

Build an Image Label Generator using Amazon Rekognition

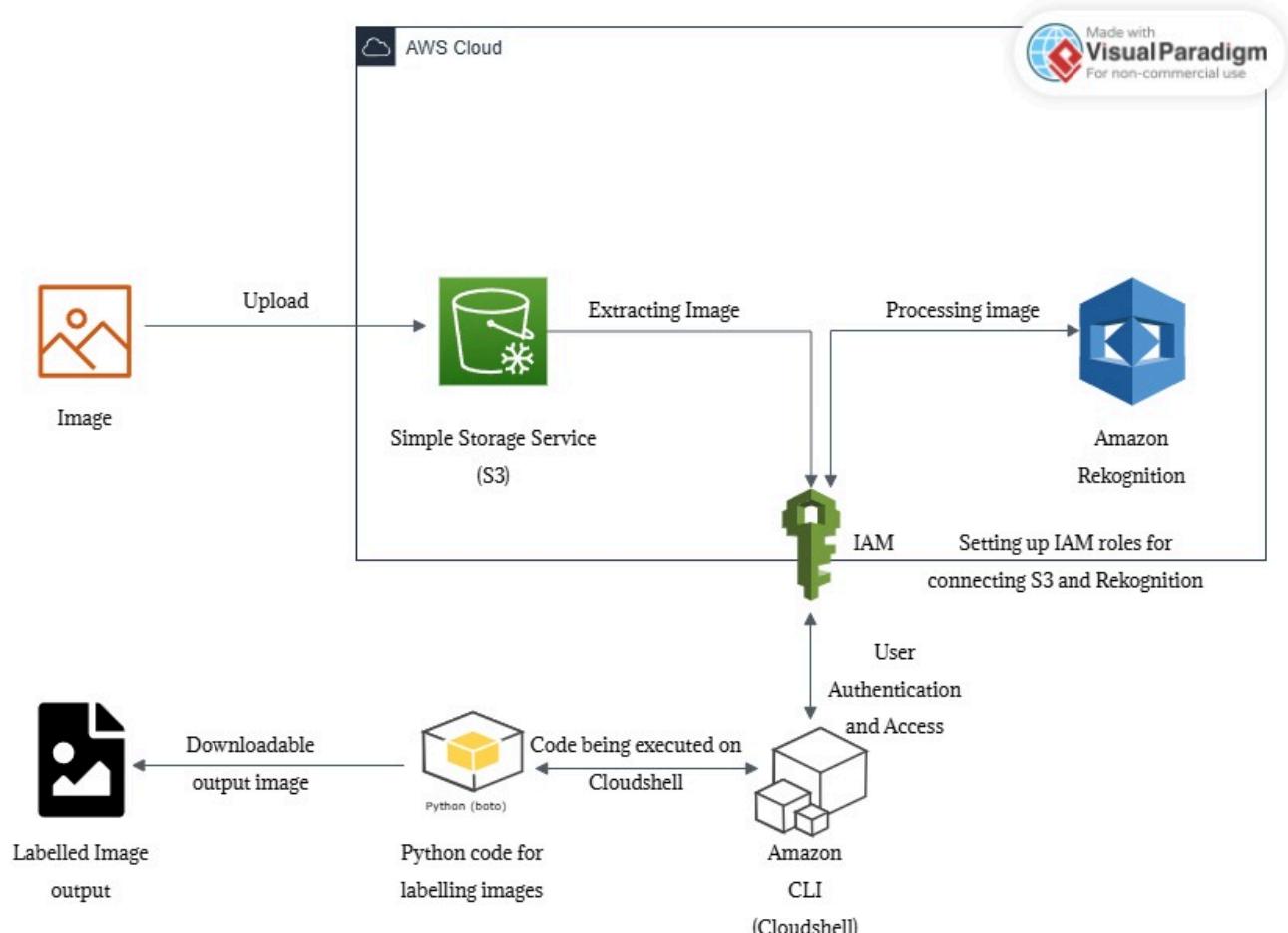
Here we will be processing images and labelling them

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.

AWS Search [Alt+S] Asia Pacific (Mumbai) Sharmapragna @ aws-sharmapragna-24

Console Home

Recently visited: VPC, Simple Notification Service, Simple Queue Service, S3 (highlighted), CloudFront, Systems Manager, EC2, IAM.

Applications (0): Region: Asia Pacific (Mumbai). Create application.

Welcome to AWS: Getting started with AWS.

AWS Health: Open issues.

Cost and usage: Current month costs \$0.00, Cost (\$).

CloudShell Feedback

AWS Search [Alt+S] Asia Pacific (Mumbai) Sharmapragna @ aws-sharmapragna-24

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): View Storage Lens dashboard.

General purpose buckets (8): Create bucket (highlighted).

Name	AWS Region	IAM Access Analyzer	Created date
cf-templates-xqkio5zuas5x-eu-north-1	Europe (Stockholm) eu-north-1	View analyzer for eu-north-1	December 20, 2023 13:14:5 (UTC+0)
cf-templates-xqkio5zuas5x-us-east-1	US East (N. Virginia) us-east-1	View analyzer for us-east-1	December 20, 2023 13:20:0 (UTC+0)
democloudfront-s3-bucket	Europe (Stockholm) eu-north-1	View analyzer for eu-north-1	January 2025, 00:03:5

CloudShell Feedback

AWS Search [Alt+S] Asia Pacific (Mumbai) Sharmapragna @ aws-sharmapragna-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

AWS Search [Alt+S] Asia Pacific (Mumbai) Sharmapragna @ aws-sharmapragna-24

Amazon S3 > Buckets > Create bucket

Object Ownership

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

aws | 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

aws | 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

(i) After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.

[Create bucket](#) (highlighted with a red box and arrow pointing down)

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

aws | 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](#) (highlighted with a red box)

► 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.

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)
mvawshurkett-pragya	Asia Pacific (Mumbai) ap-south-1	View analyzer for ap-south-1	September 17, 2024, 14:52:38 (UTC+05:30)

[Copy ARN](#) [Empty](#) [Delete](#) [Create bucket](#)

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

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

The screenshot shows the AWS S3 console with the following details:

- Breadcrumbs:** Amazon S3 > Buckets > aws-rekognition-010625
- Bucket Name:** aws-rekognition-010625
- Region:** Asia Pacific (Mumbai)
- User:** Sharmapragna @ aws-sharmapragna-24
- Object List:** Objects (0). A message states: "No objects. You don't have any objects in this bucket." A red box highlights the "Upload" button.
- Actions:** Copy S3 URI, Copy URL, Download, Open, Delete, Actions, Create folder, Upload.
- Filtering:** Find objects by prefix, Type (Name), Last modified, Size, Storage class.
- Bottom Navigation:** CloudShell, Feedback.

The screenshot shows the AWS S3 'Upload' page for the 'aws-rekognition-010625' bucket:

- Breadcrumbs:** Amazon S3 > Buckets > aws-rekognition-010625 > Upload
- Title:** Upload
- Instructions:** 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.
- Upload Area:** A large red-bordered box indicates where files can be dragged and dropped or selected via 'Add files' or 'Add folder'.
- Files and folders:** Files and folders (0). All files and folders in this table will be uploaded. A red box highlights the 'Add files' and 'Add folder' buttons.
- Destination:** Destination: s3://aws-rekognition-010625. A red box highlights the destination URL.
- Destination details:** Bucket settings that impact new objects stored in the specified destination.
- Bottom Navigation:** CloudShell, Feedback.

Added Images

Screenshot of the AWS S3 Upload interface showing five files selected for 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)

All files and folders in this table will be uploaded.

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

Screenshot of the AWS S3 Upload interface showing five files selected for upload, with one file removed.

Upload

Files and folders (5 total, 532.3 KB)

All files and folders in this table will be uploaded.

Name	Folder	Type	Size
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>

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

Upload succeeded
For more information, see the [Files and folders table](#).

Summary

Destination	Succeeded	Failed
s3://aws-rekognition-010625	5 files, 532.3 KB (100.00%)	0 files, 0 B (0%)

Files and folders (5 total, 532.3 KB)

Name	Folder	Type	Size	Status	Error
Image1.jpg	Image Set/	image/jpeg	114.3 KB	Succeeded	-
Image2.jpg	Image Set/	image/jpeg	70.7 KB	Succeeded	-
Image3.jpg	Image Set/	image/jpeg	69.2 KB	Succeeded	-
Image4.jpg	Image Set/	image/jpeg	115.5 KB	Succeeded	-
Image5.jpg	Image Set/	image/jpeg	162.7 KB	Succeeded	-

[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

IAM Dashboard [Info](#)

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

[CloudShell](#) [Feedback](#)

IAM Dashboard [Info](#)

Security recommendations

- Add MFA for root user**
Sign in as the root user (or contact your administrator) and register a multi-factor authentication (MFA) device for the root user to improve security for this account.
- Add MFA for yourself**
Add multi-factor authentication (MFA) for yourself to improve security for this account. [Add MFA](#)
- Your user, Sharmapragya, does not have any active access keys that have been unused for more than a year.**
Deactivating or deleting unused access keys improves security.

AWS Account

- Account ID: 905418461383
- Account Alias: aws-sharmapragya-24 [Edit](#) | [Delete](#)
- Sign-in URL for IAM users in this account: <https://aws-sharmapragya-24.signin.aws.amazon.com/console>

IAM resources

Resources in this AWS Account

User groups	Users	Roles	Policies	Identity providers
1	1	15	4	0

Quick Links

- [My security credentials](#)
Manage your access keys, multi-factor authentication (MFA) and other credentials.

Tools

The simulator evaluates the policies that you choose and determines the effective permissions.

© 2025, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

Identity and Access Management (IAM)			
Search IAM [Alt+S]			
Dashboard			
Access management			
User groups Users Roles Policies Identity providers Account settings Root access management <small>New</small>			
Access reports			
Access Analyzer External access Unused access Analyzer settings Credential report Organization activity			
CloudShell Feedback			

Roles (15) <small>Info</small>		
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.		
<input type="text"/> 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-Linker	-
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

Step 1			
<input checked="" type="radio"/> Select trusted entity <input type="radio"/> Step 2 <input type="radio"/> Add permissions <input type="radio"/> Step 3 <input type="radio"/> Name, review, and create	<h3>Select trusted entity <small>Info</small></h3> <p>Trusted entity type</p> <ul style="list-style-type: none"> <input checked="" type="radio"/> AWS service Allow AWS services like EC2, Lambda, or others to perform actions in this account. <input type="radio"/> AWS account Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account. <input type="radio"/> Web identity Allows users federated by the specified external web identity provider to assume this role to perform actions in this account. <input type="radio"/> SAML 2.0 federation Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account. <input type="radio"/> Custom trust policy Create a custom trust policy to enable others to perform actions in this account. <p>Use case Allow an AWS service like EC2, Lambda, or others to perform actions in this account.</p> <p>Service or use case</p> <p><input type="text" value="Choose a service or use case"/></p> <p><small>Service or use case is required.</small></p>		

Screenshot of the AWS IAM 'Create role' wizard Step 1: Select trusted entity.

The service dropdown shows 'EC2' selected. A callout box highlights the 'Web identity' option, which is described as allowing users federated by an external provider to assume the role.

Below the dropdown, a note states: "Choose a service or use case. Service or use case is required."

Screenshot of the AWS IAM 'Create role' wizard Step 2: Choose a use case for the specified service.

The 'Service or use case' dropdown is set to 'EC2'. The 'Use case' section shows the 'EC2' option selected, with a callout box describing it as allowing EC2 instances to call AWS services on behalf of the user.

A red arrow points from the 'Next' button at the bottom right towards the 'Next' button in the screenshot above.

Screenshot of the AWS IAM 'Create role' wizard Step 2: Add permissions.

The search bar shows 'AdministratorAccess'. A red arrow points to the search bar.

Permissions policies (1050)

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	

Screenshot of the AWS IAM 'Create role' wizard Step 2: Add permissions.

The search bar shows 'rekognition'. A red box highlights the search bar and the results table. A red arrow points to the highlighted row 'AmazonRekognitionCustomLabelsFull...'. Another red arrow points to the 'Next' button at the bottom right.

Permissions policies (1/1050)

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

aws 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.
 Maximum 64 characters. Use alphanumeric and '-_=.,@/_-' characters.

Description
Add a short explanation for this role.
 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

```
1 ~ [ {  
2 ~ "Version": "2012-10-17",  
3 ~ "Statement": [  
4 ~ {  
5 ~ "Effect": "Allow",  
6 ~ "Action": [  
7 ~ "sts:AssumeRole"  
8 ~ ]},  
9 ~ "Principal": {  
10 ~ "Service": [  
11 ~ "ec2.amazonaws.com"  
12 ~ ]}  
13 ~ }]  
14 ~ ]  
15 ~ ]  
16 ~ ]
```

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

aws Search [Alt+S] Global Sharmapragya @ aws-sharmapragya-24

☰ IAM > Roles > Create role

Step 1: Select trusted entities

Edit

Trust policy

```
1 ~ [ {  
2 ~ "Version": "2012-10-17",  
3 ~ "Statement": [  
4 ~ {  
5 ~ "Effect": "Allow",  
6 ~ "Action": [  
7 ~ "sts:AssumeRole"  
8 ~ ]},  
9 ~ "Principal": {  
10 ~ "Service": [  
11 ~ "ec2.amazonaws.com"  
12 ~ ]}  
13 ~ }]  
14 ~ ]  
15 ~ ]  
16 ~ ]
```

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

Screenshot of the AWS IAM 'Create role' wizard Step 2: Add permissions.

The policy summary table shows:

Policy name	Type	Attached as
AmazonRekognitionCustomLabelsFullAccess	AWS managed	Permissions policy

Step 3: Add tags section:

- Add tags - optional Info
- Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.
- No tags associated with the resource.
- [Add new tag](#)
- You can add up to 50 more tags.

Buttons at the bottom:

- Cancel
- Previous
- Create role (highlighted with a red box)

**Our Created role

Screenshot of the AWS IAM 'Roles' page.

The table lists roles:

Role name	Trusted entities	Last activity
demo-lambda-role-hingl0d7	AWS Service: lambda	-
Demo-SSM-EC2-role	AWS Service: ec2	147 days ago
DemoRoleEC2	AWS Service: ec2	312 days ago
rds-monitoring-role	AWS Service: monitoring.rds	-
RekognitionS3AccessRole-01062025 (highlighted with a red box)	AWS Service: ec2	-
s3crr_role_for_myawsbucket-pragya-v2	AWS Service: s3	244 days ago
s3replicate_role_for_myawsbucket-pragya-v2	AWS Service: batchoperations.s3	244 days ago

Details for the selected role:

Role Anywhere Info

Authenticate your non AWS workloads and securely provide access to AWS services.

Access AWS from your non AWS workloads

X.509 Standard

Temporary credentials

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**.

Screenshot of the AWS IAM Users page showing a user named "Sharmapragya". A red arrow points to the checkbox next to the user's name in the list.

Users (1/1) Info

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

User name	Path	Group	Last activity	MFA	Password age	Console last sign-in
Sharmapragya	/	1	30 minutes ago		386 days	June 01, 2025, 12:55

Actions: [Edit](#) [Delete](#) [Create user](#)

Screenshot of the AWS IAM User details page for "Sharmapragya". A red box highlights the "Add permissions" button.

Sharmapragya Info

Summary

ARN arn:aws:iam::905418461383:user/Sharmapragya	Console access Enabled without MFA	Access key 1 AKIA5FTZFKDDYNNFLU7O - 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.

Policy name	Type	Attached via
AdministratorAccess	AWS managed - job function	Group Admin

Add permissions

Screenshot of the AWS IAM User details page for "Sharmapragya". A red box highlights the "Add permissions" button.

Sharmapragya Info

Summary

ARN arn:aws:iam::905418461383:user/Sharmapragya	Console access Enabled without MFA	Access key 1 AKIA5FTZFKDDYNNFLU7O - 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.

Policy name	Type	Attached via
AdministratorAccess	AWS managed - job function	Group Admin

Add permissions

Screenshot of the AWS IAM 'Add permissions' step 1: Permissions options.

The 'Permissions options' section contains three choices:

- 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.

A red arrow points down to the 'Attach policies directly' option.

Permissions policies (1355)

Filter by Type: All types

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

Screenshot of the AWS IAM 'Add permissions' step 2: Permissions policies.

The 'Permissions options' section contains three choices:

- 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.

A red arrow points to the 'AmazonRekognitionCustomLabels...' policy in the list.

Permissions policies (1/1355)

Filter by Type: All types

Search: rekog

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

Screenshot of the AWS IAM 'Add permissions' step 2 review screen.

Review
The following policies will be attached to this user. [Learn more](#)

User details
User name
Sharmapragya

Permissions summary (1)

Name	Type	Used as
AmazonRekognitionCustomLabelsFullAccess	AWS managed	Permissions policy

Buttons: Cancel, Previous, Add permissions (highlighted with a red box).

Screenshot of the AWS IAM User summary page for 'Sharmapragya'.

Identity and Access Management (IAM)

Summary

- ARN: arn:aws:iam::905418461383:user/Sharmapragya
- Console access: Enabled without MFA
- Created: May 11, 2024, 01:24 (UTC+05:30)
- Last console sign-in: Today
- Access key 1: AKIA5FTZFKDDYNMFLU7O - Active (Used 345 days ago, 345 days old)
- Access key 2: Create access key

Permissions (2) Policies attached to the user.

Filter by Type: All types

Policy name	Type	Attached via
AdministratorAccess	AWS managed - job function	Group Admin

Buttons: Remove, Add permissions (highlighted with a blue box), Search, Sort icons.

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

The screenshot shows the AWS CloudShell home page. On the left, there's a sidebar titled 'Recently visited' with links to various AWS services like IAM, EC2, S3, VPC, etc. Below it are sections for 'Welcome to AWS' and 'AWS Health'. On the right, there's a 'Applications' section showing 0 applications in the 'ap-south-1' region. At the bottom, there are links for 'View all services', 'Create application', and 'Go to myApplications'. The URL in the address bar is <https://ap-south-1.console.aws.amazon.com/cloudshell/home?region=ap-south-1>.

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

The screenshot shows the AWS CloudShell terminal window. The title bar says 'CloudShell ap-south-1'. The terminal window contains the command `~ $ nano detect_labels.py`. The bottom status bar shows 'CloudShell Feedback' and copyright information.

The screenshot shows the AWS CloudShell terminal window. The title bar says 'CloudShell ap-south-1'. The terminal window contains the command `~ $ detect_labels.py`. Below the terminal, the nano editor interface is visible with various keyboard shortcuts at the bottom. The bottom status bar shows 'CloudShell Feedback' and copyright information.

CloudShell

ap-south-1 +

Actions ▾

detect_labels.py

Modified

```
# Get image from S3
s3 = boto3.client('s3')
s3_object = s3.get_object(Bucket=bucket, Key=photo)
image_bytes = s3_object['Body'].read()
image = Image.open(io.BytesIO(image_bytes))

# Plot
fig, ax = plt.subplots(1)
ax.imshow(image)

# Draw bounding boxes if available
for label in response['Labels']:
    for instance in label.get('Instances', []):
        box = instance['BoundingBox']
        width, height = image.size
        left = box['Left'] * width
        top = box['Top'] * height
        w = box['Width'] * width
        h = box['Height'] * height

        rect = patches.Rectangle((left, top), w, h, linewidth=2, edgecolor='red', facecolor='none')
        ax.add_patch(rect)
        ax.text(left, top - 10, label['Name'], color='red', fontsize=10, weight='bold')

plt.axis('off')
plt.show()
```

7. Run our python file

The screenshot shows the AWS CloudShell interface. At the top left is the title 'CloudShell'. To the right are three circular icons: 'Actions' with a dropdown arrow, a copy/paste icon, and a gear icon. The main area is a terminal window titled 'ap-south-1'. It contains two command entries: '~ \$ nano detect_labels.py' and '~ \$ python3 detect_labels.py'. The terminal has a dark background with light-colored text.

8. install matplotlib if not by running command

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

CloudShell

ap-south-1 +

```
~ $ nano detect_labels.py
~ $ python3 detect_labels.py
Traceback (most recent call last):
  File "/home/cloudshell-user/detect_labels.py", line 2, in <module>
    import matplotlib.pyplot as plt
ModuleNotFoundError: No module named 'matplotlib'
- $ pip3 install --user matplotlib
Collecting matplotlib
  Downloading matplotlib-3.9.4-cp39-cp39-manylinux_2_17_x86_64.manylinux2014_x86_64.whl (8.3 MB)
    8.3 MB 16.4 MB/s
Collecting numpy>=1.23
  Downloading numpy-2.0.2-cp39-cp39-manylinux_2_17_x86_64.manylinux2014_x86_64.whl (19.5 MB)
    19.5 MB 66.0 MB/s
```

9. Run python file

```
python3 detect_labels.py
```

```

CloudShell ap-south-1 + 
Collecting numpy>=1.23
  Downloading numpy-2.0.2-cp39-cp39-manylinux_2_17_x86_64.manylinux2014_x86_64.whl (19.5 MB) | 19.5 MB 66.0 MB/s
Collecting cycler>=0.10
  Downloading cycler-0.12.1-py3-none-any.whl (8.3 kB)
Collecting fonttools>=4.22.0
  Downloading fonttools-4.58.1-cp39-cp39-manylinux_2_17_x86_64.manylinux2014_x86_64.whl (4.7 MB) | 4.7 MB 77.2 MB/s
Collecting packaging>=20.0
  Downloading packaging-25.0-py3-none-any.whl (66 kB) | 66 kB 1.3 MB/s
Requirement already satisfied: python-dateutil>2.7 in /usr/lib/python3.9/site-packages (from matplotlib) (2.8.1)
Collecting kiwisolver<1.3.1
  Downloading kiwisolver-1.4.7-cp39-cp39-manylinux_2_12_x86_64.manylinux2010_x86_64.whl (1.6 MB) | 1.6 MB 99.9 MB/s
Collecting pyParsing>=2.3.1
  Downloading pyParsing-3.2.3-py3-none-any.whl (111 kB) | 111 kB 86.1 MB/s
Collecting pillow>=8
  Downloading pillow-11.2.1-cp39-cp39-manylinux_2_28_x86_64.whl (4.6 MB) | 4.6 MB 50.1 MB/s
Collecting importlib-resources>=3.2.0
  Downloading importlib_resources-6.5.2-py3-none-any.whl (37 kB)
Collecting contourpy>1.0.3
  Downloading contourpy-1.3.0-cp39-cp39-manylinux_2_17_x86_64.manylinux2014_x86_64.whl (321 kB) | 321 kB 93.6 MB/s
Requirement already satisfied: zipp>=3.1.0 in /usr/local/lib/python3.9/site-packages (from importlib-resources>=3.2.0->matplotlib) (3.21.0)
Requirement already satisfied: six>=1.5 in /usr/lib/python3.9/site-packages (from python-dateutil>2.7->matplotlib) (1.15.0)
Installing collected packages: numpy, pyParsing, pillow, packaging, kiwisolver, importlib-resources, fonttools, cycler, contourpy, matplotlib
Successfully installed contourpy-1.3.0 cycler-0.12.1 fonttools-4.58.1 importlib-resources-6.5.2 kiwisolver-1.4.7 matplotlib-3.9.4 numpy-2.0.2 packaging-25.0 pillow-11.2.1 pyParsing-3.2.3
~ $ python3 detect_labels.py

```

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

10. Download the processed image by using the following command

```

CloudShell ap-south-1 + 
~ $ nano detect_labels.py
~ $ download output_with_boxes.jpg
-bash: download: command not found
~ $ source /etc/profile.d/cloudshell.sh
-bash: /etc/profile.d/cloudshell.sh: No such file or directory
~ $ nano detect_labels.py
~ $ python3 detect_labels.py
  File "/home/cloudshell-user/detect_labels.py", line 9
    photo = 'image1.jpg'
               ^
SyntaxError: invalid syntax
~ $ nano detect_labels.py
~ $ python3 detect_labels.py
  Image saved as output_with_boxes.jpg
~ $ 

```

Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

A context menu is open for the terminal tab, showing the following options:

- ap-south-1 environment actions
- New tab
- Split into rows
- Split into columns
- Download file** (highlighted)
- Upload file
- Restart
- Delete
- Global actions
- Create VPC environment (max 2)

```

CloudShell ap-south-1 + 
~ $ nano detect_labels.py
~ $ download output_with_boxes.jpg
-bash: download: command not found
~ $ source /etc/profile.d/cloudshell.sh
-bash: /etc/profile.d/cloudshell.sh: No such file or directory
~ $ nano detect_labels.py
~ $ python3 detect_labels.py
  File "/home/cloudshell-user/detect_labels.py", line 9
    photo = 'image1.jpg'
               ^
SyntaxError: invalid syntax
~ $ nano detect_labels.py
~ $ python3 detect_labels.py
  Image saved as output_with_boxes.jpg
~ $ 

```

Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Download file



Download files from your AWS CloudShell to your local desktop. Folders are not supported.

Individual file path

You can copy the file path from the command-line and paste it below.

output_with_boxes.jpg

myfile.txt or /folder/myfile.txt.

[Cancel](#)

[Download](#)

Download file



Download files from your AWS CloudShell to your local desktop. Folders are not supported.

Individual file path

You can copy the file path from the command-line and paste it below.

output_with_boxes.jpg

myfile.txt or /folder/myfile.txt.

[Cancel](#)

Preparing download..

11. The image will be downloaded to your system

Below are some images processed by amazon rekognition



