Q2.

Create new directory

Mkdir newdir

Rename an existing directory with new name

Mv newdir directory1

Move an Existing directory to new location

Mv directory1 snap

Delete an existing directory

Rmdir directory1

Rmdir snap

Create a new file in specified directory with specified name and give read write permission to user and group

Mkdir dir1

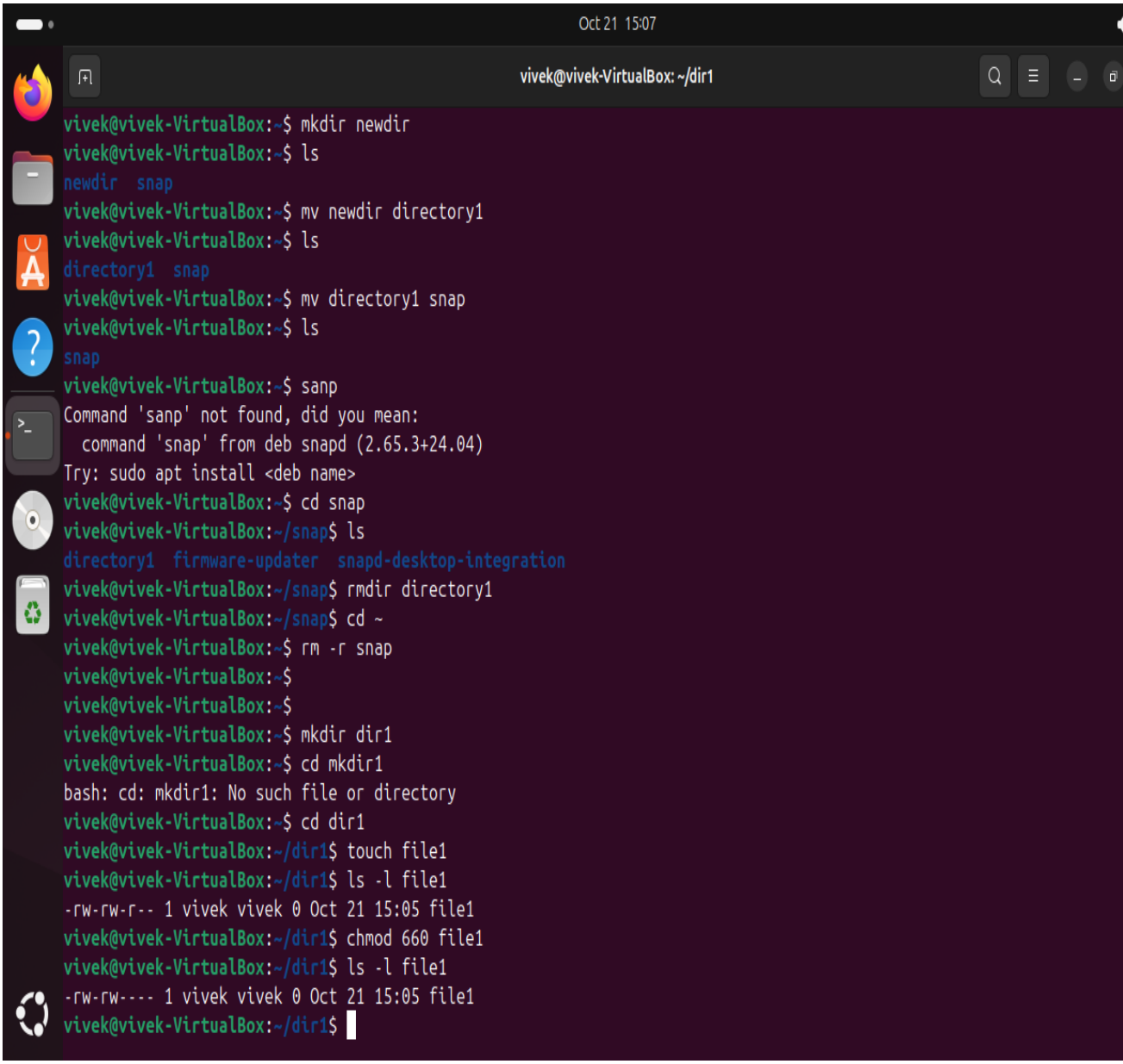
Cd dir1

Touch file1

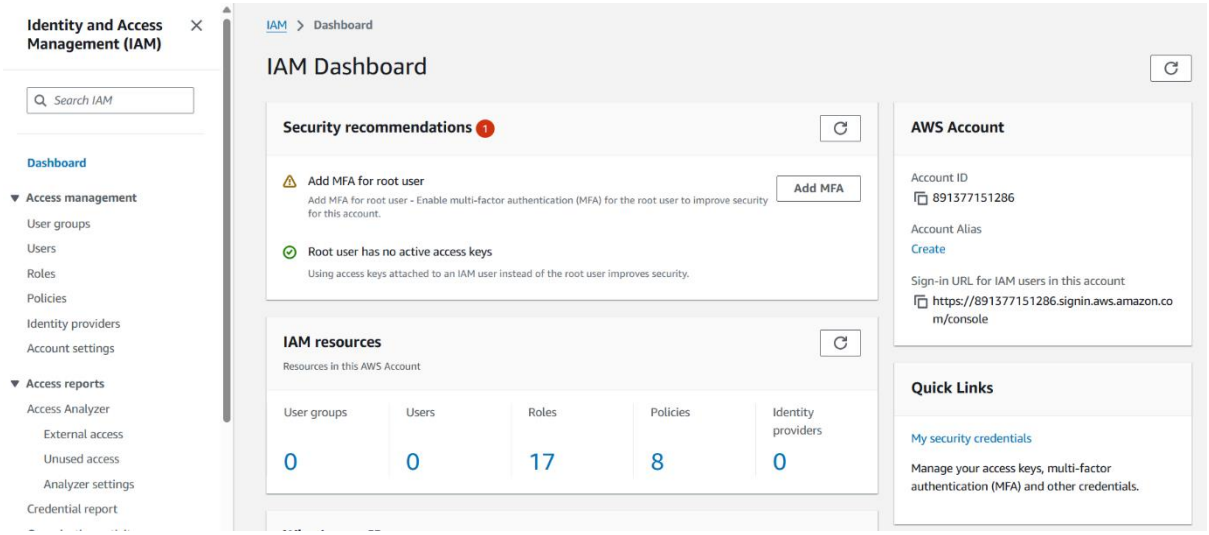
Ls -l file1

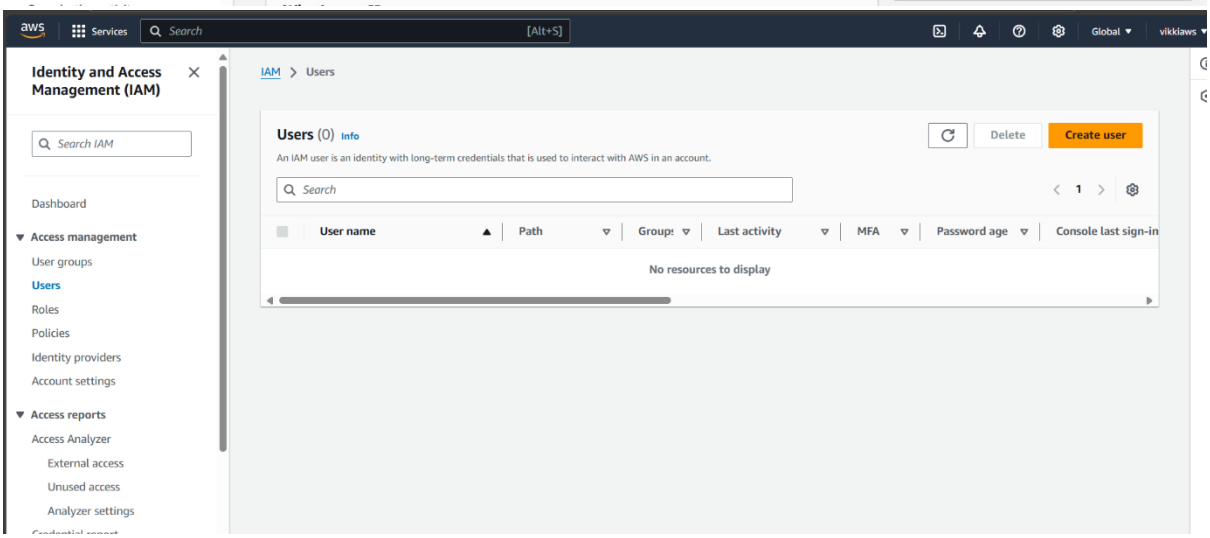
Chmod 660 file1

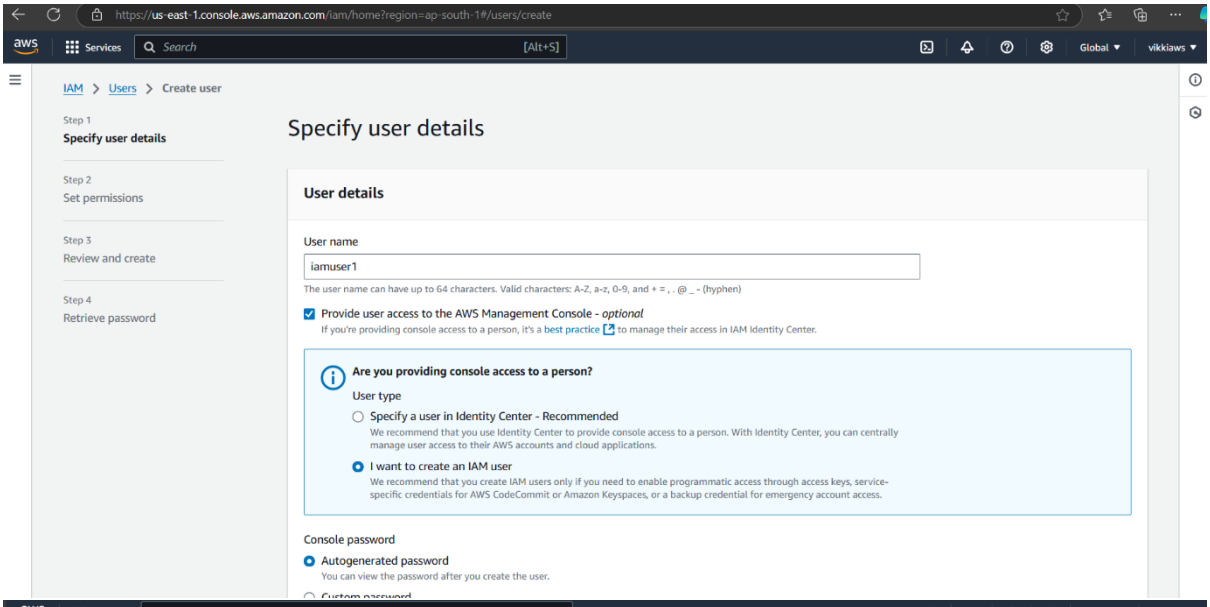
Ls -l file

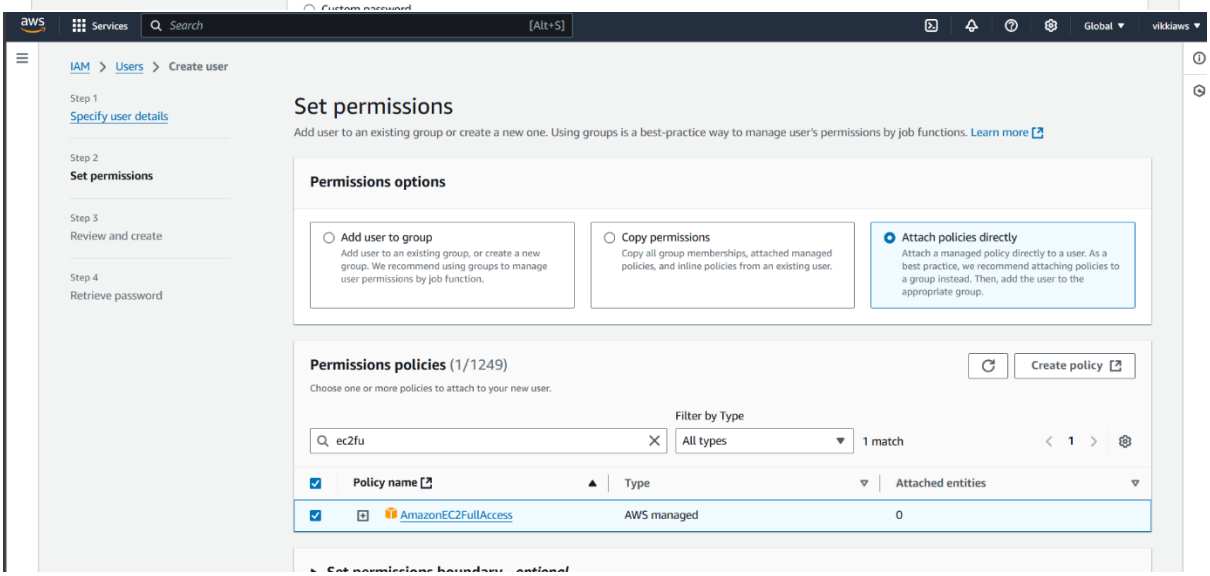

Oct 21 15:07
vivek@vivek-VirtualBox: ~/dir1
vivek@vivek-VirtualBox:~$ mkdir newdir
vivek@vivek-VirtualBox:~$ ls
newdir snap
vivek@vivek-VirtualBox:~$ mv newdir directory1
vivek@vivek-VirtualBox:~$ ls
directory1 snap
vivek@vivek-VirtualBox:~$ mv directory1 snap
vivek@vivek-VirtualBox:~$ ls
snap
vivek@vivek-VirtualBox:~$ sanp
Command 'sanp' not found, did you mean:
  command 'snap' from deb snapd (2.65.3+24.04)
Try: sudo apt install <deb name>
vivek@vivek-VirtualBox:~$ cd snap
vivek@vivek-VirtualBox:~/snap$ ls
directory1 firmware-updater snapd-desktop-integration
vivek@vivek-VirtualBox:~/snap$ rmdir directory1
vivek@vivek-VirtualBox:~/snap$ cd ~
vivek@vivek-VirtualBox:~$ rm -r snap
vivek@vivek-VirtualBox:~$
vivek@vivek-VirtualBox:~$
vivek@vivek-VirtualBox:~$ mkdir dir1
vivek@vivek-VirtualBox:~$ cd mkdir1
bash: cd: mkdir1: No such file or directory
vivek@vivek-VirtualBox:~$ cd dir1
vivek@vivek-VirtualBox:~/dir1$ touch file1
vivek@vivek-VirtualBox:~/dir1$ ls -l file1
-rw-rw-r-- 1 vivek vivek 0 Oct 21 15:05 file1
vivek@vivek-VirtualBox:~/dir1$ chmod 660 file1
vivek@vivek-VirtualBox:~/dir1$ ls -l file1
-rw-rw---- 1 vivek vivek 0 Oct 21 15:05 file1
vivek@vivek-VirtualBox:~/dir1$

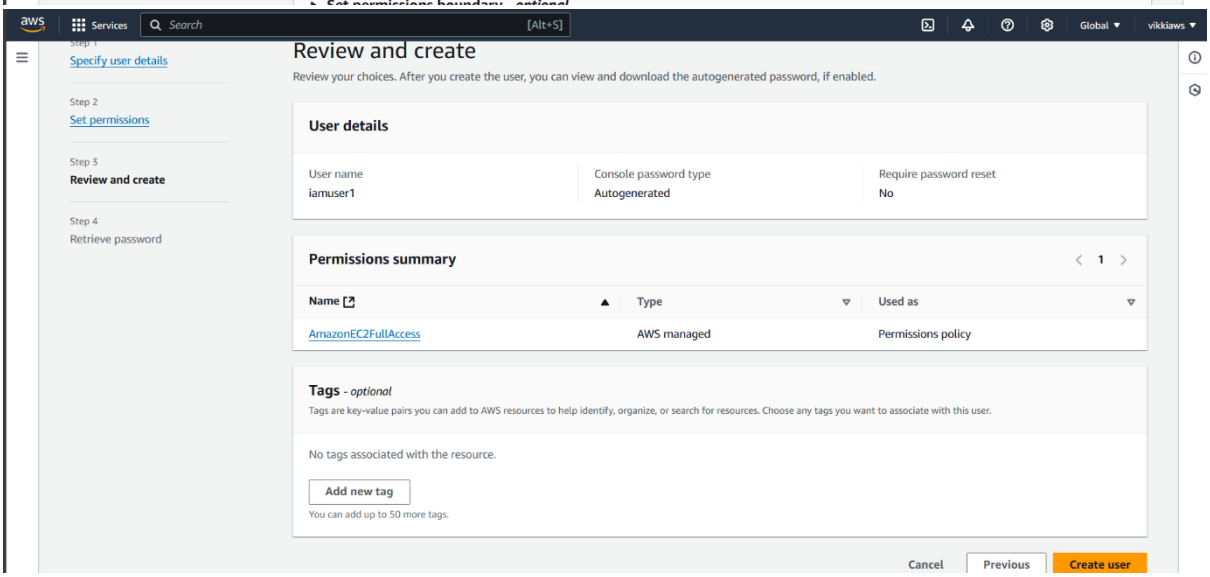
Q2.Cloud
a.

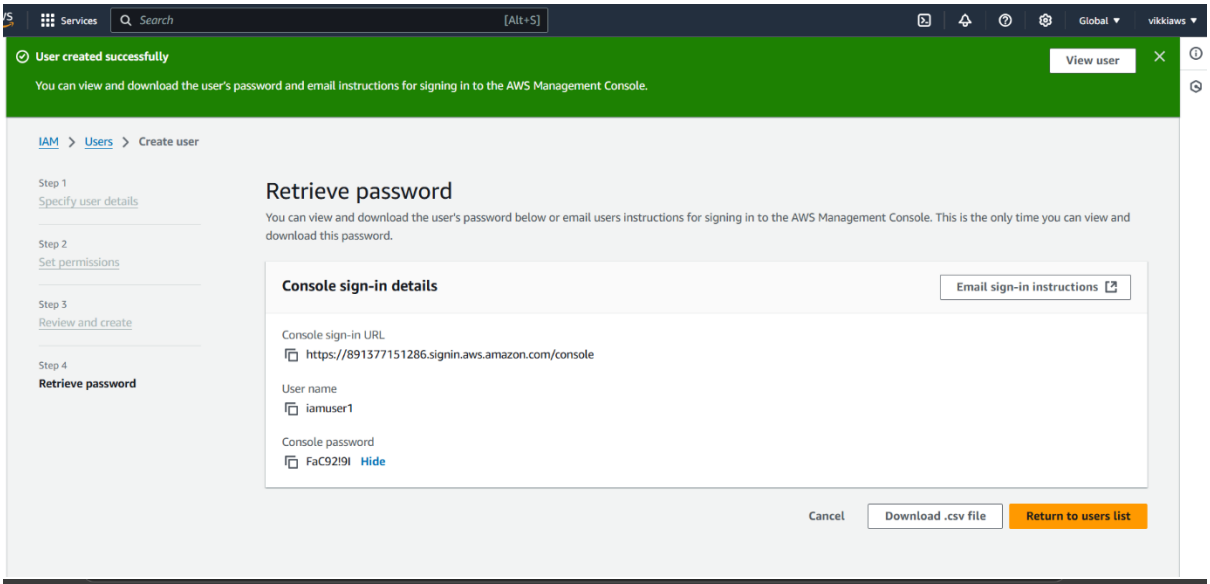

Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
IAM > Dashboard
IAM Dashboard
Security recommendations 1
Add MFA for root user
Add MFA for root user - Enable multi-factor authentication (MFA) for the root user to improve security for this account.
Add MFA
Root user has no active access keys
Using access keys attached to an IAM user instead of the root user improves security.
IAM resources
Resources in this AWS Account
User groups 0
Users 0
Roles 17
Policies 8
Identity providers 0
AWS Account
Account ID
891377151286
Account Alias
Create
Sign-in URL for IAM users in this account
https://891377151286.signin.aws.amazon.com/console
Quick Links
My security credentials
Manage your access keys, multi-factor authentication (MFA) and other credentials.

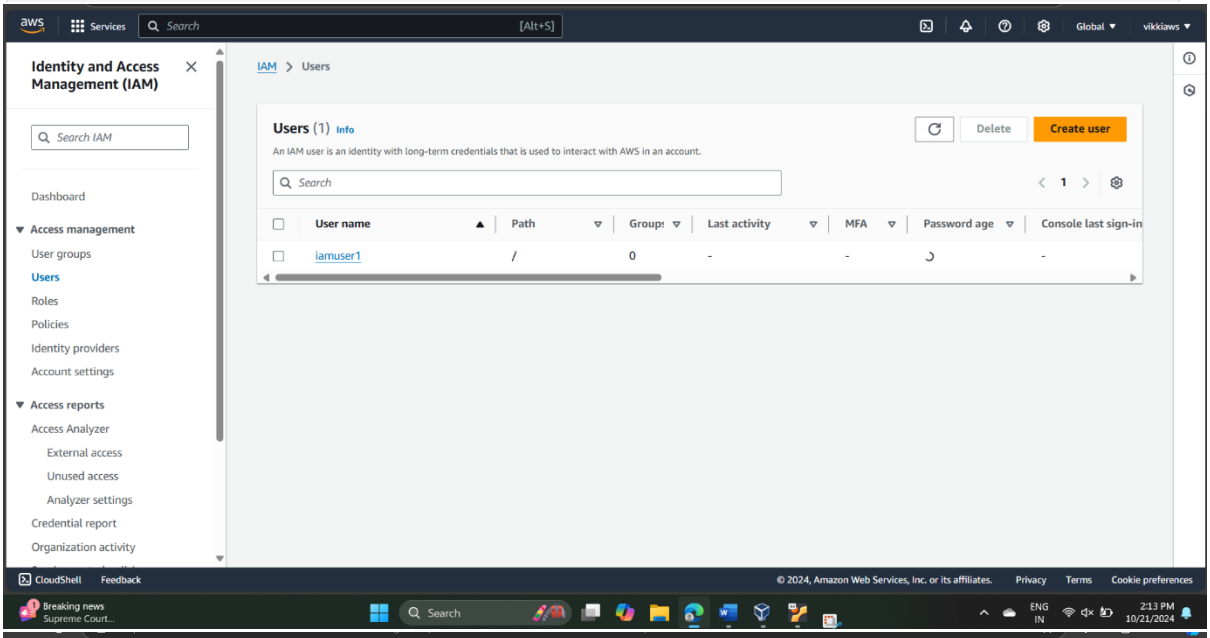

aws
Services
Search
[Alt+S]
Global
vikkiaws
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
IAM > Users
Users (0) Info
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.
Delete
Create user
Search
User name
Path
Groups
Last activity
MFA
Password age
Console last sign-in
No resources to display

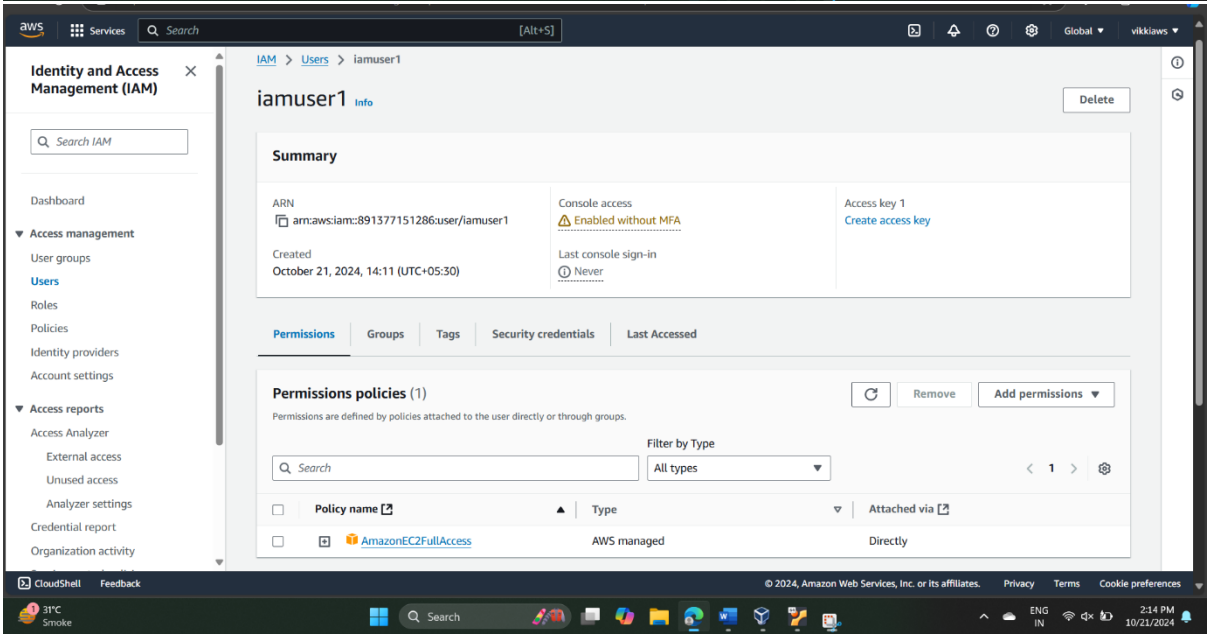

https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/users/create
aws
Services
Search
[Alt+S]
Global
vikkiaws
IAM > Users > Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
Specify user details
User details
User name
iamuser1
The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)
Provide user access to the AWS Management Console - optional
If you're providing console access to a person, it's a best practice to manage their access in IAM Identity Center.
Are you providing console access to a person?
User type
Specify a user in Identity Center - Recommended
We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications.
I want to create an IAM user
We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AWS CodeCommit or Amazon Keyspaces, or a backup credential for emergency account access.
Console password
Autogenerated password
You can view the password after you create the user.

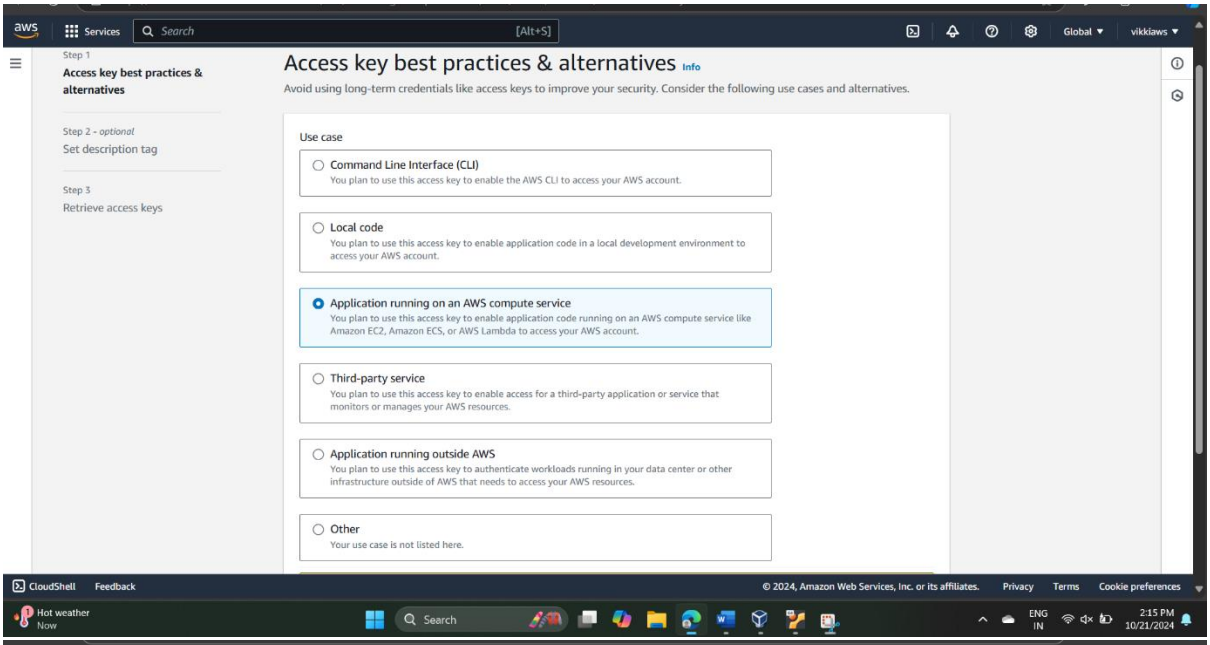

aws
Services
Search
[Alt+S]
Global
vikkiaws
IAM > Users > Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
Set permissions
Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. Learn more
Permissions options
Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.
Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.
Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.
Permissions policies (1/1249)
Choose one or more policies to attach to your new user.
Create policy
Filter by Type
ec2fu
All types
1 match
Policy name
Type
Attached entities
AmazonEC2FullAccess
AWS managed
0

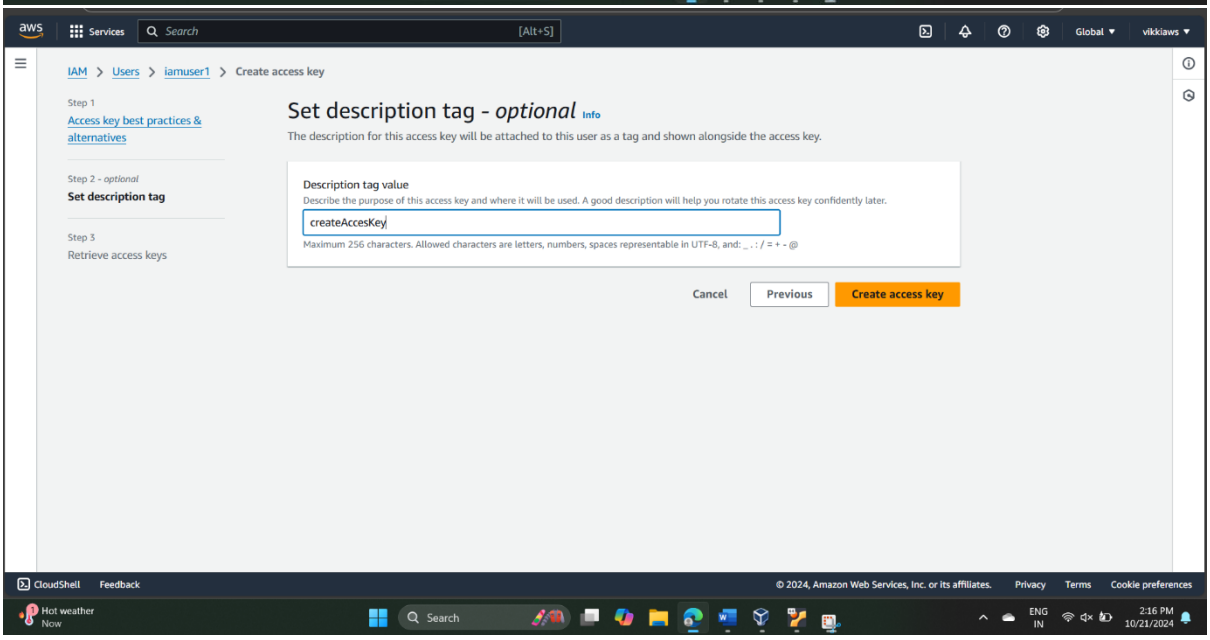

aws
Services
Search
[Alt+S]
Global
vikkiaws
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
Review and create
Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.
User details
User name
iamuser1
Console password type
Autogenerated
Require password reset
No
Permissions summary
Name
Type
Used as
AmazonEC2FullAccess
AWS managed
Permissions policy
Tags - optional
Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.
No tags associated with the resource.
Add new tag
You can add up to 50 more tags.
Cancel
Previous
Create user

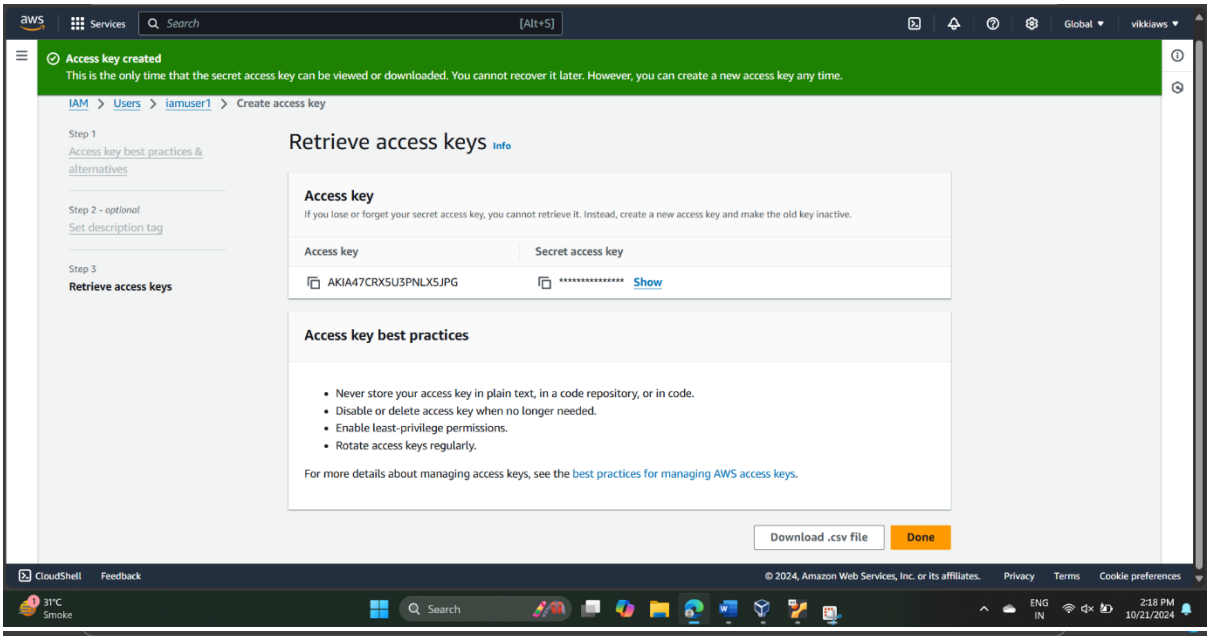

Services
Search
[Alt+S]
Global
vikkiaws
User created successfully
You can view and download the user's password and email instructions for signing in to the AWS Management Console.
View user
IAM > Users > Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Step 4
Retrieve password
Retrieve password
You can view and download the user's password below or email users instructions for signing in to the AWS Management Console. This is the only time you can view and download this password.
Console sign-in details
Email sign-in instructions
Console sign-in URL
https://891377151286.signin.aws.amazon.com/console
User name
iamuser1
Console password
FaC92!9I Hide
Cancel
Download .csv file
Return to users list

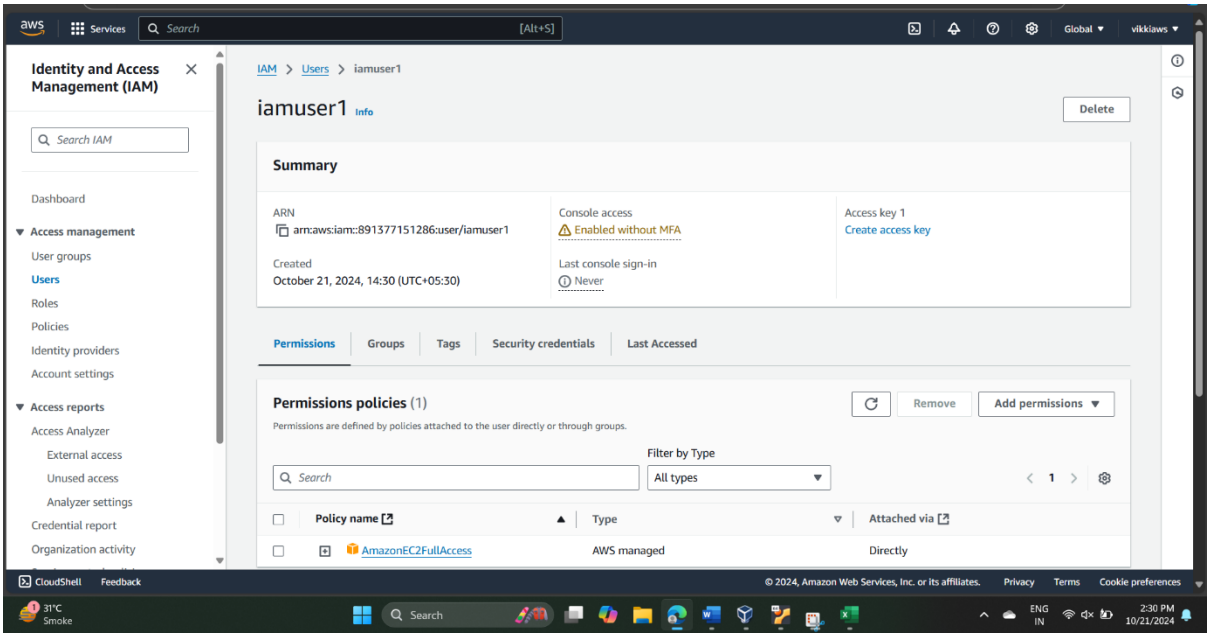

Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
Organization activity
IAM > Users
Users (1) Info
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.
Delete
Create user
Search
User name
Path
Group
Last activity
MFA
Password age
Console last sign-in
iamuser1
/
0
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

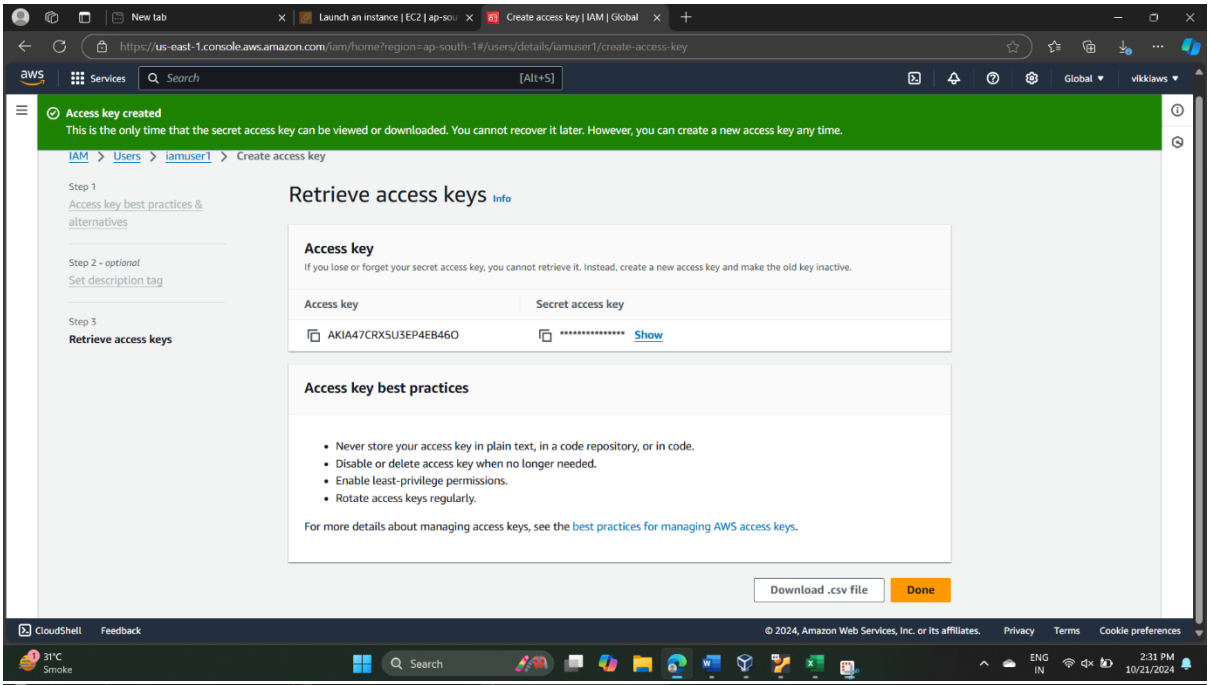

Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
Organization activity
IAM > Users > iamuser1
iamuser1 Info
Delete
Summary
ARN
arn:aws:iam::891377151286:user/iamuser1
Console access
Enabled without MFA
Access key 1
Create access key
Created
October 21, 2024, 14:11 (UTC+05:30)
Last console sign-in
Never
Permissions
Groups
Tags
Security credentials
Last Accessed
Permissions policies (1)
Permissions are defined by policies attached to the user directly or through groups.
Remove
Add permissions
Filter by Type
All types
Search
Policy name
Type
Attached via
AmazonEC2FullAccess
AWS managed
Directly
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

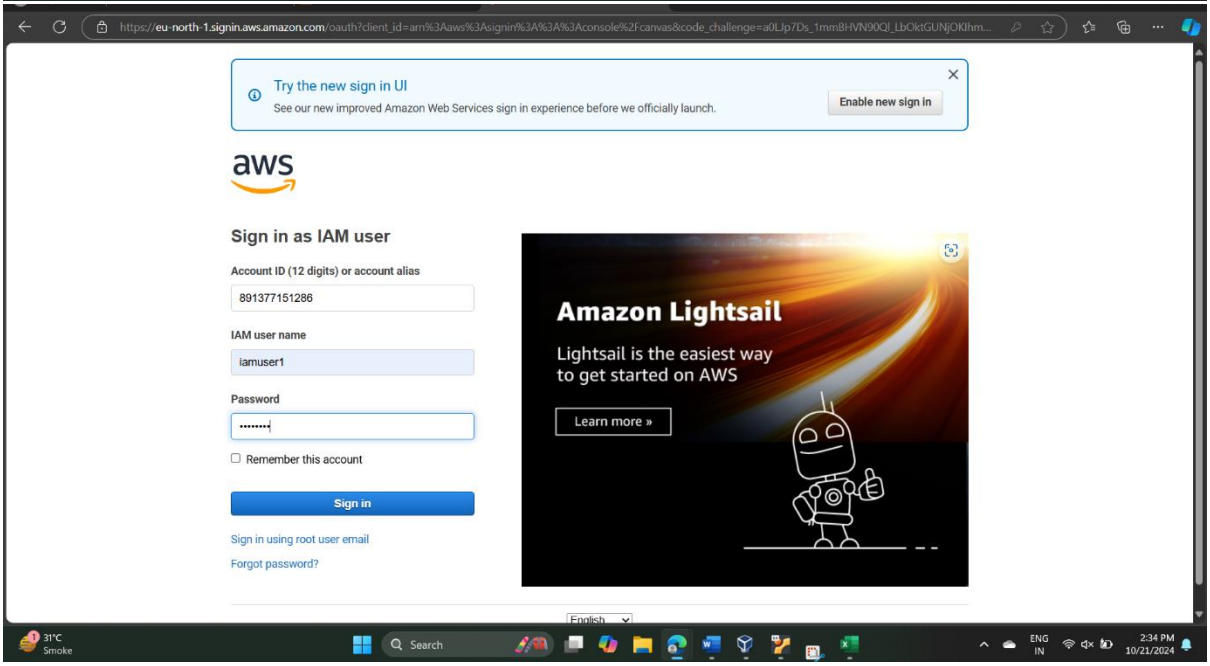

Services
Search
[Alt+S]
Global
vikkiaws
Step 1
Access key best practices & alternatives
Step 2 - optional
Set description tag
Step 3
Retrieve access keys
Access key best practices & alternatives Info
Avoid using long-term credentials like access keys to improve your security. Consider the following use cases and alternatives.
Use case
Command Line Interface (CLI)
You plan to use this access key to enable the AWS CLI to access your AWS account.
Local code
You plan to use this access key to enable application code in a local development environment to access your AWS account.
Application running on an AWS compute service
You plan to use this access key to enable application code running on an AWS compute service like Amazon EC2, Amazon ECS, or AWS Lambda to access your AWS account.
Third-party service
You plan to use this access key to enable access for a third-party application or service that monitors or manages your AWS resources.
Application running outside AWS
You plan to use this access key to authenticate workloads running in your data center or other infrastructure outside of AWS that needs to access your AWS resources.
Other
Your use case is not listed here.
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Hot weather
Now
Search
ENG
IN
2:15 PM
10/21/2024

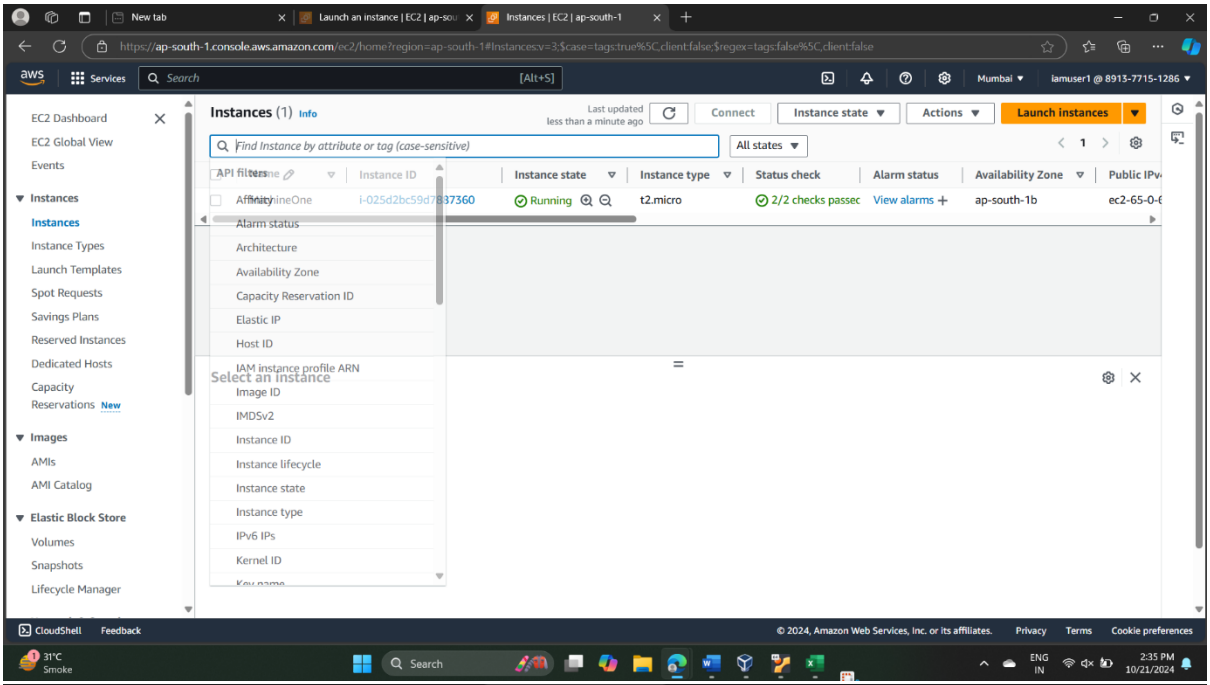

Services
Search
[Alt+S]
Global
vikkiaws
IAM
Users
iamuser1
Create access key
Step 1
Access key best practices & alternatives
Step 2 - optional
Set description tag
Step 3
Retrieve access keys
Set description tag - optional Info
The description for this access key will be attached to this user as a tag and shown alongside the access key.
Description tag value
Describe the purpose of this access key and where it will be used. A good description will help you rotate this access key confidently later.
createAccesKey
Maximum 256 characters. Allowed characters are letters, numbers, spaces representable in UTF-8, and: _ . : / = + - @
Cancel
Previous
Create access key
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Hot weather
Now
Search
ENG
IN
2:16 PM
10/21/2024

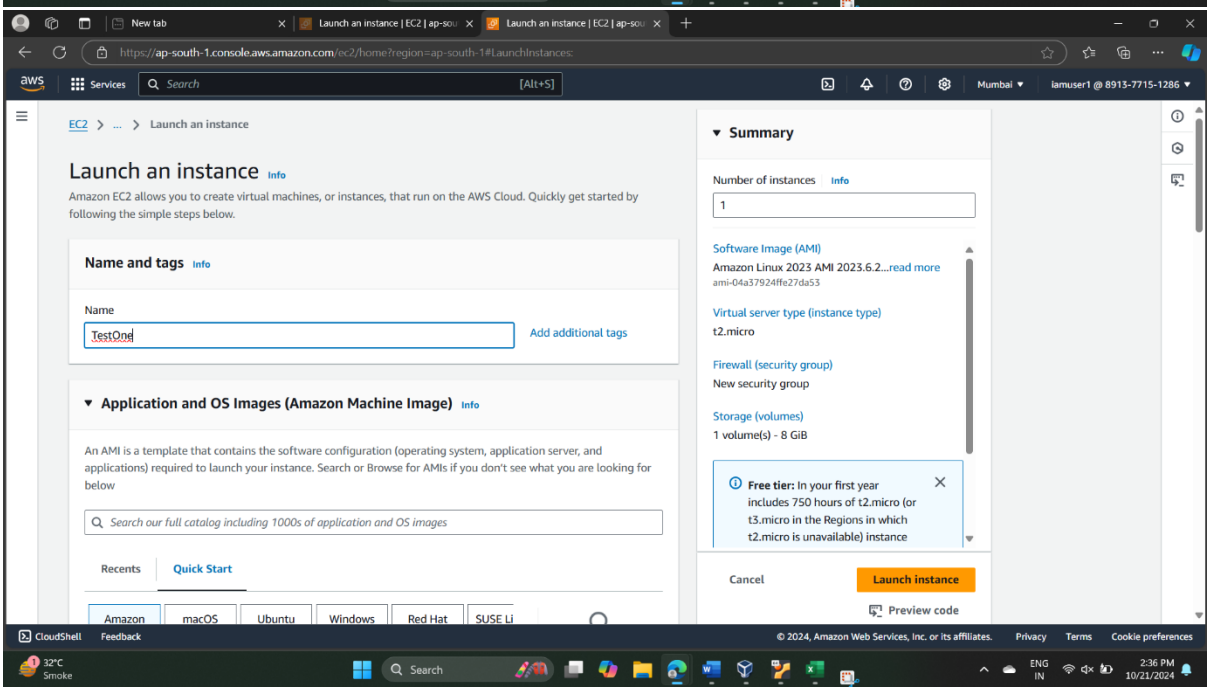

Access key created
This is the only time that the secret access key can be viewed or downloaded. You cannot recover it later. However, you can create a new access key any time.
IAM > Users > iamuser1 > Create access key
Step 1
Access key best practices & alternatives
Step 2 - optional
Set description tag
Step 3
Retrieve access keys
Retrieve access keys Info
Access key
If you lose or forget your secret access key, you cannot retrieve it. Instead, create a new access key and make the old key inactive.
Access key
Secret access key
AKIA47CRX5U3PNLX5JPG
Show
Access key best practices
Never store your access key in plain text, in a code repository, or in code.
Disable or delete access key when no longer needed.
Enable least-privilege permissions.
Rotate access keys regularly.
For more details about managing access keys, see the best practices for managing AWS access keys.
Download .csv file
Done

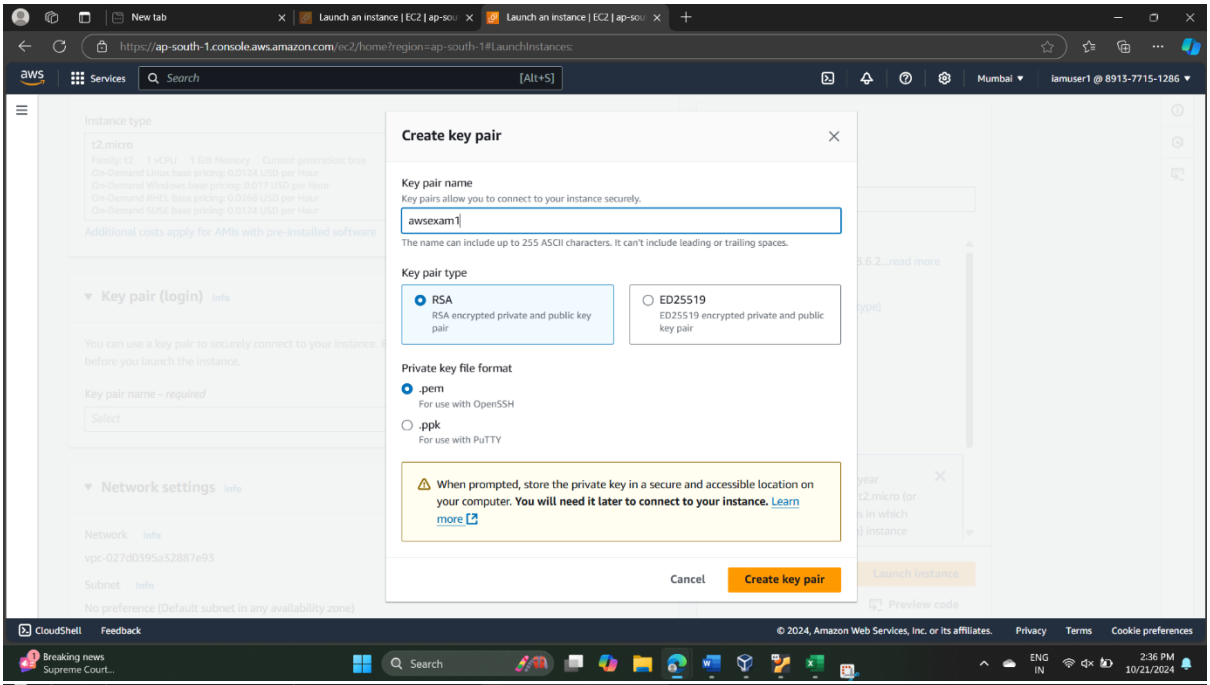

Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
Organization activity
IAM > Users > iamuser1
iamuser1 Info
Delete
Summary
ARN
arn:aws:iam::891377151286:user/iamuser1
Console access
Enabled without MFA
Access key 1
Create access key
Created
October 21, 2024, 14:30 (UTC+05:30)
Last console sign-in
Never
Permissions
Groups
Tags
Security credentials
Last Accessed
Permissions policies (1)
Permissions are defined by policies attached to the user directly or through groups.
Remove
Add permissions
Filter by Type
Search
All types
Policy name
Type
Attached via
AmazonEC2FullAccess
AWS managed
Directly

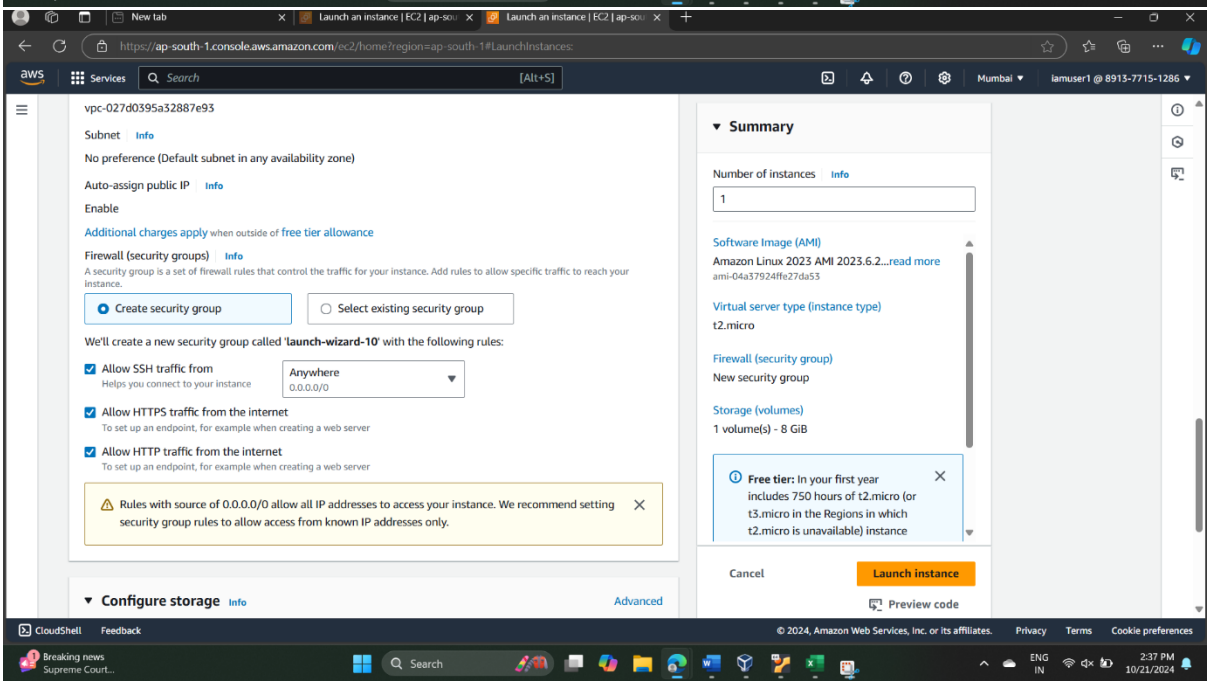

Access key created
This is the only time that the secret access key can be viewed or downloaded. You cannot recover it later. However, you can create a new access key any time.
IAM > Users > iamuser1 > Create access key
Step 1
Access key best practices & alternatives
Step 2 - optional
Set description tag
Step 3
Retrieve access keys
Retrieve access keys Info
Access key
If you lose or forget your secret access key, you cannot retrieve it. Instead, create a new access key and make the old key inactive.
Access key
Secret access key
AKIA47CRXSU3EP4EB46O
Show
Access key best practices
Never store your access key in plain text, in a code repository, or in code.
Disable or delete access key when no longer needed.
Enable least-privilege permissions.
Rotate access keys regularly.
For more details about managing access keys, see the best practices for managing AWS access keys.
Download .csv file
Done
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

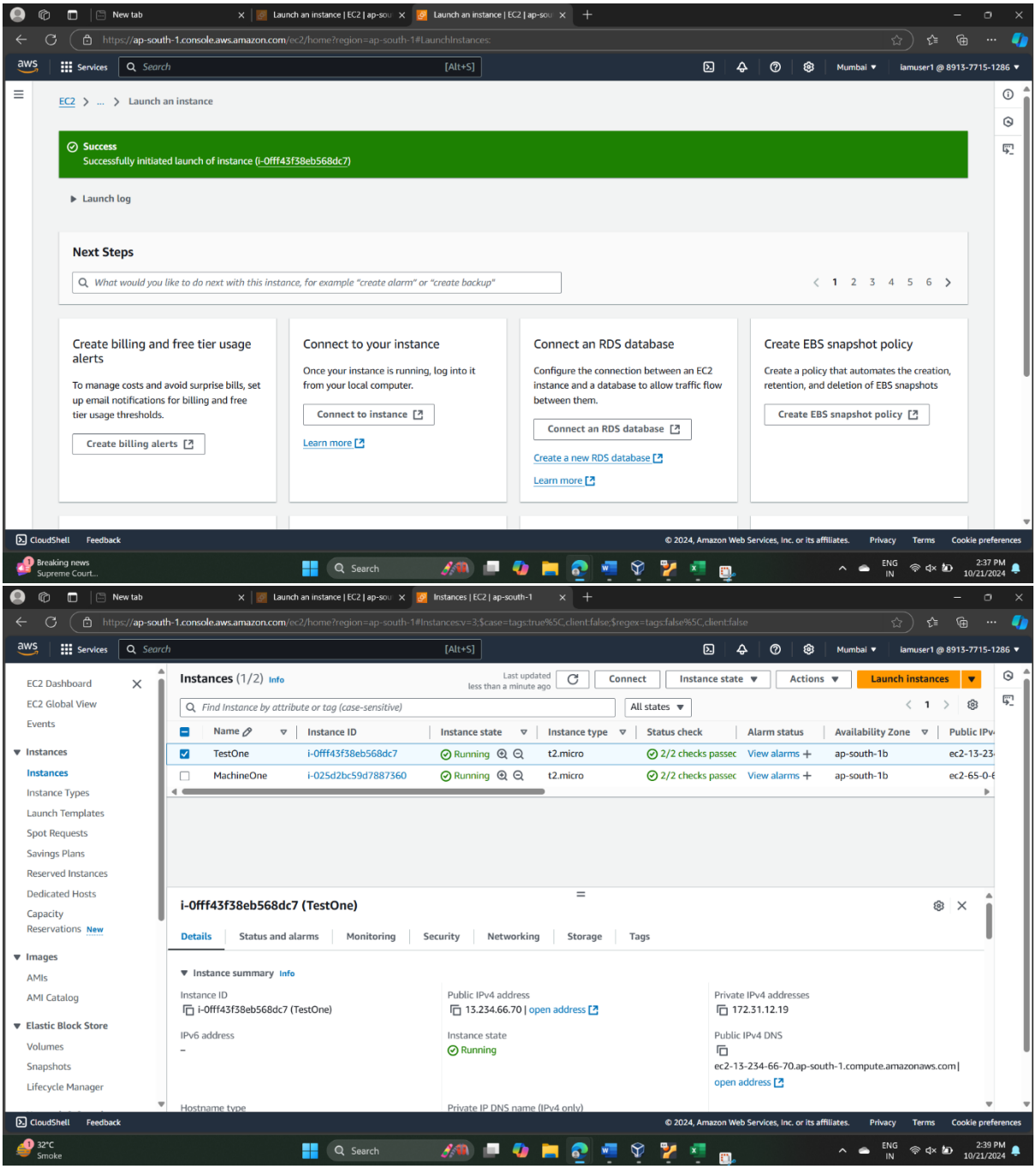

Try the new sign in UI
See our new improved Amazon Web Services sign in experience before we officially launch.
Enable new sign in
Sign in as IAM user
Account ID (12 digits) or account alias
891377151286
IAM user name
iamuser1
Password
Remember this account
Sign in
Sign in using root user email
Forgot password?
Amazon Lightsail
Lightsail is the easiest way to get started on AWS
Learn more »


Instances (1) Info
Launch instances
Instance state
Actions
Connect
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zone
Select an instance

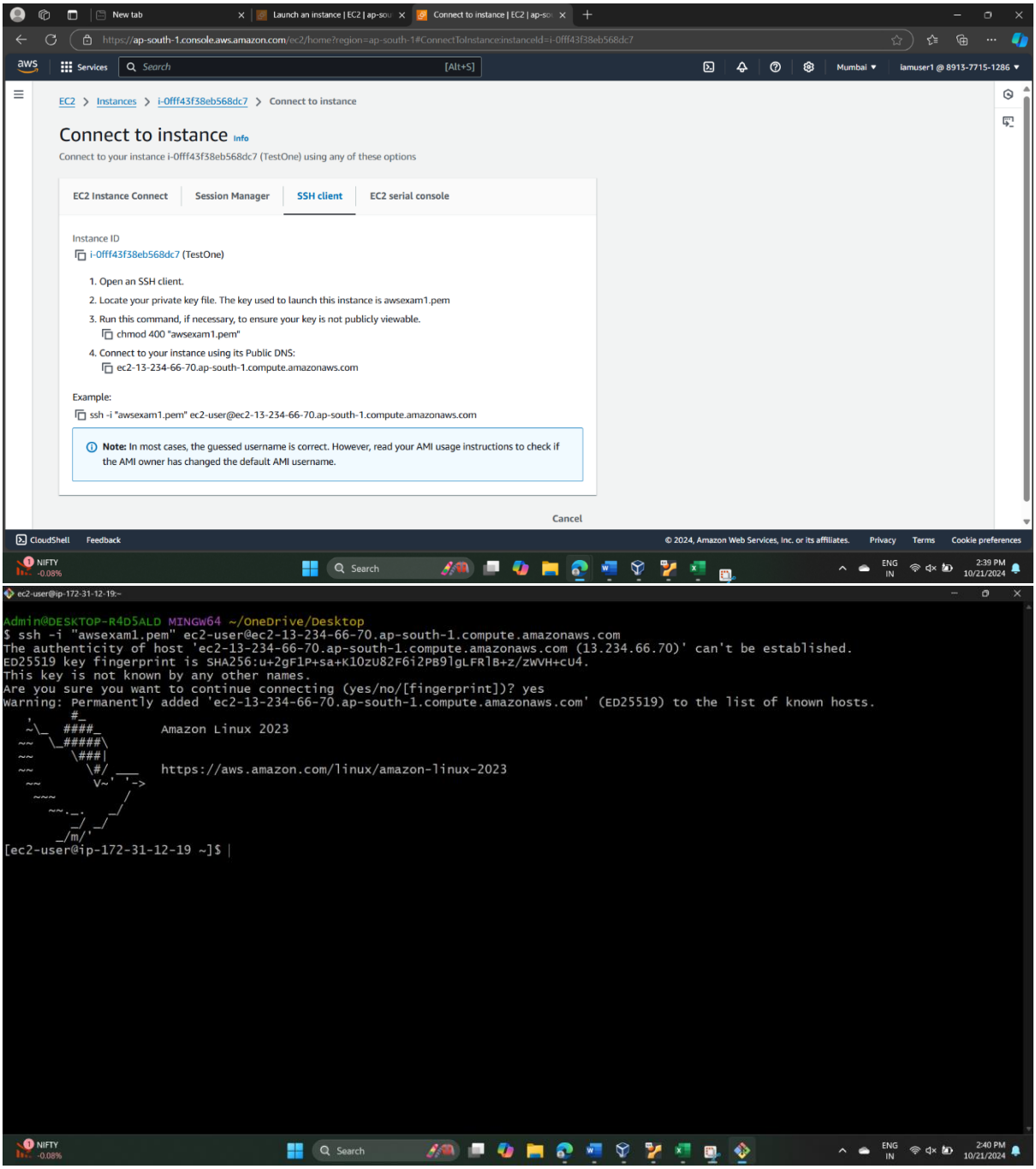

Launch an instance
Launch an instance | Info
Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.
Name and tags Info
Name
TestOne
Add additional tags
Application and OS Images (Amazon Machine Image) Info
An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below
Search our full catalog including 1000s of application and OS images
Recents
Quick Start
Amazon
macOS
Ubuntu
Windows
Red Hat
Summary
Number of instances Info
1
Software Image (AMI)
Amazon Linux 2023 AMI 2023.6.2...read more
Virtual server type (instance type)
t2.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 GiB
Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance
Cancel
Launch instance
Preview code


Create key pair
Key pair name
Key pairs allow you to connect to your instance securely.
awsexam1
The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.
Key pair type
RSA
RSA encrypted private and public key pair
ED25519
ED25519 encrypted private and public key pair
Private key file format
.pem
For use with OpenSSH
.ppk
For use with PuTTY
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
Cancel
Create key pair

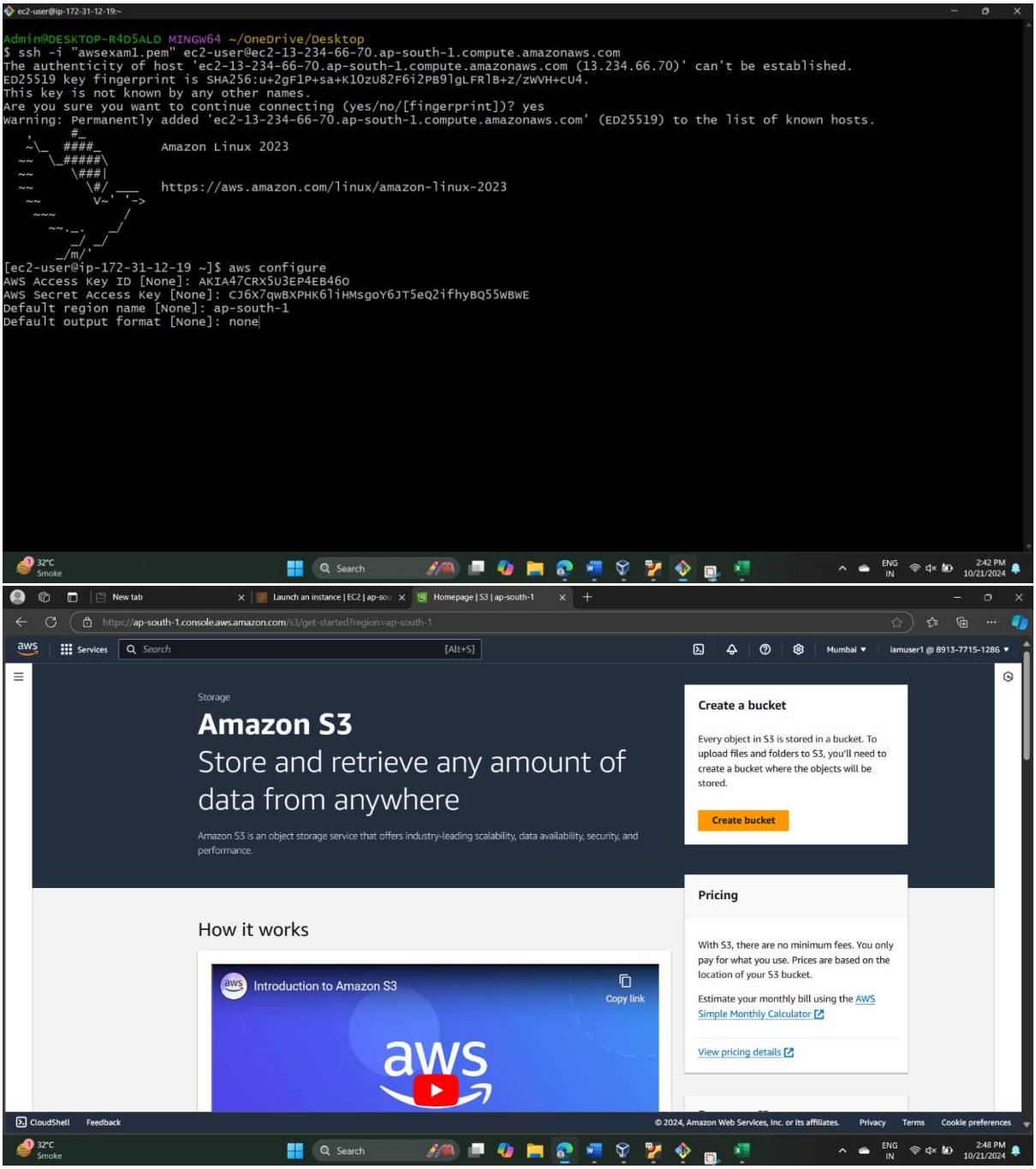

vpc-027d0395a32887e93
Subnet Info
No preference (Default subnet in any availability zone)
Auto-assign public IP Info
Enable
Additional charges apply when outside of free tier allowance
Firewall (security groups) Info
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.
Create security group
Select existing security group
We'll create a new security group called 'launch-wizard-10' with the following rules:
Allow SSH traffic from
Helps you connect to your instance
Anywhere
0.0.0.0/0
Allow HTTPS traffic from the internet
To set up an endpoint, for example when creating a web server
Allow HTTP traffic from the internet
To set up an endpoint, for example when creating a web server
Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.
Configure storage Info
Advanced
Summary
Number of instances Info
1
Software Image (AMI)
Amazon Linux 2023 AMI 2023.6.2...read more
ami-04a37924ffe27da53
Virtual server type (instance type)
t2.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 GiB
Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance
Cancel
Launch instance
Preview code


New tab
Launch an instance | EC2 | ap-sou
https://ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#LaunchInstances:
Services
Search
[Alt+S]
Mumbai
iamuser1 @ 8913-7715-1286
EC2 > ... > Launch an instance
Success
Successfully initiated launch of instance (i-0fff43f38eb568dc7)
Launch log
Next Steps
What would you like to do next with this instance, for example "create alarm" or "create backup"
Create billing and free tier usage alerts
To manage costs and avoid surprise bills, set up email notifications for billing and free tier usage thresholds.
Create billing alerts
Connect to your instance
Once your instance is running, log into it from your local computer.
Connect to instance
Learn more
Connect an RDS database
Configure the connection between an EC2 instance and a database to allow traffic flow between them.
Connect an RDS database
Create a new RDS database
Learn more
Create EBS snapshot policy
Create a policy that automates the creation, retention, and deletion of EBS snapshots
Create EBS snapshot policy
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Breaking news
Supreme Court...
Search
ENG
IN
2:37 PM
10/21/2024

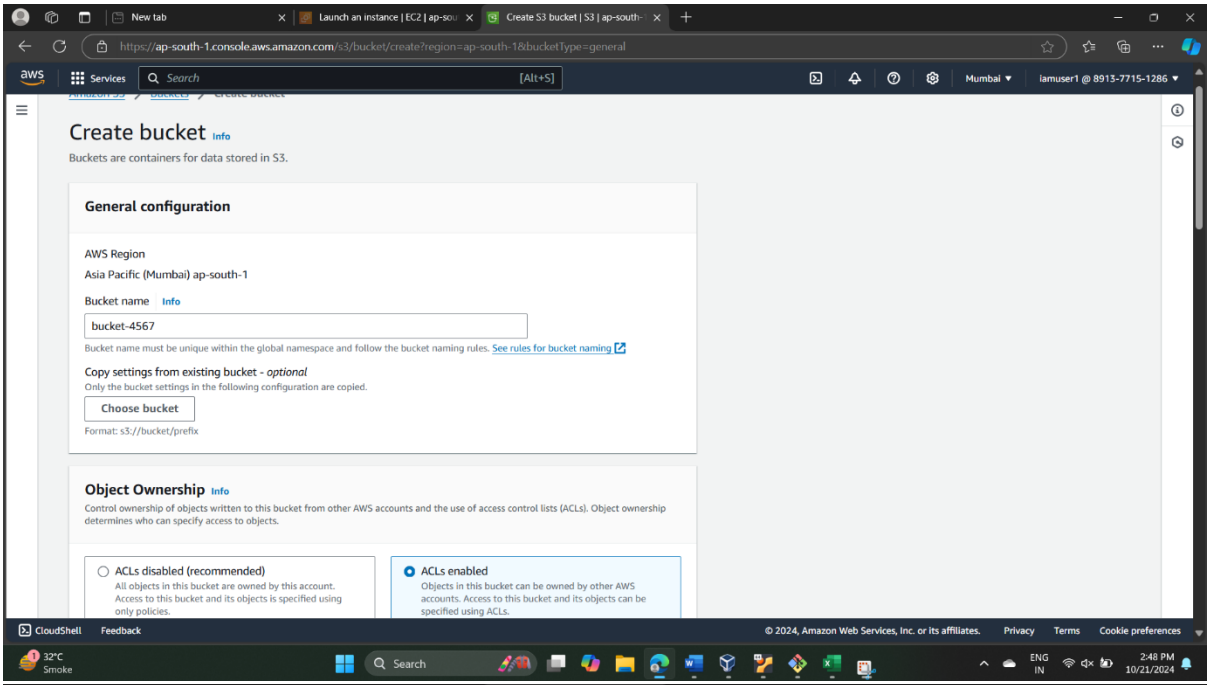
New tab
Launch an instance | EC2 | ap-sou
Instances | EC2 | ap-south-1
https://ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#Instances:v=3;$case=tags:true%5C,client:false;$regex=tags:false%5C,client:false
Services
Search
[Alt+S]
Mumbai
iamuser1 @ 8913-7715-1286
EC2 Dashboard
EC2 Global View
Events
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations New
Images
AMIs
AMI Catalog
Elastic Block Store
Volumes
Snapshots
Lifecycle Manager
Instances (1/2) Info
Last updated less than a minute ago
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
All states
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zone
Public IPv
TestOne
i-0fff43f38eb568dc7
Running
t2.micro
2/2 checks passed
View alarms
ap-south-1b
MachineOne
i-025d2bc59d7887360
Running
t2.micro
2/2 checks passed
View alarms
ap-south-1b
i-0fff43f38eb568dc7 (TestOne)
Details
Status and alarms
Monitoring
Security
Networking
Storage
Tags
Instance summary Info
Instance ID
i-0fff43f38eb568dc7 (TestOne)
Public IPv4 address
13.234.66.70 | open address
Private IPv4 addresses
172.31.12.19
IPv6 address
-
Instance state
Running
Public IPv4 DNS
ec2-13-234-66-70.ap-south-1.compute.amazonaws.com | open address
Hostname type
Private IP DNS name (IPv4 only)
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
32°C
Smoke
Search
ENG
IN
2:39 PM
10/21/2024

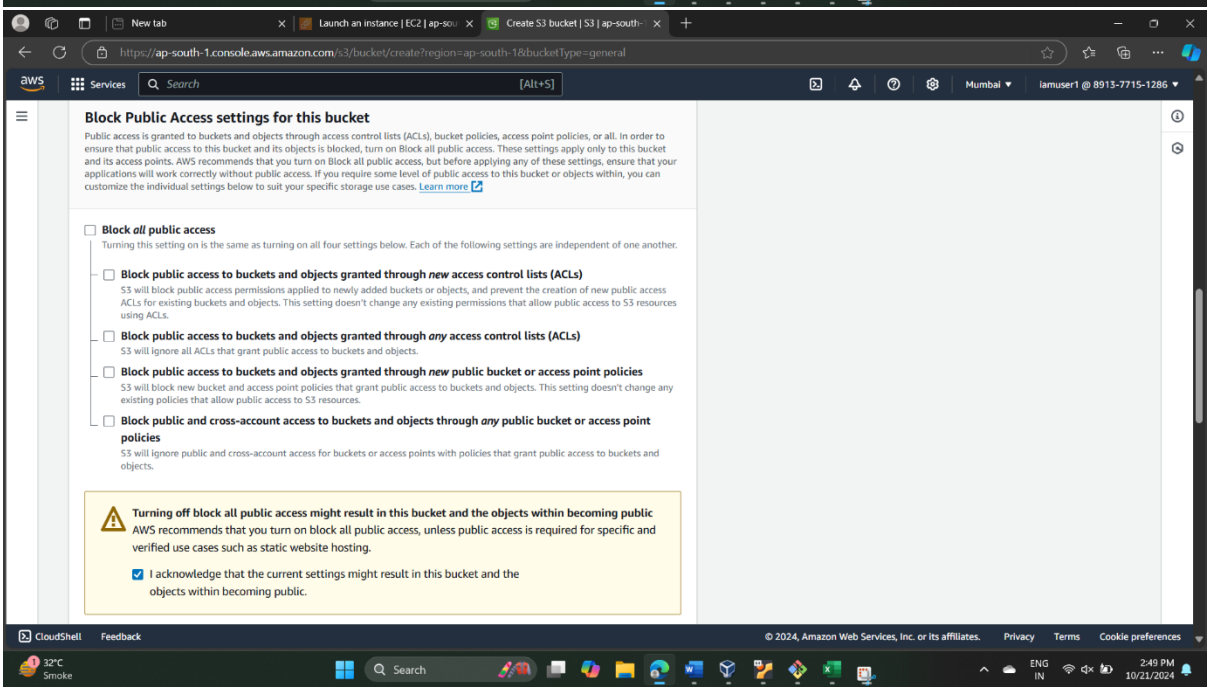

New tab
Launch an instance | EC2 | ap-sou
Connect to instance | EC2 | ap-sou
https://ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#ConnectToInstance:instanceId=i-0fff43f38eb568dc7
aws
Services
Search
[Alt+S]
Mumbai
iamuser1 @ 8913-7715-1286
EC2 > Instances > i-0fff43f38eb568dc7 > Connect to instance
Connect to instance Info
Connect to your instance i-0fff43f38eb568dc7 (TestOne) using any of these options
EC2 Instance Connect
Session Manager
SSH client
EC2 serial console
Instance ID
i-0fff43f38eb568dc7 (TestOne)
1. Open an SSH client.
2. Locate your private key file. The key used to launch this instance is awsexam1.pem
3. Run this command, if necessary, to ensure your key is not publicly viewable.
chmod 400 "awsexam1.pem"
4. Connect to your instance using its Public DNS:
ec2-13-234-66-70.ap-south-1.compute.amazonaws.com
Example:
ssh -i "awsexam1.pem" ec2-user@ec2-13-234-66-70.ap-south-1.compute.amazonaws.com
Note: In most cases, the guessed username is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI username.
Cancel
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
NIFTY
-0.08%
Search
ENG
IN
2:39 PM
10/21/2024

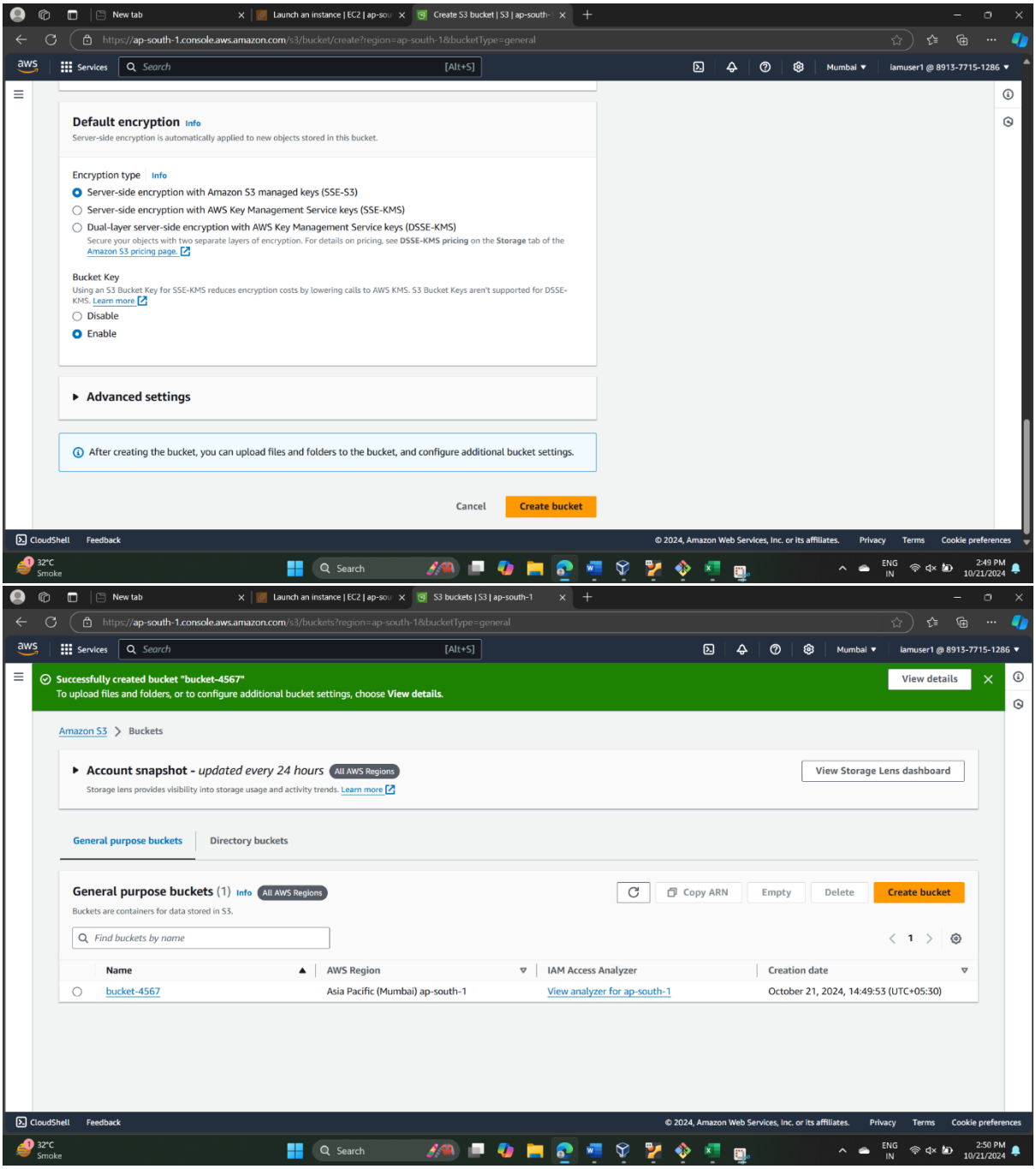
ec2-user@ip-172-31-12-19:~
Admin@DESKTOP-R4D5ALD MINGW64 ~/OneDrive/Desktop
$ ssh -i "awsexam1.pem" ec2-user@ec2-13-234-66-70.ap-south-1.compute.amazonaws.com
The authenticity of host 'ec2-13-234-66-70.ap-south-1.compute.amazonaws.com (13.234.66.70)' can't be established.
ED25519 key fingerprint is SHA256:u+2gF1P+sa+K1OzU82F6i2PB9lgLFRlB+z/zWVH+cU4.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-13-234-66-70.ap-south-1.compute.amazonaws.com' (ED25519) to the list of known hosts.
Amazon Linux 2023
https://aws.amazon.com/linux/amazon-linux-2023
[ec2-user@ip-172-31-12-19 ~]$
NIFTY
-0.08%
Search
ENG
IN
2:40 PM
10/21/2024


ec2-user@ip-172-31-12-19:~
Admin@DESKTOP-R4D5ALD MINGW64 ~/OneDrive/Desktop
$ ssh -i "awsexam1.pem" ec2-user@ec2-13-234-66-70.ap-south-1.compute.amazonaws.com
The authenticity of host 'ec2-13-234-66-70.ap-south-1.compute.amazonaws.com (13.234.66.70)' can't be established.
ED25519 key fingerprint is SHA256:u+2gF1P+sa+k1OzU82F6i2PB9lgLFR1B+z/zWVH+cU4.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-13-234-66-70.ap-south-1.compute.amazonaws.com' (ED25519) to the list of known hosts.
Amazon Linux 2023
https://aws.amazon.com/linux/amazon-linux-2023
[ec2-user@ip-172-31-12-19 ~]$ aws configure
AWS Access Key ID [None]: AKIA47CRX5U3EP4EB46O
AWS Secret Access Key [None]: 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
Default region name [None]: ap-south-1
Default output format [None]: none
32°C
Smoke
Search
ENG
IN
2:42 PM
10/21/2024

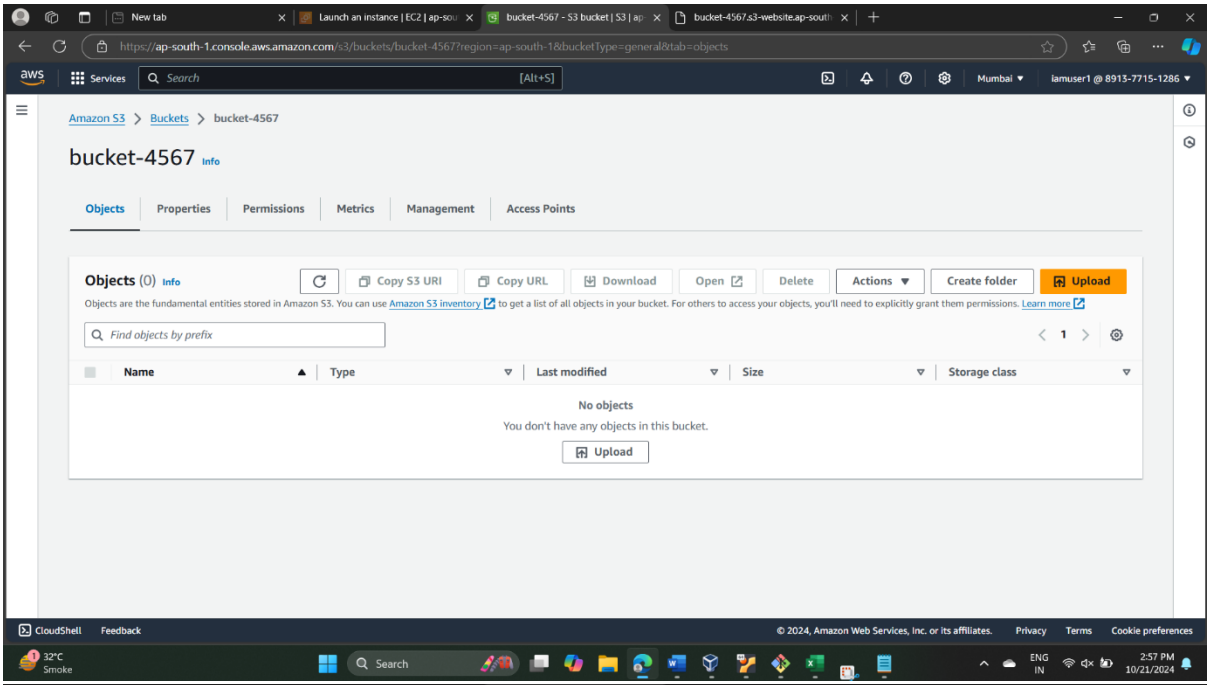
New tab
Launch an instance | EC2 | ap-sou
Homepage | S3 | ap-south-1
https://ap-south-1.console.aws.amazon.com/s3/get-started?region=ap-south-1
aws
Services
Search
[Alt+S]
Mumbai
iamuser1 @ 8913-7715-1286
Storage
Amazon S3
Store and retrieve any amount of data from anywhere
Amazon S3 is an object storage service that offers industry-leading scalability, data availability, security, and performance.
Create a bucket
Every object in S3 is stored in a bucket. To upload files and folders to S3, you'll need to create a bucket where the objects will be stored.
Create bucket
Pricing
With S3, there are no minimum fees. You only pay for what you use. Prices are based on the location of your S3 bucket.
Estimate your monthly bill using the AWS Simple Monthly Calculator
View pricing details
How it works
Introduction to Amazon S3
Copy link
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
32°C
Smoke
Search
ENG
IN
2:48 PM
10/21/2024

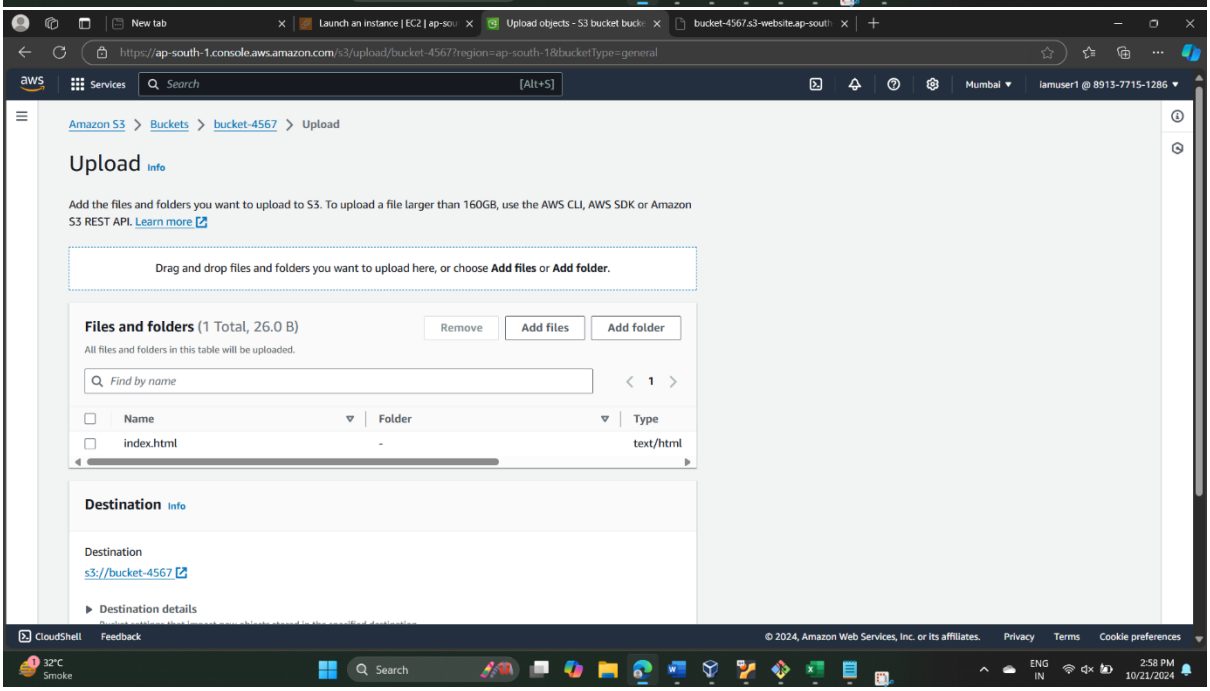

New tab
Launch an instance | EC2 | ap-sou
Create S3 bucket | S3 | ap-south-
https://ap-south-1.console.aws.amazon.com/s3/bucket/create?region=ap-south-1&bucketType=general
aws
Services
Search
[Alt+S]
Mumbai
iamuser1 @ 8913-7715-1286
Create bucket Info
Buckets are containers for data stored in S3.
General configuration
AWS Region
Asia Pacific (Mumbai) ap-south-1
Bucket name Info
bucket-4567
Bucket name must be unique within the global namespace and follow the bucket naming rules. See rules for bucket naming
Copy settings from existing bucket - optional
Only the bucket settings in the following configuration are copied.
Choose bucket
Format: s3://bucket/prefix
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.
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
32°C
Smoke
Search
ENG
IN
2:48 PM
10/21/2024

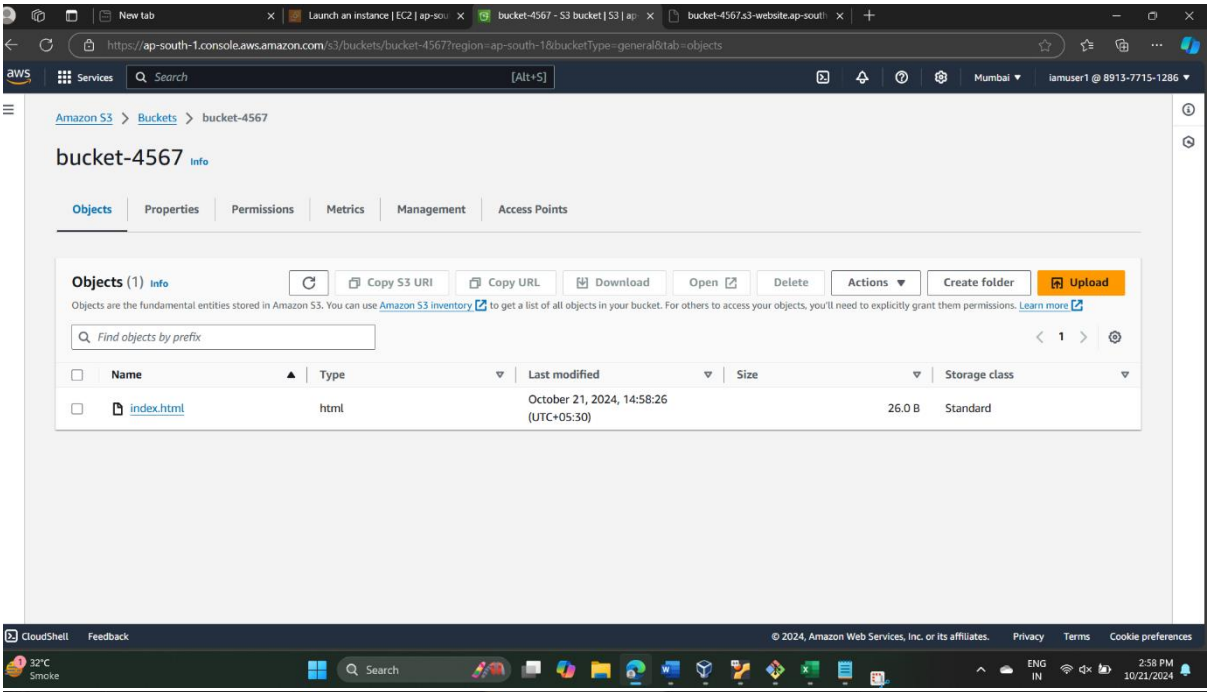

New tab
Launch an instance | EC2 | ap-sou
Create S3 bucket | S3 | ap-south-
https://ap-south-1.console.aws.amazon.com/s3/bucket/create?region=ap-south-1&bucketType=general
aws
Services
Search
[Alt+S]
Mumbai
iamuser1 @ 8913-7715-1286
Block Public Access settings for this bucket
Public access is granted 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.
I acknowledge that the current settings might result in this bucket and the objects within becoming public.
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
32°C
Smoke
Search
ENG
IN
2:49 PM
10/21/2024

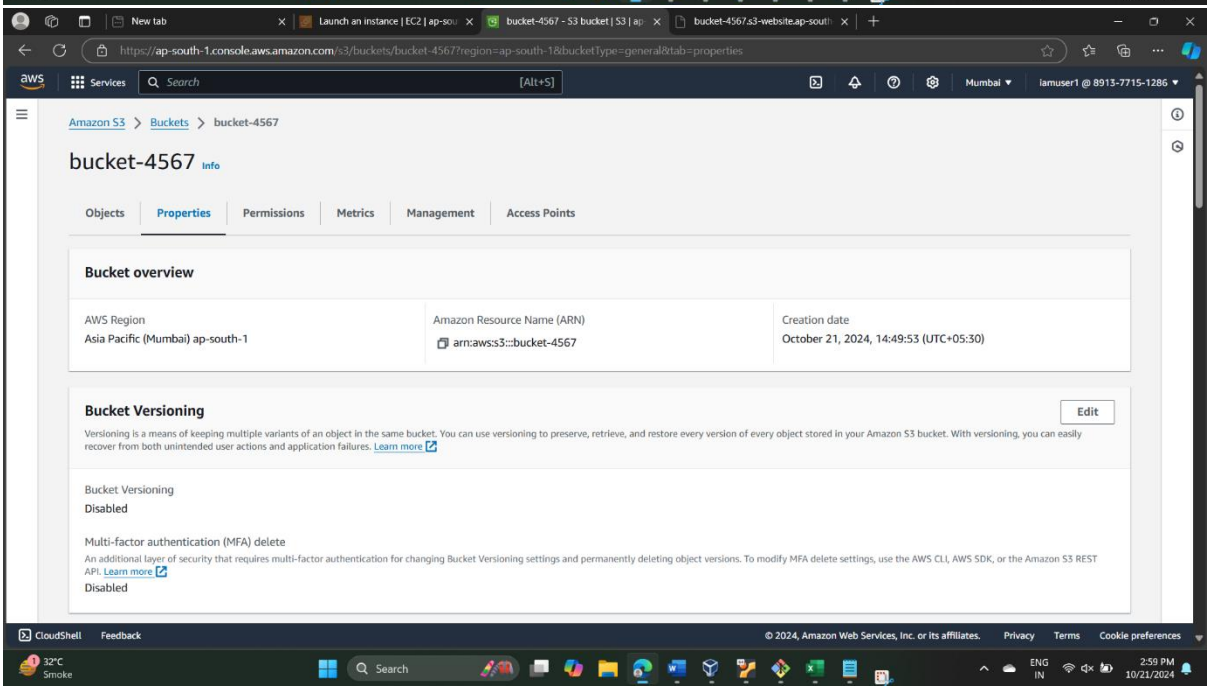

New tab
Launch an instance | EC2 | ap-sou
Create S3 bucket | S3 | ap-south-
https://ap-south-1.console.aws.amazon.com/s3/bucket/create?region=ap-south-1&bucketType=general
Services
Search
[Alt+S]
Mumbai
iamuser1 @ 8913-7715-1286
Default encryption Info
Server-side encryption is automatically applied to new objects stored in this bucket.
Encryption type Info
Server-side encryption with Amazon S3 managed keys (SSE-S3)
Server-side encryption with AWS Key Management Service keys (SSE-KMS)
Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)
Secure your objects with two separate layers of encryption. For details on pricing, see DSSE-KMS pricing on the Storage tab of the Amazon S3 pricing page.
Bucket Key
Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. Learn more
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
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
32°C
Smoke
Search
ENG
IN
2:49 PM
10/21/2024

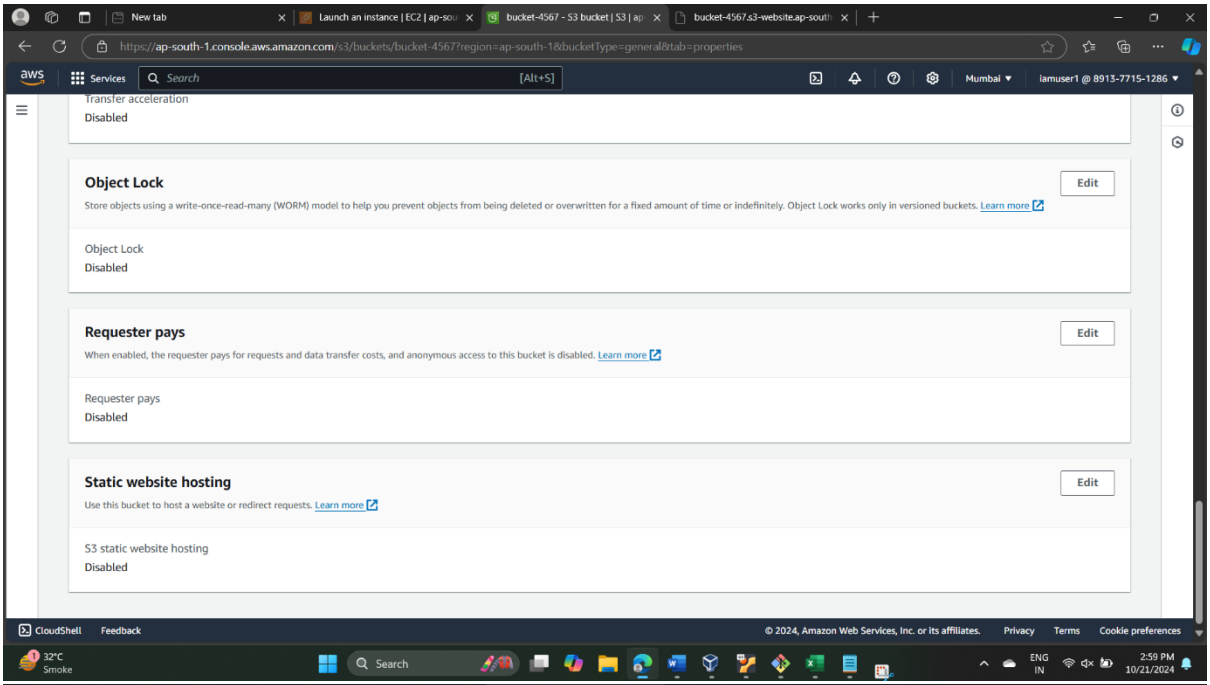
New tab
Launch an instance | EC2 | ap-sou
S3 buckets | S3 | ap-south-1
https://ap-south-1.console.aws.amazon.com/s3/buckets?region=ap-south-1&bucketType=general
Services
Search
[Alt+S]
Mumbai
iamuser1 @ 8913-7715-1286
Successfully created bucket "bucket-4567"
To upload files and folders, or to configure additional bucket settings, choose View details.
View details
Amazon S3 > Buckets
Account snapshot - updated every 24 hours
All AWS Regions
Storage lens provides visibility into storage usage and activity trends. Learn more
View Storage Lens dashboard
General purpose buckets
Directory buckets
General purpose buckets (1) Info
All AWS Regions
Buckets are containers for data stored in S3.
Copy ARN
Empty
Delete
Create bucket
Find buckets by name
1
Name
AWS Region
IAM Access Analyzer
Creation date
bucket-4567
Asia Pacific (Mumbai) ap-south-1
View analyzer for ap-south-1
October 21, 2024, 14:49:53 (UTC+05:30)
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
32°C
Smoke
Search
ENG
IN
2:50 PM
10/21/2024

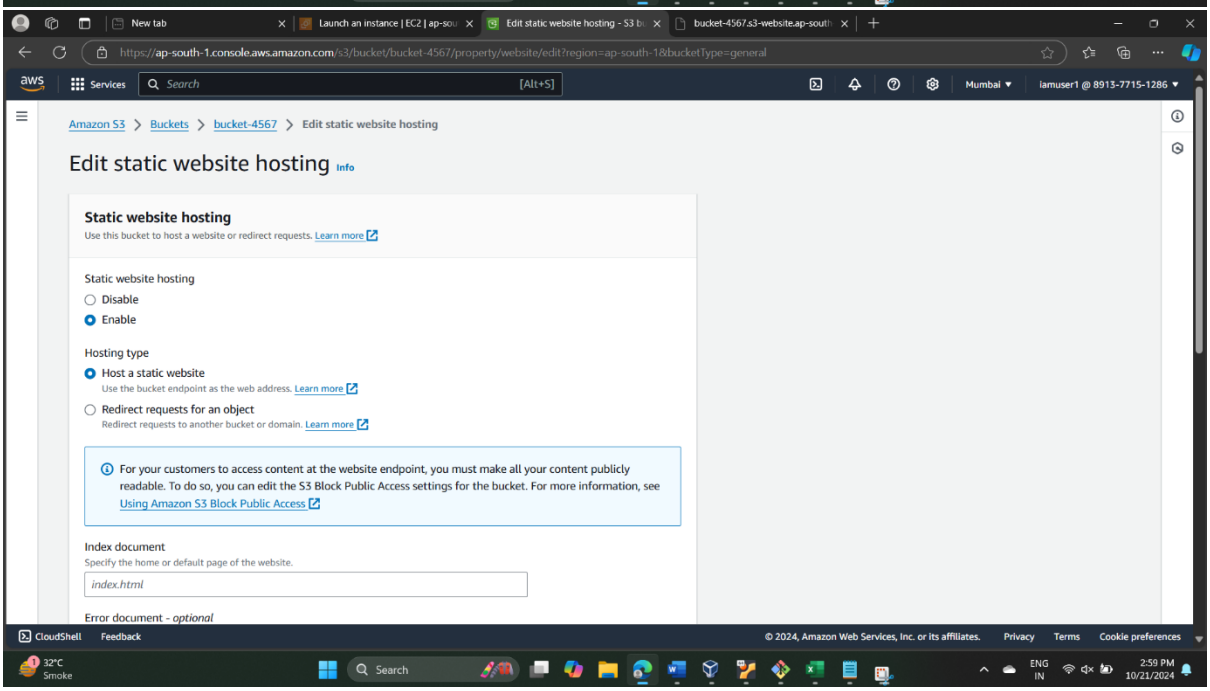

New tab
Launch an instance | EC2 | ap-sou
bucket-4567 - S3 bucket | S3 | ap
bucket-4567.s3-website.ap-south
https://ap-south-1.console.aws.amazon.com/s3/buckets/bucket-4567?region=ap-south-1&bucketType=general&tab=objects
Services
Search
[Alt+S]
Mumbai
iamuser1 @ 8913-7715-1286
Amazon S3 > Buckets > bucket-4567
bucket-4567 Info
Objects
Properties
Permissions
Metrics
Management
Access Points
Objects (0) Info
Copy S3 URI
Copy URL
Download
Open
Delete
Actions
Create folder
Upload
Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more
Find objects by prefix
Name
Type
Last modified
Size
Storage class
No objects
You don't have any objects in this bucket.
Upload
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
32°C
Smoke
Search
ENG
IN
2:57 PM
10/21/2024

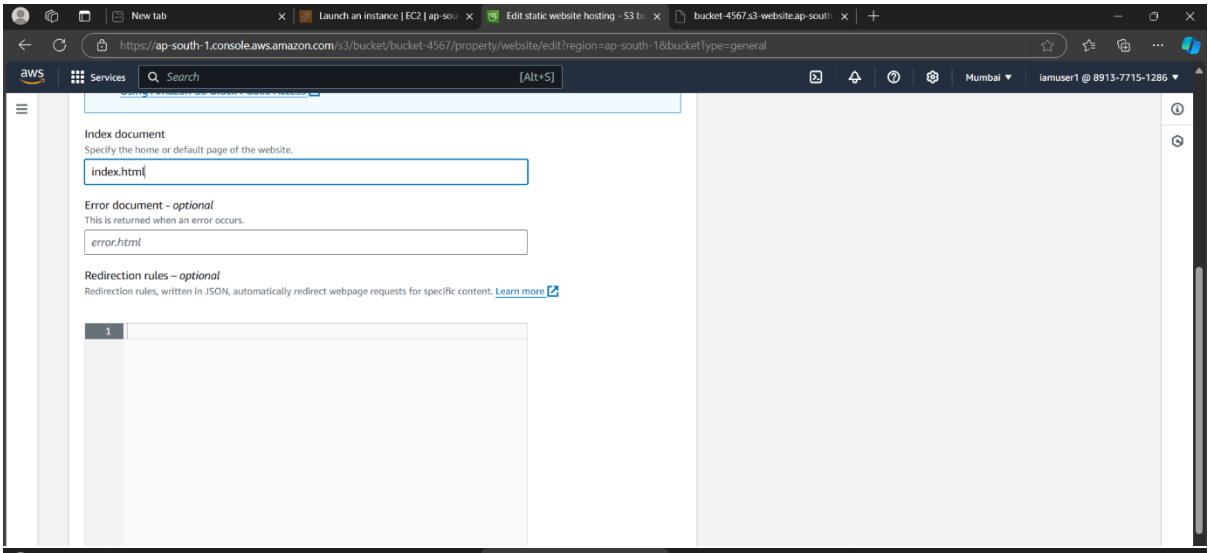

New tab
Launch an instance | EC2 | ap-sou
Upload objects - S3 bucket buck
bucket-4567.s3-website.ap-south
https://ap-south-1.console.aws.amazon.com/s3/upload/bucket-4567?region=ap-south-1&bucketType=general
Services
Search
[Alt+S]
Mumbai
iamuser1 @ 8913-7715-1286
Amazon S3 > Buckets > bucket-4567 > Upload
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 folder.
Files and folders (1 Total, 26.0 B)
Remove
Add files
Add folder
All files and folders in this table will be uploaded.
Find by name
Name
Folder
Type
index.html
-
text/html
Destination Info
Destination
s3://bucket-4567
Destination details
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
32°C
Smoke
Search
ENG
IN
2:58 PM
10/21/2024

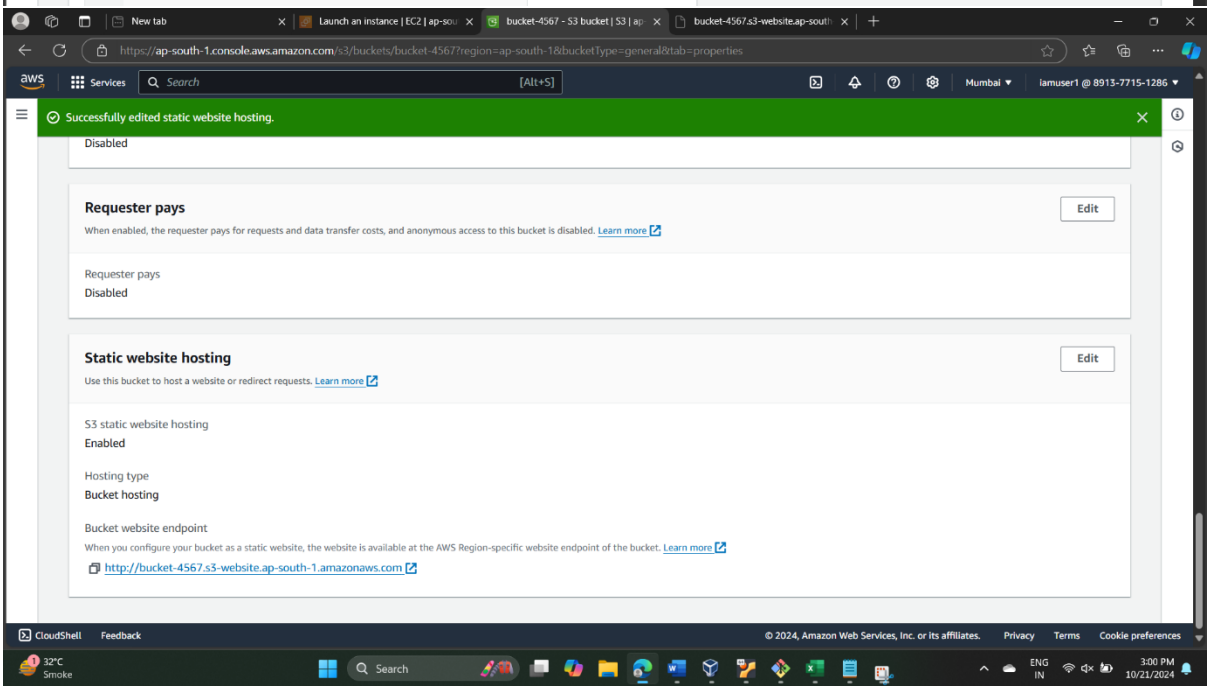

New tab
Launch an instance | EC2 | ap-sou
bucket-4567 - S3 bucket | S3 | ap
bucket-4567.s3-website.ap-south
https://ap-south-1.console.aws.amazon.com/s3/buckets/bucket-4567?region=ap-south-1&bucketType=general&tab=objects
Services
Search
[Alt+S]
Mumbai
iamuser1 @ 8913-7715-1286
Amazon S3 > Buckets > bucket-4567
bucket-4567 Info
Objects
Properties
Permissions
Metrics
Management
Access Points
Objects (1) Info
Copy S3 URI
Copy URL
Download
Open
Delete
Actions
Create folder
Upload
Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more
Find objects by prefix
Name
Type
Last modified
Size
Storage class
index.html
html
October 21, 2024, 14:58:26 (UTC+05:30)
26.0 B
Standard
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
32°C Smoke
Search
ENG IN
2:58 PM 10/21/2024

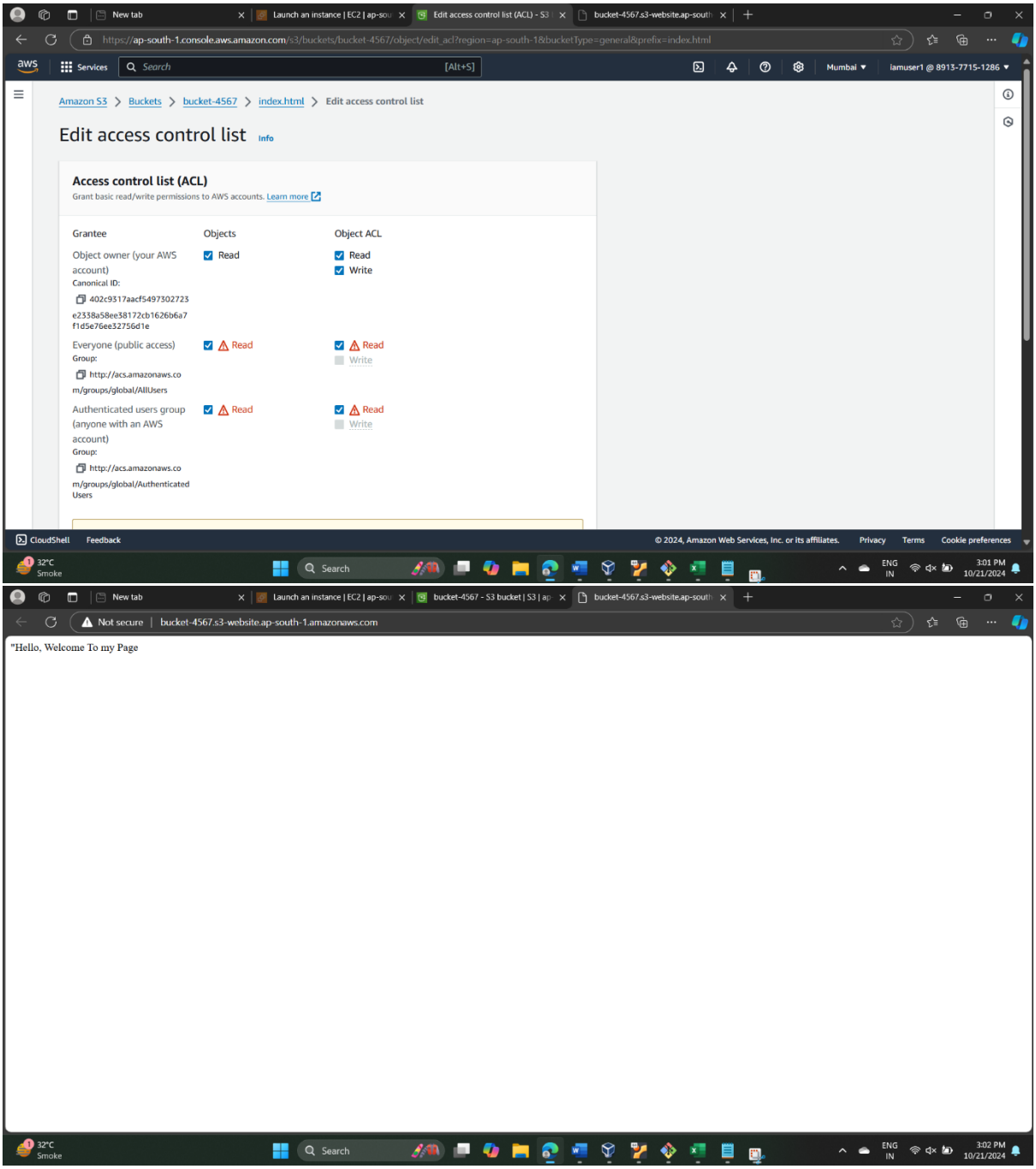

New tab
Launch an instance | EC2 | ap-sou
bucket-4567 - S3 bucket | S3 | ap
bucket-4567.s3-website.ap-south
https://ap-south-1.console.aws.amazon.com/s3/buckets/bucket-4567?region=ap-south-1&bucketType=general&tab=properties
Services
Search
[Alt+S]
Mumbai
iamuser1 @ 8913-7715-1286
Amazon S3 > Buckets > bucket-4567
bucket-4567 Info
Objects
Properties
Permissions
Metrics
Management
Access Points
Bucket overview
AWS Region
Asia Pacific (Mumbai) ap-south-1
Amazon Resource Name (ARN)
arn:aws:s3:::bucket-4567
Creation date
October 21, 2024, 14:49:53 (UTC+05:30)
Bucket Versioning
Edit
Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. Learn more
Bucket Versioning
Disabled
Multi-factor authentication (MFA) delete
An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. Learn more
Disabled
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
32°C Smoke
Search
ENG IN
2:59 PM 10/21/2024


https://ap-south-1.console.aws.amazon.com/s3/buckets/bucket-4567?region=ap-south-1&bucketType=general&tab=properties
Transfer acceleration
Disabled
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. Object Lock works only in versioned buckets. Learn more
Edit
Object Lock
Disabled
Requester pays
When enabled, the requester pays for requests and data transfer costs, and anonymous access to this bucket is disabled. Learn more
Edit
Requester pays
Disabled
Static website hosting
Use this bucket to host a website or redirect requests. Learn more
Edit
S3 static website hosting
Disabled
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


https://ap-south-1.console.aws.amazon.com/s3/bucket/bucket-4567/property/website/edit?region=ap-south-1&bucketType=general
Amazon S3 > Buckets > bucket-4567 > Edit static website hosting
Edit static website hosting Info
Static website hosting
Use this bucket to host a website or redirect requests. Learn more
Static website hosting
Disable
Enable
Hosting type
Host a static website
Use the bucket endpoint as the web address. Learn more
Redirect requests for an object
Redirect requests to another bucket or domain. Learn more
For your customers to access content at the website endpoint, you must make all your content publicly readable. To do so, you can edit the S3 Block Public Access settings for the bucket. For more information, see Using Amazon S3 Block Public Access
Index document
Specify the home or default page of the website.
index.html
Error document - optional
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


New tab
Launch an instance | EC2 | ap-sou
Edit static website hosting - S3 bu
bucket-4567.s3-website.ap-south
https://ap-south-1.console.aws.amazon.com/s3/bucket/bucket-4567/property/website/edit?region=ap-south-1&bucketType=general
Services
Search
[Alt+S]
Mumbai
iamuser1 @ 8913-7715-1286
Index document
Specify the home or default page of the website.
index.html
Error document - optional
This is returned when an error occurs.
error.html
Redirection rules – optional
Redirection rules, written in JSON, automatically redirect webpage requests for specific content. Learn more
1


New tab
Launch an instance | EC2 | ap-sou
bucket-4567 - S3 bucket | S3 | ap
bucket-4567.s3-website.ap-south
https://ap-south-1.console.aws.amazon.com/s3/buckets/bucket-4567?region=ap-south-1&bucketType=general&tab=properties
Services
Search
[Alt+S]
Mumbai
iamuser1 @ 8913-7715-1286
Successfully edited static website hosting.
Disabled
Requester pays
When enabled, the requester pays for requests and data transfer costs, and anonymous access to this bucket is disabled. Learn more
Edit
Requester pays
Disabled
Static website hosting
Use this bucket to host a website or redirect requests. Learn more
Edit
S3 static website hosting
Enabled
Hosting type
Bucket hosting
Bucket website endpoint
When you configure your bucket as a static website, the website is available at the AWS Region-specific website endpoint of the bucket. Learn more
http://bucket-4567.s3-website.ap-south-1.amazonaws.com
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
32°C
Smoke
Search
ENG
IN
3:00 PM
10/21/2024



url: http://bucket-4567.s3-website.ap-south-1.amazonaws.com