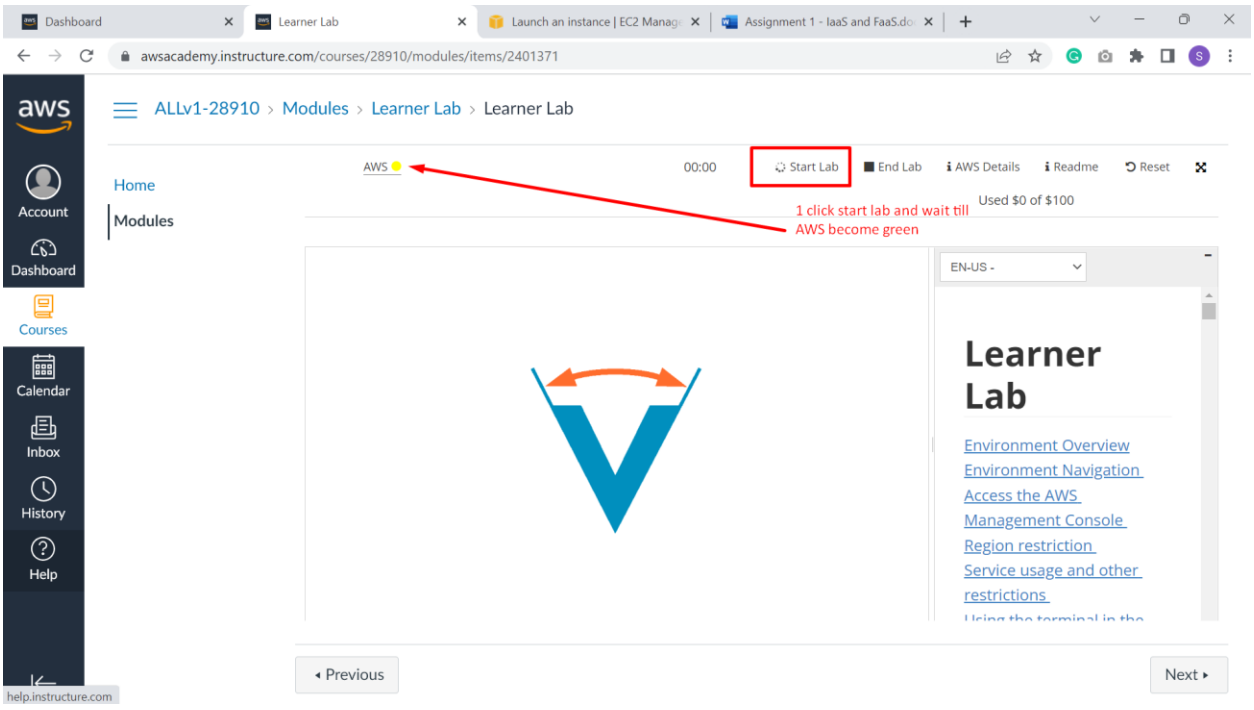
Assignment 1 – Step by step

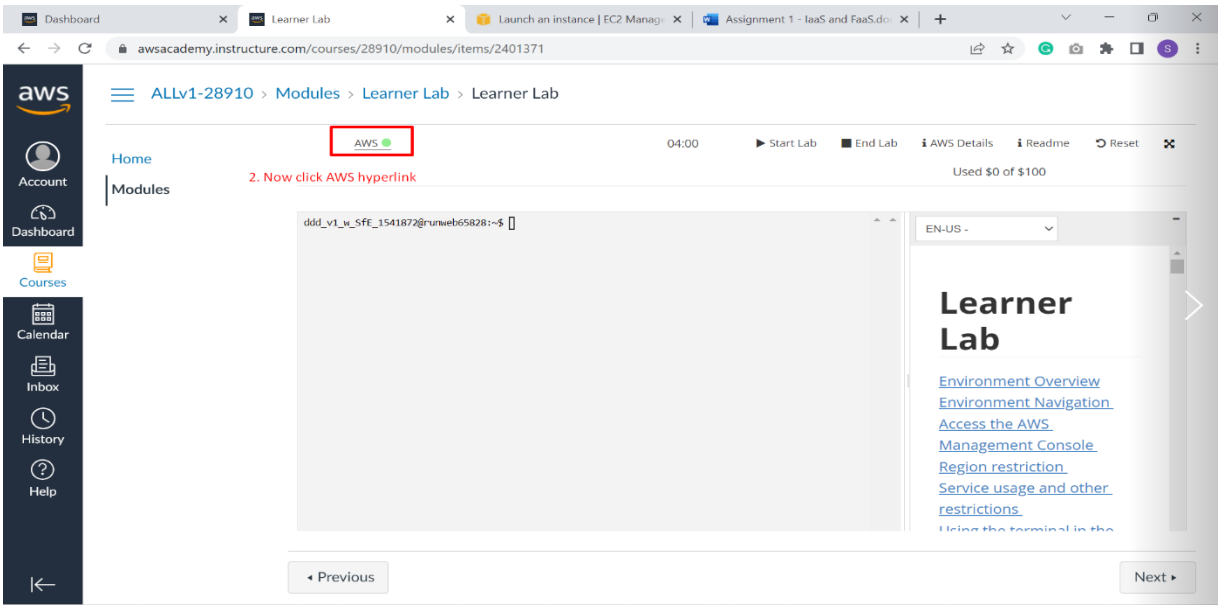
Setting up a web server on EC2

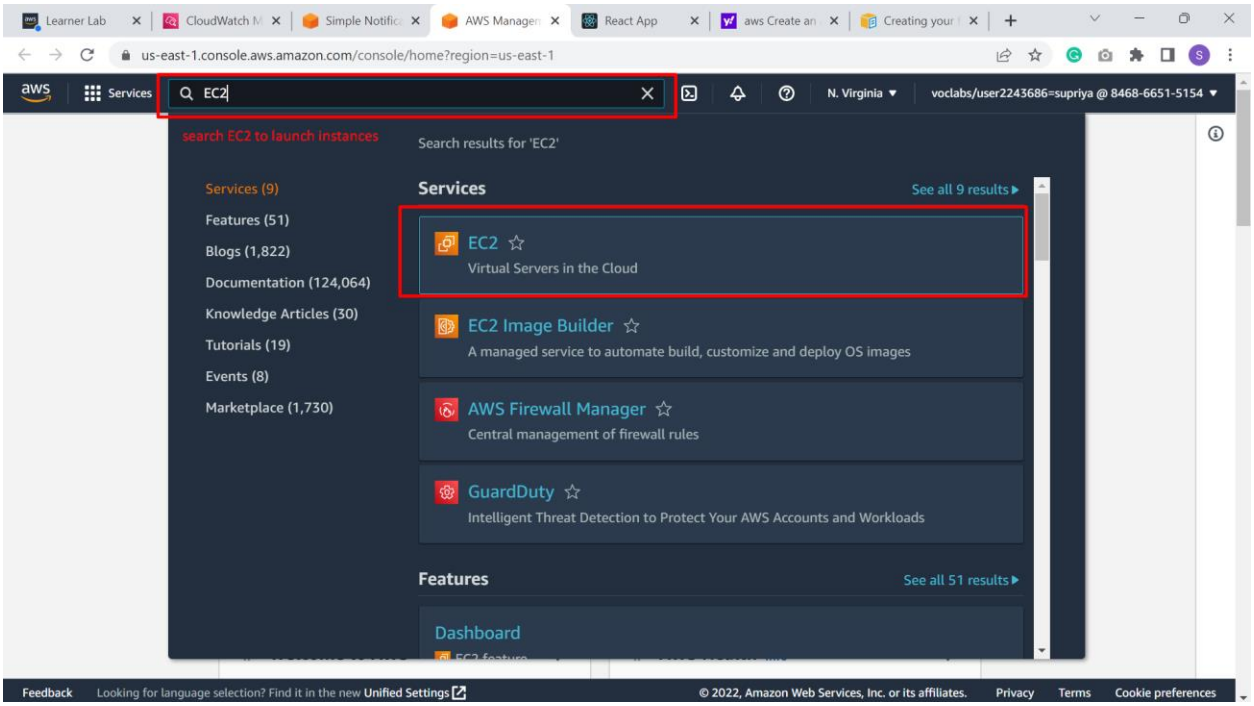
Step-by-step instructions for you to refer. There are many ways to achieve the same result. You don't have to follow it. It will waste a lot of time. Instead, you can do it on your own without following it step by step since you paid careful attention in class and understood the idea.

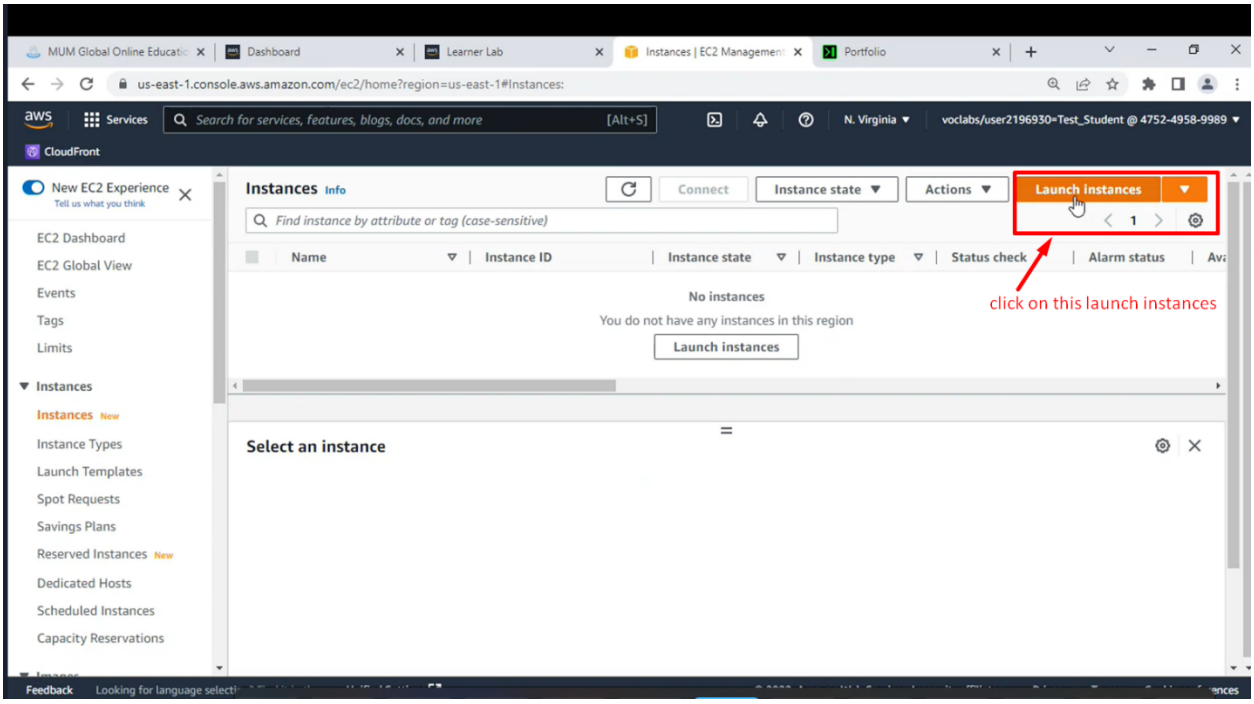
Get access to the AWS console through AWS Academy. In the AWS Academy account:

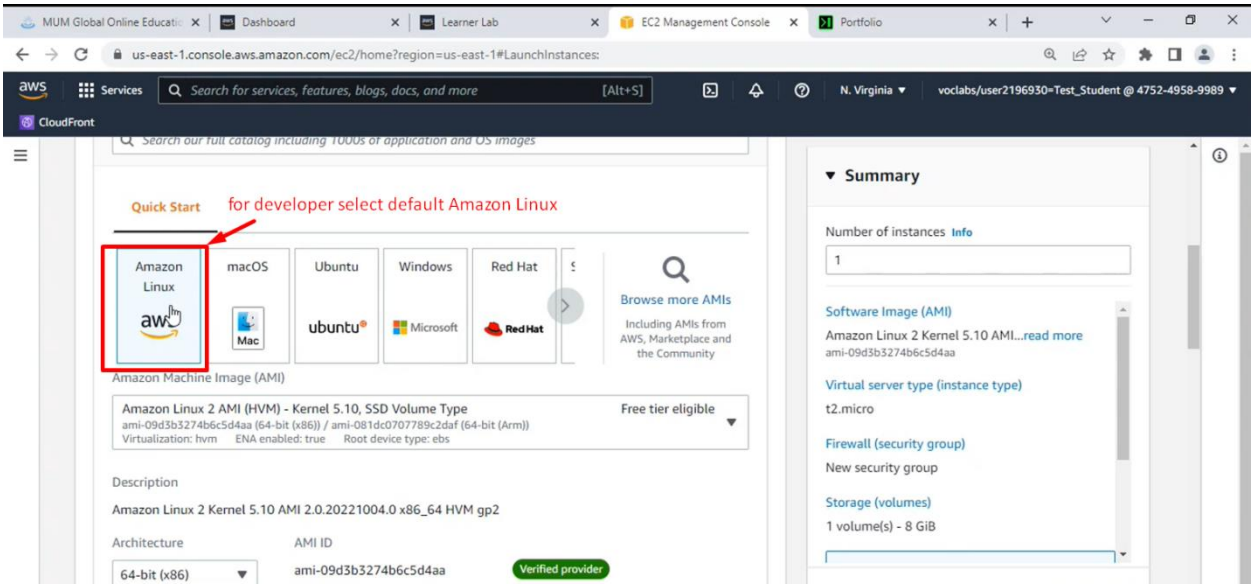
1. Spin up an EC2 instance.
    a. Allowed HTTP:80 port from the world (0.0.0.0/0) in the Network Setting panel.
    b. Expand Advanced Settings, and select the LabInstanceProfile.

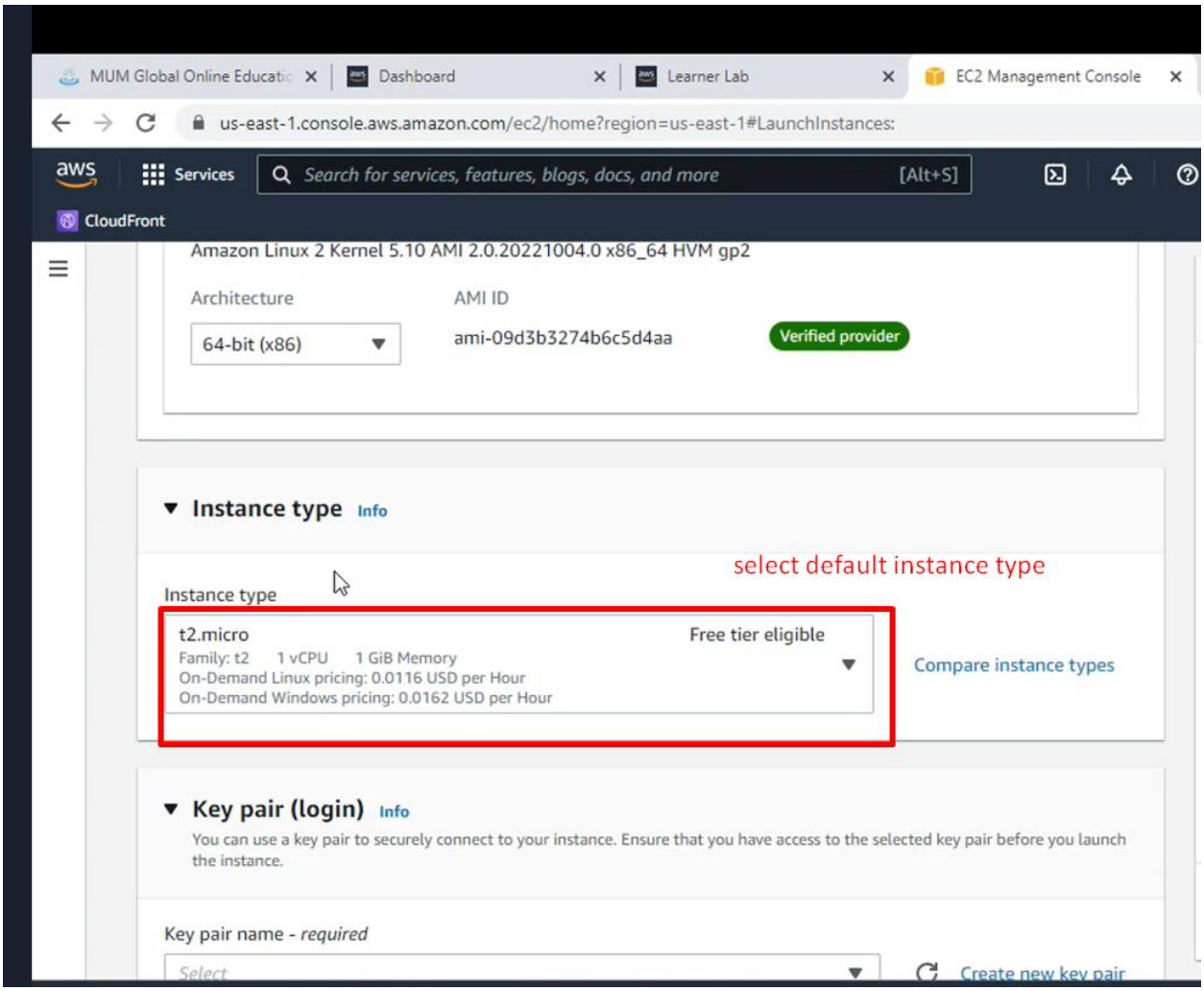


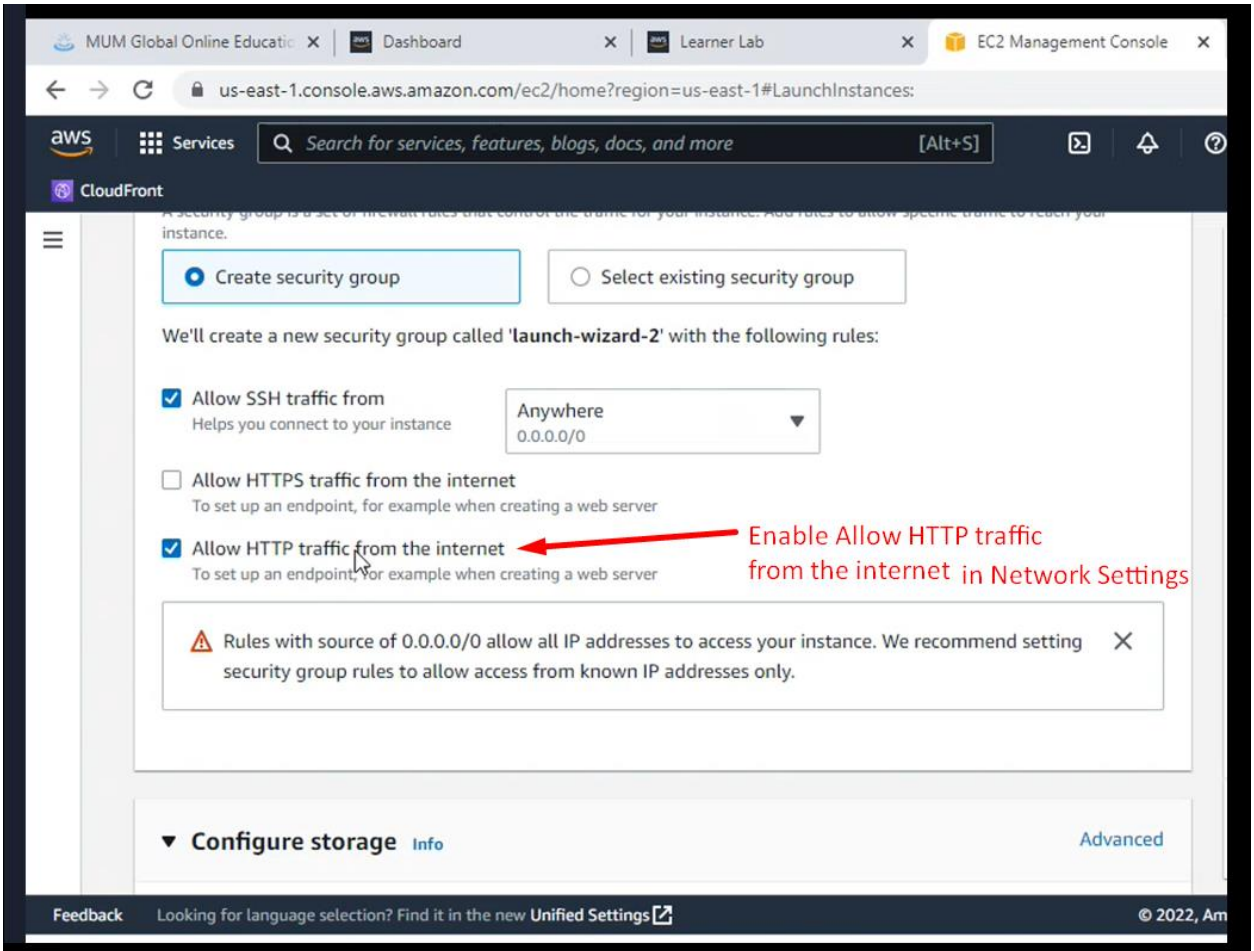


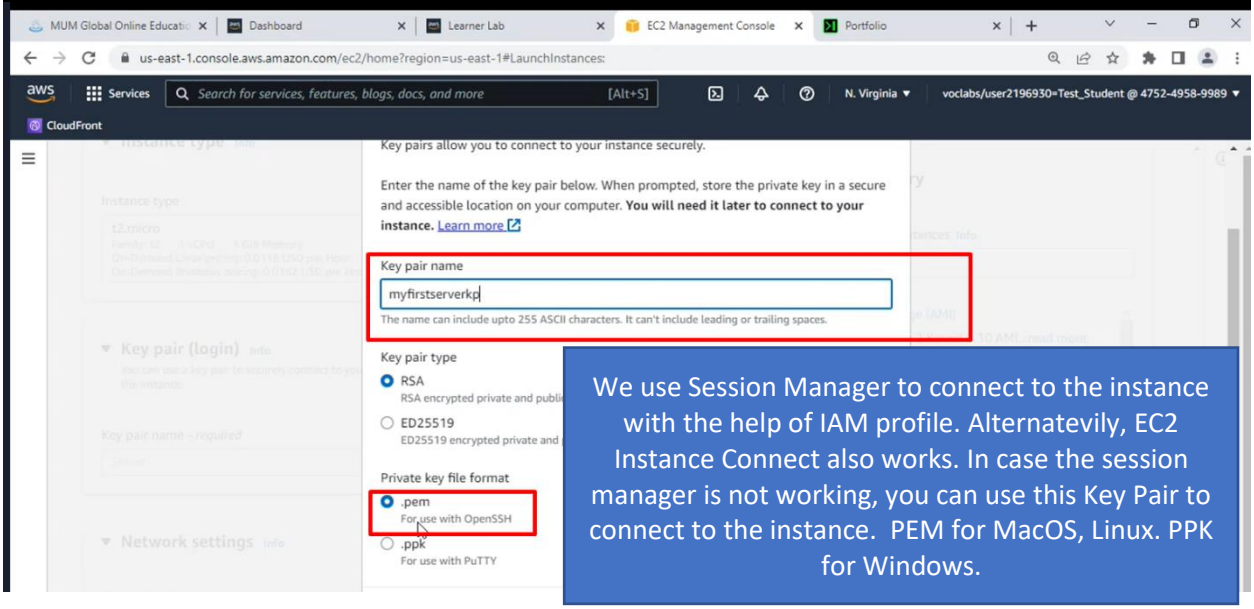

us-east-1.console.aws.amazon.com/console/home?region=us-east-1
EC2
search EC2 to launch instances
Search results for 'EC2'
Services (9)
Features (51)
Blogs (1,822)
Documentation (124,064)
Knowledge Articles (30)
Tutorials (19)
Events (8)
Marketplace (1,730)
Services
See all 9 results
EC2
Virtual Servers in the Cloud
EC2 Image Builder
A managed service to automate build, customize and deploy OS images
AWS Firewall Manager
Central management of firewall rules
GuardDuty
Intelligent Threat Detection to Protect Your AWS Accounts and Workloads
Features
See all 51 results
Dashboard
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

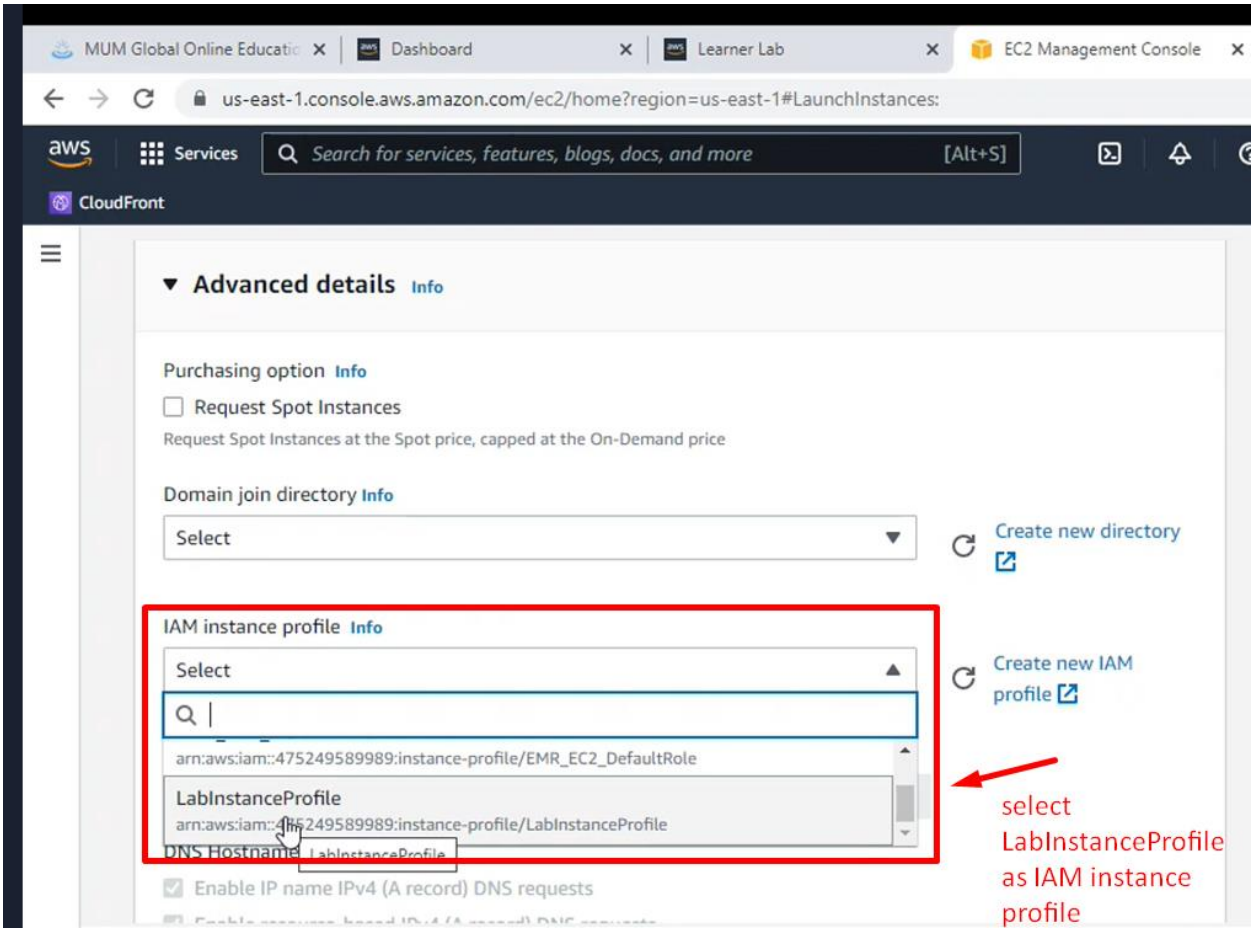

us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#Instances:
Search for services, features, blogs, docs, and more
[Alt+S]
N. Virginia
CloudFront
New EC2 Experience
EC2 Dashboard
EC2 Global View
Events
Tags
Limits
Instances
Instances New
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances New
Dedicated Hosts
Scheduled Instances
Capacity Reservations
Instances Info
Connect
Instance state
Actions
Launch instances
Find instance by attribute or tag (case-sensitive)
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
No instances
You do not have any instances in this region
Launch instances
click on this launch instances
Select an instance
Feedback

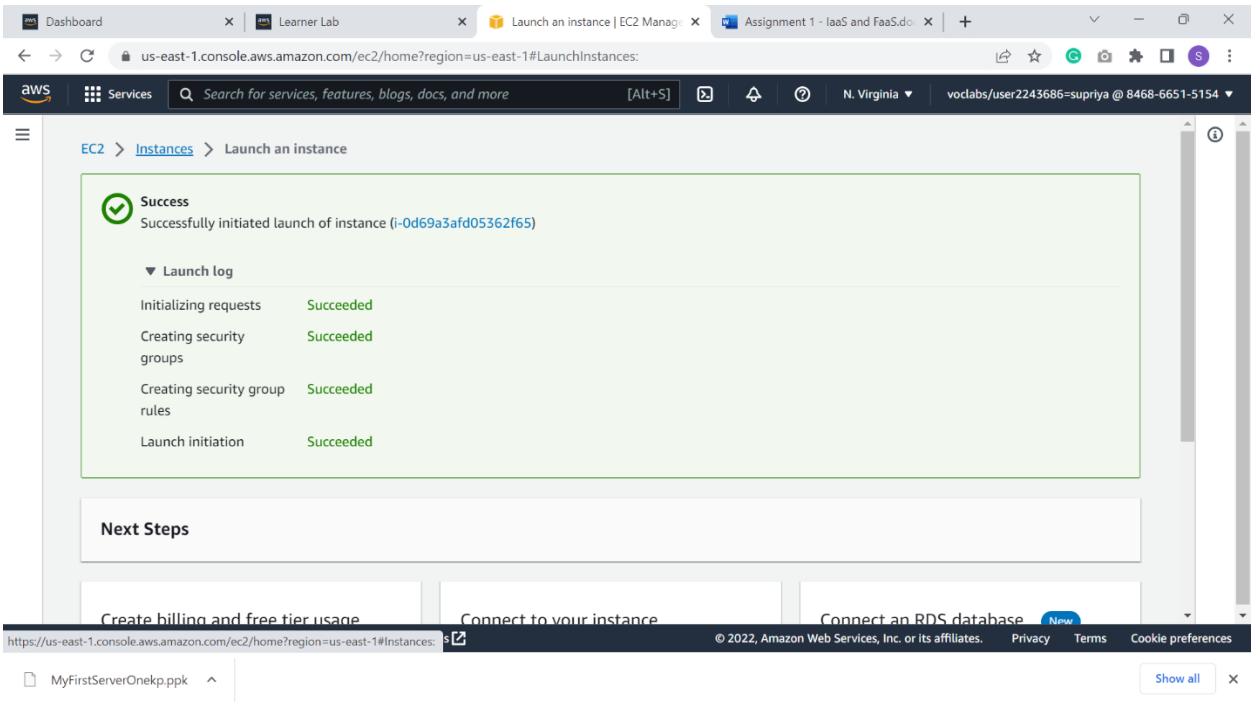

MUM Global Online Educatic
Dashboard
Learner Lab
EC2 Management Console
Portfolio
us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#LaunchInstances:
aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
N. Virginia
voclabs/user2196930=Test_Student @ 4752-4958-9989
CloudFront
Quick Start
for developer select default Amazon Linux
Amazon Linux
macOS
Ubuntu
Windows
Red Hat
Browse more AMIs
Including AMIs from AWS, Marketplace and the Community
Amazon Machine Image (AMI)
Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type
ami-09d3b3274b6c5d4aa (64-bit (x86)) / ami-081dc0707789c2daf (64-bit (Arm))
Virtualization: hvm ENA enabled: true Root device type: ebs
Free tier eligible
Description
Amazon Linux 2 Kernel 5.10 AMI 2.0.20221004.0 x86_64 HVM gp2
Architecture
AMI ID
64-bit (x86)
ami-09d3b3274b6c5d4aa
Verified provider
Summary
Number of instances Info
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

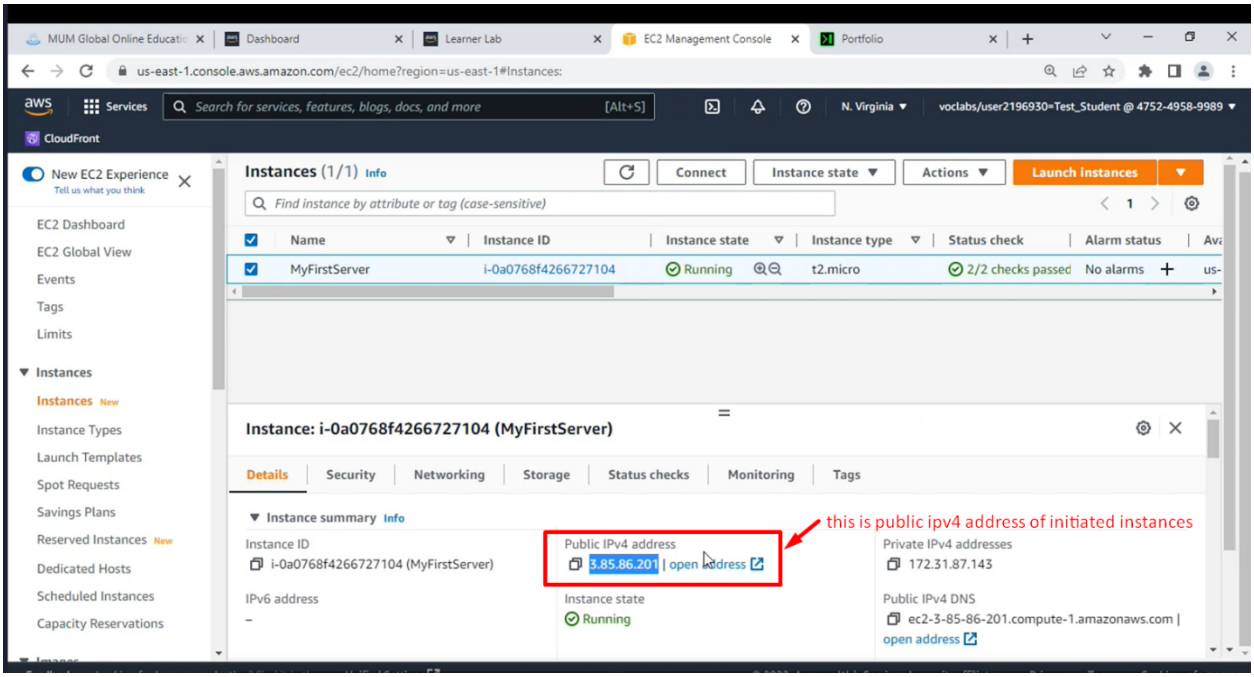

MUM Global Online Educatic
Dashboard
Learner Lab
EC2 Management Console
us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#LaunchInstances:
aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
CloudFront
Amazon Linux 2 Kernel 5.10 AMI 2.0.20221004.0 x86_64 HVM gp2
Architecture
AMI ID
64-bit (x86)
ami-09d3b3274b6c5d4aa
Verified provider
Instance type Info
select default instance type
Instance type
t2.micro
Free tier eligible
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
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 Educatic
Dashboard
Learner Lab
EC2 Management Console
us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#LaunchInstances:
Services
Search for services, features, blogs, docs, and more
[Alt+S]
CloudFront
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
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
© 2022, Am

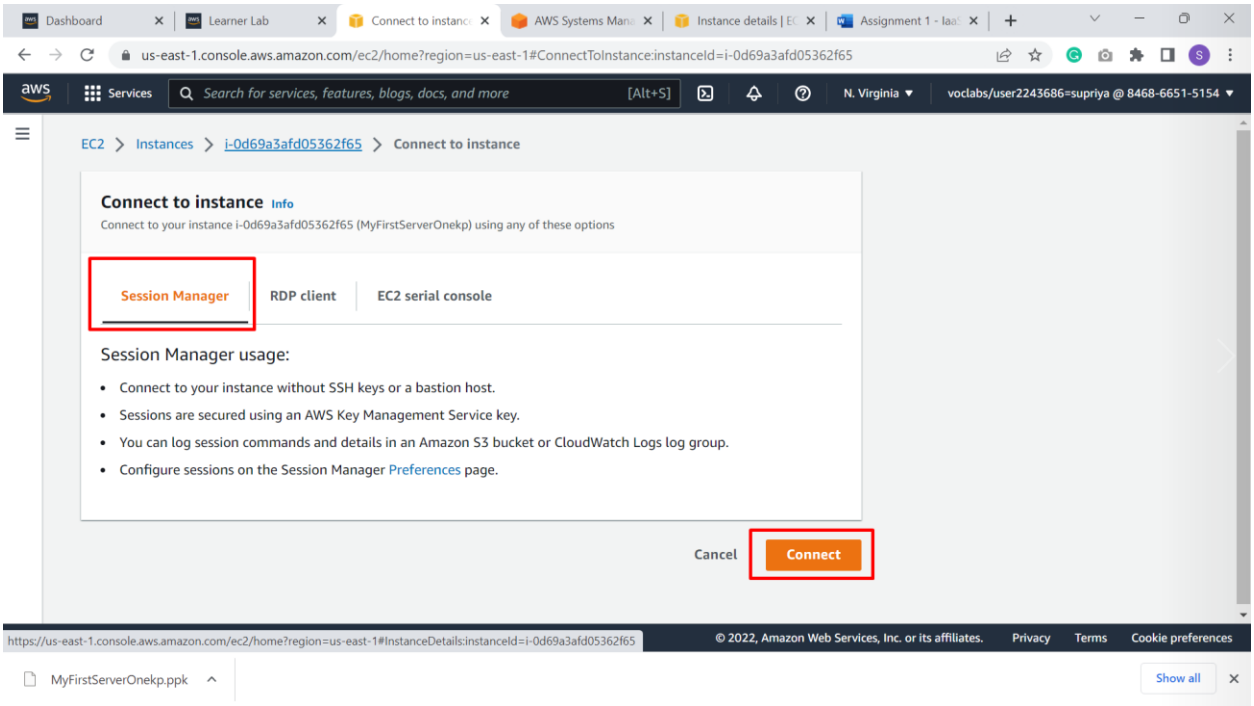

MUM Global Online Educatic
Dashboard
Learner Lab
EC2 Management Console
Portfolio
us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#LaunchInstances:
Services
Search for services, features, blogs, docs, and more
[Alt+S]
N. Virginia
voclabs/user2196930=Test_Student @ 4752-4958-9989
CloudFront
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 upto 255 ASCII characters. It can't include leading or trailing spaces.
Key pair type
RSA
RSA encrypted private and public
ED25519
ED25519 encrypted private and
Private key file format
.pem
For use with OpenSSH
.ppk
For use with PuTTY
Key pair (login)
Network settings
We use Session Manager to connect to the instance with the help of IAM profile. Alternatevily, 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 Educatio
Dashboard
Learner Lab
EC2 Management Console
us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#LaunchInstances:
Services
Search for services, features, blogs, docs, and more
[Alt+S]
CloudFront
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
Enable IP name IPv4 (A record) DNS requests
select LabInstanceProfile as IAM instance profile


Dashboard
Learner Lab
Launch an instance | EC2 Manage
Assignment 1 - IaaS and FaaS.do
us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#LaunchInstances:
Services
Search for services, features, blogs, docs, and more
[Alt+S]
N. Virginia
voclabs/user2243686=supriya @ 8468-6651-5154
EC2 > Instances > Launch an instance
Success
Successfully initiated launch of instance (i-0d69a3afd05362f65)
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:
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
MyFirstServerOnekp.ppk
Show all

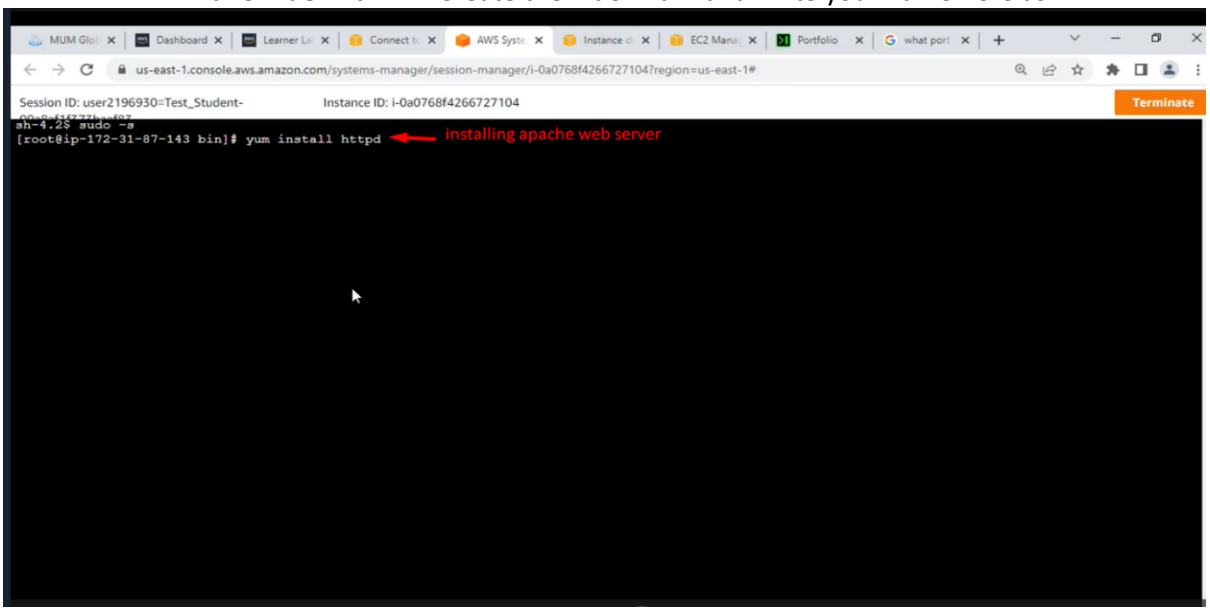


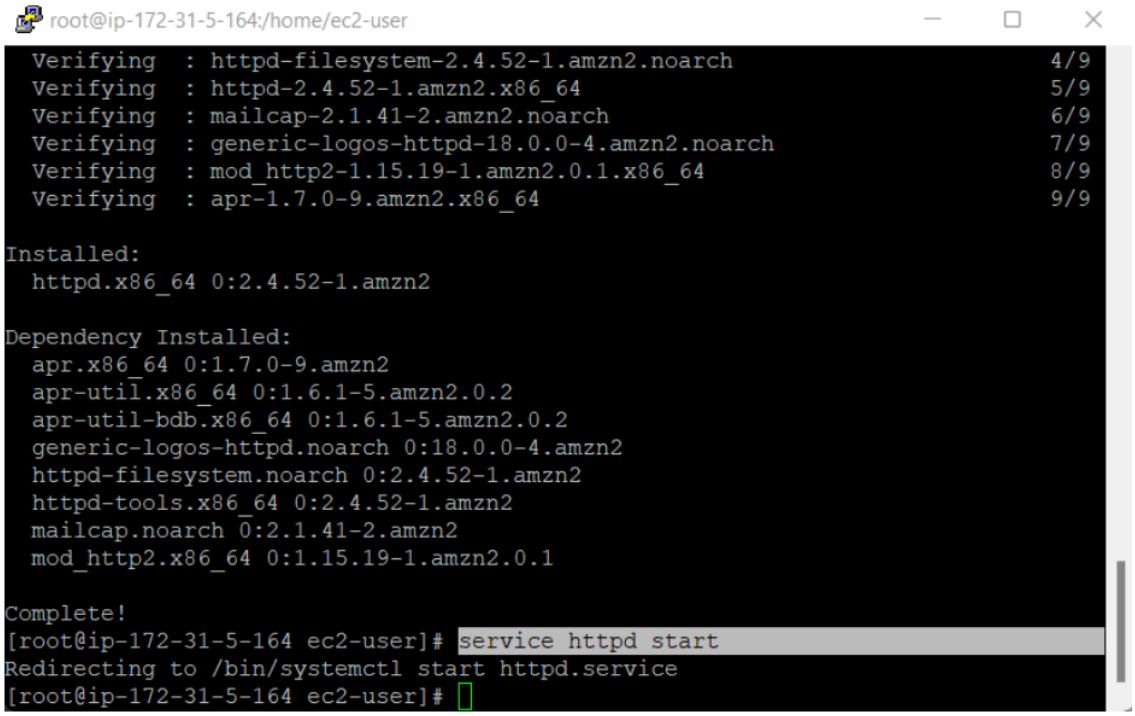
2. Configure a web server on EC2.
    a. Select the instance
    b. Hit Connect
    c. Select the “Session Manager” tab and hit Connect.

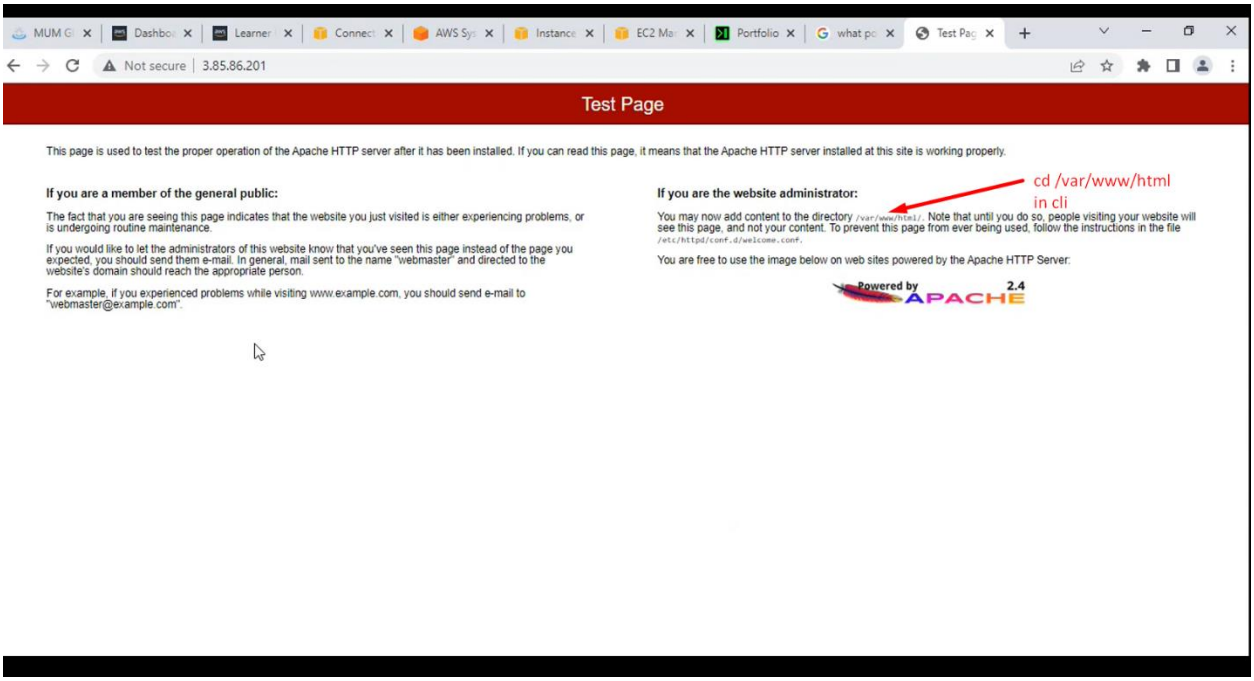


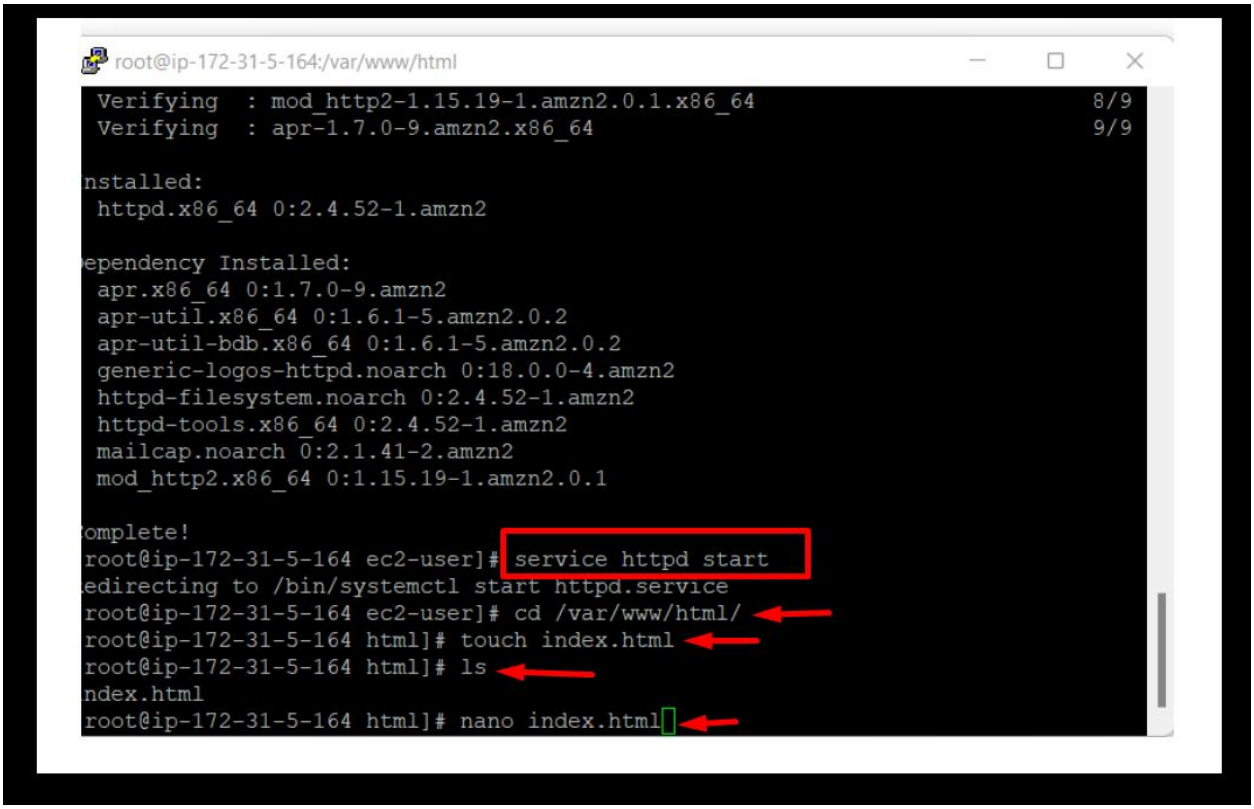
    d. To install and customize a web server:
    sudo -s => Logging as a root user so you can start the HTTPD service
    yum install httpd -y => Installing a web server
    service httpd start => Starting the server

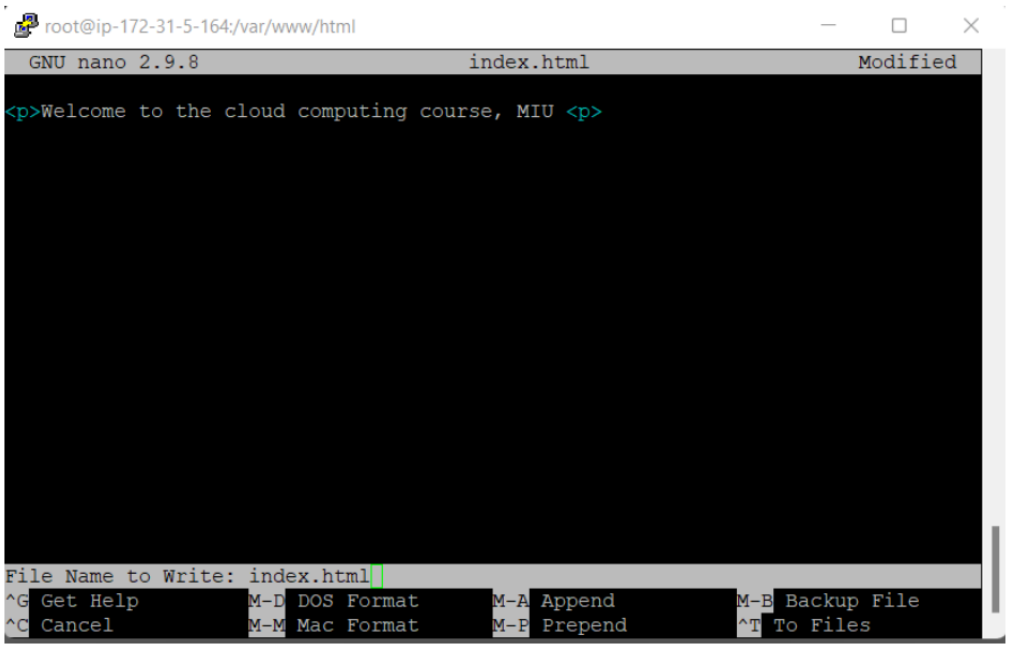
cd /var/www/html => Changing the directory to customize the default Apache page.
nano index.html => Create the index.html and write your name here as HTML.



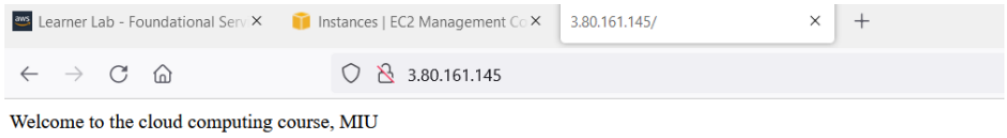



Not secure | 3.85.86.201
Test Page
This page is used to test the proper operation of the Apache HTTP server after it has been installed. If you can read this page, it means that the Apache HTTP server installed at this site is working properly.
If you are a member of the general public:
The fact that you are seeing this page indicates that the website you just visited is either experiencing problems, or is undergoing routine maintenance.
If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster" and directed to the website's domain should reach the appropriate person.
For example, if you experienced problems while visiting www.example.com, you should send e-mail to "webmaster@example.com".
If you are the website administrator:
cd /var/www/html in cli
You may now add content to the directory /var/www/html/. Note that until you do so, people visiting your website will see this page, and not your content. To prevent this page from ever being used, follow the instructions in the file /etc/httpd/conf.d/welcome.conf.
You are free to use the image below on web sites powered by the Apache HTTP Server:
Powered by APACHE 2.4


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
nstalled:
httpd.x86_64 0:2.4.52-1.amzn2
ependency 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
omplete!
root@ip-172-31-5-164 ec2-user]# service httpd start
edirecting 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
ndex.html
root@ip-172-31-5-164 html]# nano index.html

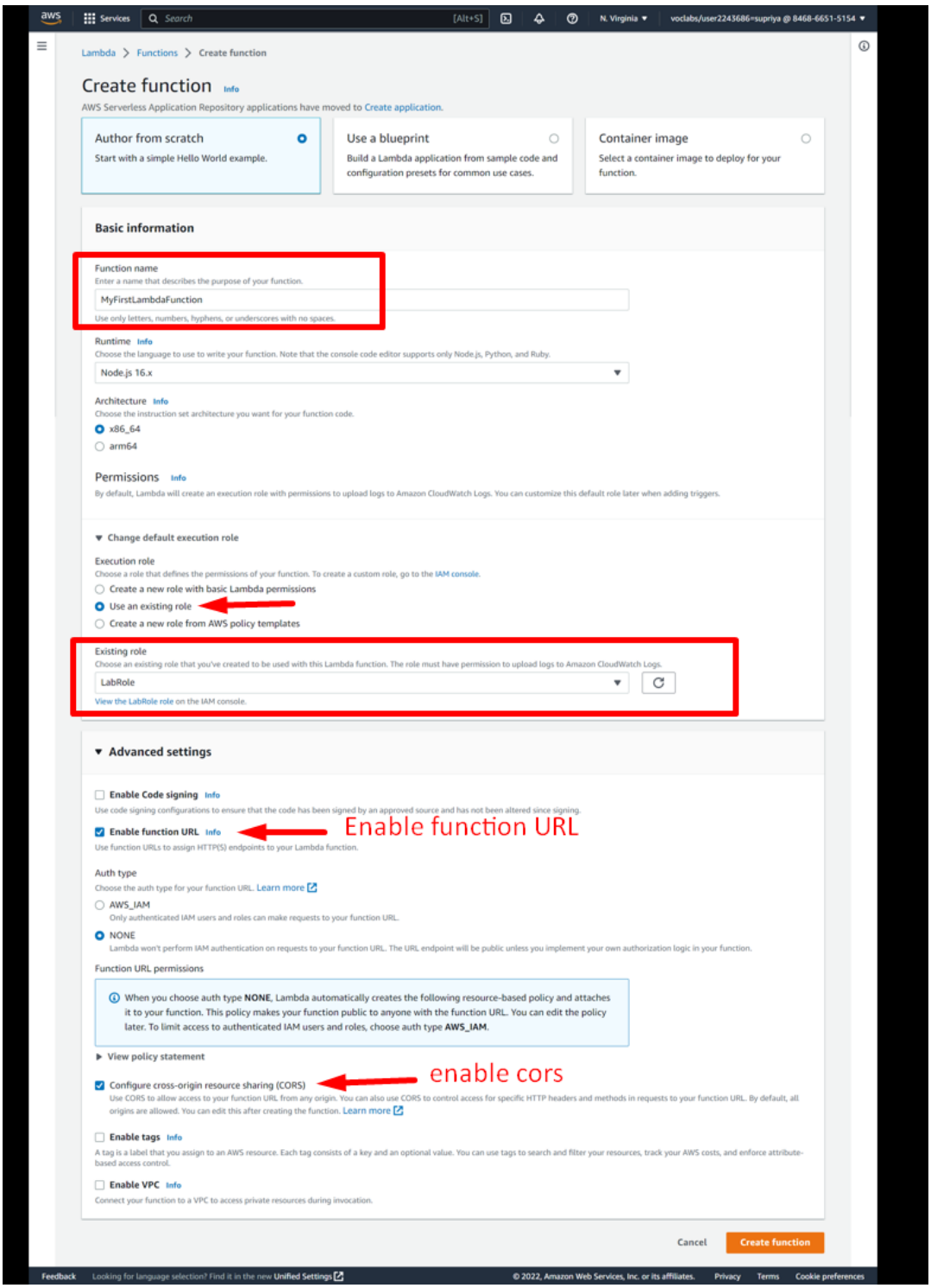


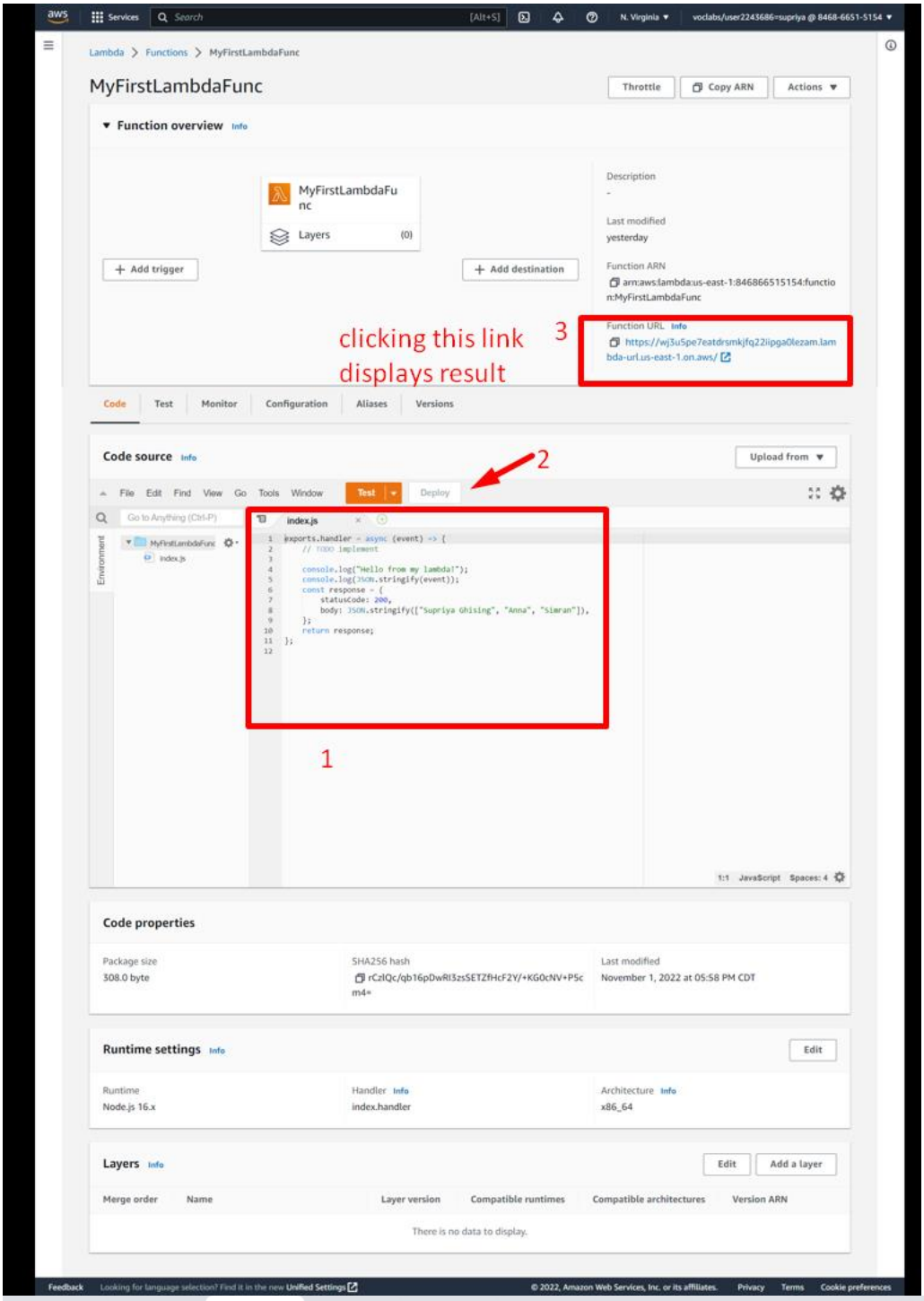
Go to the website and reload



Creating a public Lambda endpoint

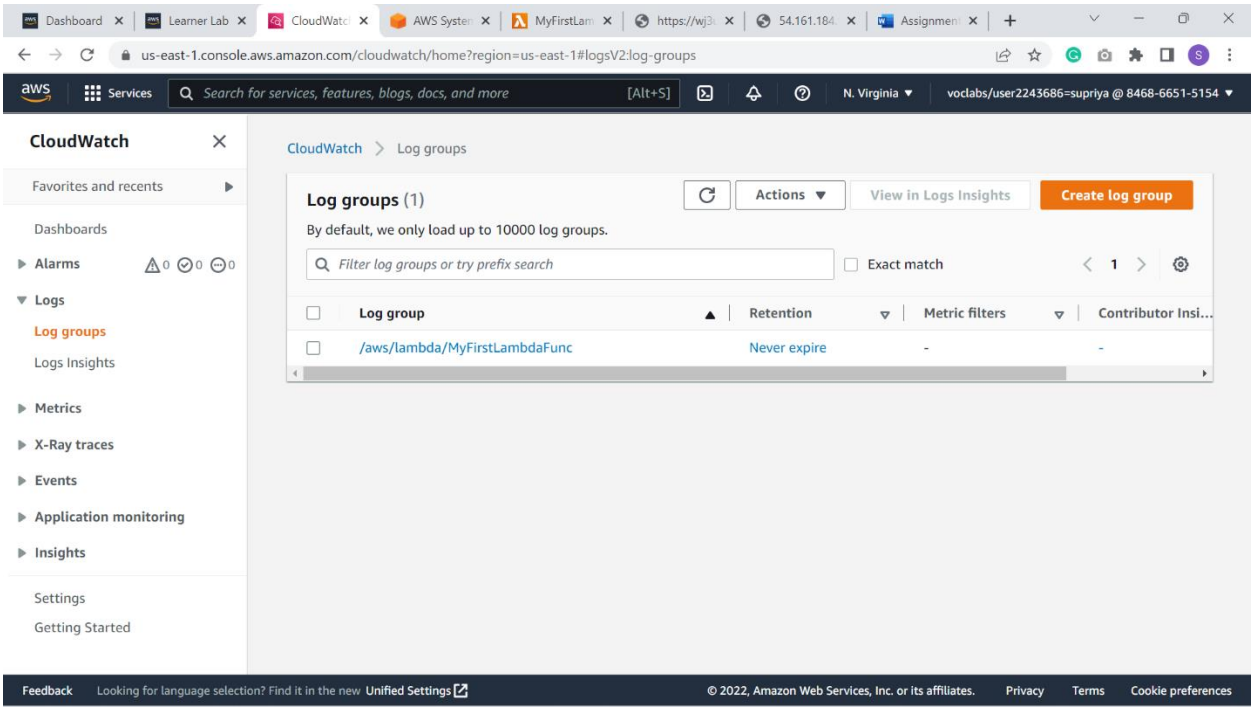
3. Creating a lambda function returns an array of strings. Make it an API by enabling the public URL.
    a. Choose the LabRole as IAM
    b. Enable URL and enable CORS





wj3u5pe7eatdrsmkjfq22iipga0lezam.lambda-url.us-east-1.on.aws

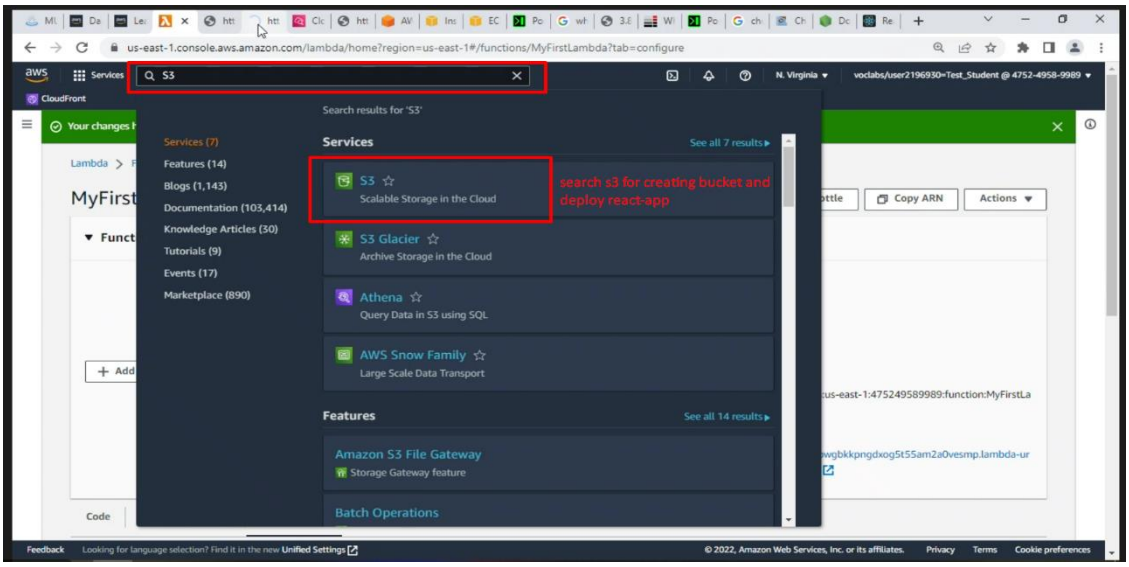
["Supriya Ghising","Anna","Simran"]

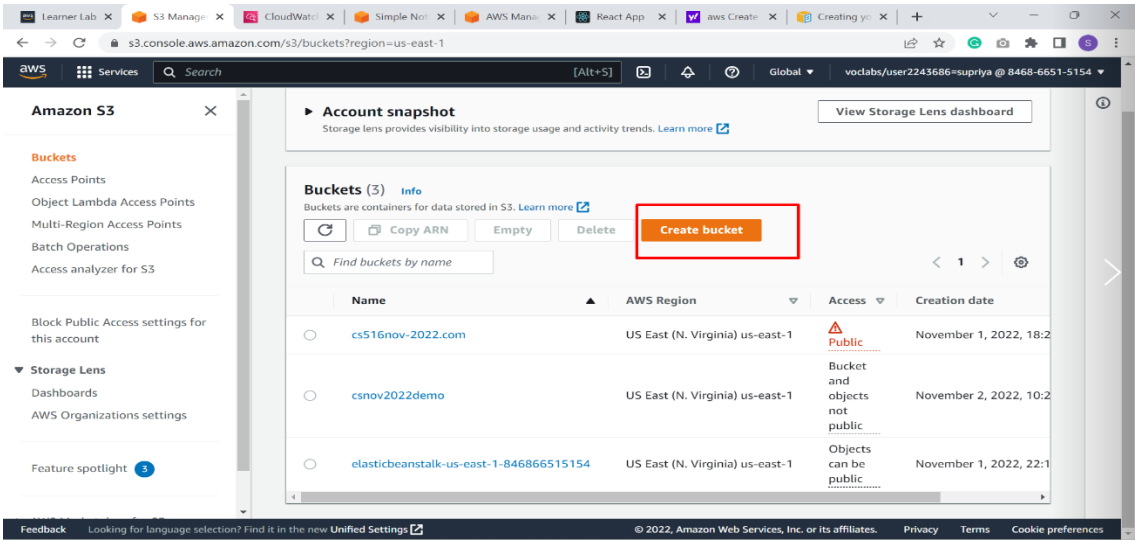

Dashboard
Learner Lab
CloudWatch
AWS System
MyFirstLam
https://wj3
54.161.184
Assignmen
us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#logsV2:log-groups
aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
N. Virginia
voclabs/user2243686=supriya @ 8468-6651-5154
CloudWatch
Favorites and recents
Dashboards
Alarms
Logs
Log groups
Logs Insights
Metrics
X-Ray traces
Events
Application monitoring
Insights
Settings
Getting Started
CloudWatch
Log groups
Log groups (1)
Actions
View in Logs Insights
Create log group
By default, we only load up to 10000 log groups.
Filter log groups or try prefix search
Exact match
1
Log group
Retention
Metric filters
Contributor Insi...
/aws/lambda/MyFirstLambdaFunc
Never expire
-
-
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

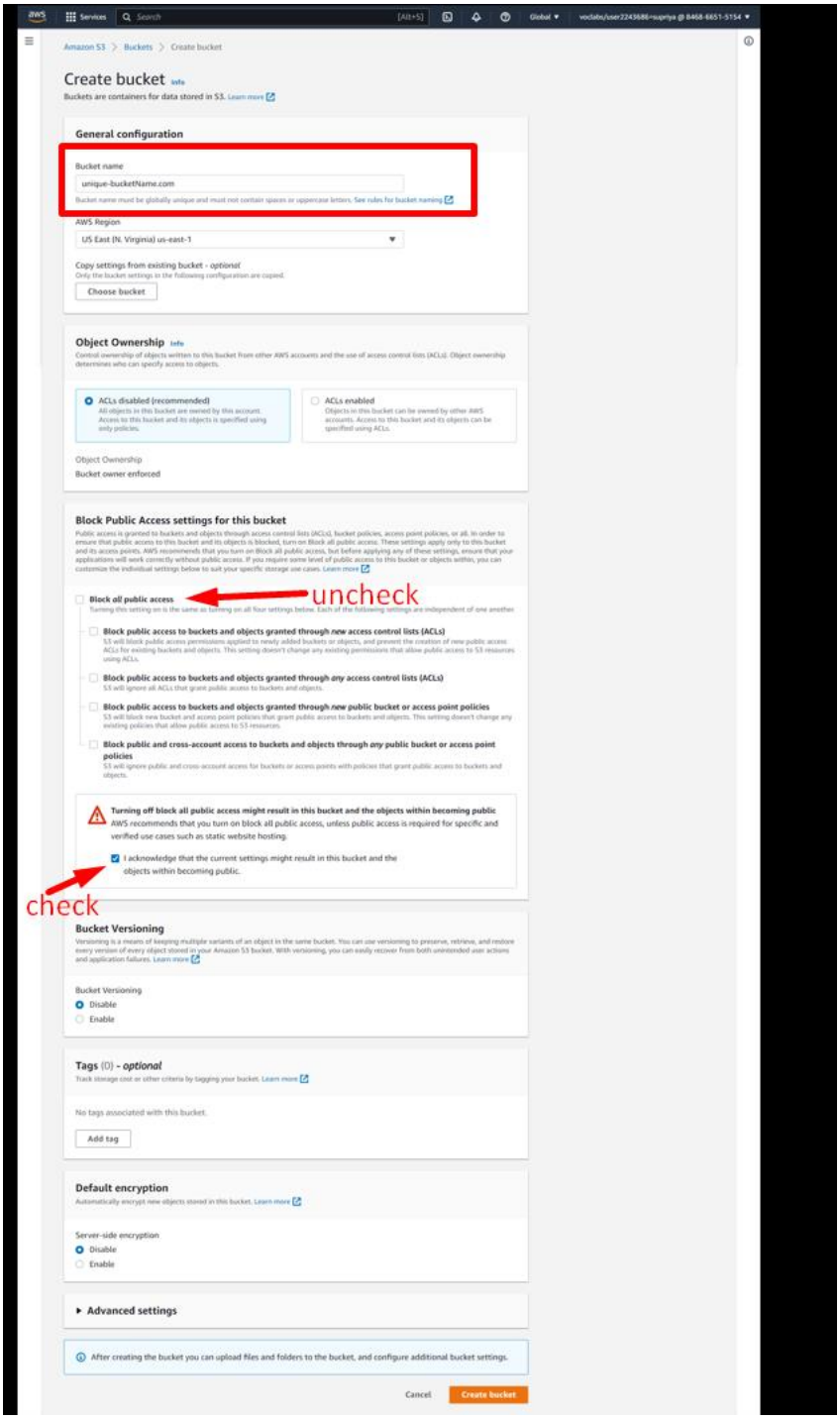
Deploying a React app to S3

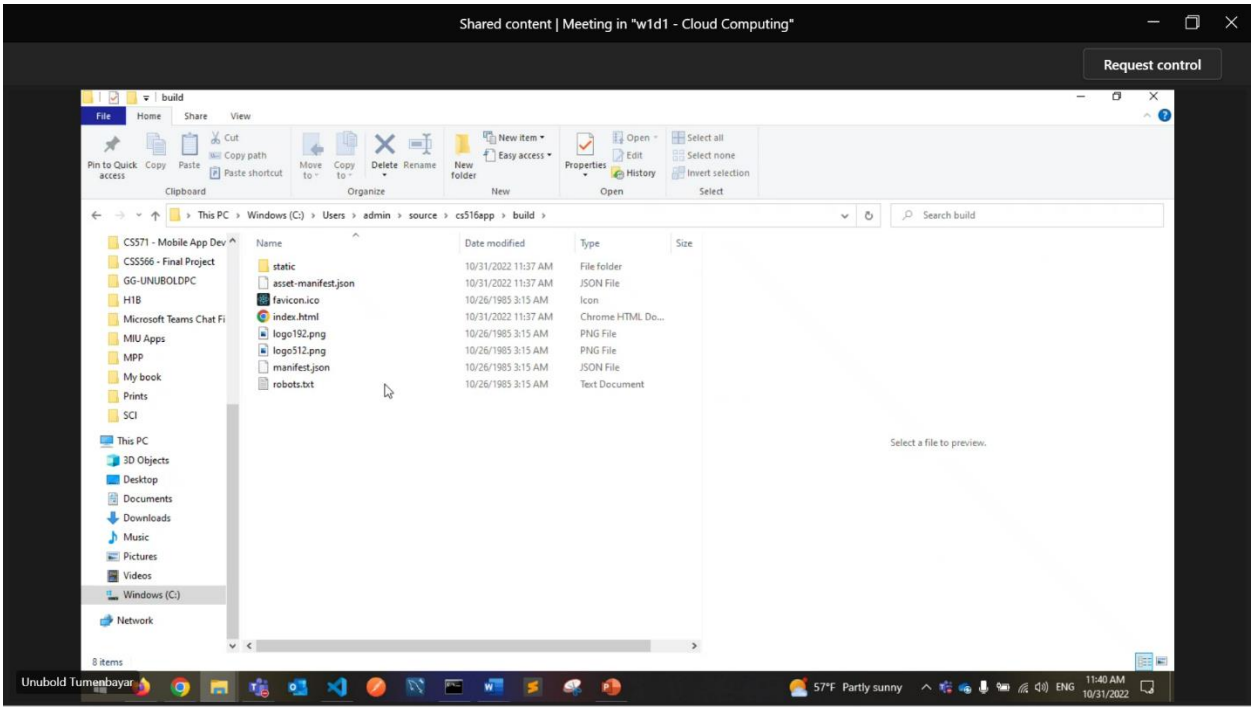
1) Deploy the front-end app in S3. Run in command prompt, npm run build

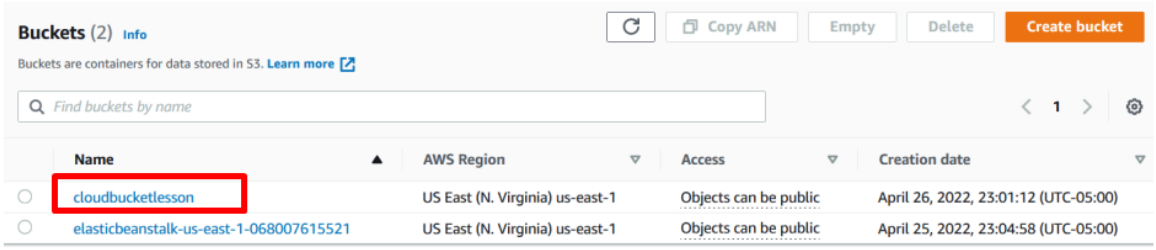
   Go to S3 AWS service and create Bucket





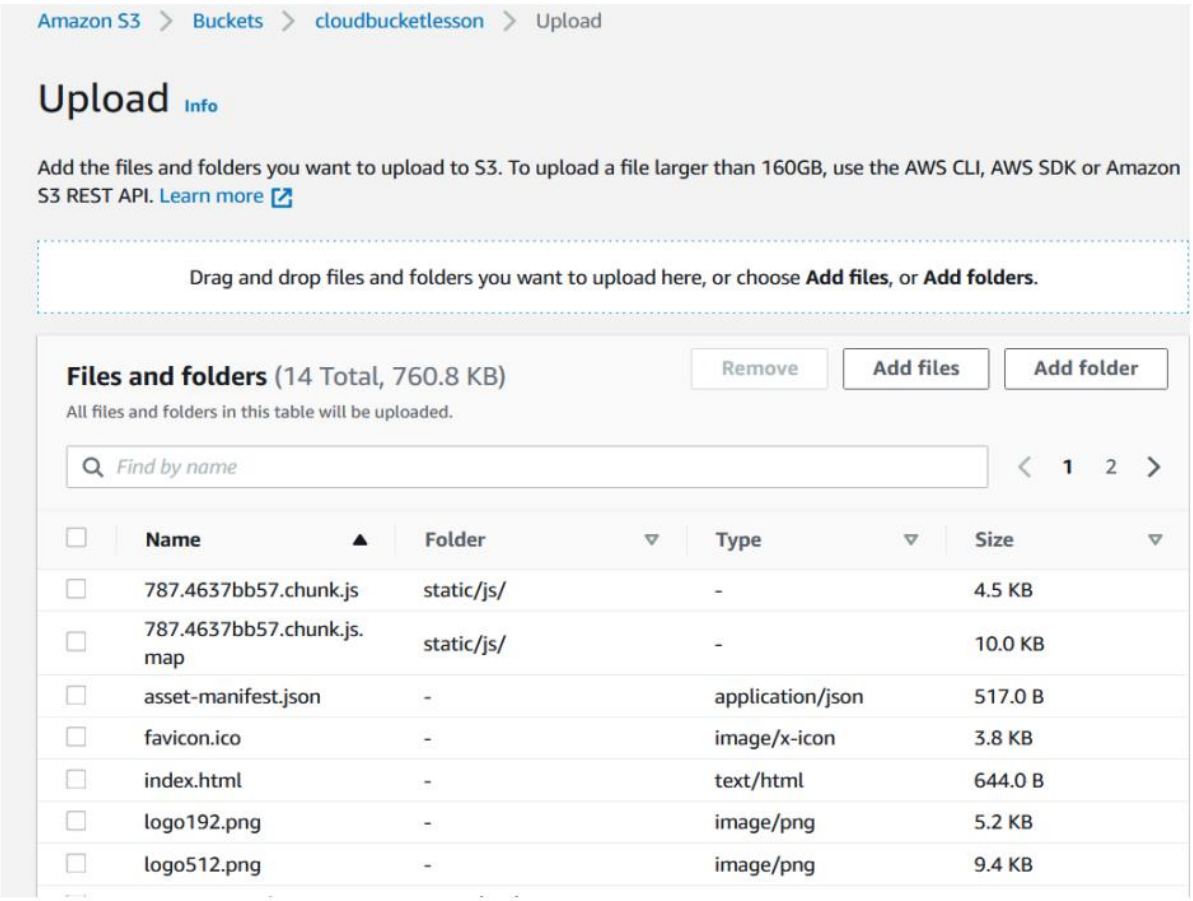

Amazon S3 > Buckets > Create bucket
Create bucket
Buckets are containers for data stored in S3.
General configuration
Bucket name
unique-bucketName.com
AWS Region
US East (N. Virginia) us-east-1
Copy settings from existing bucket - optional
Choose bucket
Object Ownership
ACLs disabled (recommended)
ACLs enabled
Object Ownership
Bucket owner enforced
Block Public Access settings for this bucket
Block all public access
uncheck
Block public access to buckets and objects granted through new access control lists (ACLs)
Block public access to buckets and objects granted through any access control lists (ACLs)
Block public access to buckets and objects granted through new public bucket or access point policies
Block public and cross-account access to buckets and objects through any public bucket or access point policies
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.
check
Bucket Versioning
Bucket Versioning
Disable
Enable
Tags (0) - optional
No tags associated with this bucket.
Add tag
Default encryption
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



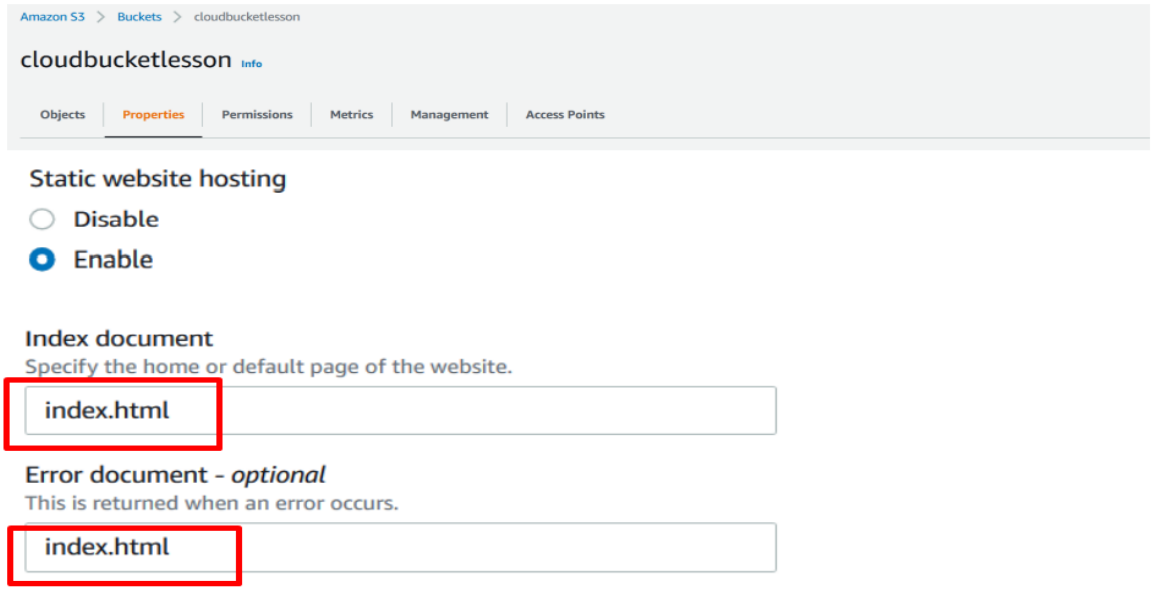


Go to the cloudbucketlesson bucket to upload build folders files of project.

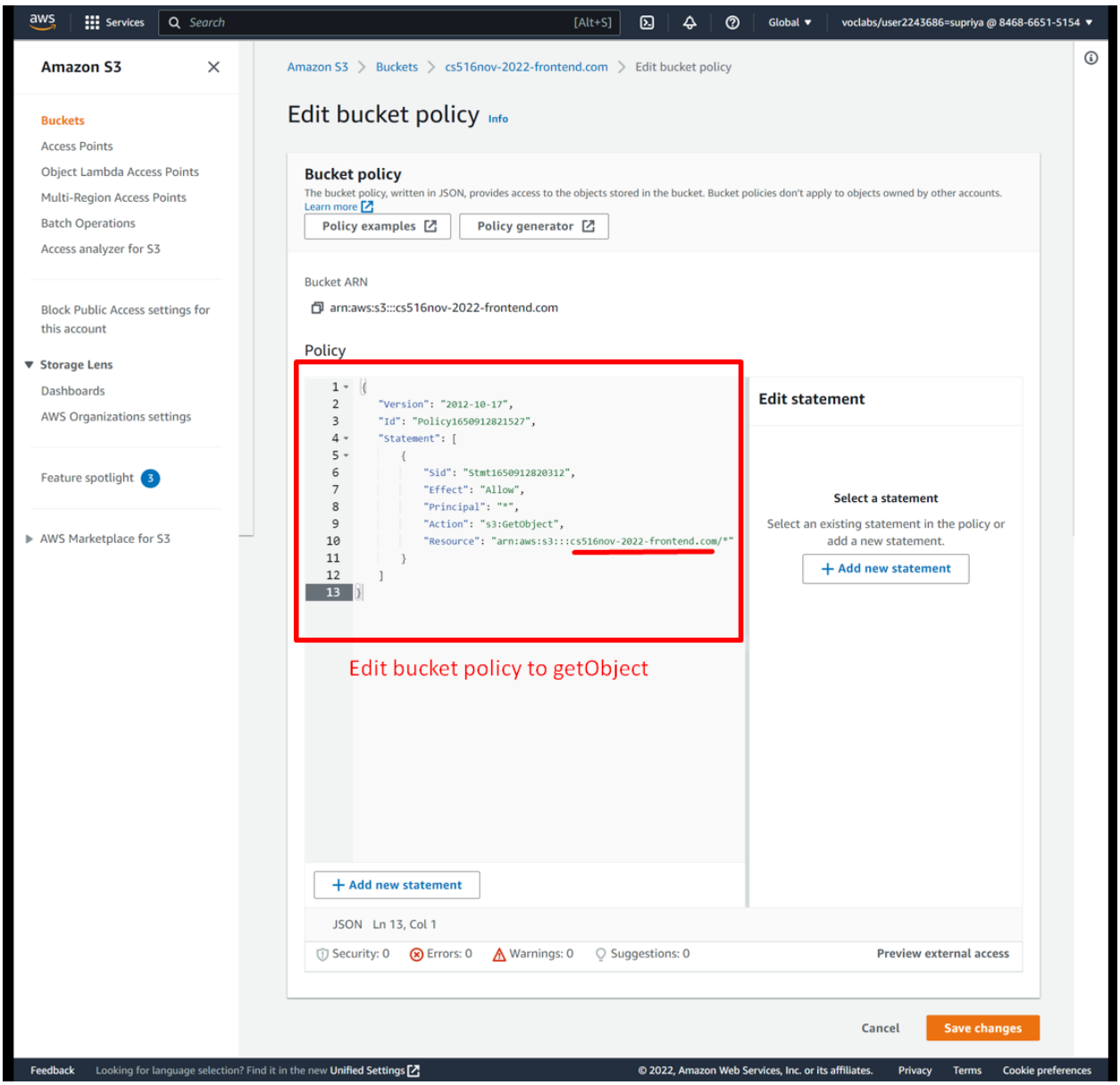
click to the created bucket and upload files or folders of project, you can upload images, videos

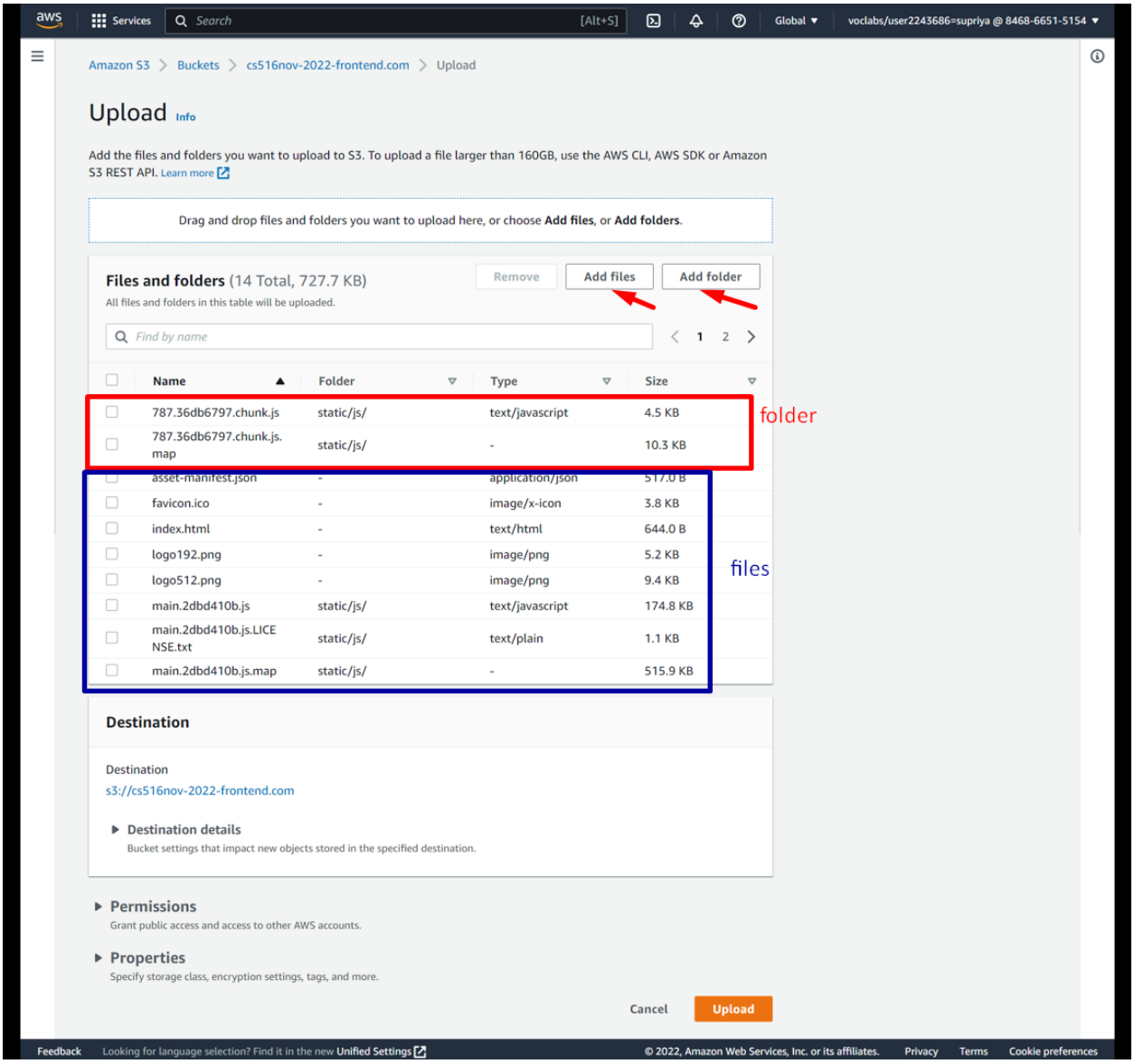


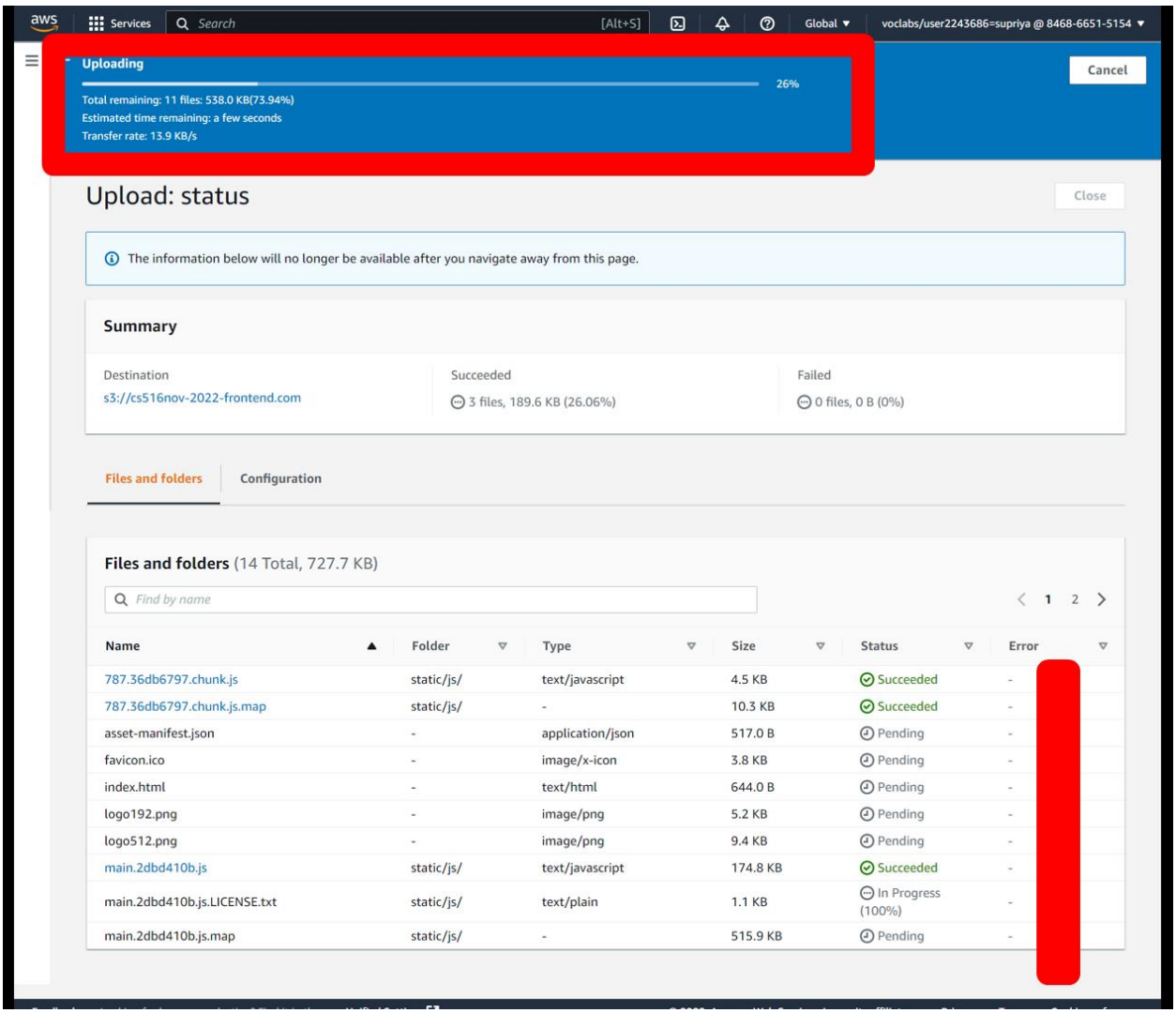
After uploading complete go to the properties tab of bucket.

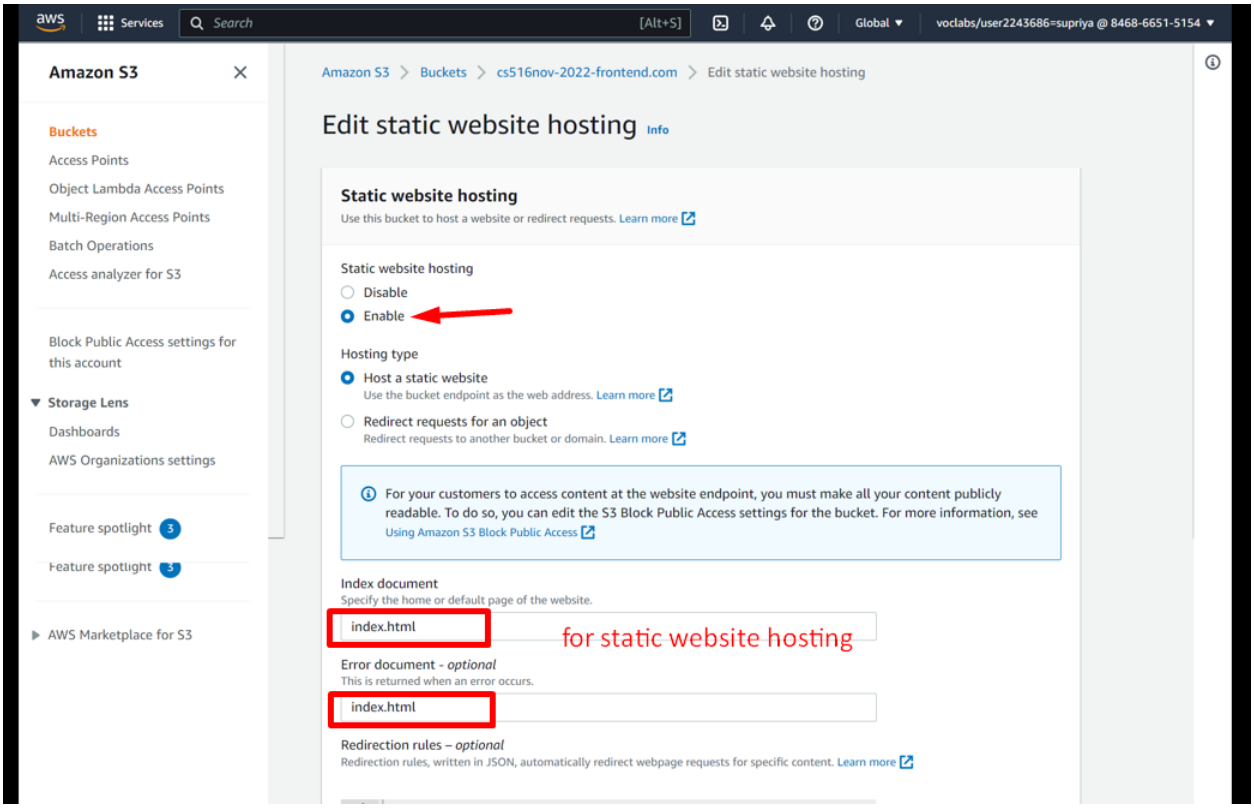


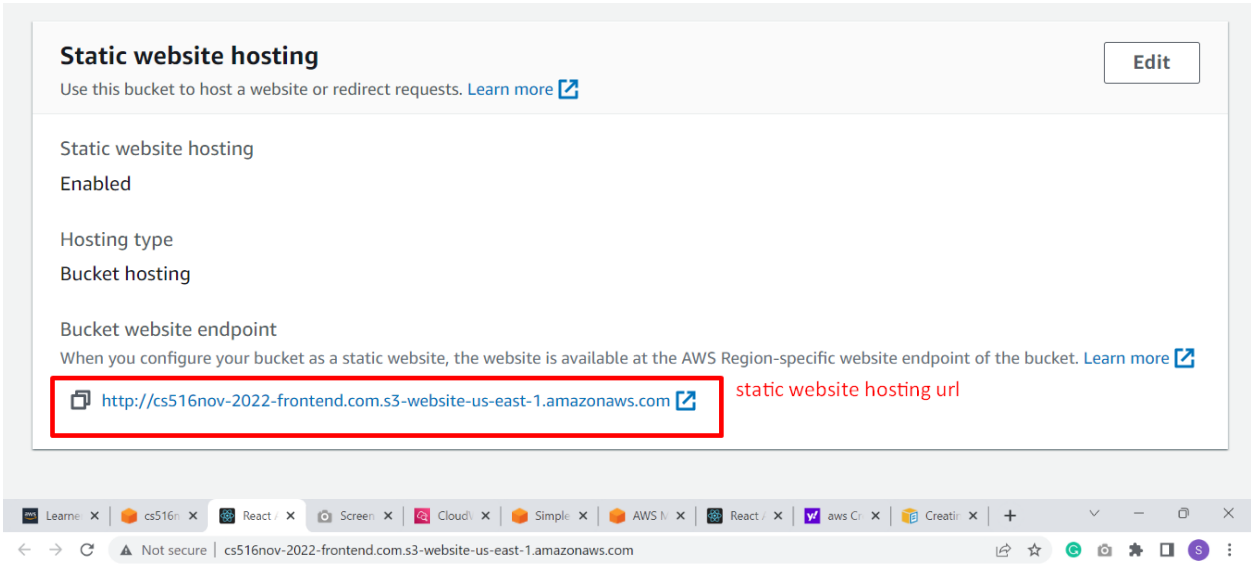
Then save changes.


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
AWS Marketplace for S3
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
{
"Version": "2012-10-17",
"Id": "Policy1650912821527",
"Statement": [
{
"Sid": "Stmt1650912820312",
"Effect": "Allow",
"Principal": "*",
"Action": "s3:GetObject",
"Resource": "arn:aws:s3:::cs516nov-2022-frontend.com/*"
}
]
}
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
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
voclabs/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 folders.
Files and folders (14 Total, 727.7 KB)
All files and folders in this table will be uploaded.
Remove
Add files
Add folder
Find by name
1 2
Name
Folder
Type
Size
787.36db6797.chunk.js
static/js/
text/javascript
4.5 KB
787.36db6797.chunk.js.map
static/js/
-
10.3 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
main.2dbd410b.js
static/js/
text/javascript
174.8 KB
main.2dbd410b.js.LICENSE.txt
static/js/
text/plain
1.1 KB
main.2dbd410b.js.map
static/js/
-
515.9 KB
folder
files
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
voclabs/user2243686=supriya @ 8468-6651-5154
Uploading
26%
Total remaining: 11 files: 538.0 KB(73.94%)
Estimated time remaining: a few seconds
Transfer rate: 13.9 KB/s
Cancel
Upload: status
Close
The information below will no longer be available after you navigate away from this page.
Summary
Destination
s3://cs516nov-2022-frontend.com
Succeeded
3 files, 189.6 KB (26.06%)
Failed
0 files, 0 B (0%)
Files and folders
Configuration
Files and folders (14 Total, 727.7 KB)
Find by name
1
2
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





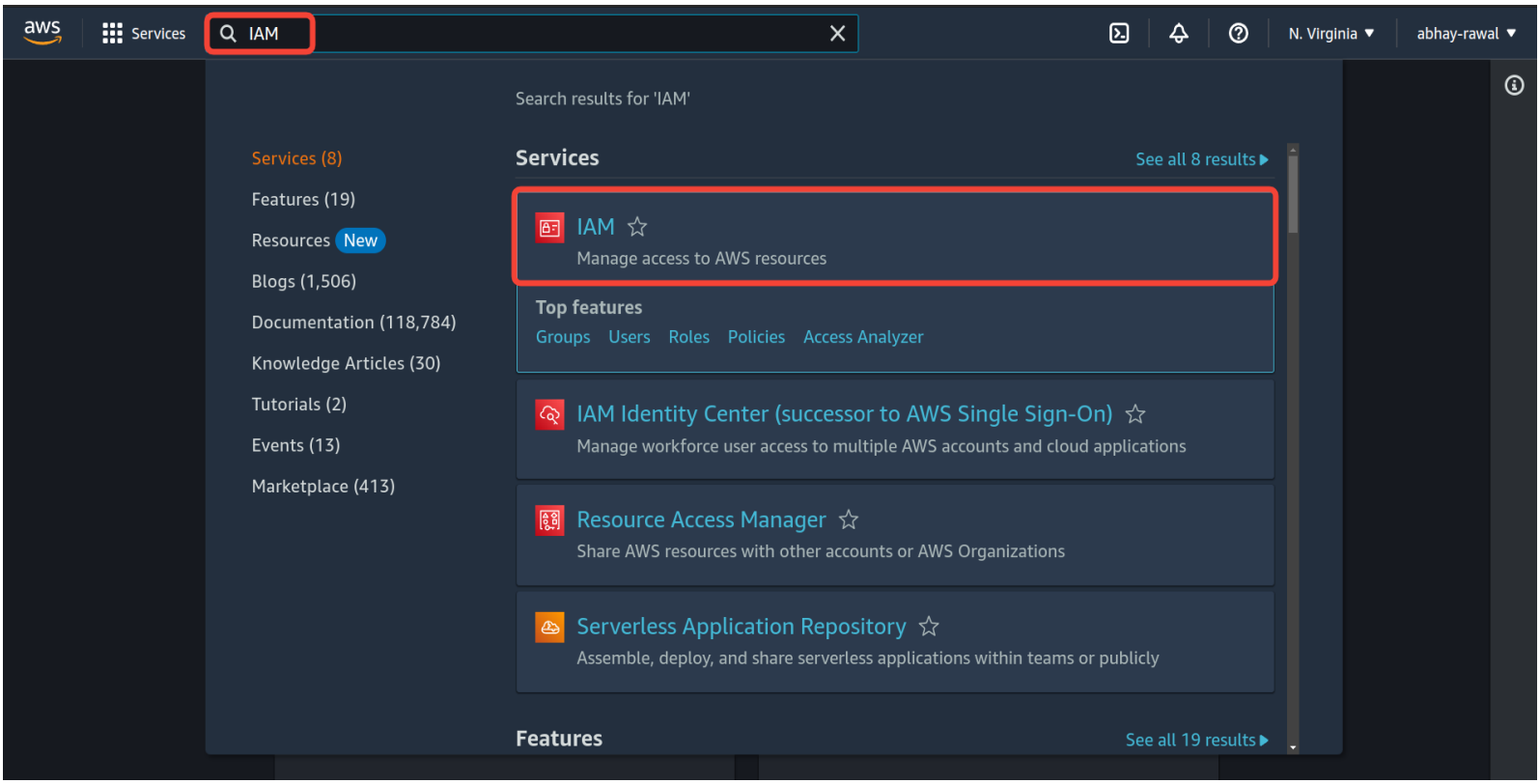
Cloud Computing course

1. Supriya Ghising
2. Anna
3. Simran

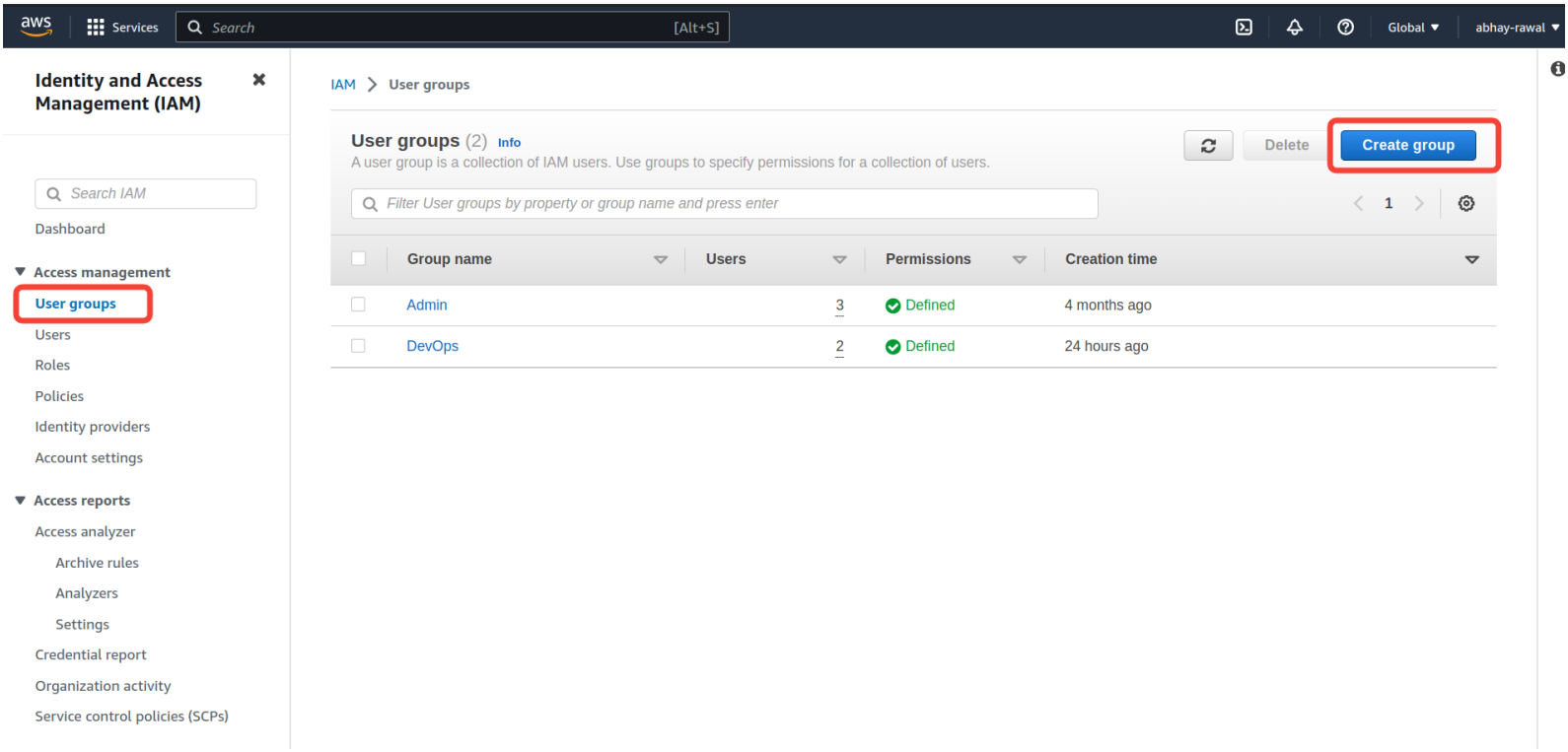
Creating an IAM user for yourself

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

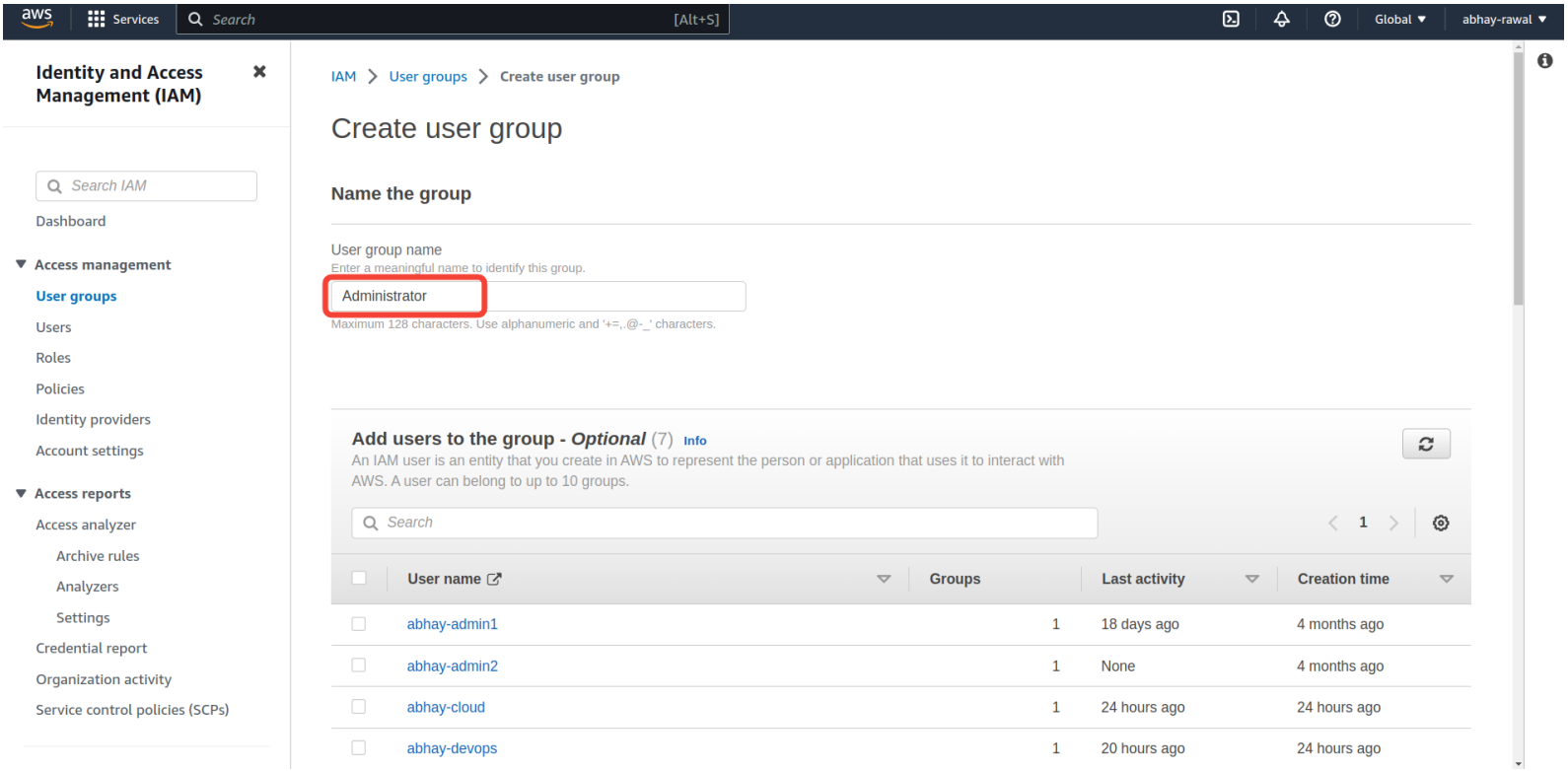
1. Sign into the AWS Management Console and open the IAM console



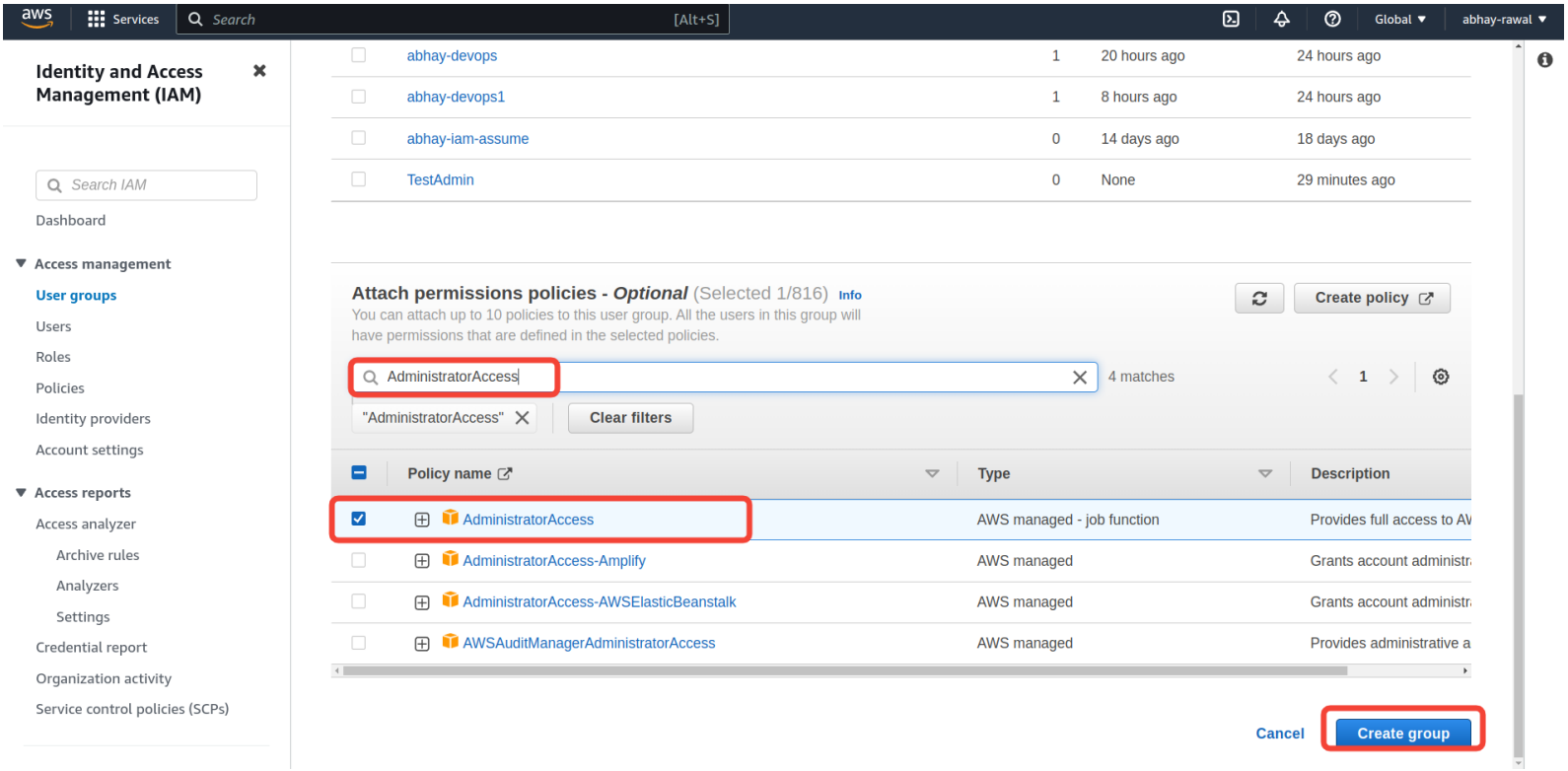
2. In the navigation pane, choose **User groups** and then choose **Create group.**



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

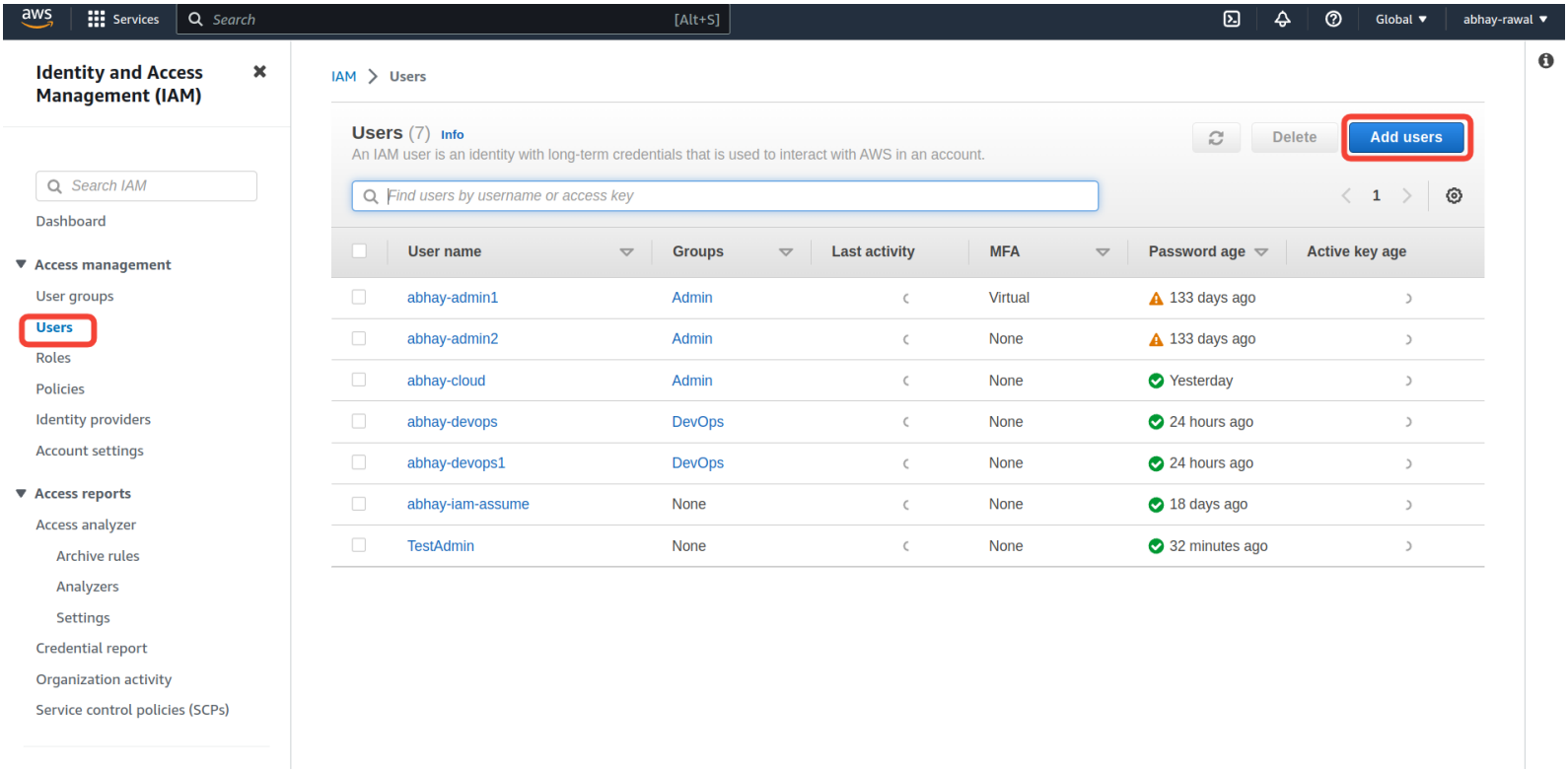


4. In the list of policies, search for A**dministratorAccess, select the check box to apply the policy to all group members**, and then Choose **Create group.**

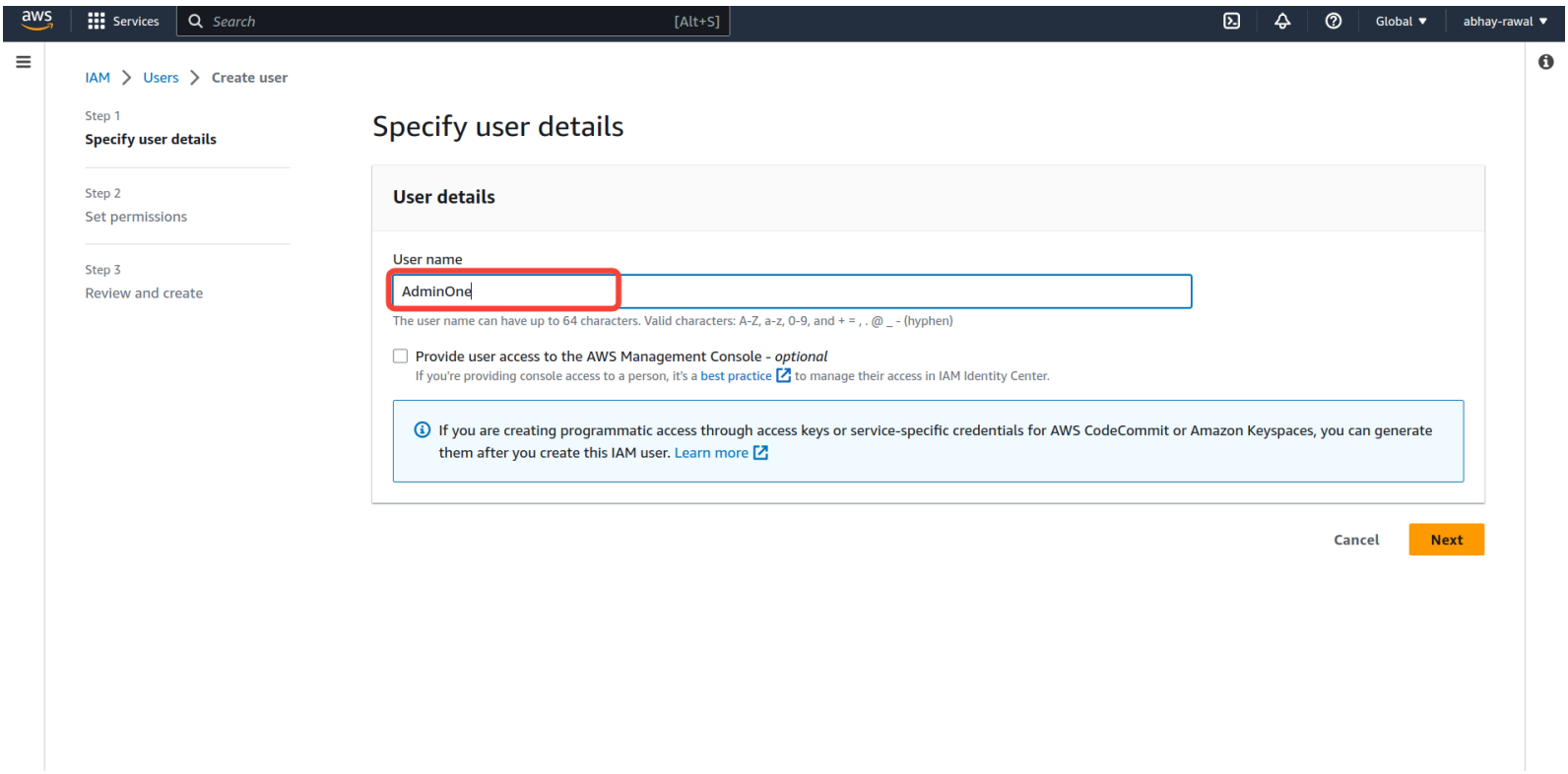


Creating IAM users and adding to a group

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



3. Type the username 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.



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.

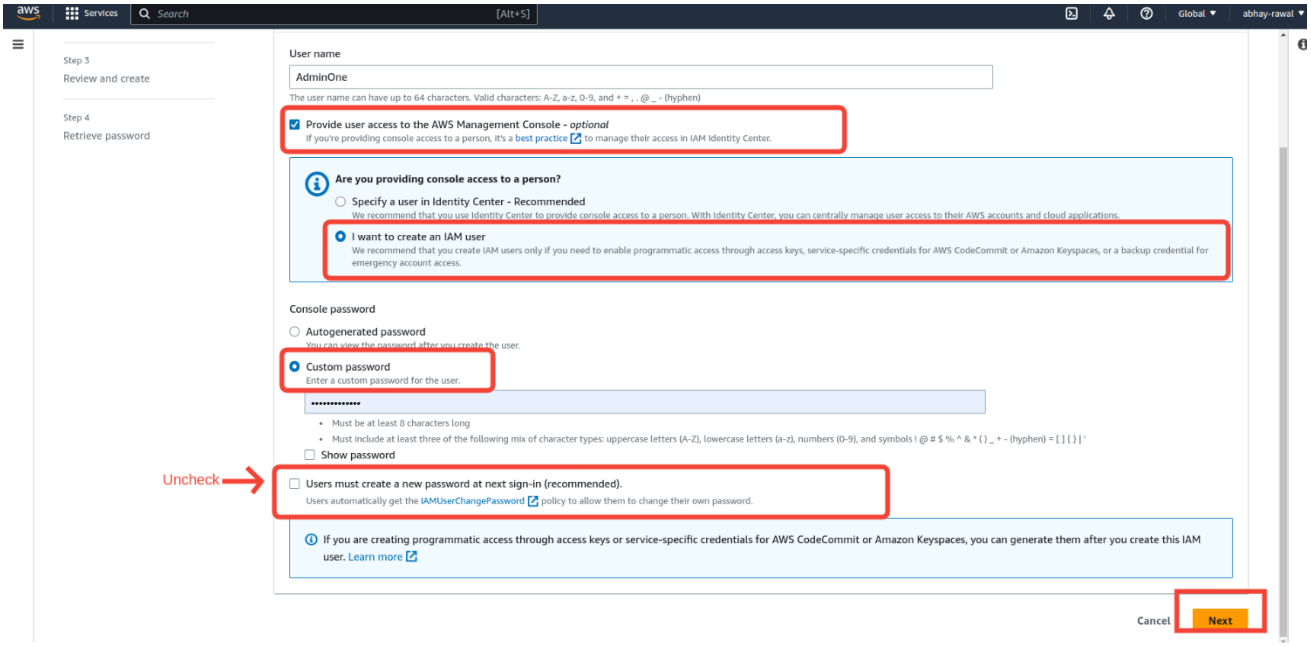
   a. Now we need to select if we want to Specify a user in Identity Center or Create an IAM user. **Choose "I want to create an IAM user".**

   - 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

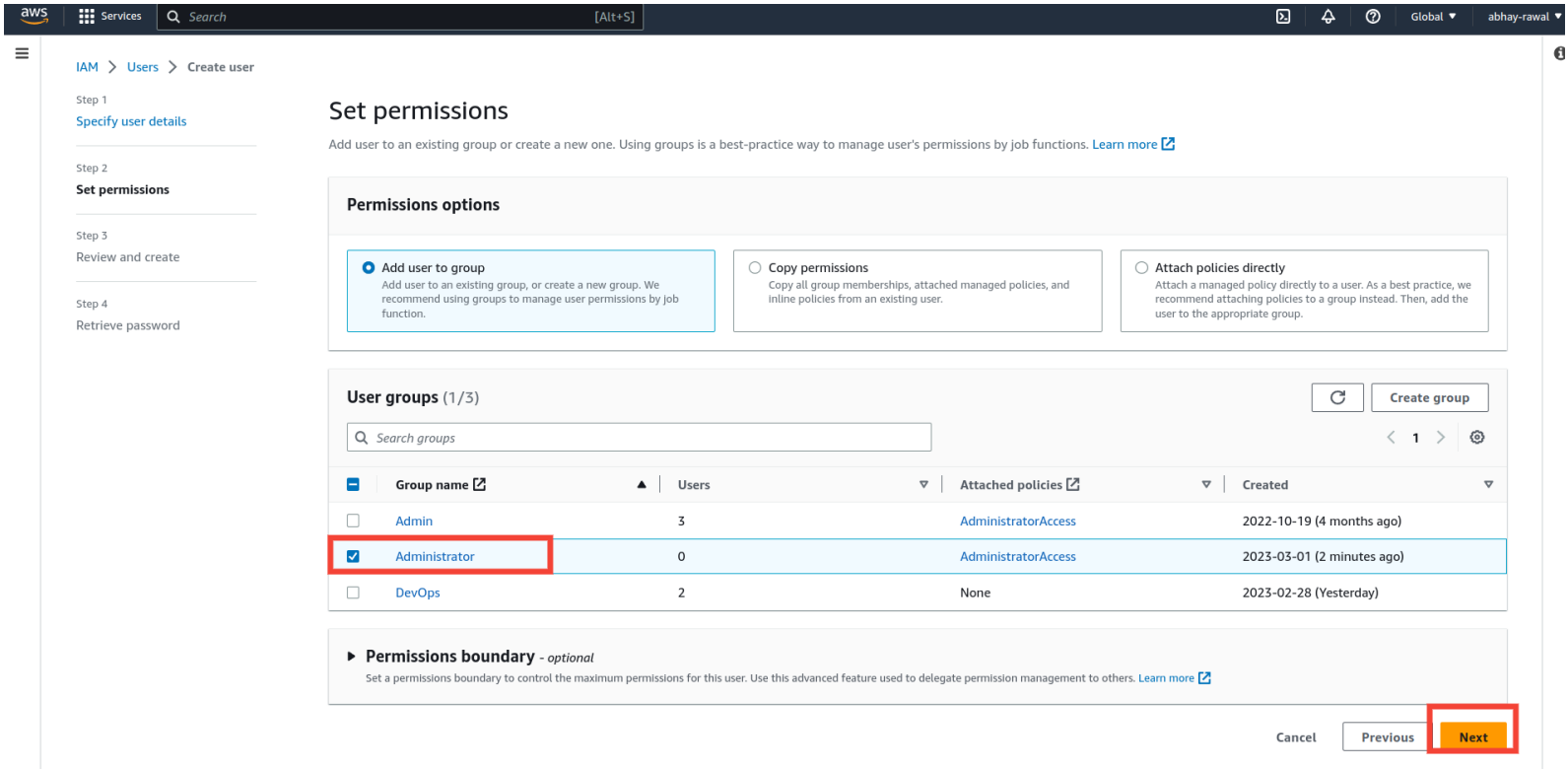
policy. You can view or download the passwords when you get to the **Final** page.

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

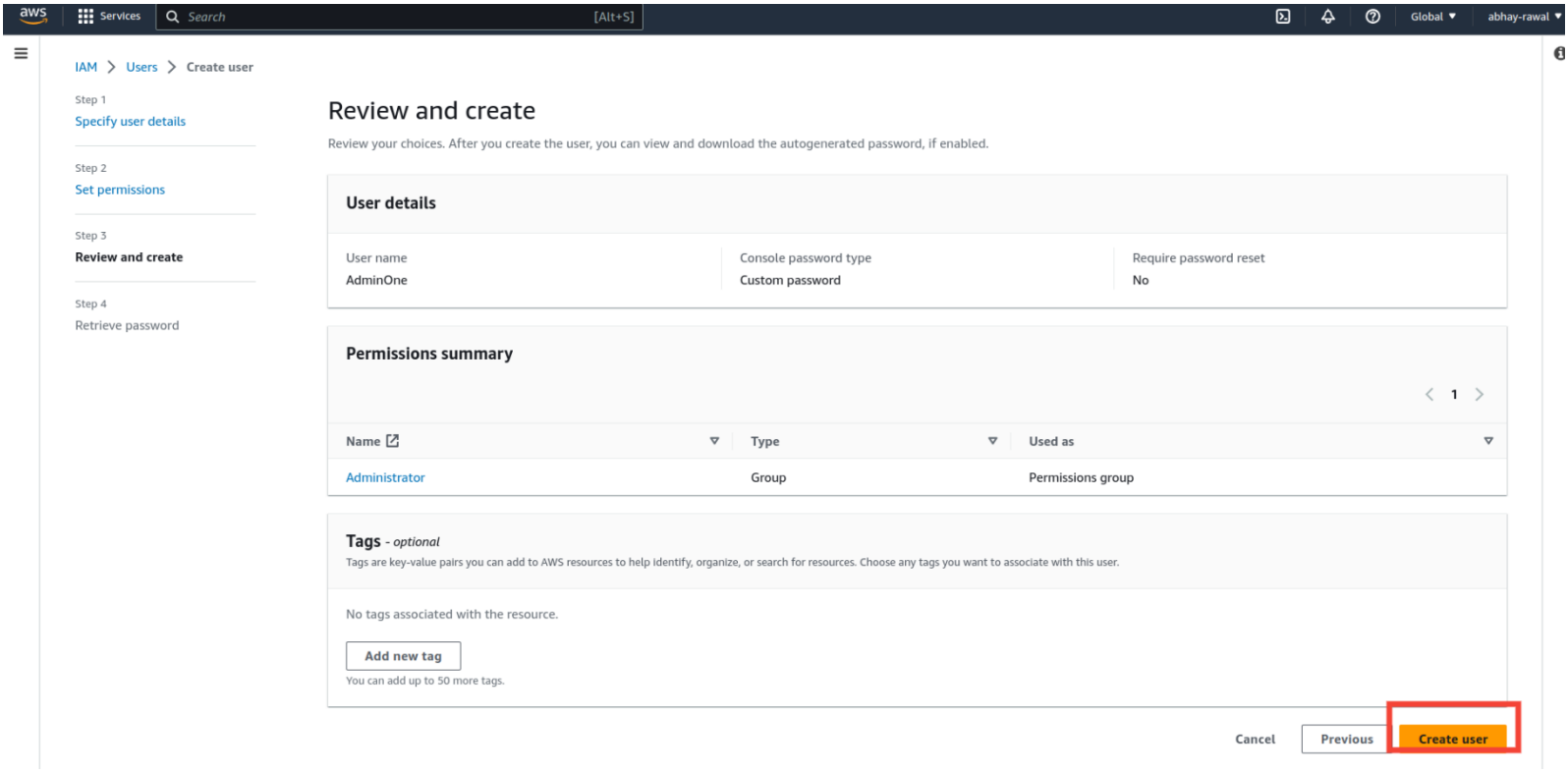
- For this demo uncheck **Users must create a new password at next sign-in.**
- Click Next



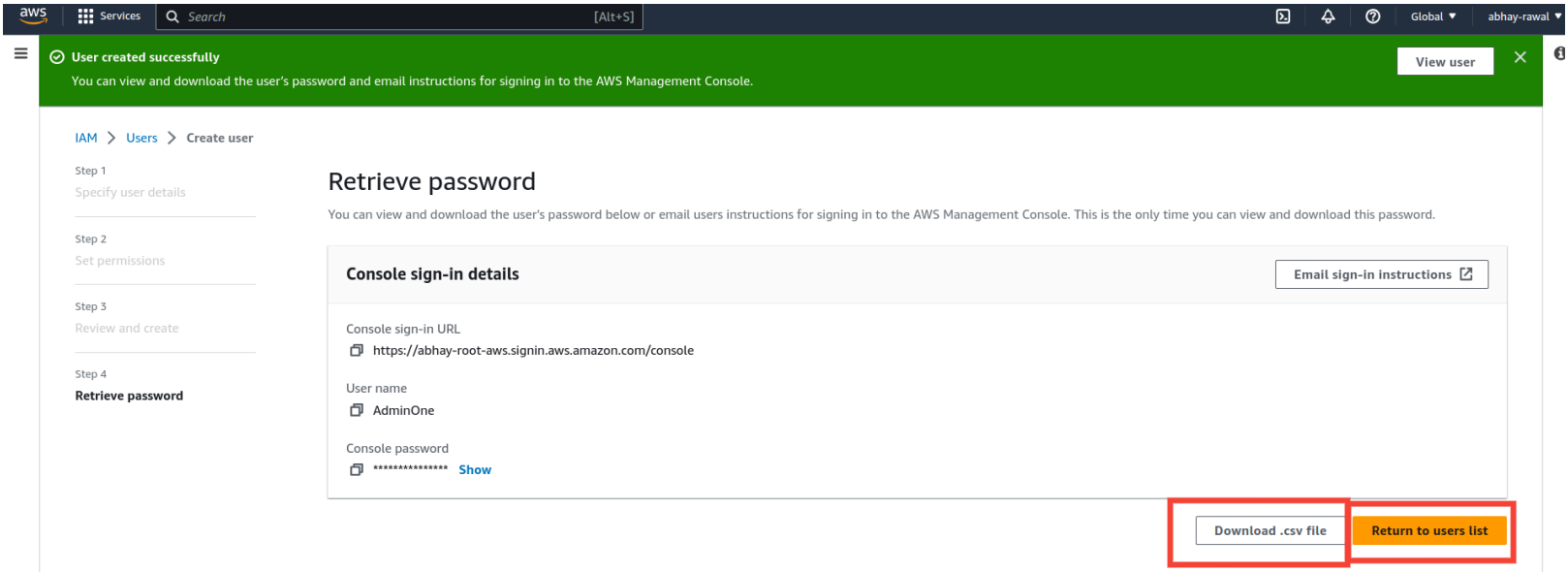
5. On the **Set permissions** page, **Add user to group**. You can select one or more existing groups.



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

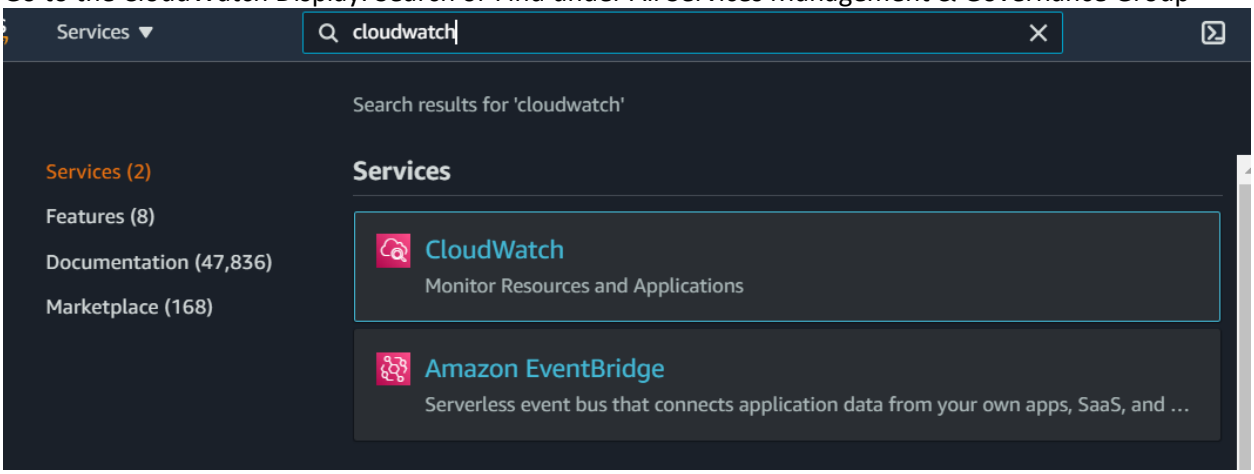


7. You will be then Redirected to Retrieve Password page. Click on Download .csv File to download credentials for the user. Then Click on Return to users list.

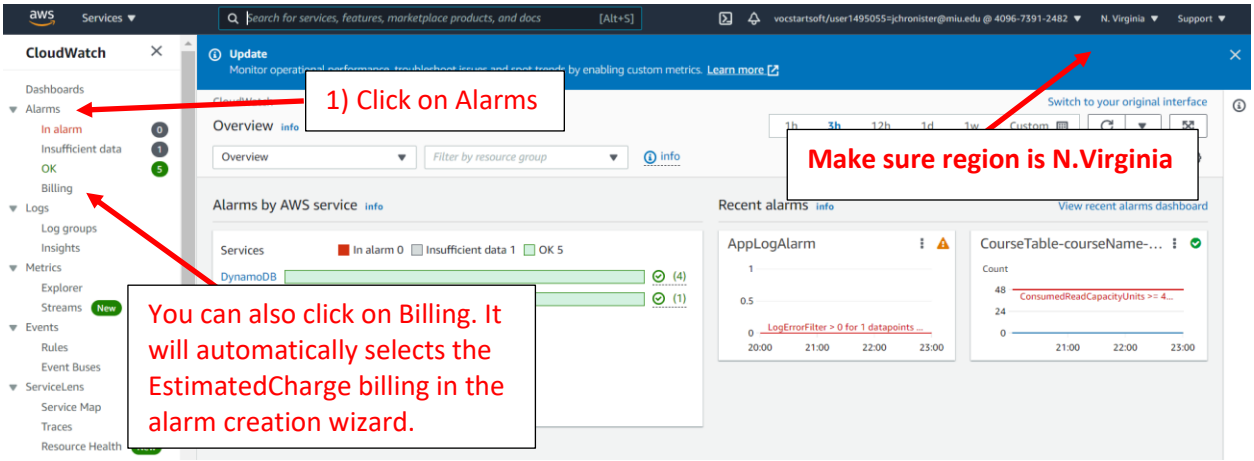


Setting up a billing alarm on CloudWatch

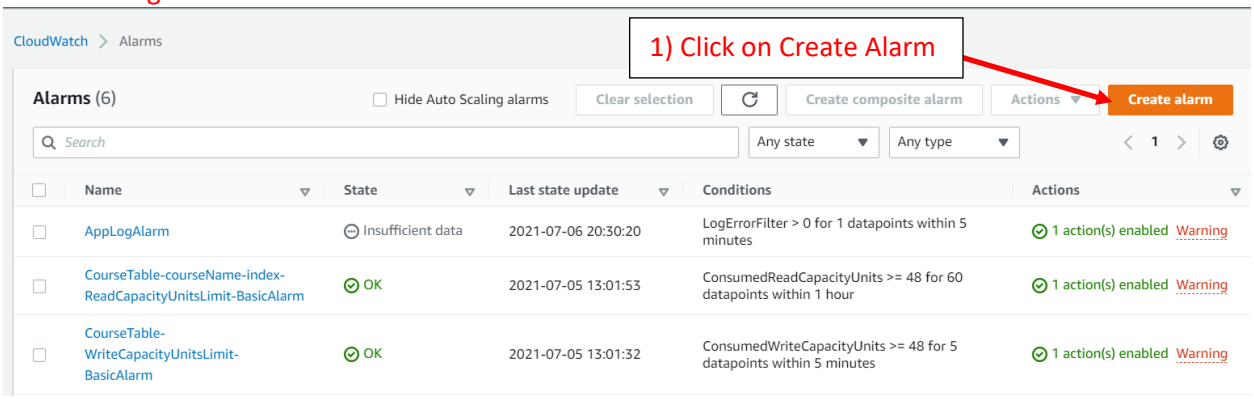
Go to the CloudWatch Display. Search or Find under All Services Management & Governance Group



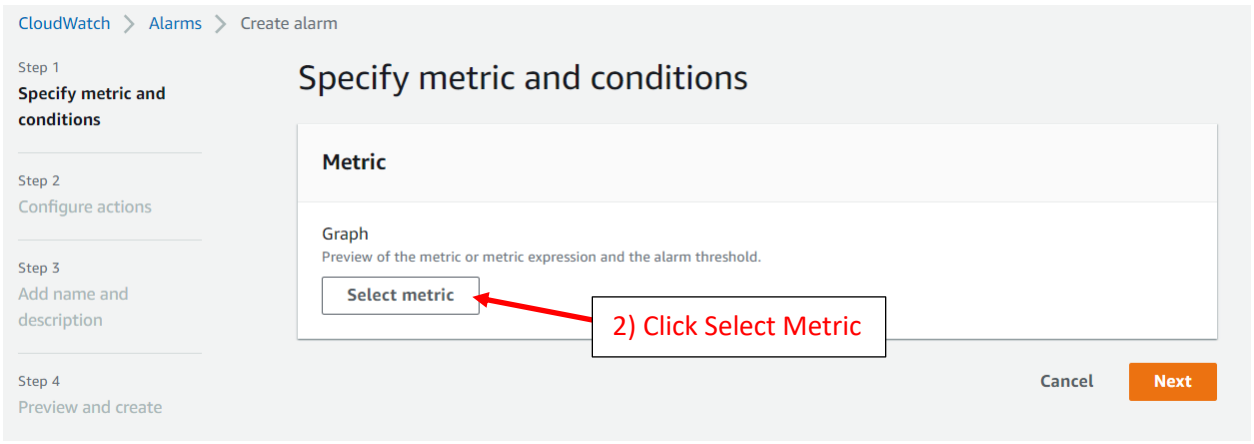
Go to the Alarms Display. You must select us-east-1 **N.Virginia** region. Otherwise, billing metric is not there.



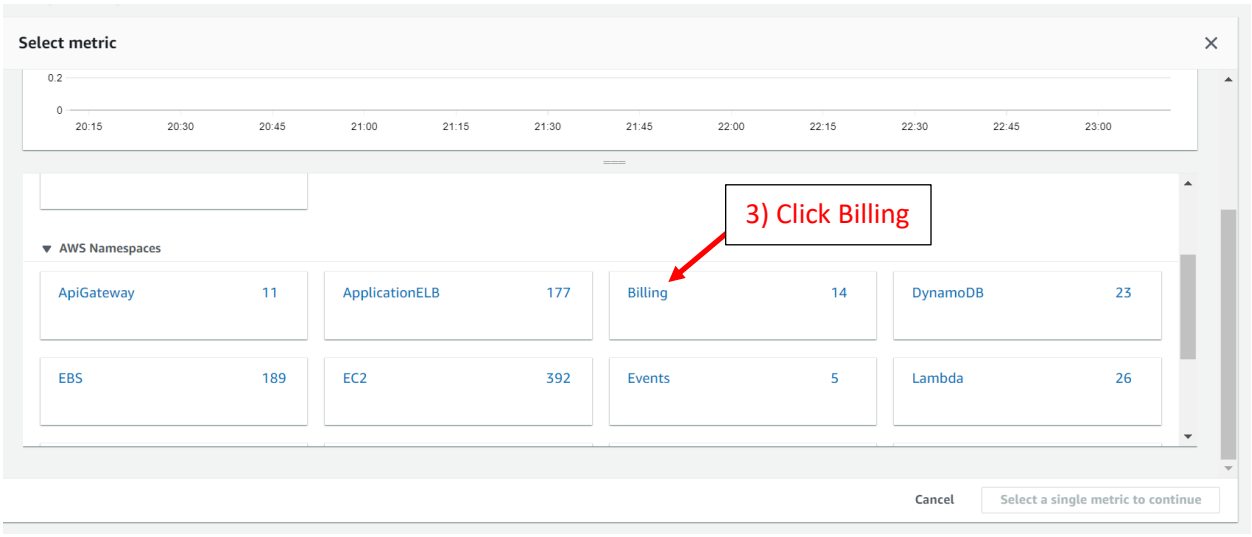
Create Billing Alarm



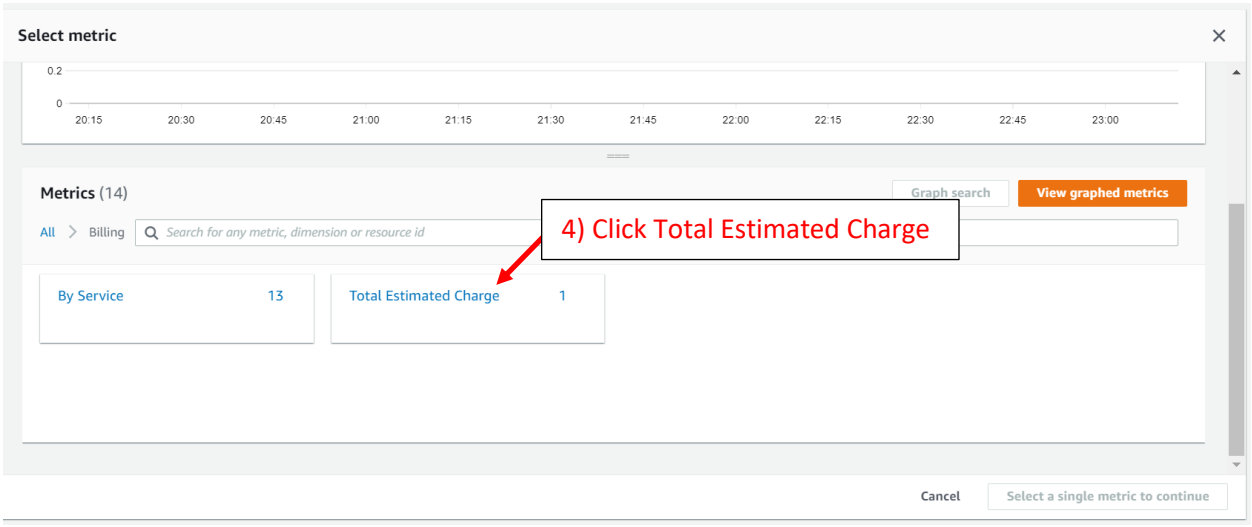
...



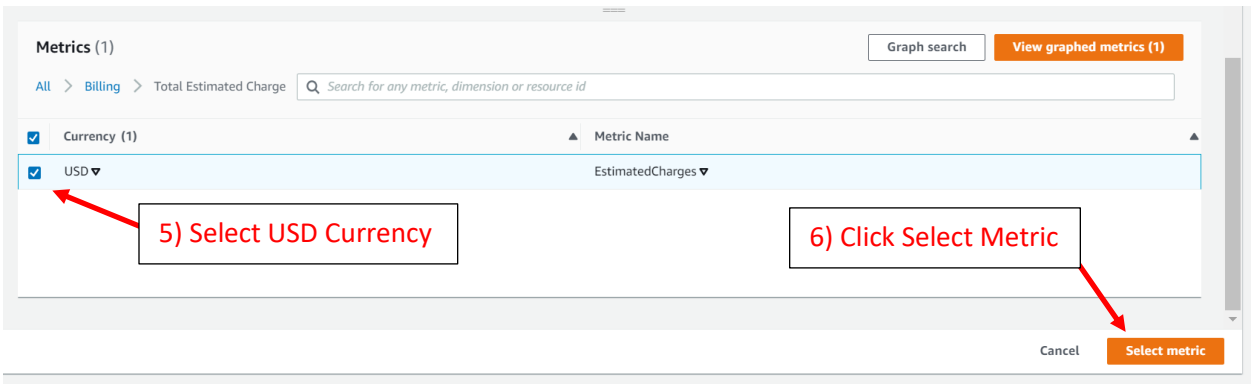
...

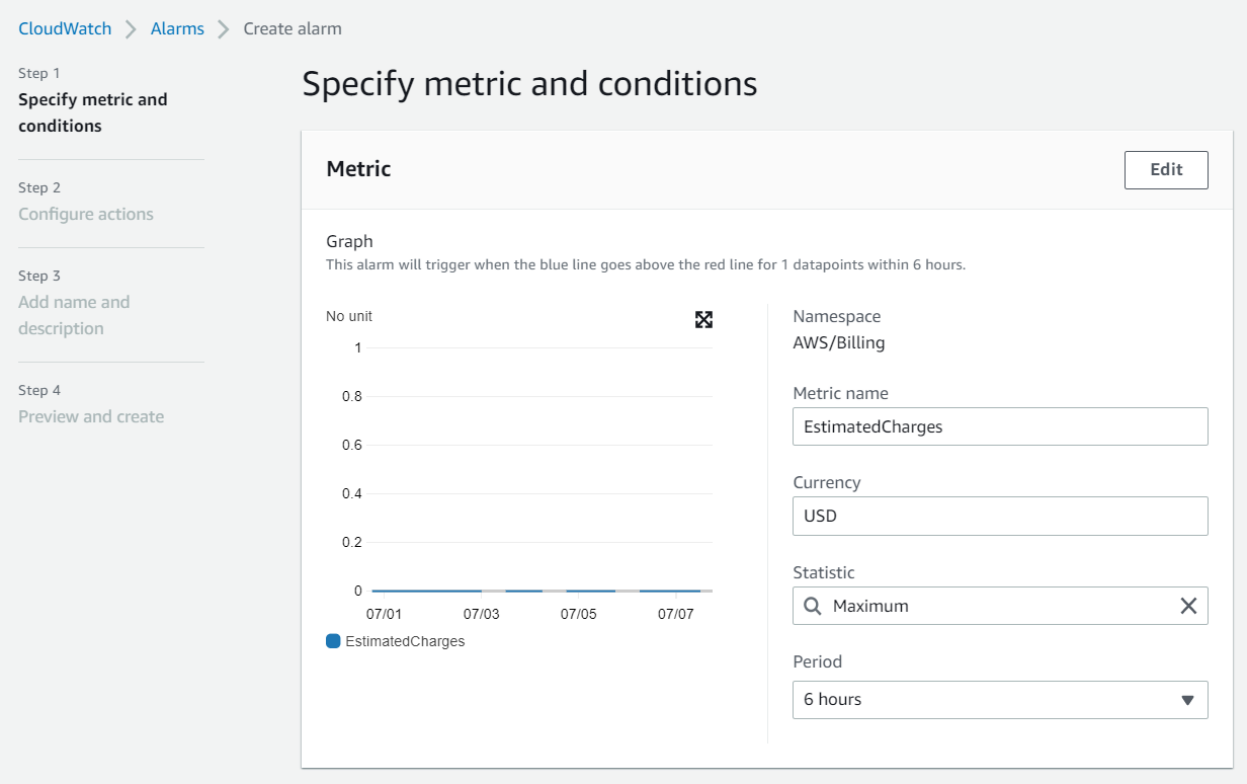

Select metric
0.2
0
20:15
20:30
20:45
21:00
21:15
21:30
21:45
22:00
22:15
22:30
22:45
23:00
3) Click Billing
AWS Namespaces
ApiGateway 11
ApplicationELB 177
Billing 14
DynamoDB 23
EBS 189
EC2 392
Events 5
Lambda 26
Cancel
Select a single metric to continue

...

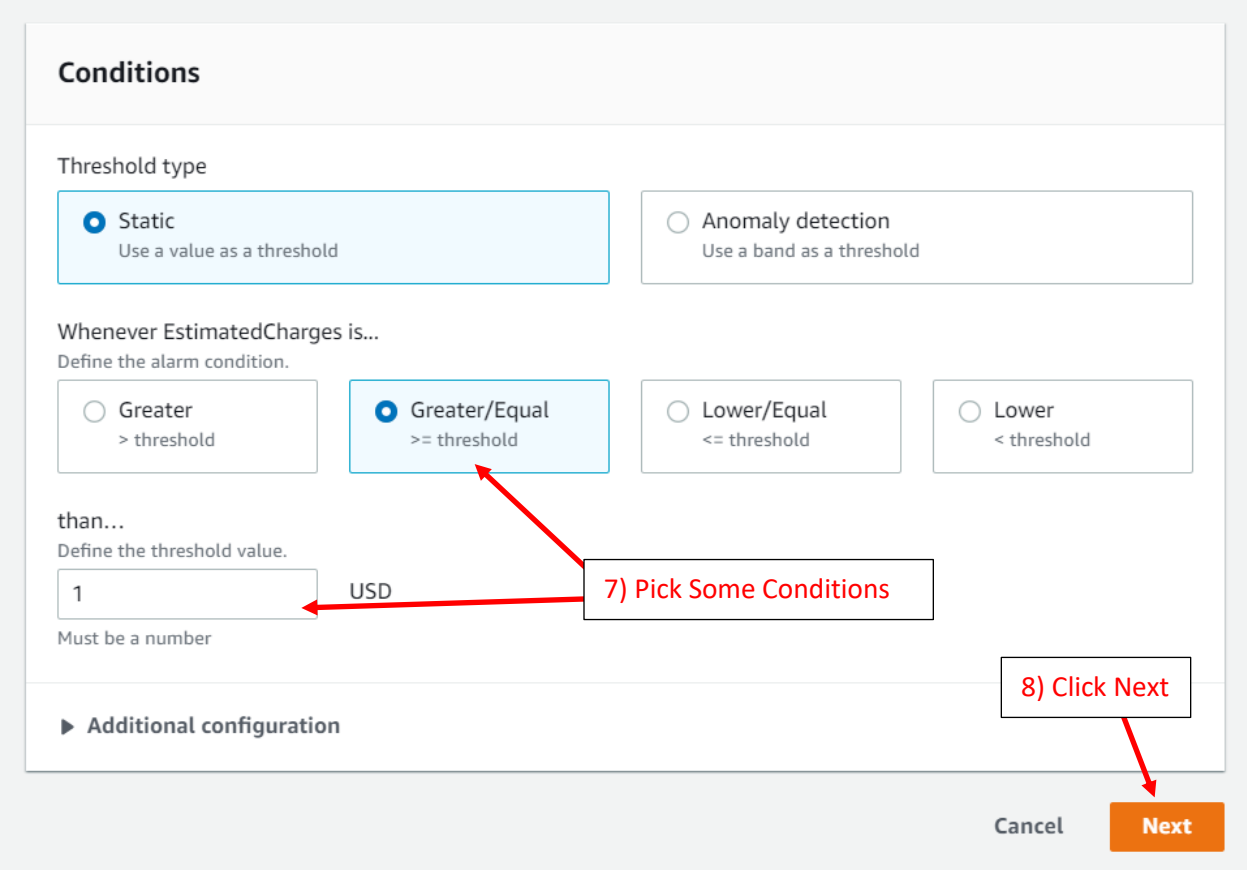

Select metric
0.2
0
20:15
20:30
20:45
21:00
21:15
21:30
21:45
22:00
22:15
22:30
22:45
23:00
Metrics (14)
Graph search
View graphed metrics
All
Billing
Search for any metric, dimension or resource id
4) Click Total Estimated Charge
By Service 13
Total Estimated Charge 1
Cancel
Select a single metric to continue

...

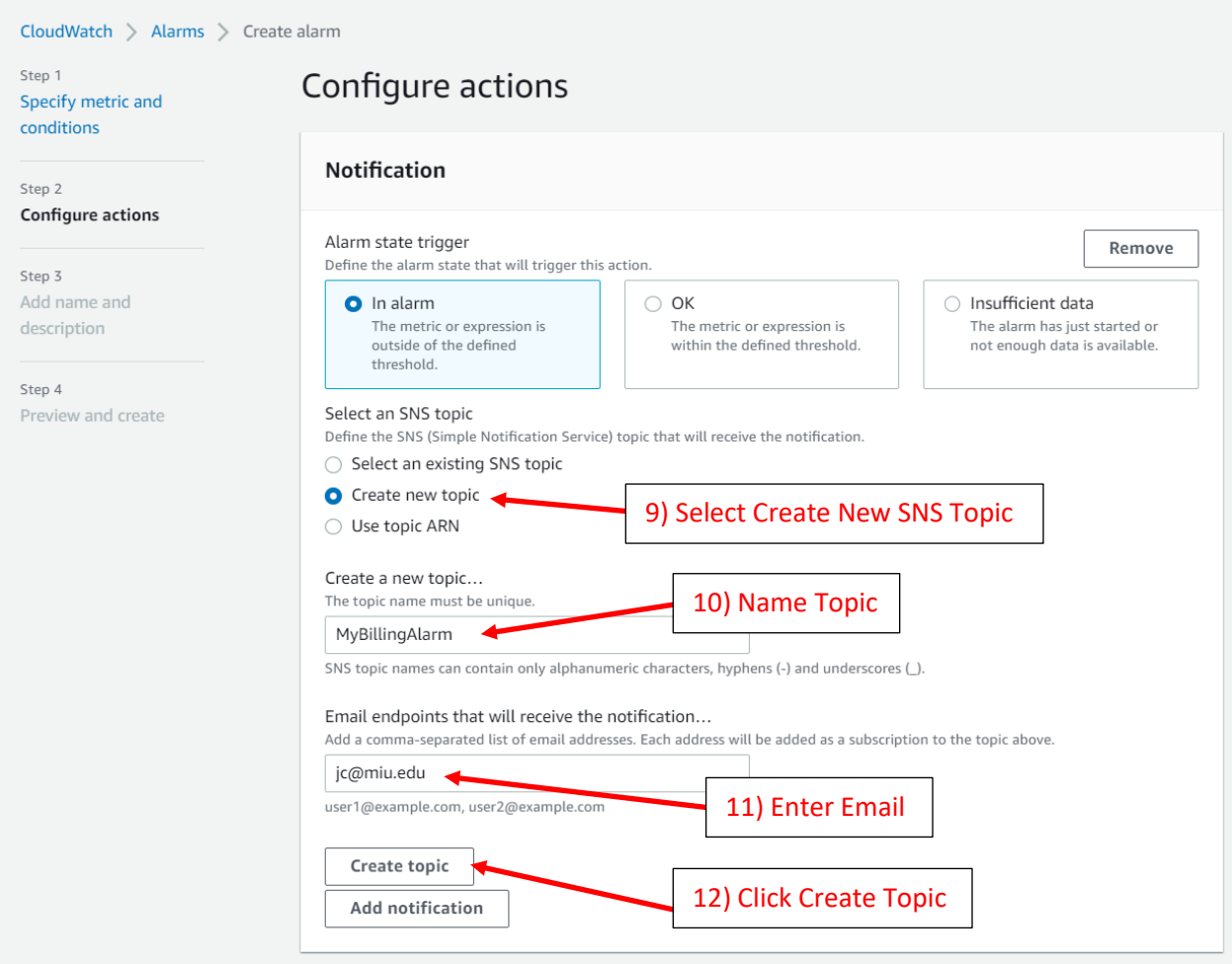

Metrics (1)
Graph search
View graphed metrics (1)
All
Billing
Total Estimated Charge
Search for any metric, dimension or resource id
Currency (1)
Metric Name
USD
EstimatedCharges
5) Select USD Currency
6) Click Select Metric
Cancel
Select metric


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

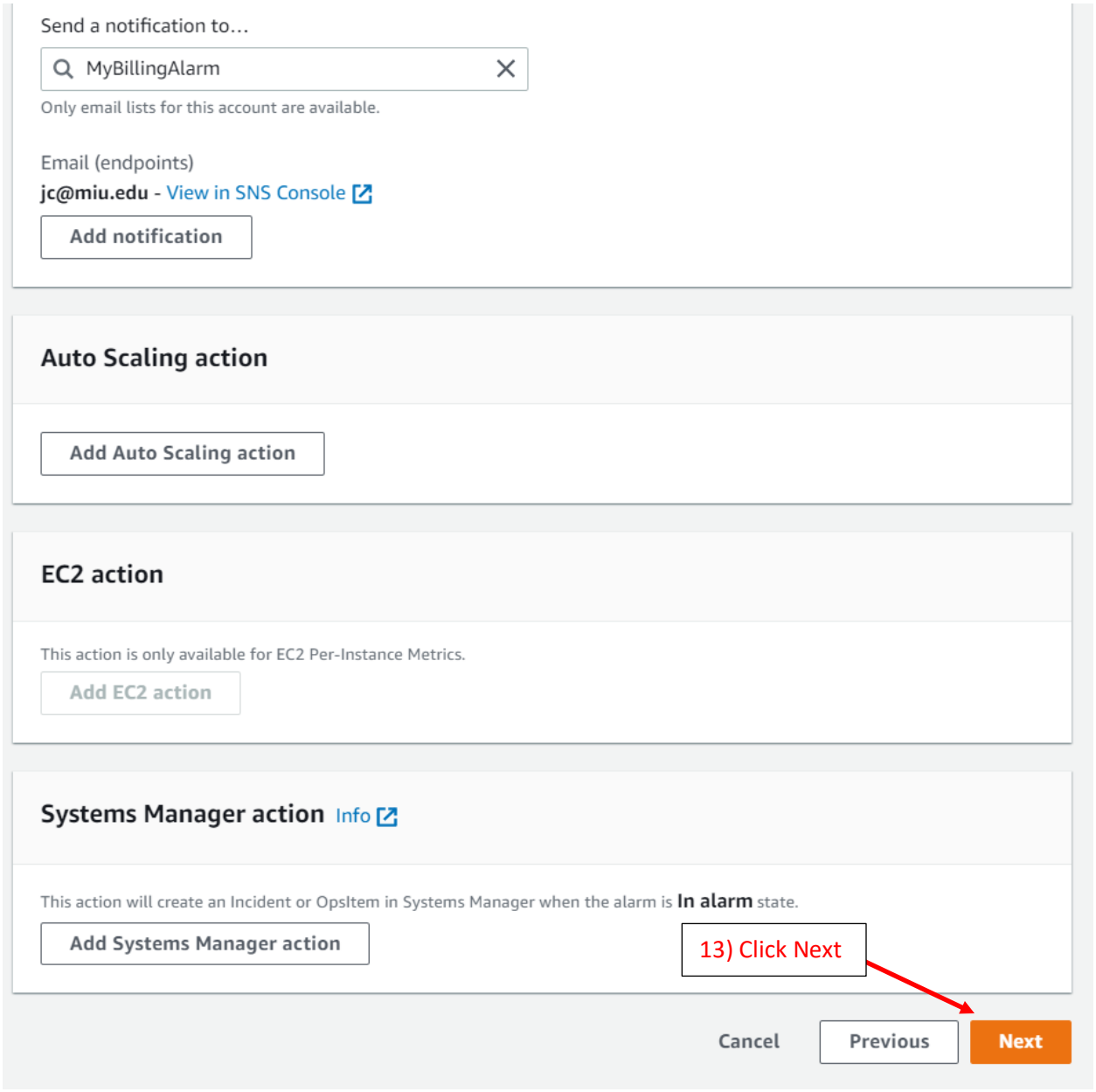
...


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

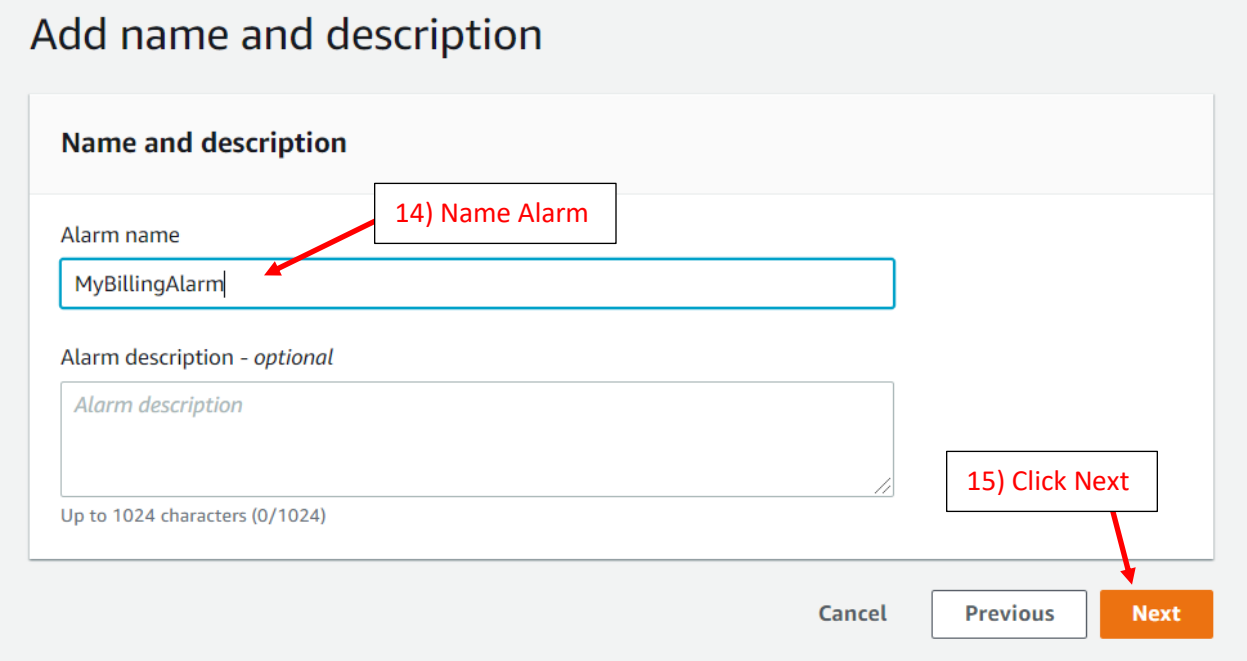
...


CloudWatch > Alarms > Create alarm
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.
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
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

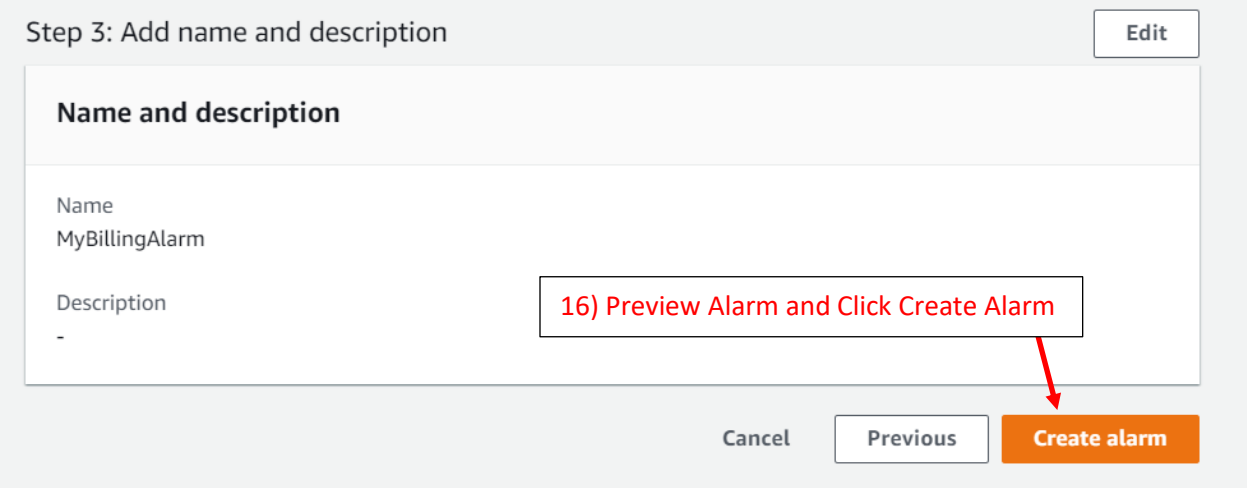
…


Send a notification to...
MyBillingAlarm
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

...

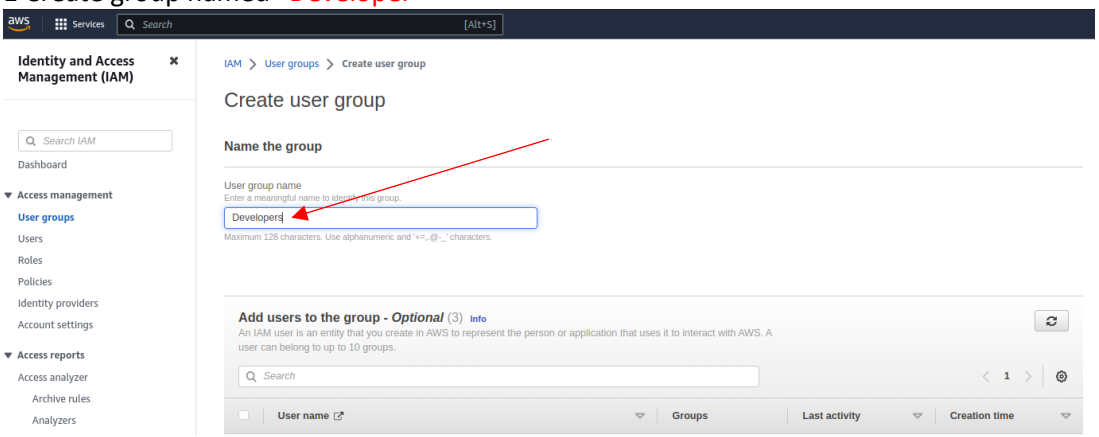

Add name and description
Name and description
14) Name Alarm
Alarm name
MyBillingAlarm
Alarm description - optional
Alarm description
Up to 1024 characters (0/1024)
15) Click Next
Cancel
Previous
Next

...


Step 3: Add name and description
Edit
Name and description
Name
MyBillingAlarm
Description
-
16) Preview Alarm and Click Create Alarm
Cancel
Previous
Create alarm

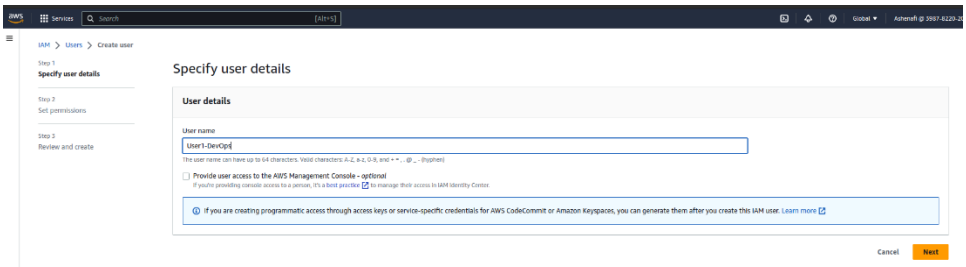
Practicing an IAM policy with a condition

1 Create group named “Developer”

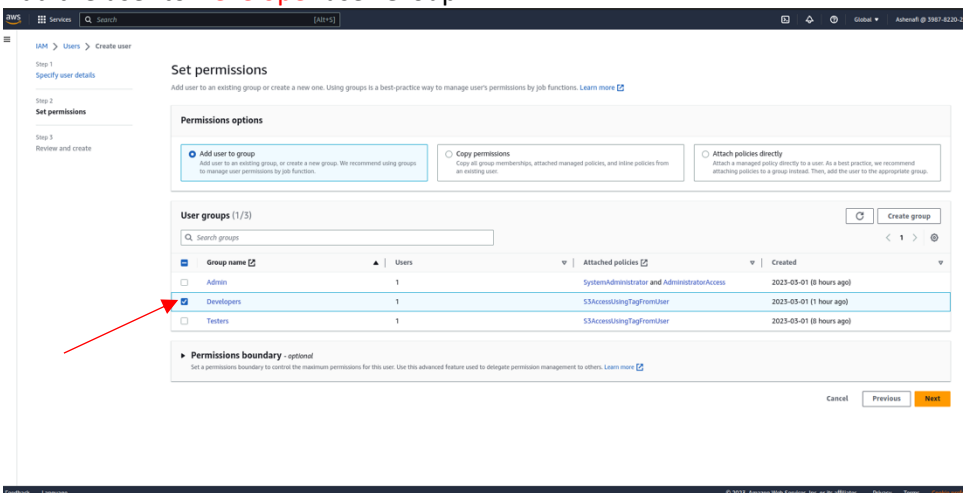


2 Create Two Users E.g

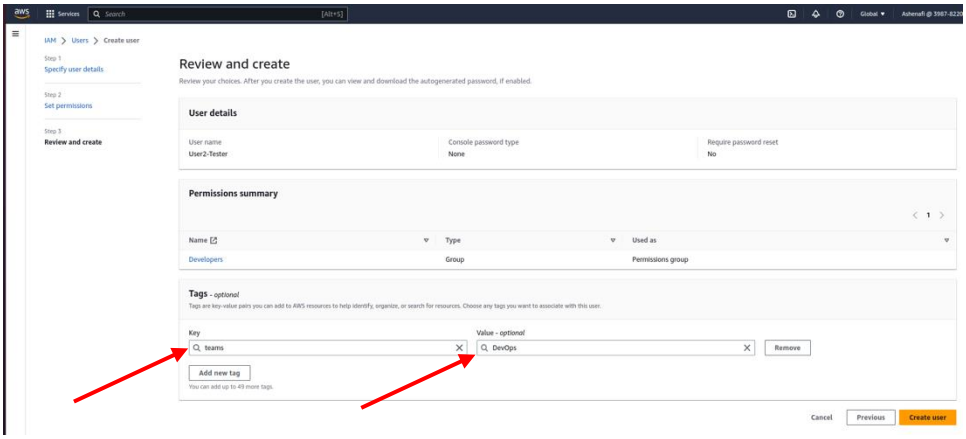
- User1-DevOps with Tag “teams” =”DevOps”



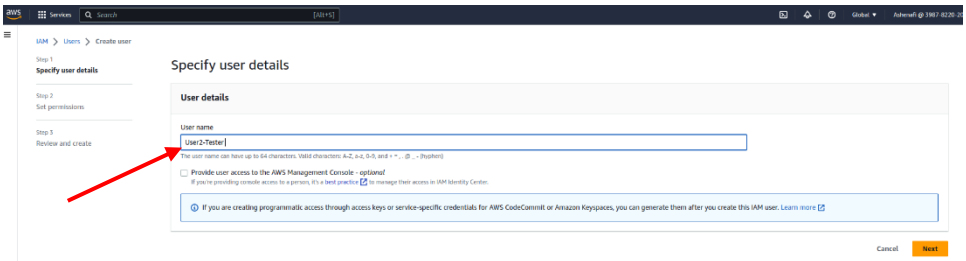
Add the user to Developer user Group



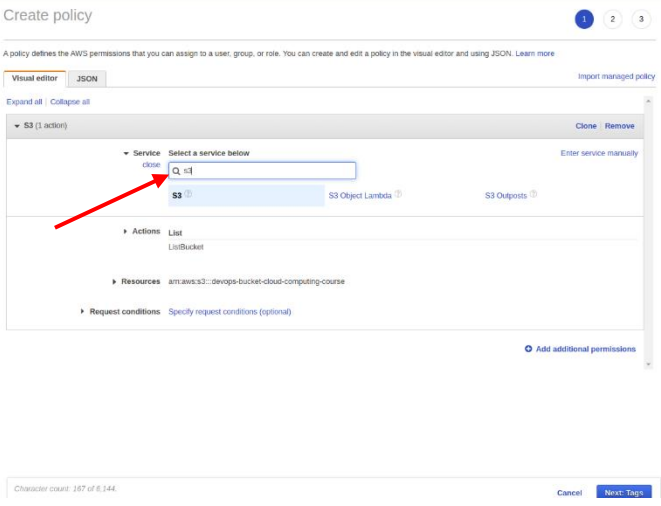
Add tag to user

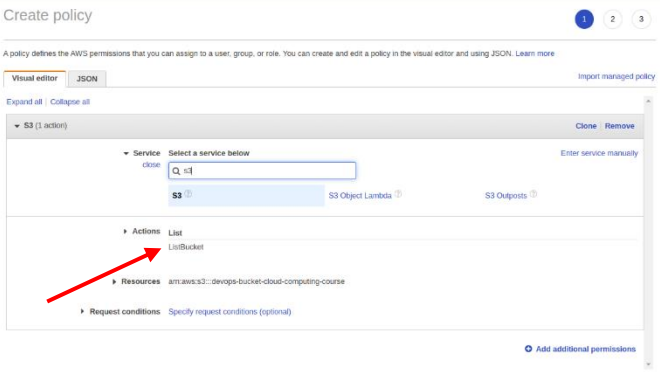


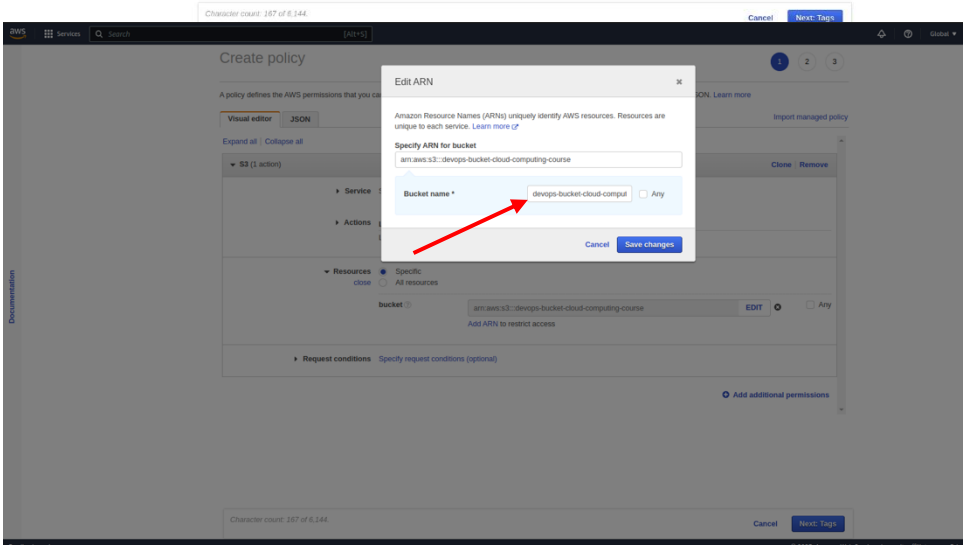
- User2-Tester

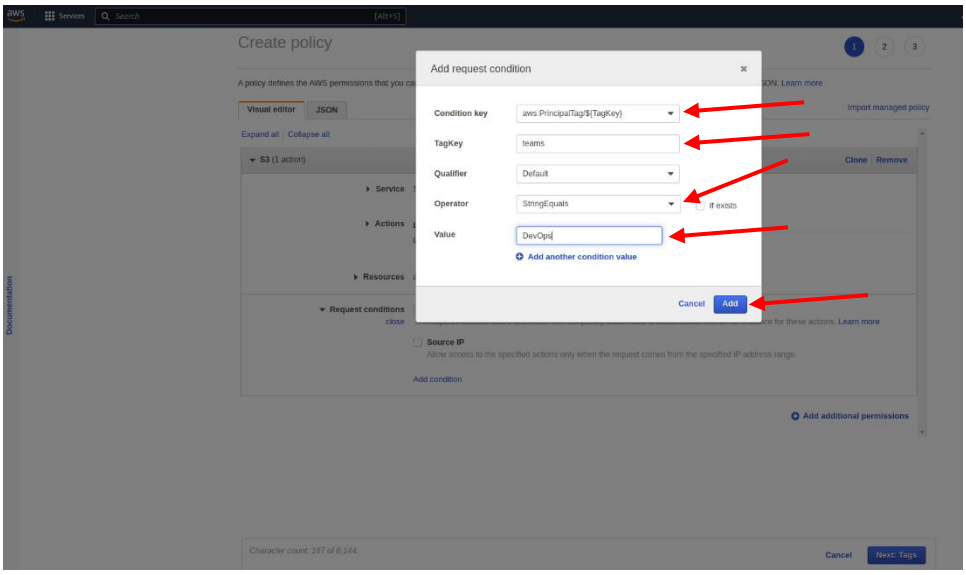


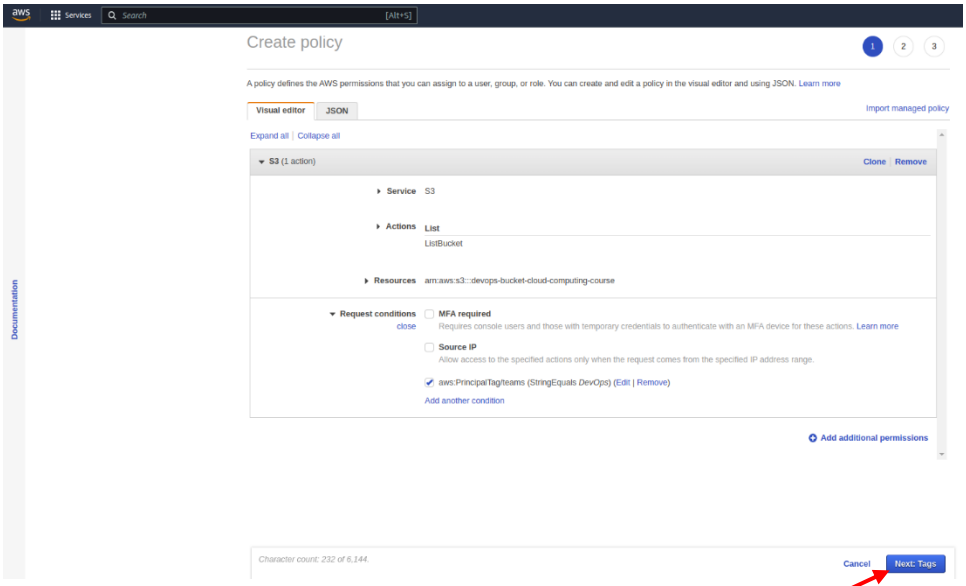
3 Create S3 Bucket
devops-bucket-cloud-computing-course
4 Put Object/file to the Bucket
file1.txt
5 Create a custom IAM policy with Condition {tag name= teams value=DevOps}

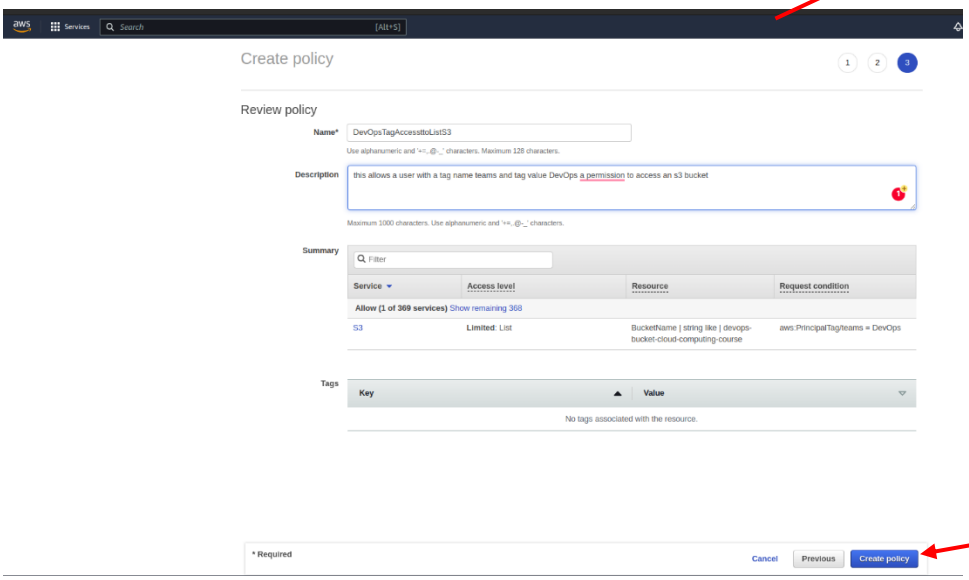



Create policy
A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. Learn more
Visual editor
JSON
Import managed policy
Expand all | Collapse all
S3 (1 action)
Clone | Remove
Service
Select a service below
Enter service manually
s3
S3
S3 Object Lambda
S3 Outposts
Actions
List
ListBucket
Resources
arn:aws:s3:::devops-bucket-cloud-computing-course
Request conditions
Specify request conditions (optional)
Add additional permissions

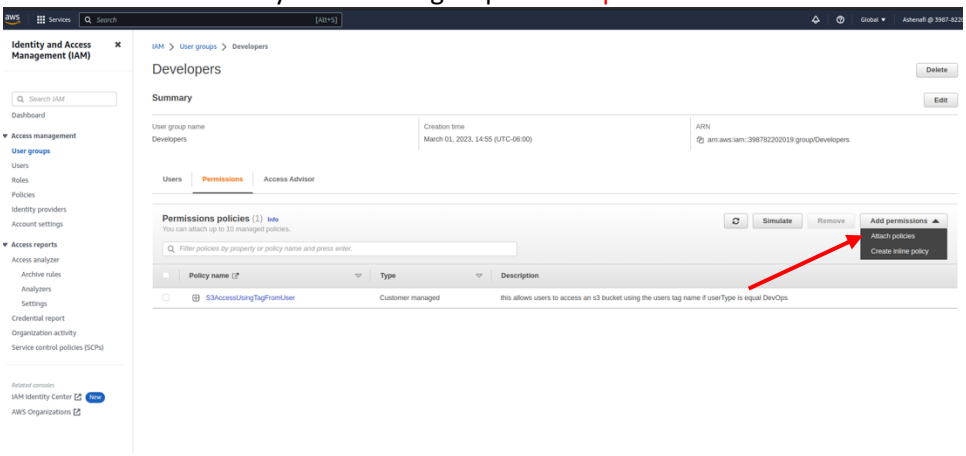

Edit ARN
Amazon Resource Names (ARNs) uniquely identify AWS resources. Resources are unique to each service. Learn more
Specify ARN for bucket
arn:aws:s3:::devops-bucket-cloud-computing-course
Bucket name *
devops-bucket-cloud-comput
Any
Cancel
Save changes
Create policy
Resources
Specific
All resources
bucket
arn:aws:s3:::devops-bucket-cloud-computing-course
EDIT
Any
Add ARN to restrict access
Request conditions
Specify request conditions (optional)
Add additional permissions
Cancel
Next: Tags

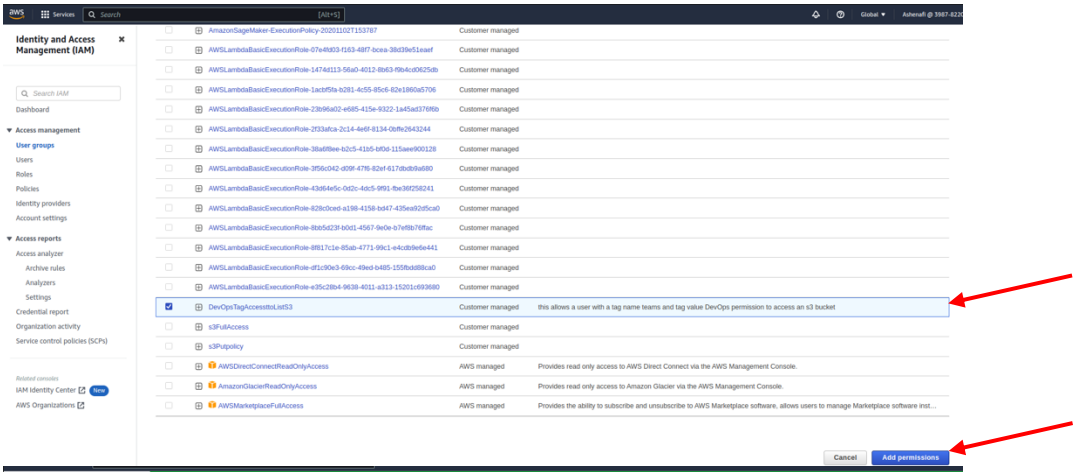

Add request condition
Condition key
aws:PrincipalTag/${TagKey}
TagKey
teams
Qualifier
Default
Operator
StringEquals
If exists
Value
DevOps
Add another condition value
Cancel
Add
Create policy
Request conditions
Source IP
Add condition
Add additional permissions
Cancel
Next: Tags

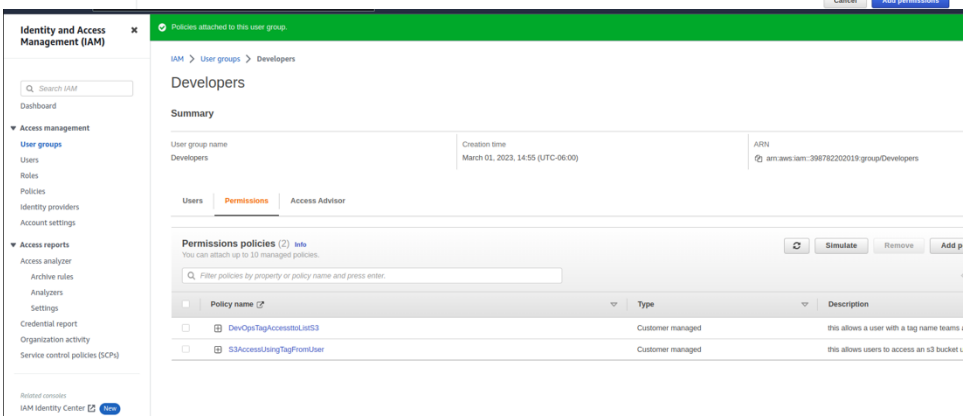




Attach the create Policy to the user group “Developers”

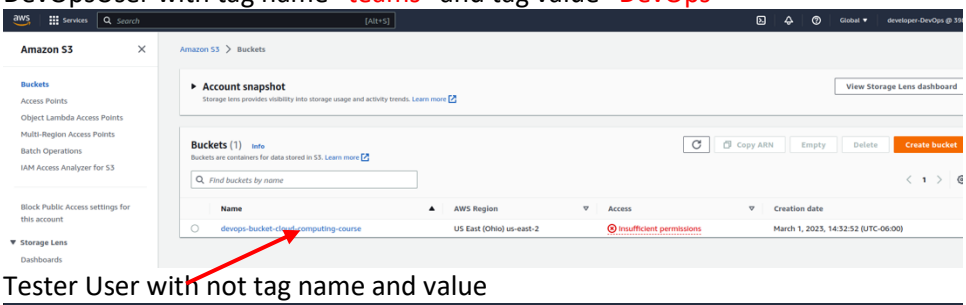






6 Test

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



Tester User with not tag name and value