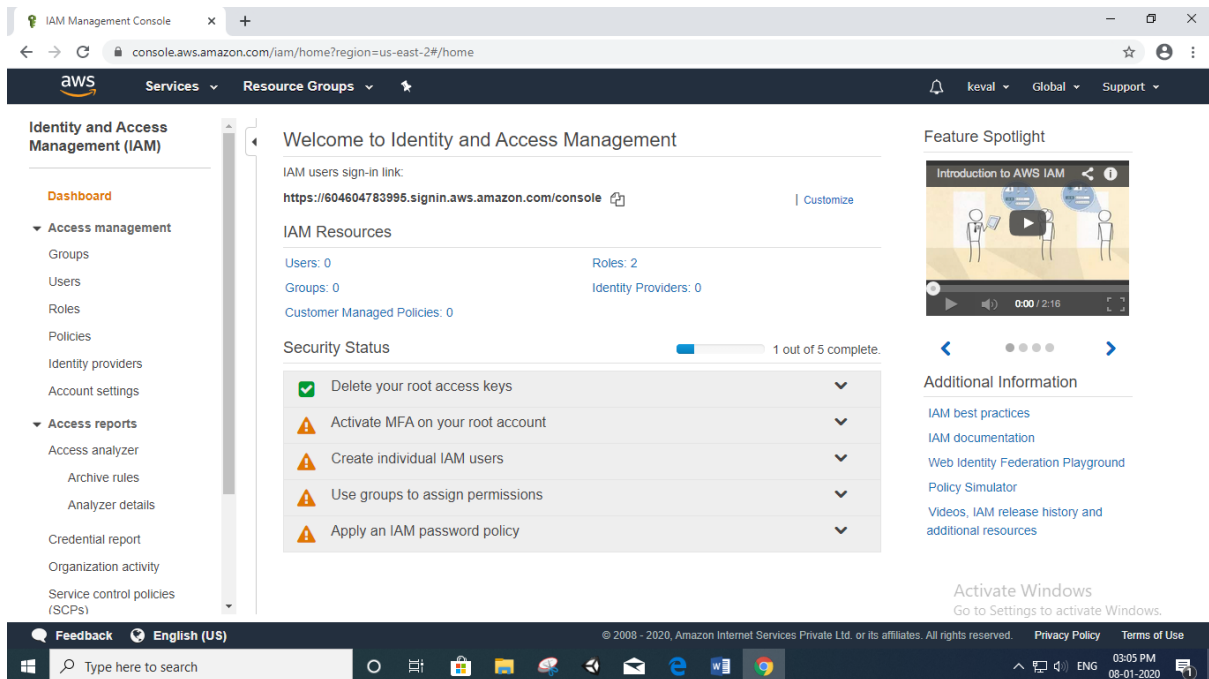


# AWS Practice

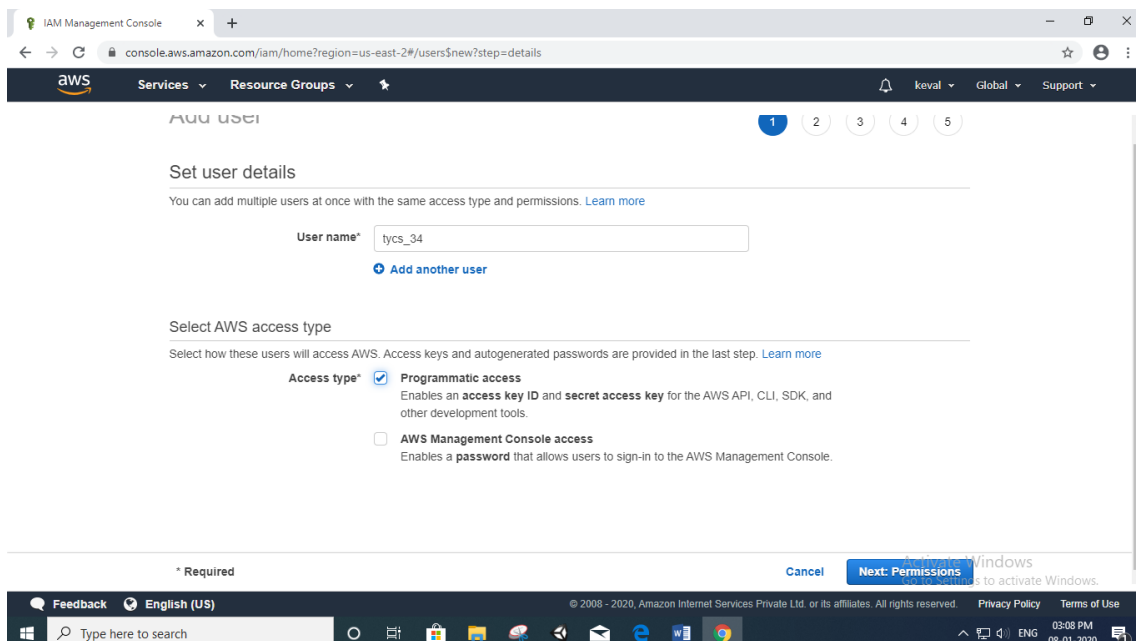
## Create IAM User and give roles

Step 1: Go to [aws.amazon.com](https://aws.amazon.com) > now click on AWS management windows then it will ask you to create new AWS account.

In services > click IAM > click user >



Step 2: Now give user name and access type > next permission



## Step 3: Next tags

The screenshot shows the AWS IAM Management Console 'Add user' wizard at Step 3, 'Set permissions'. The breadcrumb trail is 'Add user' > 1 > 2 > 3 > 4 > 5. The 'Set permissions' section has three options: 'Add user to group' (selected), 'Copy permissions from existing user', and 'Attach existing policies directly'. Below these is a 'Get started with groups' informational box with a 'Create group' button. At the bottom, there is a 'Set permissions boundary' section. The navigation bar at the bottom shows 'Cancel', 'Previous', and 'Next: Tags' buttons. The Windows taskbar is visible at the very bottom.

## Step 4: Give key value>Next review

The screenshot shows the AWS IAM Management Console 'Add user' wizard at Step 4, 'Add tags (optional)'. The breadcrumb trail is 'Add user' > 1 > 2 > 3 > 4 > 5. The 'Add tags (optional)' section explains that IAM tags are key-value pairs and provides a table to add them. The table has columns for 'Key', 'Value (optional)', and 'Remove'. One tag is already added with the key 'tycs123'. Below the table is an 'Add new key' button. A note states 'You can add 49 more tags.' The navigation bar at the bottom shows 'Cancel', 'Previous', and 'Next: Review' buttons. The Windows taskbar is visible at the very bottom.

Key	Value (optional)	Remove
tycs123		✕
<input type="text" value="Add new key"/>	<input type="text"/>	

## Step 5: Create user

IAM Management Console

console.aws.amazon.com/iam/home?region=us-east-2#/users\$new?step=review&accessKey&userNames=tycs\_34

### Add user

1 2 3 4 5

#### Review

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

**This user has no permissions**

You haven't given this user any permissions. This means that the user has no access to any AWS service or resource. Consider returning to the previous step and adding some type of permissions.

#### User details

User name	tycs_34
AWS access type	Programmatic access - with an access key
Permissions boundary	Permissions boundary is not set

#### Tags

The new user will receive the following tag

Cancel Previous **Create user**

Feedback English (US) © 2008 - 2020, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Type here to search

## Step 6: Close

IAM Management Console

console.aws.amazon.com/iam/home?region=us-east-2#/users\$new?step=final&accessKey&userNames=tycs\_34

### 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://604604783995.signin.aws.amazon.com/console>

Download .csv

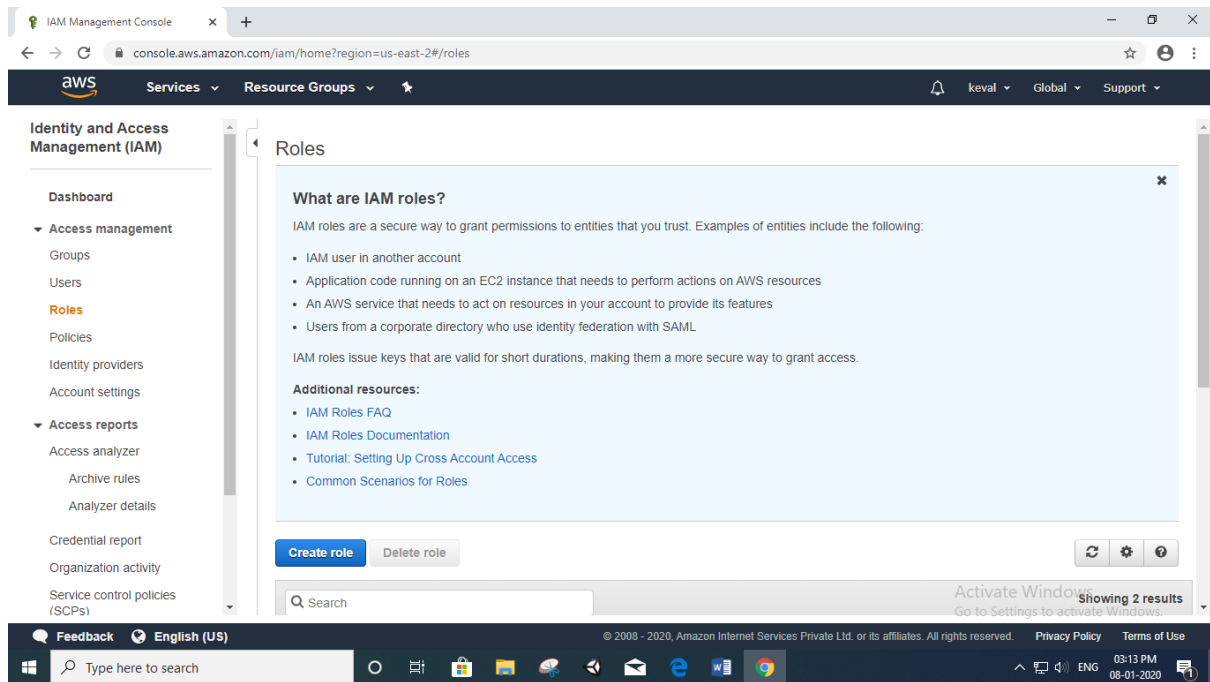
User	Access key ID	Secret access key
tycs_34	AKIAYZRKA3V5XRO7PFOD	***** Show

Activate Windows Go to Settings to activate Windows.

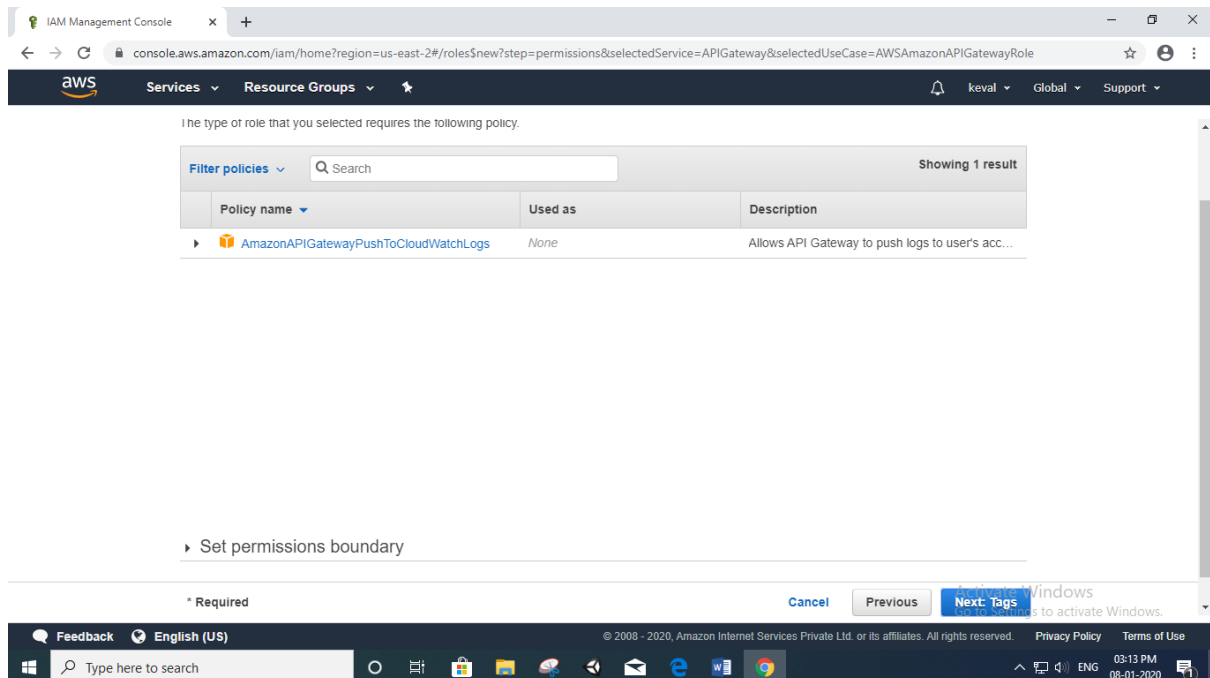
Feedback English (US) © 2008 - 2020, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Type here to search

## Step 7: Click on Roles



## Step 8: create role > Select API gateway> Next permission>next tags>next review



## Step 9: Give role name as admin>create role

The screenshot shows the 'Create role' page in the AWS IAM Management Console, specifically the 'Review' step (Step 4 of 4). The page title is 'Create role' with a progress indicator showing steps 1, 2, 3, and 4. The sub-header is 'Review'. Below this, a message states: 'Provide the required information below and review this role before you create it.'

The form contains the following fields:

- Role name:** A text input field containing 'administrator\_tycs34'. Below it, a note says: 'Use alphanumeric and '+=, @, \_' characters. Maximum 64 characters.'
- Role description:** A text area containing 'Allows API Gateway to push logs to CloudWatch Logs.' Below it, a note says: 'Maximum 1000 characters. Use alphanumeric and '+=, @, \_' characters.'
- Trusted entities:** A dropdown menu showing 'AWS service: apigateway.amazonaws.com'.
- Policies:** A section showing a selected policy: 'AmazonAPIGatewayPushToCloudWatchLogs' with a link icon.
- Permissions boundary:** A section stating 'Permissions boundary is not set'.

At the bottom, a message states: 'The new role will receive the following tag' followed by a table with one row and one column. Below this, there are three buttons: 'Cancel', 'Previous', and 'Create role' (highlighted in blue). A Windows watermark is visible in the bottom right corner.

## Step 10: Click on groups > create group >

The screenshot shows the 'Groups' page in the AWS IAM Management Console. The left sidebar shows the 'Identity and Access Management (IAM)' menu with 'Groups' selected. The main content area has a 'Create New Group' button and a 'Group Actions' dropdown. Below this is a search bar and a table with the following columns: 'Group Name', 'Users', 'Inline Policy', and 'Creation Time'. The table is empty, and a message below it states: 'No records found.' A Windows watermark is visible in the bottom right corner.

## Step 11: Give group name >next

The screenshot shows the AWS IAM Management Console interface. The left sidebar displays the 'Create New Group Wizard' with three steps: 'Step 1: Group Name', 'Step 2: Attach Policy', and 'Step 3: Review'. The main content area is titled 'Set Group Name' and includes the instruction 'Specify a group name. Group names can be edited any time.' Below this, the 'Group Name' field contains the text 'tycs34'. A note below the field states: 'Example: Developers or ProjectAlpha' and 'Maximum 128 characters'. At the bottom right, there is an 'Activate Windows' watermark and a 'Next Step' button.

Step 1: Group Name  
Step 2: Attach Policy  
Step 3: Review

Set Group Name

Specify a group name. Group names can be edited any time.

Group Name:

Example: Developers or ProjectAlpha  
Maximum 128 characters

Activate Windows  
Go to Settings to activate Windows

Next Step

## Step 12: select the amazon API and ALEXA >next step

The screenshot shows the AWS IAM Management Console interface. The left sidebar displays the 'Create New Group Wizard' with three steps: 'Step 1: Group Name', 'Step 2: Attach Policy', and 'Step 3: Review'. The main content area is titled 'Attach Policy' and includes the instruction 'Select one or more policies to attach. Each group can have up to 10 policies attached.' Below this, there is a table of policies. The table has columns for 'Policy Name', 'Attached Entities', and 'Creation Time'. The 'Policy Name' column is filtered by 'Policy Type'. The table shows 505 results. The 'AmazonAPIGatewayPushToCloudWatchLogs' policy is selected. The 'AmazonAPIGatewayAdministrator' policy is highlighted. At the bottom right, there is an 'Activate Windows' watermark and a 'Next Step' button.

Step 1: Group Name  
Step 2: Attach Policy  
Step 3: Review

Attach Policy

Select one or more policies to attach. Each group can have up to 10 policies attached.

Filter: Policy Type Search

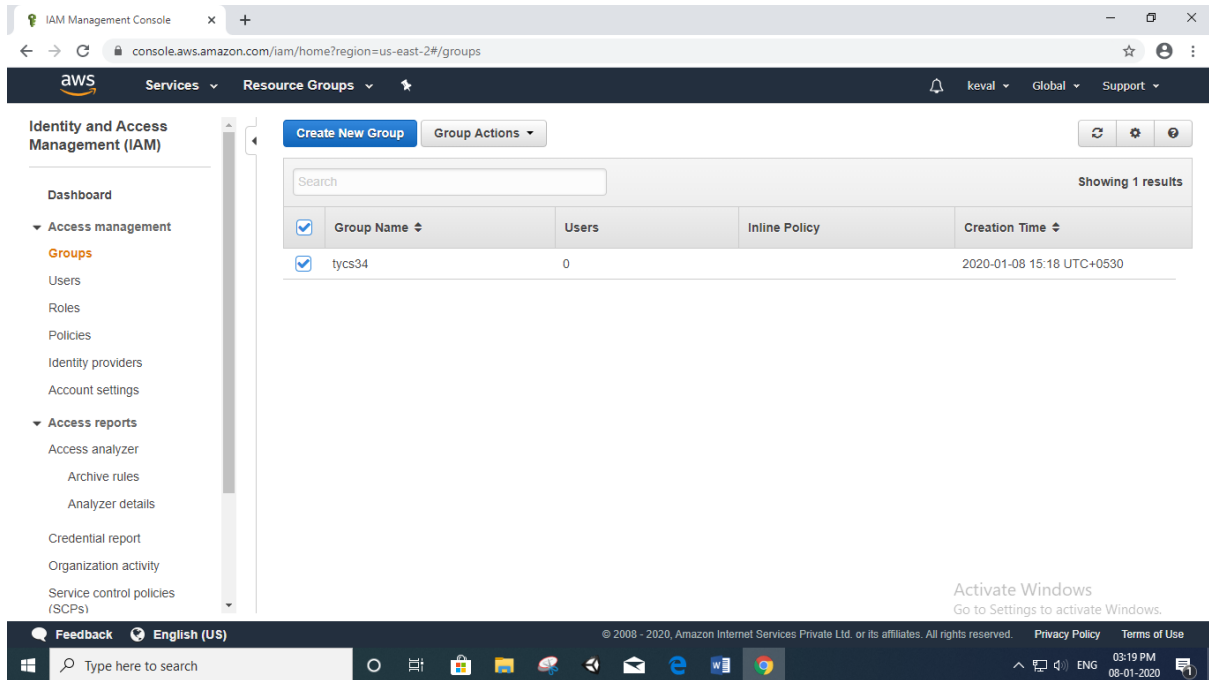
Showing 505 results

	Policy Name	Attached Entities	Creation Time
<input checked="" type="checkbox"/>	AmazonAPIGatewayPushToCloudWatchLogs	1	2015-11-12 05:11 UTC+...
<input type="checkbox"/>	AdministratorAccess	0	2015-02-07 00:09 UTC+...
<input checked="" type="checkbox"/>	AlexaForBusinessDeviceSetup	0	2017-11-30 22:17 UTC+...
<input type="checkbox"/>	AlexaForBusinessFullAccess	0	2017-11-30 22:17 UTC+...
<input type="checkbox"/>	AlexaForBusinessGatewayExecution	0	2017-11-30 22:17 UTC+...
<input type="checkbox"/>	AlexaForBusinessPolyDelegatedAccessPolicy	0	2019-10-17 01:18 UTC+...
<input type="checkbox"/>	AlexaForBusinessReadOnlyAccess	0	2017-11-30 22:17 UTC+...
<input type="checkbox"/>	AmazonAPIGatewayAdministrator	0	2015-07-09 23:04 UTC+...
<input type="checkbox"/>	AmazonAPIGatewayInvokeFullAccess	0	2015-07-09 23:06 UTC+...

Activate Windows  
Go to Settings to activate Windows

Next Step

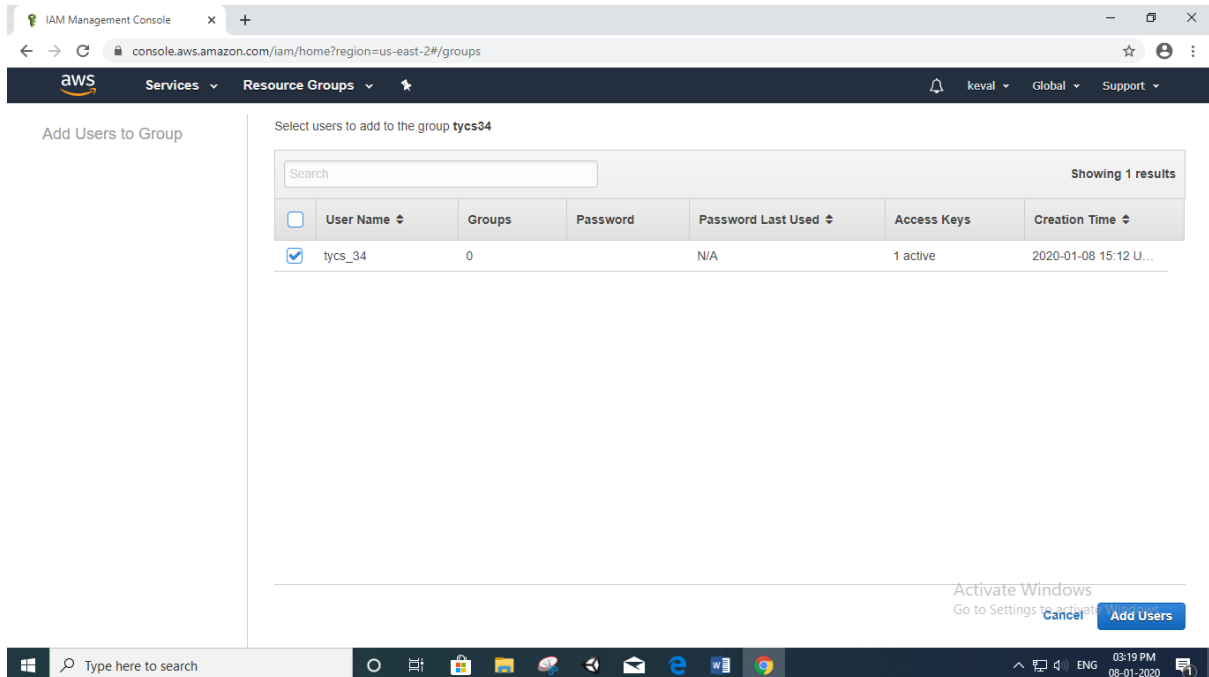
## Step 13: Click on group



The screenshot shows the AWS IAM Management Console. The left sidebar is expanded to 'Access management' > 'Groups'. The main content area shows a table of groups. The group 'tycs34' is selected, and the 'Group Actions' dropdown is open. The table has columns: Group Name, Users, Inline Policy, and Creation Time.

Group Name	Users	Inline Policy	Creation Time
tycs34	0		2020-01-08 15:18 UTC+0530

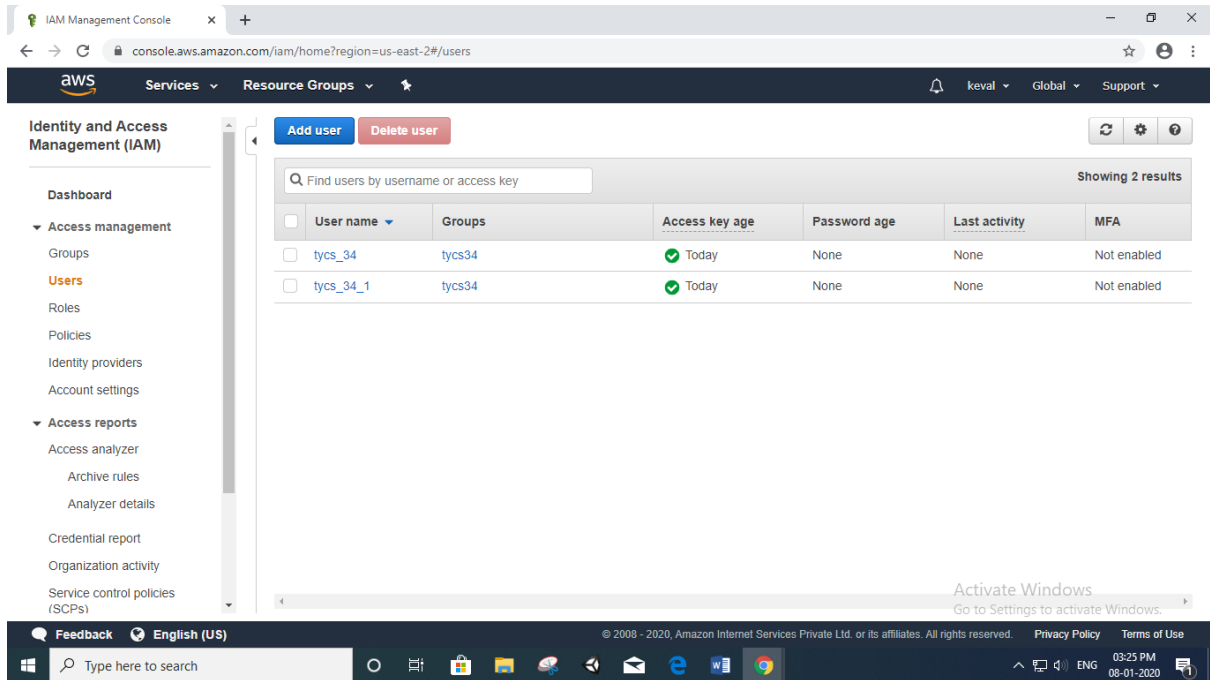
## Step 14 Go to group action >add user to group > add user



The screenshot shows the AWS IAM Management Console. The left sidebar is expanded to 'Access management' > 'Groups'. The main content area shows the 'Add Users to Group' page. The group 'tycs34' is selected, and the 'Add Users' button is visible. The table has columns: User Name, Groups, Password, Password Last Used, Access Keys, and Creation Time.

User Name	Groups	Password	Password Last Used	Access Keys	Creation Time
tycs_34	0		N/A	1 active	2020-01-08 15:12 U...

## Step 15: Click on users “OUTPUT”



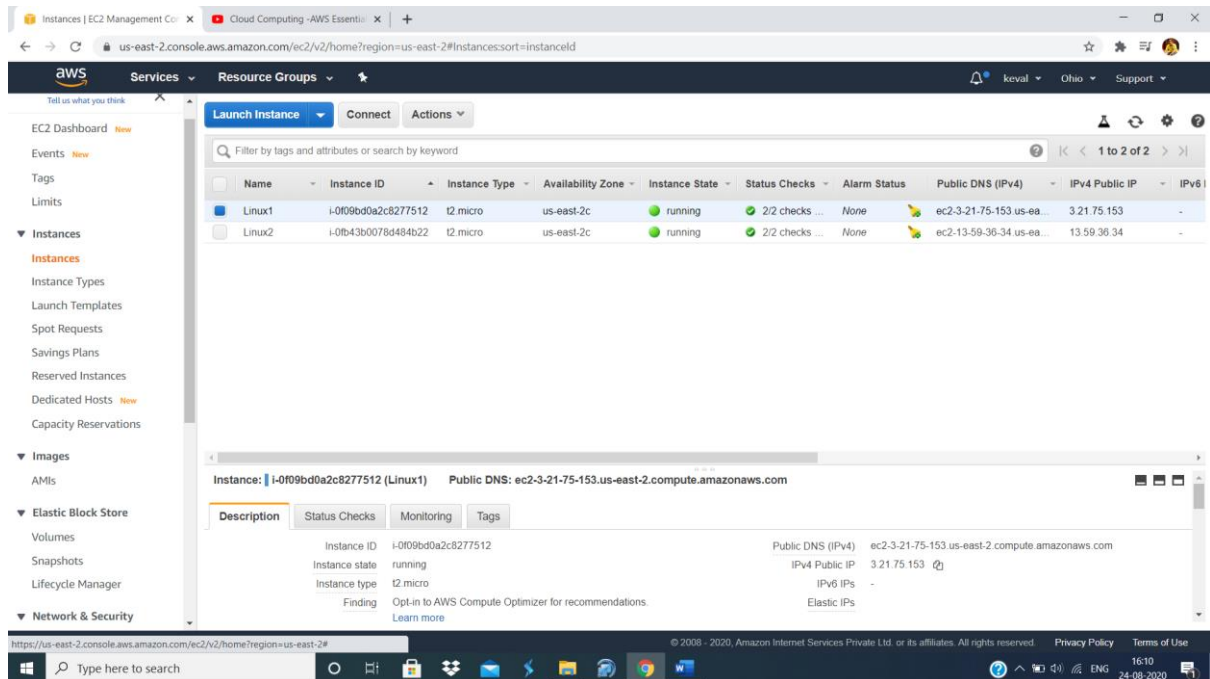
The screenshot shows the AWS IAM Management Console interface. The left sidebar contains the navigation menu with options like Dashboard, Access management, and Access reports. The main content area displays the 'Users' page, which includes a search bar and a table of users. The table has columns for User name, Groups, Access key age, Password age, Last activity, and MFA. Two users are listed: 'tycs\_34' and 'tycs\_34\_1', both associated with the 'tycs34' group. The 'tycs\_34' user is selected. The console also shows a sidebar with navigation options like Dashboard, Access management, and Access reports.

<input type="checkbox"/>	User name	Groups	Access key age	Password age	Last activity	MFA
<input checked="" type="checkbox"/>	tycs_34	tycs34	✓ Today	None	None	Not enabled
<input type="checkbox"/>	tycs_34_1	tycs34	✓ Today	None	None	Not enabled

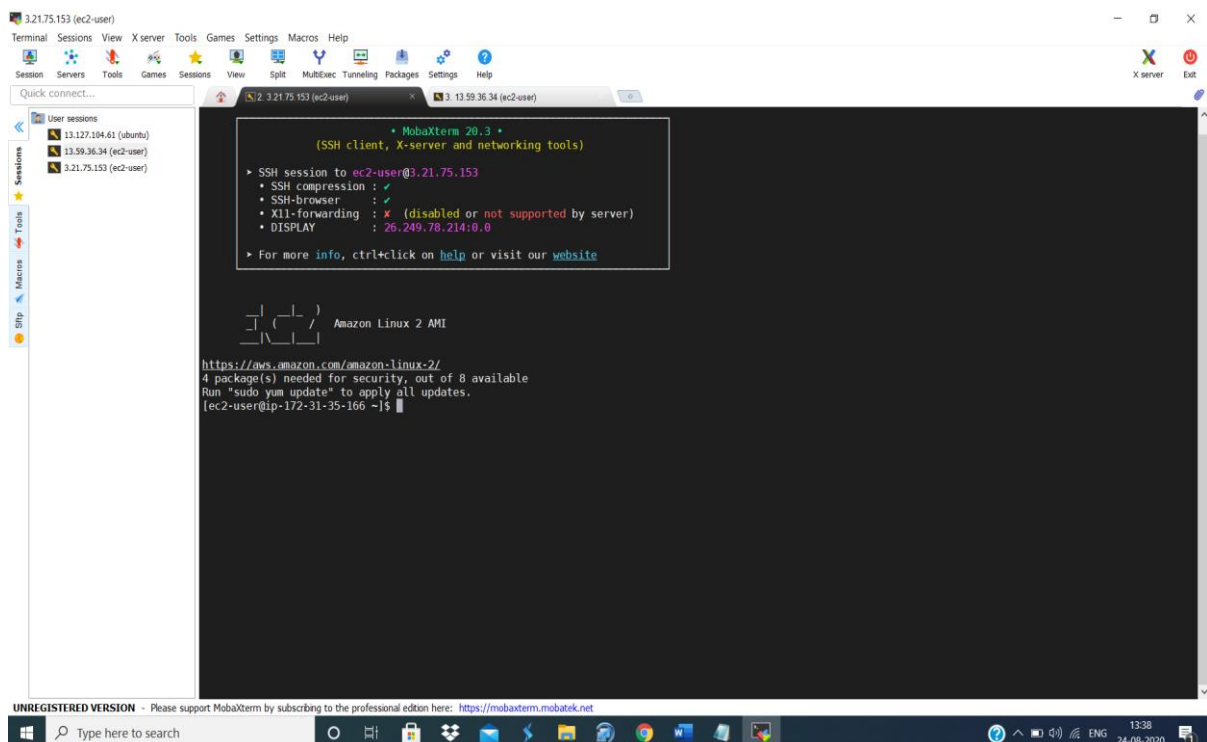


# Create a EC2 Instance and host a webpage on that instance

Step1: Create Linux instances, Use the first free Linux AMI



Step2: Launch instances using Mobaxterm



### Step3: Host html login webpage on servers

```
[root@ip-172-31-35-166 html]# vi index.html
[root@ip-172-31-35-166 html]# more index.html
<form action="action_page.php" method="post">
<div class="imgcontainer">

</div>

<div class="container">
<label for="uname"><b>Username</b></label>
<input type="text" placeholder="Enter Username" name="uname" required>

<label for="psw"><b>Password</b></label>
<input type="password" placeholder="Enter Password" name="psw" required>

<button type="submit">Login</button>

<label>
<input type="checkbox" checked="checked" name="remember"> Remember me
</label>
</div>

<div class="container" style="background-color:#f1f1f1">
<button type="button" class="cancelbtn">Cancel</button>
<span class="psw">Forgot <a href="#">password?</a></span>
</div>
</form>

[root@ip-172-31-35-166 html]# service httpd start
Redirecting to /bin/systemctl start httpd.service
[root@ip-172-31-35-166 html]#
```

port MobaXterm by subscribing to the professional edition here: <https://mobaxterm.mobatek.net>

### Step4: Check if the application is deployed on servers by copy pasting the public IP of the servers into the browser.

