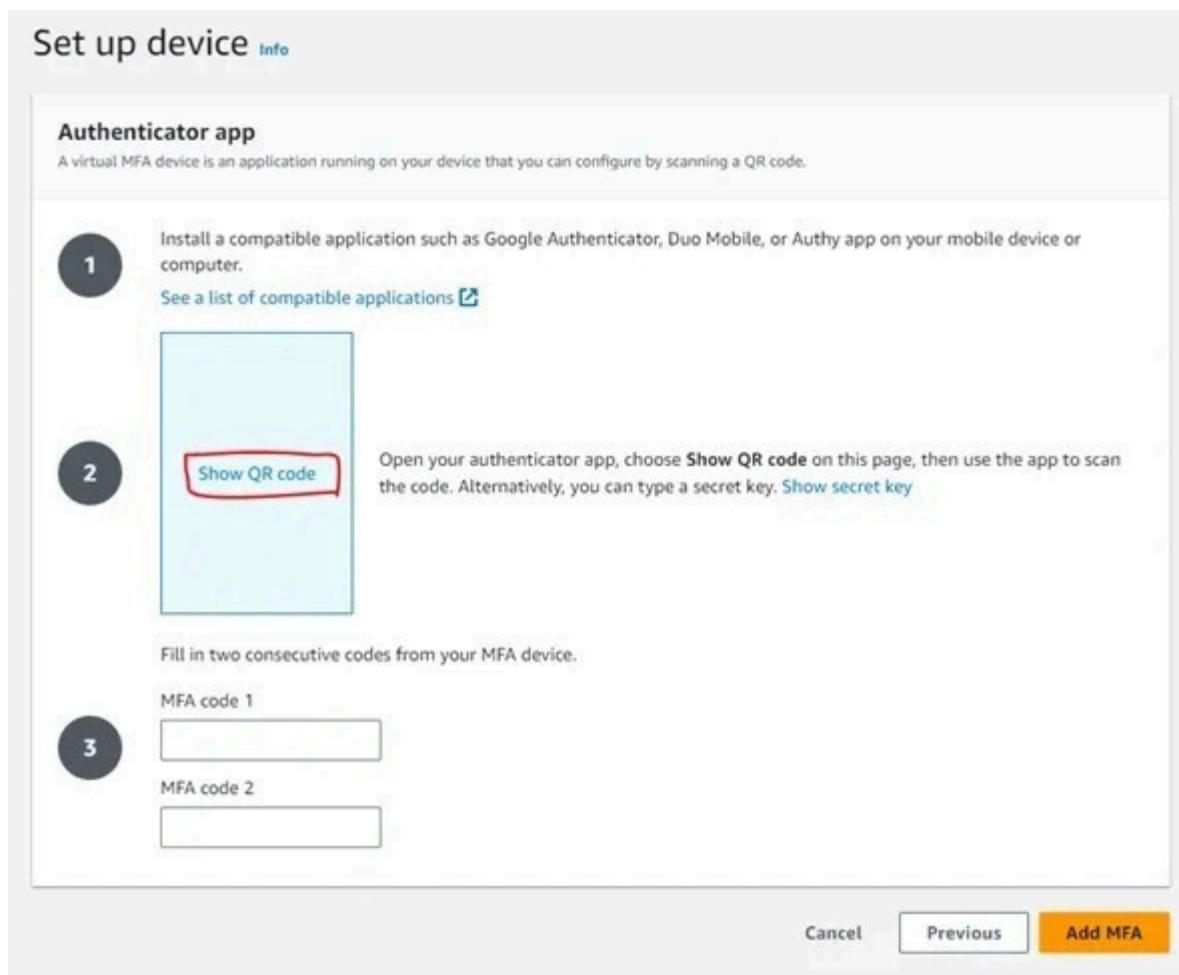
4. When the MFA wizard opens give your device a name such as MyMFADevice. Select Authenticator app and click Next.



5. The console displays info for the virtual MFA device. This is when you'll add an account on the authenticator app on your device. By now you should've installed the Authy app on your phone. From it you'll get a QR code for the next step. If you've not yet installed the app, please go ahead and do so.

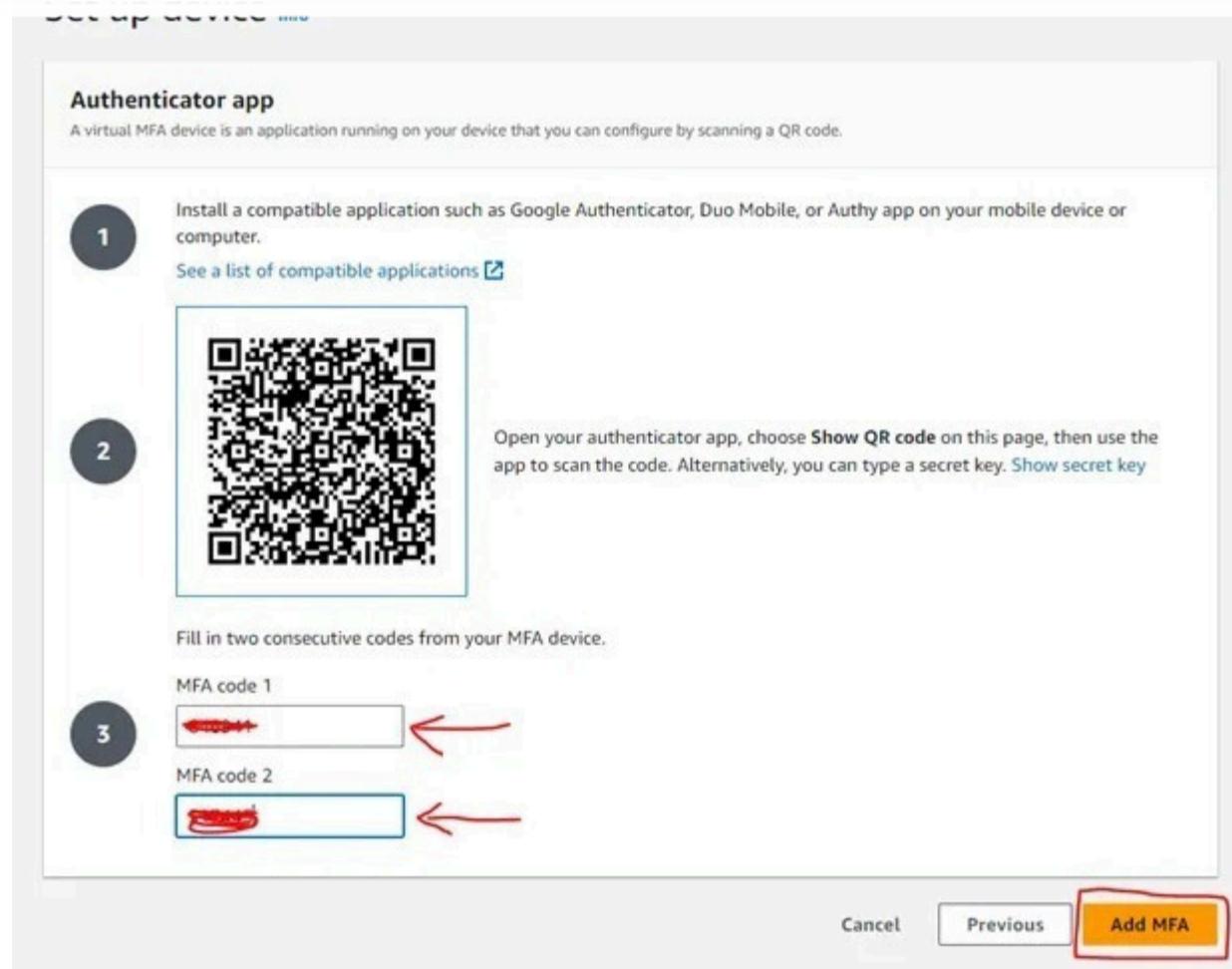
6. Open the Authy app on your device. You can add an account and select the QR code option.

7. Click on Show QR Code on the MFA wizard and then use the app to scan the QR code.



8. Once you scan the QR code, the app will start generating one-time passcodes. Use these codes to fill in the MFA code 1 and code 2 boxes with two consecutive codes. Get the first one then wait for 30 seconds to get the next. Once that's done. Click “Add MFA.”



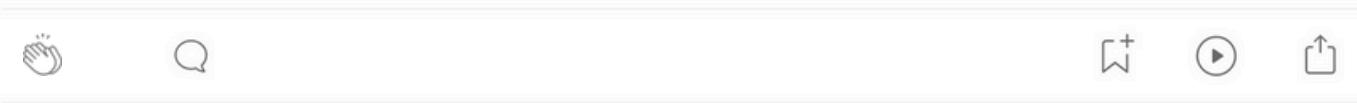


You'll get the confirmation that MFA is enabled for the user

To test it, simply logout and log back in with this same “Administrator” user. After entering your credentials, you’ll be prompted to enter a one-time passcode. Open the Authy app and copy the code provided. The app generates codes every 30 seconds.

That's it for this lab. I hope you were enriched. We learned how to create an IAM user with administrator privileges and further secure it by enabling MFA. This is a good introduction to the AWS IAM service. Thank you for reading and see you at the next one.

Creating IAM Users and Groups on AWS – A Step-by-Step Guide



Let's kick things off with a quick overview, shall we?

What is identity and access management (IAM)?

Identity and Access Management (IAM), also known as Identity Management, plays a vital role in securing cloud resources by managing user identities and controlling their access. It acts like a vigilant bouncer at a nightclub entrance, checking the guest list and granting access to the VIP areas only to authorized individuals.

Why even IAM is important?

IAM plays a vital role in keeping data safe and secure while enhancing overall efficiency. Here are the key reasons why IAM matters:

1. Keeping Data Safe: IAM protects sensitive data from hackers and unauthorized people. It uses strong security measures like passwords and extra verification steps to make sure only the right people can access the data.
2. Making Things Easier: IAM makes it easy for employees to access the things they need quickly. This helps them work faster and saves time by avoiding long access requests.
3. Following Rules: Businesses must follow rules about data protection. IAM helps them meet these rules by controlling who can access data and keeping records of who does.
4. Organizing Access: IAM manages who has access to what in an organized way. It ensures that each person only gets the access they need for their job, reducing the risk of insider issues.

What is an IAM User?

IAM users are like representatives for people or applications using AWS. They can access AWS through the console or programmatically. IAM users help manage access to AWS resources securely, and you can set permissions for them individually or in groups.

They have names and passwords for console access and can create access keys for programmatic access. IAM users ensure only authorized users and apps can access your AWS resources.

What are IAM Groups?

An IAM group is a collection of users who are grouped together based on the same access control policies. These policies define what actions the group members are allowed to perform on specific objects within the group's scope.

For example, let's say you have a group called "Developers." In the group's access control policy, you grant read-only access to all of your EC2 instances. Now, any user added to the "Developers" group will automatically have the permission to view information about those EC2 instances, but they won't have permission to make any changes to them.

Step-by-Step Guide

Here is a step-by-step guide for creating IAM groups and users.

STEP 1: Signing into your AWS account as a root user.

aws

Sign in

Root user
Account owner that performs tasks requiring unrestricted access. Learn more

IAM user
User within an account that performs daily tasks. Learn more

Root user email address

Next

By continuing, you agree to the AWS Customer Agreement or other agreement for AWS services, and the Privacy Notice. This site uses essential cookies. See our Cookie Notice for more information.

New to AWS?

[Create a new AWS account](#)

Build event-driven architectures on AWS

Take a deep dive into how EDAs help organizations increase agility and build reliable, scalable applications

[Download the guide](#)



aws Services Search [Alt+S] Stockholm ayushranjan

Console Home [Info](#)

Recently visited [Info](#)

- [Billing](#)
- [EC2](#)

[View all services](#)

Reset to default layout [+ Add widgets](#)

Welcome to AWS

- [Getting started with AWS](#) Get started
Learn the fundamentals and find valuable information to get the most out of AWS.
- [Training and certification](#) Get certified
Learn from AWS experts and advance your skills and knowledge.
- [What's new with AWS?](#) View news
Discover new AWS services, features, and Regions.

CloudShell Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

STEP 2: Search for IAM in search bar.

The screenshot shows the AWS search interface with the query 'IAM'. The results are categorized into 'Services' and 'Features'. Under 'Services', there are links to IAM, IAM Identity Center, Resource Access Manager, and Serverless Application Repository. Under 'Features', there are links to Billing, EC2, and other AWS services. The sidebar on the left shows recent activity including Billing and EC2.

You can see the IAM dashboard as below.

The screenshot shows the AWS IAM Dashboard. The left sidebar is collapsed, showing 'Access management' with 'User groups' selected. The main area displays 'IAM resources' with counts: User groups (0), Users (1), Roles (2), Policies (0), and Identity providers (0). Below this is a 'What's new' section listing recent updates. On the right, there are sections for 'AWS Account' (Account ID and Alias), 'Quick Links' (My security credentials), and 'Tools' (Policy simulator and Web identity federation playground).

STEP 3: Click on Create Group button.

The screenshot shows the AWS Identity and Access Management (IAM) console. The left sidebar is titled 'Identity and Access Management (IAM)' and includes sections for Dashboard, Access management (User groups, Users, Roles, Policies, Identity providers, Account settings), and Access reports (Access analyzer, Archive rules, Analyzers, Settings, Credential report, Organization activity, Service control policies (SCPs)). The main content area is titled 'User groups (0) Info' and contains a message: 'A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.' Below this is a search bar labeled 'Filter User groups by property or group name and press enter'. A table header row includes columns for 'Group name', 'Users', 'Permissions', and 'Creation time'. A message at the bottom of the table says 'No resources to display'. At the top right of the main area is a 'Create group' button.

STEP 4: Write the name you want to give to User Group.

The screenshot shows the 'Create user group' page within the AWS IAM console. The left sidebar is identical to the previous screenshot. The main form has a 'Name the group' section with a text input field containing 'ayushadmin'. Below it is a 'Add users to the group - Optional (1) Info' section, which lists a single user 'ayushadmin' with a checkbox next to it. The 'Attach permissions policies - Optional (869) Info' section shows a search bar with the filter 'AdministratorAccess' applied, resulting in 4 matches. A 'Create policy' button is also present in this section.

STEP 5: Please select the desired permissions in the permission section. In this case, I have granted administrator access.

Add users to this group - Optional (1) info

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 user can belong to up to 10 groups.

User name	Groups	Last activity	Creation time
ayushadmin	0	None	1 month ago

Attach permissions policies - Optional (Selected 1/869) Info

You can attach up to 10 policies to this user group. All the users in this group will have permissions that are defined in the selected policies.

Policy name	Type	Description
<input checked="" type="checkbox"/> AdministratorAccess	AWS managed - job function	Provides full access to AWS services and resources.
<input type="checkbox"/> AdministratorAccess-Amplify	AWS managed	Grants account administrative permissions while explicitly allowing direct ac...
<input type="checkbox"/> AWSAuditManagerAdministratorAccess	AWS managed	Provides administrative access to enable or disable AWS Audit Manager, upd...
<input type="checkbox"/> AdministratorAccess-AWSxElasticBeanstalk	AWS managed	Grants account administrative permissions. Explicitly allows developers and a...

Create group

Then click on create group.

ayushadmin user group created.

Group name	Users	Permissions	Creation time
ayushadmin	ayushadmin	Defined	Now

Create group

STEP 6: To create a new user, navigate to the User section located below the User Group section and select the "Add Users" option.

The screenshot shows the AWS Identity and Access Management (IAM) service interface. On the left, there's a navigation sidebar with sections like 'Access management', 'Access reports', and 'Related consoles'. The main area is titled 'Users (1) Info' and contains a table with one row for 'ayushadmin'. The table columns include 'User name', 'Groups', 'Last activity', 'MFA', 'Password age', and 'Active key age'. A green 'Add users' button is located at the top right of the table area.

STEP 7: Please enter the desired username for the user and select the option "Provide user access to AWS Management Console". Then, choose the option "I want to create an IAM User" and select "Autogenerated Password".

This screenshot shows the second step of the 'Create New IAM User' wizard. The 'User details' section is highlighted. It includes fields for 'User name' (set to 'ayushadmin'), 'Provide user access to the AWS Management Console' (checkbox checked), and 'Are you providing console access to a person?' (radio button selected for 'Want to create an IAM user'). Below this, the 'Console password' section is shown, with 'Autogenerated password' selected. At the bottom, there are notes about generating programmatic access and a 'Next Step' button.

Select the Group Name under which you want to create the User.

Set permissions

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

Permissions options

Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.

Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

User groups (1/1)

Group name	Users	Attached policies	Created
ayushadmin	0	AdministratorAccess	2023-08-07 (3 days ago)

Set permissions boundary - optional

Cancel Previous Next

Then click on Create User.

Review and create

Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.

User details

User name	ayushranjan	Console password type	Autogenerated	Require password reset	Yes
-----------	-------------	-----------------------	---------------	------------------------	-----

Permissions summary

Name	Type	Used as
ayushadmin	Group	Permissions group
IAMUserChangePassword	AWS managed	Permissions policy

Tags - optional

Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

No tags associated with the resource.

Add new tag

You can add up to 50 more tags.

Cancel Previous Create user

The screenshot shows the AWS IAM 'Create user' interface. At the top, a green banner indicates 'User created successfully'. The main area is titled 'Console sign-in details' and shows the following information:

- Console sign-in URL: [REDACTED]
- User name: ayushranjan
- Console password: [REDACTED] [Show](#)

At the bottom right are two buttons: 'Download .csv file' and 'Return to users list'.

STEP 8 : Please sign out and then attempt to sign in using your IAM user credentials.

The screenshot shows the AWS sign-in page. The left side displays the sign-in form with the following fields:

- Root user
- IAM user
- Account ID (12 digits) or account alias: ayushranjan

A blue 'Next' button is at the bottom of the form. Below it, a small note states: "By continuing, you agree to the AWS Customer Agreement or other agreement for AWS services, and the Privacy Notice. This site uses essential cookies. See our Cookie Notice for more information." A 'New to AWS?' link is also present.

To the right of the sign-in form is a promotional banner for AWS infrastructure:

INFRASTRUCTURE
Optimize cloud infrastructure costs and accelerate application innovation

Learn more >

Then it will ask to create new password as we autogenerated password

You must change your password to continue

AWS account [REDACTED]

IAM user name ayushranjan

Old password [REDACTED]

New password [REDACTED]

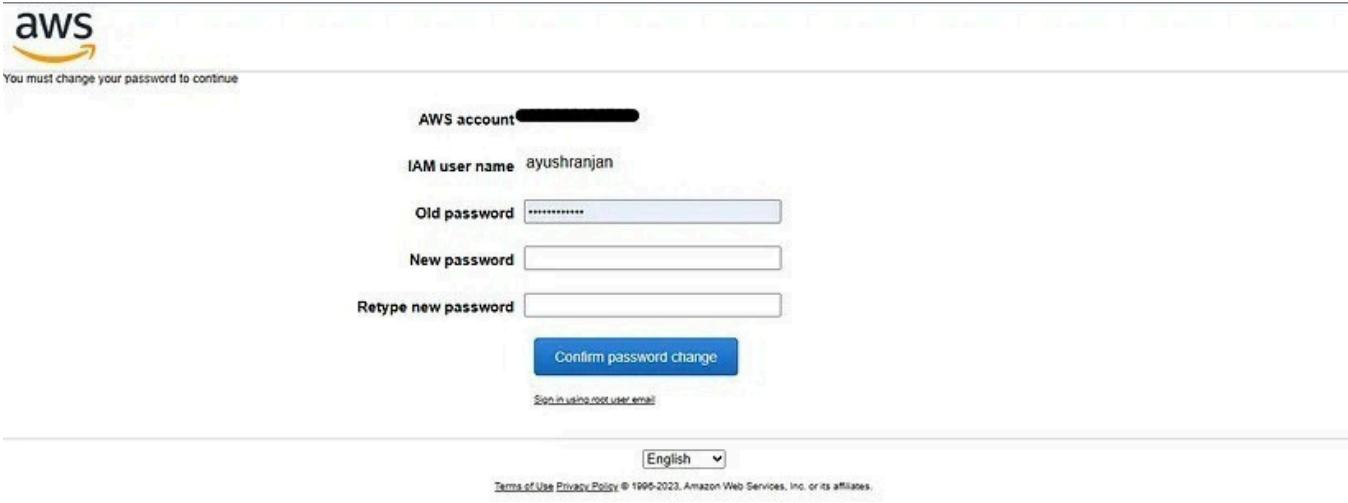
Retype new password [REDACTED]

[Confirm password change](#)

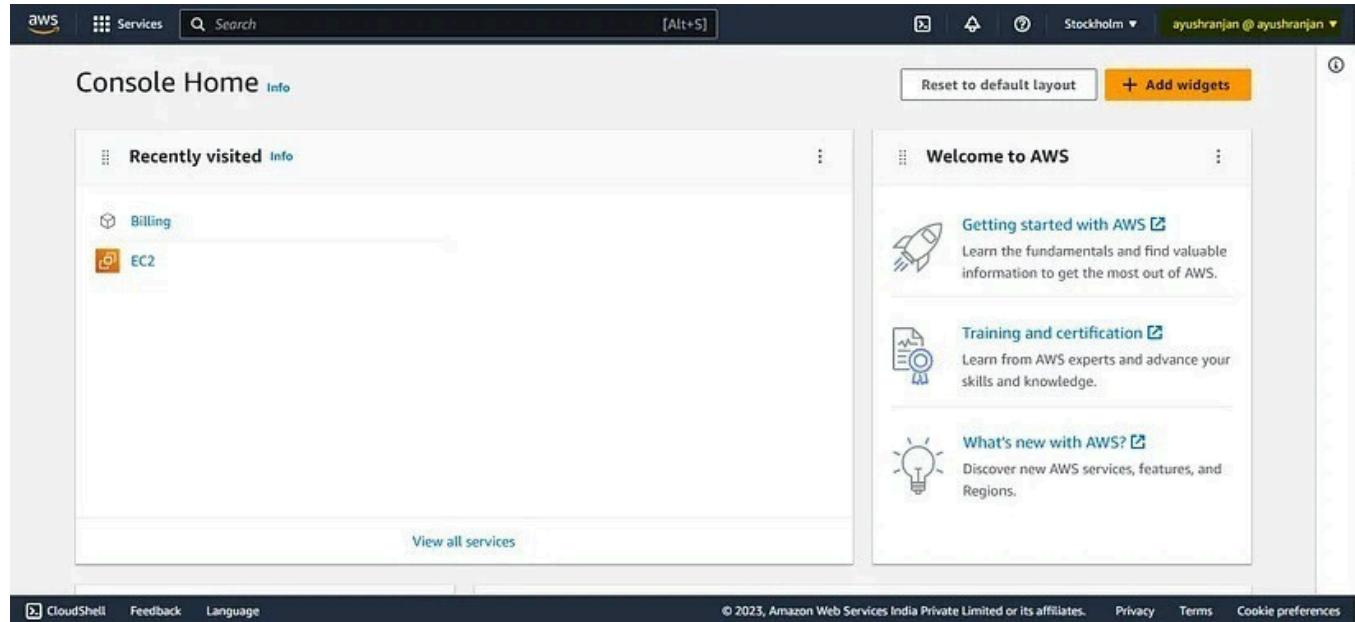
[Sign in using root user email](#)

English ▾

Terms of Use Privacy Policy © 1996-2023, Amazon Web Services, Inc. or its affiliates.

A screenshot of the AWS IAM password change interface. It shows fields for Old password, New password, and Retype new password. A 'Confirm password change' button is at the bottom. Below the form is a link to sign in using a root user email and a language selection dropdown set to English.

Congratulations, you have successfully created a new user group and added a new user to your AWS account. You can now access the AWS Home Console.

A screenshot of the AWS Home Console. The top navigation bar includes 'Services', a search bar, and a user dropdown for 'ayushranjan @ ayushranjan'. The main area has two columns. The left column, 'Recently visited', lists 'Billing' and 'EC2'. The right column, 'Welcome to AWS', features three sections: 'Getting started with AWS' (with a rocket icon), 'Training and certification' (with a person icon), and 'What's new with AWS?' (with a lightbulb icon). At the bottom, there are links for 'View all services', 'CloudShell', 'Feedback', 'Language', and copyright information.

Summary

The article discusses creating IAM (Identity and Access Management) users and groups on AWS through a step-by-step guide. IAM is crucial for securing

CREATE ROLE

The screenshot shows the AWS Identity and Access Management (IAM) service interface. The URL in the browser is <https://us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#roles>. The top navigation bar includes the AWS logo, Services, a search bar, and user information for 'rahulwagh'. The main left sidebar under 'Identity and Access Management (IAM)' has a 'Search IAM' field and a tree view with 'Dashboard', 'Access management' (which is expanded), 'Users' (with a red circle around it), and 'Roles' (also with a red circle around it). The 'Roles' link is highlighted with a red circle. The main content area shows the 'Roles' page with a header 'Roles Info' and a description: 'An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.' It features a search bar, a table with columns 'Role name' and 'Trusted entities', and a 'Create role' button.

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

IAM > Roles

Roles (27) Info

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

Search

< 1 2 >

Role name

▲ Trusted entities

[AWS Service Role For Amazon EKS](#)

AWS Service: eks (Service-Linked Role)

[AWS Service Role For Amazon EKS Nodegroup](#)

AWS Service: eks-nodegroup (Service-Linked Role)

[AWS Service Role For Amazon FSx](#)

AWS Service: fsx (Service-Linked Role)

Create Role





Services

Search

[Option+S]



Global ▾



Step 2

Add permissions

Step 3

Name, review, and create

Trusted entity type

AWS service

Allow AWS services like EC2, Lambda, or other services to perform actions in this account.

AWS account

Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

Web identity

Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

SAML 2.0 federation

Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

Custom trust policy

AWS service

Allow AWS services like EC2, Lambda, or others to perform actions in this account.

AWS account

Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

Web identity

Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

SAML 2.0 federation

Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

Custom trust policy

Create a custom trust policy to enable others to perform actions in this account.

Use case

Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Service or use case

Choose a service or use case

Cancel

Next

external web identity provider to assume this role to perform actions in this account.

a corporate directory to perform actions in this account.

Custom trust policy

Create a custom trust policy to enable others to perform actions in this account.

Use case

Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Service or use case

S3



Choose a use case for the specified service.

Use case

S3

Allows S3 to call AWS services on your behalf.

S3 Batch Operations

Allows S3 Batch Operations to call AWS services on your behalf.

Cancel

Next



<input type="checkbox"/>	 AmazonAPIGatewayFullAccess	AWS managed	Provides full access to create/edit/delete APIs, invoke APIs, and push logs to CloudWatch Logs.	
<input type="checkbox"/>	 AmazonAPIGatewayInvokeAccess	AWS managed	Provides full access to invoke APIs in Amazon API Gateway.	
<input type="checkbox"/>	 AmazonAPIGatewayLogDeliveryAccess	AWS managed	Allows API Gateway to push logs to user-defined CloudWatch Logs log groups.	
<input type="checkbox"/>	 AmazonAppFlowFullAccess	AWS managed	Provides full access to Amazon AppFlow.	
<input type="checkbox"/>	 AmazonAppFlowReadOnlyAccess	AWS managed	Provides read only access to Amazon AppFlow.	
<input type="checkbox"/>	 AmazonAppStreamFullAccess	AWS managed	Provides full access to Amazon AppStream.	
<input type="checkbox"/>	 AmazonAppStreamReadOnlyAccess	AWS managed	Amazon AppStream 2.0 access to AWS Lambda.	
<input type="checkbox"/>	 AmazonAppStreamDefaultPolicy	AWS managed	Provides read only access to Amazon AppStream.	
<input type="checkbox"/>	 AmazonAthenaFullAccess	AWS managed	Provide full access to Amazon Athena.	
<input type="checkbox"/>	 AmazonAugmentedRealityFullAccess	AWS managed	Provides access to perform all operations on Amazon Augmented Reality.	

► Set permissions boundary - *optional*

[Cancel](#)

[Previous](#)

[Next](#)

Role details

enter role name

Role name

Enter a meaningful name to identify this role.

allow-s3-access

Maximum 64 characters. Use alphanumeric and '+-=.,@-_-' characters.

Description

Add a brief description for this role.

Allows S3 to call AWS services on your behalf.

Maximum 1000 characters. Use letters (A-Z and a-z), numbers (0-9), tabs, new lines, or any of the following characters: _+=-, @-/\{()\}!#\$%^&*()~<>`

Step 1: Select trusted entities

Edit

Trust policy

```
1 - {  
2     "Version": "2012-10-17",  
3     "Statement": [  
4         {
```

12 }

①

②

Step 2: Add permissions

[Edit](#)

Permissions policy summary

Policy name **Type****Attached as**

Step 3: Add tags

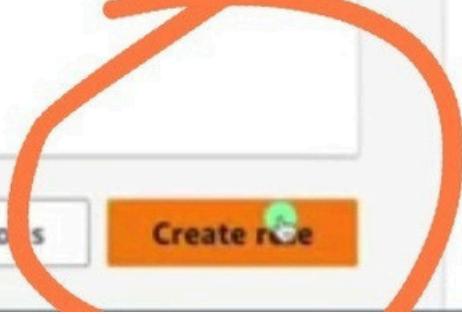
Add tags - *optional* [Info](#)

Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

[Add new tag](#)

You can add up to 50 more tags.

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

role is created but
it has no policy

View role

Roles (28) [Info](#)

Create role

An AWS role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

Search

< 1 2 > ⌂

<input type="checkbox"/>	Role name	▲ Trusted entities
<input type="checkbox"/>	AWSServiceRoleForAmazonEKSNodegroup	AWS Service: eks-nodegroup (Service-Linked Role)
<input type="checkbox"/>	AWSServiceRoleForAmazonFSx	AWS Service: fsx (Service-Linked Role)
<input type="checkbox"/>	AWSServiceRoleForApplicationAutoScaling_DynamoDBTable	AWS Service: dynamodb.application-autoscaling (Service-Linked Role)
<input type="checkbox"/>	AWSServiceRoleForAutoScaling	AWS Service: autoscaling (Service-Linked Role)
<input type="checkbox"/>	AWSServiceRoleForCloudTrail	AWS Service: cloudtrail (Service-Linked Role)
<input type="checkbox"/>	AWSServiceRoleForEc2InstanceConnect	AWS Service: ec2-instance-connect (Service-Linked Role)
<input type="checkbox"/>	AWSServiceRoleForEC2Spot	AWS Service: spot (Service-Linked Role)
<input type="checkbox"/>	AWSServiceRoleForECS	AWS Service: ecs (Service-Linked Role)

Role allow-s3-access created.

[View role](#)

Roles (28) [Info](#)

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

Q, allow

X 1 match

C

Delete

Create role

Role name

[allow-s3-access](#)

click this role

Trusted entities

AWS Service: s3

Roles Anywhere [Info](#)

[Manage](#)

Authenticate your non AWS workloads and securely provide access to AWS services.



Access AWS from your non AWS workloads

Operate your non AWS workloads using



X.509 Standard

Use your own existing PKI infrastructure or use [AWS Certificate Manager](#)



Temporary credentials

Use temporary credentials with ease and benefit from the enhanced security

April 13, 2024, 22:32 (UTC+02:00)

arn:aws:iam::242396018804:role/allow-s3-access

Last activity

Maximum session duration

1 hour

Permissions

Trust relationships

Tags

Access Advisor

Revoke sessions

Permissions policies (0) Info

You can attach up to 10 managed policies.



Simulate

Remove

Add permissions

Filter by Type

All types

Search

Policy name

Type

Attached entities

No resources to display

you can see no policy is created

▶ Permissions boundary (not set)

**now we need to
create policy**

The screenshot shows the AWS Identity and Access Management (IAM) service dashboard. In the top left, there's a sidebar with a search bar and navigation links for 'Dashboard', 'Access management' (which is expanded), 'User groups', 'Users', 'Roles', and 'Policies'. A large orange arrow points from the word 'Policies' towards the main content area. The main content area has a breadcrumb trail 'IAM > Dashboard' and a title 'IAM Dashboard'. Below this is a section titled 'Security recommendations' with a red notification badge showing '2'. Two items are listed: 'Add MFA for root user' and 'Deactivate or delete access keys for root user'. Each item has a corresponding button: 'Add MFA' and 'Manage access keys'. A large pink overlay text 'click on policy button' is placed over the 'Policies' link in the sidebar.

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

IAM > Dashboard

IAM Dashboard

Security recommendations 2

⚠️ Add MFA for root user

Add MFA for root user - Enable multi-factor authentication (MFA) for the root user to improve security for this account.

⚠️ Deactivate or delete access keys for root user

Deactivate or delete the access keys for the root user. Instead, use access keys attached to an IAM user to improve security.

Add MFA

Manage access keys

click on policy button

Policies (1191) Info

A policy is an object in AWS that defines permissions.

Filter by Type

Search

All types



Actions

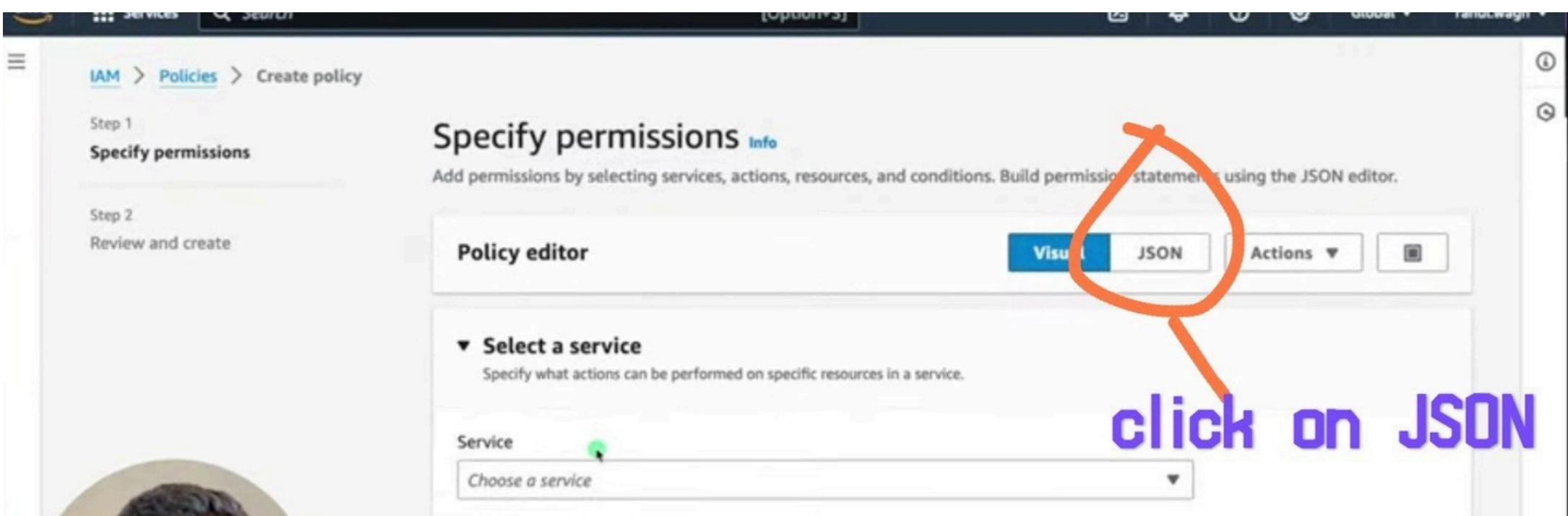
Delete

Create policy



< 1 2 3 4 5 6 7 ... 60 > ⌂

Policy name	Type	Used as	Description
AccessAnalyzerServiceRolePolicy	AWS managed	None	Allow Access Analyzer to analyze resources
AdministratorAccess	AWS managed - joined	Permissions policy	Provides full access to AWS service
AdministratorAccess	AWS managed	None	Grants account administrative permission
AdministratorAccess	AWS managed	None	Grants account administrative permission
AlexaForBusinessDeviceSetup	AWS managed	None	Provide device setup access to Alexa
AlexaForBusinessFullAccess	AWS managed	None	Grants full access to AlexaForBusiness
AlexaForBusinessFunctionExecution	AWS managed	None	Provide execution access to Alexa



e policy

Specify permissions Info

Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

Policy editor

Visual **JSON** Actions ▾

```
1 * {
2     "Version": "2012-10-17",
3     "Statement": [
4         {
5             "Sid": "AllowS3Access",
6             "Effect": "Allow",
7             "Action": "s3:*",
8             "Resource": "*"
9         }
10    ]
11 }
```

Edit statement [AllowS3Access](#) [Remove](#)

Add actions

Choose a service

Filter services

Included

S3

Available

AMP

API Gateway

API Gateway V2

The screenshot shows the AWS IAM Policy Editor interface. On the left, there's a code editor window displaying a JSON policy document. The policy defines a single statement that allows all actions on all S3 resources. On the right, there's a sidebar with tabs for 'Edit statement', 'Actions', and 'Services'. Under 'Edit statement', the 'AllowS3Access' statement is listed with a 'Remove' button. Below it, there's a section for adding actions with a 'Choose a service' dropdown and a 'Filter services' input field. The 'Included' section lists 'S3'. The 'Available' section lists 'AMP', 'API Gateway', and 'API Gateway V2'.

step 1 configure JSON

```
10      ]  
11  }
```

Included

S3



Available

AMP

API Gateway

API Gateway V2

ASC

Access Analyzer

Account

Activate

Alexa for Business

Add a resource

Add

Add a condition (optional)

Add

+ Add new statement

JSON Ln 9, Col 3

6034 of 6144 characters remaining

Security: 0

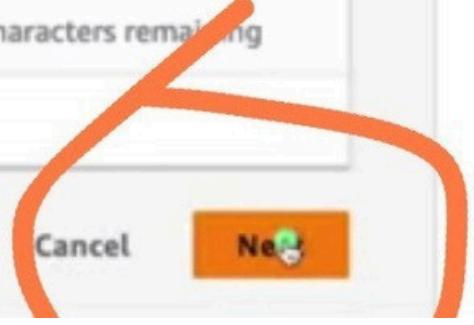
Errors: 0

Warnings: 0

Suggestions: 0

Cancel

Next



policy



Review and create [Info](#)

Review the permissions, specify details, and tags.

Policy details

Policy name

Enter a meaningful name to identify this policy.

custom-s3-allow

Maximum 128 characters. Use alphanumeric and '+,.,@-_-' characters.

Description - optional

Add a short explanation for this policy.

Maximum 1,000 characters. Use alphanumeric and '+,.,@-_-' characters.

Permissions defined in this policy [Info](#)

Edit

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it.

put name of policy

Permissions defined in this policy Info

[Edit](#)

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it.

 Search**Allow (1 of 408 services)** Show remaining 407 services

Service	▲ Access level	▼ Resource	Request cc
S3	Full access	All resources	None

Add tags - optional Info

Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

[Add new tag](#)

You can add up to 50 more tags.

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

✓ Policy custom-s3-allow created.

[View policy](#)

IAM > Policies



policy is created

Policies (1192) [Info](#)



Actions ▾

Delete

Create policy

A policy is an object in AWS that defines permissions.

Filter by Type

Search

All types ▾

< 1 2 3 4 5 6 7 ... 60 > ⌂

Policy name

Type

Used as

Description

<input type="radio"/>	<input checked="" type="checkbox"/> AccessAnalyzerSer...	AWS managed	None	Allow Access Analyzer to analyze re...
<input type="radio"/>	<input checked="" type="checkbox"/> AdministratorAccess	AWS managed - jo...	Permissions policy ...	Provides full access to AWS service
<input type="radio"/>	<input checked="" type="checkbox"/> AdministratorAcce...	AWS managed	None	Grants account administrative perr...
<input type="radio"/>	<input checked="" type="checkbox"/> AdministratorAcce...	AWS managed	None	Grants account administrative perr...
<input type="radio"/>	<input checked="" type="checkbox"/> AlexaForBusinessD...	AWS managed	None	Provide device setup access to Alex...
<input type="radio"/>	<input checked="" type="checkbox"/> AlexaForBusinessF...	AWS managed	None	Grants full access to AlexaForBusin...
<input type="radio"/>	<input checked="" type="checkbox"/> AlexaForBusinessG...	AWS managed	None	Provide gateway execution access t...

Till now we created a role
and created policy

.....

Now

I am attaching policy to the role

The screenshot shows the AWS IAM Roles page. On the left, there's a sidebar with a color palette header and several navigation items under 'Access management': 'User groups' (with a note 'click on role'), 'Roles' (circled in orange), 'Identity providers', and 'Account settings'. Under 'Access reports', there are 'Access Analyzer', 'External access', 'Unused access', and 'Analyzer settings'. The main content area has a search bar at the top with 'Q: allow' and a result count '1 match'. Below it, a table lists roles. The first row, 'allow-s3-access', is circled in orange. To the right of the table, there's a section titled 'Roles Anywhere' with three options: 'Access AWS from your non AWS workloads', 'X.509 Standard', and 'Temporary credentials'.

click on created role

Role Name	Trusted entities	AWS Service
allow-s3-access	s3	s3

Last activity

Maximum session duration

1 hour

Permissions

Trust relationships

Tags

Access Advisor

Revoke sessions

Permissions policies (0) Info

You can attach up to 10 managed policies.



Simulate

Remove

Add permissions

Attach policies

Create inline policy

Search

Filter by Type

click Attach policy

Policy name

Type

Attached entities

No resources to display

▶ Permissions boundary (not set)

▼ Generate policy based on CloudTrail events

Filter by type

custom All types 6 matches < 1 > ⚙

Policy name	Type	Description
AmazonRDSCustomInstanceProfileRolePo...	AWS managed	Allows Amazon RDS Custom to perfor...
AmazonRekognitionCustomLabelsFullAccess	AWS managed	This policy specifies rekognition and s...
AWSCodePipelineCustomActionAccess	AWS managed	Provides access for custom actions to ...
AWSElasticBeanstalkCustomPlatformforE...	AWS managed	Provide the instance in your custom pl...
AWSElasticBeanstalkManagedUpdatesCus...	AWS managed	This policy is for the AWS Elastic Beans ...
<input checked="" type="checkbox"/> custom-s3-allow	Customer managed	-

select the policy which you created previously

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

Add permissions

The screenshot shows the AWS IAM console interface. On the left, there's a sidebar with navigation links: Access management (User groups, Users, Roles, Policies, Identity providers, Account settings), and Access reports. The main area is titled "policy attached to the role" and shows a success message: "Policy was successfully attached to role." Below this, there are tabs for Permissions, Trust relationships, Tags, Access Advisor, and Revoke sessions. Under the Permissions tab, it says "Permissions policies (1) Info". A note states: "You can attach up to 10 managed policies." There are buttons for Refresh, Simulate, Remove, and Add permissions. A search bar and a filter for "All types" are also present. A table lists one policy: "Policy name" (custom-s3-allow), "Type" (Customer managed), and "Attached entities" (1). A green arrow points to the "custom-s3-allow" policy name, which is highlighted with a red oval. Another red oval highlights the success message at the top.

[Objects](#)[Properties](#)[Permissions](#)[Metrics](#)[Management](#)[Access Points](#)[Buckets](#)[Access Grants](#)[Access Points](#)[Object Lambda Access Points](#)[Multi-Region Access Points](#)[Batch Operations](#)[IAM Access Analyzer for S3](#)[Block Public Access settings for this account](#)[▼ Storage Lens](#)[Dashboards](#)[Storage Lens groups](#)[AWS Organizations settings](#)[Feature spotlight](#) 7

We were earlier created by the user but doesn't have permission

[Copy S3 URI](#)[Copy URL](#)[Download](#)[Open](#)[Delete](#)[Create folder](#)[Find objects by prefix](#)[Show versions](#)[Name](#)[Type](#)[Last modified](#)[Size](#)**Insufficient permissions to list objects**

After you or your AWS administrator has updated your permissions to allow the s3>ListBucket action, refresh this page.

[Learn more about Identity and access management in Amazon S3](#)

now basically we want to
attach policy to the user

Dashboard

▼ Access management

- User groups
- Users**
- Roles
- Policies
- Identity providers
- Account settings

▼ Access reports

- Access Analyzer
- External access
- Unused access
- Analyzer settings

Identity Center is enabled. We recommend managing workforce users' access to AWS accounts and cloud applications in Identity Center.

Learn more Watch how it works

Users (2)

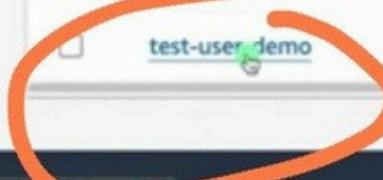
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

<input type="checkbox"/>	User name	Path	Group:	Last activity	MFA	Passw
<input type="checkbox"/>	rahul.dev	/				21
<input type="checkbox"/>	test-user-demo	/				11

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

CloudWatch Metrics <https://us-east-1.console.aws.amazon.com/home?region=us-east-1#users>

click on user



The screenshot shows the AWS IAM Permissions policies page. On the left, there's a navigation sidebar with options like Dashboard, Access management (User groups, Roles, Policies, Identity providers, Account settings), Access reports (Access Analyzer, External access, Unused access, Analyzer settings), and a section for Generate policy based on CloudTrail events.

The main content area is titled "Permissions policies (0)" and contains a message: "Permissions are defined by policies attached to the user directly or through groups." It features a search bar, a "Filter by Type" dropdown set to "All types", and a table header with columns for "Policy name" and "Type". A red arrow points from the text "click on add permission" to the "Add permissions" button in the top right corner of the table header area. Below the table, it says "No resources to display".

click on add permission

Add user to group

Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

Copy permissions

Copy all group memberships, attached managed policies, inline policies, and any existing permissions boundaries from an existing user.

Attach policy

Attach a managed policy to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

select the policy
which you created previously

Permissions policies (1194)

custom

select attach policy

Filter by Type

All types

11 matches

< 1 > ⌂

<input type="checkbox"/>	Policy name	Type	Attached entities
<input type="checkbox"/>	AmazonRDSCustomIns...	AWS managed	0
<input type="checkbox"/>	AmazonRDSCustomPre...	AWS managed	0
<input type="checkbox"/>	AmazonRDSCustomSer...	AWS managed	0
<input type="checkbox"/>	AmazonRekognitionCu...	AWS managed	0

<input type="checkbox"/>	 AmazonRDSCustomer... 	AWS managed	0
<input type="checkbox"/>	 AmazonRDSCustomSer... 	AWS managed	0
<input type="checkbox"/>	 AmazonRekognitionCu... 	AWS managed	0
<input type="checkbox"/>	 AWSApplicationAutoSc... 	AWS managed	0
<input type="checkbox"/>	 AWSCodePipelineCust... 	AWS managed	0
<input type="checkbox"/>	 AWSElasticBeanstalkCu... 	AWS managed	0
<input type="checkbox"/>	 AWSElasticBeanstalkM... 	AWS managed	0
<input type="checkbox"/>	 AWSKeyManagements... 	AWS managed	0
<input checked="" type="checkbox"/>	 custom-s3-allow 	Customer managed	1
<input type="checkbox"/>	 CustomerProfilesServic... 	AWS managed	0

Cancel

Next 

Review

User details

User name
test-user-demo

Permissions summary (1)

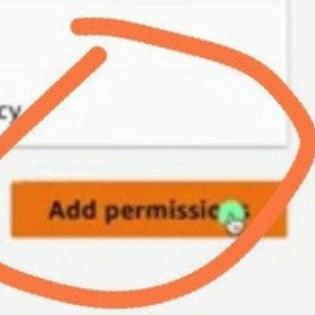
Name	Type	Used as	Permissions policy
custom-s3-allow	Customer managed		

Cancel

Previous

Add permission

< 1 >

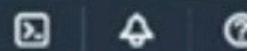




Services

Search

[Option+S]



Identity and Access Management (IAM)

Search IAM

Dashboard

▼ Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

▼ Access reports

Access Analyzer

External access

Unused access

Analyzer settings

1 policy added

April 15, 2024, 22:24 (UTC+02:00)

now successfully
attached the
policy to user

Permissions

Groups

Tags

Security credentials

Access Advisor

Permissions policies (1)

Permissions are defined by policies attached to the user directly or through groups.

Filter by Type

Search

All types

	Policy name	Type	Attached to
<input type="checkbox"/>	custom-s3-allow	Customer managed	Directly

custom-s3-allow

1 - {
2 "Version": "2012-10-17",
3 "Statement": [
4 {
5 "Sid": "AllowS3Access",
6 "Effect": "Allow",

Copy

CloudShell Feedback

© 2024 Amazon Web Services, Inc. or its affiliates.

now go back to the IAM user
now see errors are gone
(we (root user) allowed permission)

successfully attached policy

to IAM user

Amazon S3

Buckets

Access Grants

Access Points

Object Lambda Access Points

Multi-Region Access Points

Batch Operations

IAM Access Analyzer for S3

Block Public Access settings for this account

▼ Storage Lens

Dashboards

Storage Lens groups

AWS Organizations settings

Feature spotlight

7

General purpose buckets

Directory buckets

General purpose buckets (4) [Info](#) [All AWS Regions](#)

User

Copy ARN

Empty

Delete

Create bucket

Buckets are containers for data stored in S3.

Q Find buckets by name

Name	AWS Region	IAM Access Analyzer
dev-proj-1-jenkins-remote-state-bucket-123456	Europe (Ireland) eu-west-1	View analyzer for eu-west-1
dev-proj-1-remote-state-bucket-123456	Europe (Frankfurt) eu-central-1	View analyzer for eu-central-1
dev-proj-vpc-2-private-link-eu-central-1a	Europe (Frankfurt) eu-central-1	View analyzer for eu-central-1
dev-proj-vpc-endpoint-eu-west-1a	Europe (Ireland) eu-west-1	View analyzer for eu-west-1

AWS CLI configuration

Now let's install and configure AWS CLI as shown in the following steps mentioned below:

Step 1. Download and install AWS CLI: Before going to the AWS dashboard, firstly, we have to download the [CLI installer](https://docs.aws.amazon.com/cli/latest/userguide/getting-started-install.html) (<https://docs.aws.amazon.com/cli/latest/userguide/getting-started-install.html>) on the local machine (Windows, macOS, Linux).

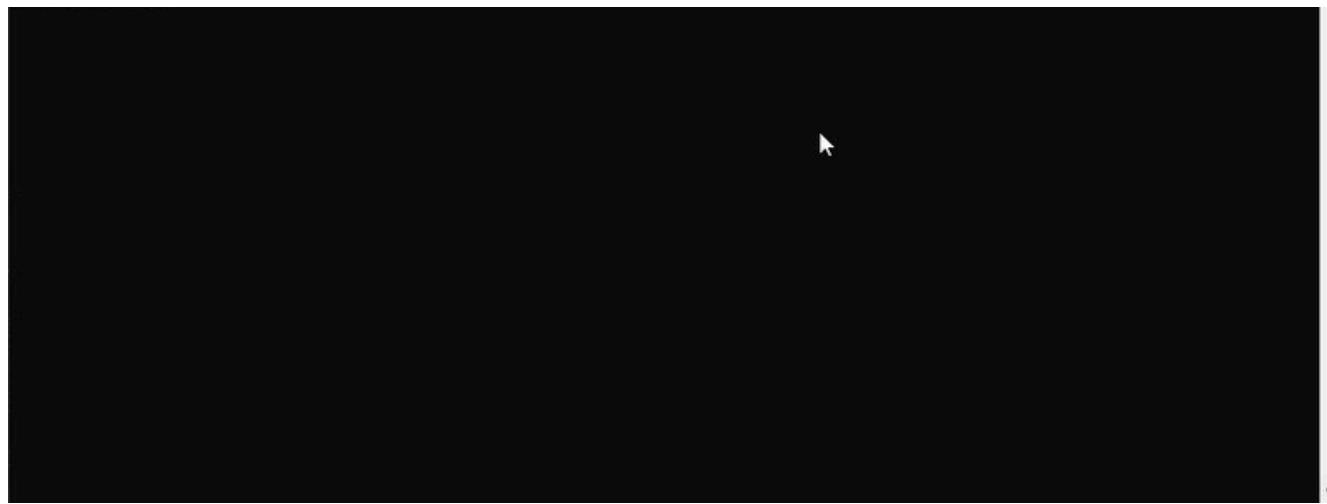
The screenshot shows the AWS Command Line Interface User Guide for Version 2. The left sidebar has sections like 'About the AWS CLI', 'Get started', 'Prerequisites', 'Install/Update', 'Past releases', 'Build and install from source', 'Amazon ECR Public/Docker', 'Setup', 'Configure the AWS CLI', 'Authentication and access credentials', 'Use the AWS CLI', and 'Code examples'. The main content area has a 'Topics' section with 'AWS CLI install and update instructions', 'Troubleshooting AWS CLI install and uninstall errors', and 'Next steps'. Below that is the 'AWS CLI install and update instructions' section, which is highlighted with a red box. It contains three expandable sections: 'Linux', 'macOS', and 'Windows'.

After that, RUN the downloaded MSI installer.

Step 2. Confirm the installation: To confirm the installation process, we must write the command version prompt's command. If the version is displayed, it indicates that CLI is installed, fortunately.

aws --

The screenshot shows a Microsoft Command Prompt window. The title bar says 'Command Prompt'. The window displays the following text:
Microsoft Windows [Version 10.0.19042.867]
(c) 2020 Microsoft Corporation. All rights reserved.
C:\Users\Anupam>aws --version
aws-cli/2.1.37 Python/3.8.8 Windows/10 exe/AMD64 prompt/off
C:\Users\Anupam>



Step 3. Configure AWS CLI: After CLI installation, we have to download the AWS Console access key.

For that, go to My Security Credentials in AWS Console by clicking on UserName on the To right Corner. Now Scroll down and you will find Access keys Click on Create New Access Key, then download the CSV file to the local machine.

The screenshot shows the AWS IAM Access Keys page. On the left, there's a sidebar with navigation links like Dashboard, Access management, Access reports, and Account settings. The main area has a heading 'Access keys (1)'. It displays a table with one row, showing details for an access key. The columns are: Access key ID (with value 'AKIAIOSFODNN7EXAMPLE'), Created on (Now), Access key last used (None), Region last used (N/A), Service last used (N/A), and Status (Active). A red box highlights the 'Create access key' button at the top right of the table.

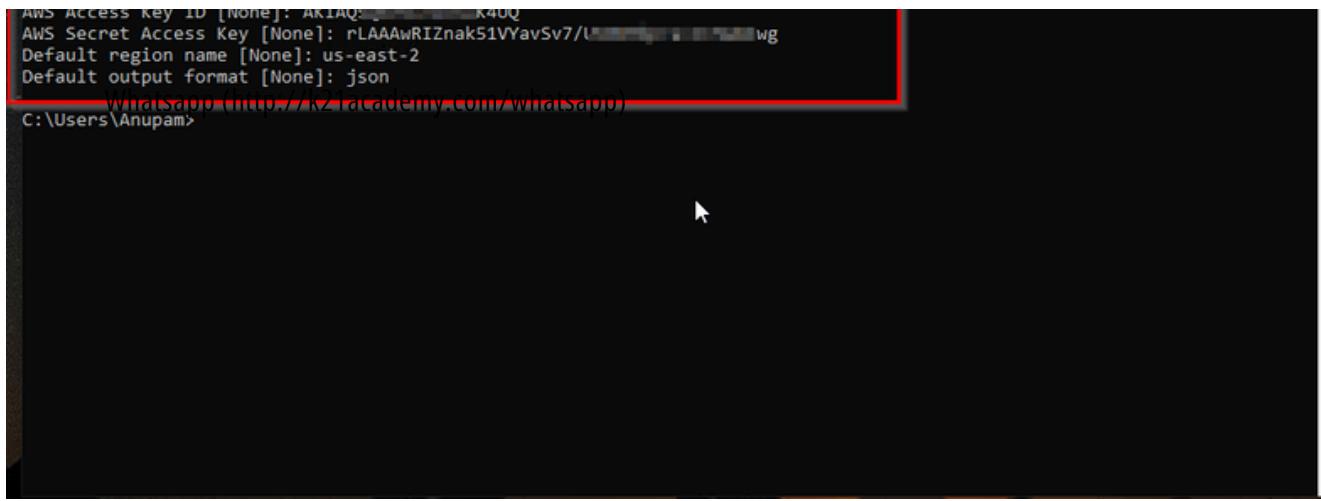
Now we can configure AWS CLI using the command: `aws configure` and fill in details like AWS keys, region, and output format.

1. AWS Access Key ID [None]: ****
 2. AWS Secret access key [None]: ****
 3. Default Region name [None]: us-east-2
- (However, you can choose any region closest to your location)
4. Default output format [None]: JSON

(When we run the command, it's going to split out some output, and there are several different options available, like how you want those outputs printed out. You can get it in JSON, YAML, or text format.)

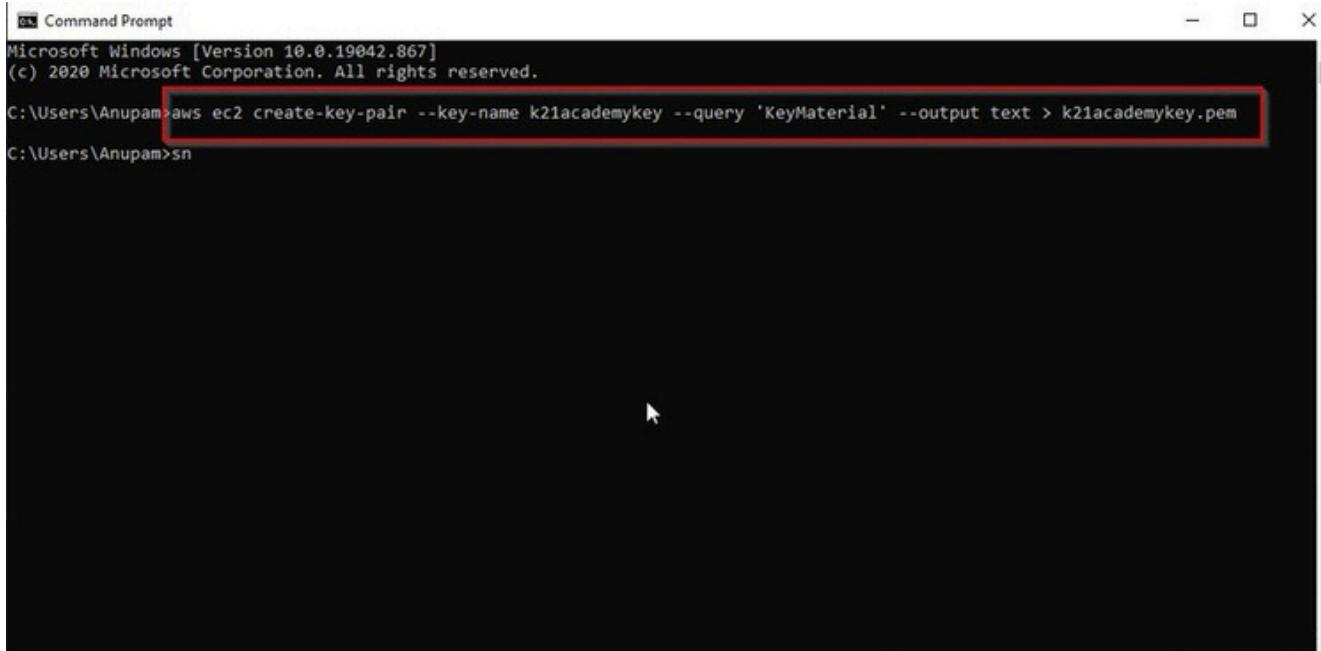
A screenshot of a Windows Command Prompt window titled 'Command Prompt'. The window shows the following text:
Microsoft Windows [Version 10.0.19042.867]
(c) 2020 Microsoft Corporation. All rights reserved.
C:\Users\Anupam>aws --version
aws-cli/2.1.37 Python/3.8.8 Windows/10 exe/AMD64 prompt/off
C:\Users\Anupam>aws configure

The command `aws configure` is highlighted with a red box.



```
AWS Access Key ID [None]: AKIAQ... K4UQ
AWS Secret Access Key [None]: rLAAAwRIznak51VYavSv7/U...
Default region name [None]: us-east-2
Default output format [None]: json
C:\Users\Anupam> www.google.com/whatsapp)
```

Step 4. Create Key Pair through CLI: Now, let's create a key pair with the help of the command :aws ec2
create-key-pair --key-name k21academykey (key pair name) --query 'KeyMaterial'
--output text > k21academykey.pem



```
Command Prompt
Microsoft Windows [Version 10.0.19042.867]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\Anupam>aws ec2 create-key-pair --key-name k21academykey --query 'KeyMaterial' --output text > k21academykey.pem
C:\Users\Anupam>sn
```

This command will create Key pair in a second, similarly to get it to verify, you can write: aws ec2
describe-key-pairs



```
Command Prompt
aws ec2 describe-key-pairs
```

```
Microsoft Windows [Version 10.0.19042.867]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\Anupam>aws ec2 create-key-pair --key-name k21academykey --query 'KeyMaterial' --output text > k21academykey.pem

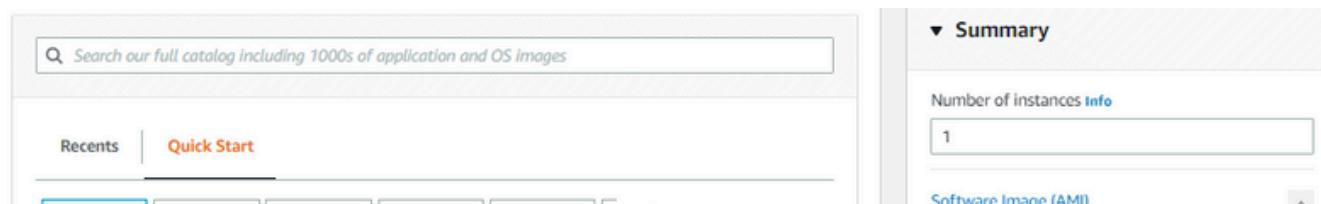
C:\Users\Anupam>aws ec2 describe-key-pairs
{
  "KeyPairs": [
    {
      "KeyId": "key-24",
      "KeyFingerprint": "61:93:4f:f2:77:f6:0e:b0:42:95:b4:6e:b5:75:6c:68:cf:b6:dc:a5",
      "KeyName": "k21-key",
      "Tags": []
    },
    {
      "KeyId": "key-0e71ld7c436",
      "KeyFingerprint": "15:1f:f6:96:15:42:60:ce:1e:bb:e1:23:eb",
      "KeyName": "k21academykey",
      "Tags": []
    },
    {
      "KeyId": "key-008d094ca040e67b6",
      "KeyFingerprint": "e1:6a:ce:69:1:10:40:10:20:2a:95:80:19:af:5c:21:64",
      "KeyName": "MyKeyPair",
      "Tags": []
    }
  ]
}

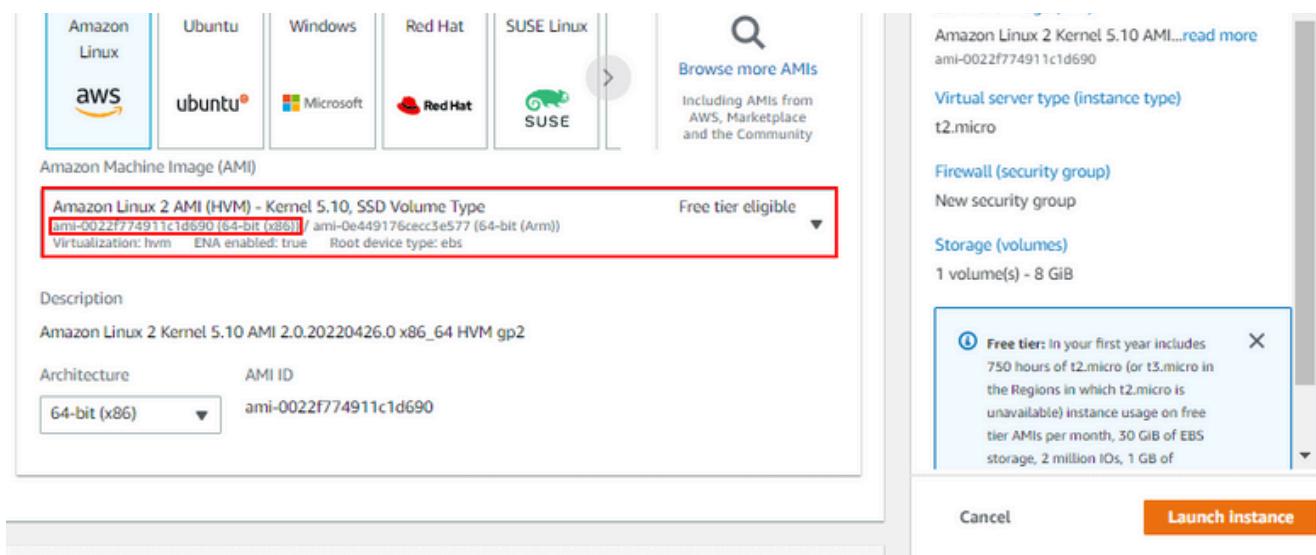
C:\Users\Anupam>
```

If you want to delete the key pair at some instance, you can use the command: aws ec2 delete-key-pair --key-name k21academykey (key pair name)

Also Read: AWS Cloud Security (<https://k21academy.com/amazon-web-services/aws-security-and-compliance/>).

Step 5. Deploy ec2 instance through CLI: Now, in the next step, we are creating and deploying the ec2 instance through CLI; before, we have to collect ami- id by going to EC2 instances > launch instance.





After collecting ami-id, you can follow the command: `aws ec2 run-instances --image-id ami-***** (write id here) --instance-type t2.micro --key-name k21academykey`

(key pair name) to launch and deploy the ec2 instance.

We can also verify the deployed instance by going to EC2 Instances in AWS Portal.

Or with the help of CLI by writing the command: `aws ec2 describe-instances`

```

Command Prompt - aws ec2 run-instances --image-id ami-05d72852800cbf29e --instance-type t2.micro --key-name k21academykey
Microsoft Windows [Version 10.0.19042.867]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\Anupam>aws ec2 run-instances --image-id ami-05d72852800cbf29e --instance-type t2.micro --key-name k21academykey
{
    "Groups": [],
    "Instances": [
        {
            "AmilaunchIndex": 0,
            "InstanceId": "i-05d72852800cbf29e"
        }
    ]
}

```

```
    "ImageId": "ami-05072652000000129e",
    "InstanceId": "i-0fid23b2545285f31",
    "InstanceType": "t2.micro",
    "KeyName": "k2iacademykey",
    "LaunchTime": "2021-04-14T08:38:09+00:00",
    "Monitoring": {
        "State": "disabled"
    },
    "Placement": {
        "AvailabilityZone": "us-east-2b",
        "GroupName": "",
        "Tenancy": "default"
    },
    "PrivateDnsName": "ip-172-31-31-183.us-east-2.compute.internal",
    "PrivateIpAddress": "172.31.31.183",
    "ProductCodes": [],
    "PublicDnsName": "",
    "State": {
        "Code": 0,
        "Name": "pending"
    },
    "StateTransitionReason": "",
    "SubnetId": "subnet-b3f514ce",
    "VpcId": "vpc-8e32b2e5",
    "Architecture": "x86_64",
    "BlockDeviceMappings": [],
    "ClientToken": "e56969a8-5e0f-4c64-b227-72208c88654f",
    "EbsOptimized": false,
    "EnaSupport": true,
    "Hypervisor": "xen",
    "NetworkInterfaces": [
        {
            "Attachment": {
                "AttachTime": "2021-04-14T08:38:09+00:00",
                "AttachmentId": "eni-attach-0cc439f76617fa2f",
                "DeleteOnTermination": true,
                "DeviceIndex": 0,
                "Status": "attaching"
            },
            "Description": "",
            "Groups": [
                {
                    "GroupName": "default",
                    "GroupId": "sg-c8e35fba"
                }
            ],
            "Ipv6Addresses": [],
            "MacAddress": "06:71:2f:85:e8:a0",
            "NetworkInterfaceId": "eni-079dd3526d56d1f5d",
            "OwnerId": "063372241087",
            "PrivateDnsName": "ip-172-31-31-183.us-east-2.compute.internal",
            "PrivateIpAddress": "172.31.31.183",
            "PrivateIpAddresses": [

```

This showed we have successfully created and deployed the EC2 instance.

AWS cloud watch



- What does website traffic look like?
- How is performance?
- How much bandwidth is my app using?
- Are compute resources optimized?



Provides visibility into AWS resources and applications

- Near-real-time **metrics** such as CPU, disk, GPU utilization
- **CloudWatch Logs** allow you to collect logs from AWS and non-AWS sources, to search/extract metrics
- **Alarms** can trigger notifications for metrics
 - Example: Alarm to notify you when you've hit CPU utilization of 90%
- **Dashboards** offer at-a-glance views



What is Amazon SNS used for?

Amazon Simple Notification Service (Amazon SNS) is a managed service that provides message delivery from publishers to subscribers (also known as producers and consumers). Publishers communicate asynchronously with subscribers by sending messages to a topic, which is a logical access point and communication channel.

Amazon Simple Notification Service

Pub/sub messaging for microservices and serverless applications.

Amazon SNS is a highly available, durable, secure, fully managed pub/sub messaging service that enables you to decouple microservices, distributed systems, and event-driven serverless applications. Amazon SNS provides topics for high-throughput, push-based, many-to-many messaging.

Benefits and features

Reliably deliver messages with durability

Amazon SNS uses cross availability zone message storage to provide high message durability. Amazon SNS reliably delivers messages to valid AWS endpoints, such as Amazon SQS queues and AWS Lambda functions.

Simplify your architecture with Message Filtering

Amazon SNS helps you simplify your pub/sub messaging architecture by offloading the message filtering logic from your subscriber systems, and message routing logic from your publisher systems.

Automatically scale your workload

Amazon SNS leverages the proven AWS cloud to dynamically scale with your application. Amazon SNS is a fully managed service, taking care of the heavy lifting related to capacity planning, provisioning, monitoring, and patching.

Keep messages private and secure

Amazon SNS topic owners can set topic policies that restrict who can publish and subscribe to a topic. Amazon SNS also ensures that data is encrypted in transit and at rest, and provides VPC endpoints for message privacy.

Create topic

Topic name

A topic is a message channel. When you publish a message to a topic, it fans out the message to all subscribed endpoints.

 MyTopic[Next step](#)[Start with an overview](#)

Pricing

Amazon SNS has no upfront costs. You pay based on the number of messages you publish, the number of messages you deliver, and any additional API calls for managing topics and subscriptions. Delivery pricing varies by endpoint type.

[Learn more](#)

Documentation

[Developer Guide](#)[API Reference](#)[FAQs](#)[Support forums](#)

Create Topic

Application Integration [Option+S]

click on create

Create topic

A topic is a message channel. When you publish a message to a topic, it fans out the message to all subscribed endpoints.

SNS, Dots

Next step

Start with an overview

Pricing

Amazon SNS has no upfront costs. You pay based on the number of messages you publish, the number of messages you deliver, and any additional API calls for managing topics and subscriptions. Delivery pricing varies by endpoint type.

Learn more

Documentation

Developer Guide
API Reference

Amazon Simple Notification Service

Pub/sub messaging for microservices and serverless applications.

Amazon SNS is a highly available, durable, secure, fully managed pub/sub messaging service that enables you to decouple microservices, distributed systems, and event-driven serverless applications. Amazon SNS provides topics for high-throughput, push-based, many-to-many messaging.

Benefits and features

Reliably deliver messages with durability
Amazon SNS uses cross availability zone message storage to provide high message durability. Amazon SNS reliably delivers messages to valid AWS endpoints, such as Amazon SQS queues and AWS Lambda functions.

Automatically scale your workload
Amazon SNS leverages the proven AWS cloud to dynamically scale with your application. Amazon SNS is a fully managed service, taking care of the heavy lifting related to capacity planning, provisioning, monitoring, and patching.

Simplify your architecture with Message Filtering
Amazon SNS helps you simplify your pub/sub messaging architecture by offloading the message filtering logic from your subscriber systems and

Keep messages private and secure
Amazon SNS topic owners can set topic policies that restrict who can publish and subscribe to a topic. Amazon SNS also ensures that data is encrypted in transit and at rest, and provides IAM authentication for

AWS Services Search [Option+S] N. Virginia knodax-demo

Create topic

Details

Type [Info](#)
Topic type cannot be modified after topic is created.

FIFO (first-in, first-out)

- Strictly-preserved message ordering
- Exactly-once message delivery
- High throughput, up to 500 publishes/second
- Subscription protocols: SQS

Standard

- Best-effort message ordering
- At-least once message delivery
- Highest throughput, up to 1000 publishes/second
- Subscription protocols: SQS, Lambda, HTTP, SMS, email, mobile application endpoints

Name
Maximum 256 characters. Can include alphanumeric characters, hyphens (-) and underscores (_).

Display name - optional [Info](#)
To use this topic with SMS subscriptions, enter a display name. Only the first 10 characters are displayed in an SMS message.

Maximum 100 characters.

Encryption - optional
Amazon SNS provides in-transit encryption by default. Enabling server-side encryption adds at-rest encryption to your topic.

Access policy - optional [Info](#)
This policy defines who can access your topic. By default, only the topic owner can publish or subscribe to the topic.

Standard topics provide Best-effort message ordering, At-least once message delivery, Highest throughput with SQS, Lambda, HTTP, SMS, email, mobile application endpoints.

SNS-Demo [Option+5] N. Virginia knodes-demo

Name
SNS-Demo
Maximum 256 characters. Can include alphanumeric characters, hyphens (-) and underscores (_).

Display name - optional Info
To use this topic with SMS subscriptions, enter a display name. Only the first 10 characters are displayed in an SMS message.
My Topic
Maximum 100 characters.

▶ Encryption - optional Info
Amazon SNS provides in-transit encryption by default. Enabling server-side encryption adds at-rest encryption to your topic.

▶ Access policy - optional Info
This policy defines who can access your topic. By default, only the topic owner can publish or subscribe to the topic.

▶ Data protection policy - optional Info
This policy defines which sensitive data to monitor and to prevent from being exchanged via your topic.

▶ Delivery policy (HTTP/S) - optional Info
The policy defines how Amazon SNS retries failed deliveries to HTTP/S endpoints. To modify the default settings, expand this section.

▶ Delivery status logging - optional Info
These settings configure the logging of message delivery status to CloudWatch Logs.

▶ Tags - optional
A tag is a metadata label that you can assign to an Amazon SNS topic. Each tag consists of a key and an optional value. You can use tags to search and filter your topics and track your

leave it as default

AWS Services Search [Option+5] My Topic Maximum 100 characters.

▶ **Encryption - optional** Info
Amazon SNS provides in-transit encryption by default. Enabling server-side encryption adds at-rest encryption to your topic.

▶ **Access policy - optional** Info
This policy defines who can access your topic. By default, only the topic owner can publish or subscribe to the topic.

▶ **Data protection policy - optional** Info
This policy defines which sensitive data to monitor and to prevent from being exchanged via your topic.

▶ **Delivery policy (HTTP/S) - optional** Info
The policy defines how Amazon SNS retries failed deliveries to HTTP/S endpoints. To modify the default settings, expand this section.

▶ **Delivery status logging - optional** Info
These settings configure the logging of message delivery status to CloudWatch Logs.

▶ **Tags - optional**
A tag is a metadata label that you can assign to an Amazon SNS topic. Each tag consists of a key and an optional value. You can use tags to search and filter your topics and track your costs. [Learn more](#)

▶ **Active tracing - optional** Info
Use AWS X-Ray active tracing for this topic to view its traces and service map in Amazon CloudWatch. Additional costs apply.

Cancel **Create topic**

AWS Services Search

Amazon SNS

Topic SNS-Demo created successfully.
You can create subscriptions and send messages to them from this topic.

Dashboard Topics Subscriptions Mobile Push notifications Text messaging (SMS) Origination numbers

SNS-Demo

Details

Name: SNS-Demo ARN: arnawsnsus-east-1:383246051810:SNS-Demo Type: Standard

Display name: Topic owner: 383246051810

click create subscription

Subscriptions Access policy Data protection policy Delivery policy (HTTP/S) Delivery status logging Encryption Tags Incoming messages

Subscriptions (0)

Search

ID Endpoint Status Protocol

No subscriptions found
You don't have any subscriptions to this topic.

Create subscription

Publish message Edit Delete Publish message

Request confirmation Confirm subscription Create subscription

The screenshot shows the AWS SNS console with a green success banner at the top stating 'Topic SNS-Demo created successfully.' Below it, there's a yellow placeholder icon. On the left, a sidebar lists various services like Dashboard, Topics, Subscriptions, and Mobile. The main area is titled 'SNS-Demo' and contains a 'Details' section with fields for Name, ARN, and Type. A large blue watermark 'click create subscription' is overlaid across the middle. At the bottom, there's a 'Subscriptions' tab with a table showing 'Subscriptions (0)' and a 'Create subscription' button.

Important changes for sending text messages (SMS) to US destinations
US mobile carriers have recently changed their regulations, and will require that all toll-free numbers (TFNs) complete a registration process with a regulatory body before September 30, 2022. If you currently have a toll-free number you must register your toll-free number by September 30, 2022 or you will no longer be able to use the toll-free number. Learn more [Learn more](#)

View origination numbers

Amazon SNS > Subscriptions > Create subscription

Create subscription

Details

Topic ARN
 X

Protocol
The type of endpoint to subscribe
Select protocol ▾
Amazon Kinesis Data Firehose
Amazon SQS 
AWS Lambda
Email
Email-JSON
HTTP
HTTPS
Platform application endpoint
SMS

select option where you want get notifications

Cancel **Create subscription**

AWS Services Search [Option+S] N. Virginia View origination

Important changes for sending text messages (SMS) to US destinations
US mobile carriers have recently changed their regulations, and will require that all toll-free numbers (TFNs) complete a registration process with a regulatory body before September 30, 2022. If you currently have a toll-free number you must register your toll-free number by September 30, 2022 or you will no longer be able to use the toll-free number. Learn more [Learn more](#)

Amazon SNS > Subscriptions > Create subscription

Create subscription

Details

Topic ARN
arn:aws:sns:us-east-1:383246081810:SNS-Demo

Protocol
The type of endpoint to subscribe
Email

Endpoint
An email address that can receive notifications from Amazon SNS.
sksingh-ccp@mailinator.com

ⓘ After your subscription is created, you must confirm it. Info

Subscription filter policy - optional
This policy filters the messages that a subscriber receives.

Redrive policy (dead-letter queue) - optional
Send undeliverable messages to a dead-letter queue.

click Create subscription

Cancel Create subscription

us-east-1.console.aws.amazon.com/sns/v3/home?region=us-east-1&subscriptionArn=aws:sns:us-east-1:383246081810:SNS-Demo:b5dca1d3-6cf4-406e-98f8-31a3c983d4e3

Amazon SNS

Important changes for sending text messages [SMS] to US destinations

US mobile carriers have recently changed their regulations, and will require that all toll-free numbers (TFNs) complete a registration process with a regulatory body before September 30, 2022. If you currently have a toll-free number you must register your toll-free number by September 30, 2022 or you will no longer be able to use the toll-free number. [Learn more](#)

View origination numbers

Subscription to SNS-Demo created successfully.

The ARN of the subscription is arn:aws:sns:us-east-1:383246081810:SNS-Demo:b5dca1d3-6cf4-406e-98f8-31a3c983d4e3.

Amazon SNS > Topics > SNS-Demo > Subscription: b5dca1d3-6cf4-406e-98f8-31a3c983d4e3

Subscription: b5dca1d3-6cf4-406e-98f8-31a3c983d4e3

Edit Delete

Details

ARN	arn:aws:sns:us-east-1:383246081810:SNS-Demo:b5dca1d3-6cf4-406e-98f8-31a3c983d4e3	Status	Pending confirmation
Endpoint	sksingh-cpp@mailinator.com	Protocol	EMAIL
Topic	SNS-Demo		
Subscription Principal	arn:aws:iam::383246081810:root		

Subscription filter policy Info

This policy filters the messages that a subscriber receives.

No filter policy configured for this subscription.

To apply a filter policy, edit this subscription.

SNS Created successfully

AWS Services Search [Option+S] N. Virginia knodax-demo

Amazon SNS X Amazon SNS > Topics > SNS-Demo

SNS-Demo

Details

Name: SNS-Demo

ARN: arn:aws:sns:us-east-1:3832461810: SNS-Demo

Type: Standard

Topic owner: [REDACTED] 3832461810

see it is pending confirmation
so now you go to your gmail account and confirm mail

Subscriptions | Access policy | CloudWatch Metrics | Delivery policy | Delivery logs | Encryption | Tags | Integration

Subscriptions (1)

ID	Endpoint	Status	Protocol
Pending confirmation	sksingh-cpp@mailinator.com	Pending confirmation	EMAIL

Edit Delete Request confirmation Confirm subscription Create subscription

The screenshot shows the AWS SNS console with a topic named 'SNS-Demo'. The 'Pending confirmation' status of a single subscription is highlighted with a yellow circle and a red rectangle. A large purple watermark with the text 'see it is pending confirmation so now you go to your gmail account and confirm mail' is overlaid on the page.

[Public Inboxes](#)[Public SMS](#)[Pricing](#)[Request Trial](#)

Use Mailinator for Email
Testing?
Apply for a FREE
Verified Pro Subscription!

Public Message > AWS Notification - Subscription Confirmation[Back](#)

To sksingh-ccp
From no-reply@sns.amazonaws.com
Sending IP 54.240.34.3
Received 2023-07-05 15:52:09

[Delete](#)[HTML](#) [JSON](#) [RAW](#) [LINKS](#) [SMTP_LOG](#) [ATTACHMENTS](#)

You have chosen to subscribe to the topic:
[arn:aws:sns:us-east-1:383246081810:SNS-Demo](#)

To confirm this subscription, click or visit the link below (If this was in error no action is necessary):
[Confirm subscription](#)

Please do [not reply directly](#) to this email. If you wish to remove yourself from receiving all future SNS subscription confirmation requests please send an email to [un-subscribe](#).

confirm mail

System Status
Terms
Privacy
Accessibility
Security
Powered by [Emailinator](#)

Screenshot of the AWS Amazon SNS console showing the "SNS-Demo" topic details and its subscription status.

The "Details" section shows:

- Name: SNS-Demo
- Display name: *
- ARN: arn:aws:sns:us-east-1:383246081810:SNS-Demo
- Topic owner: 383246081810
- Type: Standard

The "Subscriptions" tab is selected, showing one subscription:

ID	Endpoint	Status	Protocol
b5dca1d3-6cf4-405e-98f8-31a3c983d4e3	sksingh-cc@mailinator.com	Confirmed	EMAIL

A yellow circle highlights the "Endpoint" column value "sksingh-cc@mailinator.com". An orange arrow points from this highlighted area to the word "Confirmed" in the "Status" column.

now see it is confirmed

CloudWatch Alarm from EC2 Instance

Original

Instances (1/1) Info

Find instance by attribute or tag (case-sensitive)

Instance state = running

Clear filters

Name Instance ID Instance state Instance type Status check Alarm status Availability Zone Public IPv4 DNS Public IPv4 ... Elastic IP

Test Demo Ser... i-0d888d4f39c733d5d Running t2.micro 2/2 checks passed No alarms + us-east-1b ec2-3-94-116-234.com... 3.94.116.234 -

click instance

Click on Alarm status + icon

Instance: i-0d888d4f39c733d5d (Test Demo Server)

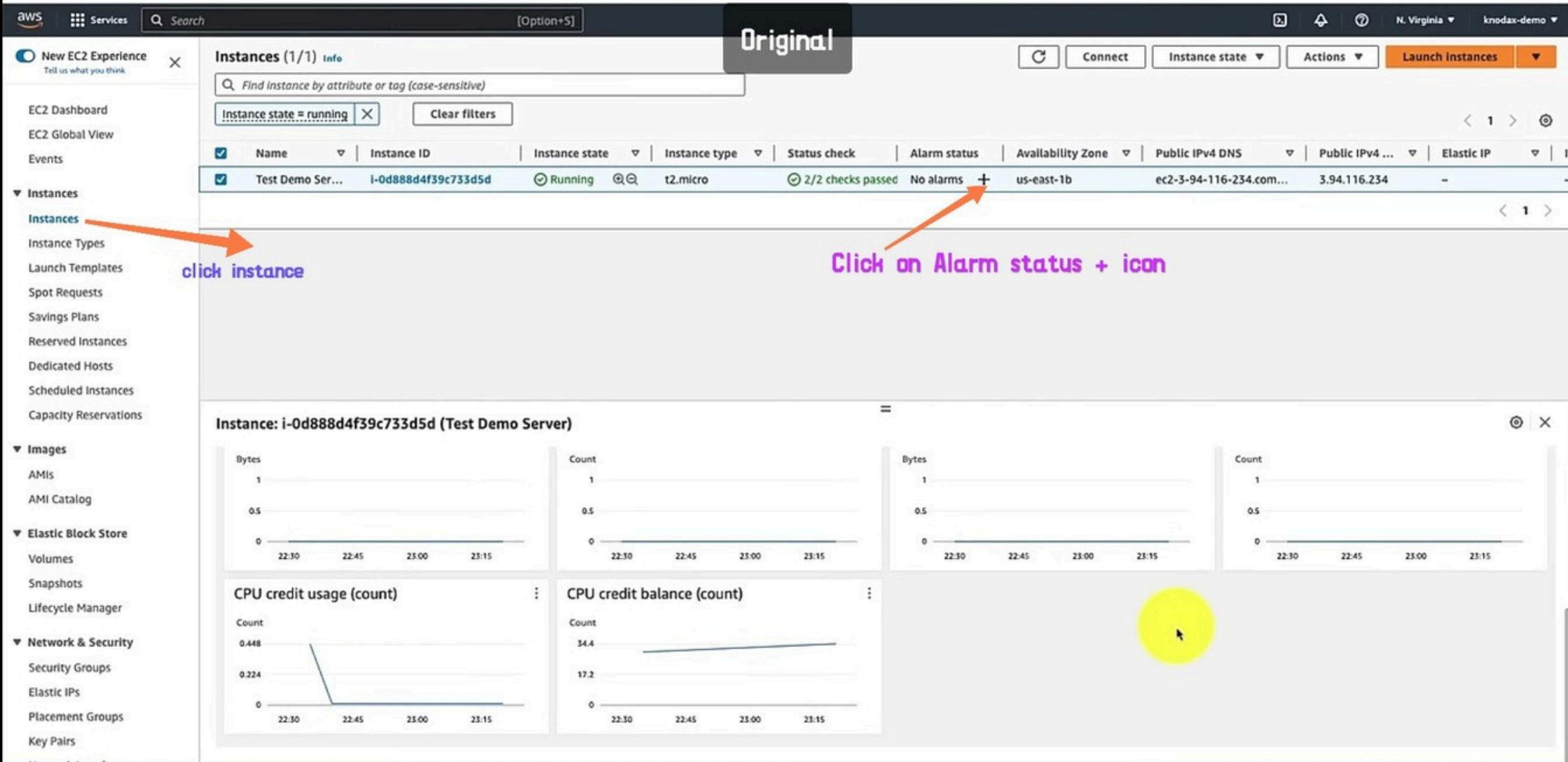
Bytes Count Bytes Count

Time	Value	Time	Value
22:30	1	22:45	1
23:00	0.5	23:15	0.5

CPU credit usage (count) CPU credit balance (count)

Count Count

Time	Value	Time	Value
22:30	0.448	22:45	34.4
23:00	0.224	23:15	17.2



EC2 > Instances > i-0d888d4f39c733d5d > Manage CloudWatch alarms

Manage CloudWatch alarms Info

Create or edit a CloudWatch alarm that monitors CloudWatch metrics for the instance.

Add or edit alarm Info

You can create a new alarm or edit an existing alarm.

Create an alarm
Create an alarm for i-0d888d4f39c733d5d

Edit an alarm
Edit an existing alarm for i-0d888d4f39c733d5d

Search for alarm

Find an alarm to modify

Select an existing alarm to edit

Alarm notification Info

Configure the alarm to send notifications to an Amazon SNS topic when it is triggered.

Q Default_CloudWatch_Alarms_Topic

Alarm action Info

Specify the action to take when the alarm is triggered.

Alarm thresholds

Specify the metric thresholds for the alarm.

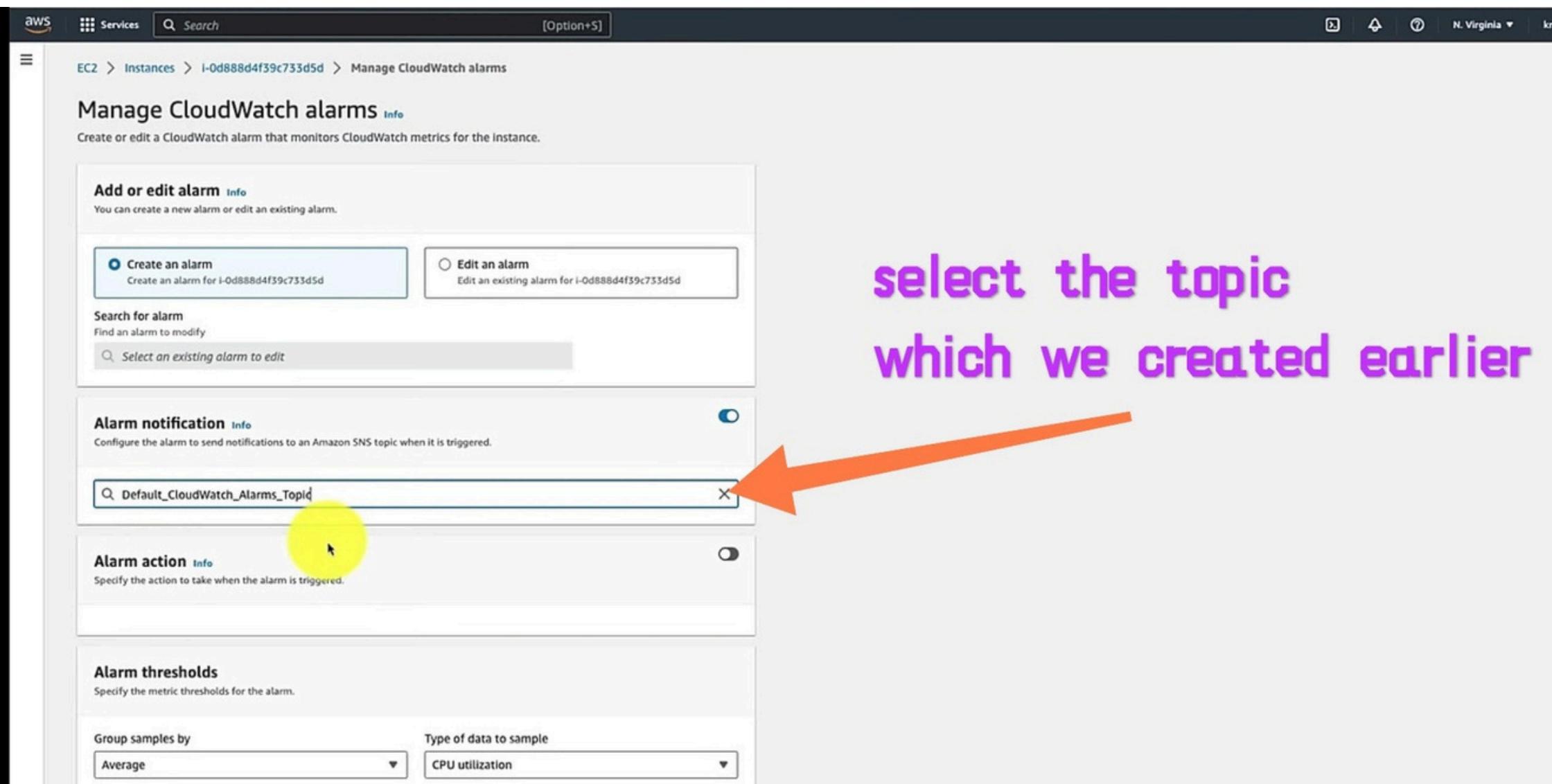
Group samples by

Average

Type of data to sample

CPU utilization

select the topic which we created earlier



Sales Services Search [Option+S] N. Virginia knodax-demo

Default_CloudWatch_Alarms_Topic

Alarm action Info
Specify the action to take when the alarm is triggered.

Alarm thresholds
Specify the metric thresholds for the alarm.

Group samples by: Average Type of data to sample: CPU utilization

Alarm when: \geq 0.99 Consecutive period: 1 Period: 5 Minutes

Alarm name: awsec2-i-0d888d4f39c733d5d-GreaterThanOrEqualToThreshold-CPUUtilization

Sample metric data Info
Sample metric data for i-0d888d4f39c733d5d

1h 3h 12h 1d 3d 1w Add to dashboard

CPU utilization (Average)

select when you notifications like loading EC2 reaches 5% you want notifications etc

us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#ManageCloudWatchAlarms:instanceId=i-0d888d4f39c733d5d

AWS Services Search [Option+S] N. Virginia knodax-demo

Specify the metric thresholds for the alarm.

Group samples by: Average Type of data to sample: CPU utilization

Alarm when: >= 0.99

Consecutive period: 1 Period: 5 Minutes

Alarm name: awsec2-i-0d888d4f39c733d5d-GreaterThanOrEqualToThreshold-CPUUtilization

Sample metric data Info
Sample metric data for i-0d888d4f39c733d5d

1h 3h 12h 1d 3d 1w Add to dashboard

CPU utilization (Average)

0.99 6.08 8.38 12.2
0 20:30 21:00 21:30 22:00 22:30 23:00 07-07-21-54

Cancel

click Create

CloudShell Feedback Language © 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

After 5 minutes you will get Notifications
in your Email

Done



Create Beanstalk

aws Services Q IAM X N. Virginia ▾ Sankar_Karra ▾

RDS Elastic Beans

Elastic Beanstalk

Applications Environments Change history

Application: BBBB Application version Saved configuration

Environment: BBBB-environment Go to environment Configuration Events Health

Services (11) Features (22) Resources New Documentation (49,338) Knowledge Articles (535) Marketplace (756) Blogs (1,761) Events (12) Tutorials (2)

Search results for 'IAM'

Services See all 11 results ▶

IAM ★ Manage access to AWS resources

Top features Groups Users Roles Policies Access Analyzer

IAM Identity Center ★ Manage workforce user access to multiple AWS accounts and cloud applications

Resource Access Manager ★ Share AWS resources with other accounts or AWS Organizations

AWS App Mesh ★ Easily monitor and control microservices

step 1 create IAM role

March 26, 2024 14:40:45 (UTC+5:20) INEO createEnvironment is starting

The screenshot shows the AWS IAM service page. The 'IAM' service card is highlighted with an orange box and a cursor is hovering over its title. The page shows search results for 'IAM' with 11 items listed. A large watermark 'step 1 create IAM role' is overlaid across the middle of the screen.

IAM Dashboard

 Search IAM

Dashboard

▼ Access management

User groups

Users

Roles

Policies

click on role

Identity providers

Account settings

▼ Access reports

Access Analyzer

External access

Unused access

Type here to search

Security recommendations 1

⚠ Add MFA for root user

Add MFA for root user - Enable multi-factor authentication (MFA) for the root user to improve security for this account.

[Add MFA](#)

✔ Root user has no active access keys

Using access keys attached to an IAM user instead of the root user improves security.

IAM resources

Resources in this AWS Account

User groups	Users	Roles	Policies	Identity providers
0	0	2	2	0

AWS Account

Account ID

[011309472392](#)

Account Alias

[Create](#)

Sign-in URL for IAM users in this account

<https://011309472392signin.aws.amazon.com/console>

Quick Links

[My security credentials](#)[Manage your access keys, multi-factor authentication, and more](#)

Identity and Access Management (IAM)

RDS Elastic Beanstalk EC2 IAM

IAM > Roles

Roles (2) Info

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by AWS services or external entities.

Search

Role name Trusted entities Last activity

Role name	Trusted entities	Last activity
AWSServiceRoleForSupport	AWS Service: support (Service-Linked)	-
AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service-Linked)	-

Create role

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access Analyzer

Feedback

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



Services

Search

[Alt+S]



Global ▾

Sankar_Karra ▾



RDS

Elastic Beanstalk

EC2

IAM

IAM > Roles > Create role

Step 1

Select trusted entity

Step 2

Add permissions

Step 3

Name, review, and create

Select trusted entity Info

Trusted entity type

AWS service

Allow AWS services like EC2, Lambda, or others to perform actions in this account.

AWS account

Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

Web identity

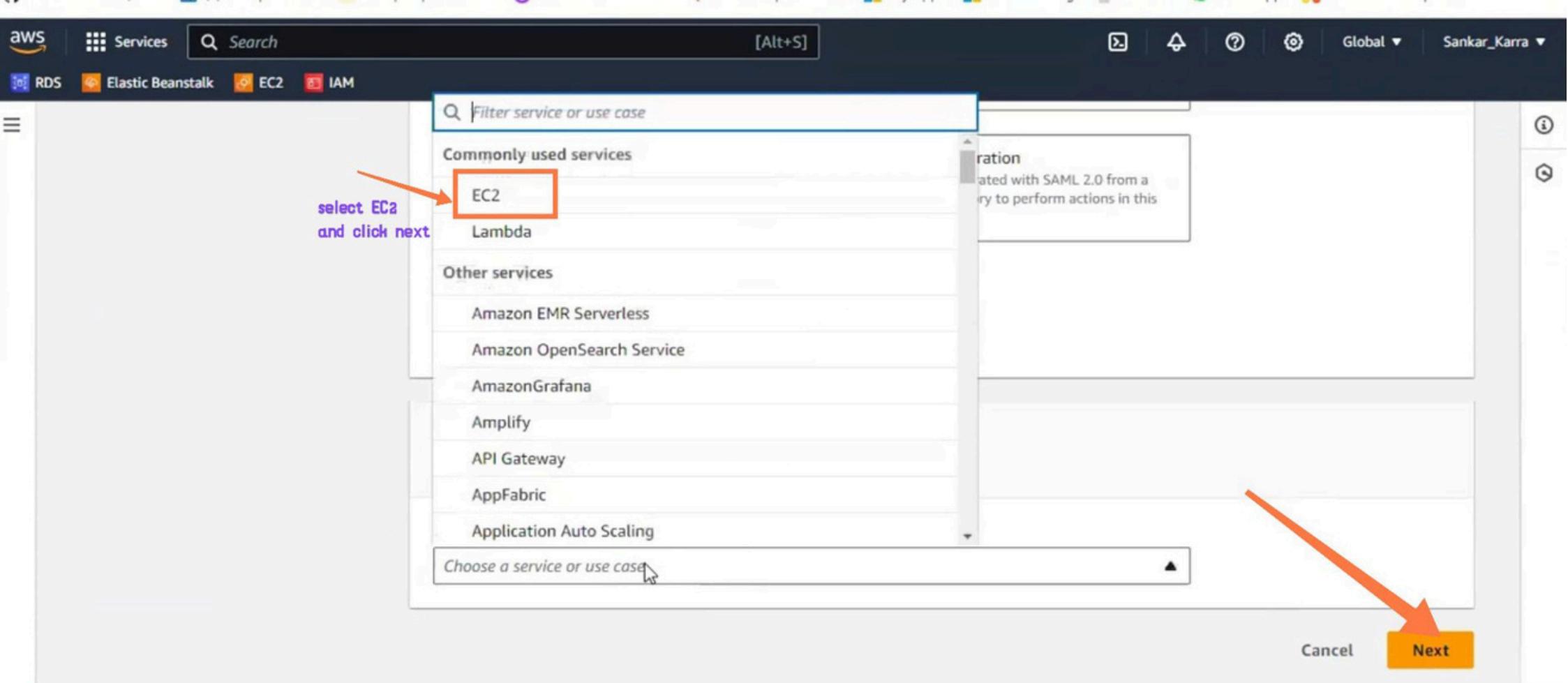
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

SAML 2.0 federation

Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

Custom trust policy

Create a custom trust policy to enable others



- AWSElasticBeanstalkWebTier
- AWSElasticBeanstalkWorkerTier
- AWSElasticBeanstalkMulticontainerDocker



select these 3 services in below



AWS Services Search [Alt+S] Global ▾ Sankar_K

RDS Elastic Beanstalk EC2 IAM

IAM > Roles > Create role

Step 1 Select trusted entity

Step 2 Add permissions

Step 3 Name, review, and create

Add permissions Info

Permissions policies (3/914) Info

Filter by Type

Q AWSElasticBeanstalkMulticontainerDocker X All types 1 match < 1 > ⌂

Policy name	Type	Description
<input checked="" type="checkbox"/> AWSElasticBeanstalkMulti...	AWS managed	Provide the instances in your multicon...

▶ Set permissions boundary - optional

Cancel Previous Next

now we added all 3 above policies for this IAM role

AWS Services Search [Alt+S] Global Sankar_Karra

RDS Elastic Beanstalk EC2 IAM

IAM > Roles > Create role

Step 1 Select trusted entity

Step 2 Add permissions

Step 3 Name, review, and create

Name, review, and create

Role details

Role name
Enter a meaningful name to identify this role.
 give a role name

Maximum 64 characters. Use alphanumeric and '+=-.,@-_` characters.

Description
Add a short explanation for this role.

Maximum 1000 characters. Use alphanumeric and '+=-.,@-_` characters.

Step 1: Select trusted entities Edit

AWS Services Search [Alt+S] Global Sankar_Karra

RDS Elastic Beanstalk EC2 IAM

15 16

Step 2: Add permissions

Permissions policy summary

Policy name	Type	Attached as
AWSElasticBeanstalkMulticontainerDocker	AWS managed	Permissions policy
AWSElasticBeanstalkWebTier	AWS managed	Permissions policy
AWSElasticBeanstalkWorkerTier	AWS managed	Permissions policy

check here we added all 3 policies

Step 3: Add tags

Add tags - optional Info

Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with this resource

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences 03:02 PM

FSD INTERVIEW GUIDE

Policy name ▾

Type

Attached as



AWSElasticBeanstalkMulticontainerDocker	AWS managed	Permissions policy
AWSElasticBeanstalkWebTier	AWS managed	Permissions policy
AWSElasticBeanstalkWorkerTier	AWS managed	Permissions policy

Step 3: Add tags

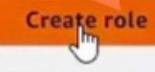
Add tags - optional Info

Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

[Add new tag](#)

You can add up to 50 more tags.

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

AWS Services Search [Alt+S] Global Sankar_Karra

RDS Elastic Beanstalk EC2 IAM

Identity and Access Management (IAM) X

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access Analyzer

Role r1 created.

View role X

Search Role name Trusted entities Last activity

IAM role is created

Manage

Roles Anywhere Info

Access AWS from your non AWS workloads

Operate your non AWS workloads using the same authentication and authorization strategy that you use within AWS.

X.509 Standard

Use your own existing PKI infrastructure or use AWS Certificate Manager Private Certificate Authority [\[\]](#) to authenticate identities.

Temporary credentials

Use temporary credentials with ease and benefit from the enhanced security they provide.

**Now we need to
create Elastic Beanstalk**

Kannadasan Kar... LinkedIn Notepad | Online Note... Online Courses | Learn... Coverdr | Online Film... My Apps Time Tracking ASKOK WhatsApp Show down & Spec...

AWS Services Search [Alt+S] RDS Elastic Beanstalk IAM

Identity and Access Management (IAM) View role X

Search IAM

Dashboard

Access management

- User groups
- Users
- Roles**
- Policies
- Identity providers
- Account settings

Access reports

Access Analyzer

Elastic Beanstalk 2 IAM

Role r1 created.

Role name Trusted entities Last activity

click Elastic Beanstalk

Authenticate your non AWS workloads and securely provide access to AWS services.

Access AWS from your non AWS workloads

Operate your non AWS workloads using the same authentication and authorization strategy that you use within AWS.

X.509 Standard

Use your own existing PKI infrastructure or use [AWS Certificate Manager Private Certificate Authority](#) to authenticate identities.

Temporary credentials

Use temporary credentials with ease and benefit from the enhanced security they provide.

Manage

Identity and Access Management (IAM)

View role X

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access Analyzer

RDS Elastic Beanstalk IAM

Role r1 created.

Role name Trusted entities Last activity

click Elastic Beanstalk

Authenticate your non AWS workloads and securely provide access to AWS services.

Access AWS from your non AWS workloads

Operate your non AWS workloads using the same authentication and authorization strategy that you use within AWS.

X.509 Standard

Use your own existing PKI infrastructure or use [AWS Certificate Manager Private Certificate Authority](#) to authenticate identities.

Temporary credentials

Use temporary credentials with ease and benefit from the enhanced security they provide.

Manage

AWS Services Search [Alt+S] N. Virginia ▾ Sankar_Karra ▾

RDS Elastic Beanstalk EC2 IAM

Elastic Beanstalk X Elastic Beanstalk Applications

Applications Environments Change history

Recent environments

- BBBB-env
- Build-env
- A-env

Applications (1) Info

Filter results matching the display value

Application name Environments Date created Last modified

Application name	Environments	Date created	Last modified
BBBB	BBBB-env (terminated)	March 26, 2024 14:49:26 (...	March 26, 2024 14:49:26 (...

Actions Create application

click create application



Services

Search

[Alt+S]



N. Virginia ▾

Sankar_Karra ▾



RDS



Elastic Beanstalk



EC2



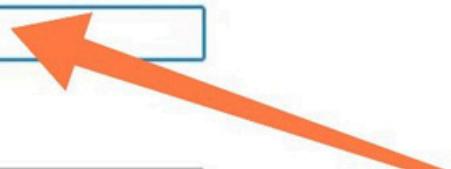
IAM



Application name

test12

Maximum length of 100 characters.

**give name**

Description

Tags

Apply up to 50 tags. You can use tags to group and filter your resources. A tag is a key-value pair. The key must be unique within the resource and is case-sensitive. [Learn more](#)

No tags associated with the resource.

[Add new tag](#)

You can add 50 more tags.

Karthikarai (kar... (c) REED | LinkedIn Notepad | Online N... Online Courses - le... iLOVEPDF | Online F... My Apps Time Tracking Ashok H WhatsApp Slow Down & Speed...

AWS Services Search [Alt+S] N. Virginia Sankar_Karra

RDS Elastic Beanstalk EC2 IAM

test14 Maximum length of 100 characters.

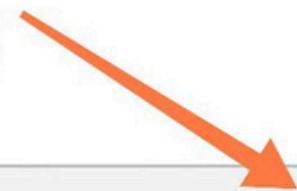
Description

Tags

Apply up to 50 tags. You can use tags to group and filter your resources. A tag is a key-value pair. The key must be unique within the resource and is case-sensitive. [Learn more](#)

No tags associated with the resource.

Add new tag You can add 50 more tags.

click create 

Cancel Create

AWS Services Search [Alt+S] N. Virginia Sankar_Karra

RDS Elastic Beanstalk EC2 IAM

Elastic Beanstalk X Elastic Beanstalk > Applications > test12

Applications Environments Change history

Application: test12 Application versions Saved configurations

Recent environments BBBB-env Build-env A-env

Application test12 environments (0) Info Actions Create new environment

Filter environments < 1 > ⚙

Environ... ▲ | Health ▽ | Date cre... ▽ | Domain ▽ | Running ... ▽ | Platform ▽ | Pla

No environments
No environments currently exist for this application.

Create environment

click create environment

Step 1

Configure environment

Step 2

Configure service access

Step 3 - optional

Set up networking, database, and tags

Step 4 - optional

Configure instance traffic and scaling

Step 5 - optional

Configure updates, monitoring, and logging

Step 6

Review

Configure environment Info

Environment tier Info

Amazon Elastic Beanstalk has two types of environment tiers to support different types of web applications.

Web server environment

Run a website, web application, or web API that serves HTTP requests. [Learn more](#)

Worker environment

Run a worker application that processes long-running workloads on demand or performs tasks on a schedule. [Learn more](#)

Application information Info

Application name

Maximum length of 100 characters.



Services

Search

[Alt+S]



N. Virginia ▾

Sankar_Karra ▾

RDS

Elastic Beanstalk

EC2

IAM

Configure instance traffic and scaling

Step 5 - optional

Configure updates, monitoring, and logging

Step 6

Review

Application information Info

Application name

Maximum length of 100 characters.

▶ Application tags (optional)

Environment information Info

Choose the name, subdomain and description for your environment. These cannot be changed later.

Environment name

Must be from 4 to 40 characters in length. The name can contain only letters, numbers, and hyphens. It can't start or end with a hyphen. This name must be unique within a region in your account.



Services

Search

[Alt+S]



N. Virginia ▾

Sankar_Karra ▾



RDS



Elastic Beanstalk



EC2



IAM

▶ Application tags (optional)



Environment information Info

Choose the name, subdomain and description for your environment. These cannot be changed later.

Environment name

Test12-env

Must be from 4 to 40 characters in length. The name can contain only letters, numbers, and hyphens. It can't start or end with a hyphen. This name must be unique within a region in your account.

Domain

test12

.us-east-1.elasticbeanstalk.com

Check availability

Environment description

give domain name



Services

Search

[Alt+S]



N. Virginia ▾

Sankar_Karra ▾



Elastic Beanstalk



EC2



IAM



Managed platform

Platforms published and maintained by Amazon Elastic Beanstalk. [Learn more](#)

Custom platform

Platforms created and owned by you. This option is unavailable if you have no platforms.

Platform

Choose a platform

.NET Core on Linux

.NET on Windows Server

Docker

Go

Java

Node.js

PHP

Python

Ruby

Tomcat

Existing version

Application versions that you have uploaded.

select platform based
on requirement
now I'm selecting java



aws Services Search [Alt+S] N. Virginia ▾ Sankar_Karr

RDS Elastic Beanstalk EC2 IAM

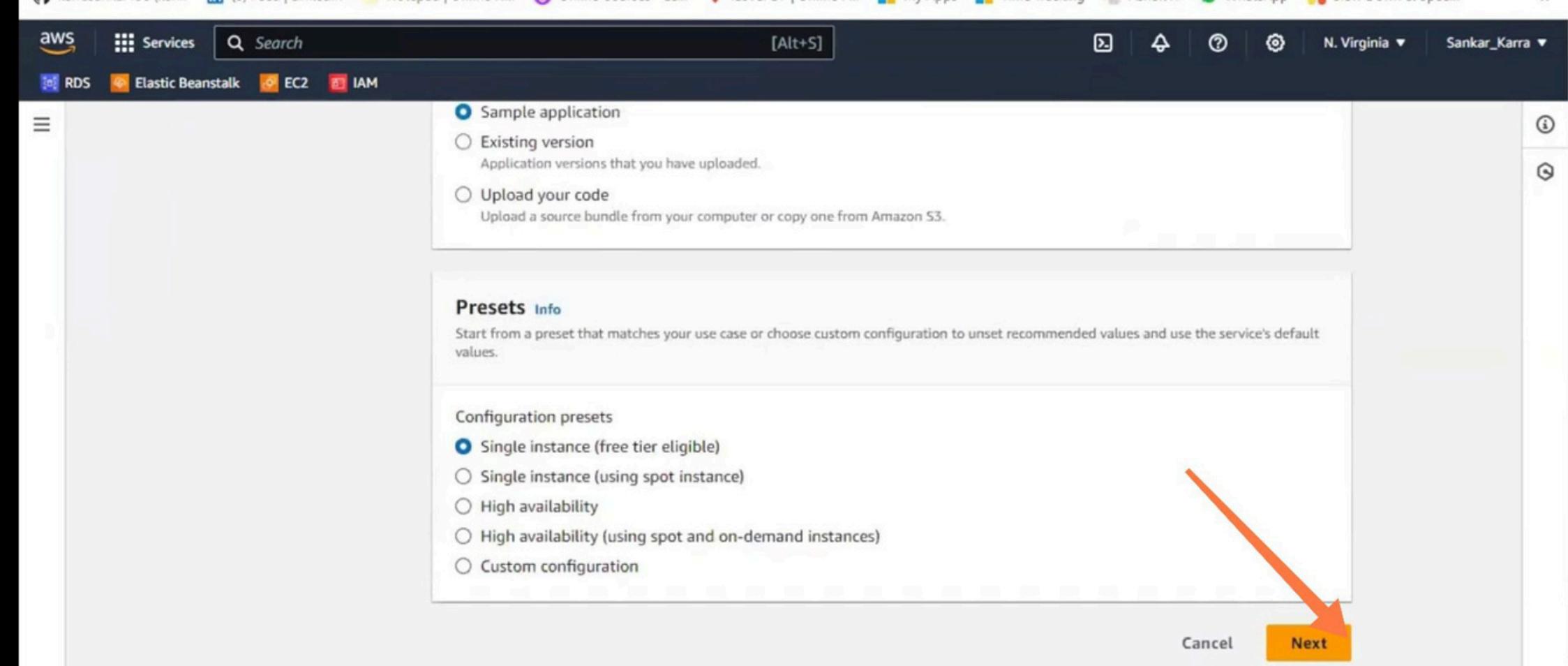
select sample application if you have file of code the upload your code

Sample application
 Existing version
Application versions that you have uploaded.
 Upload your code
Upload a source bundle from your computer or copy one from Amazon S3.

Presets [Info](#)
Start from a preset that matches your use case or choose custom configuration to unset recommended values and use the service's default values.

Configuration presets
 Single instance (free tier eligible)
 Single instance (using spot instance)
 High availability
 High availability (using spot and on-demand instances)
 Custom configuration

Cancel **Next**



AWS Services Search [Alt+S] N. Virginia ▾ Sankar_Karra ▾

RDS Elastic Beanstalk EC2 IAM

Set up networking, database, and tags

Step 4 - optional Configure instance traffic and scaling

Step 5 - optional Configure updates, monitoring, and logging

Step 6 Review

Service role

Create and use new service role

Use an existing service role

Existing service roles

Choose an existing IAM role for Elastic Beanstalk to assume as a service role. The existing IAM role must have the required IAM managed policies.

EC2 key pair

Select an EC2 key pair to securely log in to your EC2 instances. Learn more

Choose a key pair

EC2 instance profile

Choose an IAM instance profile with managed policies that allow your EC2 instances to perform required operations.

View permission details

select existing role and IAM role which we created previously

Cancel Skip to review Previous Next

[Configure updates, monitoring, and logging](#)

[View permission details](#)

Step 6

[Review](#)

EC2 key pair

Select an EC2 key pair to securely log in to your EC2 instances. [Learn more](#)

Choose a key pair



EC2 instance profile

Choose an IAM instance profile with managed policies that allow your EC2 instances to perform required operations.

r1



[View permission details](#)

**select EC2 instance profile
in that select role which we created
previously**

Cancel

[Skip to review](#)

[Previous](#)

Next

© 2024, Amazon Web Services, Inc. or its affiliates.

[Privacy](#)

[Terms](#)

[Cookie preferences](#)



RDS



Elastic Beanstalk



EC2



IAM

Step 1
Configure environment

Step 2
Configure service access

Step 3 - optional
Set up networking, database, and tags

Step 4 - optional
Configure instance traffic and scaling

Step 5 - optional
Configure updates, monitoring, and logging

Step 6
Review

Set up networking, database, and tags - *optional* Info

Virtual Private Cloud (VPC)

VPC

Launch your environment in a custom VPC instead of the default VPC. You can create a VPC and subnets in the VPC management console.

[Learn more](#)

 vpc-04f1a12bfb33c6cbb | (172.31.0.0/16)

right now select
default VPC



Instance settings

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

Public IP address

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

 Activated

Karradasankar I/O (Kar... LinkedIn Notepad | Online N... Online Courses - Le... iLovePDF | Online F... My Apps Time Tracking Ashok II WhatsApp Slow Down & Speed...

w Services Search [Alt+S]

RDS Elastic Beanstalk EC2 IAM

and logging

Step 6 Review

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

Activated

Instance subnets

Filter instance subnets

	Availability Zone	Subnet	CIDR	Name
<input type="checkbox"/>	us-east-1e	subnet-006d28cf4...	172.31.48.0/20	
<input type="checkbox"/>	us-east-1a	subnet-07b1bc9aa...	172.31.16.0/20	
<input type="checkbox"/>	us-east-1f	subnet-08f2c4f38f...	172.31.64.0/20	
<input type="checkbox"/>	us-east-1c	subnet-0c395c22b...	172.31.0.0/20	
<input type="checkbox"/>	us-east-1b	subnet-0d7c3c3c4...	172.31.32.0/20	

select public ip address





Services

Search

[Alt+S]



N. Virginia ▾

Sankar_Karra ▾

RDS

Elastic Beanstalk

EC2

IAM

Create snapshot

Elastic Beanstalk saves a snapshot of the database and then deletes it. You can restore a database from a snapshot when you add a DB to an Elastic Beanstalk environment or when you create a standalone database. You might incur charges for storing database snapshots.

Retain

The decoupled database will remain available and operational external to Elastic Beanstalk.

Delete

Elastic Beanstalk terminates the database. The database will no longer be available.

note: do not select any database option because we are launching just sample application

Tags

Apply up to 50 tags. You can use tags to group and filter your resources. A tag is a key-value pair. The key must be unique within the resource and is case-sensitive. [Learn more](#)

No tags associated with the resource.

[Add new tag](#)

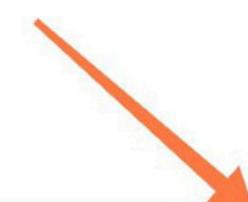
You can add 50 more tags.

Cancel

[Skip to review](#)

[Previous](#)

[Next](#)





Services

Search

[Alt+S]

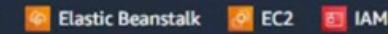


N. Virginia ▾

Sankar_Karra ▾



RDS



Elastic Beanstalk



EC2



IAM



Step 1

[Configure environment](#)

Step 2

[Configure service access](#)

Step 3 - optional

[Set up networking, database, and tags](#)

Step 4 - optional

[Configure instance traffic and scaling](#)

Step 5 - optional

[Configure updates, monitoring, and logging](#)

Step 6

Review

Review Info

Step 1: Configure environment

Edit

Environment information

Environment tier

Web server environment

Application name

test12

Environment name

Test12-env

Application code

Sample application

Platform

arn:aws:elasticbeanstalk:us-east-1::platform/Corretto 17

running on 64bit Amazon Linux 2023/4.2.1

step 4 and 5
just click next next

Step 2: Configure service access

Edit

CloudShell Feedback

© 2024, Amazon Web Services, Inc. or its affiliates.

Privacy

Terms

Cookie preferences

aws Services Search [Alt+S] N. Virginia ▾ Sankar_Karra ▾

RDS Elastic Beanstalk EC2 IAM

Platform software

Lifecycle	Log streaming	Logs retention
false	Deactivated	7
Rotate logs	Update level	X-Ray enabled
Deactivated	minor	Deactivated

Environment properties

Key	Value
GRADLE_HOME	/usr/local/gradle
M2	/usr/local/apache-maven/bin
M2_HOME	/usr/local/apache-maven

click submit 

Cancel Previous **Submit**

aws Services Search [Alt+S] N. Virginia ▾ Sankar_Karra ▾

RDS Elastic Beanstalk EC2 IAM

Elastic Beanstalk

Elastic Beanstalk is launching your environment. This will take a few minutes.

check here how Beanstalk configuring

Platform state
Supported

Events Health Logs Monitoring Alarms Managed updates Tags

Application: test12

- Application versions
- Saved configurations

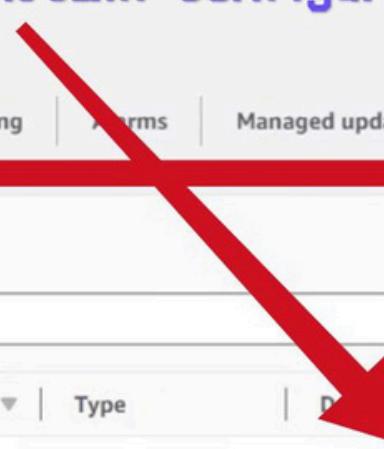
Environment: Test12-env

- Go to environment
- Configuration
- Events
- Health

Events (2) Info

Filter events by text, property or value

Time	Type	Details
March 26, 2024 15:04:57 (UTC+5:30)	INFO	Using elasticbeanstalk-us-east-1-011309472392 as Amazon S3 storage bucket for environment data.
March 26, 2024 15:04:56 (UTC+5:30)	INFO	createEnvironment is starting.



aws Services Search [Alt+S] N. Virginia Sankar_Karra

RDS Elastic Beanstalk EC2 IAM

Elastic Beanstalk

Environment successfully launched.

Test12-env Info

Actions ▼ Upload and deploy

Environment overview

Health	Ok	Environment ID	e-zc4wjuedxh
Domain	test12.us-east-1.elasticbeanstalk.com	Application name	test12

Platform Change version

Platform	Corretto 17 running on 64bit Amazon Linux 2023/4.2.1
Running version	-
Platform state	Supported

successfully launched environment or created beanstalk

Events Health Logs Monitoring Alarms Managed updates Tags