**TS SDP4 (Cloud DevOps)**

**ID NO:** 190030677 **Name:** K. Sravani

**Skilling-5**

Create a S3 bucket and edit the bucket policy for the EC2 access from your account with the specific IAM role option. Create the IAM role for EC2 instance to access the other AWS services. Push the source code which you are having in your local system to the S3 bucket through AWS CLI commands. Create DynamoDB table for your application and connect with your EC2 instance. Launch the website with S3 bucket and DynamoDB connection with your EC2 instance.

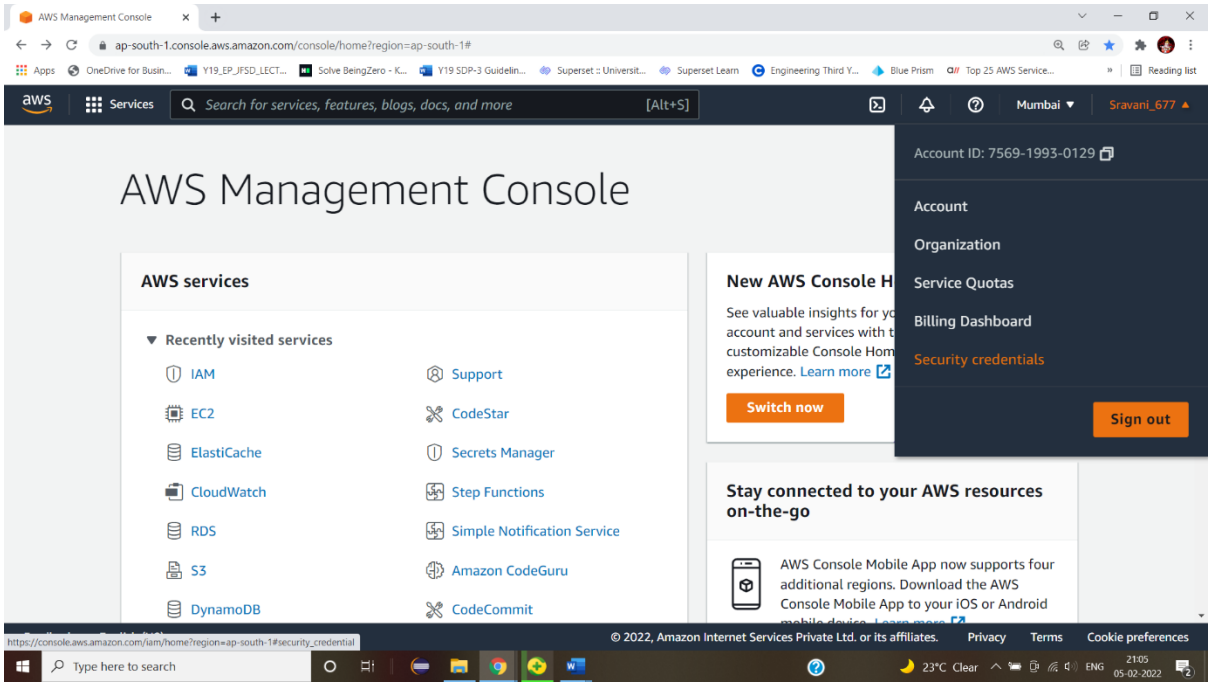
## Steps:

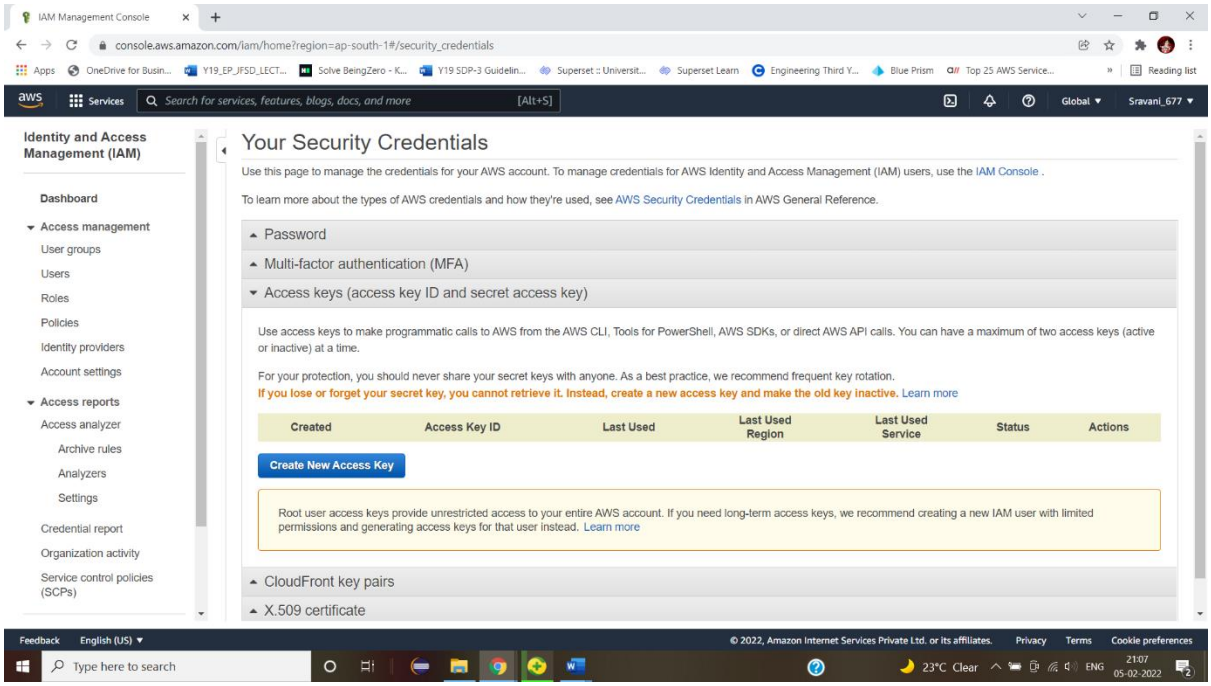
1.Create the s3 bucket select the s3 services

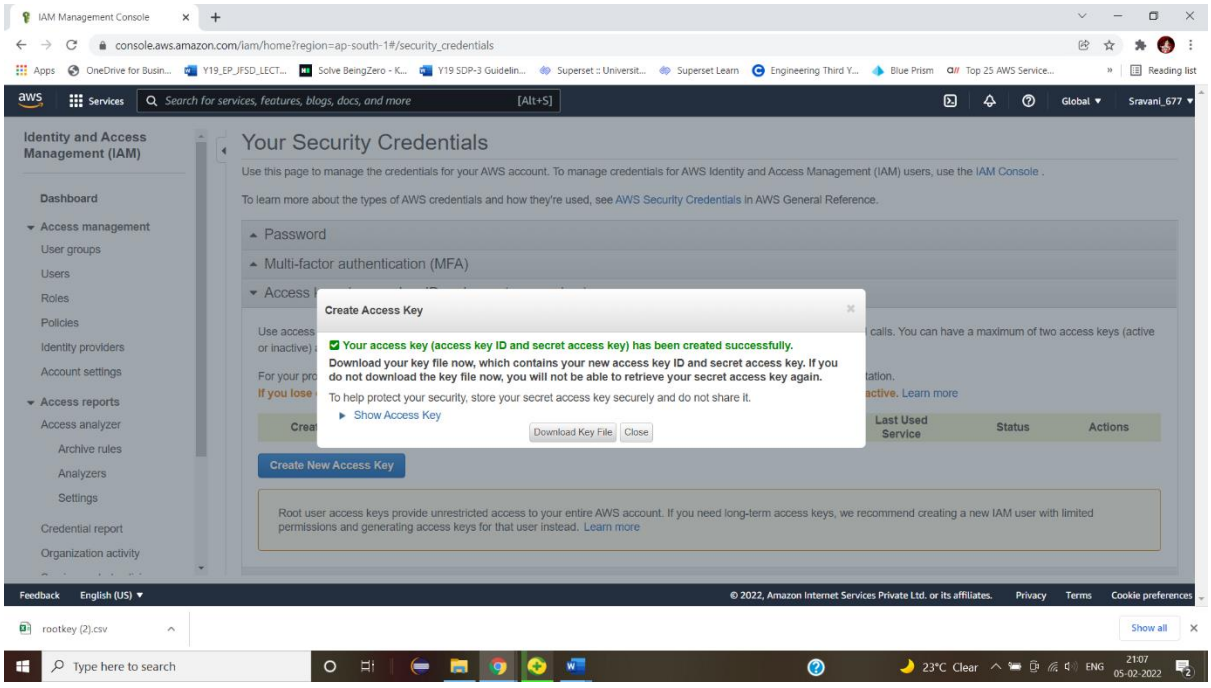
2.select s3 bucket and unable block all public access and enable acli public

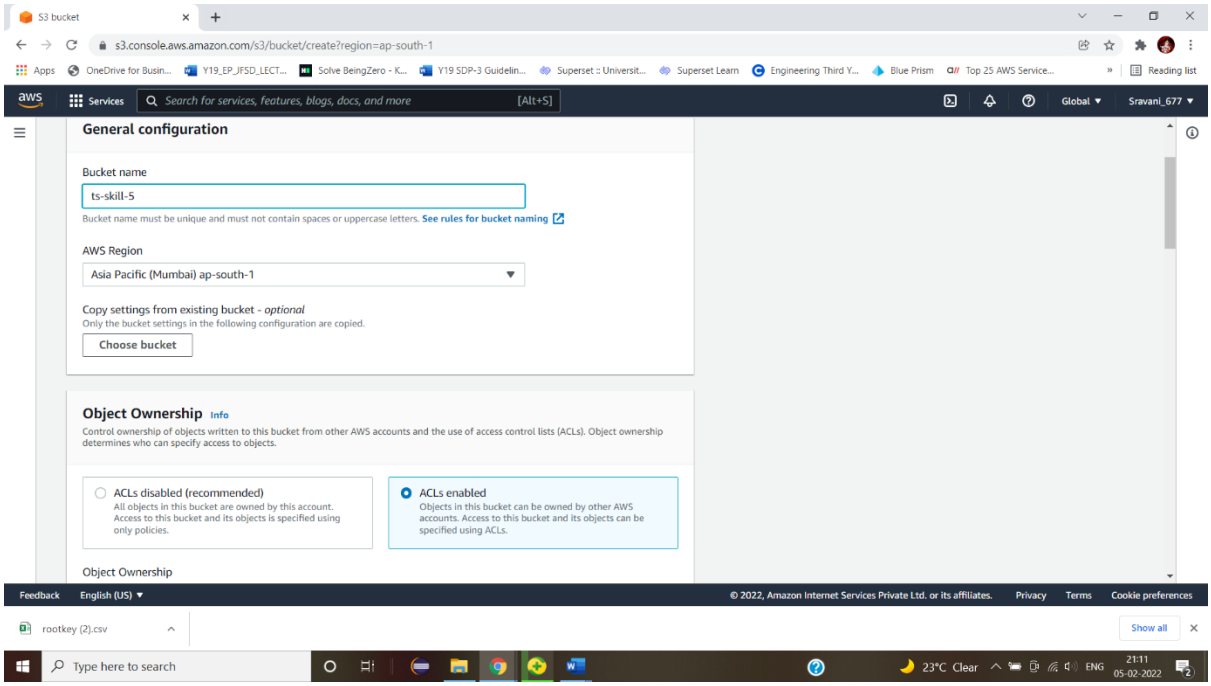
3.open command and execute the following commands

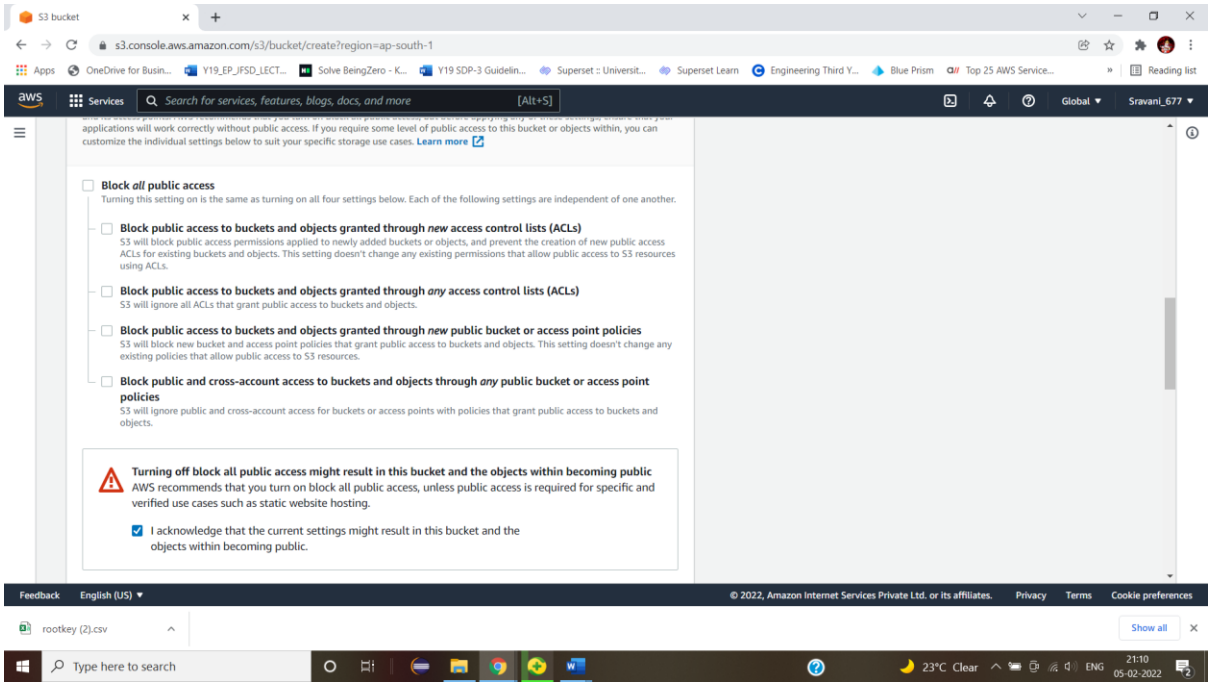
- aws configure --profile aws-devopsuse
- Provide the access key and secret access key
- aws s3 mb s3://BUCKET-NAME --region ap-south-1 --profile aws-devopsReplace the bucket name with the bucket created before and change the region

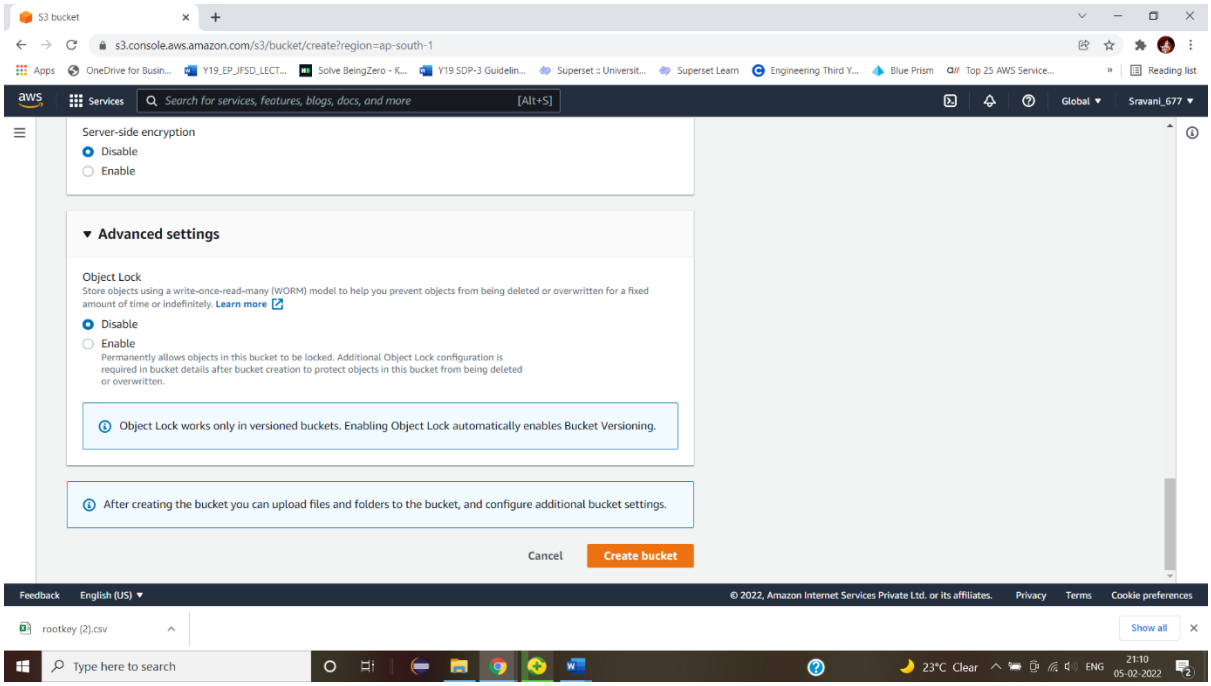


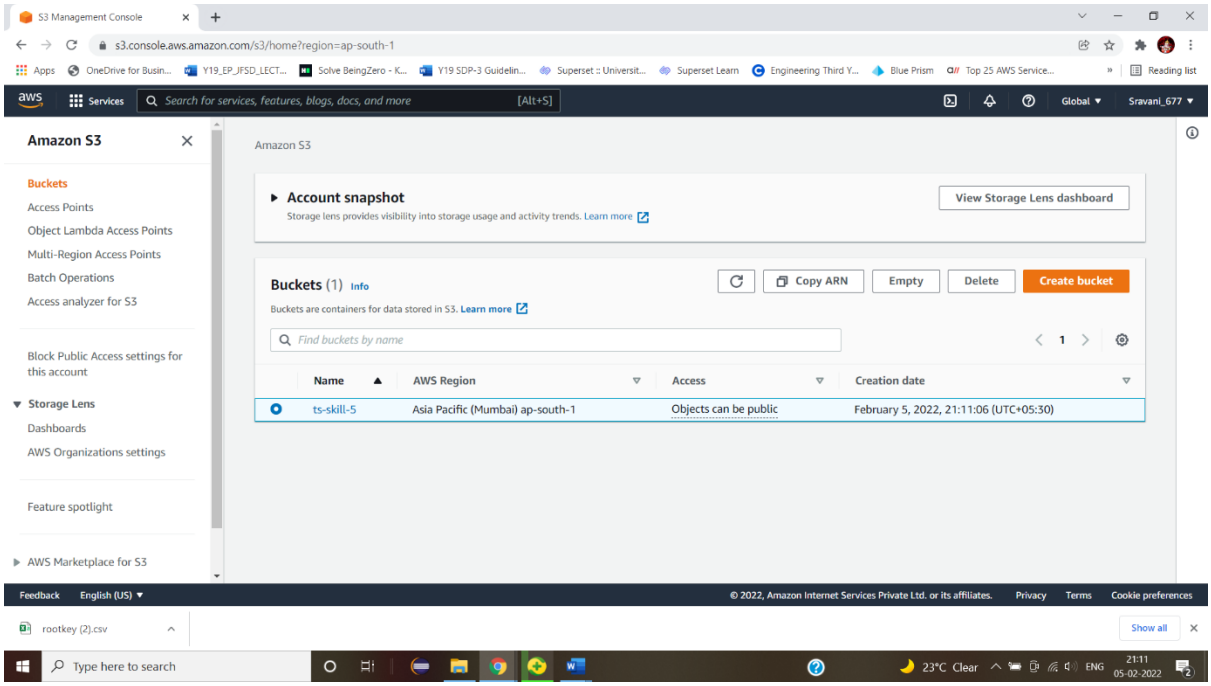

IAM Management Console
console.aws.amazon.com/iam/home?region=ap-south-1#/security_credentials
Services
Search for services, features, blogs, docs, and more
[Alt+S]
Global
Sravani_677
Identity and Access Management (IAM)
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access analyzer
Archive rules
Analyzers
Settings
Credential report
Organization activity
Service control policies (SCPs)
Your Security Credentials
Use this page to manage the credentials for your AWS account. To manage credentials for AWS Identity and Access Management (IAM) users, use the IAM Console .
To learn more about the types of AWS credentials and how they're used, see AWS Security Credentials in AWS General Reference.
Password
Multi-factor authentication (MFA)
Access keys (access key ID and secret access key)
Use access keys to make programmatic calls to AWS from the AWS CLI, Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time.
For your protection, you should never share your secret keys with anyone. As a best practice, we recommend frequent key rotation.
If you lose or forget your secret key, you cannot retrieve it. Instead, create a new access key and make the old key inactive. Learn more
Created
Access Key ID
Last Used
Last Used Region
Last Used Service
Status
Actions
Create New Access Key
Root user access keys provide unrestricted access to your entire AWS account. If you need long-term access keys, we recommend creating a new IAM user with limited permissions and generating access keys for that user instead. Learn more
CloudFront key pairs
X.509 certificate
Feedback
English (US)
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
23°C Clear
ENG
21:07
05-02-2022

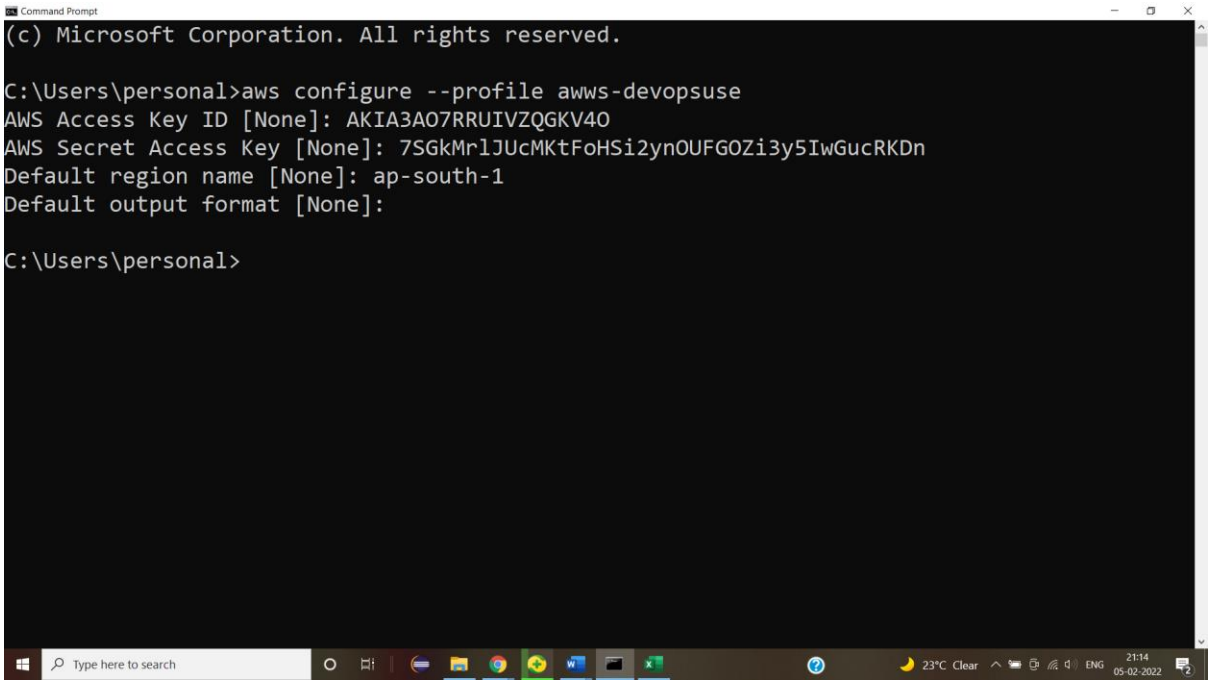

IAM Management Console
console.aws.amazon.com/iam/home?region=ap-south-1#/security_credentials
Identity and Access Management (IAM)
Your Security Credentials
Create Access Key
Your access key (access key ID and secret access key) has been created successfully.
Download your key file now, which contains your new access key ID and secret access key. If you do not download the key file now, you will not be able to retrieve your secret access key again.
To help protect your security, store your secret access key securely and do not share it.
Show Access Key
Download Key File
Close
Create New Access Key
Root user access keys provide unrestricted access to your entire AWS account. If you need long-term access keys, we recommend creating a new IAM user with limited permissions and generating access keys for that user instead. Learn more
Feedback
English (US)
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences
rootkey (2).csv
Show all
Type here to search
23°C Clear
ENG
21:07
05-02-2022

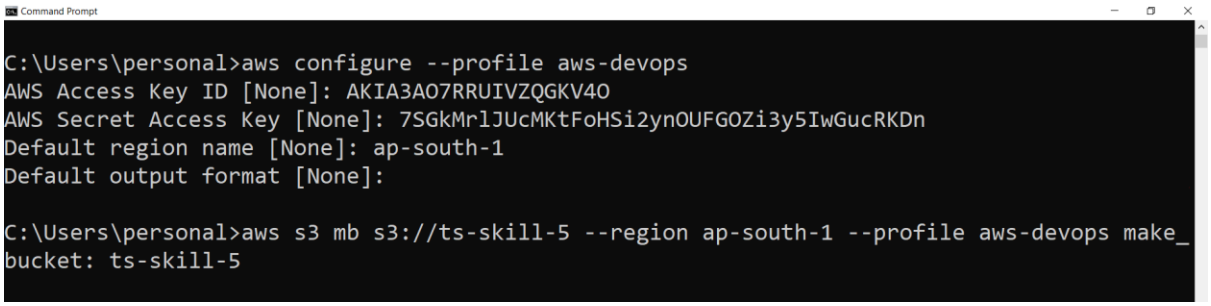

S3 bucket
s3.console.aws.amazon.com/s3/bucket/create?region=ap-south-1
Services
Search for services, features, blogs, docs, and more [Alt+S]
Global
Sravani_677
General configuration
Bucket name
ts-skill-5
Bucket name must be unique and must not contain spaces or uppercase letters. See rules for bucket naming
AWS Region
Asia Pacific (Mumbai) ap-south-1
Copy settings from existing bucket - optional
Only the bucket settings in the following configuration are copied.
Choose bucket
Object Ownership Info
Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.
ACLs disabled (recommended)
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.
ACLs enabled
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.
Object Ownership
Feedback
English (US)
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences
rootkey (2).csv
Show all
Type here to search
23°C Clear
ENG
21:11
05-02-2022

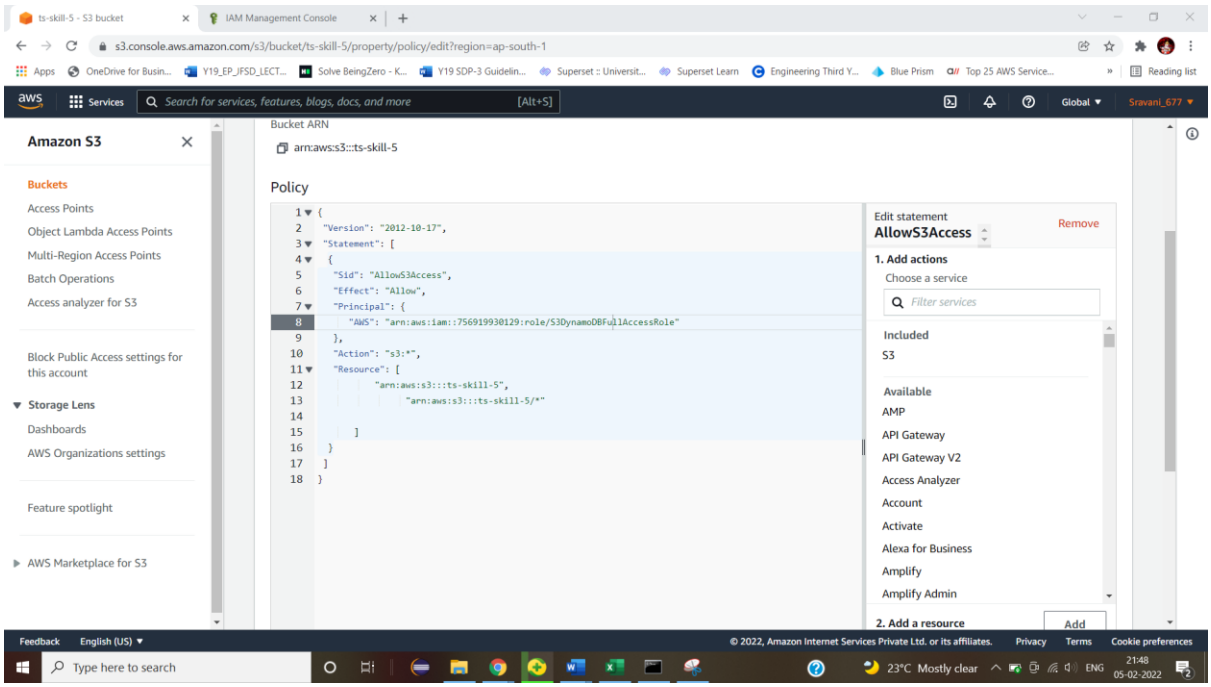

S3 bucket
s3.console.aws.amazon.com/s3/bucket/create?region=ap-south-1
Services
Search for services, features, blogs, docs, and more [Alt+S]
Global
Sravani_677
applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more
Block all public access
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.
Block public access to buckets and objects granted through new access control lists (ACLs)
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
Block public access to buckets and objects granted through any access control lists (ACLs)
S3 will ignore all ACLs that grant public access to buckets and objects.
Block public access to buckets and objects granted through new public bucket or access point policies
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
Block public and cross-account access to buckets and objects through any public bucket or access point policies
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.
Turning off block all public access might result in this bucket and the objects within becoming public
AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.
I acknowledge that the current settings might result in this bucket and the objects within becoming public.
Feedback
English (US)
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences
rootkey (2).csv
Show all
Type here to search
23°C Clear
ENG
21:10
05-02-2022

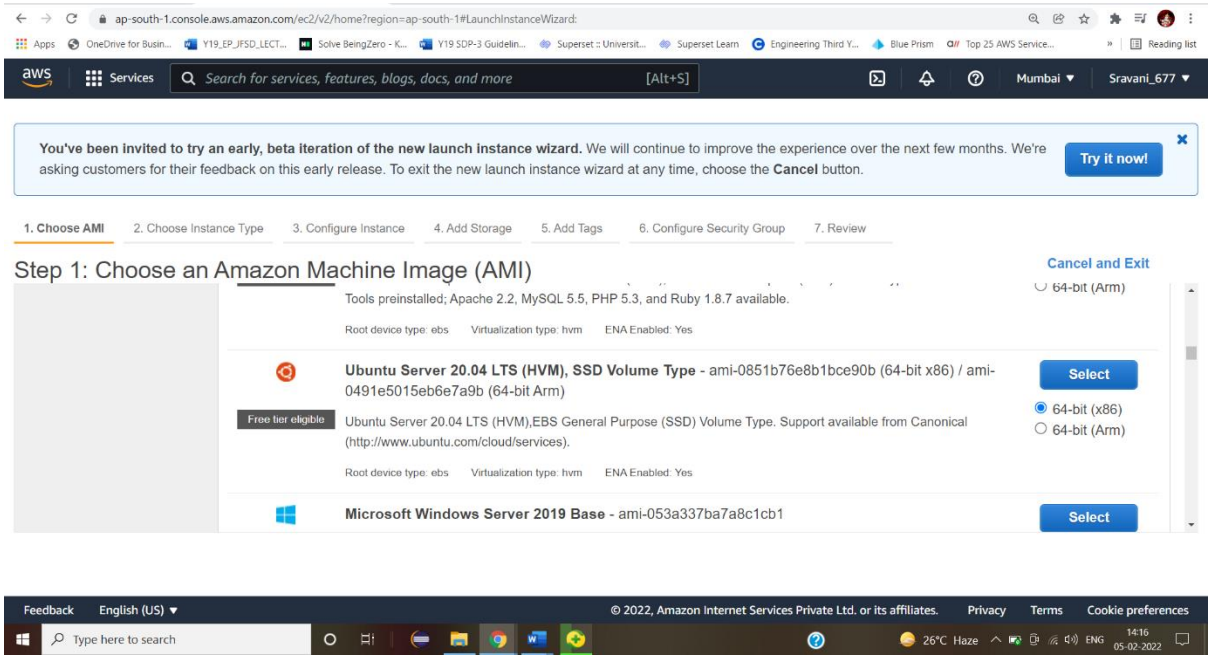

S3 bucket
s3.console.aws.amazon.com/s3/bucket/create?region=ap-south-1
Server-side encryption
Disable
Enable
Advanced settings
Object Lock
Store objects using a write-once-read-many (WORM) model to help you prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely. Learn more
Disable
Enable
Permanently allows objects in this bucket to be locked. Additional Object Lock configuration is required in bucket details after bucket creation to protect objects in this bucket from being deleted or overwritten.
Object Lock works only in versioned buckets. Enabling Object Lock automatically enables Bucket Versioning.
After creating the bucket you can upload files and folders to the bucket, and configure additional bucket settings.
Cancel
Create bucket
Feedback
English (US)
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences
rootkey (2).csv
Show all
Type here to search
23°C Clear
ENG
21:10
05-02-2022

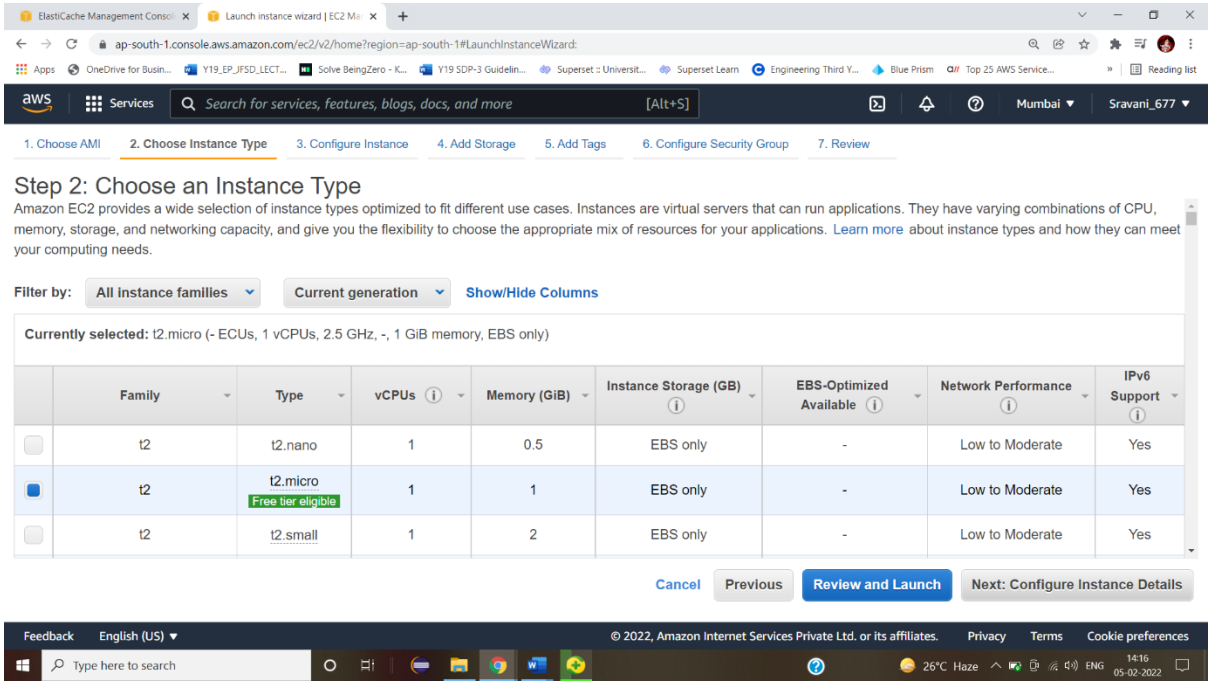

S3 Management Console
s3.console.aws.amazon.com/s3/home?region=ap-south-1
Amazon S3
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
Access analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight
AWS Marketplace for S3
Amazon S3
Account snapshot
Storage lens provides visibility into storage usage and activity trends. Learn more
View Storage Lens dashboard
Buckets (1) Info
Buckets are containers for data stored in S3. Learn more
Copy ARN
Empty
Delete
Create bucket
Find buckets by name
Name
AWS Region
Access
Creation date
ts-skill-5
Asia Pacific (Mumbai) ap-south-1
Objects can be public
February 5, 2022, 21:11:06 (UTC+05:30)
Feedback
English (US)
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences
rootkey (2).csv
Show all
Type here to search
23°C Clear
ENG
21:11
05-02-2022

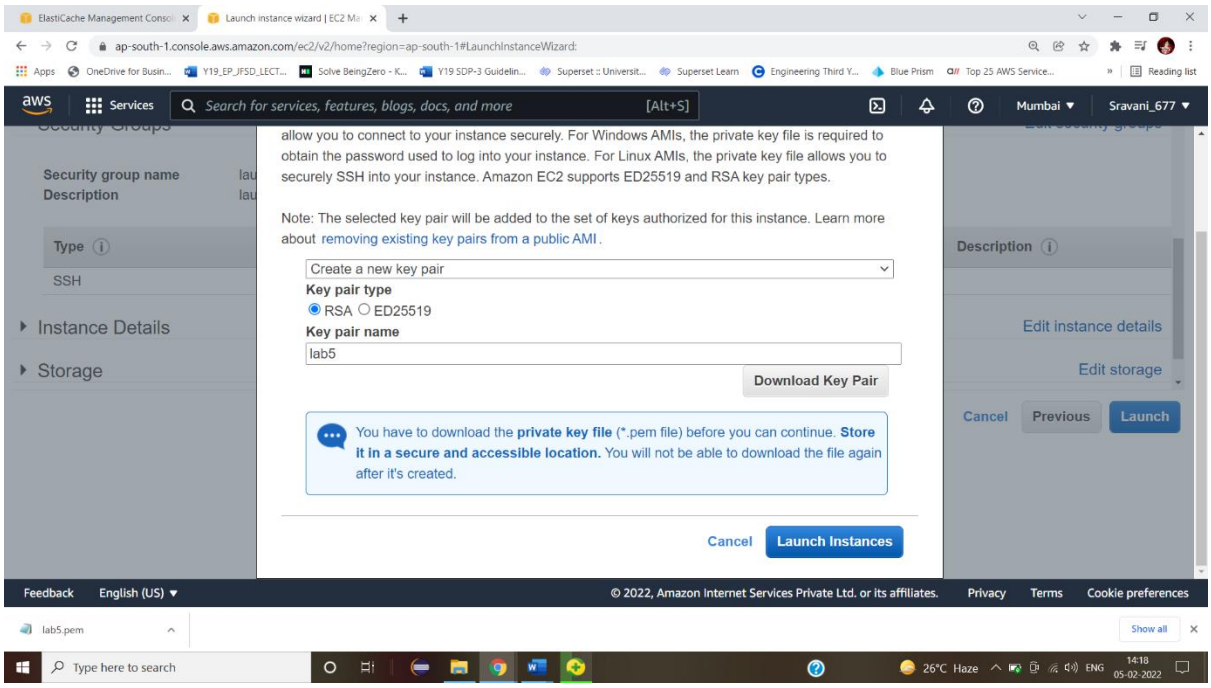

Command Prompt
(c) Microsoft Corporation. All rights reserved.
C:\Users\personal>aws configure --profile awws-devopsuse
AWS Access Key ID [None]: AKIA3AO7RRUIVZQGKV4O
AWS Secret Access Key [None]: 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
Default region name [None]: ap-south-1
Default output format [None]:
C:\Users\personal>
Type here to search
23°C Clear
ENG
21:14
05-02-2022

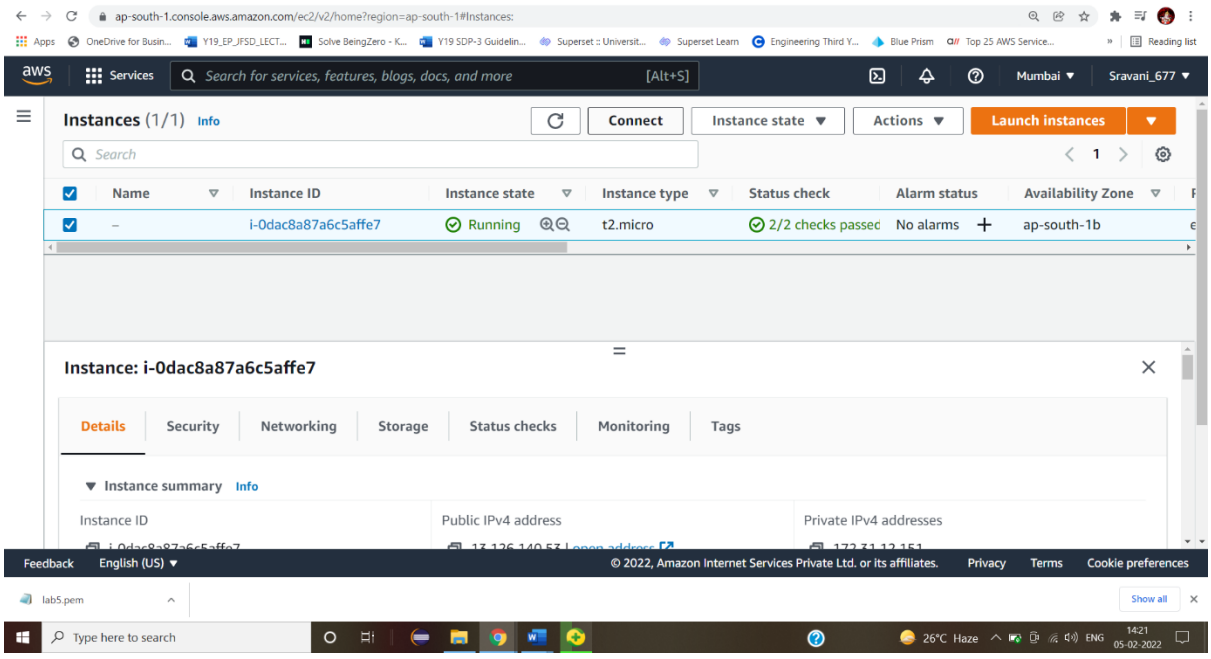

Command Prompt
C:\Users\personal>aws configure --profile aws-devops
AWS Access Key ID [None]: AKIA3AO7RRUIVZQGKV4O
AWS Secret Access Key [None]: 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
Default region name [None]: ap-south-1
Default output format [None]:
C:\Users\personal>aws s3 mb s3://ts-skill-5 --region ap-south-1 --profile aws-devops make_
bucket: ts-skill-5


ts-skill-5 - S3 bucket
IAM Management Console
s3.console.aws.amazon.com/s3/bucket/ts-skill-5/property/policy/edit?region=ap-south-1
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 ARN
arn:aws:s3:::ts-skill-5
Policy
{
"Version": "2012-10-17",
"Statement": [
{
"Sid": "AllowS3Access",
"Effect": "Allow",
"Principal": {
"AWS": "arn:aws:iam::756919930129:role/S3DynamoDBFullAccessRole"
},
"Action": "s3:*",
"Resource": [
"arn:aws:s3:::ts-skill-5",
"arn:aws:s3:::ts-skill-5/*"
]
}
]
}
Edit statement
AllowS3Access
Remove
1. Add actions
Choose a service
Filter services
Included
S3
Available
AMP
API Gateway
API Gateway V2
Access Analyzer
Account
Activate
Alexa for Business
Amplify
Amplify Admin
2. Add a resource
Add
Feedback
English (US)
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
23°C Mostly clear
ENG
21:48
05-02-2022


ap-south-1.console.aws.amazon.com/ec2/v2/home?region=ap-south-1#LaunchInstanceWizard:
Services
Search for services, features, blogs, docs, and more [Alt+S]
Mumbai
Sravani_677
You've been invited to try an early, beta iteration of the new launch instance wizard. We will continue to improve the experience over the next few months. We're asking customers for their feedback on this early release. To exit the new launch instance wizard at any time, choose the Cancel button.
Try it now!
1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 1: Choose an Amazon Machine Image (AMI)
Cancel and Exit
Tools preinstalled; Apache 2.2, MySQL 5.5, PHP 5.3, and Ruby 1.8.7 available.
Root device type: ebs Virtualization type: hvm ENA Enabled: Yes
Ubuntu Server 20.04 LTS (HVM), SSD Volume Type - ami-0851b76e8b1bce90b (64-bit x86) / ami-0491e5015eb6e7a9b (64-bit Arm)
Select
Free tier eligible
Ubuntu Server 20.04 LTS (HVM),EBS General Purpose (SSD) Volume Type. Support available from Canonical (http://www.ubuntu.com/cloud/services).
64-bit (x86)
64-bit (Arm)
Root device type: ebs Virtualization type: hvm ENA Enabled: Yes
Microsoft Windows Server 2019 Base - ami-053a337ba7a8c1cb1
Select
Feedback
English (US)
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
26°C Haze
ENG
14:16
05-02-2022


ElastiCache Management Consol
Launch instance wizard | EC2 Ma
ap-south-1.console.aws.amazon.com/ec2/v2/home?region=ap-south-1#LaunchInstanceWizard:
Services
Search for services, features, blogs, docs, and more [Alt+S]
Mumbai
Sravani_677
1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 2: Choose an Instance Type
Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. Learn more about instance types and how they can meet your computing needs.
Filter by: All instance families Current generation Show/Hide Columns
Currently selected: t2.micro (- ECUs, 1 vCPUs, 2.5 GHz, -, 1 GiB memory, EBS only)
Family | Type | vCPUs | Memory (GiB) | Instance Storage (GB) | EBS-Optimized Available | Network Performance | IPv6 Support
t2 | t2.nano | 1 | 0.5 | EBS only | - | Low to Moderate | Yes
t2 | t2.micro Free tier eligible | 1 | 1 | EBS only | - | Low to Moderate | Yes
t2 | t2.small | 1 | 2 | EBS only | - | Low to Moderate | Yes
Cancel
Previous
Review and Launch
Next: Configure Instance Details
Feedback
English (US)
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
26°C Haze
ENG
14:16
05-02-2022

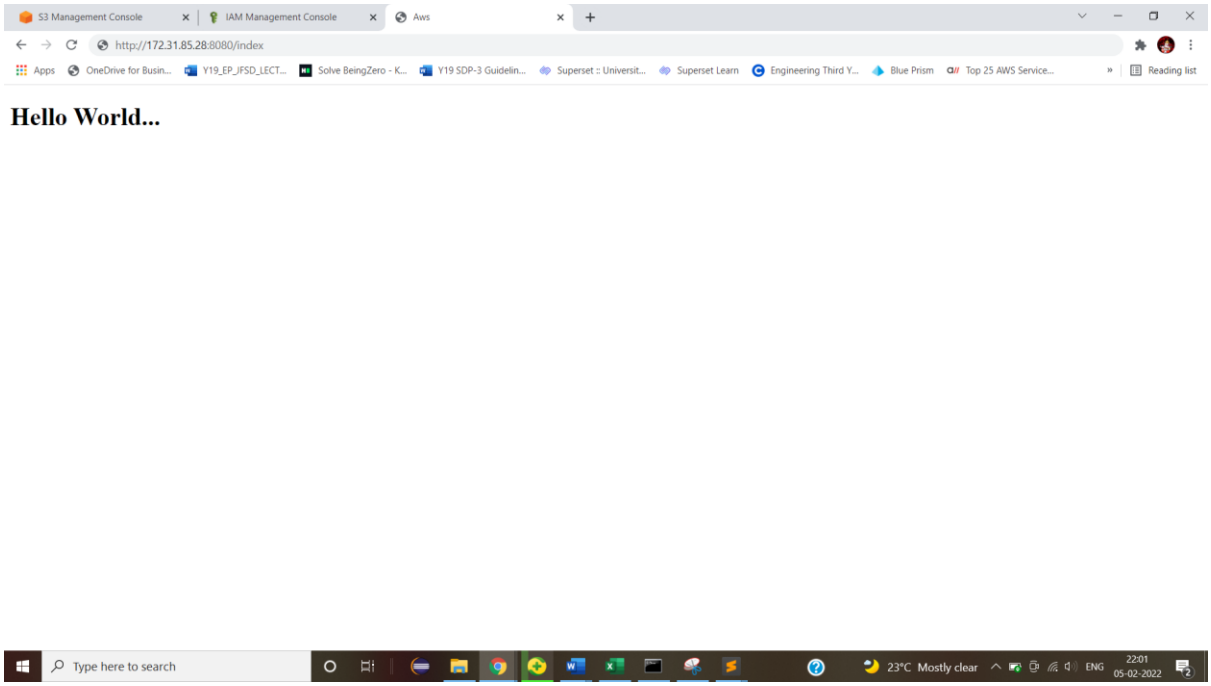

ap-south-1.console.aws.amazon.com/ec2/v2/home?region=ap-south-1#LaunchInstanceWizard:
Search for services, features, blogs, docs, and more [Alt+S]
Mumbai
Sravani_677
allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance. Amazon EC2 supports ED25519 and RSA key pair types.
Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI.
Create a new key pair
Key pair type
RSA ED25519
Key pair name
lab5
Download Key Pair
You have to download the private key file (*.pem file) before you can continue. Store it in a secure and accessible location. You will not be able to download the file again after it's created.
Cancel
Launch Instances
Security group name
Description
Type
SSH
Instance Details
Storage
Edit instance details
Edit storage
Cancel
Previous
Launch
Feedback
English (US)
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences
lab5.pem
Show all
Type here to search
26°C Haze
ENG
14:18
05-02-2022


ap-south-1.console.aws.amazon.com/ec2/v2/home?region=ap-south-1#Instances:
Search for services, features, blogs, docs, and more [Alt+S]
Mumbai
Sravani_677
Instances (1/1) Info
Connect
Instance state
Actions
Launch instances
Search
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zone
i-0dac8a87a6c5affe7
Running
t2.micro
2/2 checks passed
No alarms
ap-south-1b
Instance: i-0dac8a87a6c5affe7
Details
Security
Networking
Storage
Status checks
Monitoring
Tags
Instance summary Info
Instance ID
Public IPv4 address
Private IPv4 addresses
Feedback
English (US)
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences
lab5.pem
Show all
Type here to search
26°C Haze
ENG
14:21
05-02-2022

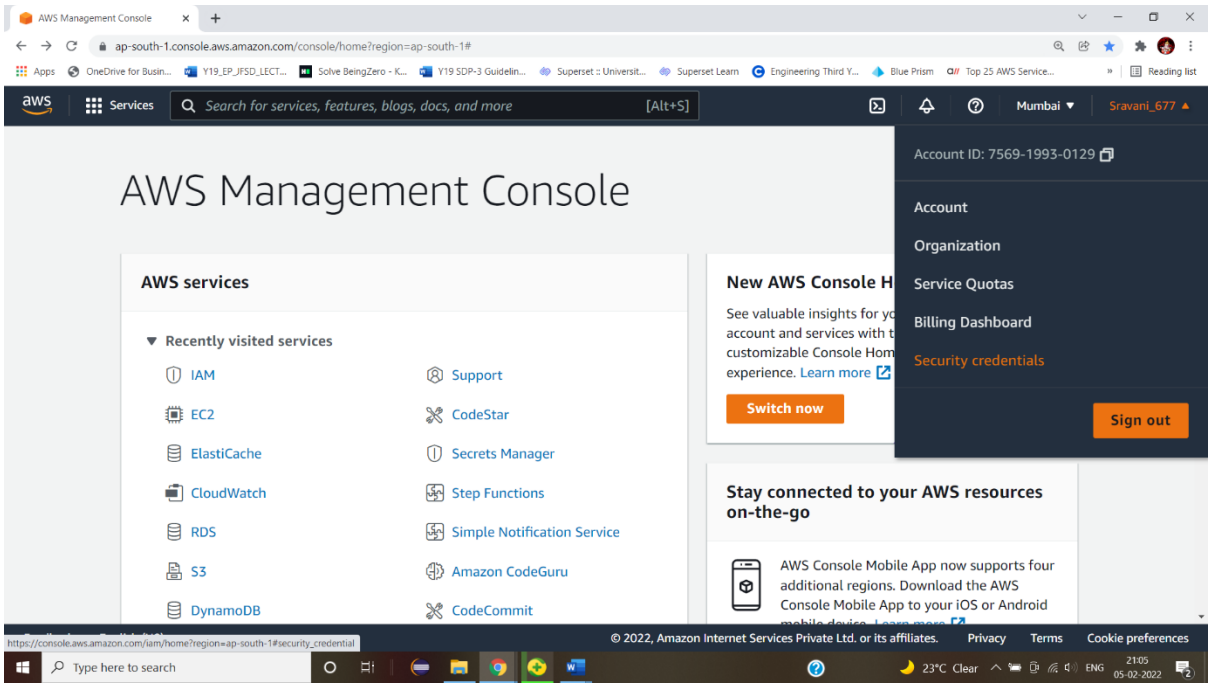
```
Last login: Sat Feb  5 08:53:46 2022 from ec2-18-206-107-24.compute-1.amazonaws.com

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

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-172-31-87-210 ~]$ wget https://adcskill51.s3.amazonaws.com/dynamodb.zip
--2022-02-05 08:55:34--  https://adcskill51.s3.amazonaws.com/dynamodb.zip
Resolving adcskill51.s3.amazonaws.com (adcskill51.s3.amazonaws.com)... 52.216.200.91
Connecting to adcskill51.s3.amazonaws.com (adcskill51.s3.amazonaws.com)|52.216.200.91|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1249347 (1.2M) [application/zip]
Saving to: 'dynamodb.zip'

100%[=======================================================================================================>] 1,249,347   --.-K/s   in 0.05s

2022-02-05 08:55:34 (23.5 MB/s) - 'dynamodb.zip' saved [1249347/1249347]

[ec2-user@ip-172-31-87-210 ~]$
```

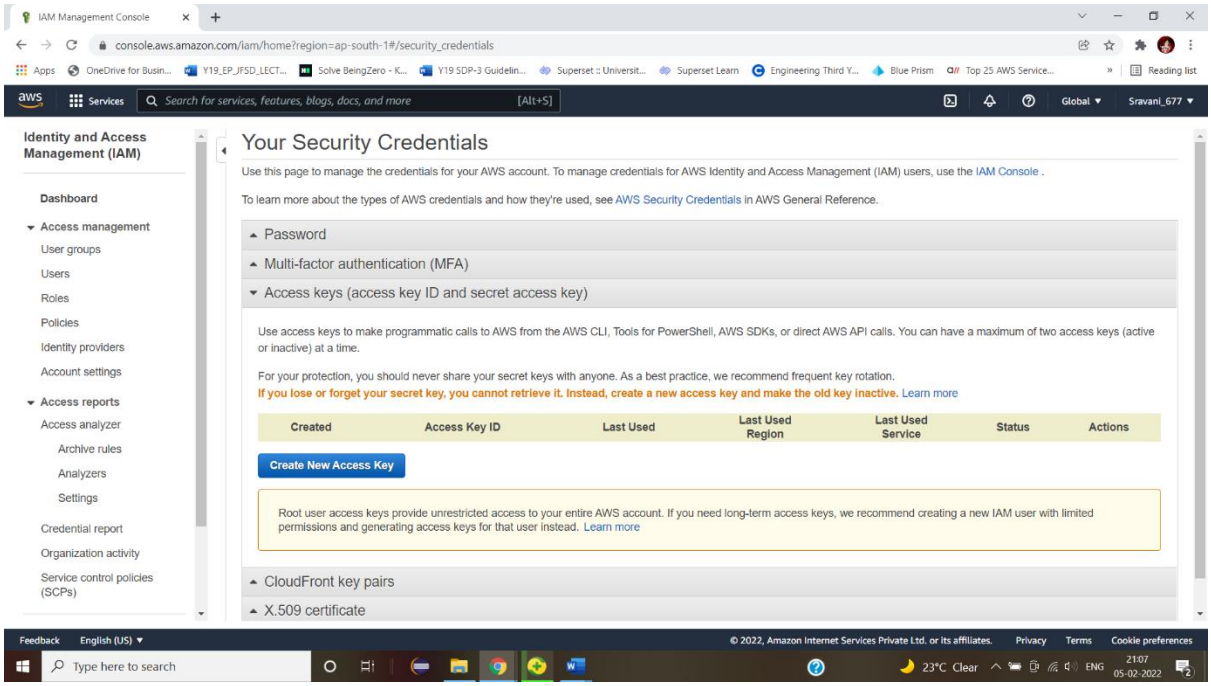
```
[ec2-user@ip-172-31-87-210 ~]$ pip3 install flask
Defaulting to user installation because normal site-packages is not writeable
Collecting flask
  Downloading Flask-2.0.2-py3-none-any.whl (95 kB)
     |████████████████████████████████| 95 kB 5.7 MB/s
Collecting Jinja2>=3.0
  Downloading Jinja2-3.0.3-py3-none-any.whl (133 kB)
     |████████████████████████████████| 133 kB 31.4 MB/s
Collecting itsdangerous>=2.0
  Downloading itsdangerous-2.0.1-py3-none-any.whl (18 kB)
Collecting click>=7.1.2
  Downloading click-8.0.3-py3-none-any.whl (97 kB)
     |████████████████████████████████| 97 kB 10.8 MB/s
Collecting Werkzeug>=2.0
  Downloading Werkzeug-2.0.2-py3-none-any.whl (288 kB)
     |████████████████████████████████| 288 kB 33.2 MB/s
Collecting MarkupSafe>=2.0
  Downloading MarkupSafe-2.0.1-cp37-cp37m-manylinux2010_x86_64.whl (31 kB)
Collecting importlib-metadata; python_version < "3.8"
  Downloading importlib_metadata-4.10.1-py3-none-any.whl (17 kB)
Collecting typing-extensions>=3.6.4; python_version < "3.8"
  Downloading typing_extensions-4.0.1-py3-none-any.whl (22 kB)
Collecting zipp>=0.5
  Downloading zipp-3.7.0-py3-none-any.whl (5.3 kB)
Installing collected packages: MarkupSafe, Jinja2, itsdangerous, typing-extensions, zipp, importlib-metadata, click, Werkzeug, flask
Successfully installed Jinja2-3.0.3 MarkupSafe-2.0.1 Werkzeug-2.0.2 click-8.0.3 flask-2.0.2 importlib-metadata-4.10.1 itsdangerous-2.0.1 typing-
.1 zipp-3.7.0
[ec2-user@ip-172-31-87-210 ~]$ pip3 install boto3
```

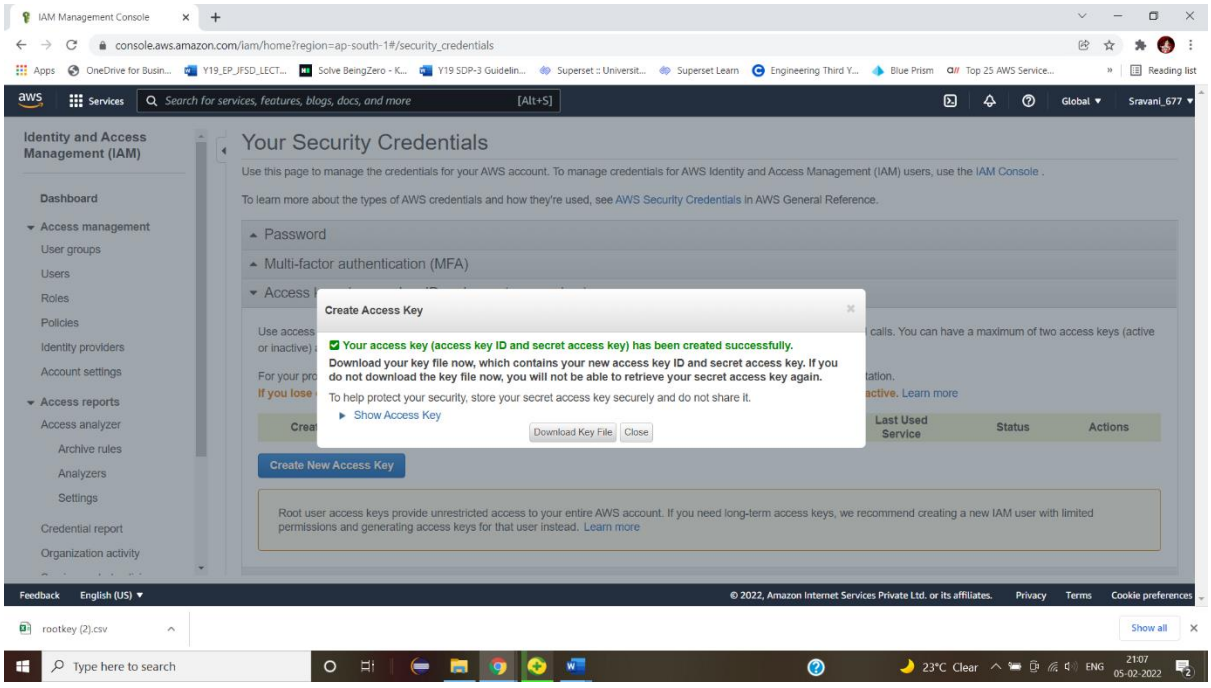
```
  GNU nano 2.9.8                                                  task.py

from flask import Flask, render_template, request
import boto3
from botocore.exceptions import ClientError
#import sqlite3 as db;

app = Flask(__name__)

dynamodb = boto3.resource('dynamodb', endpoint_url="http://dynamodb.us-east-1.amazonaws.com")
@app.route('/index')
@app.route('/')
def hello():
        return "Hello world!";
if __name__ == "__main__":
        app.run (debug = True, host='0.0.0.0', port=8080);
```

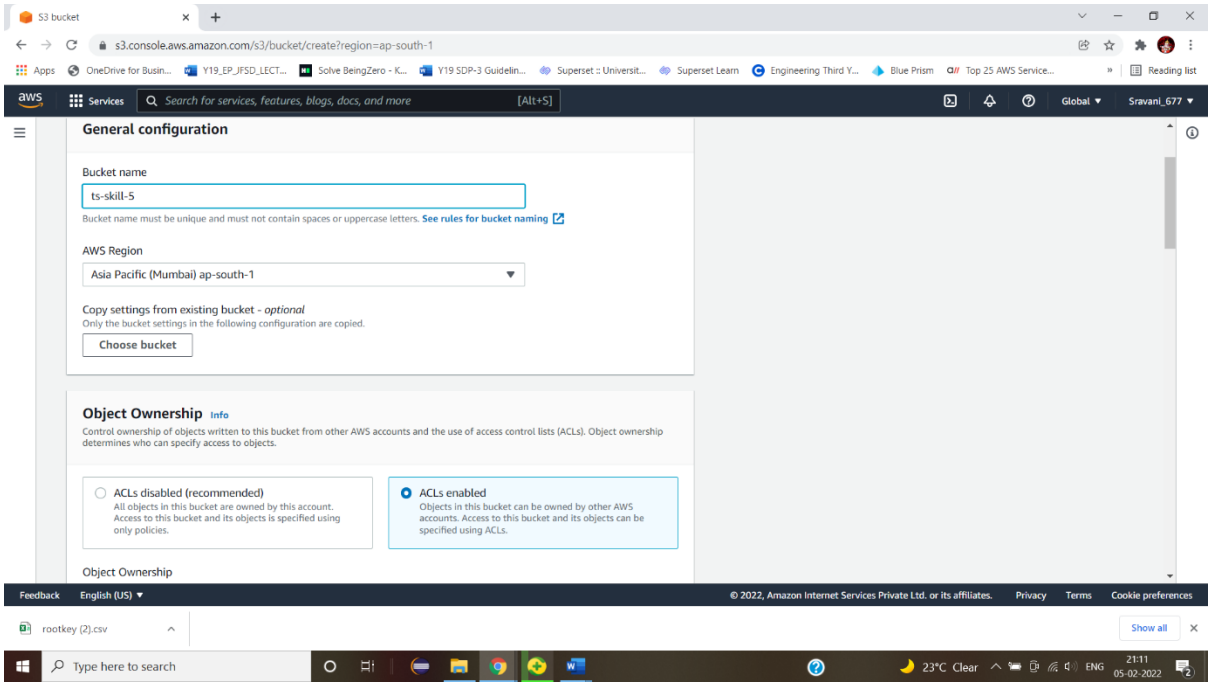


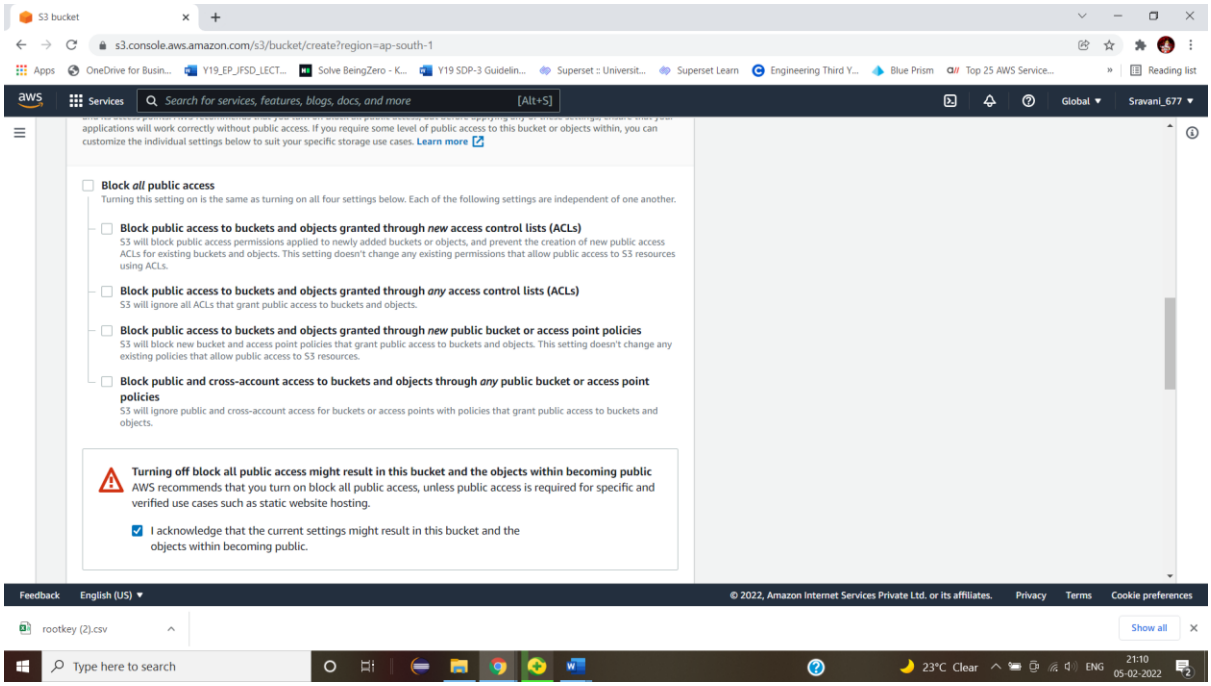

Create AWS Lamda serverless compute and use S3 bucket to trigger the Lamda function, do some operation in the Lamda function and record the logs in AWS CloudWatch.

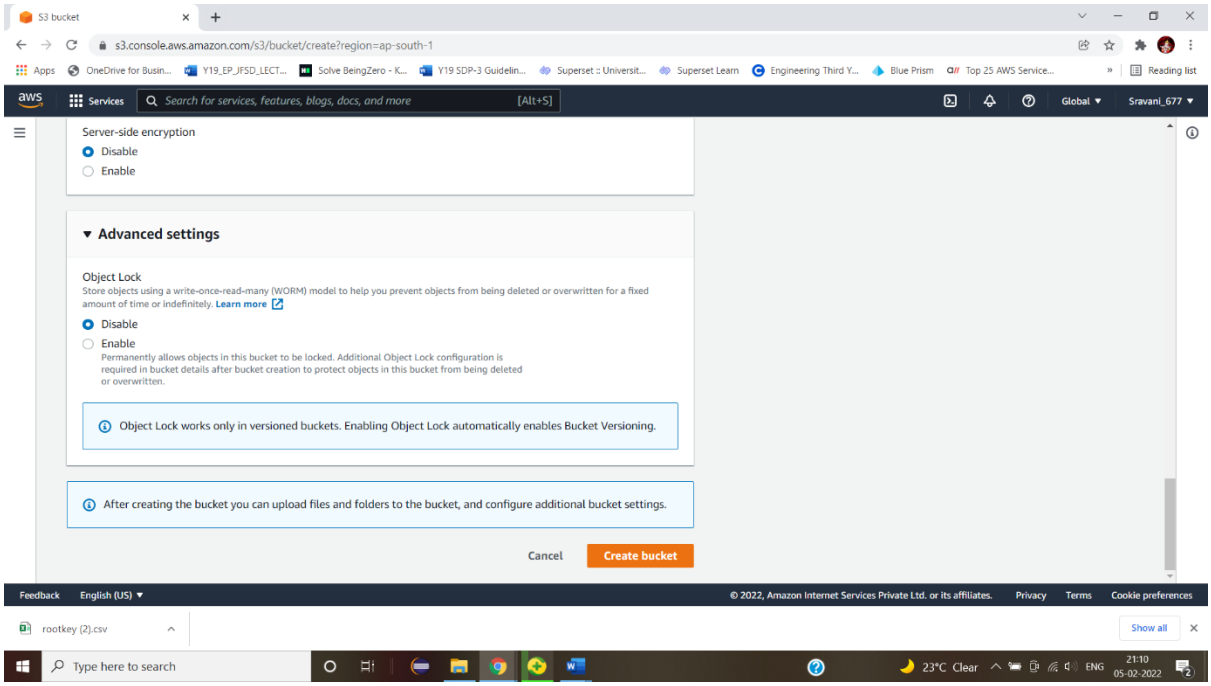


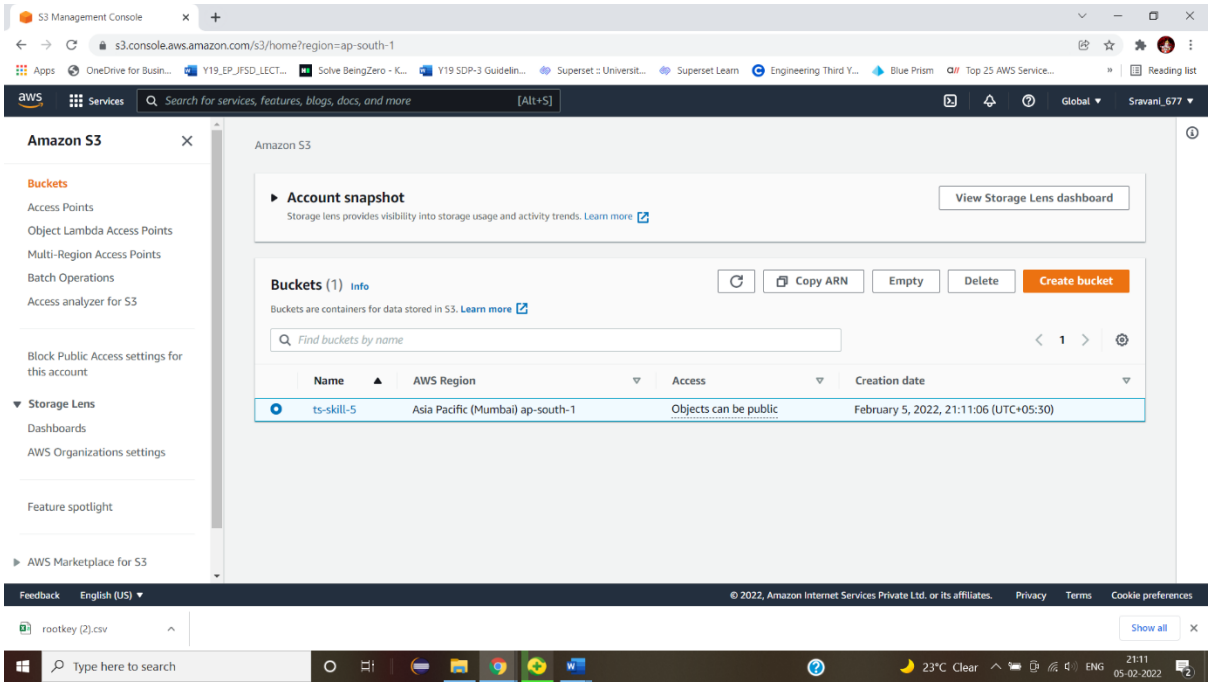

IAM Management Console
console.aws.amazon.com/iam/home?region=ap-south-1#/security_credentials
Services
Search for services, features, blogs, docs, and more
[Alt+S]
Global
Sravani_677
Identity and Access Management (IAM)
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access analyzer
Archive rules
Analyzers
Settings
Credential report
Organization activity
Service control policies (SCPs)
Your Security Credentials
Use this page to manage the credentials for your AWS account. To manage credentials for AWS Identity and Access Management (IAM) users, use the IAM Console .
To learn more about the types of AWS credentials and how they're used, see AWS Security Credentials in AWS General Reference.
Password
Multi-factor authentication (MFA)
Access keys (access key ID and secret access key)
Use access keys to make programmatic calls to AWS from the AWS CLI, Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time.
For your protection, you should never share your secret keys with anyone. As a best practice, we recommend frequent key rotation.
If you lose or forget your secret key, you cannot retrieve it. Instead, create a new access key and make the old key inactive. Learn more
Created
Access Key ID
Last Used
Last Used Region
Last Used Service
Status
Actions
Create New Access Key
Root user access keys provide unrestricted access to your entire AWS account. If you need long-term access keys, we recommend creating a new IAM user with limited permissions and generating access keys for that user instead. Learn more
CloudFront key pairs
X.509 certificate
Feedback
English (US)
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
23°C Clear
ENG
21:07
05-02-2022

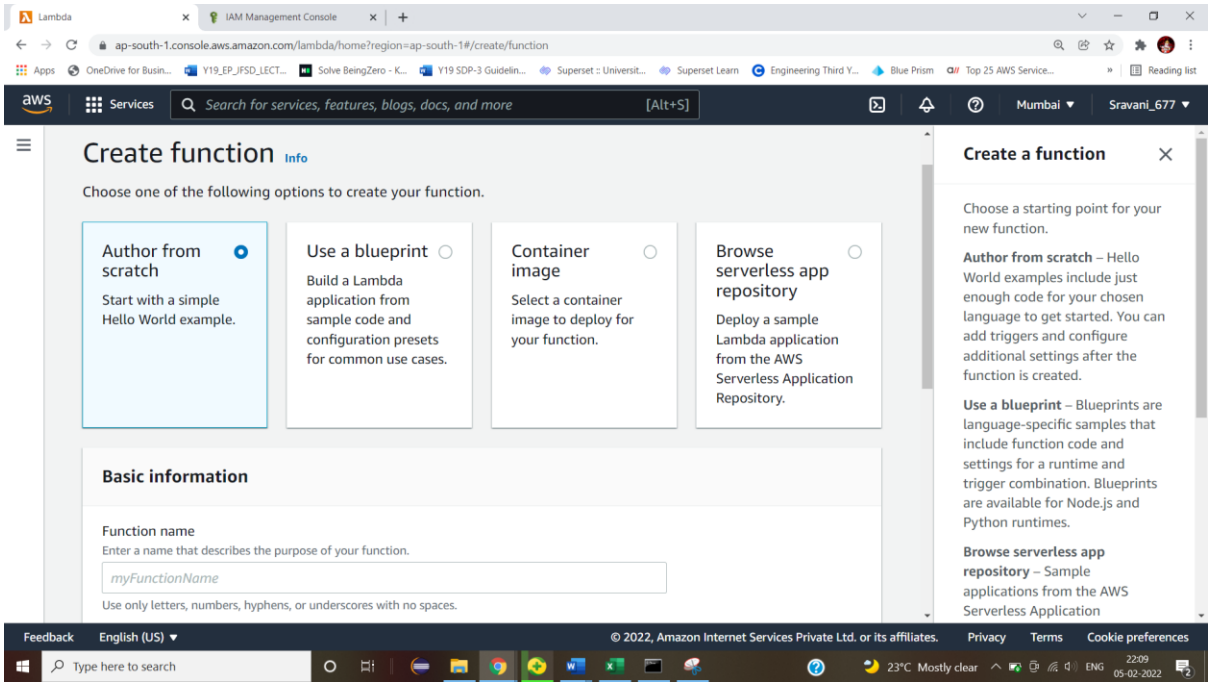

IAM Management Console
console.aws.amazon.com/iam/home?region=ap-south-1#/security_credentials
Identity and Access Management (IAM)
Your Security Credentials
Create Access Key
Your access key (access key ID and secret access key) has been created successfully.
Download your key file now, which contains your new access key ID and secret access key. If you do not download the key file now, you will not be able to retrieve your secret access key again.
To help protect your security, store your secret access key securely and do not share it.
Show Access Key
Download Key File
Close
Create New Access Key
Root user access keys provide unrestricted access to your entire AWS account. If you need long-term access keys, we recommend creating a new IAM user with limited permissions and generating access keys for that user instead. Learn more
Feedback
English (US)
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences
rootkey (2).csv
Show all
Type here to search
23°C Clear
ENG
21:07
05-02-2022

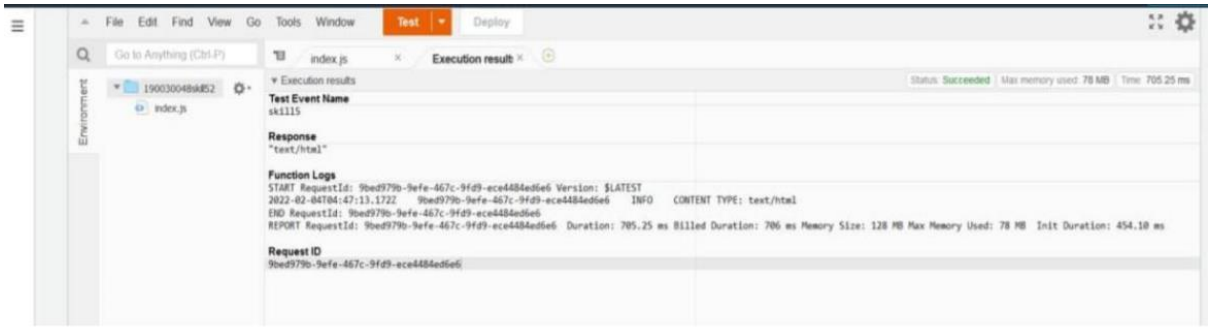

S3 bucket
s3.console.aws.amazon.com/s3/bucket/create?region=ap-south-1
Services
Search for services, features, blogs, docs, and more [Alt+S]
Global
Sravani_677
General configuration
Bucket name
ts-skill-5
Bucket name must be unique and must not contain spaces or uppercase letters. See rules for bucket naming
AWS Region
Asia Pacific (Mumbai) ap-south-1
Copy settings from existing bucket - optional
Only the bucket settings in the following configuration are copied.
Choose bucket
Object Ownership Info
Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.
ACLs disabled (recommended)
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.
ACLs enabled
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.
Object Ownership
Feedback
English (US)
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences
rootkey (2).csv
Show all
Type here to search
23°C Clear
ENG
21:11
05-02-2022

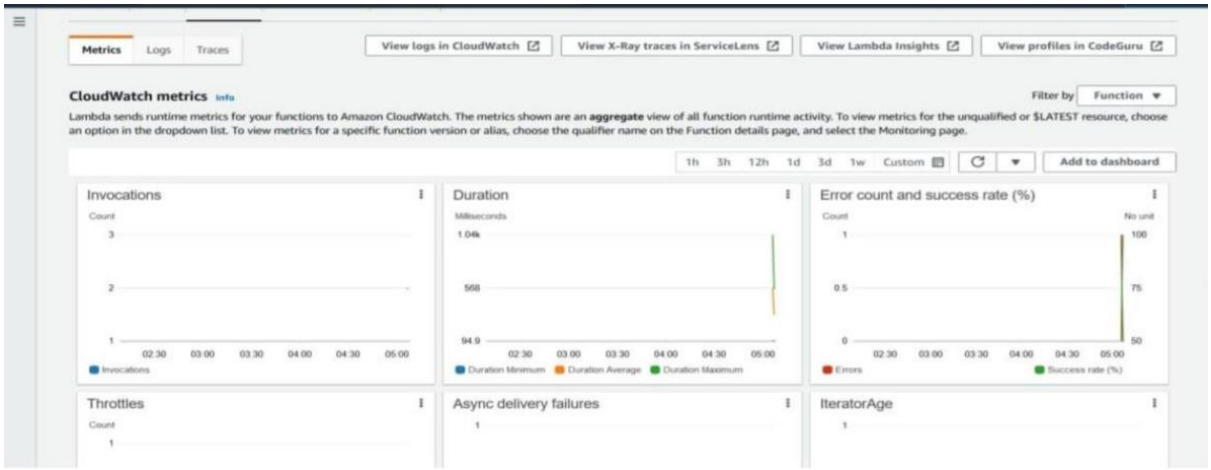

S3 bucket
s3.console.aws.amazon.com/s3/bucket/create?region=ap-south-1
Services
Search for services, features, blogs, docs, and more [Alt+S]
Global
Sravani_677
applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more
Block all public access
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.
Block public access to buckets and objects granted through new access control lists (ACLs)
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
Block public access to buckets and objects granted through any access control lists (ACLs)
S3 will ignore all ACLs that grant public access to buckets and objects.
Block public access to buckets and objects granted through new public bucket or access point policies
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
Block public and cross-account access to buckets and objects through any public bucket or access point policies
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.
Turning off block all public access might result in this bucket and the objects within becoming public
AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.
I acknowledge that the current settings might result in this bucket and the objects within becoming public.
Feedback
English (US)
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences
rootkey (2).csv
Show all
Type here to search
23°C Clear
ENG
21:10
05-02-2022


S3 bucket
s3.console.aws.amazon.com/s3/bucket/create?region=ap-south-1
Server-side encryption
Disable
Enable
Advanced settings
Object Lock
Store objects using a write-once-read-many (WORM) model to help you prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely. Learn more
Disable
Enable
Permanently allows objects in this bucket to be locked. Additional Object Lock configuration is required in bucket details after bucket creation to protect objects in this bucket from being deleted or overwritten.
Object Lock works only in versioned buckets. Enabling Object Lock automatically enables Bucket Versioning.
After creating the bucket you can upload files and folders to the bucket, and configure additional bucket settings.
Cancel
Create bucket
Feedback
English (US)
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences
rootkey (2).csv
Show all
Type here to search
23°C Clear
ENG
21:10
05-02-2022


S3 Management Console
s3.console.aws.amazon.com/s3/home?region=ap-south-1
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
Account snapshot
Storage lens provides visibility into storage usage and activity trends. Learn more
View Storage Lens dashboard
Buckets (1) Info
Buckets are containers for data stored in S3. Learn more
Copy ARN
Empty
Delete
Create bucket
Find buckets by name
Name
AWS Region
Access
Creation date
ts-skill-5
Asia Pacific (Mumbai) ap-south-1
Objects can be public
February 5, 2022, 21:11:06 (UTC+05:30)
Feedback
English (US)
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences
rootkey (2).csv
Show all
Type here to search
23°C Clear
ENG
21:11
05-02-2022


Lambda
IAM Management Console
ap-south-1.console.aws.amazon.com/lambda/home?region=ap-south-1#/create/function
Services
Search for services, features, blogs, docs, and more [Alt+S]
Mumbai
Sravani_677
Create function Info
Choose one of the following options to create your function.
Author from scratch
Start with a simple Hello World example.
Use a blueprint
Build a Lambda application from sample code and configuration presets for common use cases.
Container image
Select a container image to deploy for your function.
Browse serverless app repository
Deploy a sample Lambda application from the AWS Serverless Application Repository.
Basic information
Function name
Enter a name that describes the purpose of your function.
myFunctionName
Use only letters, numbers, hyphens, or underscores with no spaces.
Create a function
Choose a starting point for your new function.
Author from scratch – Hello World examples include just enough code for your chosen language to get started. You can add triggers and configure additional settings after the function is created.
Use a blueprint – Blueprints are language-specific samples that include function code and settings for a runtime and trigger combination. Blueprints are available for Node.js and Python runtimes.
Browse serverless app repository – Sample applications from the AWS Serverless Application
Feedback
English (US)
© 2022, Amazon Internet Services Private Ltd. or its affiliates.
Privacy
Terms
Cookie preferences
Type here to search
23°C Mostly clear
ENG
22:09
05-02-2022


File Edit Find View Go Tools Window
Test
Deploy
Execution result
Execution results
Test Event Name
sk1115
Response
"text/html"
Function Logs
START RequestId: 9bed979b-9efe-467c-9fd9-ece4484ed6e6 Version: $LATEST
2022-02-04T04:47:13.172Z 9bed979b-9efe-467c-9fd9-ece4484ed6e6 INFO CONTENT TYPE: text/html
END RequestId: 9bed979b-9efe-467c-9fd9-ece4484ed6e6
REPORT RequestId: 9bed979b-9efe-467c-9fd9-ece4484ed6e6 Duration: 705.25 ms Billed Duration: 706 ms Memory Size: 128 MB Max Memory Used: 78 MB Init Duration: 454.10 ms
Request ID
9bed979b-9efe-467c-9fd9-ece4484ed6e6


Metrics
Logs
Traces
View logs in CloudWatch
View X-Ray traces in ServiceLens
View Lambda Insights
View profiles in CodeGuru
CloudWatch metrics Info
Lambda sends runtime metrics for your functions to Amazon CloudWatch. The metrics shown are an aggregate view of all function runtime activity. To view metrics for the unqualified or $LATEST resource, choose an option in the dropdown list. To view metrics for a specific function version or alias, choose the qualifier name on the Function details page, and select the Monitoring page.
Filter by Function
1h 3h 12h 1d 3d 1w Custom
Add to dashboard
Invocations
Duration
Error count and success rate (%)
Throttles
Async delivery failures
IteratorAge