

Assignment 1 – IaaS and FaaS

1. Spin up an EC2 instance

aws Services Search [Alt+S]

▼ Network settings Info Edit

Network Info
vpc-0bd3ae12c47444b6c

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-2' with the following rules:

☒ Allow SSH traffic from
Helps you connect to your instance Anywhere
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

⚠ 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. ✕

2. IAM instance profile setting in Advance Settings –

▼ **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](#)

LabInstanceProfile
arn:aws:iam::242306694058:instance-profile/LabInstanceProfile ▼

 [Create new IAM profile](#) 

Hostname type [Info](#)

IP name ▼

DNS Hostname [Info](#)

☒ Enable IP name IPv4 (A record) DNS requests

☒ Enable resource-based IPv4 (A record) DNS requests

☐ Enable resource-based IPv6 (AAAA record) DNS requests

3. Configure web server

Session manager connect

EC2 > Instances > i-07347386ec12f3974 > Connect to instance

Connect to instance [Info](#)

Connect to your instance i-07347386ec12f3974 (TanvirMIUWebServer) using any of these options

EC2 Instance Connect

Session Manager

SSH 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

4. After installing APACHE, creating index.html

Session ID: user2294082=tanvir-0ea4e5eafc82e5ada

Instance ID: i-07347386ec12f3974

GNU nano 2.9.8

ii

Tanvir Zobair Mahboob

```
^G Get Help
^X Exit
```

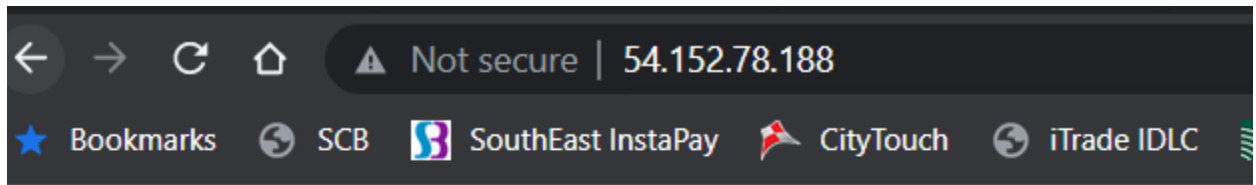
```
^O Write Out
^R Read File
```

^W Where Is
^\\ Replace

^K Cut Text
^U Uncut Text

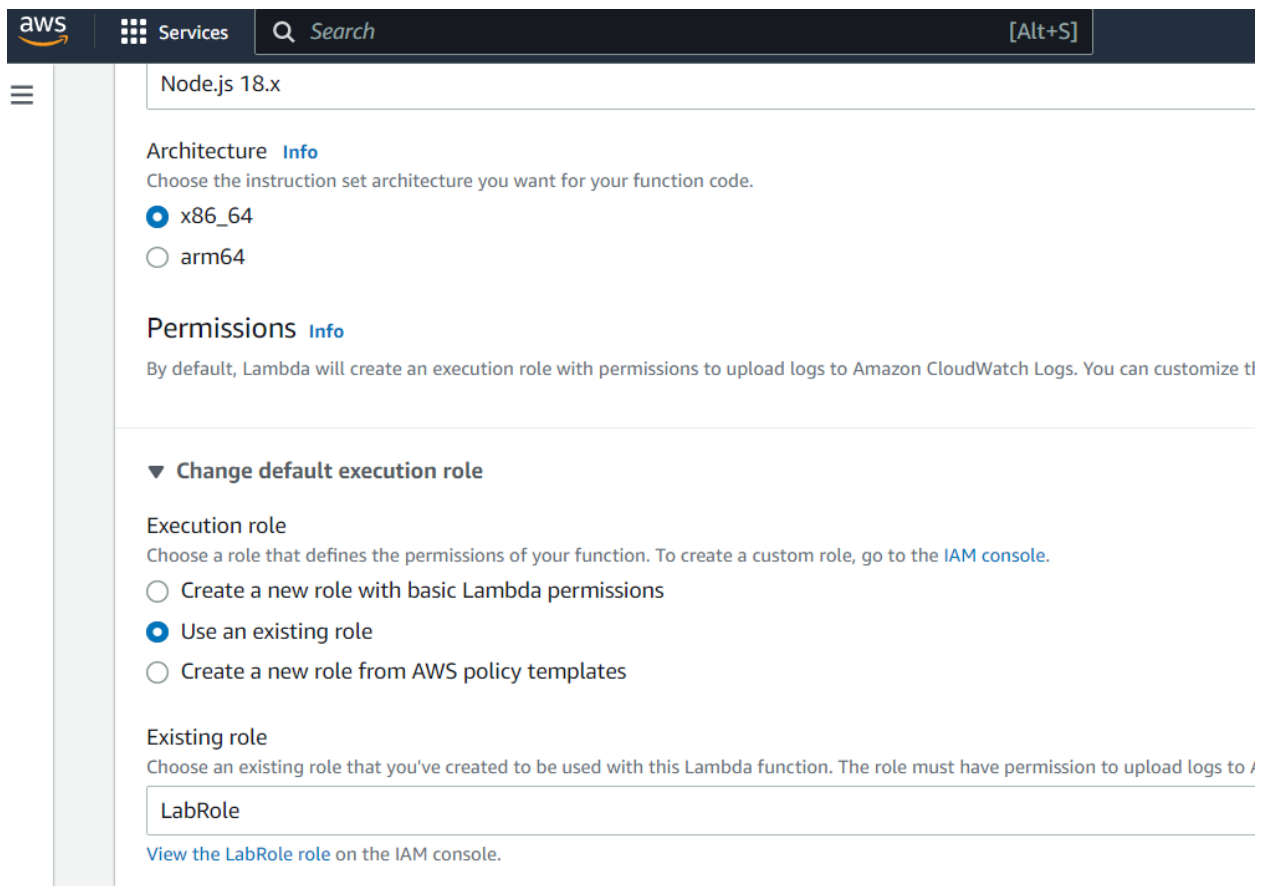
^J Justify
^T To Spell

5. Html run with browser






Fanvir Zobair Mahboob

6. Creating Lambda



7. Enabling public API by function URL and enabling CORS

  Services [Alt+S]



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

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

☒ **Enable function URL** [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

Function URL permissions

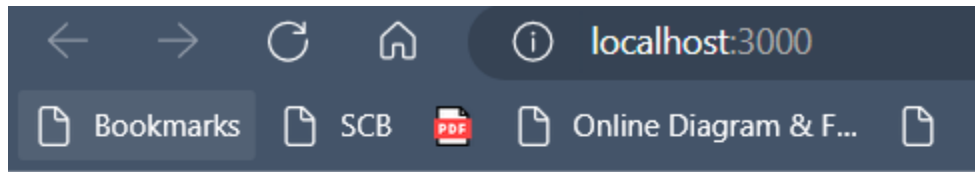
 When you choose auth type **NONE**, Lambda automatically creates the following resource-based URL. You can edit the policy later. To limit access to authenticated IAM users and roles, cho

► **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 sp

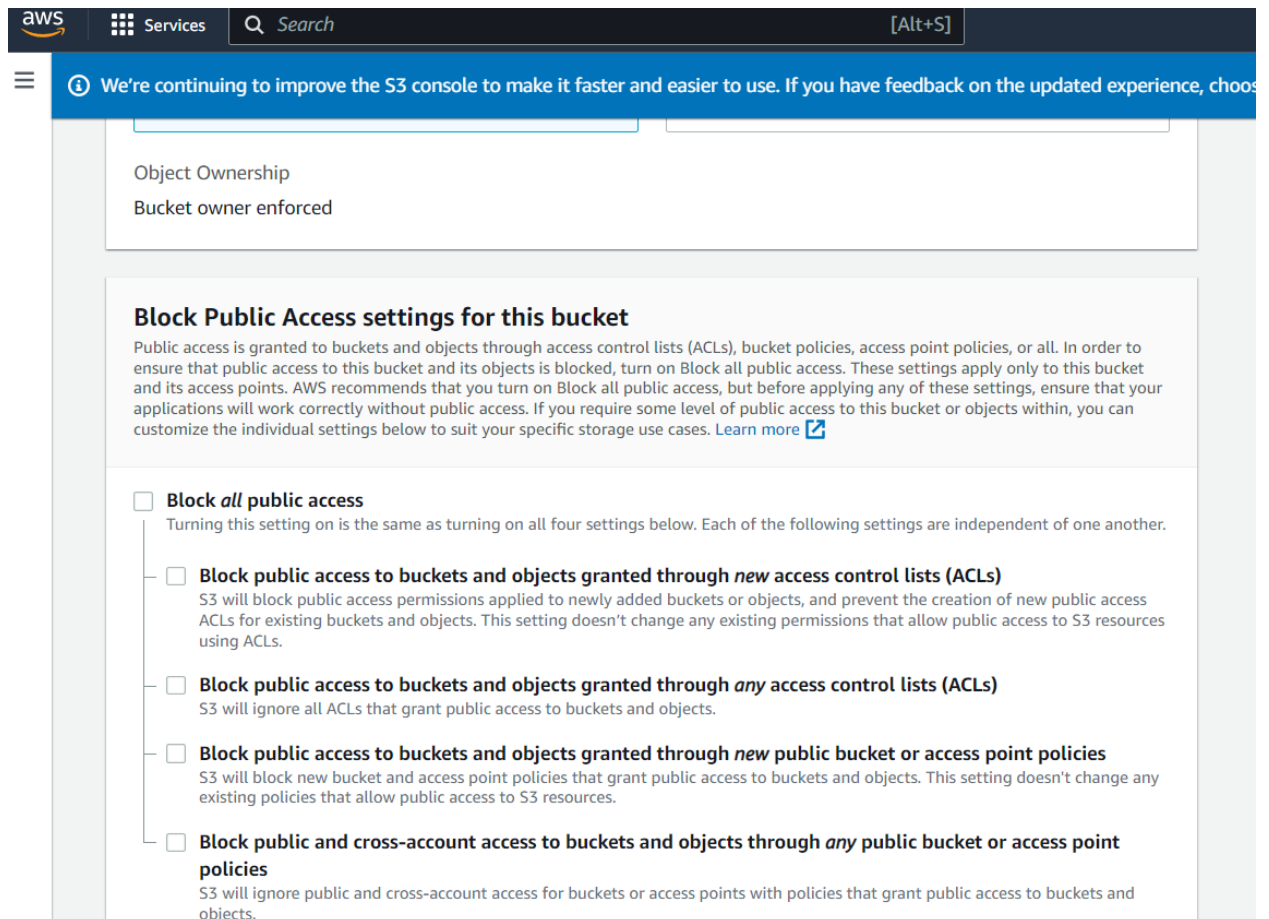
8. Output of Lambda from localhost react app



Cloud Computing course

1. STUDENT 1
2. STUDENT 2
3. STUDENT 3
4. STUDENT 4

9. Creating bucket in S3




10. Writing policy to make all objects in the bucket public –

Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket

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

11. Enable static page hosting

 We're continuing to improve the S3 console to make it faster and easier to use. If you have feedback on the updated experience, please let us know.

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*

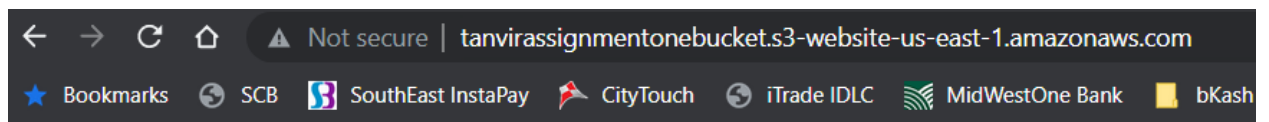
This is returned when an error occurs.

index.html

Redirection rules – *optional*

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

12. React app successfully deployed in bucket –

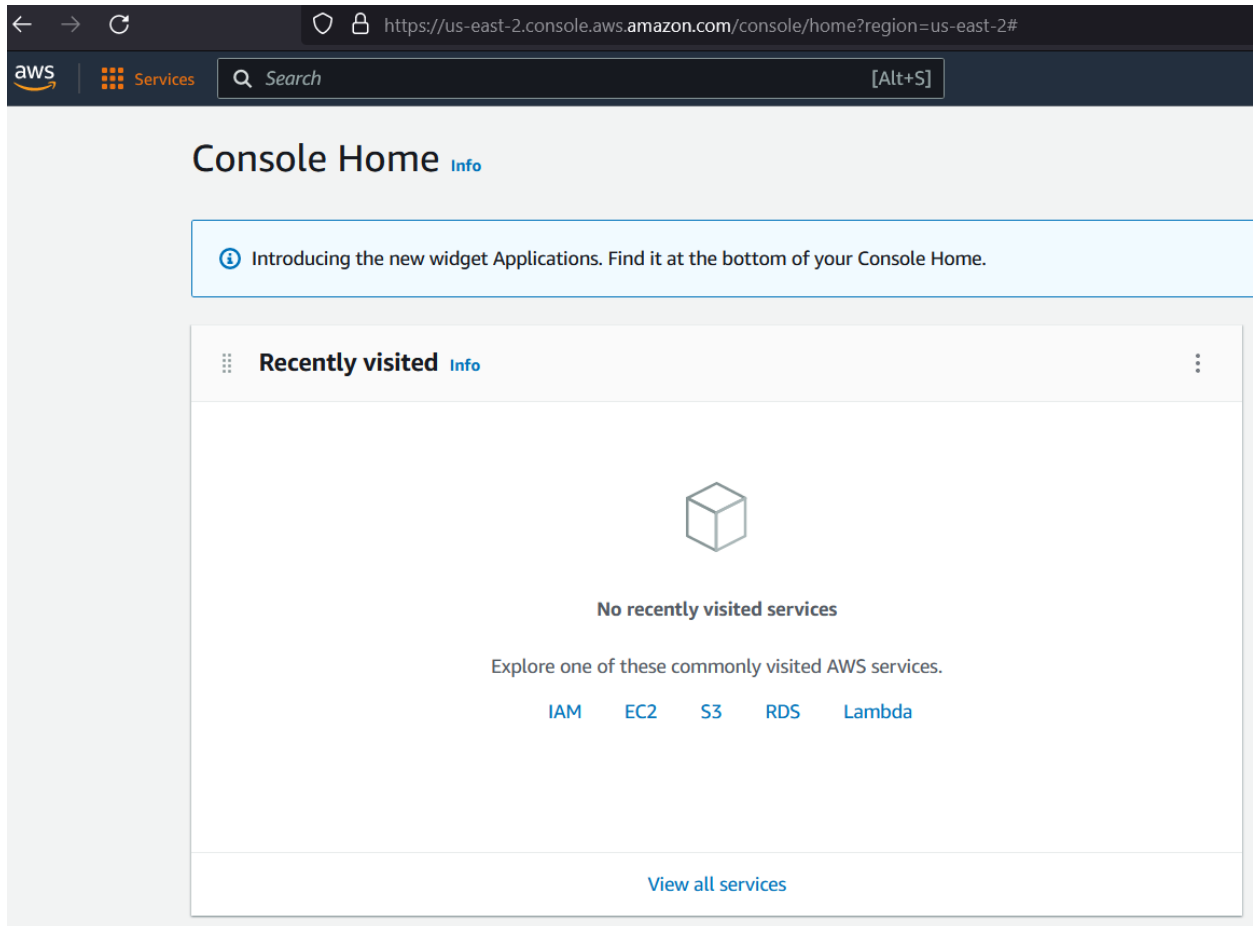


Cloud Computing course

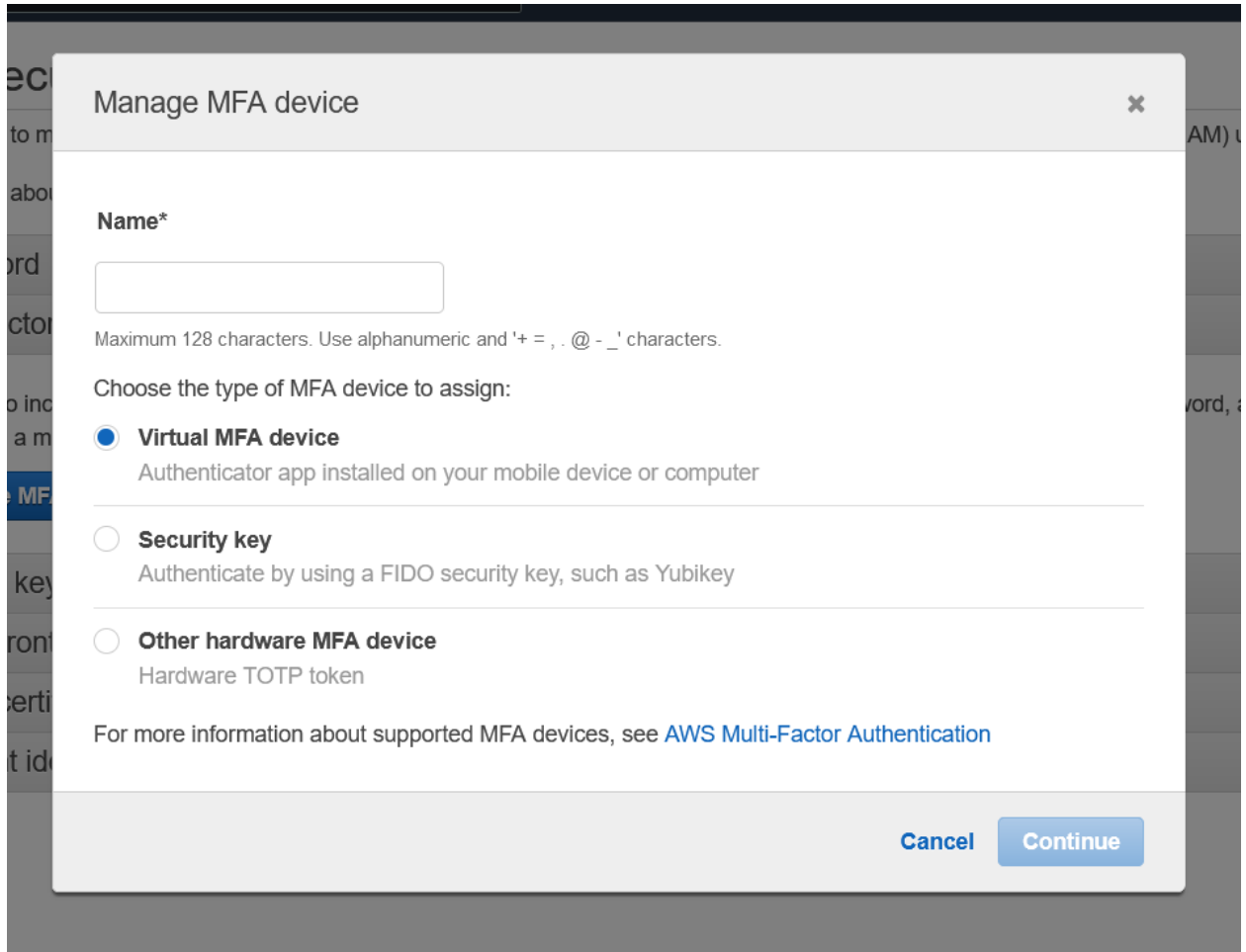
1. STUDENT 1
2. STUDENT 2
3. STUDENT 3
4. STUDENT 4

Create Own AWS Account

1. First AWS root user created for personal account



2. Enable MFA for root user



The screenshot shows a 'Manage MFA device' dialog box with a close button (X) in the top right corner. It contains a text input field for 'Name*' with a placeholder and a note: 'Maximum 128 characters. Use alphanumeric and '+ = , . @ - _ ' characters.' Below this is a section titled 'Choose the type of MFA device to assign:' with three radio button options: 'Virtual MFA device' (selected), 'Security key', and 'Other hardware MFA device'. Each option has a descriptive subtitle. At the bottom right are 'Cancel' and 'Continue' buttons. A link to 'AWS Multi-Factor Authentication' is provided for more information.

Manage MFA device ✕

Name*

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

Choose the type of MFA device to assign:

☒ **Virtual MFA device**
Authenticator app installed on your mobile device or computer

☐ **Security key**
Authenticate by using a FIDO security key, such as Yubikey

☐ **Other hardware MFA device**
Hardware TOTP token

For more information about supported MFA devices, see [AWS Multi-Factor Authentication](#)


Cancel Continue

Set up virtual MFA device

1. Install a compatible app on your mobile device or computer

See a [list of compatible applications](#)

2. Use your virtual MFA app and your device's camera to scan the QR code



Alternatively, you can type the secret key. [Show secret key](#)

3. Type two consecutive MFA codes below

MFA code 1

Cancel

Previous

Assign MFA

Set up virtual MFA device

✔

This virtual MFA will be required during sign-in.

You can register up to 8 MFA devices of any combination of the currently [supported MFA types](#) with your AWS account root and IAM user. With multiple MFA devices, you only need one MFA device to sign in to the AWS console or create a session through the [AWS CLI](#) with that user.

Close

3. Create IAM profile user

▼ IAM User and Role Access to Billing Information

[Edit](#)

Use the **Activate IAM Access** setting to allow IAM users and roles access to pages of the Billing and Cost Management console. This setting alone doesn't grant IAM users and roles the necessary permissions for these console pages. In addition to activating IAM access, you must also attach the required IAM policies to those users or roles. For more information, see [Granting access to your billing information and tools](#).

If this setting is deactivated, then IAM users and roles in this account can't access the Billing and Cost Management console pages, even if they have administrator access or the required IAM policies.

The **Activate IAM Access** setting does not control access to:

- The console pages for AWS Cost Anomaly Detection, Savings Plans overview, Savings Plans inventory, Purchase Savings Plans, and Savings Plan cart
- The Cost Management view in the AWS Console Mobile Application
- The Billing and Cost Management SDK APIs (AWS Cost Explorer, AWS Budgets, and AWS Cost and Usage Report APIs)
- The Customer Carbon Footprint Tool on the Cost & Usage Reports console page

IAM user/role access to billing information is activated.

Add user



Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name*

[+ Add another user](#)

Select AWS access type

Select how these users will primarily access AWS. If you choose only programmatic access, it does NOT prevent users from accessing the console using an assumed role. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

- Select AWS credential type* ☒ **Access key - Programmatic access**
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.
- ☒ **Password - AWS Management Console access**
Enables a **password** that allows users to sign-in to the AWS Management Console.

Console password* ☐ Autogenerated password
☒ Custom password

☐ Show password

Create group

Create a group and select the policies to be attached to the group. Using groups is a best-practice way to manage users' permissions by job functions, AWS service access, or your custom permissions.
[Learn more](#)

Group name

Administrators





Create policy

Refresh

Filter policies

Search

Showing 794 results

	Policy name	Type	Used as	Description
<input checked="" type="checkbox"/>	 AdministratorAccess	Job function	None	Provides full access to AWS services and resources.
<input type="checkbox"/>	 AdministratorAccess-Amplify	AWS managed	None	Grants account administrative permissions while explicitly allowing direct acce...
<input type="checkbox"/>	 AdministratorAccess-AWSElastic...	AWS managed	None	Grants account administrative permissions. Explicitly allows developers and a...
<input type="checkbox"/>	 AlexaForBusinessDeviceSetup	AWS managed	None	Provide device setup access to AlexaForBusiness services

Cancel

Create group

Add user



Review

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

User details

User name	Administrator
AWS access type	Programmatic access and AWS Management Console access
Console password type	Custom
Require password reset	Yes
Permissions boundary	Permissions boundary is not set

Permissions summary

The user shown above will be added to the following groups.

Type	Name
Group	Administrators
Managed policy	IAMUserChangePassword

Tags

No tags were added.

Add user

1 2 3 4 5



Success

You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

Users with AWS Management Console access can sign-in at: <https://390937139765.signin.aws.amazon.com/console>

Download .csv

	User	Access key ID	Secret access key	Email login instructions
▶	✓ Administrator	AKIAVWBNLLI2WH7HR25N	***** Show	Send email



The user [Administrator](#) have been created.

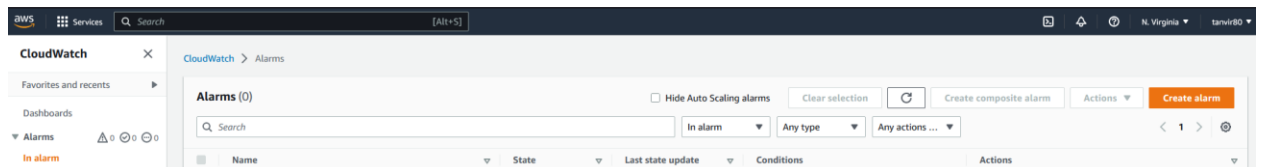
IAM > Users

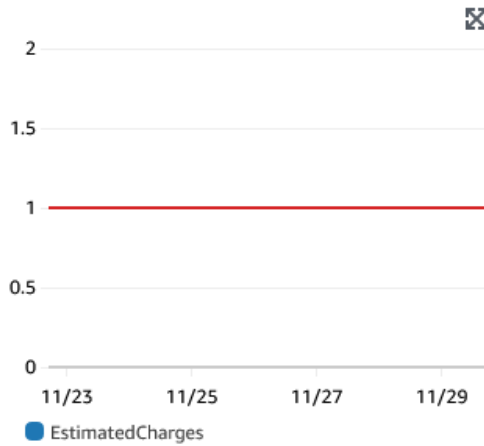
Users (1) Info

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

Find users by username or access key

4. Setting up a billing alarm on CloudWatch





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

Configure actions

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.

Send a notification to the following 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 to notify other accounts

Create a new topic...

The topic name must be unique.

MyBillingAlarm

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.

tanvirmahboob@gmail.com

user1@example.com, user2@example.com

Create topic

Add notification

Add name and description

Name and description

Alarm name

Alarm description - *optional*

Alarm description

Up to 1024 characters (0/1024)

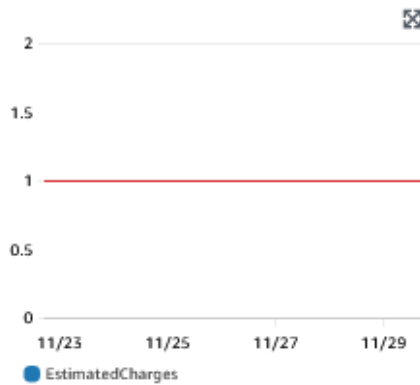
Cancel

Previous

Next

Graph

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



Namespace
AWS/Billing

Metric name
EstimatedCharges

Currency
USD

Statistic
Maximum

Period
6 hours

Conditions

Threshold type
Static

Whenever **EstimatedCharges** is
Greater/Equal (\geq)

than...
1

► **Additional configuration**

Step 2: Configure actions

Edit

Actions

Notification
When In alarm, send a notification to "MyBillingAlarm"

Step 3: Add name and description

Edit

Name and description

Name
MyBillingAlarm

Description
-

Cancel

Previous

Create alarm

☑ Successfully created alarm [MyBillingAlarm](#).

ⓘ **Some subscriptions are pending confirmation**

Amazon SNS doesn't send messages to an endpoint until the subscription is confirmed

CloudWatch > Alarms

Billing alarms (1)

☐ Hide Auto Scaling alarms

Clear selection



Create composite alarm

Action

🔍 Search

Any state ▼

Any type ▼

Any actions ... ▼

<input type="checkbox"/>	Name	State	Last state update	Conditions	Actions
<input type="checkbox"/>	MyBillingAlarm	⊖ Insufficient data	2022-11-29 17:15:37	EstimatedCharges >= 1 for 1 datapoints within 6 hours	☑ Actions enabled Warning