

Assignment 1 – Step by step

Setting up a web server on EC2

Step-by-step instructions for you to refer. There are many ways to achieve the same result. You don't have to follow it. It will waste a lot of time. Instead, you can do it on your own without following it step by step since you paid careful attention in class and understood the idea.

Get access to the AWS console through AWS Academy. In the AWS Academy account:

1. Spin up an EC2 instance.
 - a. Allowed HTTP:80 port from the world (0.0.0.0/0) in the Network Setting panel.
 - b. Expand Advanced Settings, and select the LabInstanceProfile.

The screenshot shows the AWS Academy Learner Lab interface. On the left is a sidebar with icons for Account, Dashboard, Courses, Calendar, Inbox, History, and Help. The main area shows the path: ALLv1-28910 > Modules > Learner Lab > Learner Lab. A large blue V-shaped icon with a red arrow pointing to its center is in the center. At the top right, there are buttons for Start Lab (highlighted with a red box), End Lab, AWS Details, Readme, and Reset. Below these are instructions: "1 click start lab and wait till AWS become green". The status bar at the bottom says "Used \$0 of \$100". On the right, a sidebar titled "Learner Lab" lists links: Environment Overview, Environment Navigation, Access the AWS Management Console, Region restriction, Service usage and other restrictions, and Using the terminal in the. Navigation buttons "Previous" and "Next" are at the bottom.

The screenshot shows the AWS Academy Learner Lab interface after the "AWS" link has been clicked. The "AWS" button now has a green background and a green circle with a white dot. The main area shows the path: ALLv1-28910 > Modules > Learner Lab > Learner Lab. Below the path, the text "2. Now click AWS hyperlink" is displayed. The central area shows a terminal window with the command "dd1_v1_v_SFF_1541872@runweb65828:~\$". The status bar at the bottom says "Used \$0 of \$100". The right sidebar and navigation buttons remain the same as in the previous screenshot.

The screenshot shows the AWS search results page. The search bar at the top contains the query "EC2". Below the search bar, there is a sidebar with links to various AWS services and features. The main content area displays search results for "EC2". The first result, "EC2" (Virtual Servers in the Cloud), is highlighted with a red box. Other results listed include "EC2 Image Builder", "AWS Firewall Manager", and "GuardDuty".

The screenshot shows the AWS EC2 Instances management page. The left sidebar is expanded to show the "Instances" section, specifically the "Instances" sub-section. The main area displays the "Instances Info" table, which is currently empty. At the top right of the table, there is a "Launch instances" button. A red box highlights this button, and a red arrow points to it with the instruction "click on this launch instances".

Quick Start for developer select default Amazon Linux

Amazon Linux

macOS Ubuntu Windows Red Hat

Amazon Machine Image (AMI)

Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type

ami-09d3b3274b6c5d4aa (64-bit (x86)) / ami-081dc0707789c2daf (64-bit (Arm))

Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Amazon Linux 2 Kernel 5.10 AMI 2.0.20221004.0 x86_64 HVM gp2

Architecture

64-bit (x86)

AMI ID

ami-09d3b3274b6c5d4aa

Verified provider

Number of instances

1

Software Image (AMI)

Amazon Linux 2 Kernel 5.10 AMI...read more

ami-09d3b3274b6c5d4aa

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GiB

Amazon Linux 2 Kernel 5.10 AMI 2.0.20221004.0 x86_64 HVM gp2

Architecture

64-bit (x86)

AMI ID

ami-09d3b3274b6c5d4aa

Verified provider

▼ Instance type Info

Instance type

t2.micro

Family: t2 1 vCPU 1 GiB Memory

On-Demand Linux pricing: 0.0116 USD per Hour

On-Demand Windows pricing: 0.0162 USD per Hour

Free tier eligible

select default instance type

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

Select

Create new key pair

MUM Global Online Education | Dashboard | Learner Lab | EC2 Management Console

us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#LaunchInstances

AWS Services Search for services, features, blogs, docs, and more [Alt+S]

CloudFront

Create security group Select existing security group

We'll create a new security group called 'launch-wizard-2' with the following rules:

Allow SSH traffic from Anywhere
Helps you connect to your instance 0.0.0.0/0

Allow HTTPS traffic from the internet To set up an endpoint, for example when creating a web server

Allow HTTP traffic from the internet To set up an endpoint, for example when creating a web server

Enable Allow HTTP traffic from the internet in Network Settings

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

▼ Configure storage Info Advanced

Feedback Looking for language selection? Find it in the new Unified Settings [i]

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

MUM Global Online Education | Dashboard | Learner Lab | EC2 Management Console | Portfolio

us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#LaunchInstances

AWS Services Search for services, features, blogs, docs, and more [Alt+S]

CloudFront

Instance type: t2.micro

Key pairs allow you to connect to your instance securely.

Enter the name of the key pair below. When prompted, store the private key in a secure and accessible location on your computer. You will need it later to connect to your instance. [Learn more](#)

Key pair name: myfirstserverkp

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

Key pair type: RSA

ED25519

Private key file format: .pem

.ppk

We use Session Manager to connect to the instance with the help of IAM profile. Alternatively, EC2 Instance Connect also works. In case the session manager is not working, you can use this Key Pair to connect to the instance. PEM for MacOS, Linux. PPK for Windows.

MUM Global Online Education | Dashboard | Learner Lab | EC2 Management Console

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

Services | CloudFront | Search for services, features, blogs, docs, and more [Alt+S]

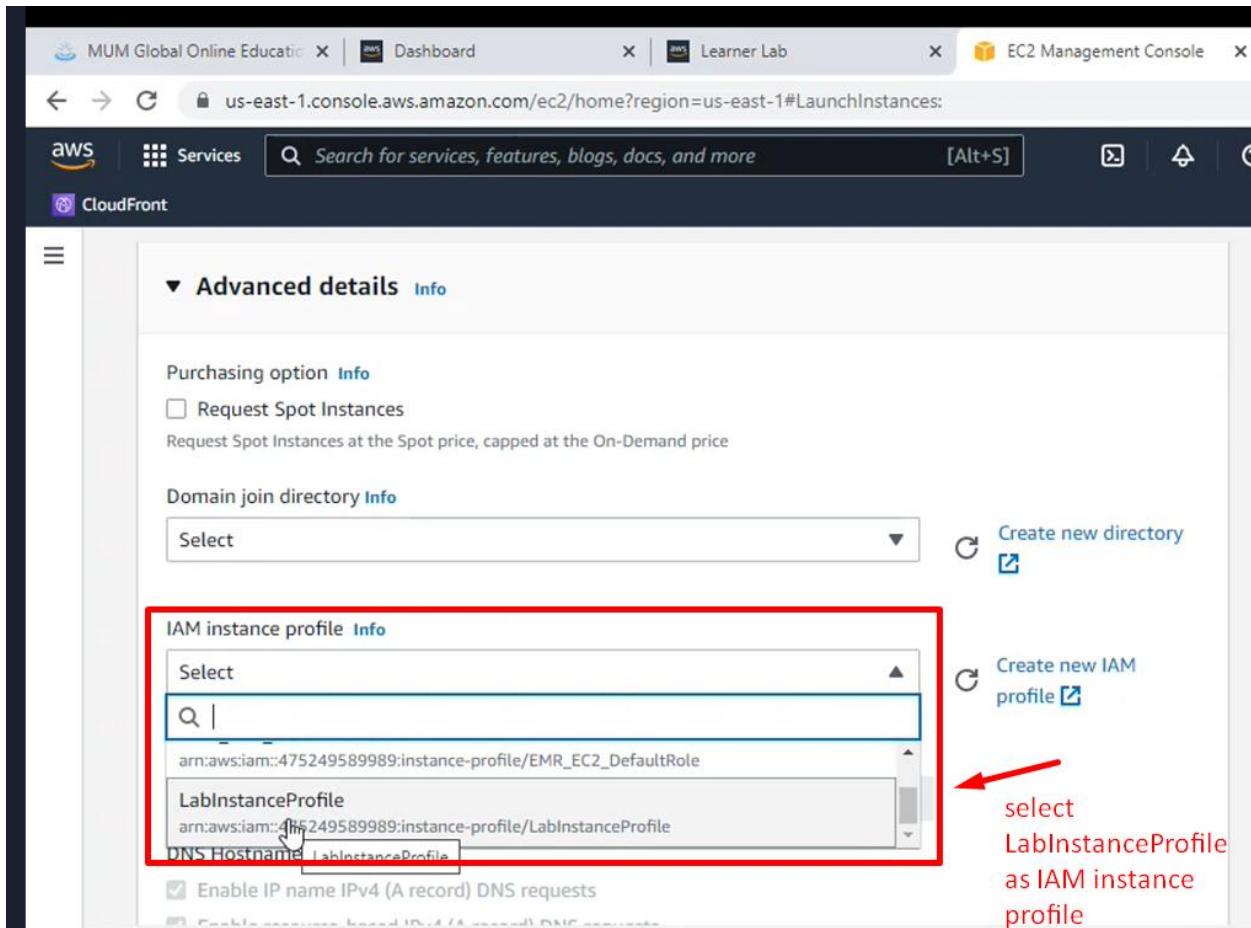
Advanced details [Info](#)

Purchasing option [Info](#)
 Request Spot Instances
Request Spot Instances at the Spot price, capped at the On-Demand price

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

IAM instance profile [Info](#)
Select [Create new IAM profile](#)
arn:aws:iam::475249589989:instance-profile/EMR_EC2_DefaultRole
LabInstanceProfile [arn:aws:iam::475249589989:instance-profile/LabInstanceProfile](#)
DNS Hostname: LabInstanceProfile [LabInstanceProfile](#)
 Enable IP name IPv4 (A record) DNS requests

select LabInstanceProfile as IAM instance profile



Dashboard | Learner Lab | Launch an instance | EC2 Management | Assignment 1 - IaaS and FaaS.d | + | N. Virginia | vclabs/user2243686=supriya @ 8468-6651-5154

EC2 > Instances > Launch an instance

Success
Successfully initiated launch of instance (i-0d69a3af05362f65)

Launch log

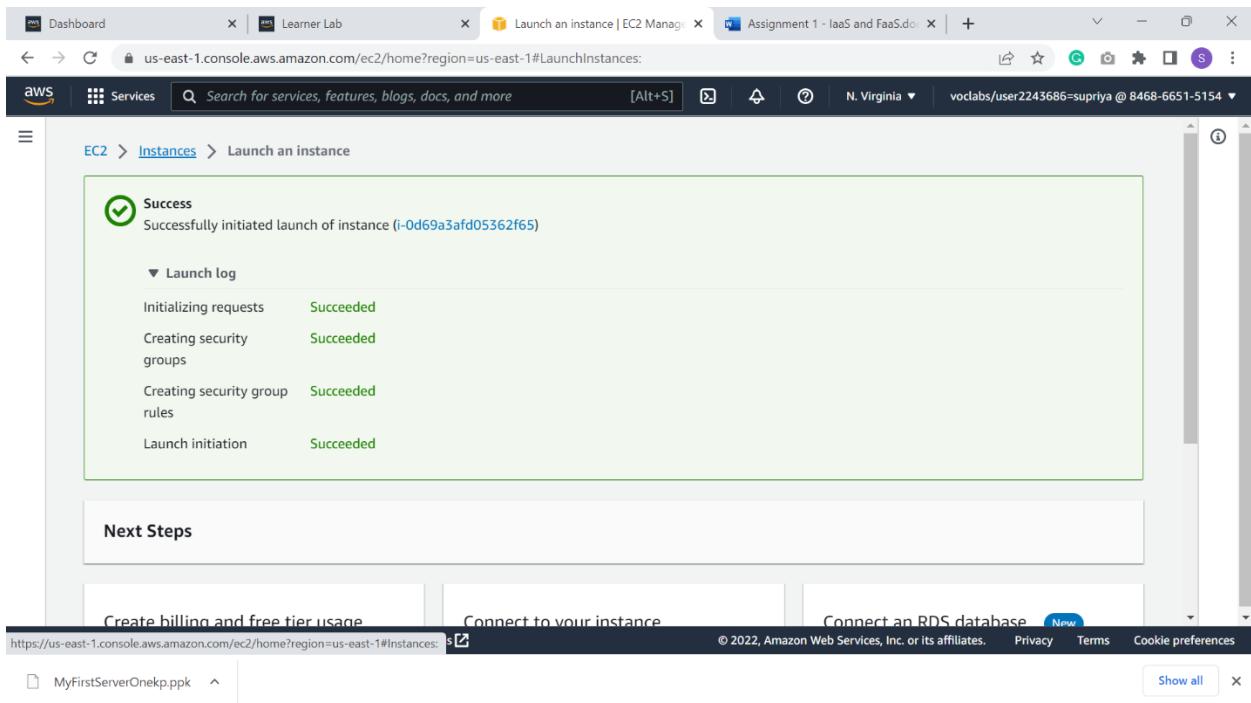
Initializing requests	Succeeded
Creating security groups	Succeeded
Creating security group rules	Succeeded
Launch initiation	Succeeded

Next Steps

Create billing and free tier usage | Connect to your instance | Connect an RDS database [New](#)

https://us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#Instances: [MyFirstServerOnekp.ppk](#) Show all

© 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences



MUM Global Online Education X Dashboard X Learner Lab X EC2 Management Console X Portfolio X

us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#Instances:

aws Services Search for services, features, blogs, docs, and more [Alt+S]

N. Virginia v voclabs/user2196930>Test_Student @ 4752-4958-9989

New EC2 Experience Tell us what you think

EC2 Dashboard EC2 Global View Events Tags Limits

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

Instances (1/1) Info Find instance by attribute or tag (case-sensitive)

Name Instance ID Instance state Instance type Status check Alarm status Available

MyFirstServer i-0a0768f4266727104 Running t2.micro 2/2 checks passed No alarms + us-east-1

Instance: i-0a0768f4266727104 (MyFirstServer)

Details Security Networking Storage Status checks Monitoring Tags

Instance summary Instance ID i-0a0768f4266727104 (MyFirstServer) Public IPv4 address 3.85.86.201 | open Address

IPv6 address Instance state Running Private IPv4 addresses 172.31.87.143

Public IPv4 DNS ec2-3-85-86-201.compute-1.amazonaws.com | open address

2. Configure a web server on EC2.

- Select the instance
- Hit Connect
- Select the “Session Manager” tab and hit Connect.

Dashboard X Learner Lab X Connect to instance X AWS Systems Manager X Instance details | EC2 X Assignment 1 - lab X

us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#ConnectToInstance:instanceId=i-0d69a3afd05362f65

aws Services Search for services, features, blogs, docs, and more [Alt+S]

N. Virginia v voclabs/user2243686=supriya @ 8468-6651-5154

EC2 > Instances > i-0d69a3afd05362f65 > Connect to instance

Connect to instance Info Connect to your instance i-0d69a3afd05362f65 (MyFirstServerOnekp) using any of these options

Session Manager RDP client EC2 serial console

Session Manager usage:

- Connect to your instance without SSH keys or a bastion host.
- Sessions are secured using an AWS Key Management Service key.
- You can log session commands and details in an Amazon S3 bucket or CloudWatch Logs log group.
- Configure sessions on the Session Manager Preferences page.

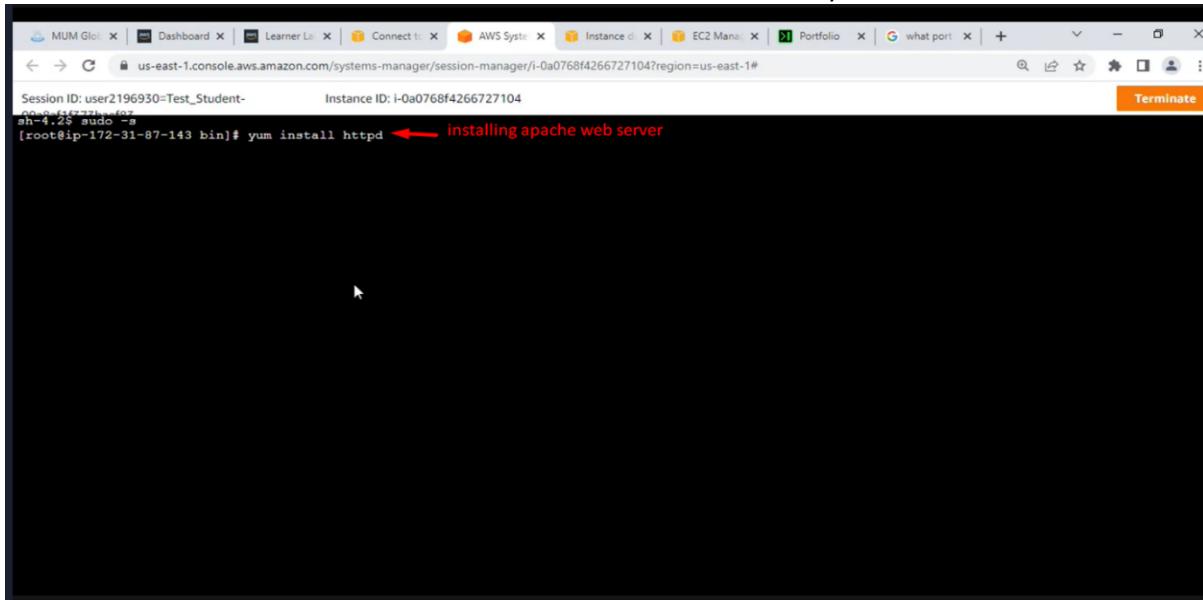
Cancel Connect

https://us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#InstanceDetails:instanceId=i-0d69a3afd05362f65 © 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

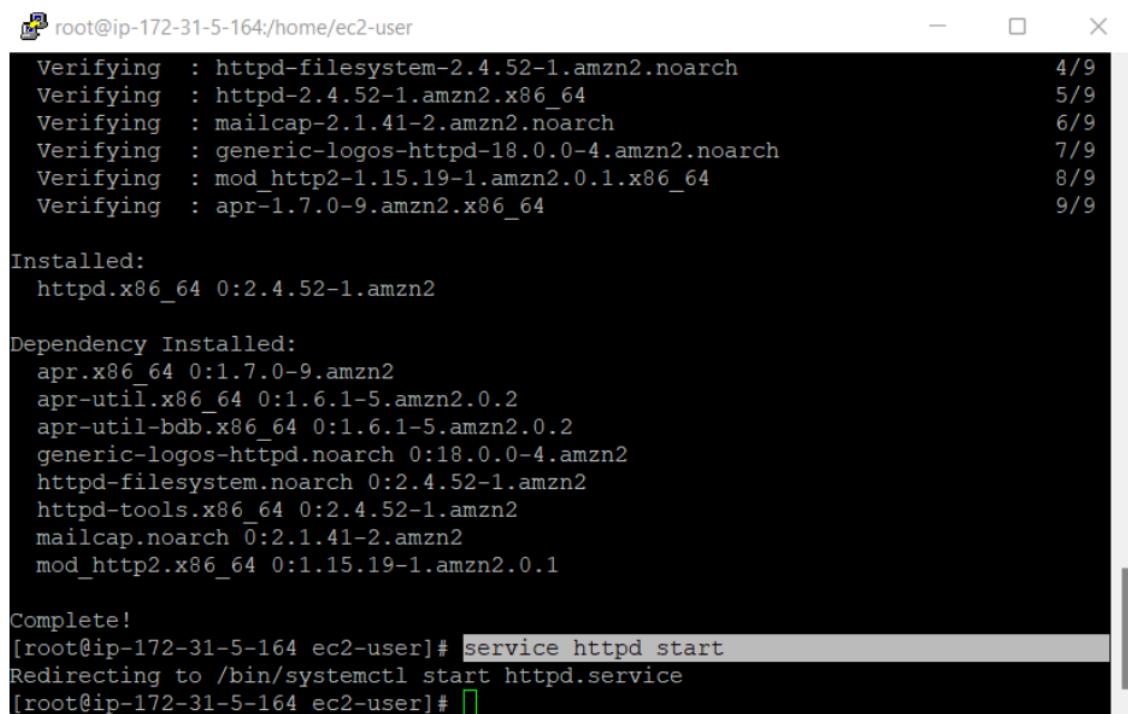
MyFirstServerOnekp.ppk Show all

- To install and customize a web server:
`sudo -s` => Logging as a root user so you can start the HTTPD service
`yum install httpd -y` => Installing a web server
`service httpd start` => Starting the server

cd /var/www/html => Changing the directory to customize the default Apache page.
nano index.html => Create the index.html and write your name here as HTML.



Session ID: user2196930-Test_Student-
Instance ID: i-0a0768f4266727104
[root@ip-172-31-87-143 bin]# yum install httpd installing apache web server

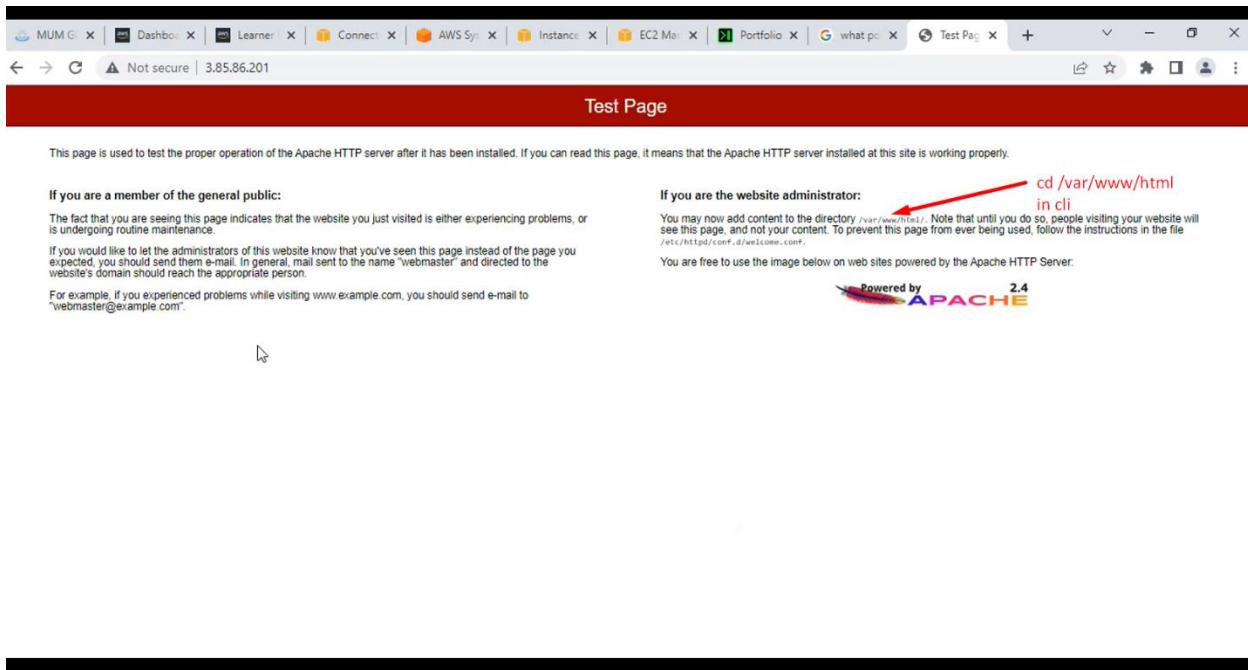


```
root@ip-172-31-5-164:/home/ec2-user
Verifying : httpd-filesystem-2.4.52-1.amzn2.noarch 4/9
Verifying : httpd-2.4.52-1.amzn2.x86_64 5/9
Verifying : mailcap-2.1.41-2.amzn2.noarch 6/9
Verifying : generic-logos-httpd-18.0.0-4.amzn2.noarch 7/9
Verifying : mod_http2-1.15.19-1.amzn2.0.1.x86_64 8/9
Verifying : apr-1.7.0-9.amzn2.x86_64 9/9

Installed:
httpd.x86_64 0:2.4.52-1.amzn2

Dependency Installed:
apr.x86_64 0:1.7.0-9.amzn2
apr-util.x86_64 0:1.6.1-5.amzn2.0.2
apr-util-bdb.x86_64 0:1.6.1-5.amzn2.0.2
generic-logos-httpd.noarch 0:18.0.0-4.amzn2
httpd-filesystem.noarch 0:2.4.52-1.amzn2
httpd-tools.x86_64 0:2.4.52-1.amzn2
mailcap.noarch 0:2.1.41-2.amzn2
mod_http2.x86_64 0:1.15.19-1.amzn2.0.1

Complete!
[root@ip-172-31-5-164 ec2-user]# service httpd start
Redirecting to /bin/systemctl start httpd.service
[root@ip-172-31-5-164 ec2-user]# [ ]
```



```
root@ip-172-31-5-164:/var/www/html
Verifying : mod_http2-1.15.19-1.amzn2.0.1.x86_64          8/9
Verifying : apr-1.7.0-9.amzn2.x86_64                      9/9

Installed:
  httpd.x86_64 0:2.4.52-1.amzn2

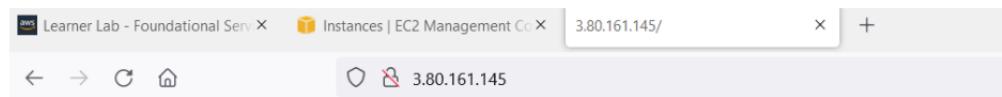
Dependency Installed:
  apr.x86_64 0:1.7.0-9.amzn2
  apr-util.x86_64 0:1.6.1-5.amzn2.0.2
  apr-util-bdb.x86_64 0:1.6.1-5.amzn2.0.2
  generic-logos-htpd.noarch 0:18.0.0-4.amzn2
  httpd-filesystem.noarch 0:2.4.52-1.amzn2
  httpd-tools.x86_64 0:2.4.52-1.amzn2
  mailcap.noarch 0:2.1.41-2.amzn2
  mod_http2.x86_64 0:1.15.19-1.amzn2.0.1

Complete!
root@ip-172-31-5-164 ec2-user]# service httpd start
Redirecting to /bin/systemctl start httpd.service
root@ip-172-31-5-164 ec2-user]# cd /var/www/html/ ←
root@ip-172-31-5-164 html]# touch index.html ←
root@ip-172-31-5-164 html]# ls ←
index.html
root@ip-172-31-5-164 html]# nano index.html ←
```

```
root@ip-172-31-5-164:/var/www/html
GNU nano 2.9.8           index.html           Modified
<p>Welcome to the cloud computing course, MIU <p>

File Name to Write: index.html
^G Get Help      M-D DOS Format      M-A Append      M-B Backup File
^C Cancel       M-M Mac Format      M-P Prepend     ^T To Files
```

Go to the website and reload



Welcome to the cloud computing course, MIU

Creating a public Lambda endpoint

3. Creating a lambda function returns an array of strings. Make it an API by enabling the public URL.
 - a. Choose the LabRole as IAM
 - b. Enable URL and enable CORS

The screenshot shows the 'Create function' wizard in the AWS Lambda console. The 'Basic information' section is highlighted with a red box around the 'Function name' field, which contains 'MyFirstLambdaFunction'. Below it, the 'Runtime' is set to 'Node.js 16.x'. The 'Architecture' section shows 'x86_64' selected. In the 'Permissions' section, the 'Use an existing role' option is selected, and the 'LabRole' is chosen from the dropdown. A red arrow points to this selection. The 'Advanced settings' section is also highlighted with a red box. Under 'Auth type', 'NONE' is selected. The 'Enable function URL' checkbox is checked, with a red arrow pointing to it and the text 'Enable function URL' written above it. Another red arrow points to the 'Configure cross-origin resource sharing (CORS)' checkbox, with the text 'enable cors' written above it. At the bottom right, there are 'Cancel' and 'Create function' buttons.

The screenshot shows the AWS Lambda console interface for the function 'MyFirstLambdaFunc'. The top navigation bar includes 'Services', 'Search', 'Lambda > Functions > MyFirstLambdaFunc', and account information 'N. Virginia' and 'vodlabs/user2243686=supriya @ 8468-6651-5154'.

Function overview

- MyFirstLambdaFunc** icon
- Layers**: (0)
- + Add trigger**
- + Add destination**

Description: -

Last modified: yesterday

Function ARN: arn:aws:lambda:us-east-1:846866515154:function:MyFirstLambdaFunc

Function URL: <https://wj3u5pe7eatdrsmkjfq22ipga0le zam.lambda-url.us-east-1.on.aws/>

Code source (Info) **Test** (2) **Deploy**

index.js

```
1  exports.handler = async (event) => {
2    // TODO implement
3    console.log("Hello from my lambda!");
4    console.log(`Name: ${event}`);
5    const response = {
6      statusCode: 200,
7      body: JSON.stringify(["Supriya Ghising", "Anna", "Simran"]),
8    };
9    return response;
10  };
11
12
```

Code properties

Package size 508.0 byte	SHA256 hash rCzIQC/qb16pDwRl3zsSETZfhcF2Y/+KG0cNV+P5cm4=	Last modified November 1, 2022 at 05:58 PM CDT
----------------------------	---	---

Runtime settings (Info) **Edit**

Runtime Node.js 16.x	Handler Info index.handler	Architecture Info x86_64
-------------------------	--------------------------------------	------------------------------------

Layers (Info) **Edit** **Add a layer**

Merge order	Name	Layer version	Compatible runtimes	Compatible architectures	Version ARN
There is no data to display.					

Feedback: Looking for language selection? Find it in the new [Unified Settings](#). © 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Learner L | MyFirstL | https://w | CloudW | Simple N | AWS Ma | React Ap | aws Cre | Creating | +

wj3u5pe7eatdrsmkjfq22ipga0le zam.lambda-url.us-east-1.on.aws

["Supriya Ghising", "Anna", "Simran"]

The screenshot shows the AWS CloudWatch service dashboard. On the left, a sidebar menu for 'CloudWatch' is open, showing various navigation options like Dashboards, Alarms, Logs (with 'Log groups' selected), Metrics, X-Ray traces, Events, Application monitoring, Insights, Settings, and Getting Started. The main content area is titled 'Log groups' and displays a table of log groups. The table has one entry:

Log group	Retention	Metric filters	Contributor Ins...
/aws/lambda/MyFirstLambdaFunc	Never expire	-	-

At the top of the main content area, there are buttons for 'Actions', 'View in Logs Insights', and 'Create log group'. A search bar at the top says 'Filter log groups or try prefix search' with an 'Exact match' checkbox. There are also navigation arrows and a refresh button.

Deploying a React app to S3

- 1) Deploy the front-end app in S3. Run in command prompt, npm run build

Go to S3 AWS service and create Bucket

The screenshot shows the AWS Lambda console search results for 'S3'. A red box highlights the search bar at the top with the text 'Q S3'. Below it, a red box highlights the 'S3' service entry, which is described as 'Scalable Storage in the Cloud'. To the right of the service entry, a note says 'search s3 for creating bucket and deploy react-app'.

The screenshot shows the AWS S3 buckets list page. A red box highlights the 'Create bucket' button. The table lists three existing buckets:

Name	AWS Region	Access	Creation date
cs516nov-2022.com	US East (N. Virginia) us-east-1	Public	November 1, 2022, 18:2
csnov2022demo	US East (N. Virginia) us-east-1	Bucket and objects not public	November 2, 2022, 10:2
elasticbeanstalk-us-east-1-846866515154	US East (N. Virginia) us-east-1	Objects can be public	November 1, 2022, 22:1

Amazon S3 > Buckets > Create bucket

Create bucket Info

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

General configuration

Bucket name Bucket name must be globally unique and must not contain spaces or uppercase letters. See rules for bucket naming.

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

Copy settings from existing bucket - optional Only the bucket settings in the following configuration are copied. [Choose bucket](#)

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 access points.

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.

Object Ownership Bucket owner enforced

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 prevent public access to your buckets and objects, AWS recommends that you turn on Block all public access. If your application needs to access private objects, AWS recommends that you turn off 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 before to set your specific usage cases. [Learn more](#)

Block all public access ← uncheck
 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 from newly added buckets or objects, and prevent the creation of new public access ACLs for buckets and objects. This setting does not affect existing public access that may have been granted 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.

← check
 I acknowledge that the current settings 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.

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](#)

Disable
 Enable

Tags (0) - optional

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

No tags associated with this bucket. [Add tag](#)

Default encryption

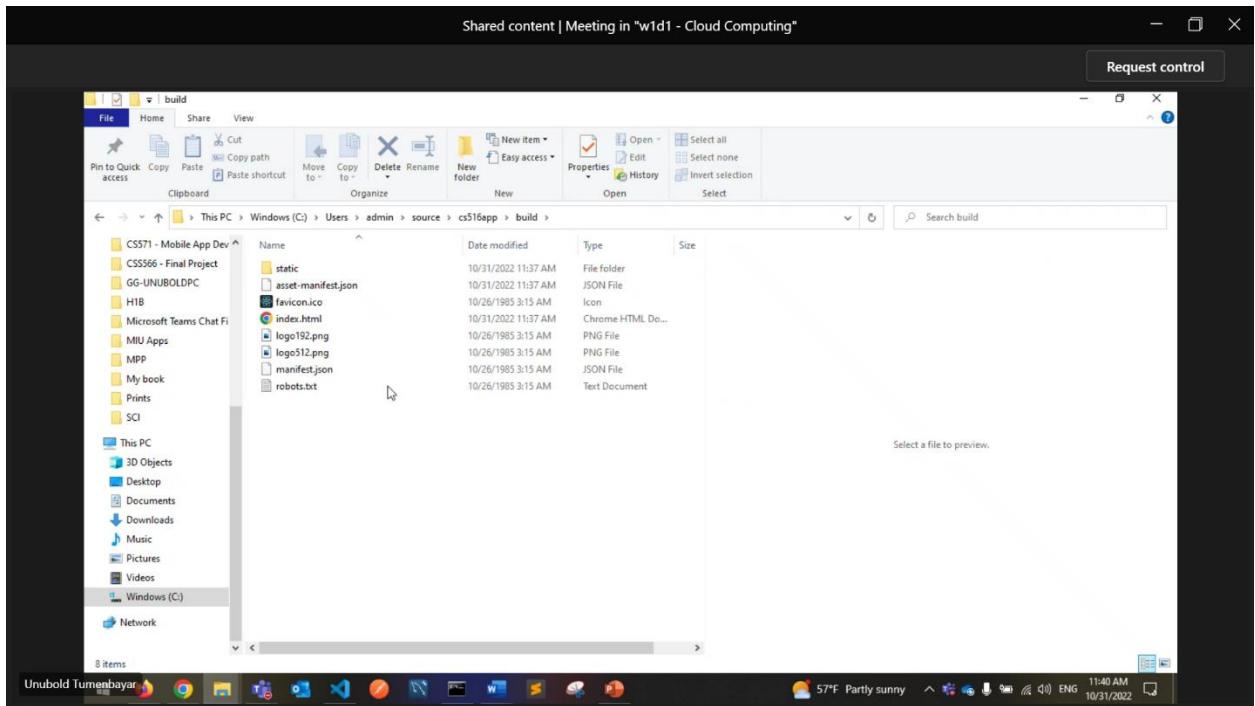
Automatically encrypt new objects stored in this bucket. [Learn more](#)

Server-side encryption
 Disable
 Enable

Advanced settings

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

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



Buckets (2) Info				
Create bucket				
Buckets are containers for data stored in S3. <small>Learn more</small>				
<input type="text"/> Find buckets by name				
Name	AWS Region	Access	Creation date	
cloudbucketlesson	US East (N. Virginia) us-east-1	Objects can be public	April 26, 2022, 23:01:12 (UTC-05:00)	Copy ARN Empty Delete
elasticbeanstalk-us-east-1-068007615521	US East (N. Virginia) us-east-1	Objects can be public	April 25, 2022, 23:04:58 (UTC-05:00)	

Go to the **cloudbucketlesson** bucket to upload build folders files of project.

click to the created bucket and upload files or folders of project, you can upload images, videos

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 folders**.

Files and folders (14 Total, 760.8 KB)

All files and folders in this table will be uploaded.

[Remove](#)

[Add files](#)

[Add folder](#)

[Find by name](#)

< 1 2 >

<input type="checkbox"/>	Name	Folder	Type	Size
<input type="checkbox"/>	787.4637bb57.chunk.js	static/js/	-	4.5 KB
<input type="checkbox"/>	787.4637bb57.chunk.js.map	static/js/	-	10.0 KB
<input type="checkbox"/>	asset-manifest.json	-	application/json	517.0 B
<input type="checkbox"/>	favicon.ico	-	image/x-icon	3.8 KB
<input type="checkbox"/>	index.html	-	text/html	644.0 B
<input type="checkbox"/>	logo192.png	-	image/png	5.2 KB
<input type="checkbox"/>	logo512.png	-	image/png	9.4 KB

After uploading complete go to the properties tab of bucket.

cloudbucketlesson Info

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

Static website hosting

- Disable
- Enable

Index document

Specify the home or default page of the website.

Error document - optional

This is returned when an error occurs.

Then save changes.

Amazon S3 > Buckets > cs516nov-2022-frontend.com > Edit bucket policy

Edit bucket policy Info

Bucket policy
The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts.
[Learn more](#)

[Policy examples](#) [Policy generator](#)

Bucket ARN
`arn:aws:s3:::cs516nov-2022-frontend.com`

Policy

```
1 * {
2   "Version": "2012-10-17",
3   "Id": "Policy1650912821527",
4   "Statement": [
5     {
6       "Sid": "Stmt1650912820312",
7       "Effect": "Allow",
8       "Principal": "*",
9       "Action": "s3:GetObject",
10      "Resource": "arn:aws:s3:::cs516nov-2022-frontend.com/*"
11    }
12  ]
13 }
```

Edit statement

Select a statement
Select an existing statement in the policy or add a new statement.

[+ Add new statement](#)

Edit bucket policy to getObject

[+ Add new statement](#)

JSON Ln 13, Col 1

Security: 0 Errors: 0 Warnings: 0 Suggestions: 0 [Preview external access](#)

Cancel [Save changes](#)

AWS Services Search [Alt+S] Global v vocabs/user2243686=supriya @ 8468-6651-5154

Amazon S3 > Buckets > cs516nov-2022-frontend.com > Upload

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 (14 Total, 727.7 KB)

All files and folders in this table will be uploaded.

<input type="checkbox"/>	Name	Folder	Type	Size
<input type="checkbox"/>	787.36db6797.chunk.js	static/js/	text/javascript	4.5 KB
<input type="checkbox"/>	787.36db6797.chunk.js.map	static/js/	-	10.3 KB
<input type="checkbox"/>	asset-manifest.json	-	application/json	517.0 B
<input type="checkbox"/>	favicon.ico	-	image/x-icon	3.8 KB
<input type="checkbox"/>	index.html	-	text/html	644.0 B
<input type="checkbox"/>	logo192.png	-	image/png	5.2 KB
<input type="checkbox"/>	logo512.png	-	image/png	9.4 KB
<input type="checkbox"/>	main.2dbd410b.js	static/js/	text/javascript	174.8 KB
<input type="checkbox"/>	main.2dbd410b.js.LICENSE.txt	static/js/	text/plain	1.1 KB
<input type="checkbox"/>	main.2dbd410b.js.map	static/js/	-	515.9 KB

Destination

Destination
<s3://cs516nov-2022-frontend.com>

▶ **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**

Feedback Looking for language selection? Find it in the new Unified Settings [\[\]](#)

© 2022, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

AWS Services Search [Alt+S] Global v voclabs/user2243686=supriya @ 8468-6651-5154 ▾

Uploading
Total remaining: 11 files: 538.0 KB(73.94%)
Estimated time remaining: a few seconds
Transfer rate: 13.9 KB/s

Cancel Close

Upload: status

The information below will no longer be available after you navigate away from this page.

Summary

Destination	Succeeded	Failed
s3://cs516nov-2022-frontend.com	3 files, 189.6 KB (26.06%)	0 files, 0 B (0%)

Files and folders (14 Total, 727.7 KB)

Name	Folder	Type	Size	Status	Error
787.36db6797.chunk.js	static/js/	text/javascript	4.5 KB	✓ Succeeded	-
787.36db6797.chunk.js.map	static/js/	-	10.3 KB	✓ Succeeded	-
asset-manifest.json	-	application/json	517.0 B	⌚ Pending	-
favicon.ico	-	image/x-icon	3.8 KB	⌚ Pending	-
index.html	-	text/html	644.0 B	⌚ Pending	-
logo192.png	-	image/png	5.2 KB	⌚ Pending	-
logo512.png	-	image/png	9.4 KB	⌚ Pending	-
main.2dbd410b.js	static/js/	text/javascript	174.8 KB	✓ Succeeded	-
main.2dbd410b.js.LICENSE.txt	static/js/	text/plain	1.1 KB	⌚ In Progress (100%)	-
main.2dbd410b.js.map	static/js/	-	515.9 KB	⌚ Pending	-

AWS Services Search [Alt+S] Global v voclabs/user2243686=supriya @ 8468-6651-5154 ▾

Amazon S3

Buckets Access Points Object Lambda Access Points Multi-Region Access Points Batch Operations Access analyzer for S3

Block Public Access settings for this account

Storage Lens Dashboards AWS Organizations settings

Feature spotlight 3 Feature spotlight 3

AWS Marketplace for S3

Edit static website hosting Info

Static website hosting

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

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.
 for static website hosting

Error document - optional
This is returned when an error occurs.

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

Static website hosting

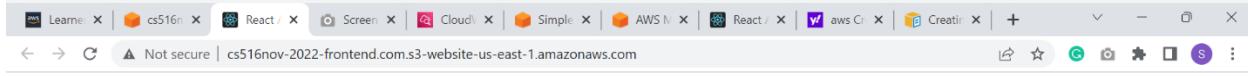
Use this bucket to host a website or redirect requests. [Learn more](#)

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://cs516nov-2022-frontend.com.s3-website-us-east-1.amazonaws.com> static website hosting url



Cloud Computing course

1. Supriya Ghising
2. Anna
3. Simran

Creating an IAM user for yourself

To create an IAM user group and attach policies with admin Access

1. Sign into the AWS Management Console and open the IAM console

The screenshot shows the AWS Management Console search results for 'IAM'. The search bar at the top has 'IAM' typed into it. On the left, there's a sidebar with categories like Services (8), Features (19), Resources (New), Blogs (1,506), Documentation (118,784), Knowledge Articles (30), Tutorials (2), Events (13), and Marketplace (413). The main area displays a list of services under 'Services'. The 'IAM' service card is highlighted with a red box. It features an icon of a person, the text 'IAM ☆', and the subtitle 'Manage access to AWS resources'. Below this, there's a 'Top features' section with links for Groups, Users, Roles, Policies, and Access Analyzer. Other services listed include 'IAM Identity Center (successor to AWS Single Sign-On)', 'Resource Access Manager', and 'Serverless Application Repository'. At the bottom, there are 'See all 8 results' and 'See all 19 results' buttons.

2. In the navigation pane, choose **User groups** and then choose **Create group**.

The screenshot shows the AWS Identity and Access Management (IAM) console. The left sidebar is titled 'Identity and Access Management (IAM)' and contains several navigation options: 'Search IAM', 'Dashboard', 'Access management' (with 'User groups' highlighted and a red box around it), 'Users', 'Roles', 'Policies', 'Identity providers', 'Account settings', 'Access reports' (with 'Archive rules', 'Analyzers', 'Settings', 'Credential report', 'Organization activity', and 'Service control policies (SCPs)' listed). The main content area is titled 'User groups (2) Info' and includes a description: '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 lists two user groups: 'Admin' (3 users, Defined, 4 months ago) and 'DevOps' (2 users, Defined, 24 hours ago). The 'Create group' button is located at the top right of the table area, also with a red box around it.

<input type="checkbox"/>	Group name	Users	Permissions	Creation time
<input type="checkbox"/>	Admin	3	Defined	4 months ago
<input type="checkbox"/>	DevOps	2	Defined	24 hours ago

3. Type the name of the group in **User group name**

S | Services | Search [Alt+S] | Global ▾ | abhay-rawal ▾ | ⓘ

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups **(Selected)**
- Users
- Roles
- Policies
- Identity providers
- Account settings

Access reports

- Access analyzer
- Archive rules
- Analyzers
- Settings
- Credential report
- Organization activity
- Service control policies (SCPs)

IAM > User groups > Create user group

Create user group

Name the group

User group name
Enter a meaningful name to identify this group.

Administrator

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

Add users to the group - Optional (7) 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.

<input type="checkbox"/>	User name	Groups	Last activity	Creation time
<input type="checkbox"/>	abhay-admin1	1	18 days ago	4 months ago
<input type="checkbox"/>	abhay-admin2	1	None	4 months ago
<input type="checkbox"/>	abhay-cloud	1	24 hours ago	24 hours ago
<input type="checkbox"/>	abhay-devops	1	20 hours ago	24 hours ago

4. In the list of policies, search for **AdministratorAccess**, select the check box to apply the policy to all group members, and then Choose **Create group**.

The screenshot shows the 'Attach permissions policies' dialog in the AWS IAM console. At the top, it says 'Optional (Selected 1/816)' and 'Info'. Below is a search bar with 'AdministratorAccess' and a 'Clear filters' button. A table lists policies: 'AdministratorAccess' (selected, highlighted with a red box), 'AdministratorAccess-Amplify', 'AdministratorAccess-AWSElasticBeanstalk', and 'AWSAuditManagerAdministratorAccess'. The 'AdministratorAccess' row includes columns for Type (AWS managed - job function) and Description (Provides full access to AWS services). At the bottom right are 'Cancel' and 'Create group' buttons, with 'Create group' also highlighted with a red box.

Policy name	Type	Description
<input checked="" type="checkbox"/> AdministratorAccess	AWS managed - job function	Provides full access to AWS services
<input type="checkbox"/> AdministratorAccess-Amplify	AWS managed	Grants account administrator access to AWS Amplify
<input type="checkbox"/> AdministratorAccess-AWSElasticBeanstalk	AWS managed	Grants account administrator access to AWS Elastic Beanstalk
<input type="checkbox"/> AWSAuditManagerAdministratorAccess	AWS managed	Provides administrative access to AWS Audit Manager

Creating IAM users and adding to a group

1. Sign into the AWS Management Console and open the IAM console
2. In the navigation pane, choose **Users** and then select **Add users**.

The screenshot shows the AWS Identity and Access Management (IAM) service interface. On the left, there's a navigation sidebar with various options like Dashboard, User groups, Roles, Policies, Identity providers, Account settings, and more. Under 'Access management', the 'Users' option is selected and highlighted with a red box. The main content area shows a table of existing IAM users. The columns include User name, Groups, Last activity, MFA, Password age, and Active key age. The table lists seven users: abhay-admin1, abhay-admin2, abhay-cloud, abhay-devops, abhay-devops1, abhay-iam-assume, and TestAdmin. A blue box highlights the 'Add users' button at the top right of the table header.

	User name	Groups	Last activity	MFA	Password age	Active key age
<input type="checkbox"/>	abhay-admin1	Admin	()	Virtual	⚠ 133 days ago	()
<input type="checkbox"/>	abhay-admin2	Admin	()	None	⚠ 133 days ago	()
<input type="checkbox"/>	abhay-cloud	Admin	()	None	✓ Yesterday	()
<input type="checkbox"/>	abhay-devops	DevOps	()	None	✓ 24 hours ago	()
<input type="checkbox"/>	abhay-devops1	DevOps	()	None	✓ 24 hours ago	()
<input type="checkbox"/>	abhay-iam-assume	None	()	None	✓ 18 days ago	()
<input type="checkbox"/>	TestAdmin	None	()	None	✓ 32 minutes ago	()

- Type the user name for the new user. This is the sign-in name for AWS.
- If you want to add multiple users, choose to **Add another user** for each additional user and type their usernames. You can add up to 10 users at one time.

The screenshot shows the AWS IAM 'Create user' wizard. The top navigation bar includes the AWS logo, 'Services' dropdown, search bar, and user 'abhay-rawal'. The left sidebar shows steps: 'Step 1 Specify user details' (selected), 'Step 2 Set permissions', and 'Step 3 Review and create'. The main content area is titled 'Specify user details' and contains a 'User details' section. The 'User name' field is highlighted with a red border and contains the value 'AdminOne'. Below it is a note: 'The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)'. There is an optional checkbox 'Provide user access to the AWS Management Console - optional' which is unchecked. A note below it says: '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 right are 'Cancel' and 'Next' buttons.

4. Select the type of access this set of users will have. If you want to Provide user access to the AWS Management Console, Click on Checkbox. For this demo we will click on Checkbox.

Note: If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user.

- a. Now we need to select if we want to Specify a user in Identity Center or Create an IAM user. **Choose "I want to create an IAM user".**
 - After selecting **I want to create an IAM user**, you can choose one of the Password:
 - a. **Autogenerated password.** Each user gets a randomly generated password that meets the account password

policy. You can view or download the passwords when you get to the **Final** page.

b. **Custom password.** Each user is assigned the password that you type in the box.

- For this demo uncheck **Users must create a new password at next sign-in.**
- Click Next

The screenshot shows the AWS IAM User Creation process. In Step 3, the 'User name' is set to 'AdminOne'. Under 'Provide user access to the AWS Management Console - optional', the 'I want to create an IAM user' option is selected. In the 'Console password' section, 'Custom password' is chosen, and a password is entered. A red box highlights the 'Custom password' section. A red arrow points to the 'Uncheck' button next to the 'Users must create a new password at next sign-in (recommended)' checkbox. The 'Next' button is also highlighted with a red box.

5. On the **Set permissions** page, **Add user to group**. You can select one or more existing groups.

The screenshot shows the AWS IAM 'Create user' wizard at Step 2: Set permissions. The 'Add user to group' option is selected. The 'User groups' table lists three groups: Admin, Administrator, and DevOps. The 'Administrator' row is selected and highlighted with a red box. At the bottom right, the 'Next Step' button is highlighted with a red box.

Step 1 Specify user details

Step 2 Set permissions

Step 3 Review and create

Step 4 Retrieve password

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 (1/3)

Group name	Users	Attached policies	Created
Admin	3	AdministratorAccess	2022-10-19 (4 months ago)
<input checked="" type="checkbox"/> Administrator	0	AdministratorAccess	2023-03-01 (2 minutes ago)
DevOps	2	None	2023-02-28 (Yesterday)

Permissions boundary - optional
Set a permissions boundary to control the maximum permissions for this user. Use this advanced feature used to delegate permission management to others. [Learn more](#)

Cancel Previous **Next**

6. On Review and Create Page, Click on Create User. You can also create Tags on this page. (Optional).

The screenshot shows the 'Review and create' step of the AWS IAM 'Create user' wizard. On the left, a sidebar lists steps: Step 1 (Specify user details), Step 2 (Set permissions), Step 3 (Review and create), and Step 4 (Retrieve password). The main area displays 'User details' (User name: AdminOne, Console password type: Custom password, Require password reset: No) and a 'Permissions summary' table showing one group assignment: Administrator (Group, Used as Permissions group). Below this is a 'Tags - optional' section with an 'Add new tag' button and a note about adding up to 50 more tags. At the bottom right are 'Cancel', 'Previous', and a prominent yellow 'Create user' button, which is highlighted with a red box.

7. You will be then Redirected to Retrieve Password page. Click on Download .csv File to download credentials for the user. Then Click on Return to users list.

warn | Services Search [Alt+S] Global abhay-rawal

User created successfully
You can view and download the user's password and email instructions for signing in to the AWS Management Console.

IAM > Users > Create user

Step 1 Specify user details

Step 2 Set permissions

Step 3 Review and create

Step 4 Retrieve password

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

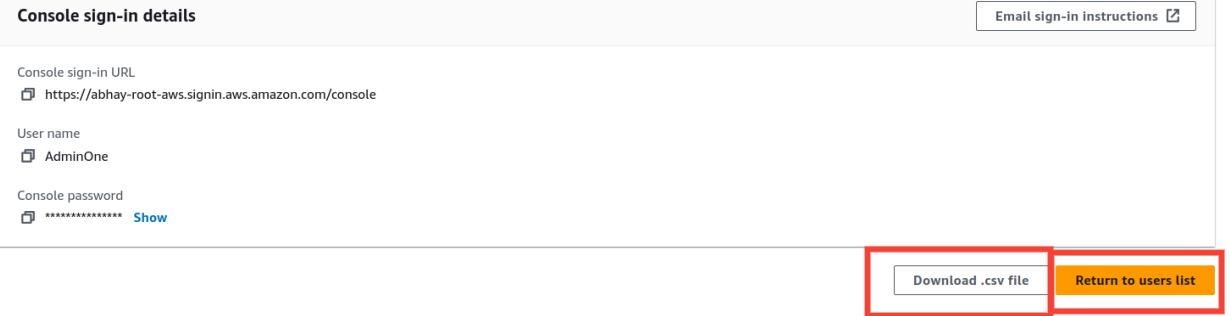
Email sign-in instructions

Console sign-in URL: https://abhay-root-aws.signin.aws.amazon.com/console

User name: AdminOne

Console password: ***** Show

Download .csv file Return to users list



Setting up a billing alarm on CloudWatch

Go to the CloudWatch Display. Search or Find under All Services Management & Governance Group

Services ▾

Search results for 'cloudwatch'

Services (2)

Features (8)

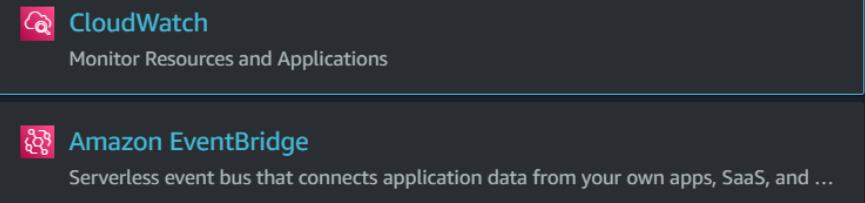
Documentation (47,836)

Marketplace (168)

Services

CloudWatch Monitor Resources and Applications

Amazon EventBridge Serverless event bus that connects application data from your own apps, SaaS, and ...



Go to the Alarms Display. You must select us-east-1 N.Virginia region. Otherwise, billing metric is not there.

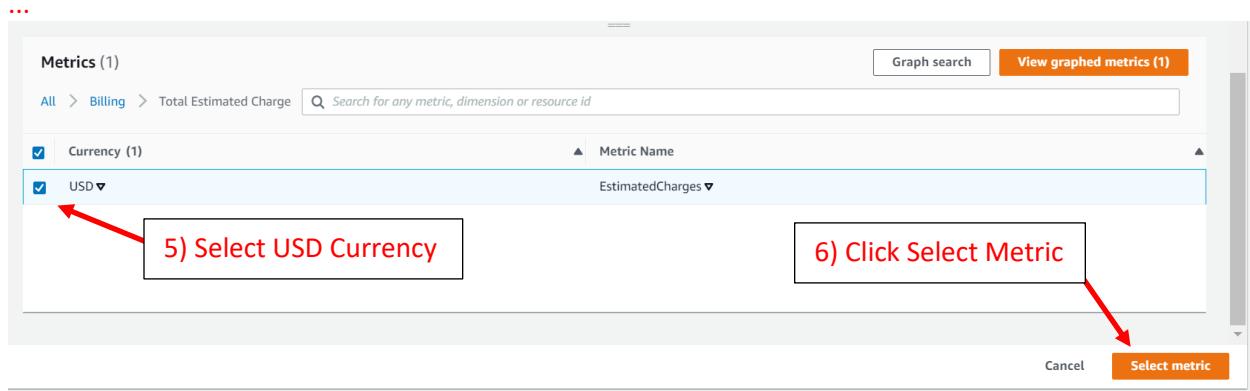
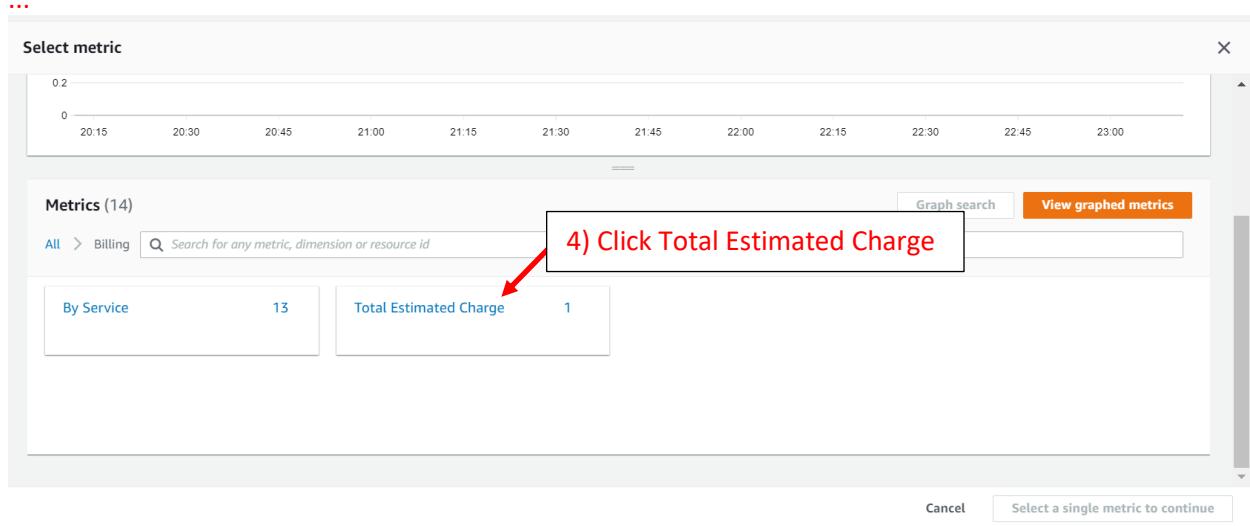
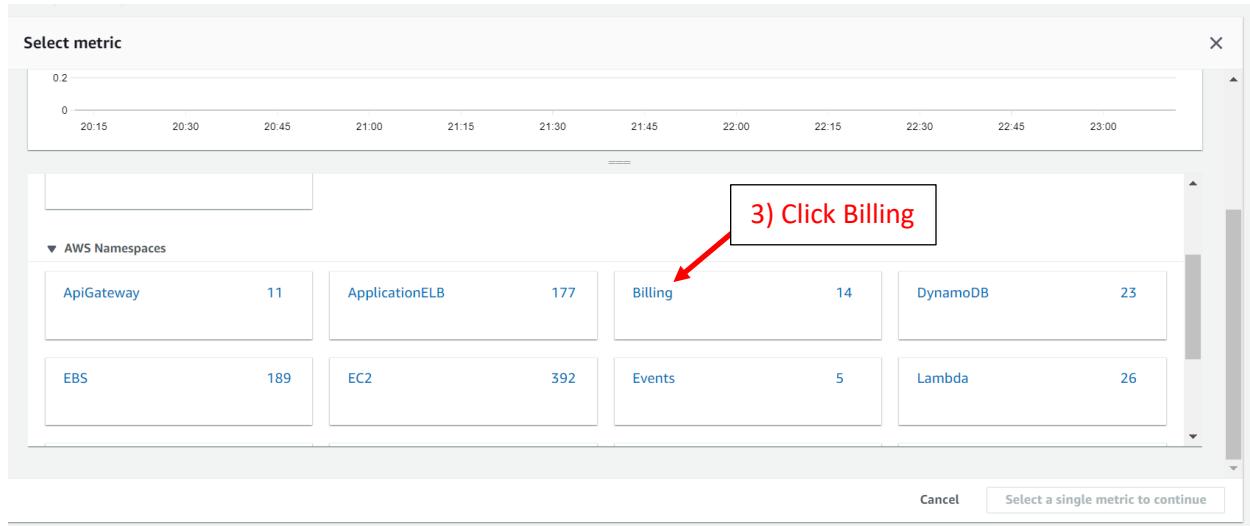


The screenshot shows the AWS CloudWatch Metrics interface. On the left, a sidebar lists various services: Dashboards, Alarms, Logs, Metrics, Events, Rules, ServiceLens, and Resource Health. The 'Alarms' section is highlighted with a red arrow and a callout box containing the text '1) Click on Alarms'. The main pane displays an 'Overview' of alarms, with a red box highlighting the 'Recent alarms' section. A red arrow points from the 'Recent alarms' box to another red box containing the text 'Make sure region is N.Virginia'. Below the overview, there's a section titled 'Alarms by AWS service' which includes a chart for 'DYNAMODB'.

Create Billing Alarm

This screenshot shows the 'Create Billing Alarm' wizard at Step 1: 'Specify metric and conditions'. The left sidebar shows steps: Step 1 (current), Step 2, Step 3, and Step 4. The main area has a title 'Specify metric and conditions'. It contains a 'Metric' section with a 'Graph' preview and a 'Select metric' button. A red box highlights the 'Select metric' button with the text '2) Click Select Metric'. To the right, there are 'Cancel' and 'Next' buttons.

This screenshot continues the 'Create Billing Alarm' wizard at Step 1. The left sidebar shows steps: Step 1 (current), Step 2, Step 3, and Step 4. The main area has a title 'Specify metric and conditions'. It contains a 'Metric' section with a 'Graph' preview and a 'Select metric' button. A red box highlights the 'Select metric' button with the text '2) Click Select Metric'. To the right, there are 'Cancel' and 'Next' buttons.



Step 1
Specify metric and conditions

Step 2
Configure actions

Step 3
Add name and description

Step 4
Preview and create

Specify metric and conditions

Metric

Edit

Graph

This alarm will trigger when the blue line goes above the red line for 1 datapoints within 6 hours.

No unit

1



0.8

0.6

0.4

0.2

0

07/01 07/03 07/05 07/07

EstimatedCharges

Namespace

AWS/Billing

Metric name

EstimatedCharges

Currency

USD

Statistic

Maximum



Period

6 hours

Conditions

Threshold type

Static

Use a value as a threshold

Anomaly detection

Use a band as a threshold

Whenever EstimatedCharges is...

Define the alarm condition.

Greater
> threshold

Greater/Equal

\geq threshold

Lower/Equal
 \leq threshold

Lower
< threshold

than...

Define the threshold value.

1

USD

7) Pick Some Conditions

Must be a number

► Additional configuration

8) Click Next

Cancel

Next

Step 1
Specify metric and conditions

Step 2
Configure actions

Step 3
Add name and description

Step 4
Preview and create

Configure actions

Notification

Alarm state trigger

Define the alarm state that will trigger this action.

In alarm

The metric or expression is outside of the defined threshold.

OK

The metric or expression is within the defined threshold.

Remove

Insufficient data

The alarm has just started or not enough data is available.

Select an SNS topic

Define the SNS (Simple Notification Service) topic that will receive the notification.

Select an existing SNS topic

Create new topic

Use topic ARN

9) Select Create New SNS Topic

Create a new topic...

The topic name must be unique.

MyBillingAlarm

10) Name Topic

SNS topic names can contain only alphanumeric characters, hyphens (-) and underscores (_).

Email endpoints that will receive the notification...

Add a comma-separated list of email addresses. Each address will be added as a subscription to the topic above.

jc@miu.edu

user1@example.com, user2@example.com

11) Enter Email

Create topic

Add notification

12) Click Create Topic

...

Send a notification to...

MyBillingAlarm

X

Only email lists for this account are available.

Email (endpoints)

jc@miu.edu - [View in SNS Console](#)

Add notification

Auto Scaling action

Add Auto Scaling action

EC2 action

This action is only available for EC2 Per-Instance Metrics.

Add EC2 action

Systems Manager action [Info](#)

This action will create an Incident or OpsItem in Systems Manager when the alarm is **In alarm** state.

Add Systems Manager action

13) Click Next

Cancel

Previous

Next

...

Add name and description

Name and description

Alarm name 14) Name Alarm

MyBillingAlarm

Alarm description - optional

Alarm description

Up to 1024 characters (0/1024)

15) Click Next

Cancel Previous Next

Step 3: Add name and description Edit

Name and description

Name
MyBillingAlarm

Description
-

16) Preview Alarm and Click Create Alarm

Cancel Previous Create alarm

Practicing an IAM policy with a condition

1 Create group named “Developer”

Screenshot of the AWS IAM 'Create user group' page. The 'User group name' field contains 'Developers'. The left sidebar shows 'Access management' with 'User groups' selected.

2 Create Two Users E.g

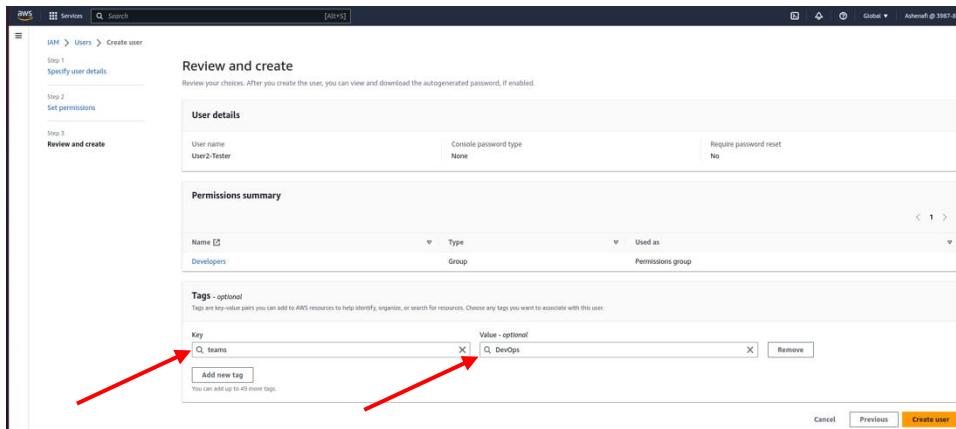
- User1-DevOps with Tag “teams” =”DevOps”

Screenshot of the AWS IAM 'Specify user details' step. The 'User name' field contains 'User1-devOps'. The left sidebar shows 'Step 1 Specify user details' selected.

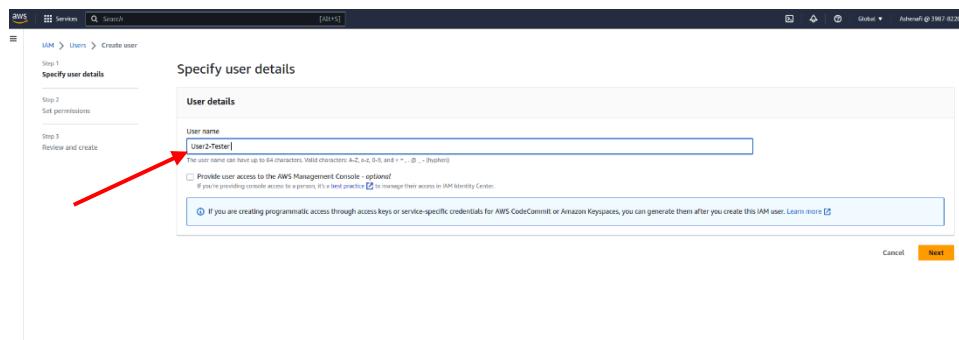
Add the user to Developer user Group

Screenshot of the AWS IAM 'Set permissions' step. The 'User groups' section shows 'Developers' selected. The left sidebar shows 'Step 2 Set permissions' selected.

Add tag to user



- **User2-Tester**



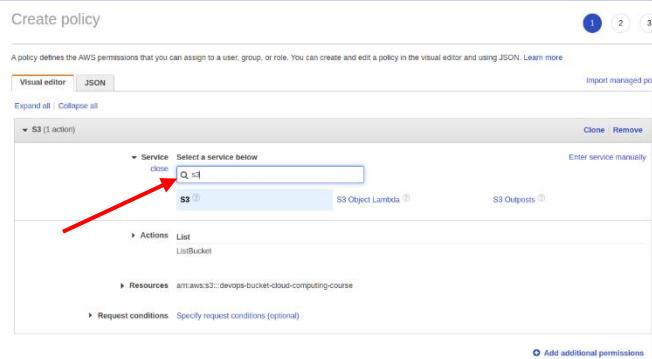
3 Create S3 Bucket

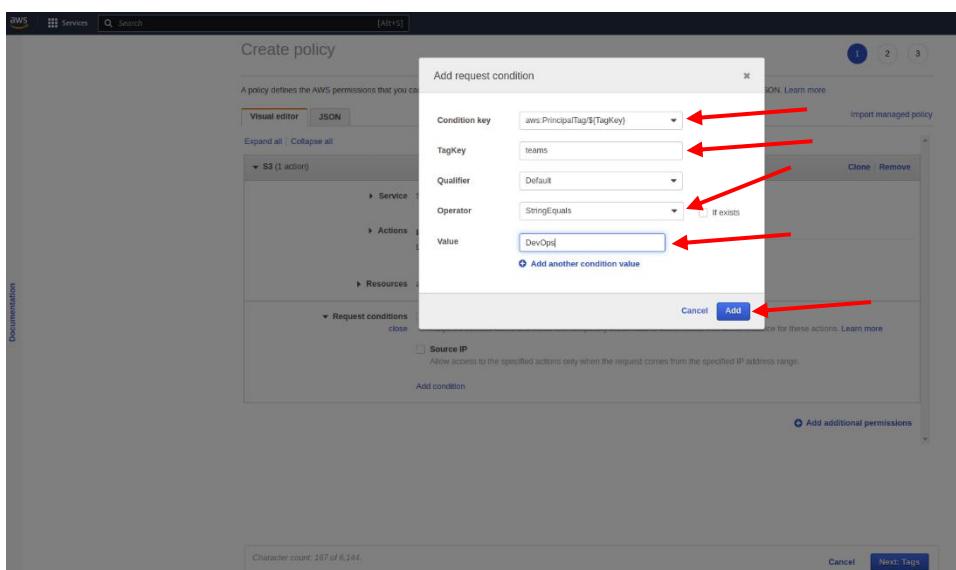
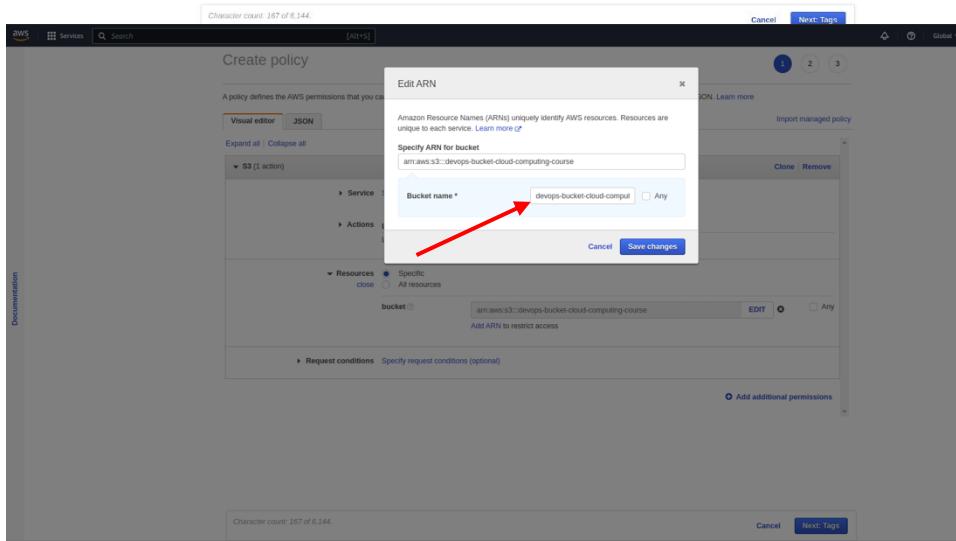
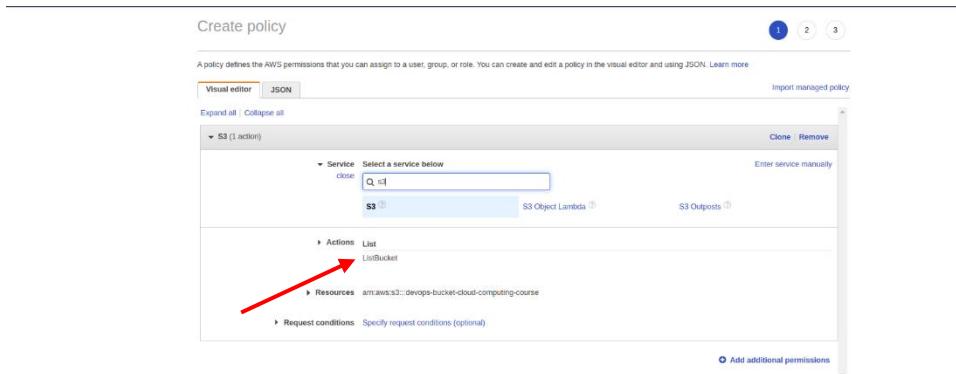
devops-bucket-cloud-computing-course

4 Put Object/file to the Bucket

file1.txt

5 Create a custom IAM policy with Condition {tag name= **teams** value=**DevOps**}





Create policy

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. Learn more

Visual editor JSON

Import managed policy

Documentation

Expand all | Collapse all

S3 (1 action)

Service: S3

Actions: List
ListBucket

Resources: arn:aws:s3:::devops-bucket-cloud-computing-course

Request conditions:

- MFA required
- Source IP
- aws:PrincipalTag/teams (StringEquals DevOps) (Edit | Remove)

Add another condition

Add additional permissions

Character count: 232 of 6,144.

Cancel Next: Tags

Create policy

Review policy

Name*: DevOpsTagAccessToListS3

Description: this allows a user with a tag name teams and tag value DevOps a permission to access an s3 bucket

Summary

Service	Access level	Resource	Request condition
S3	Limited: List	BucketName string like devops-bucket-cloud-computing-course	aws:PrincipalTag/teams = DevOps

Tags

Key	Value
No tags associated with the resource.	

Attach the create Policy to the user group “Developers”

IAM > User groups > Developers

Developers

Summary

User group name: Developers

Creation time: March 01, 2023, 14:55 (UTC-06:00)

ARN: arn:aws:iam:398782202019:group/Developers

Permissions

Permissions policies (1) Info

You can attach up to 10 managed policies.

Policy name: S3AccessUsingTagFromUser

Type: Customer managed

Description: this allows users to access an s3 bucket using the users tag name if userType is equal DevOps

Actions: Delete, Edit, Attach policies, Create inline policy

The screenshot shows the AWS IAM Policies list. A specific policy, "DevOpsTagAccessIotListS3", is highlighted with a red arrow pointing to its name. The policy description states: "this allows a user with a tag name teams and tag value DevOps permission to access an s3 bucket".

The screenshot shows the IAM User Groups page for the "Developers" group. The "Permissions" tab is selected, displaying the attached policies. A red arrow points to the "Add permissions" button at the top right of the list.

6 Test

Log in using both users created above and try to access your S3 buckets
DevOpsUser with tag name “**teams**” and tag value “**DevOps**”

The screenshot shows the Amazon S3 Buckets list. A specific bucket, "devops-bucket-ebs-computing-course", is highlighted with a red arrow. The bucket details show it was created on March 1, 2023, at 14:32:52 UTC-06:00.

Tester User with not tag name and value

The screenshot shows the Amazon S3 Buckets list for the Tester User. The list is currently empty, showing "No buckets". A red arrow points to the "Create bucket" button at the bottom right of the list.