Assignment 1 – IaaS and FaaS

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.
2. Configure a web server on EC2.
    a. Select the instance
    b. Hit Connect
    c. Select the "Session Manager" tab and hit Connect.
    d. 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.

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
4. Call the API in React and deploy the front-end app in S3.
    a. Install NodeJS on your laptop
    b. npx create-react-app appname
    c. npm install axios
    d. npm start – to start your front-end app
    e. npm run build – after testing, build the app
    f. create a bucket and deselect "Block public access"
    g. drop all files inside the build folder into the bucket.
    h. Write a policy that makes all objects in the bucket public. Refer to the next section.
    i. Enable "static website hosting" and define the index.html as the index and error page.
5. Create your own AWS account. You must connect your credit or bank card otherwise, services will be unavailable. Do the following 3 tasks. Then don't do anything else without my approval. Otherwise, It will charge you. If you want to practice something in AWS, use the Academy account.
    a. Enable MFA for the root user.
    b. Create an admin group with an administrator policy. Create a user for yourself in that group. Always use that IAM user. Not your root user.
    c. Set up a billing alarm.
6. Attach an IAM profile to your instance that has the following policies
    a. Session manager (It is already there)
    b. S3 read-only
    c. RDS read-only

Snippets

The bucket policy that makes all objects inside it public:

```
{
  "Id": "Policy1650912821527",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1650912820312",
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::<yourbucket>/*",
      "Principal": "*"
    }
  ]
}
```

```javascript
import axios from "axios";
import { useEffect, useState } from "react";

export default function App() {
  const [students, setstudents] = useState([]);

  useEffect(() => {
    async function fetchStudents() {
      const studentsFromLambda = (
        await axios.get(
          "your lambda URL"
        )
      ).data;
      setstudents(studentsFromLambda);
      console.log(studentsFromLambda);
    }

    fetchStudents();
  }, []);
  return (
    <div>
      Cloud Computing course
      <ol>
        {students.map((student) => (
          <li>{student}</li>
        ))}
      </ol>
    </div>
  );
}
```
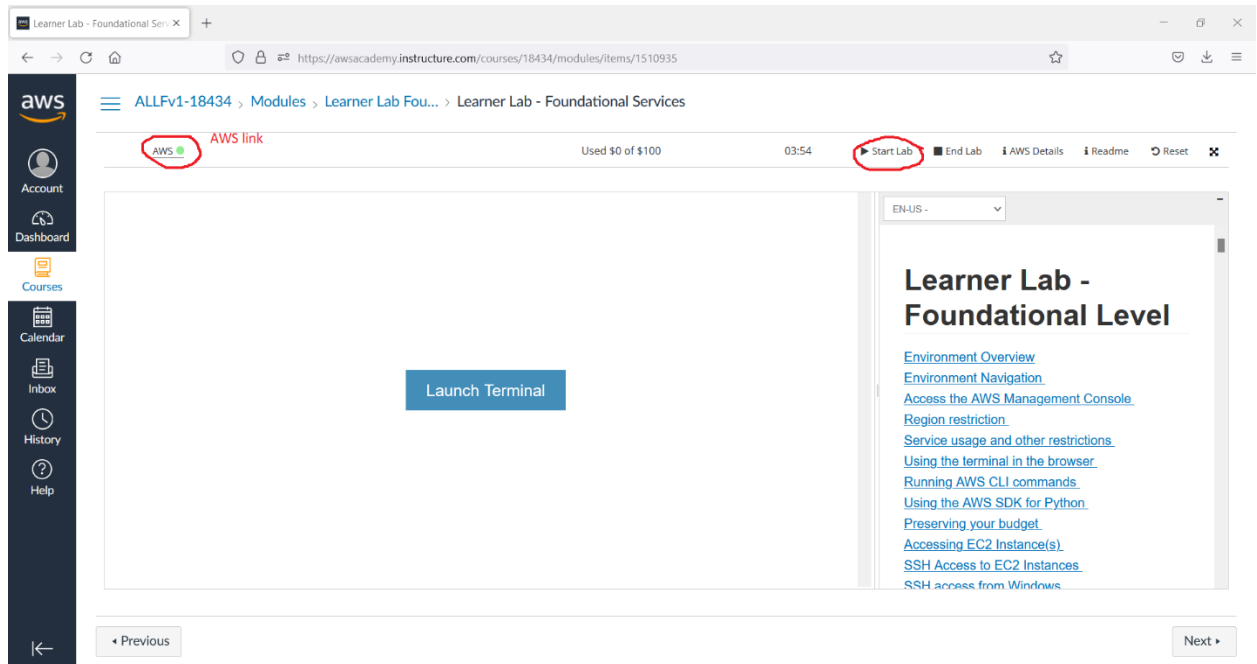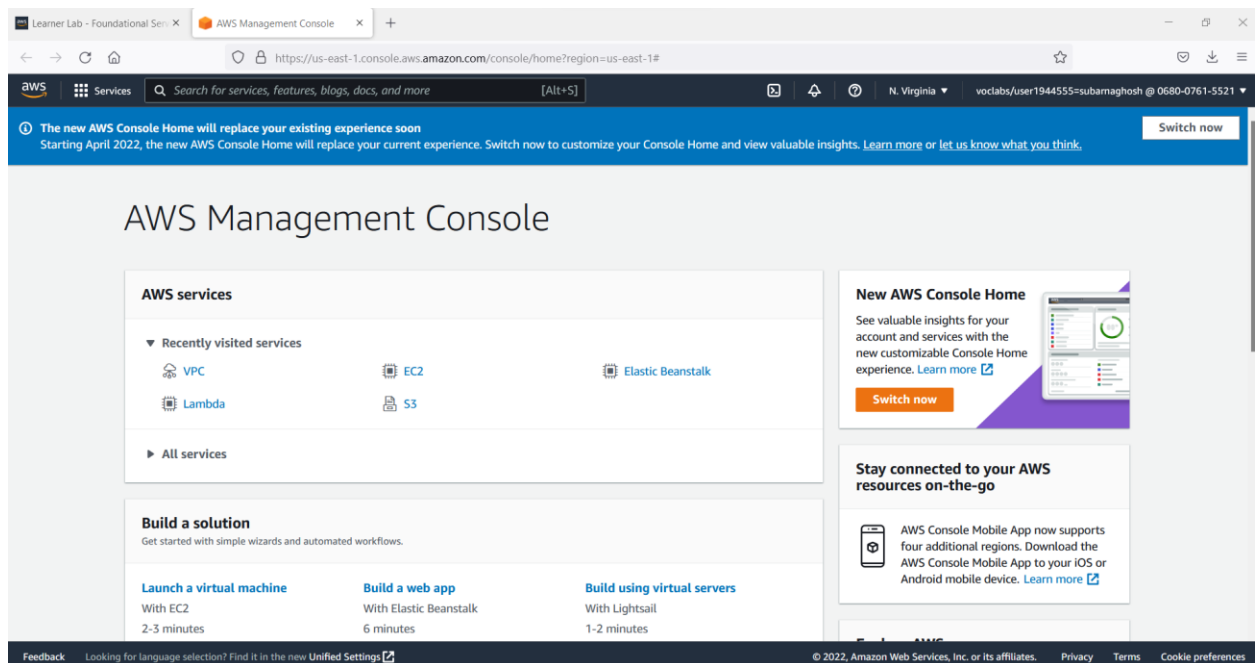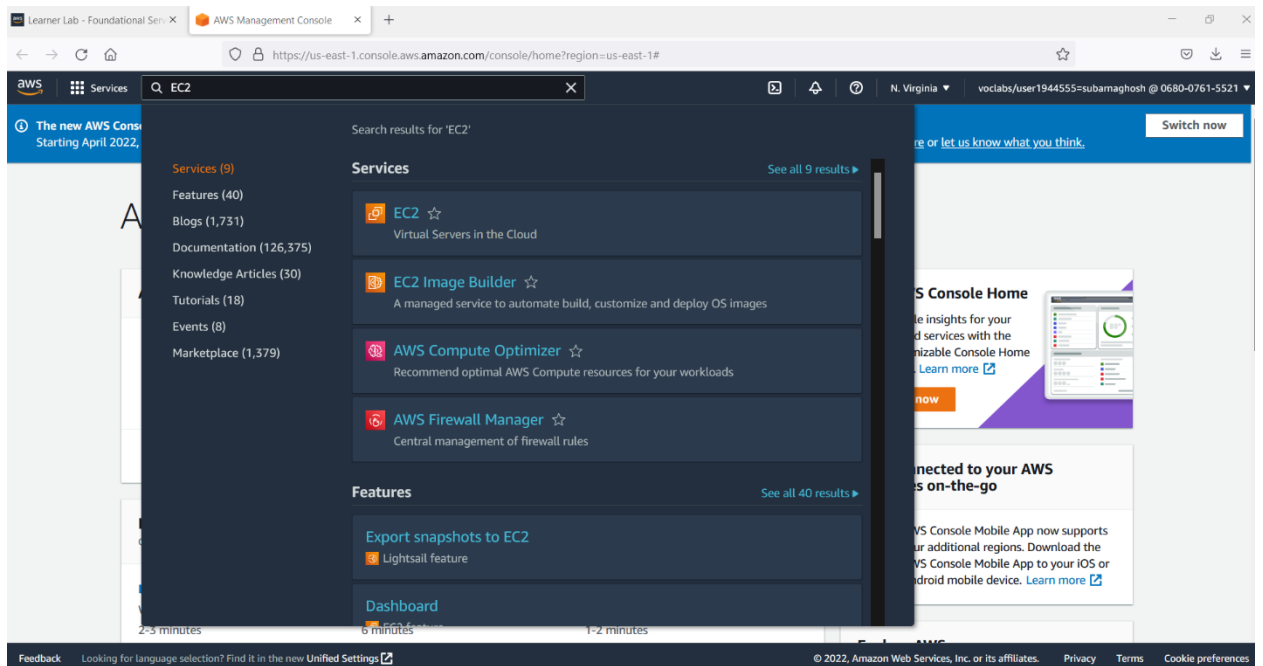
Setting up a web server on EC2

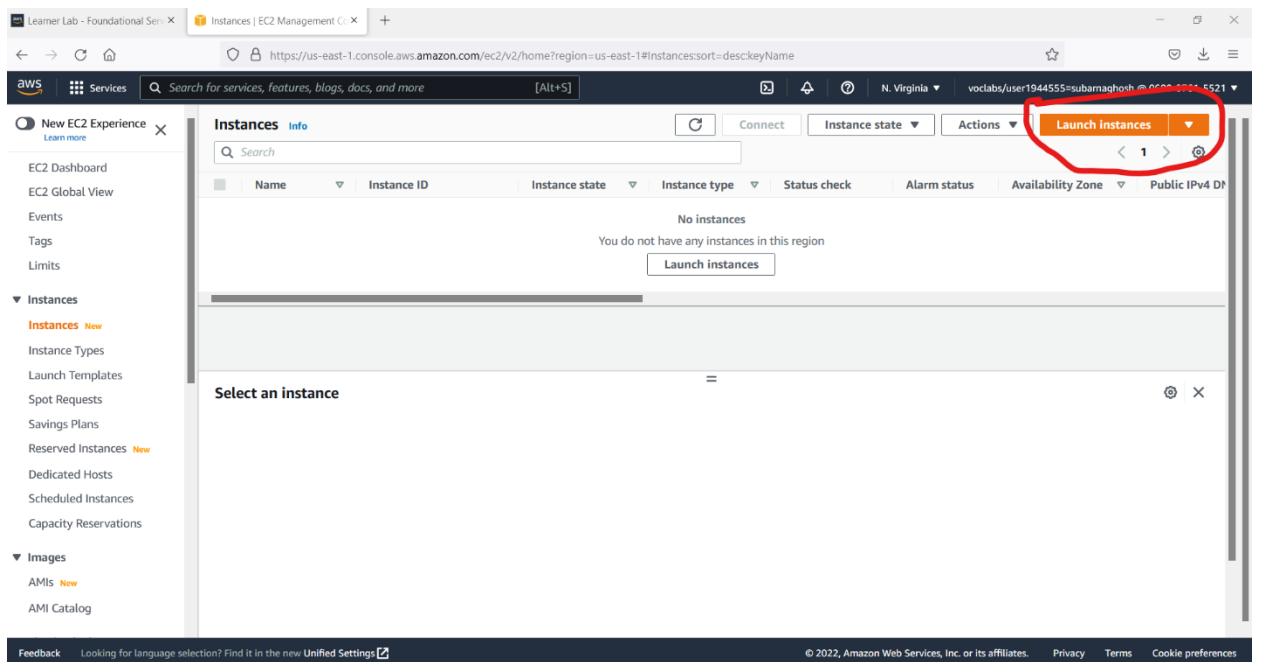1) Create an account in AWS student academy and then go to Courses -> module -> Foundational services then start lab.

2) Go to AWS link

3) Search EC2 service

4) Go to EC2 and launch instances

5) Name and tags

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

Name

My first cloud server

Add additional tags

6) Application and OS image

aws ::: Services | Search for services, features, blogs, docs, and more [Alt+S] | N. Virginia ▼ | voclabs/user19445

▼ **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

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

Recents | **Quick Start**

| Amazon Linux | Ubuntu | Windows | Red Hat | SUSE Linux | Browse more AMIs |
| aws | ubuntu | Microsoft | Red Hat | SUSE | Including AMIs from AWS, Marketplace and the Community |

Amazon Machine Image (AMI)

Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type
ami-0f9fc25dd2506cf6d (64-bit (x86)) / ami-06b8f0fe534eceb95 (64-bit (Arm))
Virtualization: hvm   ENA enabled: true   Root device type: ebs

Free tier eligible

Description

Amazon Linux 2 Kernel 5.10 AMI 2.0.20220419.0 x86_64 HVM gp2

Architecture

64-bit (x86) ▼

AMI ID

ami-0f9fc25dd2506cf6d

▼ **Summary**

Number of instances Info

1

Software Image (AMI)
Amazon Linux 2 Kernel 5.10 AMI...read more
ami-0f9fc25dd2506cf6d

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 ✕

Cancel | **Launch instance**

7) Instance type

8) Key pair setup

9) Create new key pair

After creating key pair, it downloads the .ppk file.

10) Launch instance

11) Launch initiating and successful
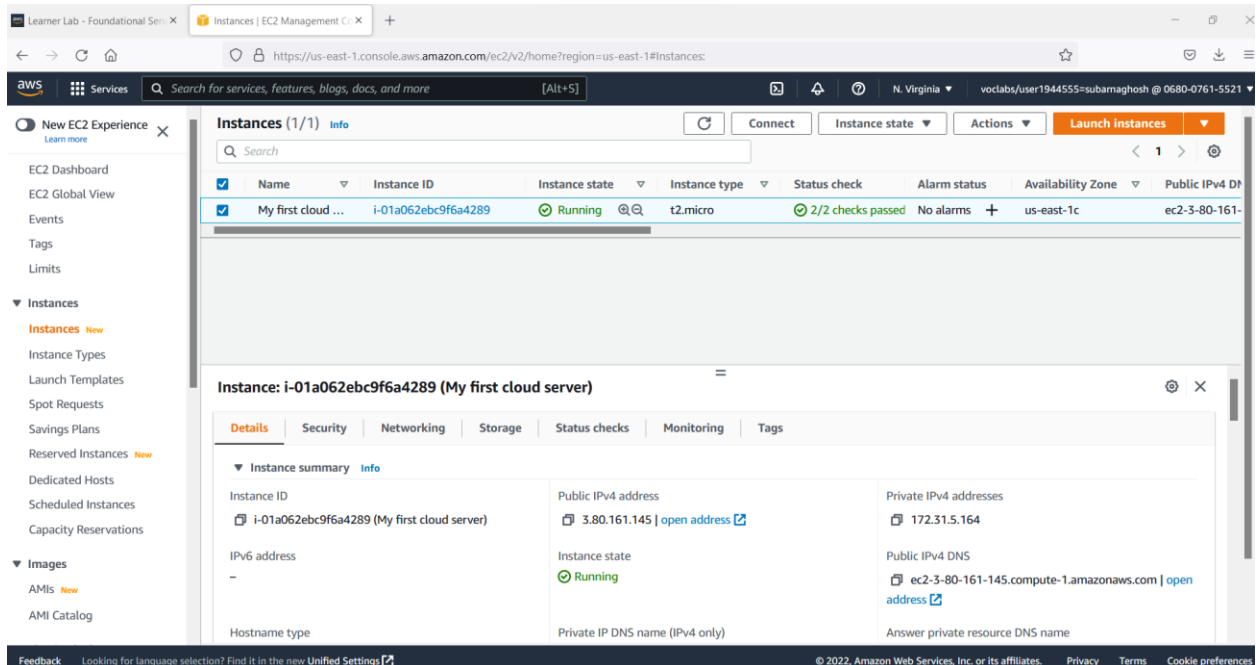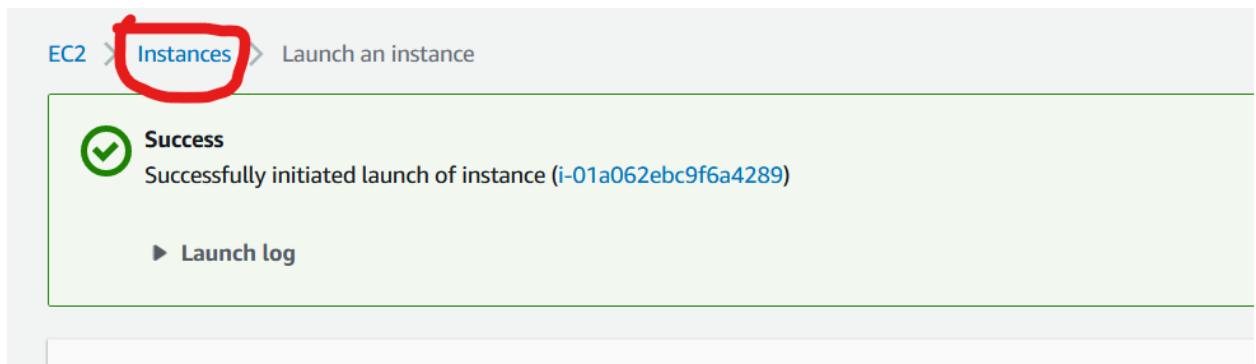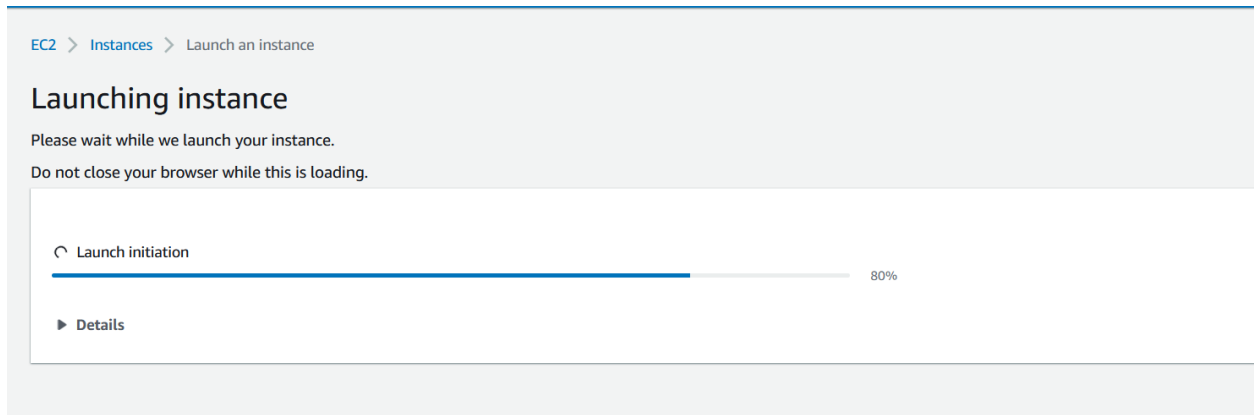
12) Click on instance ID and go to the security tab

13) Click on the security groups ID and edit inbound rules

14) Add SSH and HTTP inbound rule

15) Go to PuTTy Configuration and setup public IP and key

PuTTY Configuration

? ✕

Category:

- Session
  - Logging
- Terminal
  - Keyboard
  - Bell
  - Features
- Window
  - Appearance
  - Behaviour
  - Translation
  - Selection
  - Colours
- Connection
  - Data
  - Proxy
  - SSH
  - Serial
  - Telnet
  - Rlogin
  - SUPDUP

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address)   Port

3.80.161.145   22

Connection type:

⦿ SSH   ◯ Serial   ◯ Other: Telnet ⌄

Load, save or delete a stored session

Saved Sessions

Default Settings   Load

                                   Save

                                   Delete

Close window on exit:
◯ Always   ◯ Never   ⦿ Only on clean exit

About   Help   Open   Cancel

PuTTY Configuration

? ✕

Category:

- Logging
- Terminal
  - Keyboard
  - Bell
  - Features
- Window
  - Appearance
  - Behaviour
  - Translation
  - Selection
  - Colours
- Connection
  - Data
  - Proxy
  - SSH
    - Kex
    - Host keys
    - Cipher
    - Auth
    - TTY
    - X11
    - Tunnels
    - Bugs
    - More bugs

Options controlling SSH authentication

☑ Display pre-authentication banner (SSH-2 only)
☐ Bypass authentication entirely (SSH-2 only)
☐ Disconnect if authentication succeeds trivially

Authentication methods
☑ Attempt authentication using Pageant
☐ Attempt TIS or CryptoCard auth (SSH-1)
☑ Attempt "keyboard-interactive" auth (SSH-2)

Authentication parameters
☐ Allow agent forwarding
☐ Allow attempted changes of username in SSH-2
Private key file for authentication:

C:\Users\Asus\Downloads\my first key pair.   Browse...

About   Help   Open   Cancel

3.80.161.145 - PuTTY

PuTTY Security Alert

The server's host key is not cached in the registry. You have no guarantee that the server is the computer you think it is.

The server's ssh-ed25519 key fingerprint is:
ssh-ed25519 255 SHA256:Qles9ZNiHrpOo5+zk4NS41eELnTD6ufEbp9TOZ8zHeQ

If you trust this host, press "Accept" to add the key to PuTTY's cache and carry on connecting.

If you want to carry on connecting just once, without adding the key to the cache, press "Connect Once".

If you do not trust this host, press "Cancel" to abandon the connection.

Help   More info...   Accept   Connect Once   Cancel

Spot
Savin

ec2-user@ip-172-31-5-164:~

```
login as: ec2-user
Authenticating with public key "my first key pair"

       __|  __|_  )
       _|  (     /    Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-172-31-5-164 ~]$
```

root@ip-172-31-5-164:/home/ec2-user — □ X

```
      __|  __|_  )
      _|  (     /    Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-172-31-5-164 ~]$ sudo -s
[root@ip-172-31-5-164 ec2-user]# yum install httpd
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
amzn2-core                                              | 3.7 kB     00:00
Resolving Dependencies
--> Running transaction check
---> Package httpd.x86_64 0:2.4.52-1.amzn2 will be installed
--> Processing Dependency: httpd-tools = 2.4.52-1.amzn2 for package: httpd-2.4.5
2-1.amzn2.x86_64
--> Processing Dependency: httpd-filesystem = 2.4.52-1.amzn2 for package: httpd-
2.4.52-1.amzn2.x86_64
--> Processing Dependency: system-logos-httpd for package: httpd-2.4.52-1.amzn2.
x86_64
--> Processing Dependency: mod_http2 for package: httpd-2.4.52-1.amzn2.x86_64
--> Processing Dependency: httpd-filesystem for package: httpd-2.4.52-1.amzn2.x8
6_64
--> Processing Dependency: /etc/mime.types for package: httpd-2.4.52-1.amzn2.x86
_64
```


root@ip-172-31-5-164:/home/ec2-user — □ X

```
  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]#
```

16) Access public IP from browser
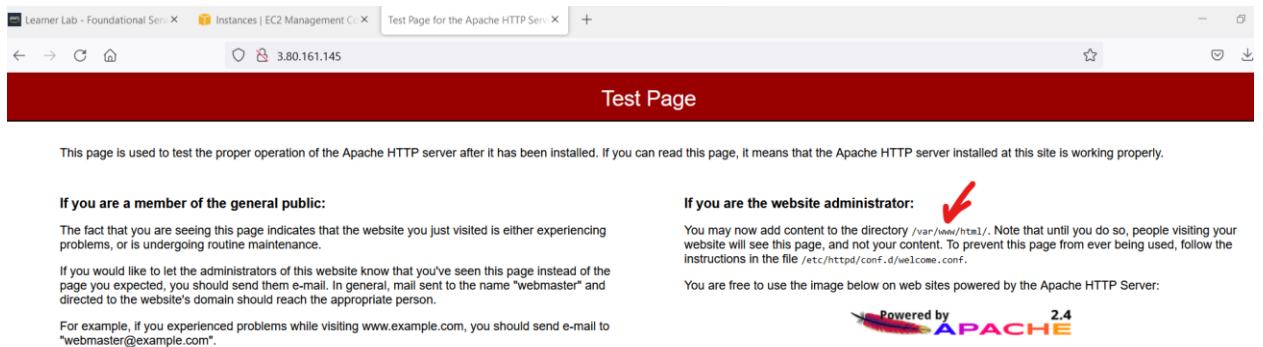
17) Go to console and go to /var/www/html/ to create index.html file

18) Go to the website and reload

Welcome to the cloud computing course, MIU
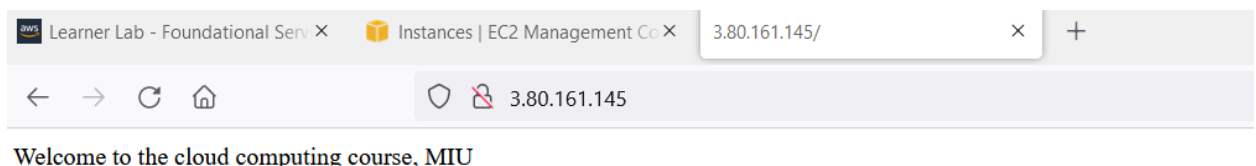
Creating Lambda with public URL
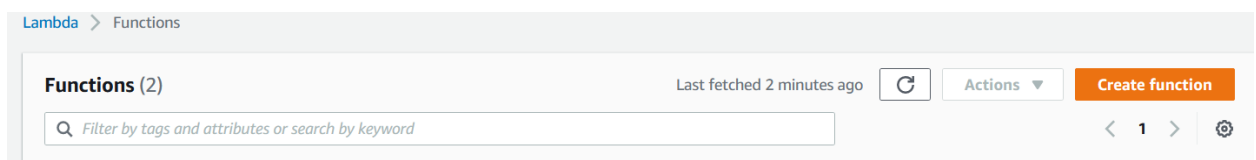
Create function Info

Choose one of the following options to create your function.

Author from scratch ⦿	Use a blueprint ○	Container image ○	Browse serverless app repository ○
Start with a simple Hello World example.	Build a Lambda application from sample code and configuration presets for common use cases.	Select a container image to deploy for your function.	Deploy a sample Lambda application from the AWS Serverless Application Repository.

Basic information

Function name
Enter a name that describes the purpose of your function.

> MyFirstLambda

Use only letters, numbers, hyphens, or underscores with no spaces.

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

> Node.js 14.x ▼

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

⦿ x86_64
○ arm64

Permissions Info

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

▼ **Change default execution role**

Execution role
Choose a role that defines the permissions of your function. To create a custom role, go to the IAM console.

○ Create a new role with basic Lambda permissions
⦿ Use an existing role
○ Create a new role from AWS policy templates

Existing role
Choose an existing role that you've created to be used with this Lambda function. The role must have permission to upload logs to Amazon CloudWatch Logs.

> LabRole ▼   ⟳

View the LabRole role on the IAM console.

▼ **Advanced settings**

☐ **Enable Code signing** Info
Use code signing configurations to ensure that the code has been signed by an approved source and has not been altered since signing.

☑ **Enable function URL - _new_** Info
Use function URLs to assign HTTP(S) endpoints to your Lambda function.

Auth type
Choose the auth type for your function URL. Learn more ⎘
○ AWS_IAM
Only authenticated IAM users and roles can make requests to your function URL.
⦿ NONE
Lambda won't perform IAM authentication on requests to your function URL.. The URL endpoint will be public unless you implement your own authorization logic in your function.

Function URL permissions

> ⓘ When you choose auth type **NONE**, Lambda automatically creates the following resource-based policy and attaches it to your function. This policy makes your function public to anyone with the function URL. You can edit the policy later. To limit access to authenticated IAM users and roles, choose auth type **AWS_IAM**.

▶ View policy statement

☑ **Configure cross-origin resource sharing (CORS)**
Use CORS to allow access to your function URL from any origin. You can also use CORS to control access for specific HTTP headers and methods in requests to your function URL. By default, all origins are allowed. You can edit this after creating the function. Learn more ⎘

☐ **Enable VPC** Info
Connect your function to a VPC to access private resources during invocation.

☐ **Enable tags** 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, track your AWS costs, and enforce attribute-based access control.

Cancel   **Create function**

MyFirstLambda

Throttle | Copy ARN | Actions ▼

▼ **Function overview** Info

MyFirstLambda

Layers (0)

+ Add trigger

+ Add destination

Description
-

Last modified
5 minutes ago

Function ARN
arn:aws:lambda:us-east-1:068007615521:function:MyFirstLambda

Function URL Info
https://5aqhs6qw5opslrxlu3eqnkgiuu0jnksw.lambda-url.us-east-1.on.aws/

← → C ⌂   🔒 https://5aqhs6qw5opslrxlu3eqnkgiuu0jnksw.lambda-url.us-east-1.**on.aws**

JSON   Raw Data   Headers

Save Copy Collapse All Expand All ▽ Filter JSON

"Hello from Lambda!"

1) Configure test event

File Edit Find View Go Tools Window   **Test** ▼   Deploy

Go to Anything (Ctrl-P)   index.js   ✕   ⊕

▼ 📁 MyFirstLambda - /   ⚙▼
    ◇ index.js

```
1  exports.handler = async (event) => {
2      console.log("Hi");
3      // TODO implement
4      const response = {
5          statusCode: 200,
6          body: JSON.stringify(["s1", "s2", "s3"]),
7      };
8      return response;
9  };
```

Configure test event ✕

A test event is a JSON object that mocks the structure of requests emitted by AWS services to invoke a Lambda function. Use it to see the function's invocation result.

To invoke your function without saving an event, configure the JSON event, then choose Test.

Test event action

○ Create new event   ○ Edit saved event

Event name

MytestEvent

Maximum of 25 characters consisting of letters, numbers, dots, hyphens and underscores.

Event sharing settings

○ Private
This event is only available in the Lambda console and to the event creator. You can configure a total of 10. Learn more ⎘

○ Shareable
This event is available to IAM users within the same account who have permissions to access and use shareable events. Learn more ⎘

Template - *optional*

hello-world ▼

Event JSON   Format JSON

```
1  {
2      "key1": "value1",
3      "key2": "value2",
4      "key3": "value3"
5  }
```


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

Create bucket Info

Buckets are containers for data stored in S3. Learn more [↗]

General configuration

Bucket name

cloudbucketlesson

Bucket name must be 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

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.

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**

↻   ⧉ Copy ARN   Empty   Delete   **Create bucket**

Buckets are containers for data stored in S3. **Learn more** ⬀

🔍 Find buckets by name   ‹ 1 › ⚙

	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)
○	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)

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

Amazon S3 > Buckets > cloudbucketlesson > 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 folders**.

Files and folders (14 Total, 760.8 KB)

All files and folders in this table will be uploaded.

Remove | Add files | Add folder

Q Find by name   < 1 2 >

☐	Name ▲	Folder ▽	Type ▽	Size ▽
☐	787.4637bb57.chunk.js	static/js/	–	4.5 KB
☐	787.4637bb57.chunk.js.map	static/js/	–	10.0 KB
☐	asset-manifest.json	–	application/json	517.0 B
☐	favicon.ico	–	image/x-icon	3.8 KB
☐	index.html	–	text/html	644.0 B
☐	logo192.png	–	image/png	5.2 KB
☐	logo512.png	–	image/png	9.4 KB

After uploading complete go to the properties tab of bucket.

Amazon S3 > Buckets > cloudbucketlesson

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.

index.html

Error document - *optional*

This is returned when an error occurs.

index.html

Then save changes.

Static website hosting

Use this bucket to host a website or redirect requests. **Learn more** ↗

Edit

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://cloudbucketlesson.s3-website-us-east-1.amazonaws.com ↗

To access the link you have to change the permission. Go to Permission tab

cloudbucketlesson Info

| Objects | Properties | **Permissions** | Metrics | Management | Access Points |

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** ↗

Edit   Delete

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** ↗

Go to the Policy generator

Step 1: Select Policy Type

A Policy is a container for permissions. The different types of policies you can create are an IAM Policy, an S3 Bucket Policy, an SNS Topic Policy, a VPC Endpoint Policy, and an SQS Queue Policy.

Select Type of Policy [S3 Bucket Policy ▾]

Step 2: Add Statement(s)

A statement is the formal description of a single permission. See a description of elements that you can use in statements.

Effect ● Allow   ○ Deny

Principal [*]
Use a comma to separate multiple values.

AWS Service [Amazon S3 ▾]   ☐ All Services ('*')
Use multiple statements to add permissions for more than one service.

Actions [1 Action(s) Selected ▾]   ☐ All Actions ('*')

Amazon Resource Name (ARN) [s3:::cloudbucketlesson/*]
ARN should follow the following format: arn:aws:s3:::${BucketName}/${KeyName}.
Use a comma to separate multiple values.

Add Conditions (Optional)

[**Add Statement**]

Step 3: Generate Policy

A *policy* is a document (written in the Access Policy Language) that acts as a container for one or more statements.

Add one or more statements above to generate a policy.

To get ARN go to the bucket overview and copy it.

Bucket overview

AWS Region	Amazon Resource Name (ARN)	Creation date
US East (N. Virginia) us-east-1	🗐 arn:aws:s3:::cloudbucketlesson	April 26, 2022, 23:01:12 (UTC-05:00)

Then generate policy and add this to bucket policy.

You added the following statements. Click the button below to Generate a policy.

Principal(s)	Effect	Action	Resource	Conditions
• *	Allow	• s3:GetObject	arn:aws:s3:::cloudbucketlesson/*	*None*

Step 3: Generate Policy

A *policy* is a document (written in the Access Policy Language) that acts as a container for one or more statements.

[**Generate Policy**]   **Start Over**

Policy JSON Document   ✖

Click below to edit. To save the policy, copy the text below to a text editor.
Changes made below will **not be reflected in the policy generator tool.**

```json
{
  "Id": "Policy1651033640085",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1651033604077",
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::cloudbucketlesson/*",
      "Principal": "*"
    }
  ]
}
```

This AWS Policy Generator is provided for informational purposes only, you are still responsible for your use of Amazon Web Services technologies and ensuring
that your use is in compliance with all applicable terms and conditions. This AWS Policy Generator is provided as is without warranty of any kind, whether

Close

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** ↗

Bucket ARN

▢ arn:aws:s3:::cloudbucketlesson

Policy

```json
 1 ▾ {
 2      "Id": "Policy1651033640085",
 3      "Version": "2012-10-17",
 4 ▾    "Statement": [
 5 ▾      {
 6          "Sid": "Stmt1651033604077",
 7 ▾        "Action": [
 8            "s3:GetObject"
 9          ],
10          "Effect": "Allow",
11          "Resource": "arn:aws:s3:::cloudbucketlesson/*",
12          "Principal": "*"
13        }
14      ]
15 }
```

cloudbucketlesson Info

Publicly accessible

| Objects | Properties | **Permissions** | Metrics | Management | Access Points |

Permissions overview

Access

⚠ Public
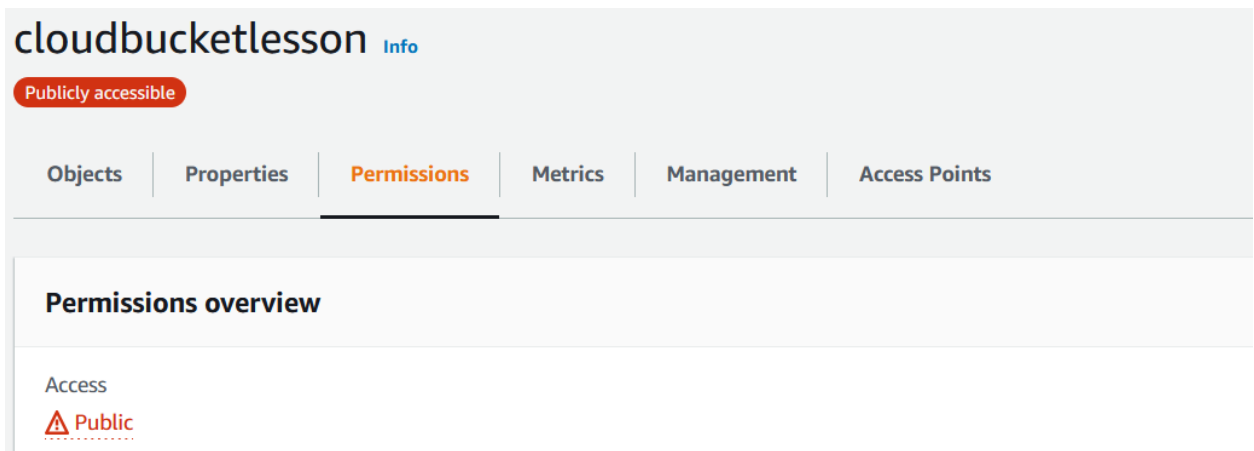
Setting up a billing alarm on CloudWatch

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

| Services ▼ | Q cloudwatch | ✕ | Σ |

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 …
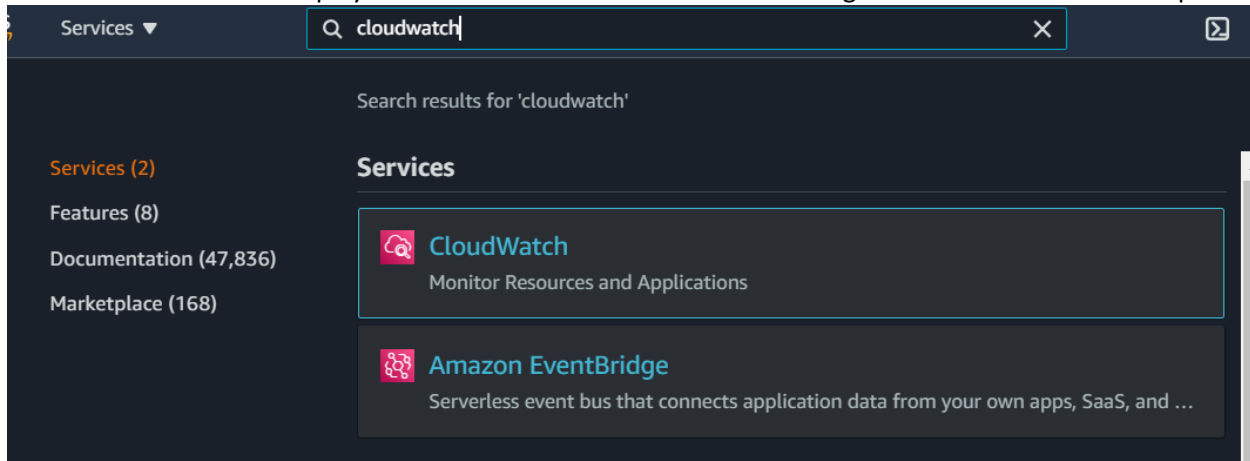
Go to the Alarms Display
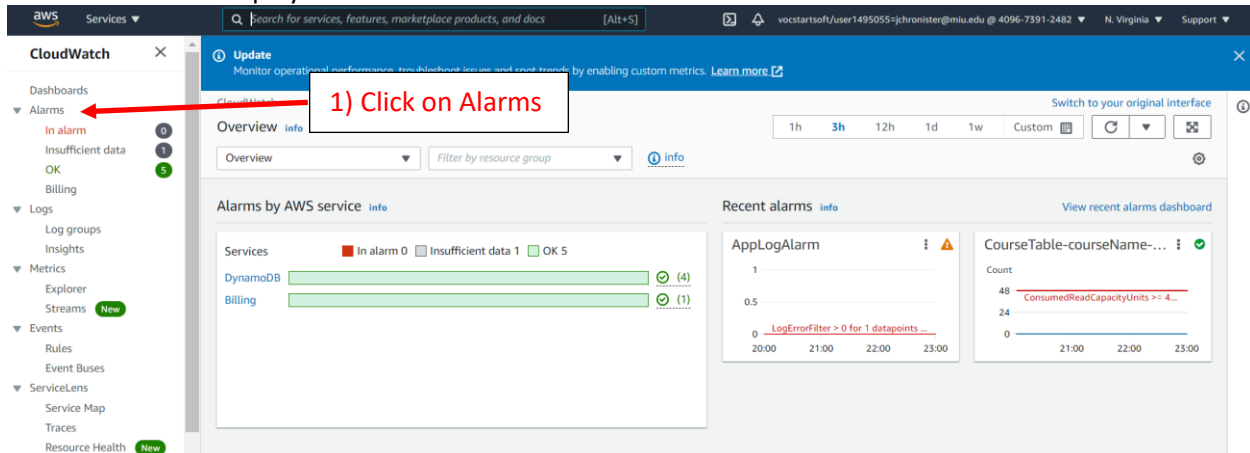
Create Billing Alarm

Alarms (6)

☐ Hide Auto Scaling alarms   Clear selection   ⟳   Create composite alarm   Actions ▾   **Create alarm**

1) Click on Create Alarm

🔍 Search   Any state ▾   Any type ▾   ‹ 1 › ⚙

☐	Name ▽	State ▽	Last state update ▽	Conditions	Actions ▽
☐	AppLogAlarm	⊖ Insufficient data	2021-07-06 20:30:20	LogErrorFilter > 0 for 1 datapoints within 5 minutes	⊘ 1 action(s) enabled Warning
☐	CourseTable-courseName-index-ReadCapacityUnitsLimit-BasicAlarm	⊘ OK	2021-07-05 13:01:53	ConsumedReadCapacityUnits >= 48 for 60 datapoints within 1 hour	⊘ 1 action(s) enabled Warning
☐	CourseTable-WriteCapacityUnitsLimit-BasicAlarm	⊘ OK	2021-07-05 13:01:32	ConsumedWriteCapacityUnits >= 48 for 5 datapoints within 5 minutes	⊘ 1 action(s) enabled Warning

...

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

Graph
Preview of the metric or metric expression and the alarm threshold.

Select metric

2) Click Select Metric

Cancel   **Next**

...

Select metric   ✕

0.2

0

20:15   20:30   20:45   21:00   21:15   21:30   21:45   22:00   22:15   22:30   22:45   23:00

3) Click Billing

▾ AWS Namespaces

ApiGateway 11	ApplicationELB 177	Billing 14	DynamoDB 23
EBS 189	EC2 392	Events 5	Lambda 26

Cancel   Select a single metric to continue

...

Select metric   ✕

```
0.2
  0
   20:15   20:30   20:45   21:00   21:15   21:30   21:45   22:00   22:15   22:30   22:45   23:00
```

Metrics (14)   Graph search   **View graphed metrics**

All › Billing   🔍 Search for any metric, dimension or resource id

By Service	13	Total Estimated Charge	1

4) Click Total Estimated Charge

Cancel   Select a single metric to continue

...

Metrics (1)   Graph search   **View graphed metrics (1)**

All › Billing › Total Estimated Charge   🔍 Search for any metric, dimension or resource id

☑	Currency (1) ▲	Metric Name ▲
☑	USD ▾	EstimatedCharges ▾

5) Select USD Currency   **6) Click Select Metric**

Cancel   **Select metric**

CloudWatch › Alarms › Create alarm

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**
>= threshold

○ **Lower/Equal**
<= threshold

○ **Lower**
< threshold

than...
Define the threshold value.

`1`   USD

Must be a number

7) Pick Some Conditions

8) Click Next

▶ Additional configuration

Cancel   **Next**

...

CloudWatch > Alarms > Create alarm

Configure actions

Step 1
Specify metric and conditions

Step 2
Configure actions

Step 3
Add name and description

Step 4
Preview and create

Notification

Alarm state trigger
Define the alarm state that will trigger this action.

[Remove]

- ● **In alarm**
  The metric or expression is outside of the defined threshold.
- ○ **OK**
  The metric or expression is within the defined threshold.
- ○ **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   **9) Select Create New SNS Topic**
- ○ Use topic ARN

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`   **11) Enter Email**

user1@example.com, user2@example.com

[Create topic]   **12) Click Create Topic**

[Add notification]

…

Send a notification to...

🔍 MyBillingAlarm ✕

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

16) Preview Alarm and Click Create Alarm

Description
-

Cancel   Previous   **Create alarm**