Build an Image Label Generator using Amazon Rekognition

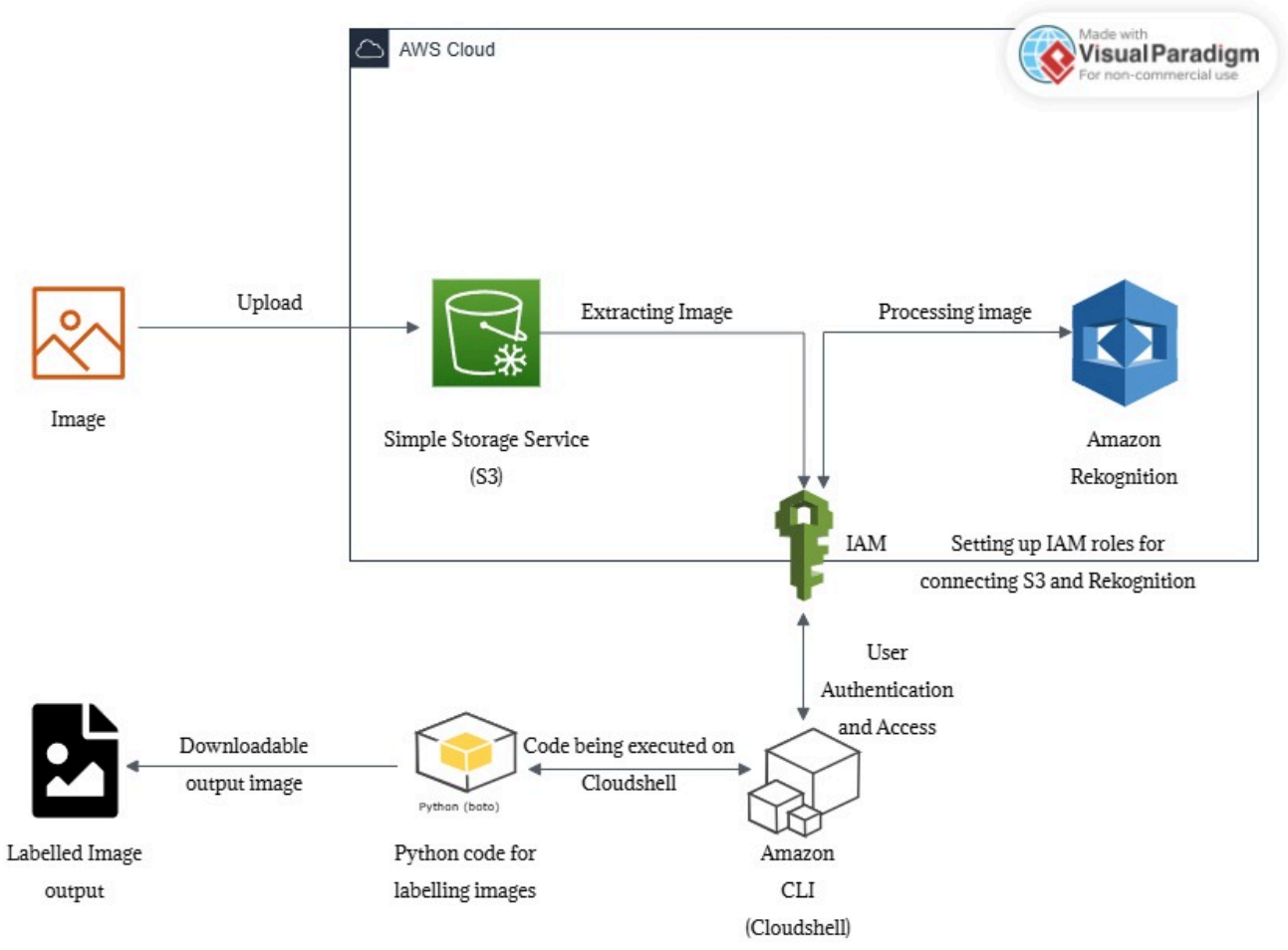
Here we will be processing images and labelling them

1. set up a s3 bucket with repository of images we want to analyze
2. next create an iam role making sure s3 and amazon rekognition have access to each other
3. install amazon cli, use some code for detect lable option
4. use a python library "MATPLOTLIB" to visualize labels and add bounding boxes to add items identified in the images

Use Cases

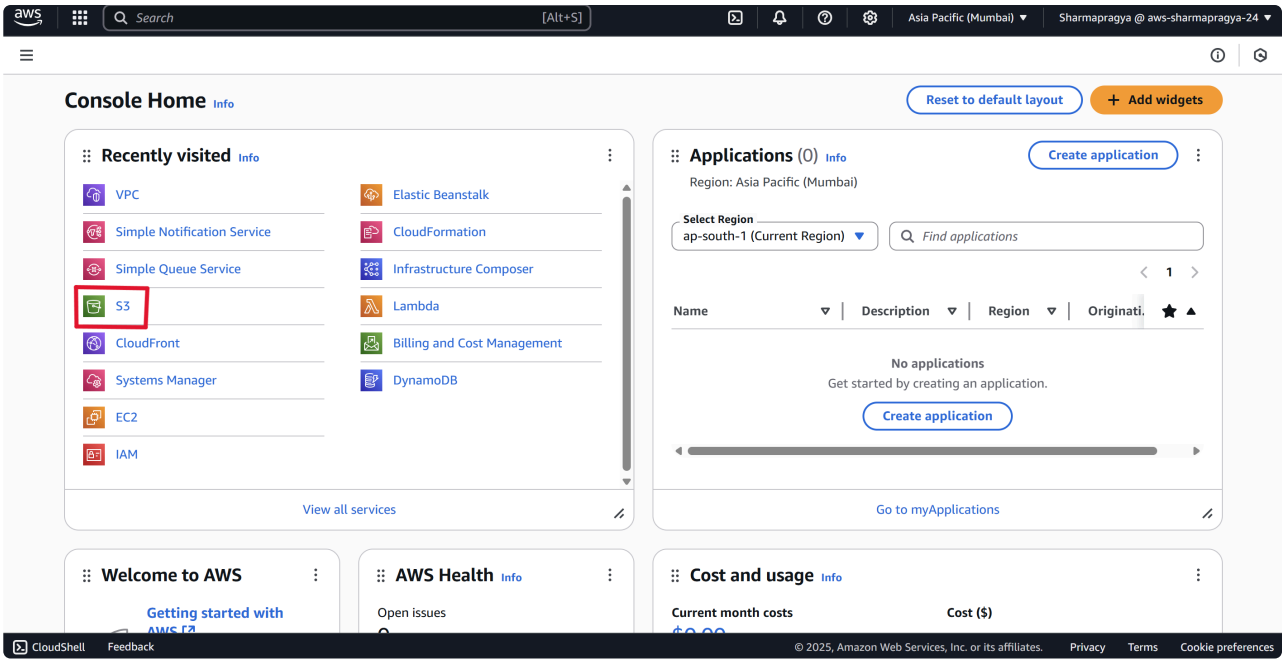
1. in a smart surveillance system to recognize suspicious objects and activites.
2. Identifying products in a store for inventory management
3. Analyzing customer behavior on retail stores
4. Providing accessibility options for those who are visually impaired

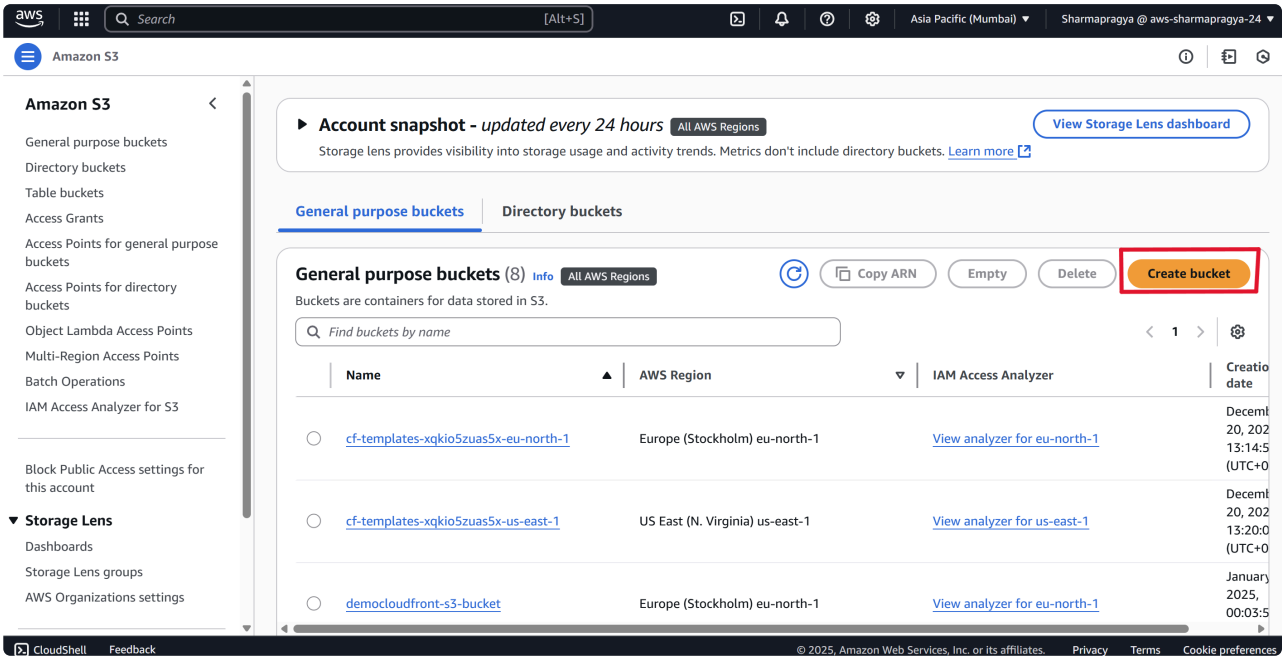
Architecture diagram

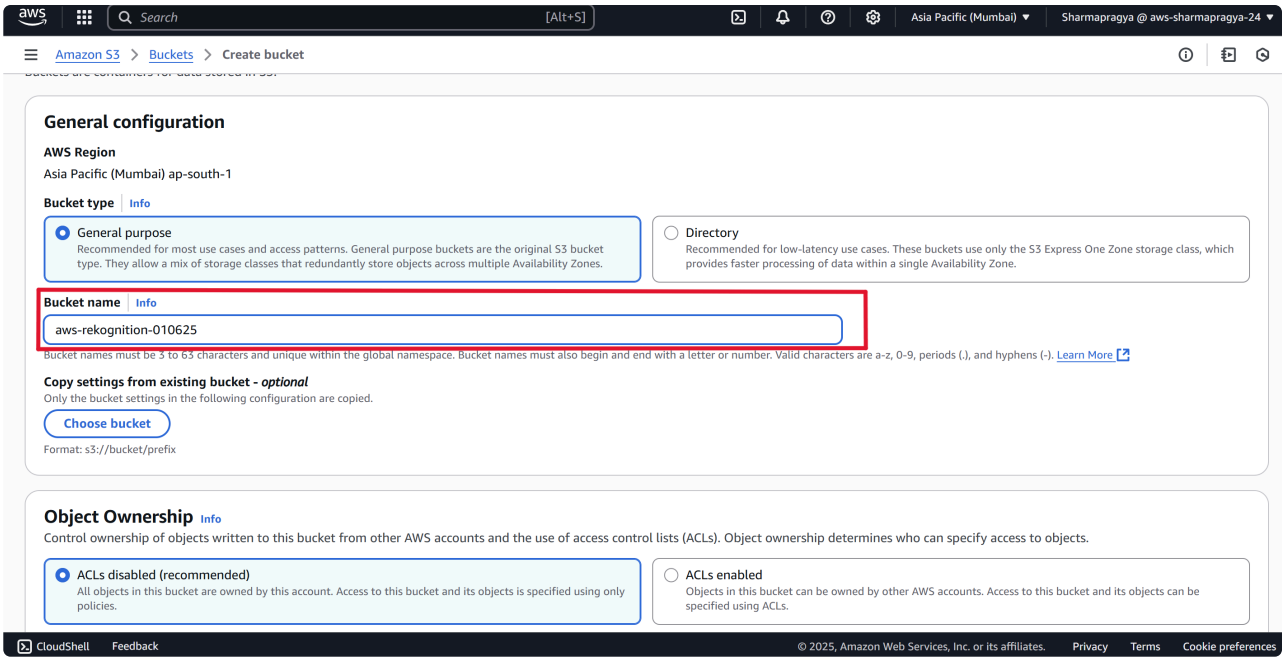


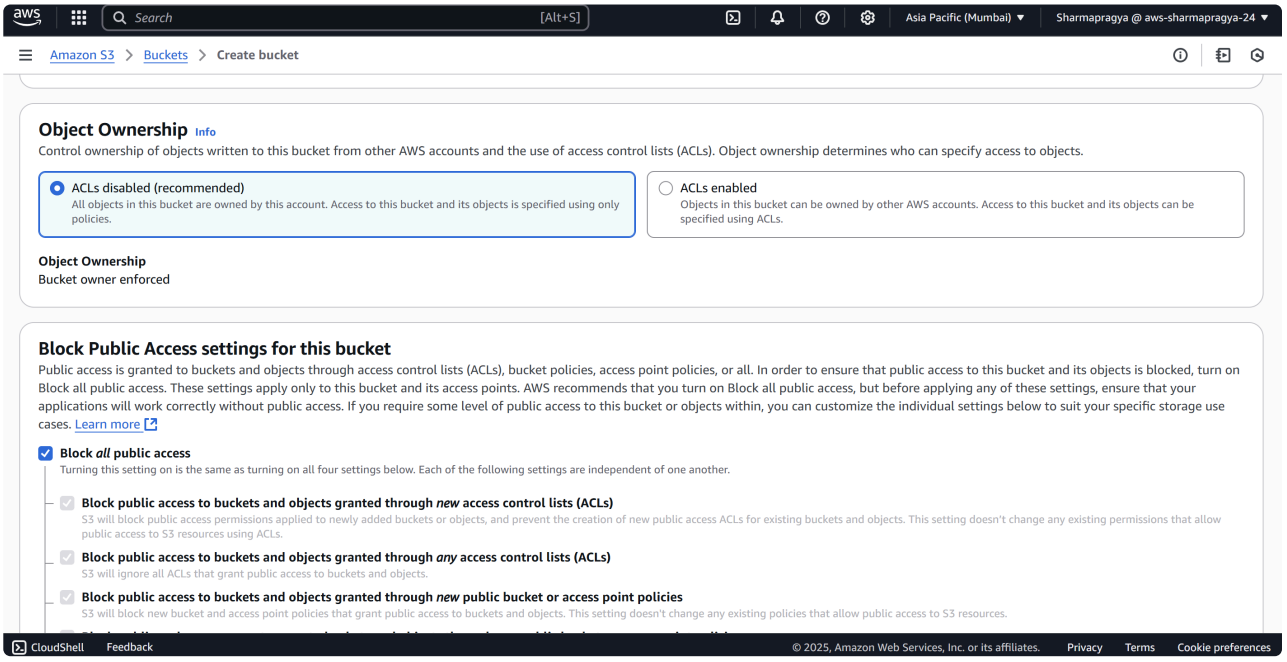
Steps for Building an image label generator using Amazon rekognition

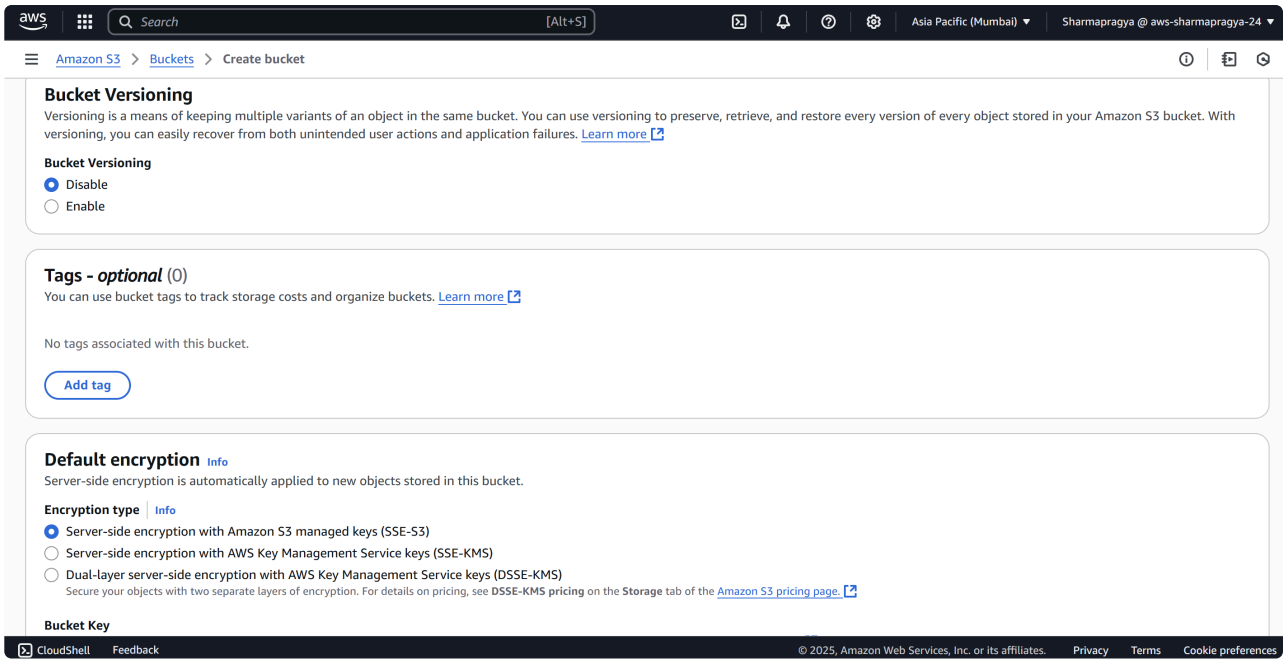
1. **Create an S3 bucket.

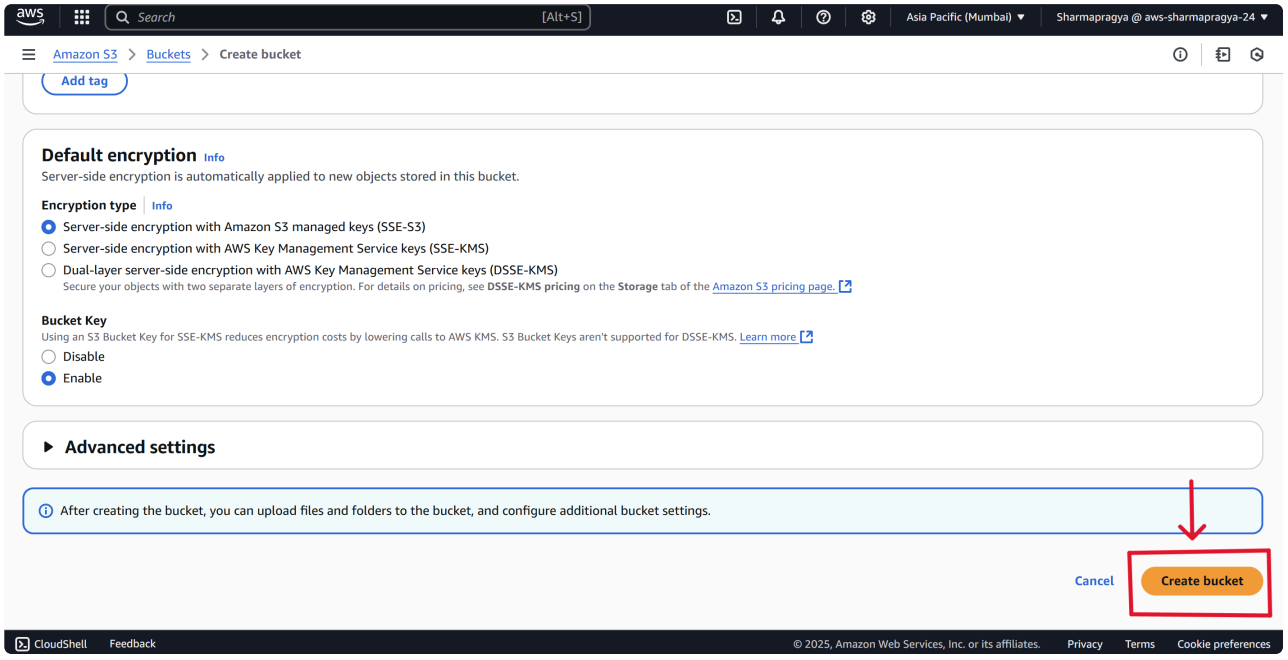

Search [Alt+S]
Asia Pacific (Mumbai)
Sharmapragya @ aws-sharmapragya-24
Console Home Info
Reset to default layout
+ Add widgets
Recently visited Info
VPC
Simple Notification Service
Simple Queue Service
S3
CloudFront
Systems Manager
EC2
IAM
Elastic Beanstalk
CloudFormation
Infrastructure Composer
Lambda
Billing and Cost Management
DynamoDB
View all services
Applications (0) Info
Create application
Region: Asia Pacific (Mumbai)
Select Region
ap-south-1 (Current Region)
Find applications
Name
Description
Region
Originati.
No applications
Get started by creating an application.
Create application
Go to myApplications
Welcome to AWS
Getting started with AWS
AWS Health Info
Open issues
Cost and usage Info
Current month costs
Cost ($)
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

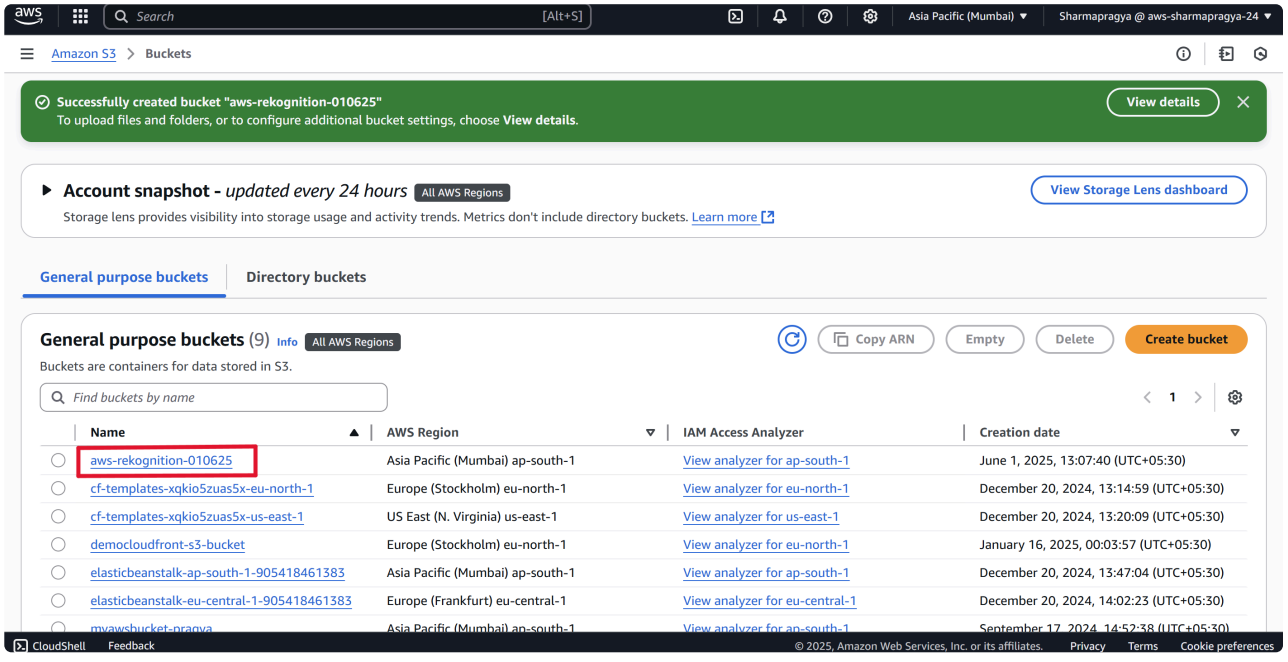

Search [Alt+S]
Asia Pacific (Mumbai)
Sharmapragya @ aws-sharmapragya-24
Amazon S3
Amazon S3
General purpose buckets
Directory buckets
Table buckets
Access Grants
Access Points for general purpose buckets
Access Points for directory buckets
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
Storage Lens groups
AWS Organizations settings
Account snapshot - updated every 24 hours
All AWS Regions
Storage lens provides visibility into storage usage and activity trends. Metrics don't include directory buckets. Learn more
View Storage Lens dashboard
General purpose buckets
Directory buckets
General purpose buckets (8) Info
All AWS Regions
Buckets are containers for data stored in S3.
Copy ARN
Empty
Delete
Create bucket
Find buckets by name
Name
AWS Region
IAM Access Analyzer
Creation date
cf-templates-xqkio5zuas5x-eu-north-1
Europe (Stockholm) eu-north-1
View analyzer for eu-north-1
cf-templates-xqkio5zuas5x-us-east-1
US East (N. Virginia) us-east-1
View analyzer for us-east-1
democloudfront-s3-bucket
Europe (Stockholm) eu-north-1
View analyzer for eu-north-1
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Search
[Alt+S]
Asia Pacific (Mumbai)
Sharmapragya @ aws-sharmapragya-24
Amazon S3 > Buckets > Create bucket
General configuration
AWS Region
Asia Pacific (Mumbai) ap-south-1
Bucket type Info
General purpose
Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.
Directory
Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.
Bucket name Info
aws-rekognition-010625
Bucket names must be 3 to 63 characters and unique within the global namespace. Bucket names must also begin and end with a letter or number. Valid characters are a-z, 0-9, periods (.), and hyphens (-). Learn More
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
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

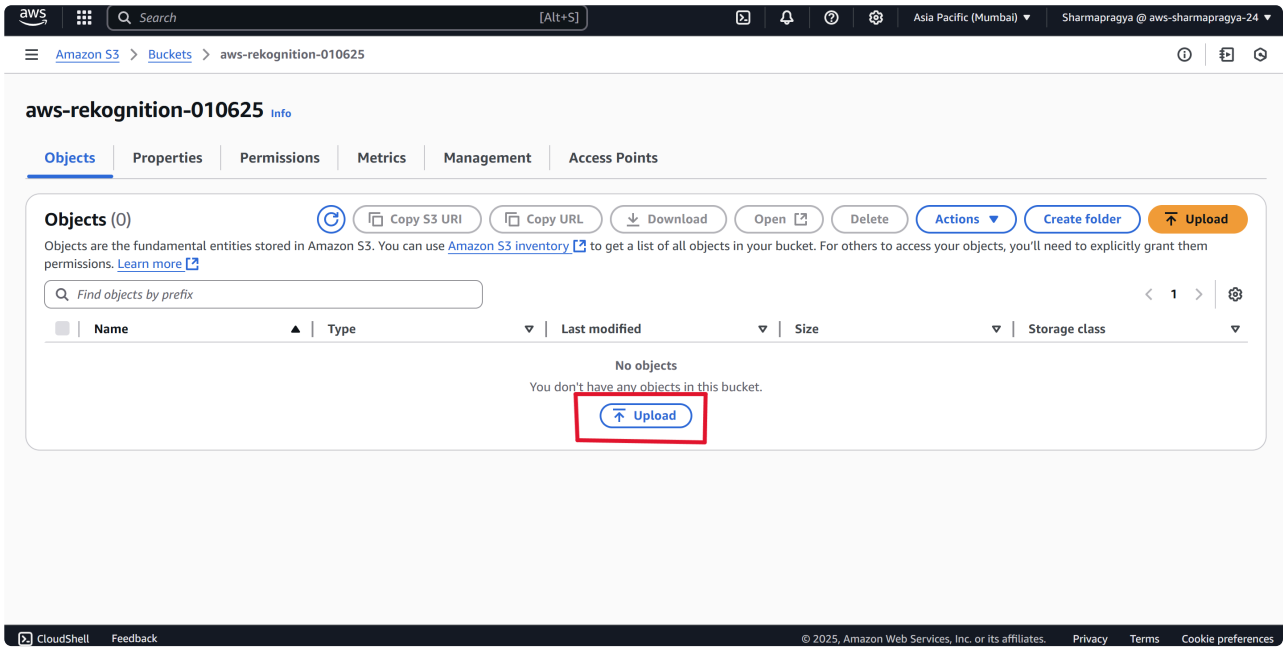

Search
[Alt+S]
Asia Pacific (Mumbai)
Sharmapragya @ aws-sharmapragya-24
Amazon S3 > Buckets > Create bucket
Object Ownership Info
Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access 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
Bucket owner enforced
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.
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

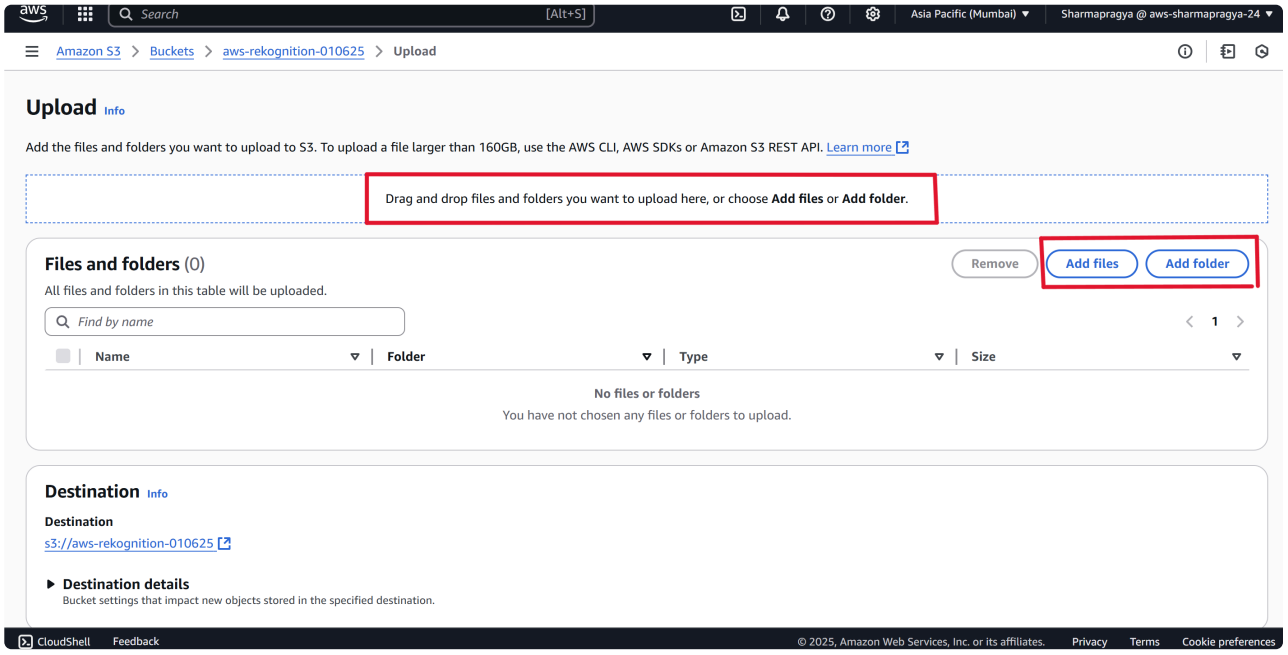

Search [Alt+S]
Asia Pacific (Mumbai)
Sharmapragya @ aws-sharmapragya-24
Amazon S3 > Buckets > Create bucket
Bucket Versioning
Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. Learn more
Bucket Versioning
Disable
Enable
Tags - optional (0)
You can use bucket tags to track storage costs and organize buckets. Learn more
No tags associated with this bucket.
Add tag
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
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Search [Alt+S]
Asia Pacific (Mumbai)
Sharmapragya @ aws-sharmapragya-24
Amazon S3 > Buckets > Create bucket
Add tag
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
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

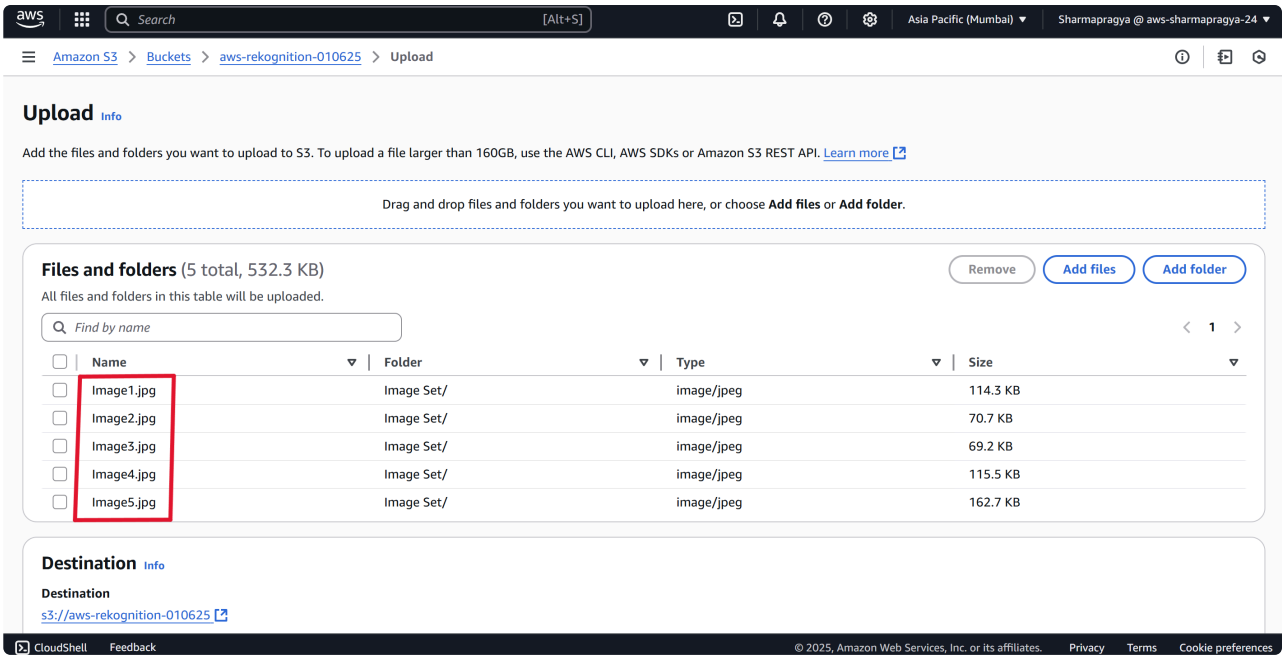

Search [Alt+S]
Asia Pacific (Mumbai)
Sharmapragya @ aws-sharmapragya-24
Amazon S3 > Buckets
Successfully created bucket "aws-rekognition-010625"
To upload files and folders, or to configure additional bucket settings, choose View details.
View details
Account snapshot - updated every 24 hours
All AWS Regions
Storage lens provides visibility into storage usage and activity trends. Metrics don't include directory buckets. Learn more
View Storage Lens dashboard
General purpose buckets
Directory buckets
General purpose buckets (9) Info
All AWS Regions
Buckets are containers for data stored in S3.
Copy ARN
Empty
Delete
Create bucket
Find buckets by name
Name
AWS Region
IAM Access Analyzer
Creation date
aws-rekognition-010625
Asia Pacific (Mumbai) ap-south-1
View analyzer for ap-south-1
June 1, 2025, 13:07:40 (UTC+05:30)
cf-templates-xqkio5zuas5x-eu-north-1
Europe (Stockholm) eu-north-1
View analyzer for eu-north-1
December 20, 2024, 13:14:59 (UTC+05:30)
cf-templates-xqkio5zuas5x-us-east-1
US East (N. Virginia) us-east-1
View analyzer for us-east-1
December 20, 2024, 13:20:09 (UTC+05:30)
democloudfront-s3-bucket
Europe (Stockholm) eu-north-1
View analyzer for eu-north-1
January 16, 2025, 00:03:57 (UTC+05:30)
elasticbeanstalk-ap-south-1-905418461383
Asia Pacific (Mumbai) ap-south-1
View analyzer for ap-south-1
December 20, 2024, 13:47:04 (UTC+05:30)
elasticbeanstalk-eu-central-1-905418461383
Europe (Frankfurt) eu-central-1
View analyzer for eu-central-1
December 20, 2024, 14:02:23 (UTC+05:30)
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

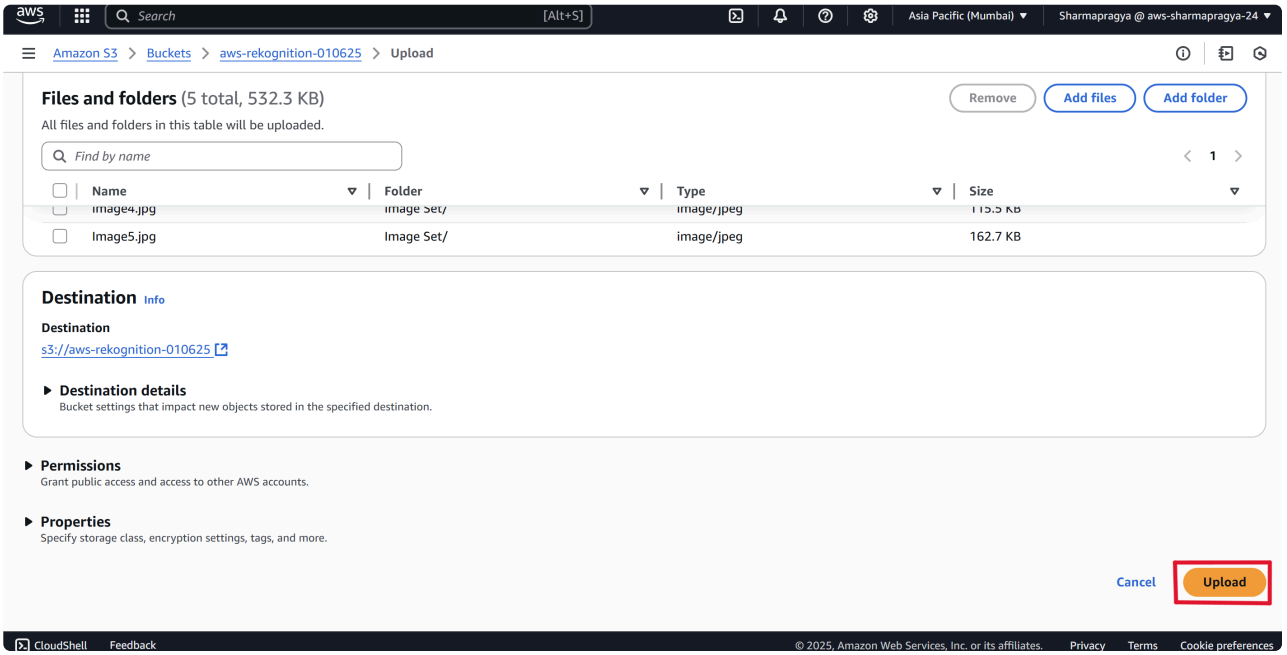
2. **Upload Images to the newly created S3 bucket

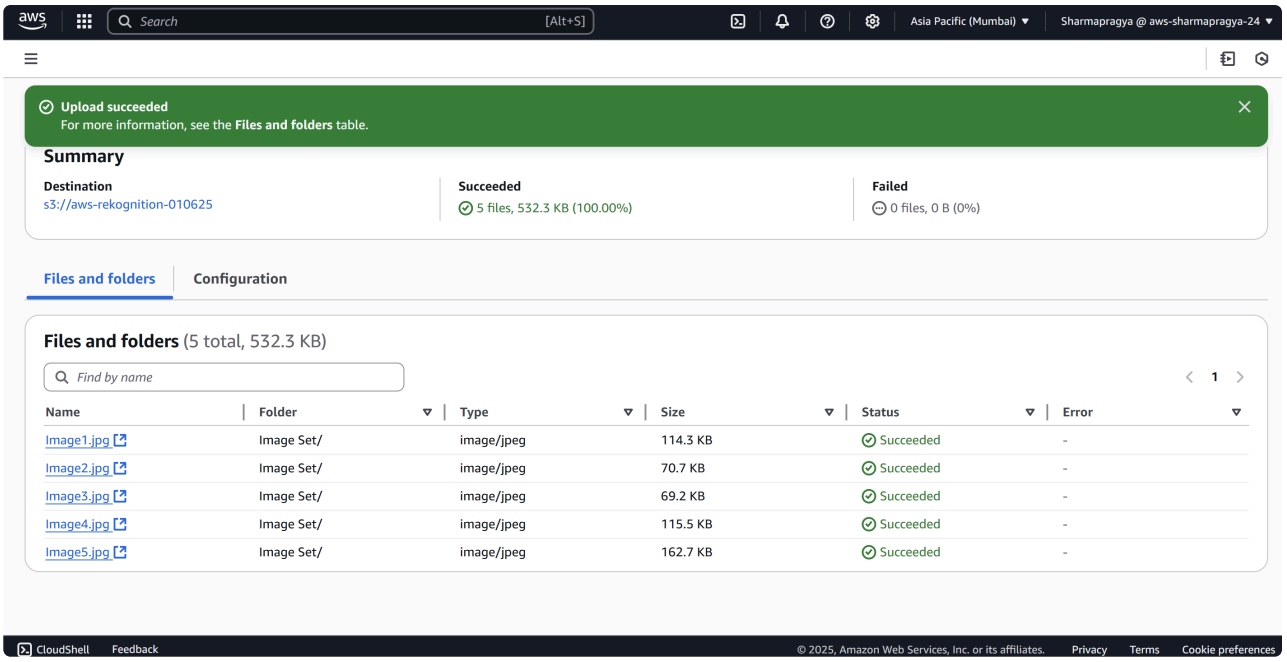




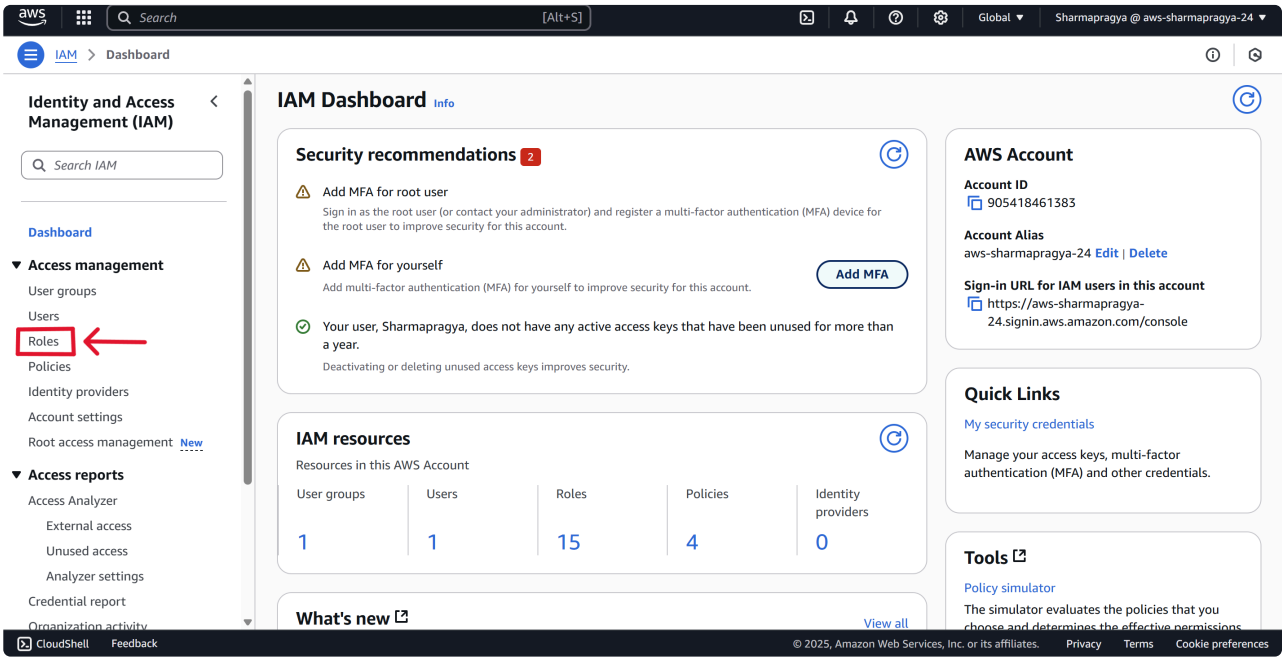
Added Images

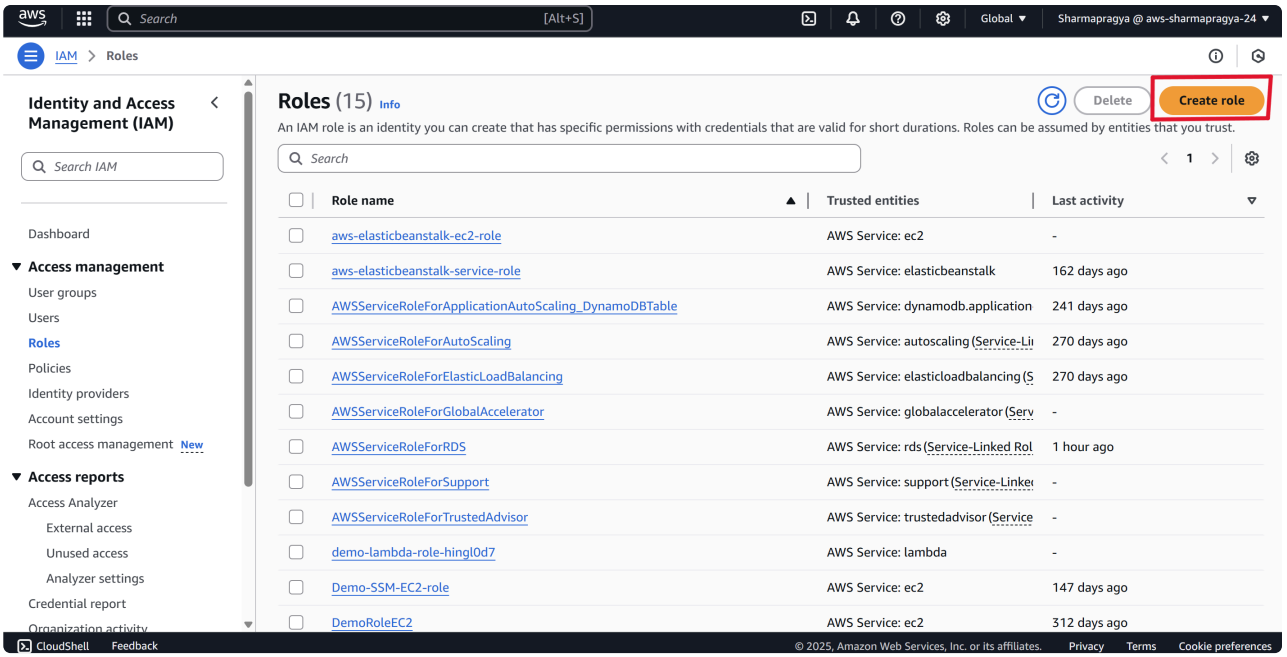

Search [Alt+S]
Asia Pacific (Mumbai)
Sharmapragya @ aws-sharmapragya-24
Amazon S3 > Buckets > aws-rekognition-010625 > Upload
Upload Info
Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDKs or Amazon S3 REST API. Learn more
Drag and drop files and folders you want to upload here, or choose Add files or Add folder.
Files and folders (5 total, 532.3 KB)
Remove
Add files
Add folder
All files and folders in this table will be uploaded.
Find by name
1
Name
Folder
Type
Size
Image1.jpg
Image Set/
image/jpeg
114.3 KB
Image2.jpg
Image Set/
image/jpeg
70.7 KB
Image3.jpg
Image Set/
image/jpeg
69.2 KB
Image4.jpg
Image Set/
image/jpeg
115.5 KB
Image5.jpg
Image Set/
image/jpeg
162.7 KB
Destination Info
Destination
s3://aws-rekognition-010625
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

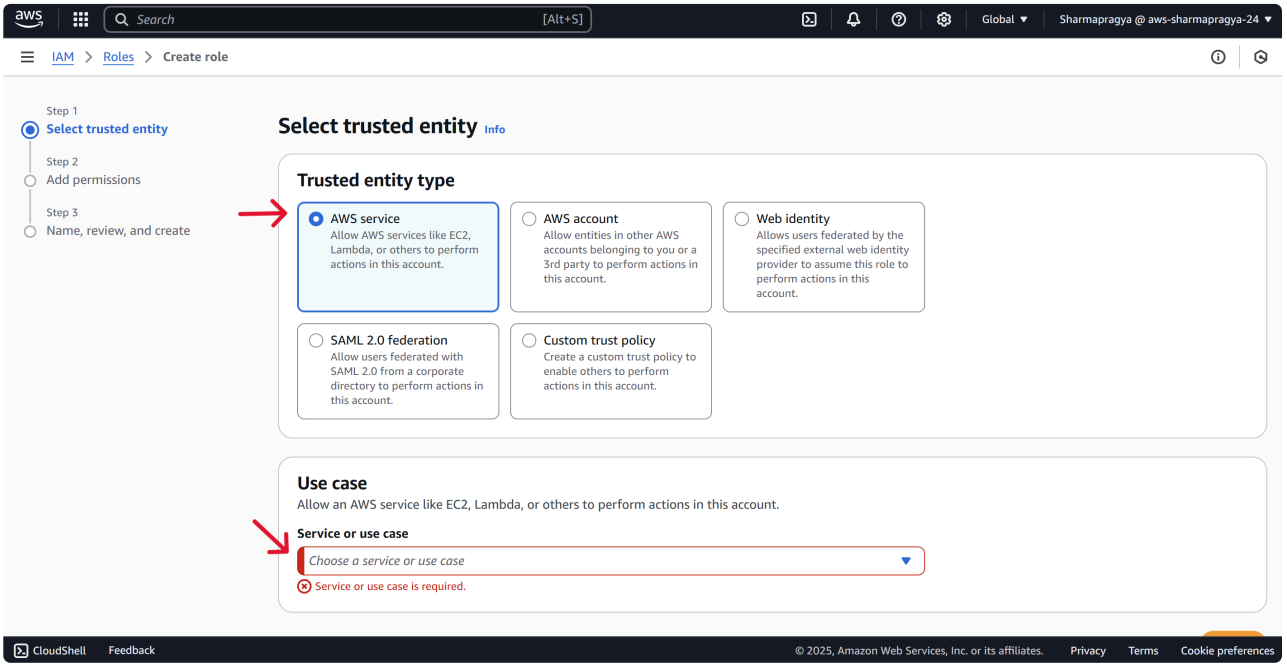

Search [Alt+S]
Asia Pacific (Mumbai)
Sharmapragya @ aws-sharmapragya-24
Amazon S3 > Buckets > aws-rekognition-010625 > Upload
Files and folders (5 total, 532.3 KB)
Remove
Add files
Add folder
All files and folders in this table will be uploaded.
Find by name
1
Name
Folder
Type
Size
Image5.jpg
Image Set/
image/jpeg
162.7 KB
Destination Info
Destination
s3://aws-rekognition-010625
Destination details
Bucket settings that impact new objects stored in the specified destination.
Permissions
Grant public access and access to other AWS accounts.
Properties
Specify storage class, encryption settings, tags, and more.
Cancel
Upload
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

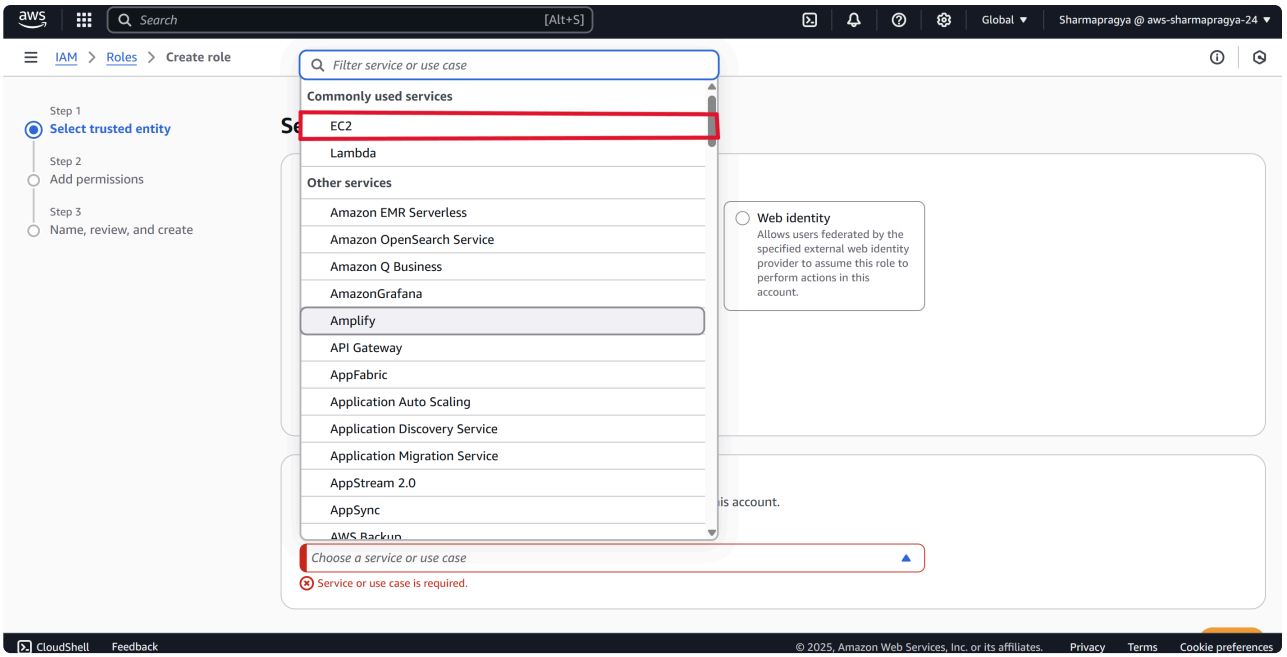


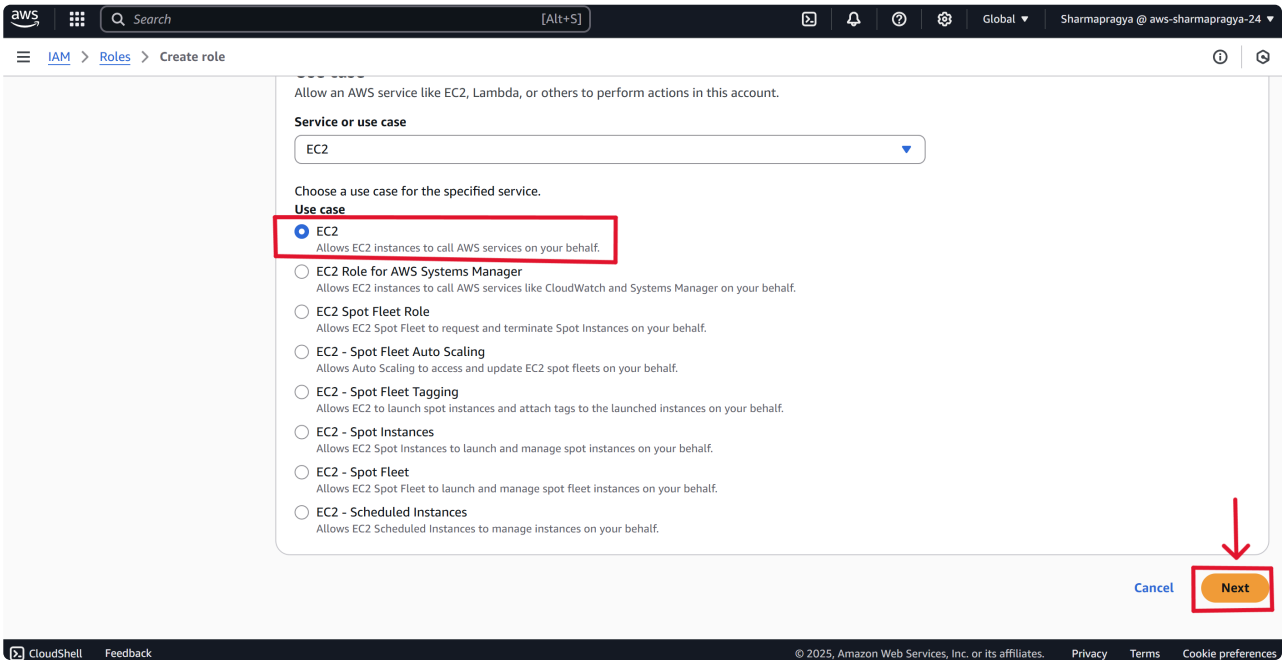
3. Creating an IAM role to make sure s3 and amazon rekognition have access to each other

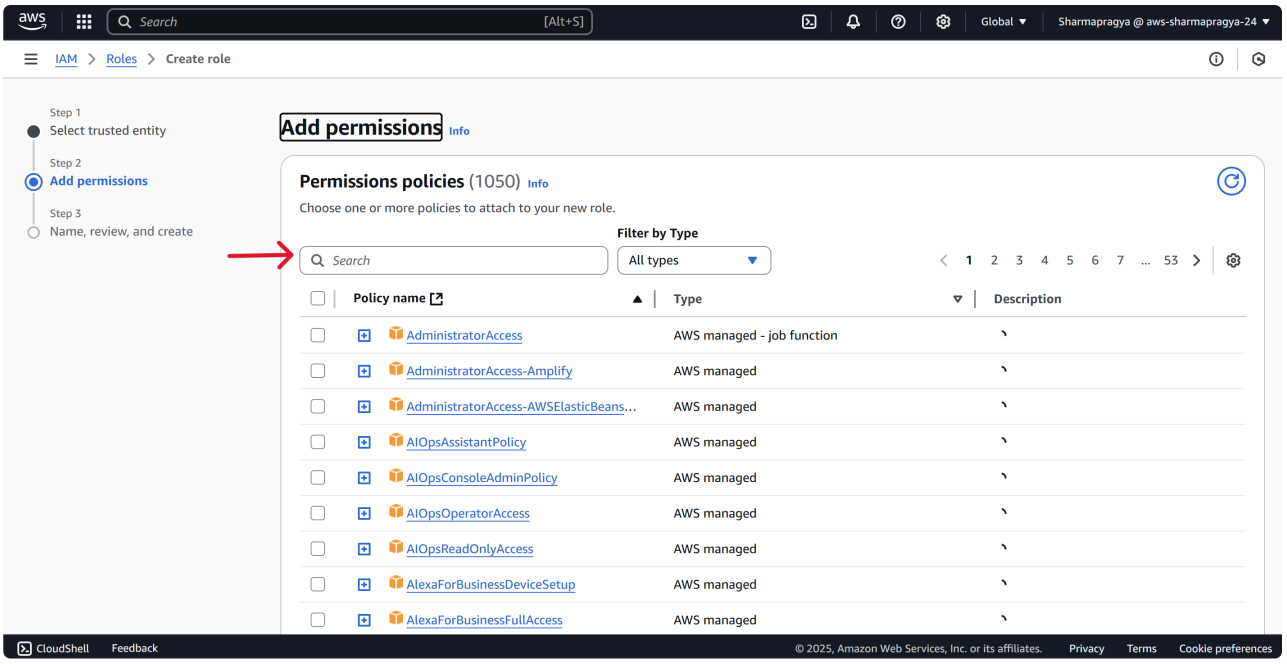


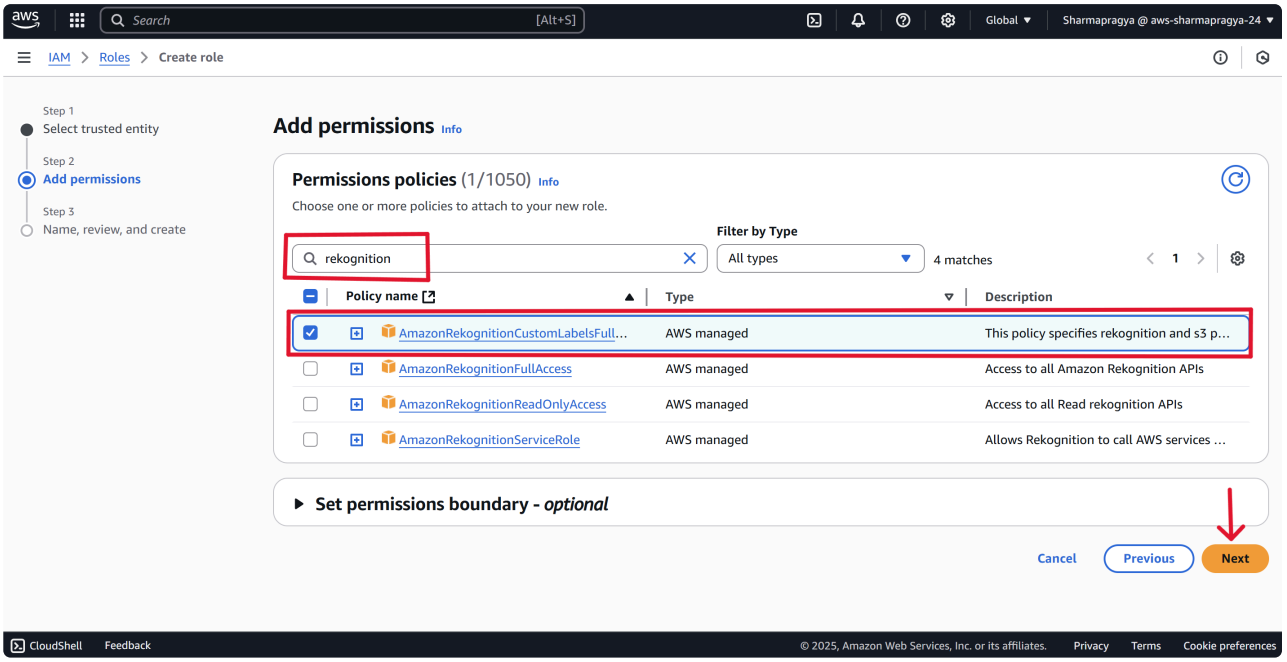

Search [Alt+S]
Global
Sharmapragya @ aws-sharmapragya-24
IAM > Roles
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
Roles (15) Info
An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.
Delete
Create role
Search
Role name
Trusted entities
Last activity
aws-elasticbeanstalk-ec2-role
AWS Service: ec2
aws-elasticbeanstalk-service-role
AWS Service: elasticbeanstalk
162 days ago
AWSServiceRoleForApplicationAutoScaling_DynamoDBTable
AWS Service: dynamodb.application
241 days ago
AWSServiceRoleForAutoScaling
AWS Service: autoscaling (Service-Li
270 days ago
AWSServiceRoleForElasticLoadBalancing
AWS Service: elasticloadbalancing (S
270 days ago
AWSServiceRoleForGlobalAccelerator
AWS Service: globalaccelerator (Serv
AWSServiceRoleForRDS
AWS Service: rds (Service-Linked Rol
1 hour ago
AWSServiceRoleForSupport
AWS Service: support (Service-Linke
AWSServiceRoleForTrustedAdvisor
AWS Service: trustedadvisor (Service
demo-lambda-role-hingl0d7
AWS Service: lambda
Demo-SSM-EC2-role
AWS Service: ec2
147 days ago
DemoRoleEC2
AWS Service: ec2
312 days ago
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

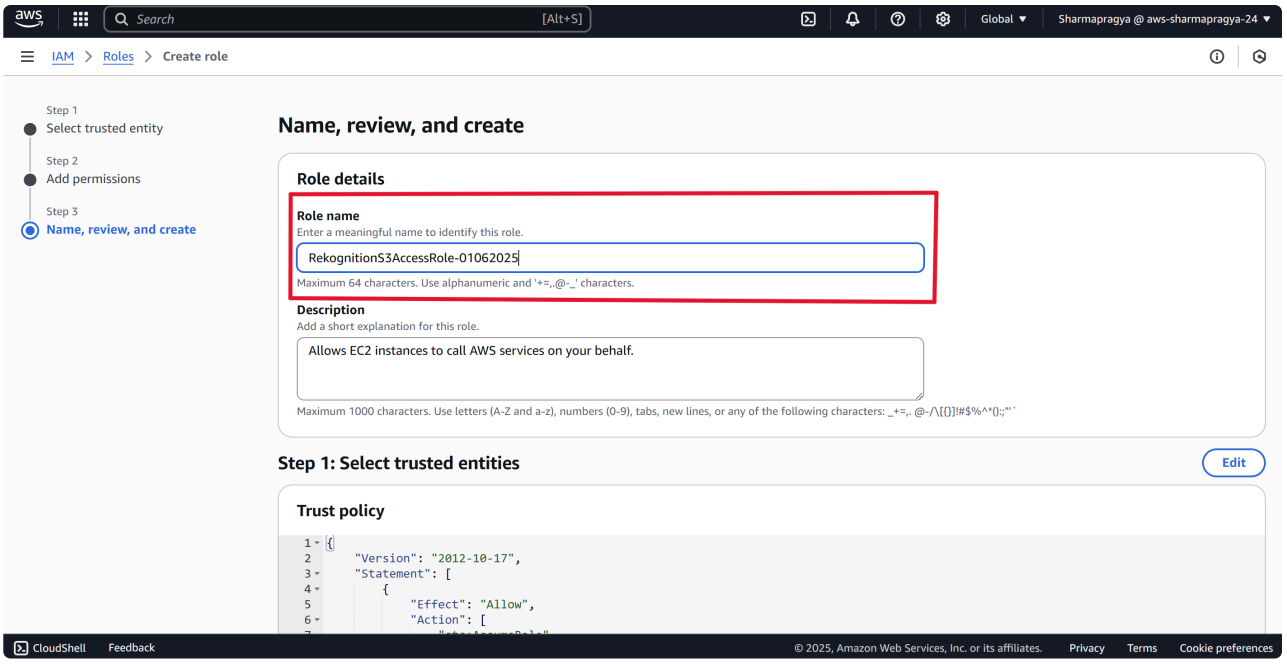

Search [Alt+S]
Global
Sharmapragya @ aws-sharmapragya-24
IAM > Roles > Create role
Step 1
Select trusted entity
Step 2
Add permissions
Step 3
Name, review, and create
Select trusted entity Info
Trusted entity type
AWS service
Allow AWS services like EC2, Lambda, or others to perform actions in this account.
AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.
Web identity
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.
SAML 2.0 federation
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.
Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.
Use case
Allow an AWS service like EC2, Lambda, or others to perform actions in this account.
Service or use case
Choose a service or use case
Service or use case is required.
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

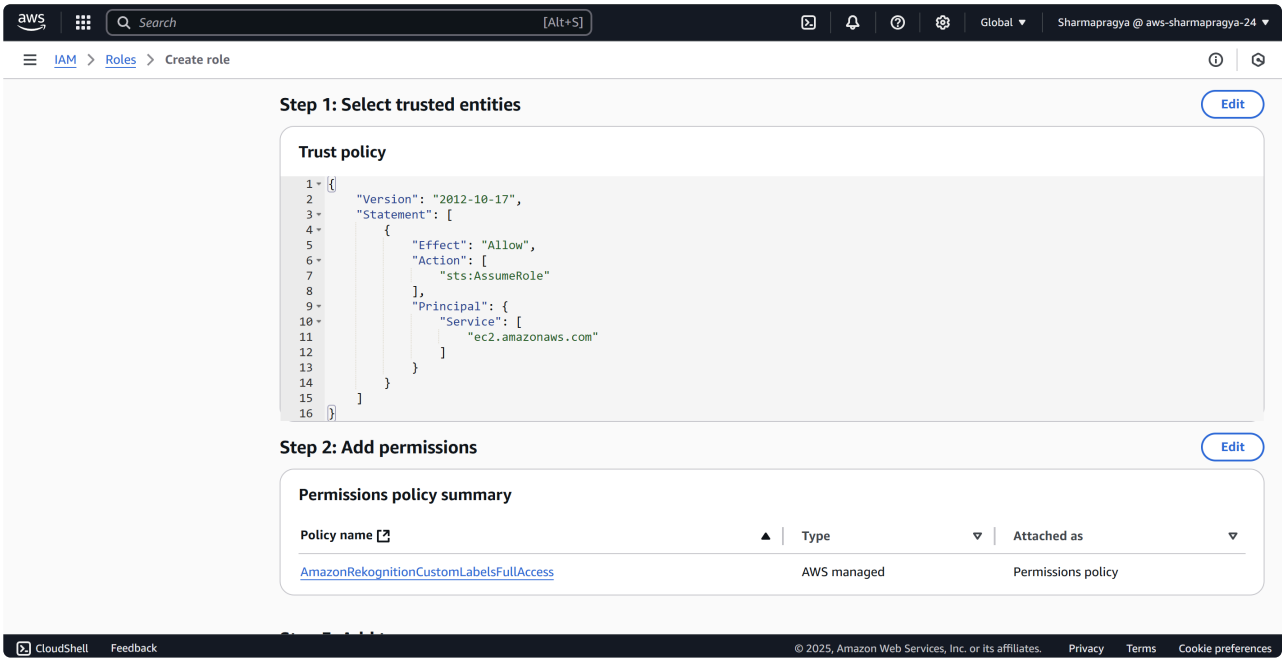

Search
[Alt+S]
Global
Sharmapragya @ aws-sharmapragya-24
IAM
Roles
Create role
Step 1
Select trusted entity
Step 2
Add permissions
Step 3
Name, review, and create
Filter service or use case
Commonly used services
EC2
Lambda
Other services
Amazon EMR Serverless
Amazon OpenSearch Service
Amazon Q Business
AmazonGrafana
Amplify
API Gateway
AppFabric
Application Auto Scaling
Application Discovery Service
Application Migration Service
AppStream 2.0
AppSync
AWS Backup
Web identity
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.
Choose a service or use case
Service or use case is required.
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

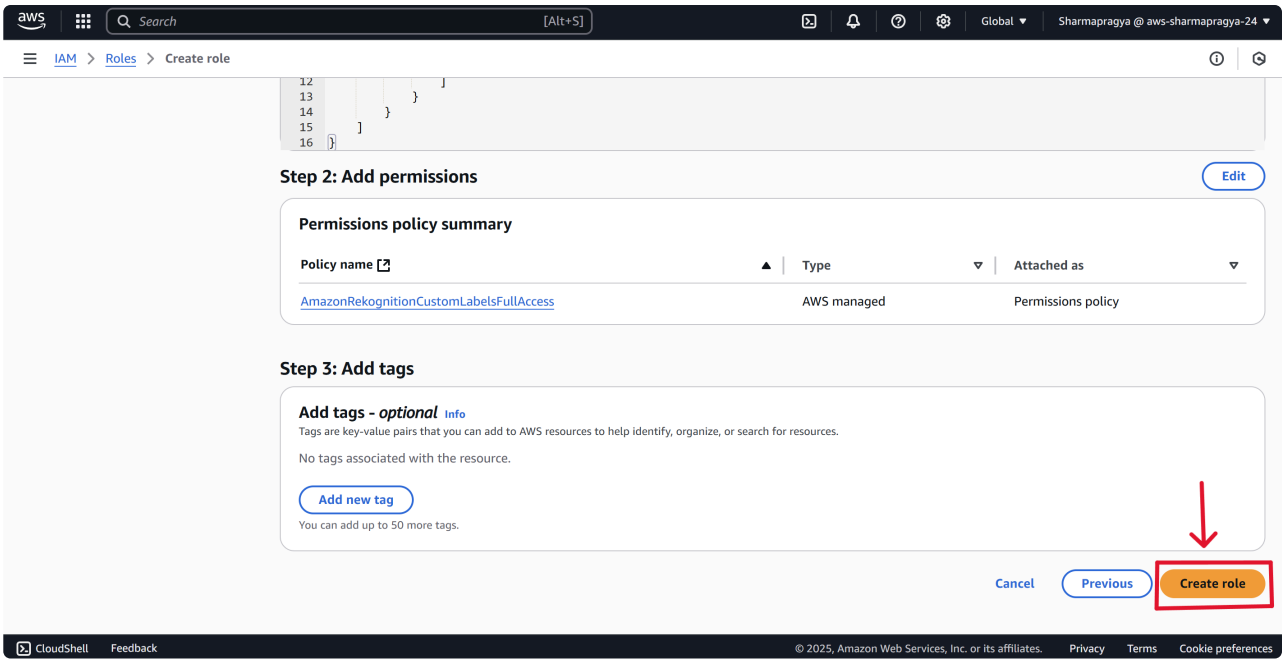

Search
[Alt+S]
Global
Sharmapragya @ aws-sharmapragya-24
IAM
Roles
Create role
Allow an AWS service like EC2, Lambda, or others to perform actions in this account.
Service or use case
EC2
Choose a use case for the specified service.
Use case
EC2
Allows EC2 instances to call AWS services on your behalf.
EC2 Role for AWS Systems Manager
Allows EC2 instances to call AWS services like CloudWatch and Systems Manager on your behalf.
EC2 Spot Fleet Role
Allows EC2 Spot Fleet to request and terminate Spot Instances on your behalf.
EC2 - Spot Fleet Auto Scaling
Allows Auto Scaling to access and update EC2 spot fleets on your behalf.
EC2 - Spot Fleet Tagging
Allows EC2 to launch spot instances and attach tags to the launched instances on your behalf.
EC2 - Spot Instances
Allows EC2 Spot Instances to launch and manage spot instances on your behalf.
EC2 - Spot Fleet
Allows EC2 Spot Fleet to launch and manage spot fleet instances on your behalf.
EC2 - Scheduled Instances
Allows EC2 Scheduled Instances to manage instances on your behalf.
Cancel
Next
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Search [Alt+S]
Global
Sharmapragya @ aws-sharmapragya-24
IAM > Roles > Create role
Step 1
Select trusted entity
Step 2
Add permissions
Step 3
Name, review, and create
Add permissions Info
Permissions policies (1050) Info
Choose one or more policies to attach to your new role.
Search
Filter by Type
All types
1 2 3 4 5 6 7 ... 53
Policy name
Type
Description
AdministratorAccess
AWS managed - job function
AdministratorAccess-Amplify
AWS managed
AdministratorAccess-AWSElasticBeans...
AWS managed
AIOpsAssistantPolicy
AWS managed
AIOpsConsoleAdminPolicy
AWS managed
AIOpsOperatorAccess
AWS managed
AIOpsReadOnlyAccess
AWS managed
AlexaForBusinessDeviceSetup
AWS managed
AlexaForBusinessFullAccess
AWS managed
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

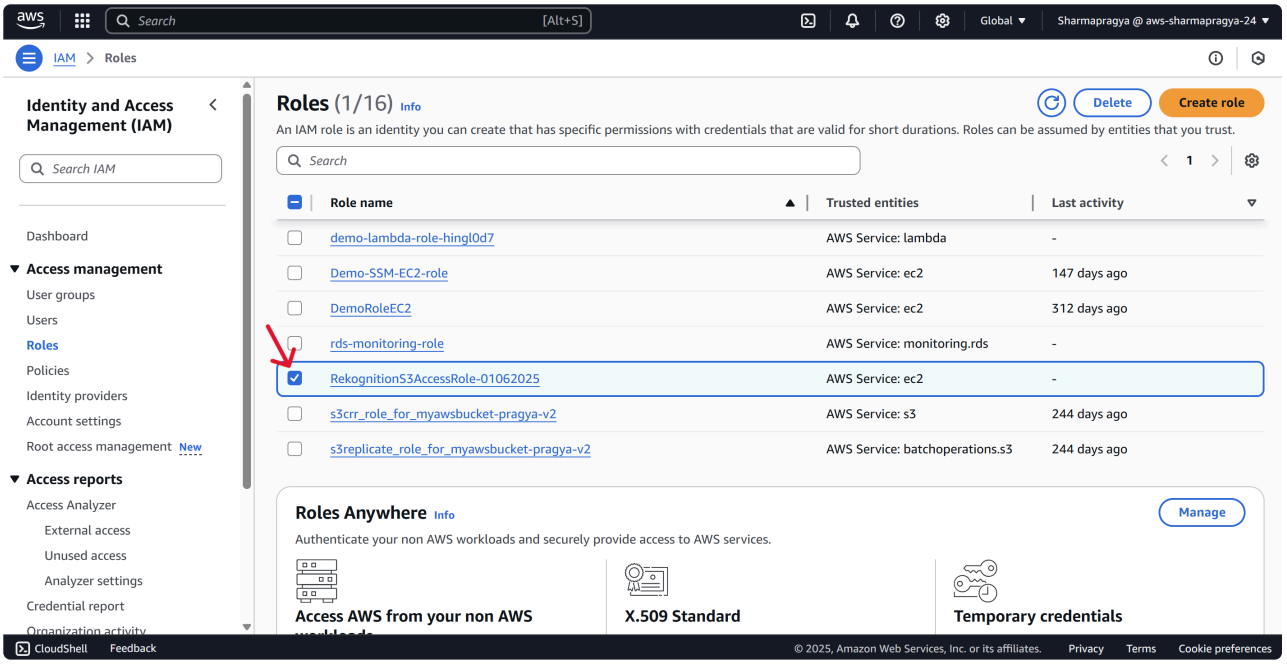

Search [Alt+S]
Global
Sharmapragya @ aws-sharmapragya-24
IAM > Roles > Create role
Step 1
Select trusted entity
Step 2
Add permissions
Step 3
Name, review, and create
Add permissions Info
Permissions policies (1/1050) Info
Choose one or more policies to attach to your new role.
rekognition
Filter by Type
All types
4 matches
1
Policy name
Type
Description
AmazonRekognitionCustomLabelsFull...
AWS managed
This policy specifies rekognition and s3 p...
AmazonRekognitionFullAccess
AWS managed
Access to all Amazon Rekognition APIs
AmazonRekognitionReadOnlyAccess
AWS managed
Access to all Read rekognition APIs
AmazonRekognitionServiceRole
AWS managed
Allows Rekognition to call AWS services ...
Set permissions boundary - optional
Cancel
Previous
Next
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Search [Alt+S]
Global
Sharmapragya @ aws-sharmapragya-24
IAM > Roles > Create role
Step 1
Select trusted entity
Step 2
Add permissions
Step 3
Name, review, and create
Name, review, and create
Role details
Role name
Enter a meaningful name to identify this role.
RekognitionS3AccessRole-01062025
Maximum 64 characters. Use alphanumeric and '+=,.@-_' characters.
Description
Add a short explanation for this role.
Allows EC2 instances to call AWS services on your behalf.
Maximum 1000 characters. Use letters (A-Z and a-z), numbers (0-9), tabs, new lines, or any of the following characters: _+=,. @-/\[{}]!#$%^*();"' `
Step 1: Select trusted entities
Edit
Trust policy
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Action": [
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Search [Alt+S]
Global
Sharmapragya @ aws-sharmapragya-24
IAM > Roles > Create role
Step 1: Select trusted entities
Edit
Trust policy
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Action": [
"sts:AssumeRole"
],
"Principal": {
"Service": [
"ec2.amazonaws.com"
]
}
}
]
}
Step 2: Add permissions
Edit
Permissions policy summary
Policy name
Type
Attached as
AmazonRekognitionCustomLabelsFullAccess
AWS managed
Permissions policy
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

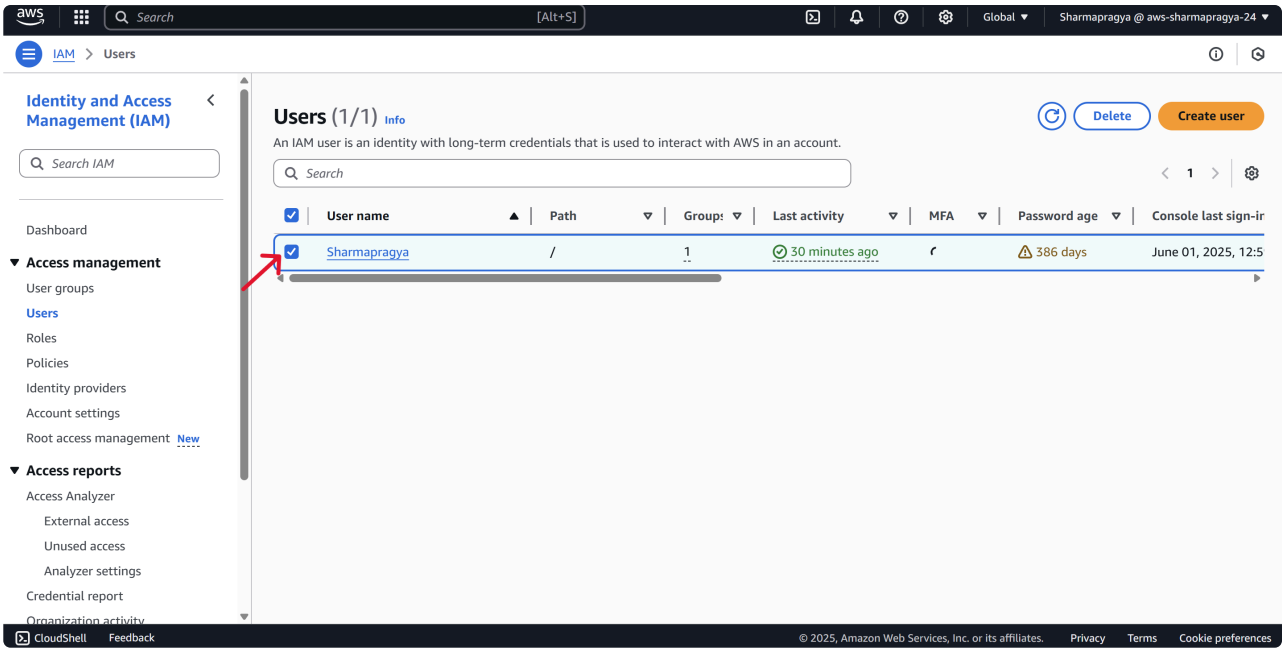


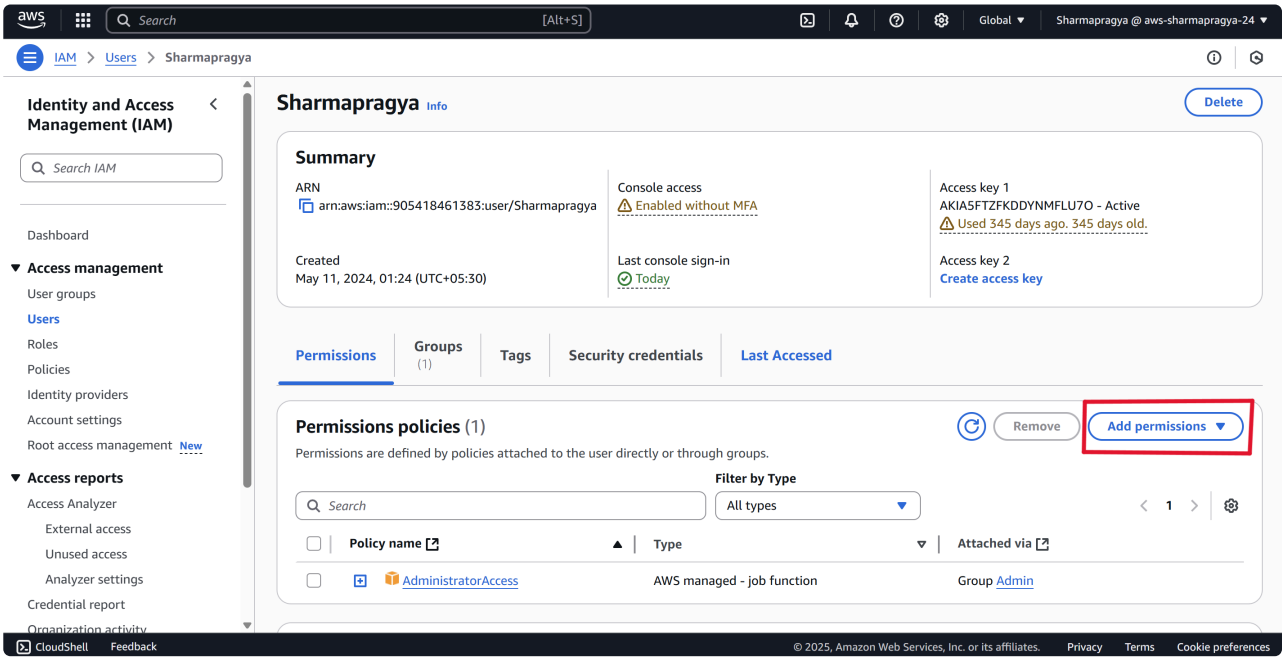
**Our Created role

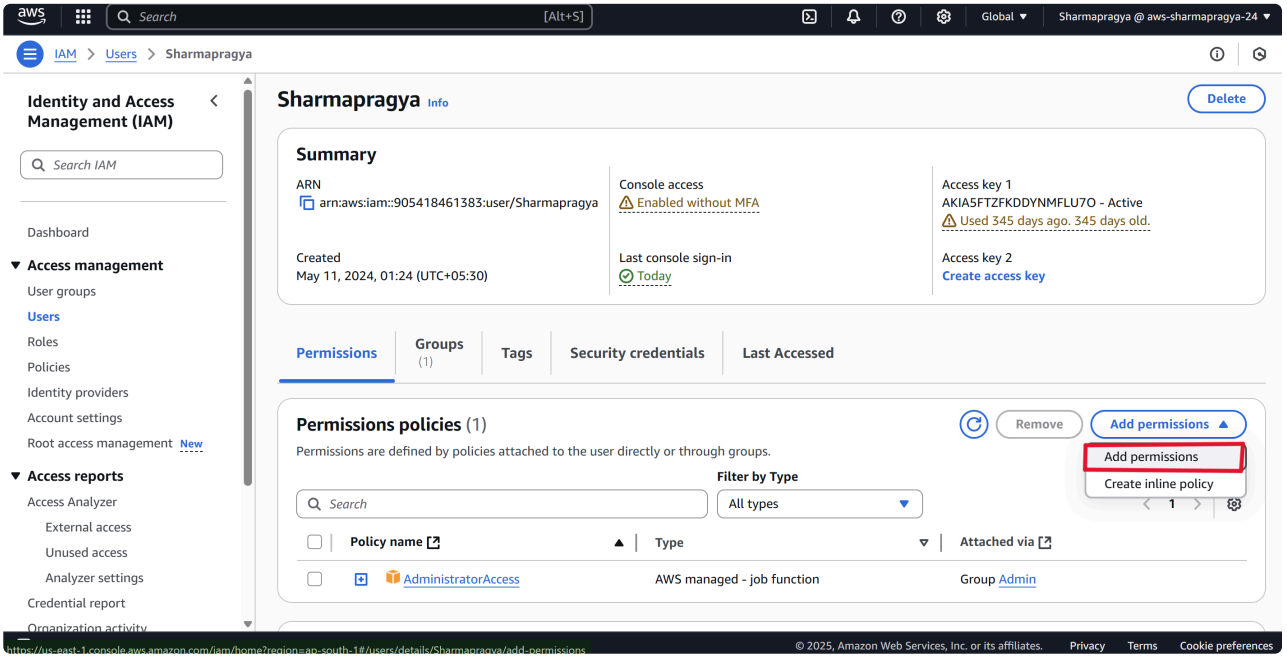


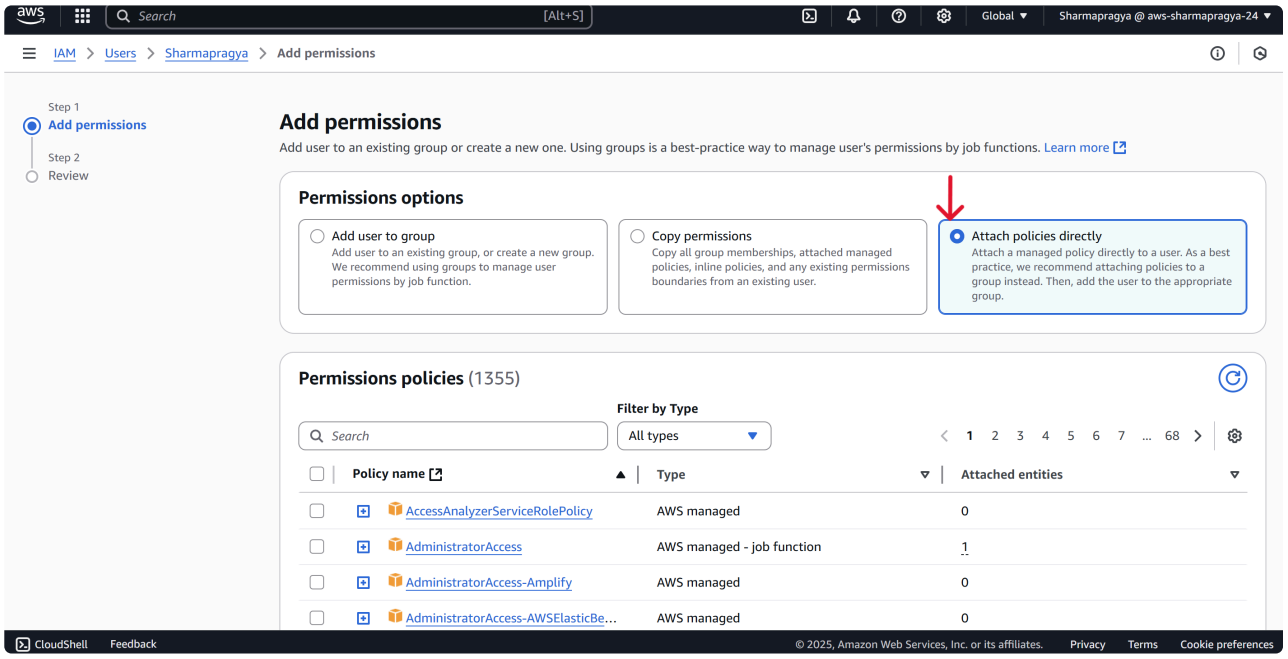
4. Setting up IAM policy for user

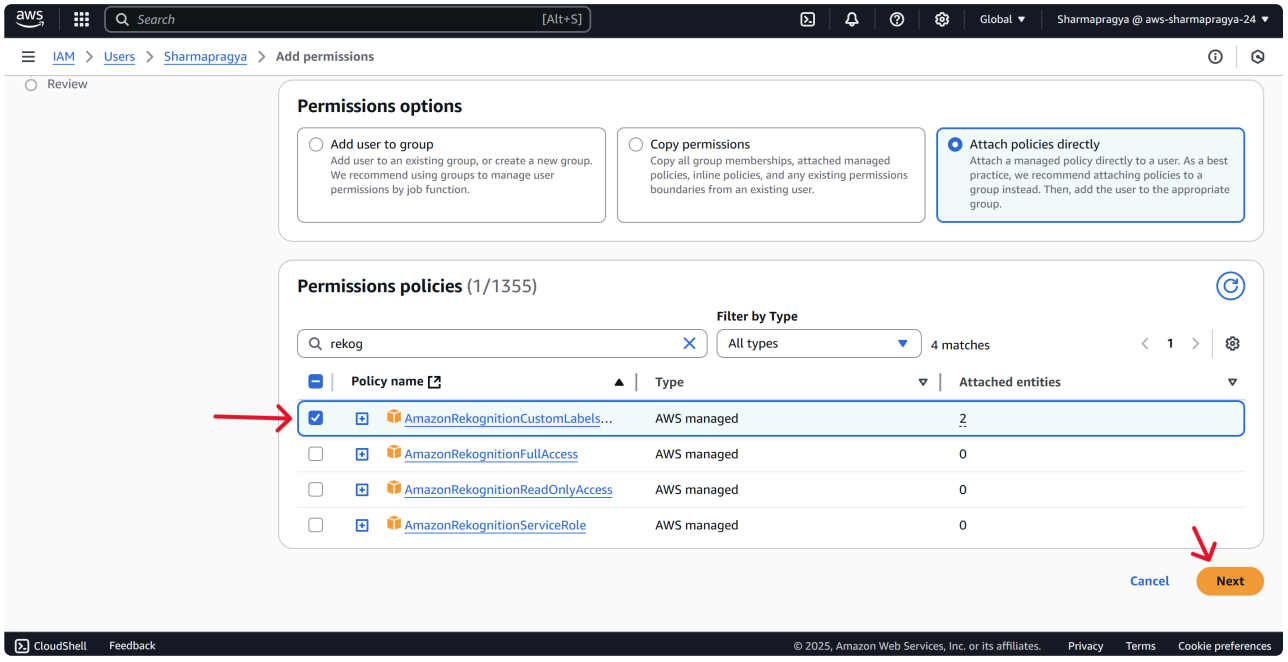
   We needed an **IAM policy** for the user in **Amazon CloudShell** because **CloudShell runs with your IAM user's permissions**, so without the correct permissions, it cannot access **Amazon S3** or **Amazon Rekognition**.

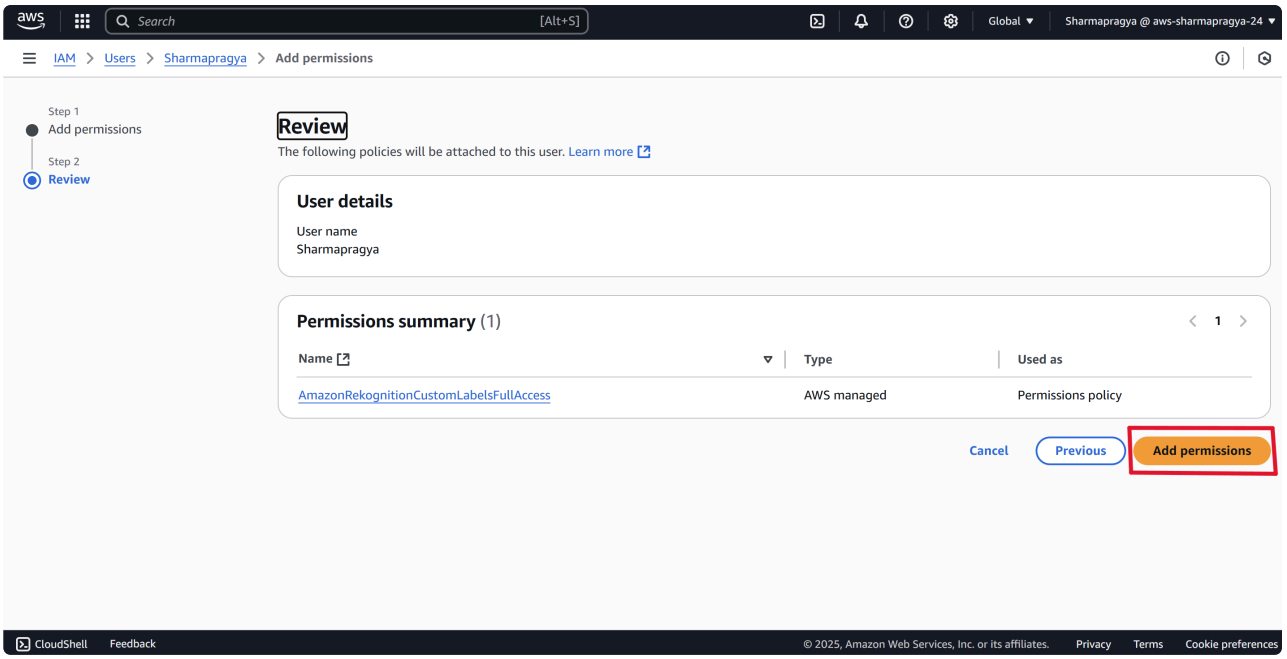

Search [Alt+S]
Global
Sharmapragya @ aws-sharmapragya-24
IAM > Users
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
Organization activity
Users (1/1) 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
Groups
Last activity
MFA
Password age
Console last sign-in
Sharmapragya
/
1
30 minutes ago
386 days
June 01, 2025, 12:5
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

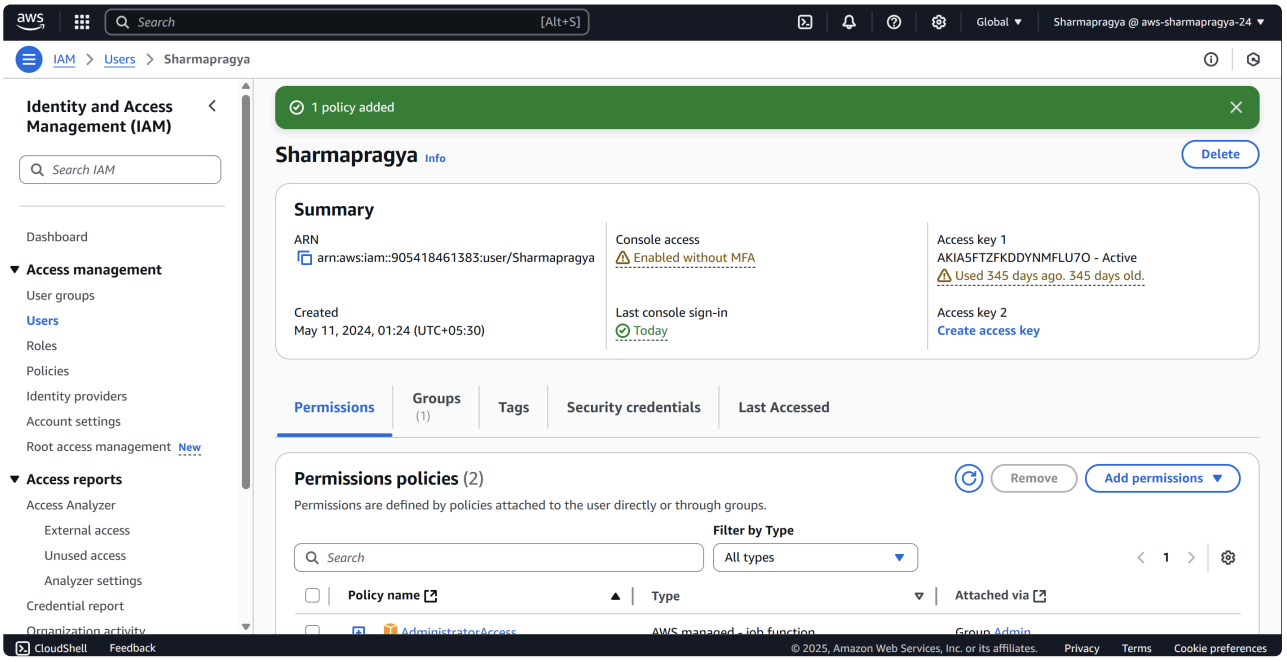

Search [Alt+S]
Global
Sharmapragya @ aws-sharmapragya-24
IAM > Users > Sharmapragya
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
Organization activity
Sharmapragya Info
Delete
Summary
ARN
arn:aws:iam::905418461383:user/Sharmapragya
Console access
Enabled without MFA
Access key 1
AKIA5FTZFKDDYNMFLU7O - Active
Used 345 days ago. 345 days old.
Created
May 11, 2024, 01:24 (UTC+05:30)
Last console sign-in
Today
Access key 2
Create access key
Permissions
Groups (1)
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
AdministratorAccess
AWS managed - job function
Group Admin
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Search [Alt+S]
Global
Sharmapragya @ aws-sharmapragya-24
IAM > Users > Sharmapragya
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Root access management New
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
Organization activity
Sharmapragya Info
Delete
Summary
ARN
arn:aws:iam::905418461383:user/Sharmapragya
Console access
Enabled without MFA
Access key 1
AKIA5FTZFKDDYNMFLU7O - Active
Used 345 days ago. 345 days old.
Created
May 11, 2024, 01:24 (UTC+05:30)
Last console sign-in
Today
Access key 2
Create access key
Permissions
Groups (1)
Tags
Security credentials
Last Accessed
Permissions policies (1)
Permissions are defined by policies attached to the user directly or through groups.
Remove
Add permissions
Add permissions
Create inline policy
Filter by Type
Search
All types
Policy name
Type
Attached via
AdministratorAccess
AWS managed - job function
Group Admin
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

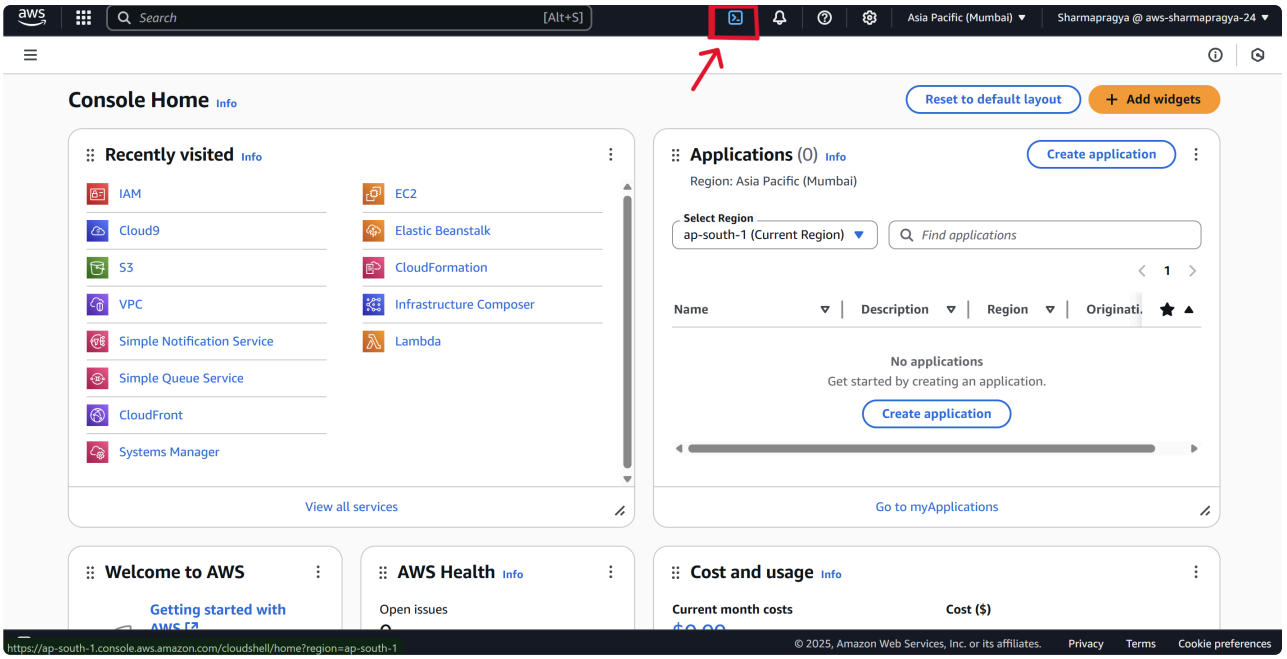

Search [Alt+S]
Global
Sharmapragya @ aws-sharmapragya-24
IAM > Users > Sharmapragya > Add permissions
Step 1
Add permissions
Step 2
Review
Add permissions
Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. Learn more
Permissions 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, inline policies, and any existing permissions boundaries 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 (1355)
Filter by Type
Search
All types
1 2 3 4 5 6 7 ... 68
Policy name
Type
Attached entities
AccessAnalyzerServiceRolePolicy AWS managed 0
AdministratorAccess AWS managed - job function 1
AdministratorAccess-Amplify AWS managed 0
AdministratorAccess-AWSElasticBe... AWS managed 0
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Search [Alt+S]
Global
Sharmapragya @ aws-sharmapragya-24
IAM > Users > Sharmapragya > Add permissions
Review
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, inline policies, and any existing permissions boundaries 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 (1/1355)
Filter by Type
rekog
All types
4 matches
1
Policy name
Type
Attached entities
AmazonRekognitionCustomLabels... AWS managed 2
AmazonRekognitionFullAccess AWS managed 0
AmazonRekognitionReadOnlyAccess AWS managed 0
AmazonRekognitionServiceRole AWS managed 0
Cancel
Next
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

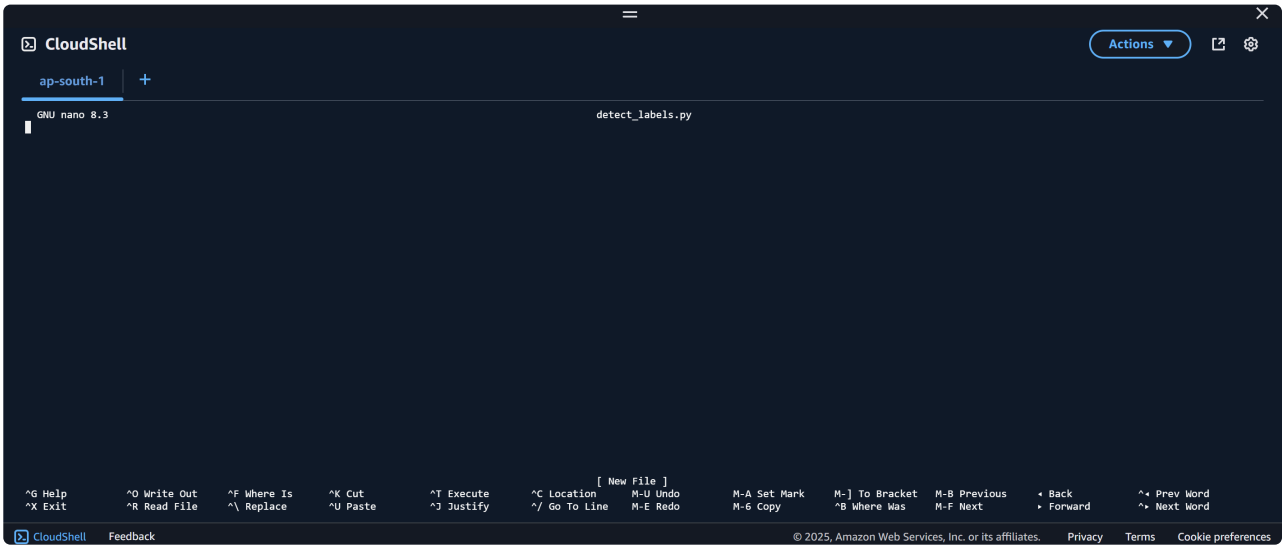




5. Now run amazon cloudshell for our amazon rekognition to work



6. Creating a python file for image rekognition in amazon cloudshell



7. Run our python file

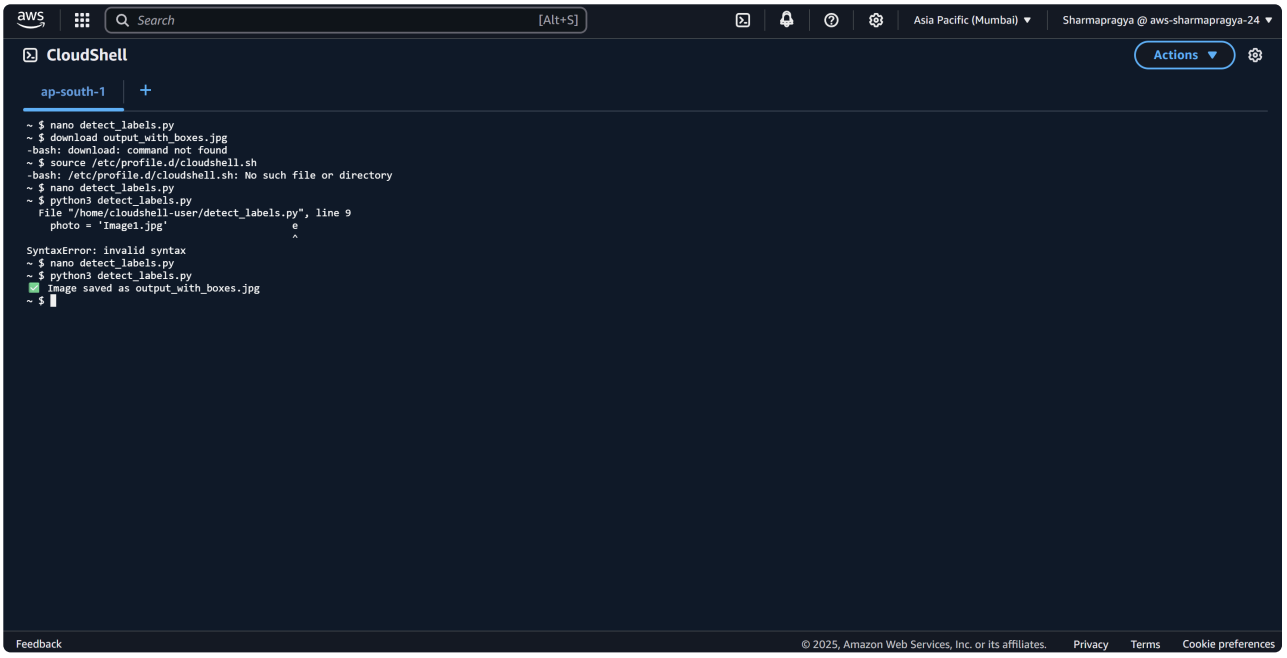
8. install matplotlib if not by running command

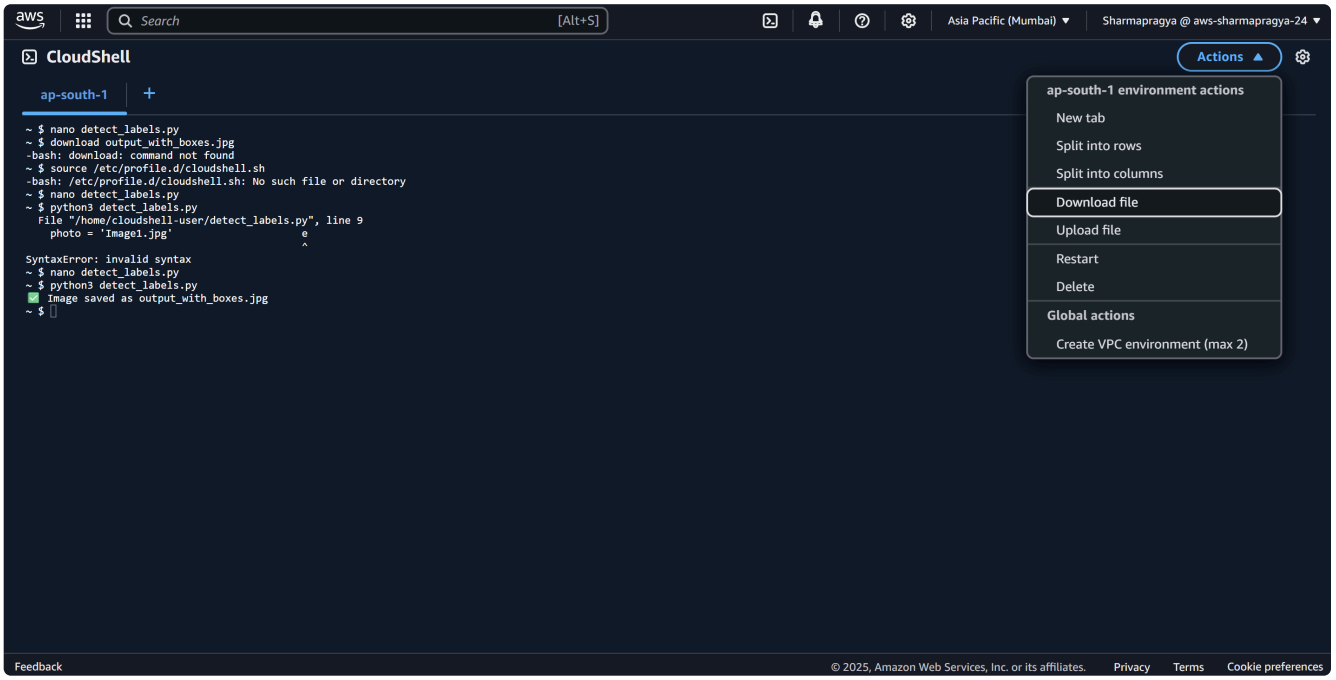
```
pip3 install --user matplotlib
```

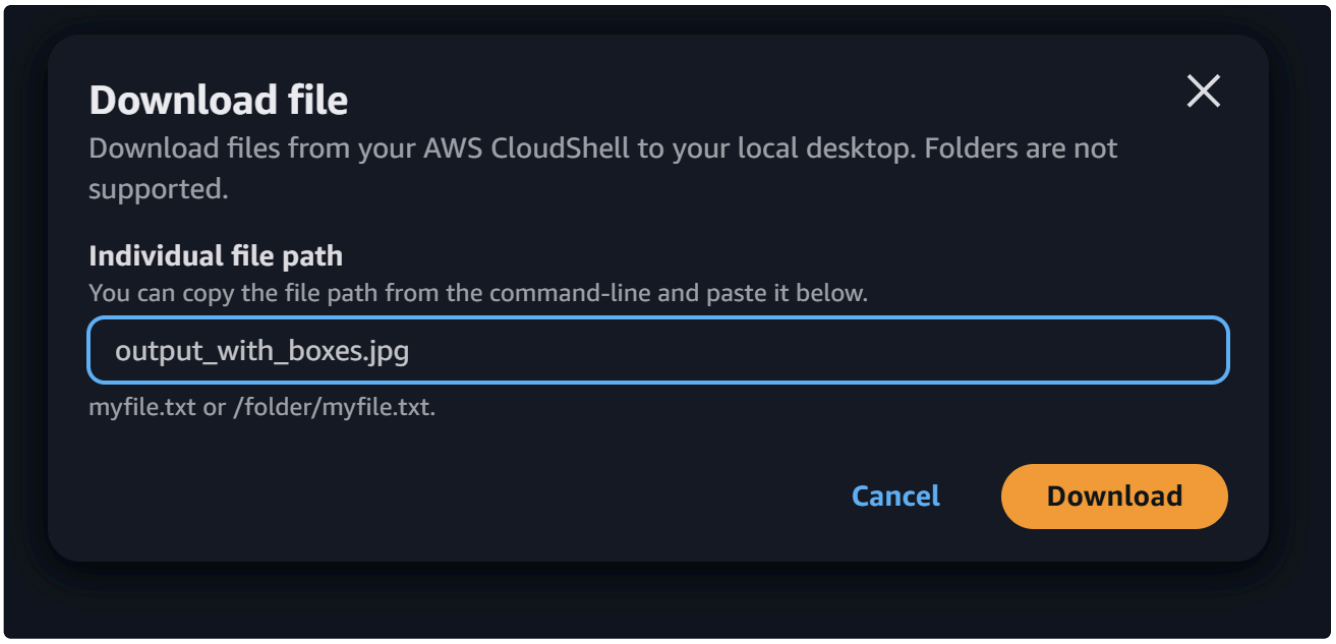
9. Run python file

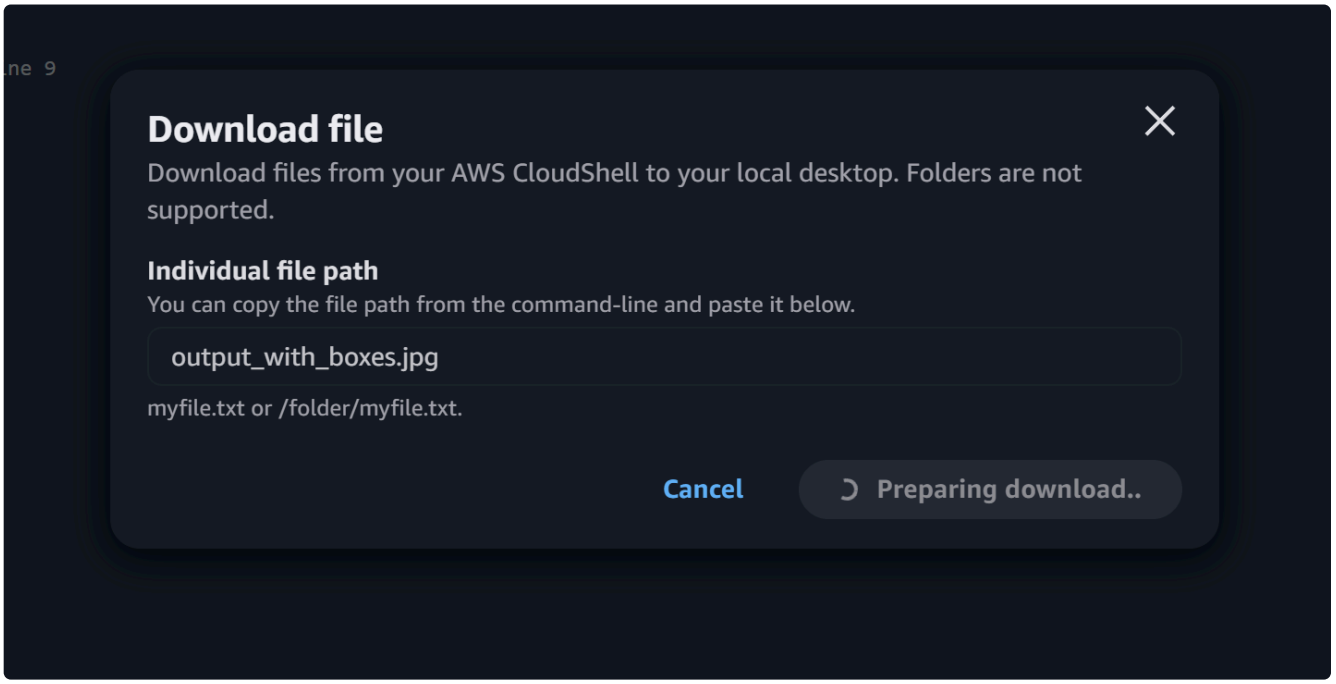
```
python3 detect_labels.py
```

10. Download the processed image by using the following command



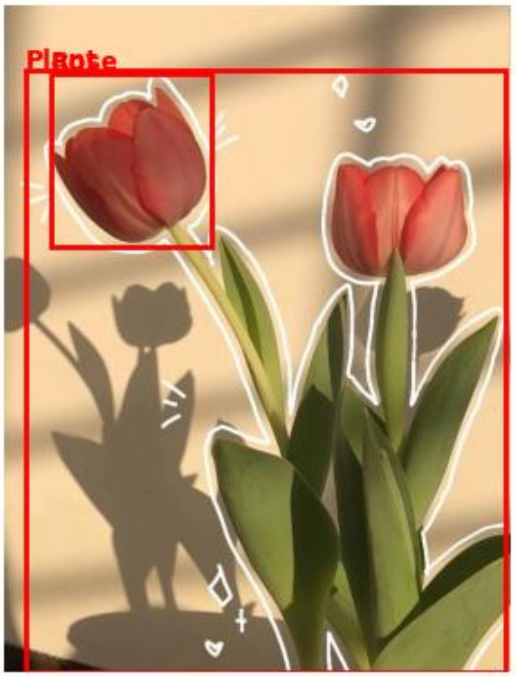






11. The image will be downloaded to your system

Below are some images processed by amazon rekognition


Plant


Person
Candle
Mobile Phone


Person