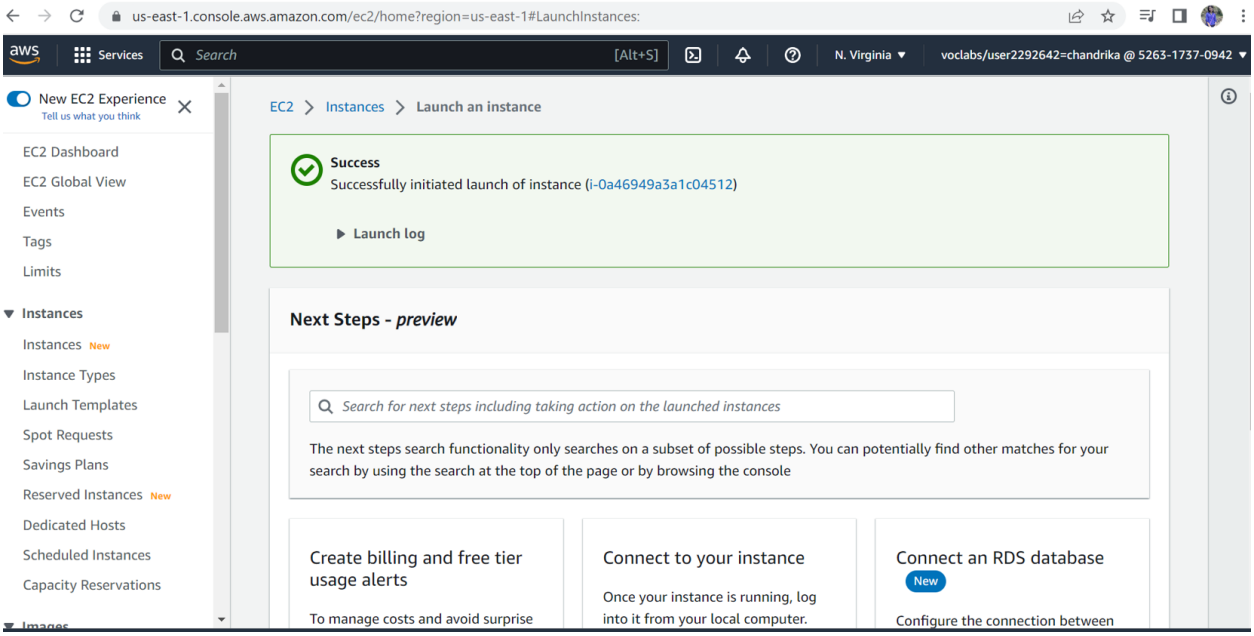
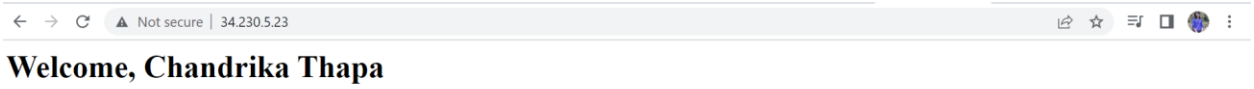
Day 1st Assignment Lab

```
sh-4.2$ sudo s
sudo: s: command not found
sh-4.2$ sudo -s
[root@ip-172-31-30-251 bin]# yum install httpd -y
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
Resolving Dependencies
--> Running transaction check
---> Package httpd.x86_64 0:2.4.54-1.amzn2 will be installed
--> Processing Dependency: httpd-tools = 2.4.54-1.amzn2 for package: httpd-2.4.54-1.amzn2.x86_64
--> Processing Dependency: httpd-filesystem = 2.4.54-1.amzn2 for package: httpd-2.4.54-1.amzn2.x86_64
--> Processing Dependency: system-logos-httpd for package: httpd-2.4.54-1.amzn2.x86_64
--> Processing Dependency: mod_http2 for package: httpd-2.4.54-1.amzn2.x86_64
--> Processing Dependency: httpd-filesystem for package: httpd-2.4.54-1.amzn2.x86_64
--> Processing Dependency: /etc/mime.types for package: httpd-2.4.54-1.amzn2.x86_64
--> Processing Dependency: libaprutil-1.so.0()(64bit) for package: httpd-2.4.54-1.amzn2.x86_64
--> Processing Dependency: libapr-1.so.0()(64bit) for package: httpd-2.4.54-1.amzn2.x86_64
--> Running transaction check
---> Package apr.x86_64 0:1.7.0-9.amzn2 will be installed
---> Package apr-util.x86_64 0:1.6.1-5.amzn2.0.2 will be installed
--> Processing Dependency: apr-util-bdb(x86-64) = 1.6.1-5.amzn2.0.2 for package: apr-util-1.6.1-5.amzn2.0.2.x86_64
---> Package generic-logos-httpd.noarch 0:18.0.0-4.amzn2 will be installed
---> Package httpd-filesystem.noarch 0:2.4.54-1.amzn2 will be installed
---> Package httpd-tools.x86_64 0:2.4.54-1.amzn2 will be installed
---> Package mailcap.noarch 0:2.1.41-2.amzn2 will be installed
---> Package mod_http2.x86_64 0:1.15.19-1.amzn2.0.1 will be installed
--> Running transaction check
---> Package apr-util-bdb.x86_64 0:1.6.1-5.amzn2.0.2 will be installed
--> Finished Dependency Resolution

Dependencies Resolved
```

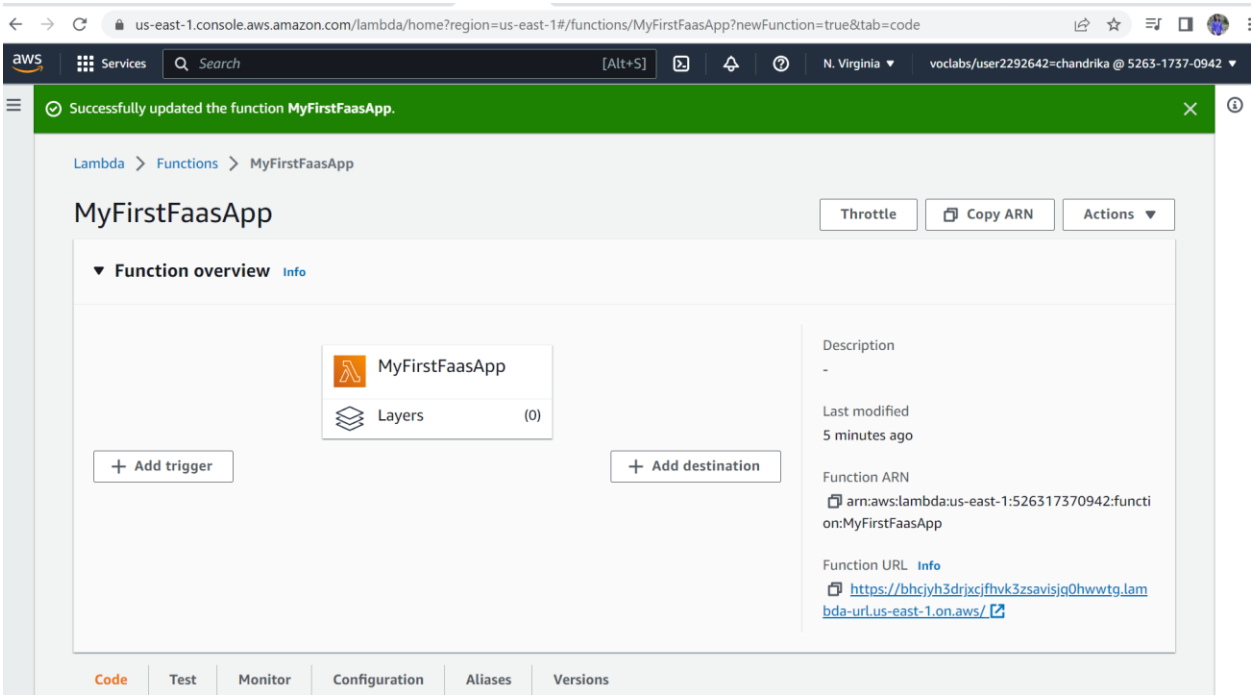
```
  Installing : httpd-tools-2.4.54-1.amzn2.x86_64
  Installing : httpd-filesystem-2.4.54-1.amzn2.noarch
  Installing : generic-logos-httpd-18.0.0-4.amzn2.noarch
  Installing : mailcap-2.1.41-2.amzn2.noarch
  Installing : mod_http2-1.15.19-1.amzn2.0.1.x86_64
  Installing : httpd-2.4.54-1.amzn2.x86_64
  Verifying  : apr-util-1.6.1-5.amzn2.0.2.x86_64
  Verifying  : apr-util-bdb-1.6.1-5.amzn2.0.2.x86_64
  Verifying  : httpd-tools-2.4.54-1.amzn2.x86_64
  Verifying  : mod_http2-1.15.19-1.amzn2.0.1.x86_64
  Verifying  : httpd-2.4.54-1.amzn2.x86_64
  Verifying  : mailcap-2.1.41-2.amzn2.noarch
  Verifying  : generic-logos-httpd-18.0.0-4.amzn2.noarch
  Verifying  : httpd-filesystem-2.4.54-1.amzn2.noarch
  Verifying  : apr-1.7.0-9.amzn2.x86_64

Installed:
  httpd.x86_64 0:2.4.54-1.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 0:2.4.54-1.amzn2     httpd-tools.x86_64 0:2.4.54-1.amzn2
  mailcap.noarch 0:2.1.41-2.amzn2               mod_http2.x86_64 0:1.15.19-1.amzn2.0.1

Complete!
[root@ip-172-31-30-251 bin]# service httpd start
Redirecting to /bin/systemctl start httpd.service
[root@ip-172-31-30-251 bin]# cd /var/www/html
[root@ip-172-31-30-251 html]# nano index.html
[root@ip-172-31-30-251 html]# nano index.html
[root@ip-172-31-30-251 html]#
[root@ip-172-31-30-251 html]#
```

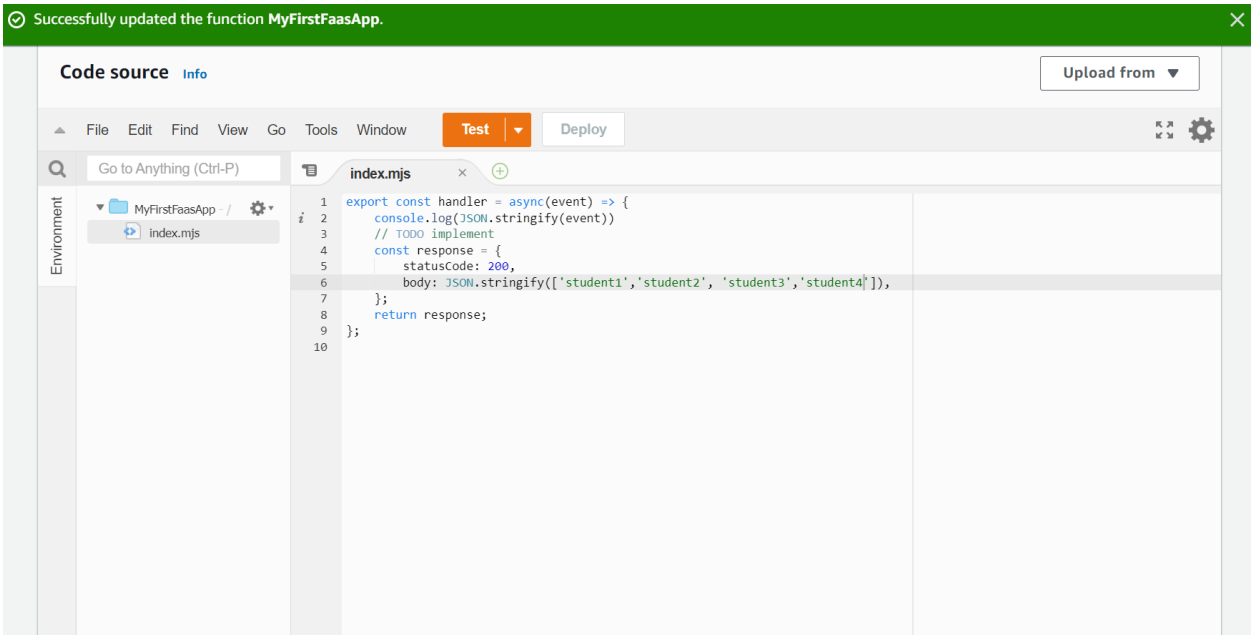
Creating EC2 instance(IAAS)





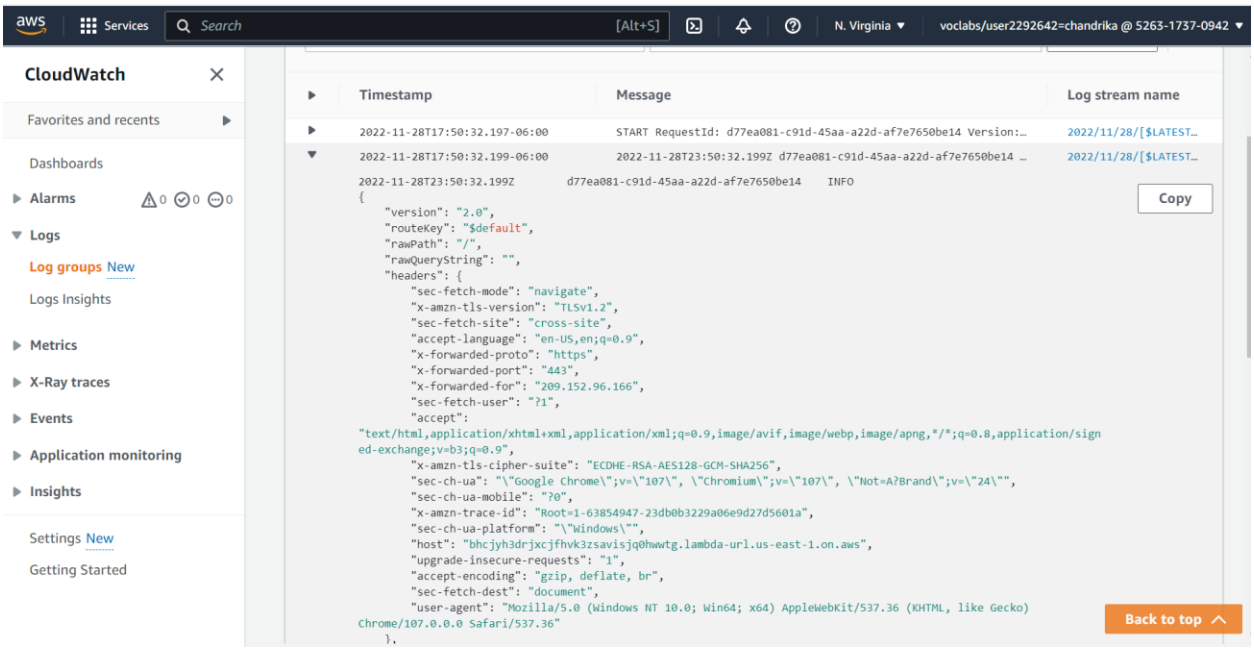
Creating Lambda (FAAS)



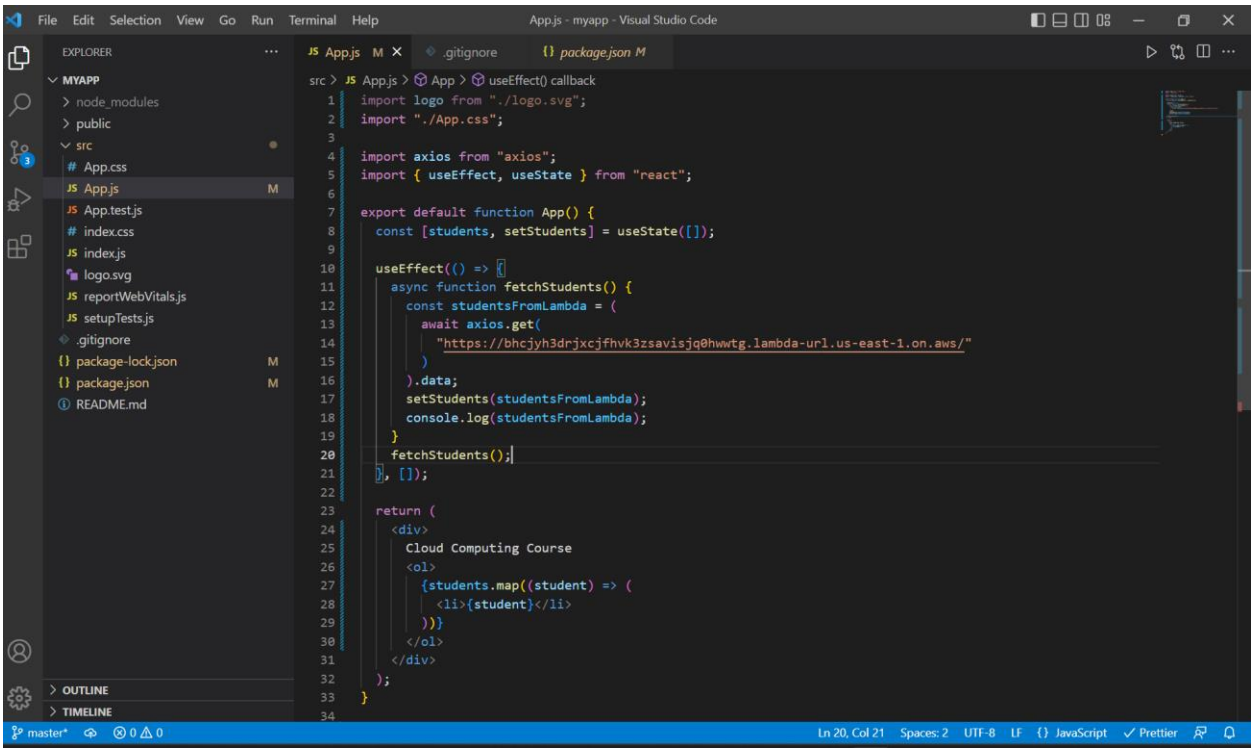


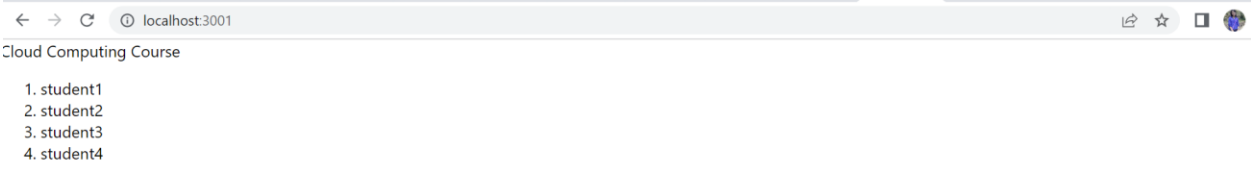
bhcjyh3drjxcjfhvk3zsavisjq0hwwtg.lambda-url.us-east-1.on.aws

["student1","student2","student3","student4"]

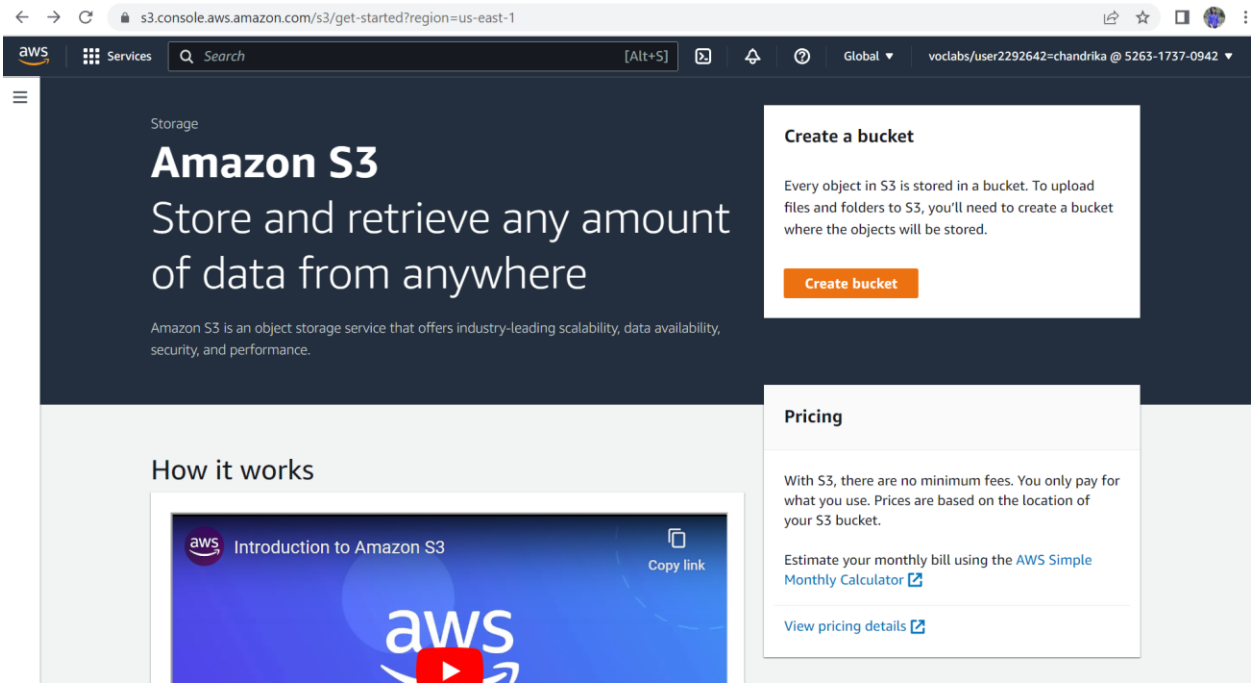


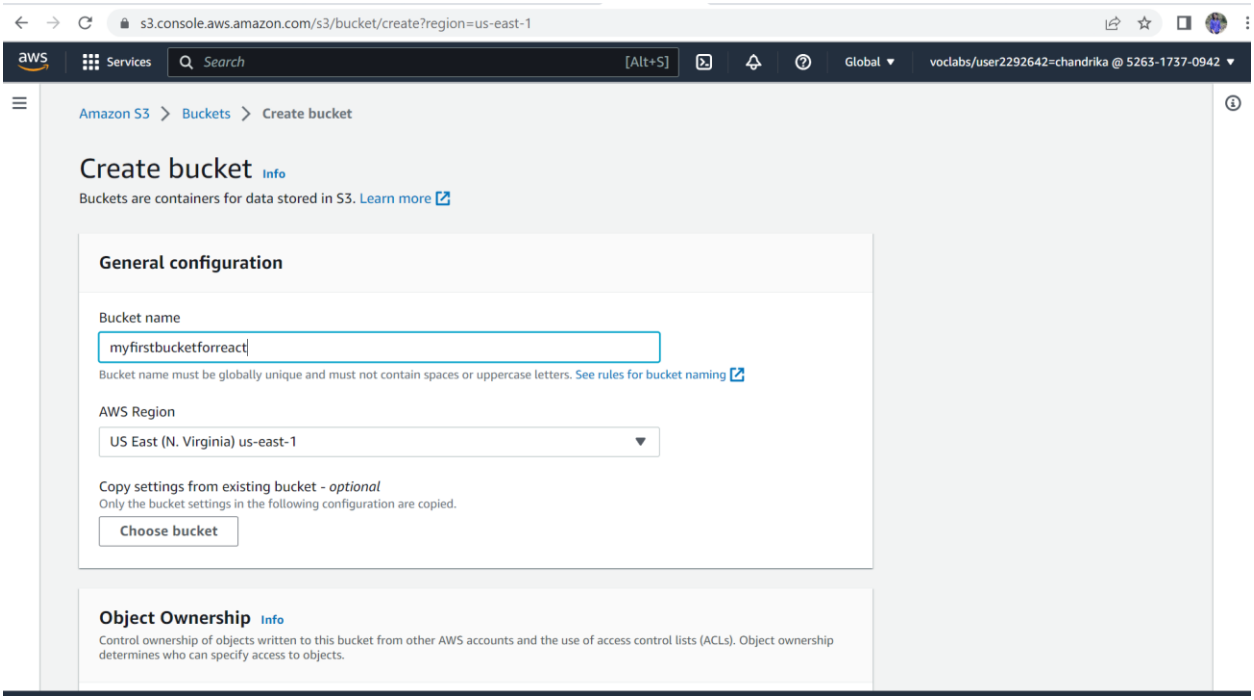
React app calling AWS FAAS

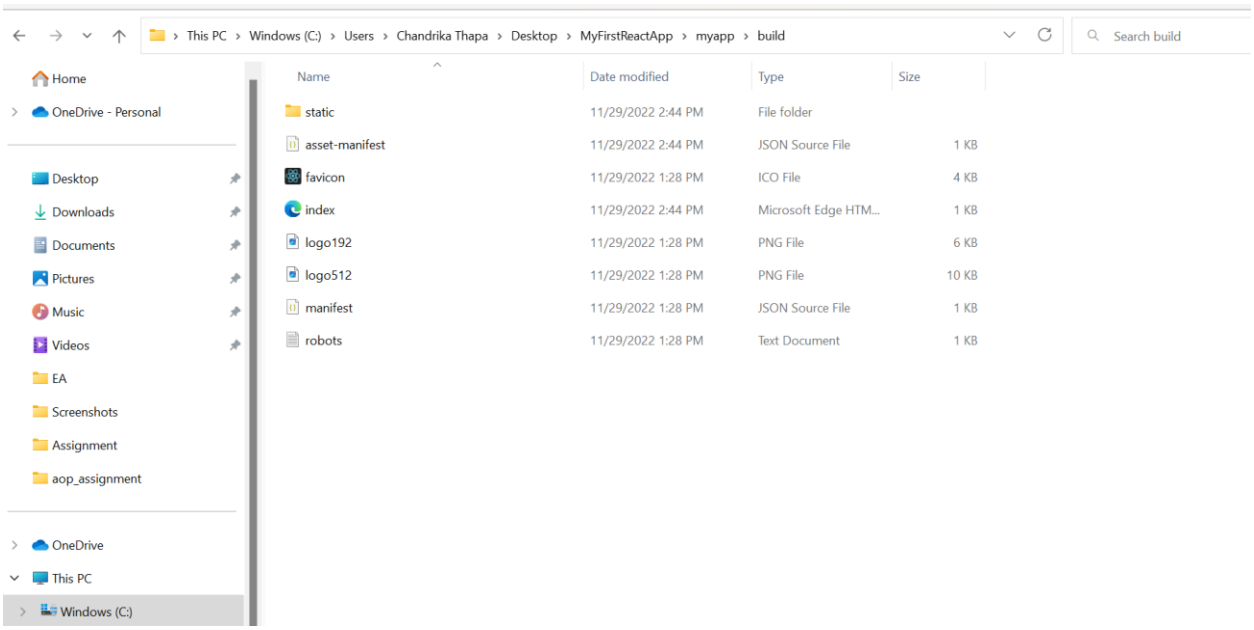


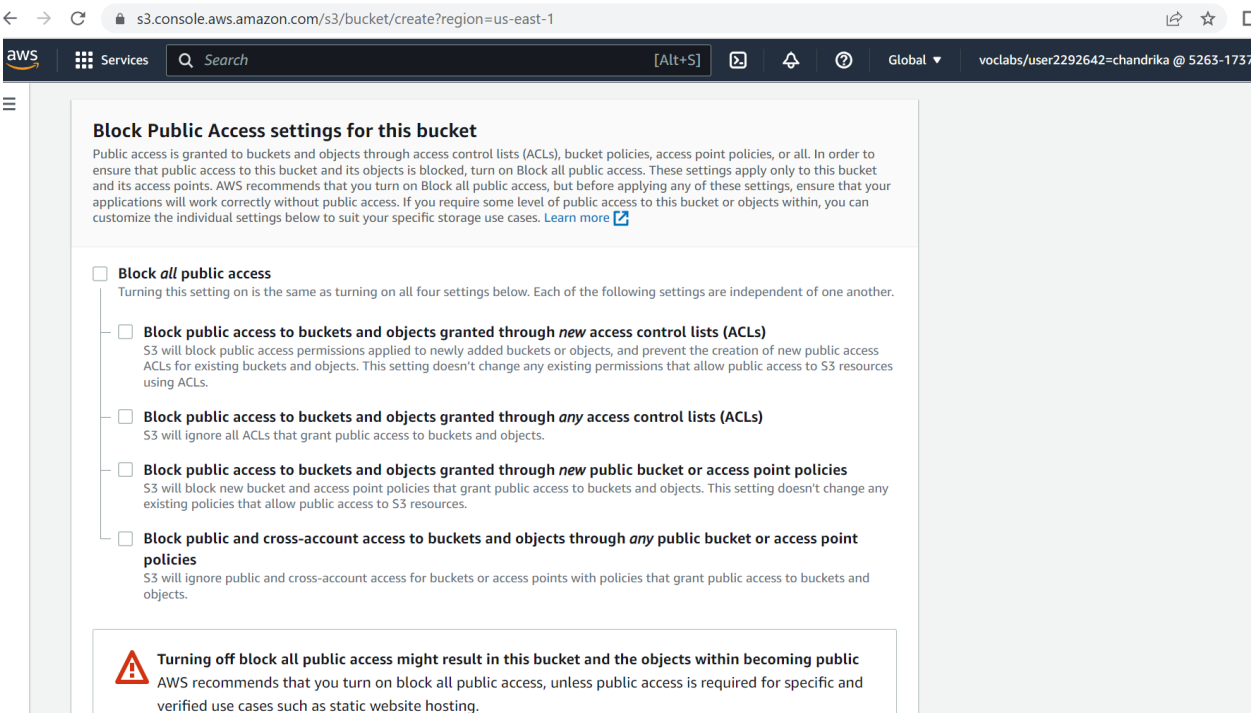


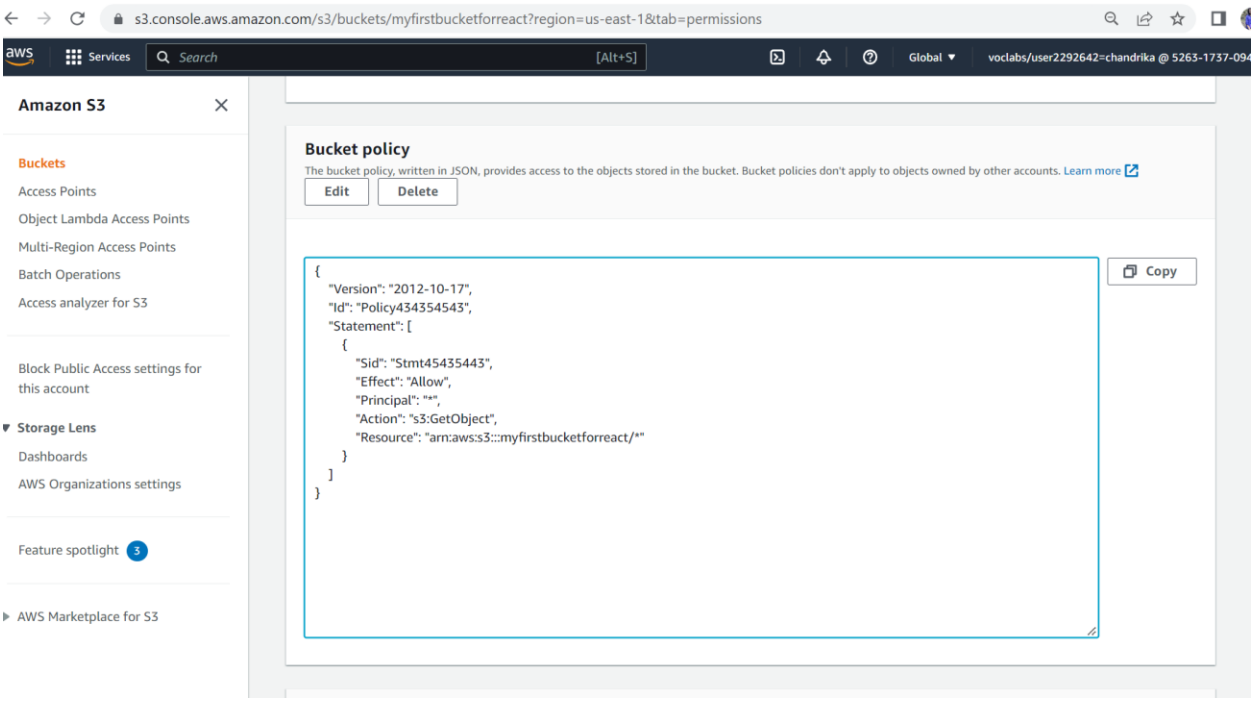
Deploying react app in s3

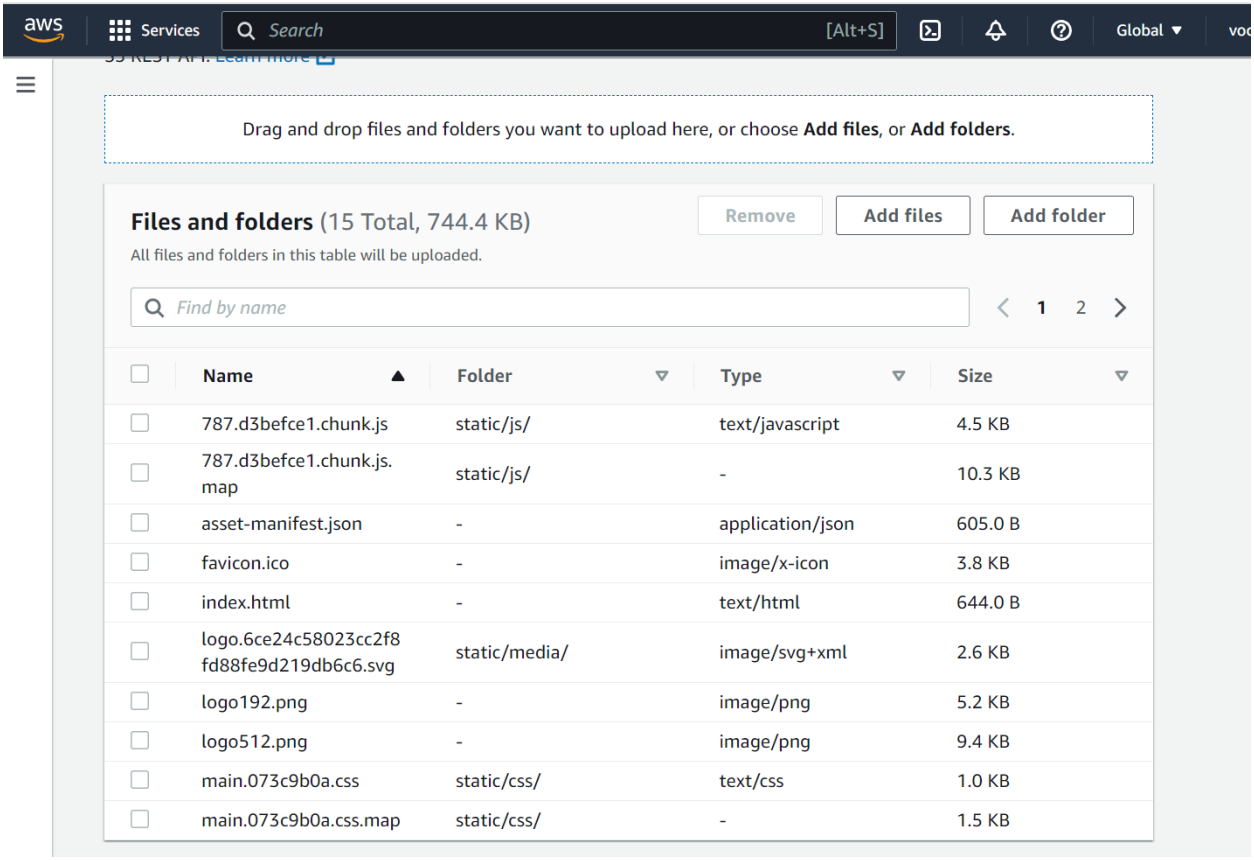


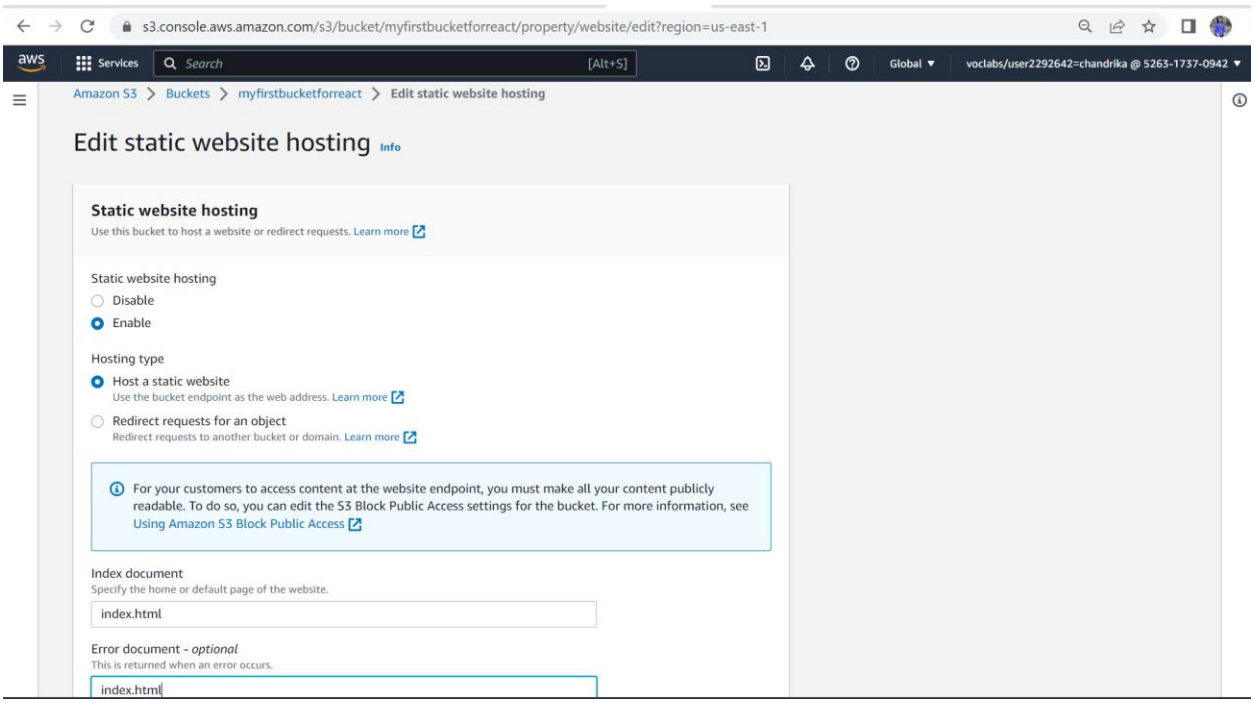


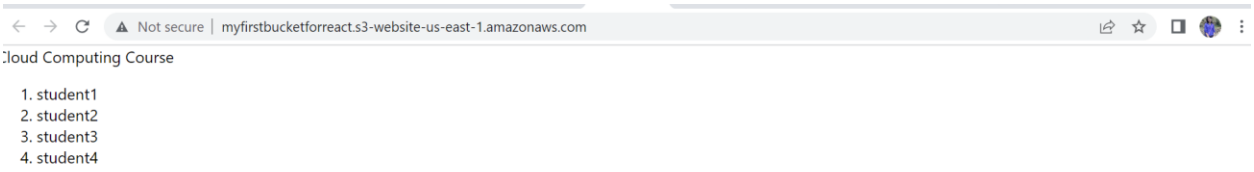

This PC › Windows (C:) › Users › Chandrika Thapa › Desktop › MyFirstReactApp › myapp › build
Search build
Home
OneDrive - Personal
Desktop
Downloads
Documents
Pictures
Music
Videos
EA
Screenshots
Assignment
aop_assignment
OneDrive
This PC
Windows (C:)
Name
Date modified
Type
Size
static 11/29/2022 2:44 PM File folder
asset-manifest 11/29/2022 2:44 PM JSON Source File 1 KB
favicon 11/29/2022 1:28 PM ICO File 4 KB
index 11/29/2022 2:44 PM Microsoft Edge HTM... 1 KB
logo192 11/29/2022 1:28 PM PNG File 6 KB
logo512 11/29/2022 1:28 PM PNG File 10 KB
manifest 11/29/2022 1:28 PM JSON Source File 1 KB
robots 11/29/2022 1:28 PM Text Document 1 KB


s3.console.aws.amazon.com/s3/bucket/create?region=us-east-1
aws
Services
Search
[Alt+S]
Global
voclabs/user2292642=chandrika @ 5263-1737
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.


s3.console.aws.amazon.com/s3/buckets/myfirstbucketforreact?region=us-east-1&tab=permissions
aws
Services
Search
[Alt+S]
Global
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
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
Copy
{
"Version": "2012-10-17",
"Id": "Policy434354543",
"Statement": [
{
"Sid": "Stmt45435443",
"Effect": "Allow",
"Principal": "*",
"Action": "s3:GetObject",
"Resource": "arn:aws:s3:::myfirstbucketforreact/*"
}
]
}


aws
Services
Search
[Alt+S]
Global
Drag and drop files and folders you want to upload here, or choose Add files, or Add folders.
Files and folders (15 Total, 744.4 KB)
Remove
Add files
Add folder
All files and folders in this table will be uploaded.
Find by name
1
2
Name
Folder
Type
Size
787.d3befce1.chunk.js
static/js/
text/javascript
4.5 KB
787.d3befce1.chunk.js.map
static/js/
-
10.3 KB
asset-manifest.json
-
application/json
605.0 B
favicon.ico
-
image/x-icon
3.8 KB
index.html
-
text/html
644.0 B
logo.6ce24c58023cc2f8fd88fe9d219db6c6.svg
static/media/
image/svg+xml
2.6 KB
logo192.png
-
image/png
5.2 KB
logo512.png
-
image/png
9.4 KB
main.073c9b0a.css
static/css/
text/css
1.0 KB
main.073c9b0a.css.map
static/css/
-
1.5 KB

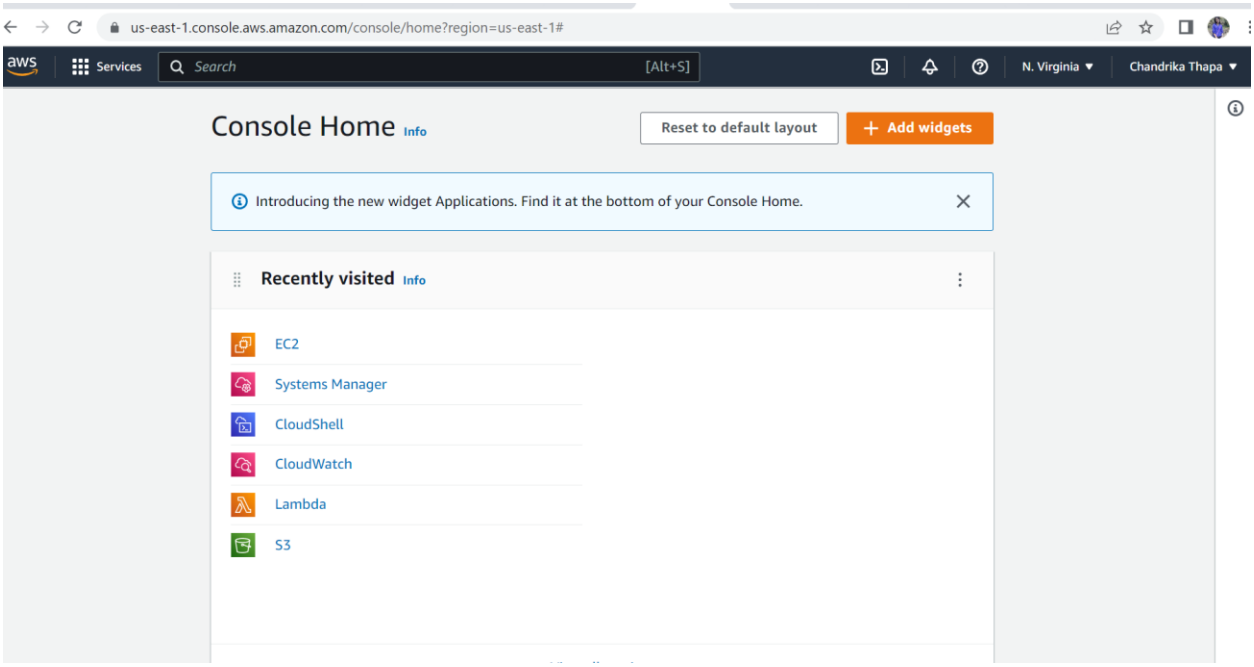




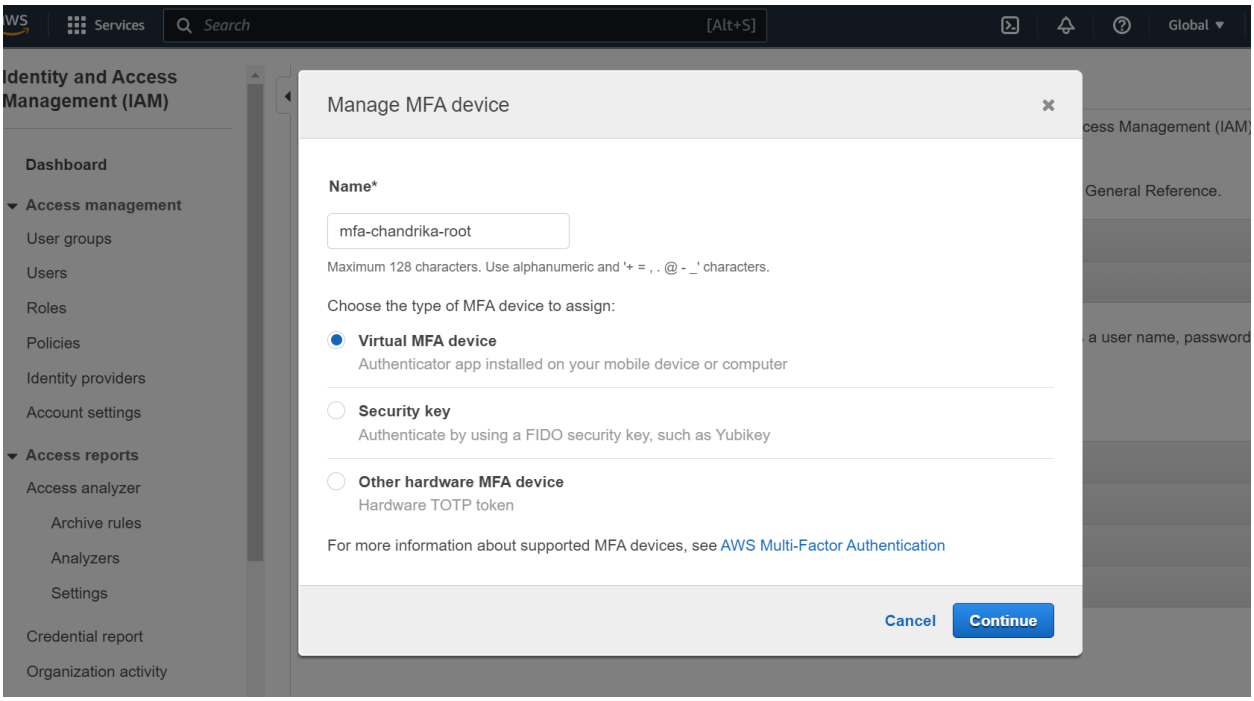
Cloud Computing Course

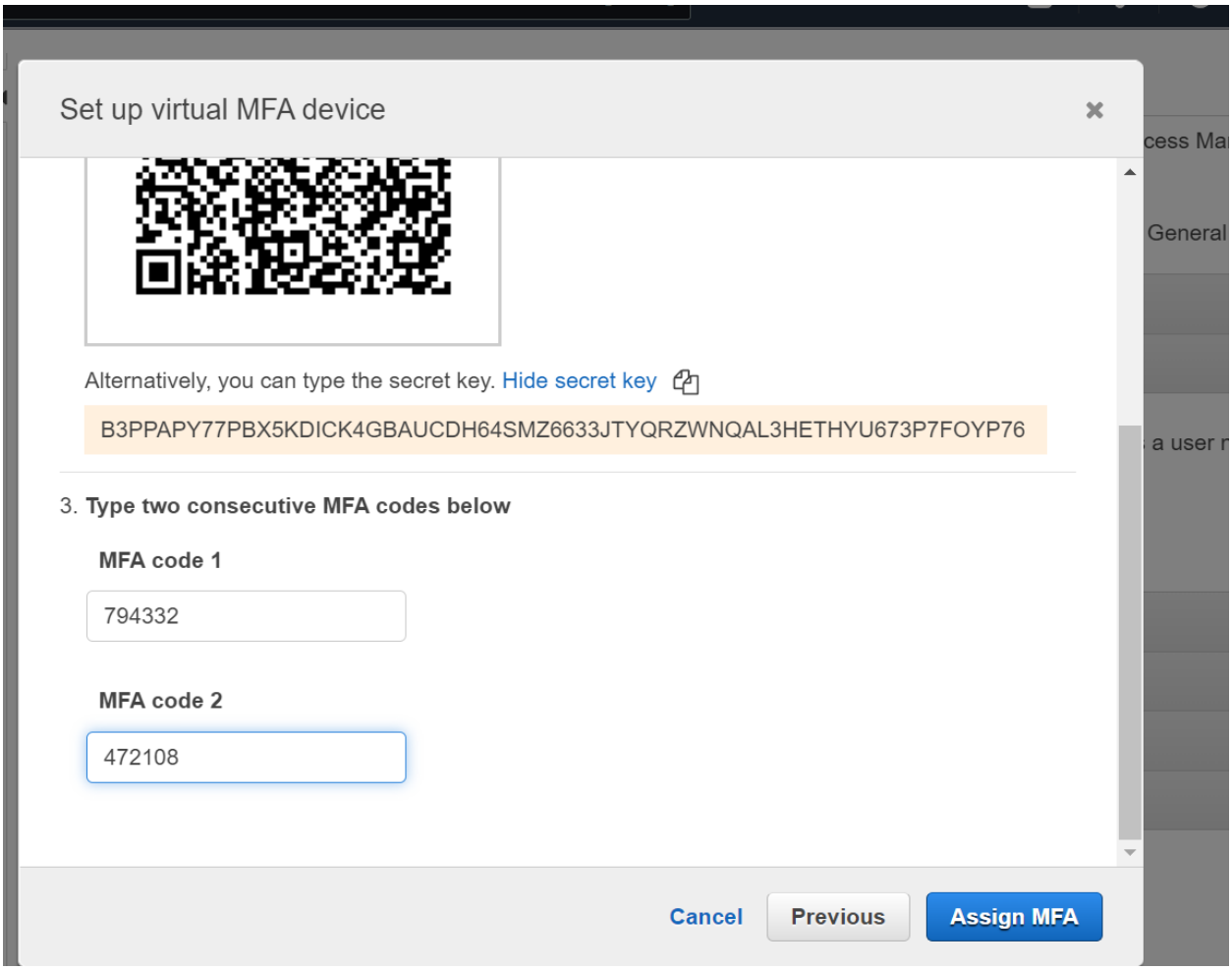
1. student1
2. student2
3. student3
4. student4

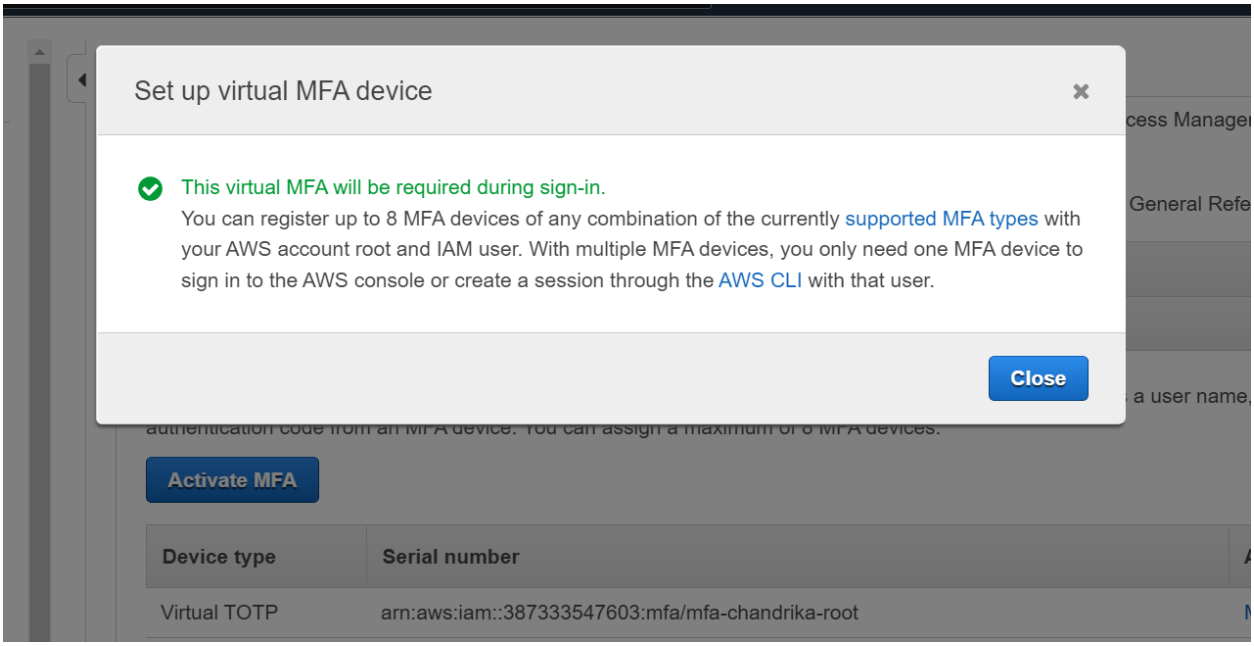
Creating personal AWS account (root user)

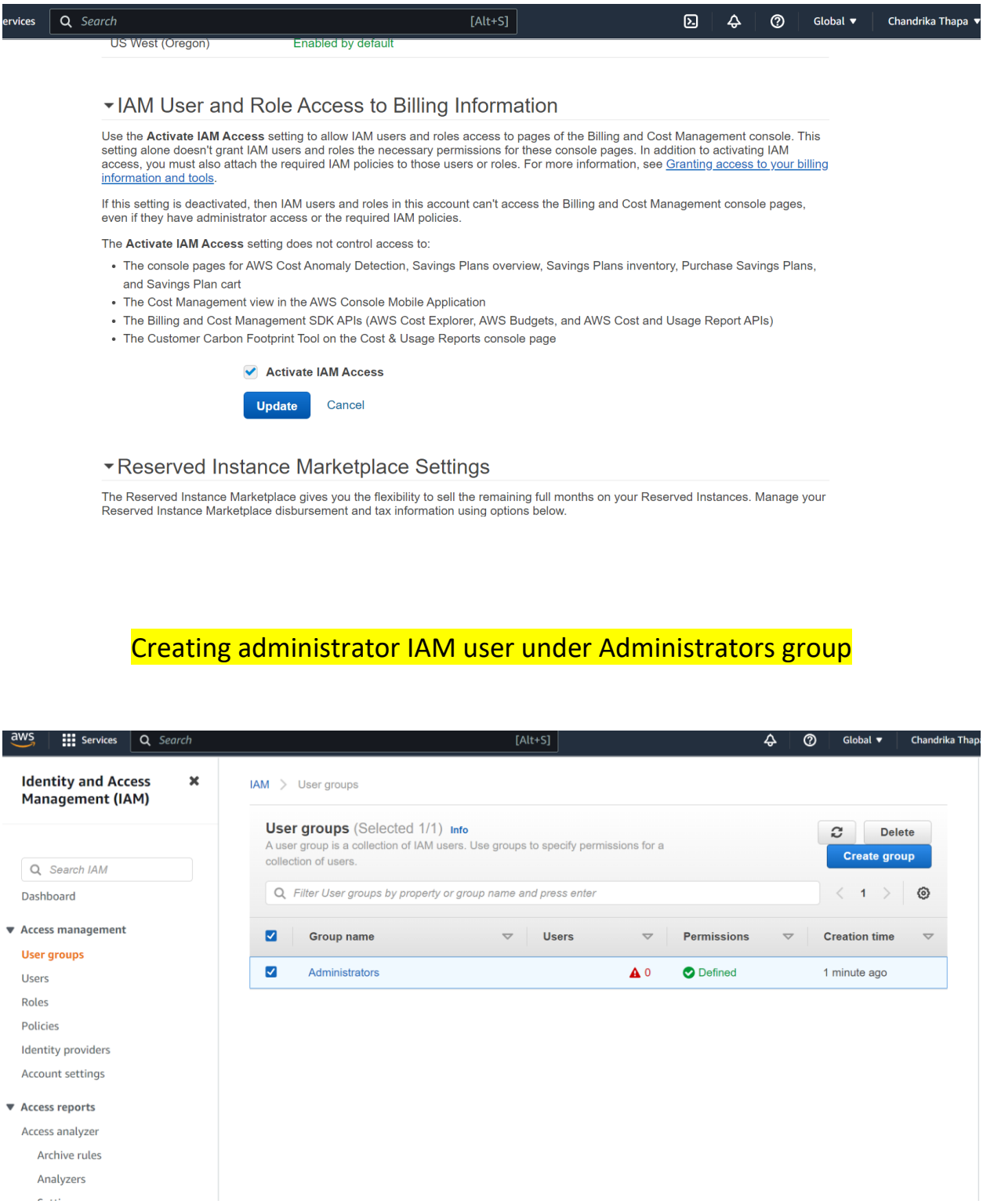


Enabling MFA in root user

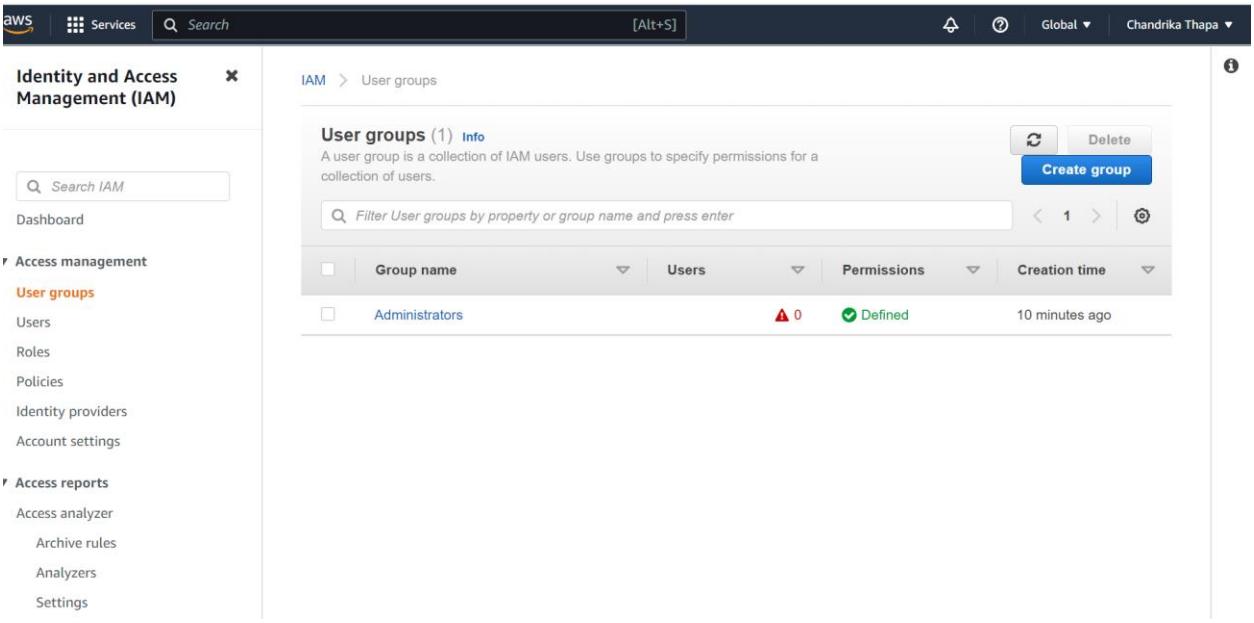


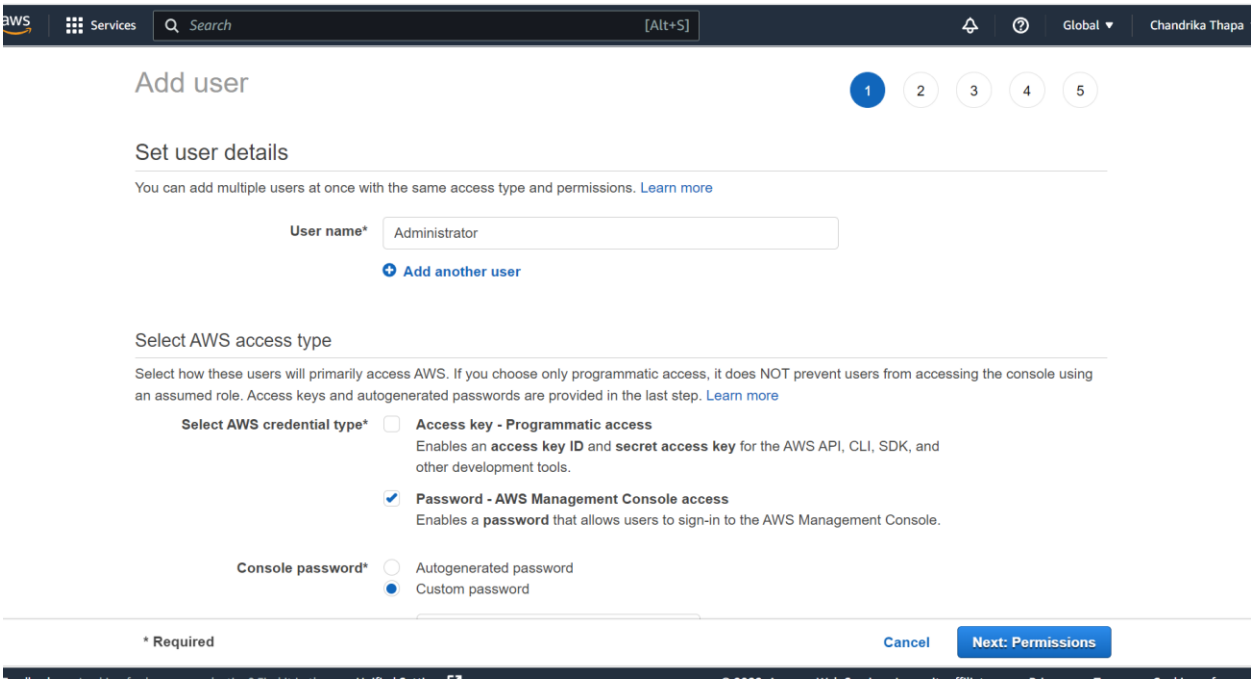

Set up virtual MFA device
Alternatively, you can type the secret key. Hide secret key
B3PPAPY77PBX5KDICK4GBAUCDH64SMZ6633JTYQRZWNQAL3HETHYU673P7FOYP76
3. Type two consecutive MFA codes below
MFA code 1
794332
MFA code 2
472108
Cancel
Previous
Assign MFA

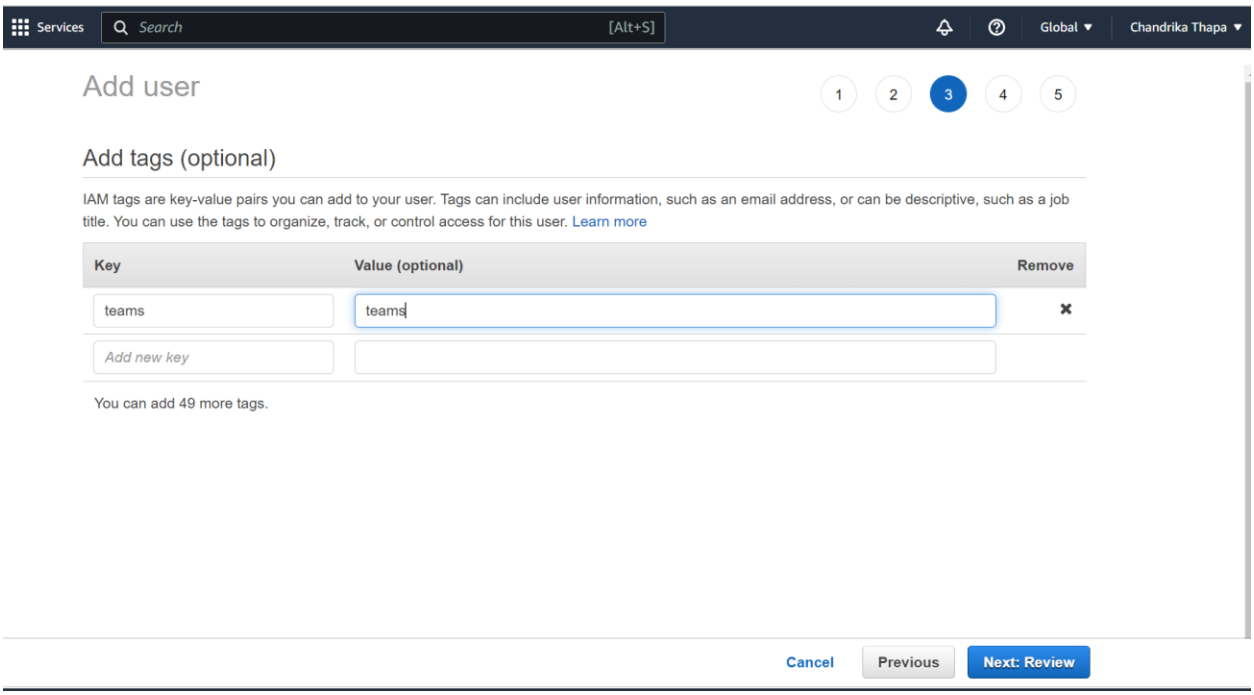

Set up virtual MFA device
This virtual MFA will be required during sign-in.
You can register up to 8 MFA devices of any combination of the currently supported MFA types with your AWS account root and IAM user. With multiple MFA devices, you only need one MFA device to sign in to the AWS console or create a session through the AWS CLI with that user.
Close
Activate MFA
Device type
Serial number
Virtual TOTP
arn:aws:iam::387333547603:mfa/mfa-chandrika-root

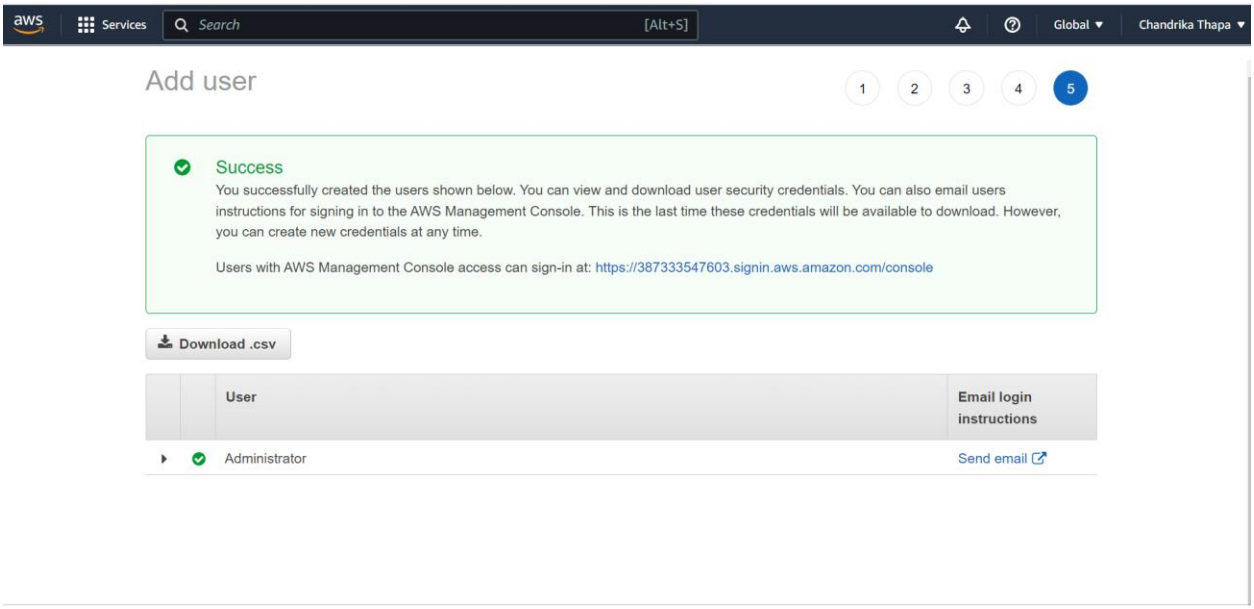


Creating administrator IAM user under Administrators group

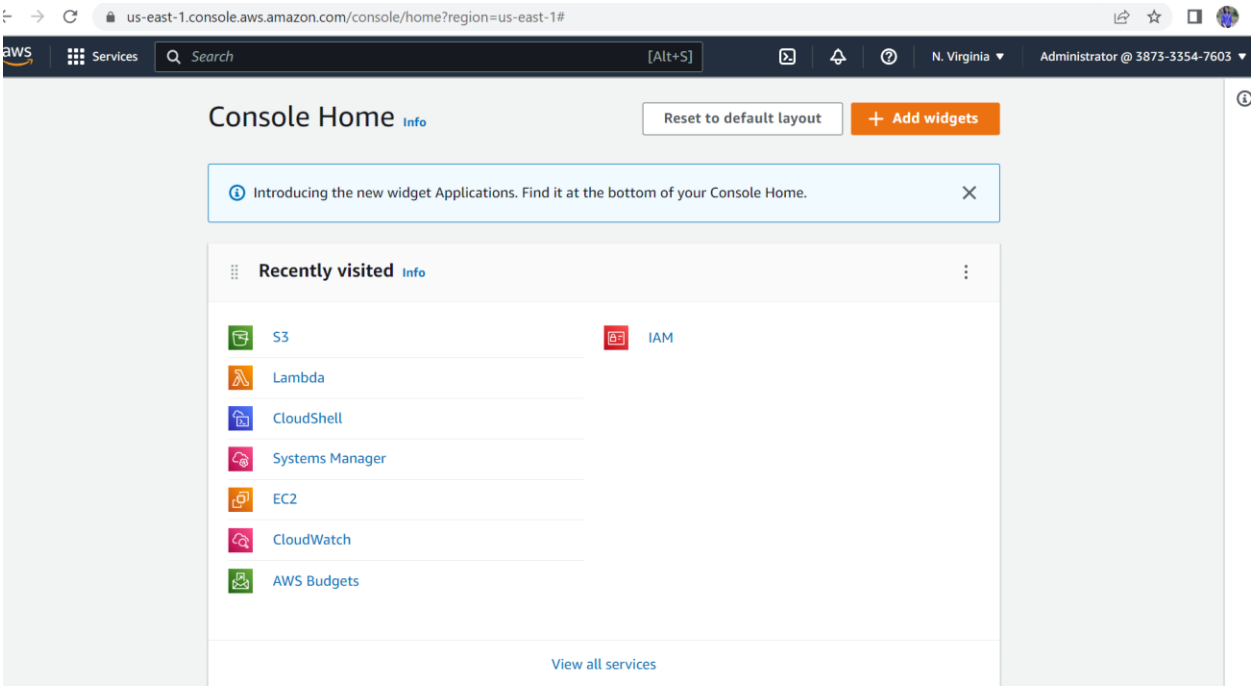

aws
Services
Search
[Alt+S]
Global
Chandrika Thapa
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access analyzer
Archive rules
Analyzers
Settings
IAM > User groups
User groups (1) Info
A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.
Delete
Create group
Filter User groups by property or group name and press enter
1
Group name
Users
Permissions
Creation time
Administrators
0
Defined
10 minutes ago


aws
Services
Search
[Alt+S]
Global
Chandrika Thapa
Add user
1
2
3
4
5
Set user details
You can add multiple users at once with the same access type and permissions. Learn more
User name*
Administrator
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
* Required
Cancel
Next: Permissions

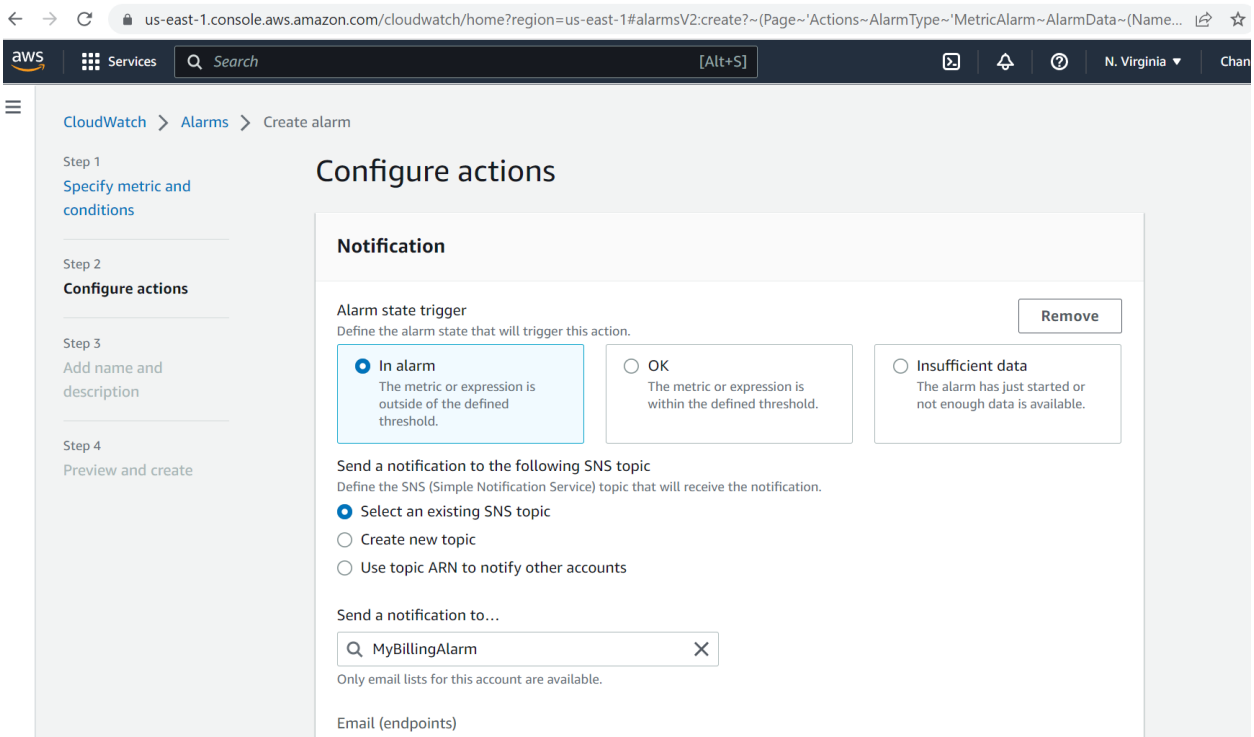

Services
Search
[Alt+S]
Global
Chandrika Thapa
Add user
1
2
3
4
5
Add tags (optional)
IAM tags are key-value pairs you can add to your user. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can use the tags to organize, track, or control access for this user. Learn more
Key
Value (optional)
Remove
teams
teams
Add new key
You can add 49 more tags.
Cancel
Previous
Next: Review

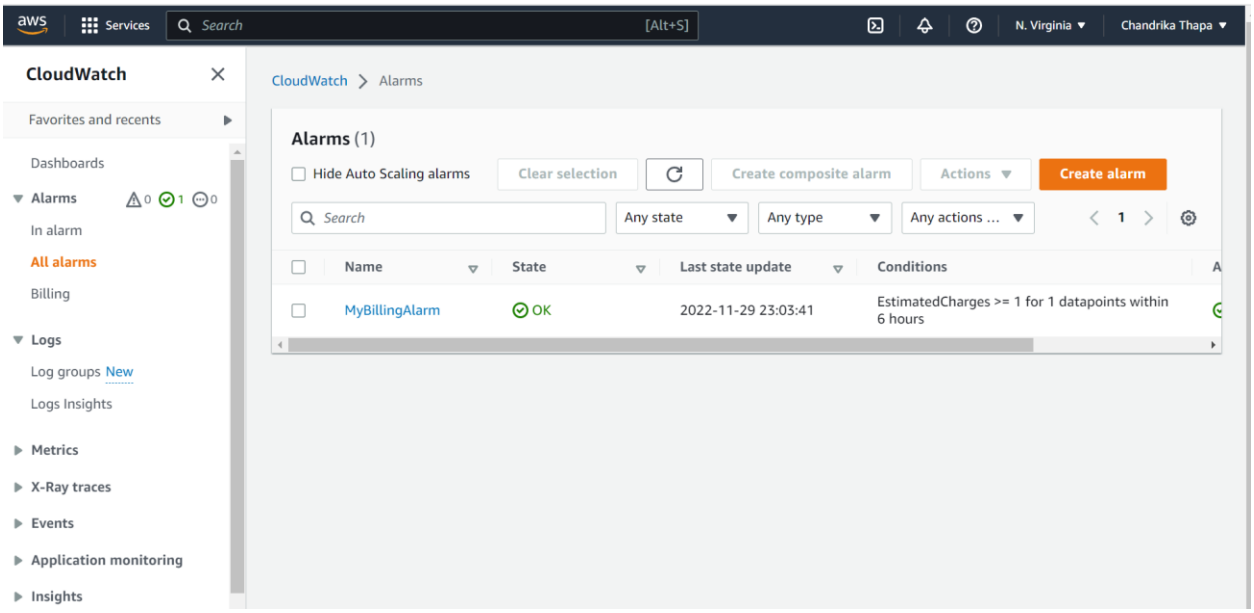

aws
Services
Search
[Alt+S]
Global
Chandrika Thapa
Add user
1
2
3
4
5
Success
You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials 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://387333547603.signin.aws.amazon.com/console
Download .csv
User
Email login instructions
Administrator
Send email

Logging in as administrator user



Setting billing alarm for root user




aws
Services
Search
[Alt+S]
N. Virginia
Chandrika Thapa
CloudWatch
Favorites and recents
Dashboards
Alarms
0
1
0
In alarm
All alarms
Billing
Logs
Log groups
New
Logs Insights
Metrics
X-Ray traces
Events
Application monitoring
Insights
CloudWatch
Alarms
Alarms (1)
Hide Auto Scaling alarms
Clear selection
Create composite alarm
Actions
Create alarm
Search
Any state
Any type
Any actions ...
1
Name
State
Last state update
Conditions
MyBillingAlarm
OK
2022-11-29 23:03:41
EstimatedCharges >= 1 for 1 datapoints within 6 hours