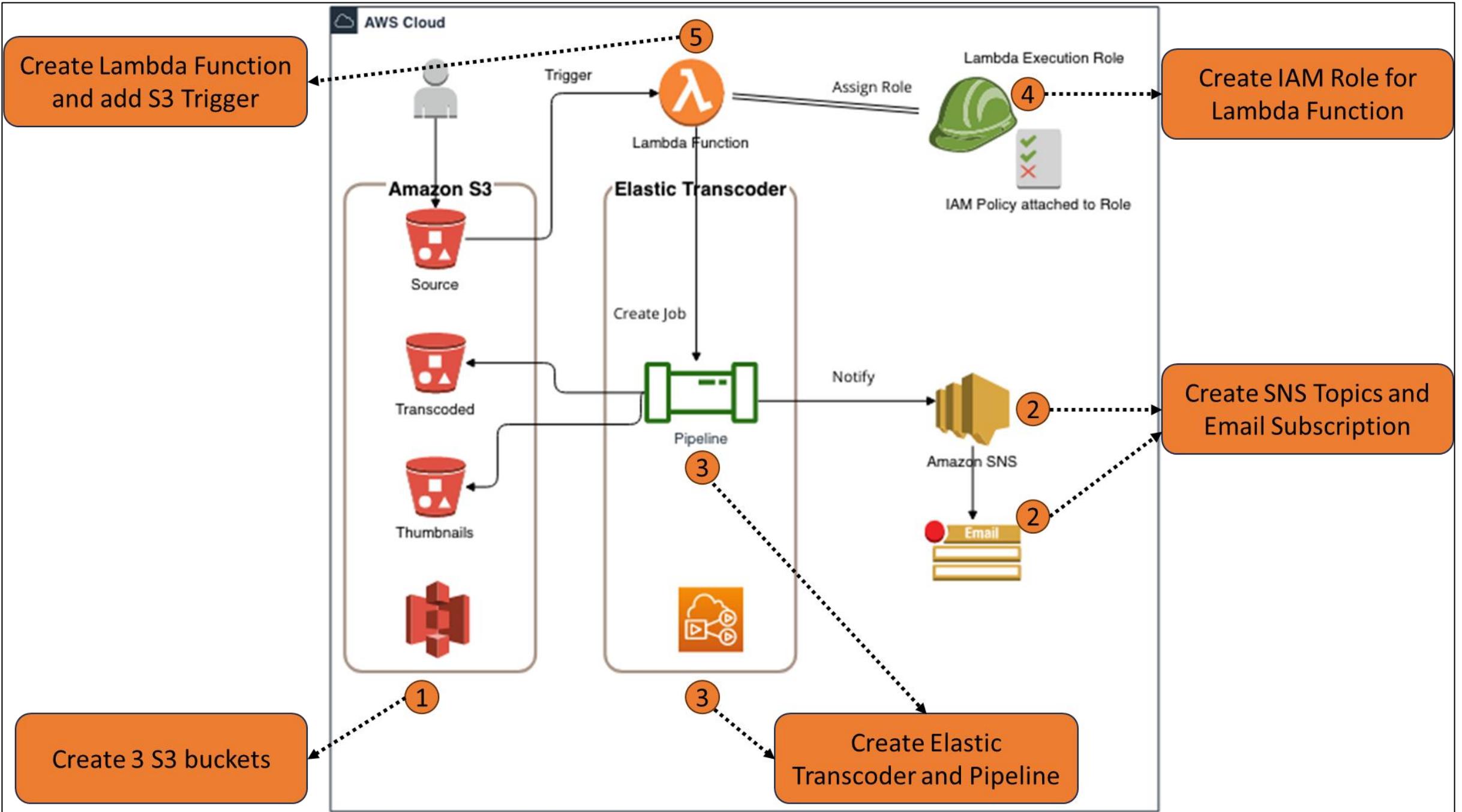


# Project - Transcoding Videos Project



1-) Create 3 S3 Buckets

Console Home EC2 IAM RDS DynamoDB ElastiCache VPC CloudFormation S3 Elastic Kubernetes Service EFS R

## Amazon S3

Buckets

Access Points

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

AWS Organizations settings

Feature spotlight 7

AWS Marketplace for S3

Amazon S3 > Buckets > Create bucket

### Create bucket Info

Buckets are containers for data stored in S3. [Learn more](#)

#### General configuration

Bucket name  Bucket name must be unique within the global namespace and follow the bucket naming rules. [See rules for bucket naming](#)

AWS Region

Copy settings from existing bucket - *optional*  
Only the bucket settings in the following configuration are copied.  
[Choose bucket](#)

#### Object Ownership Info

Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

**ACLs disabled (recommended)**  
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

**ACLs enabled**  
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

Object Ownership  
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.
- 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.

#### 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

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](#)

**▼ Account snapshot**Last updated: Sep 22, 2023 by Storage Lens. Metrics are generated every 24 hours. [Learn more](#)[View Storage Lens dashboard](#)Total storage  
332.5 KBObject count  
7Average object size  
47.5 KBYou can enable advanced metrics in the  
"default-account-dashboard" configuration.**Buckets (3) [Info](#)**Buckets are containers for data stored in S3. [Learn more](#)  [Empty](#) [Delete](#) [Create bucket](#)

<input type="text"/> Find buckets by name				
Name	AWS Region	Access	Creation date	
<a href="#">kenan-source-bucket</a>	US East (N. Virginia) us-east-1	Bucket and objects not public	September 24, 2023, 01:13:24 (UTC+03:00)	
<a href="#">kenan-thumbnails-bucket</a>	US East (N. Virginia) us-east-1	Bucket and objects not public	September 24, 2023, 01:17:32 (UTC+03:00)	
<a href="#">kenan-transcoded-bucket</a>	US East (N. Virginia) us-east-1	Bucket and objects not public	September 24, 2023, 01:16:48 (UTC+03:00)	

2-) Create SNS Topics and Email Subscription

A screenshot of the AWS Amazon SNS service console. The left sidebar shows navigation links: Dashboard, Topics (which is highlighted with a red box), Subscriptions, Mobile (with sub-links: Push notifications, Text messaging (SMS), Origination numbers), and a CloudWatch Metrics link. The main content area is titled 'Amazon.SNS > Topics'. It displays a table header for 'Topics (0)' with columns for Name, Type, and ARN. Below the table, a message says 'No topics' and 'To get started, create a topic.' with a 'Create topic' button. The top navigation bar includes the AWS logo, a search bar with placeholder 'Arama', a keyboard shortcut '[Alt+S]', and various service icons like CloudFormation, S3, Elastic Kubernetes Service, EFS, Route 53, Elastic Beanstalk, CloudWatch, Lambda, API Gateway, CloudFront, Amazon EventBridge, Cloud9, Simple Notification Service, Simple Queue Service, and Certificates. On the far right of the top bar, there are account and region information: 'N. Virginia' and 'Knnkic @ k...'. The bottom right corner of the 'Create topic' button has an orange arrow pointing towards it.

## Create topic

### Details



Type | [Info](#)

Topic type cannot be modified after topic is created

FIFO (first-in, first-out)

- Strictly-preserved message ordering
- Exactly-once message delivery
- High throughput, up to 300 publishes/second
- Subscription protocols: SQS

Standard

- Best-effort message ordering
- At-least once message delivery
- Highest throughput in publishes/second
- Subscription protocols: SQS, Lambda, HTTP, SMS, email, mobile application endpoints

Name

Transcoder-SNS-Topic

Maximum 256 characters. Can include alphanumeric characters, hyphens (-) and underscores (\_).

Display name - optional | [Info](#)

To use this topic with SMS subscriptions, enter a display name. Only the first 10 characters are displayed in an SMS message.

Transcoder-SNS-Topic

Maximum 100 characters.

► **Encryption - optional**

Amazon SNS provides in-transit encryption by default. Enabling server-side encryption adds at-rest encryption to your topic.

► **Access policy - optional** [Info](#)

This policy defines who can access your topic. By default, only the topic owner can publish or subscribe to the topic.

► **Data protection policy - optional** [Info](#)

This policy defines which sensitive data to monitor and to prevent from being exchanged via your topic.

► **Delivery policy (HTTP/S) - optional** [Info](#)

The policy defines how Amazon SNS retries failed deliveries to HTTP/S endpoints. To modify the default settings, expand this section.

► **Delivery status logging - optional** [Info](#)

These settings configure the logging of message delivery status to CloudWatch Logs.

► **Tags - optional**

A tag is a metadata label that you can assign to an Amazon SNS topic. Each tag consists of a key and an optional value. You can use tags to search and filter your topics and track your costs. [Learn more](#) 

► **Active tracing - optional** [Info](#)

Use AWS X-Ray active tracing for this topic to view its traces and service map in Amazon CloudWatch. Additional costs apply.



Cancel

Create topic

## Topics (1)

[Edit](#)[Delete](#)[Publish message](#)[Create topic](#)[Search](#)

&lt; 1 &gt;



Name

ARN

[Transcoder-SNS-Topic](#)

Standard

arn:aws:sns:us-eas:

oder-SNS-Topic

[Amazon SNS](#) > [Topics](#) > [Transcoder-SNS-Topic](#)

## Transcoder-SNS-Topic

[Edit](#)[Delete](#)[Publish message](#)

## Details

## Name

Transcoder-SNS-Topic

## Display name

Transcoder-SNS-Topic

## ARN

arn:aws:

Transcoder-SNS-Topic

## Topic owner

## Type

Standard

[Subscriptions](#)[Access policy](#)[Data protection policy](#)[Delivery policy \(HTTP/S\)](#)[Delivery status logging](#)[Encryption](#)[Tags](#)[Integrations](#)[Create subscription](#)

## Subscriptions (0)

[Edit](#)[Delete](#)[Request confirmation](#)[Confirm subscription](#)

&lt; 1 &gt;

[Search](#)

ID

Endpoint

Status

Protocol

No subscriptions found

You don't have any subscriptions to this topic.

[Create subscription](#)

## Create subscription

### Details

#### Topic ARN

arn:aws:sns:u...2:Transcoder-SNS-Topic X

#### Protocol

The type of endpoint to subscribe

Email



#### Endpoint

An email address that can receive notifications from Amazon SNS.

@gmail.com

After your subscription is created, you must confirm it. [Info](#)

#### ► Subscription filter policy - *optional* [Info](#)

This policy filters the messages that a subscriber receives.

#### ► Redrive policy (dead-letter queue) - *optional* [Info](#)

Send undeliverable messages to a dead-letter queue.



Cancel

Create subscription

⌚ Subscription to Transcoder-SNS-Topic created successfully.  X

The ARN of the subscription is arn:aws:

Amazon SNS > Topics > Transcoder-SNS-Topic > Subscription:

## Subscription: 13b95

**Details**

ARN	arn:a	58	Status	Pending confirmation
Endpoint	@gmail.com		Protocol	EMAIL
Topic	Transcoder-SNS-Topic			
Subscription Principal	arn:a			

[Subscription filter policy](#) | [Redrive policy \(dead-letter queue\)](#)

**Subscription filter policy** Info

This policy filters the messages that a subscriber receives.

No filter policy configured for this subscription.  
To apply a filter policy, edit this subscription.

Transcoder-SNS-Topic <no-reply@sns.amazonaws.com>  
Alici: ben ▾

Bu ileti neden spam klasöründe? ileti, geçmişte spam olarak tanımlanan iletilere benziyor.

Spam olmadığını bildir

You have chosen to subscribe to the topic:  
arn:av :Transcoder-SNS-Topic

To confirm this subscription, click or visit the link below (If this was in error no action is necessary):  
[Confirm subscription](#)

Please do not reply directly to this email. If you wish to remove yourself from receiving all future SNS subscription confirmation requests please send an email to [sns-opt-out](#)

← Yanıtla → Yönlendir

S3 Management Console | Transcoder-SNS-Topic | Topics | AWS Notification - Subscription | Subscription confirm

aws Simple Notification Service

**Subscription confirmed!**

You have successfully subscribed.

Your subscription's id is:  
arn:z:  
4260-aa6c-3242afff5368

If it was not your intention to subscribe, [click here to unsubscribe](#).

## Transcoder-SNS-Topic

[Edit](#)[Delete](#)[Publish message](#)

## Details

Name  
Transcoder-SNS-Topic

Display name  
Transcoder-SNS-Topic

ARN  
arn:aws:sns:us-east-1:123456789012:Transcoder-SNS-Topic

Topic owner

Type  
Standard

[Subscriptions](#)[Access policy](#)[Data protection policy](#)[Delivery policy \(HTTP/S\)](#)[Delivery status logging](#)[Encryption](#)[Tags](#)[Integrations](#)

## Subscriptions (2)

[Edit](#)[Delete](#)[Request confirmation](#)[Confirm subscription](#)[Create subscription](#)< 1 > ⚙️#[13b95187-f884-4260-aa6c-3242afff5368](#)[Endpoint](#)

gmail.com

[Status](#)✓ Confirmed[Protocol](#)EMAIL[6750833e-3b45-4727-95e8-9c73ce39e1b6](#)

74

✓ Confirmed

SMS

3-) Create Elastic Transcoder Pipeline

Screenshot of the AWS CloudSearch search results page for 'Transcoder'.

The search bar at the top shows 'Transcoder'. Below it, the results are categorized:

- Services (3)
- Features (1)
- Resources **New**
- Blogs (35)
- Documentation (1,262)
- Events (1)
- Marketplace (107)

The first result under 'Services' is highlighted with a red box:

**Elastic Transcoder** ☆  
Easy-to-Use Scalable Media Transcoding

The other two services listed are:

- MediaConvert** ☆  
Convert file-based content for broadcast and multiscreen delivery
- MediaPackage** ☆  
Deliver video to many devices using just-in-time format conversion.

Below the search results, there is a horizontal navigation bar with various AWS service icons.

Welcome to Amazon Elastic Transcoder

**Create a new Pipeline**

Amazon Elastic Transcoder lets you convert digital media stored in Amazon S3 into the audio and video codecs and the containers required by consumer playback devices. For example, you can convert large, high-quality digital media files into formats that users can play back on mobile devices, tablets, web browsers, and connected televisions.

Elastic Transcoder has three components:

- **Pipelines** are queues that manage your transcoding jobs. Elastic Transcoder begins to process jobs in the order in which you add them to a pipeline. Typically, you'll create at least two pipelines, one for standard-priority jobs and one for high-priority jobs. Most jobs go into the standard-priority pipeline; you use the high-priority pipeline only when you need a file to be transcoded immediately.
- **Jobs** specify the settings that aren't included in the preset, for example, the file to transcode and whether to create thumbnails. Each job converts one file into one different format. When you create a job, Elastic Transcoder adds it to the pipeline you specify. If there are already jobs in the pipeline, Elastic Transcoder begins processing the new job when resources are available.
- **Presets** are templates that specify most of the settings for the transcoded media file. Elastic Transcoder includes some default presets for common formats. You can also create your own presets. When you create a job, you specify which preset to use.

**Amazon Elastic Transcoder at a glance**

**Create a pipeline**  
  
Give your pipeline a name that identifies which jobs go into that pipeline, for example, standard priority.

**Create a preset. (Optional)**  
  
If your requirements correspond with one of the default presets, you can skip this step.

**Create a job**  
  
When you click Create, Elastic Transcoder automatically adds it to the specified pipeline for processing.

**Create New Pipeline**

A pipeline is a queue for your transcoding jobs. You can have more than one pipeline per AWS account. You can use multiple pipelines to organize your transcoding workflow, for example, by having one pipeline for standard-priority jobs and one for high-priority jobs.

Pipeline Name  ⓘ

Input Bucket  ⓘ The Amazon S3 bucket in which you saved the input files.

IAM Role  ⓘ These roles are the roles belonging to you that are assumable by Elastic Transcoder. They must grant Elastic Transcoder the correct permissions on your S3 buckets and SNS topics for jobs to be triggered. Elastic Transcoder creates a reusable, default IAM role. [View the policy](#).

**Configuration for Amazon S3 Bucket for Transcoded Files and Playlists**

Bucket  ⓘ

Storage Class  ⓘ

[+ Add Permission](#)

**Configuration for Amazon S3 Bucket for Thumbnails**

Bucket  ⓘ

Storage Class  ⓘ

[+ Add Permission](#)

**Notifications (Optional)**

**Encryption (Optional)**

**Create New Pipeline**

A pipeline is a queue for your transcoding jobs. You can have more than one pipeline per AWS account.

Pipeline Name  ⓘ

Input Bucket  ⓘ — Amazon S3 Buckets in this region — [kenan-source-bucket](#) [kenan-thumbnails-bucket](#) [kenan-transcoded-bucket](#)

IAM Role  ⓘ These roles are the roles belonging to you that are assumable by Elastic Transcoder. They must grant Elastic Transcoder the correct permissions on your S3 buckets and SNS topics for jobs to be triggered. Elastic Transcoder creates a reusable, default IAM role. [View the policy](#).

**Configuration for Amazon S3 Bucket for Transcoded Files and Playlists**

Bucket  ⓘ — Amazon S3 Buckets in this region — [kenan-source-bucket](#) [kenan-thumbnails-bucket](#) [kenan-transcoded-bucket](#)

Storage Class  ⓘ

[+ Add Permission](#)

**Configuration for Amazon S3 Bucket for Thumbnails**

Bucket  ⓘ — Amazon S3 Buckets in this region — [kenan-source-bucket](#) [kenan-thumbnails-bucket](#) [kenan-transcoded-bucket](#)

Storage Class  ⓘ

[+ Add Permission](#)

**Create Pipeline**

**Notifications (Optional)**

On Progressing Event:  No Notifications  Use an existing SNS topic  Create a New SNS Topic  
Select a Topic: Transcoder-SNS-Topic

On Warning Event:  No Notifications  Use an existing SNS topic  Create a New SNS Topic  
Select a Topic: Transcoder-SNS-Topic

On Completion Event:  No Notifications  Use an existing SNS topic  Create a New SNS Topic  
Select a Topic: Transcoder-SNS-Topic

On Error Event:  No Notifications  Use an existing SNS topic  Create a New SNS Topic  
Select a Topic: Transcoder-SNS-Topic

**Encryption (Optional)**

AWS KMS Key ARN:  Default  Custom

 Cancel Create Pipeline

**Pipelines** Create New Pipeline Create New Job Edit Pause Activate Remove

Jobs Presets

Name	Input Bucket	Bucket for Transcoded Files	Bucket for Thumbnails	Status
my-pipeline-for-S3-buckets	kenan-source-bucket	kenan-transcoded-bucket	kenan-thumbnails-bucket	Active

**Pipelines**

**Create New Job** Edit Pause Activate Remove

Jobs Presets

▼ Summary

ARN	arn:aws:elastictranscoder:us-east-1:835642848432:pipeline/1695509174947-xtfacd
Name	my-pipeline-for-S3-buckets
Pipeline ID	1695509174947-xtfacd
Status	Active
Input Bucket	kenan-source-bucket

▼ Configuration for Amazon S3 Bucket for Transcoded Files and Playlists

Bucket	kenan-transcoded-bucket
Storage Class	Standard
Grantee Type	Grantee
	Access

▼ Configuration for Amazon S3 Bucket for Thumbnails

Bucket	kenan-thumbnails-bucket
Storage Class	Standard
Grantee Type	Grantee
	Access

▼ Job Details

Status for the 100 most recent jobs for this pipeline:

Submitted Jobs	0
Progressing Jobs	0
Successful Jobs	0
Failed Jobs	0

▼ Permissions

The following IAM roles have been granted access to this pipeline:

arn:aws:iam:[REDACTED]/Elastic\_Transcoder\_Default\_Role

▼ Notifications

When the following events occur, Elastic Transcoder sends a message to the corresponding Simple Notification Service topic.

Notify upon successful completion	arn:aws:sns:[REDACTED]Transcoder-SNS-Topic
Notify upon progression	arn:aws:sns:[REDACTED]Transcoder-SNS-Topic

4-) Create IAM Role for Lambda Function

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users
- Roles
- Policies
- Identity providers
- Account settings

Access reports

- Access analyzer
- Archive rules
- Analyzers
- Settings
- Credential report
- Organization activity
- Service control policies (SCPs)

Related consoles

- IAM Identity Center
- AWS Organizations

IAM > Policies

Policies (1141) Info

A policy is an object in AWS that defines permissions.

Filter policies by property or policy name and press enter.

Actions Create policy

Policy name	Type	Used as	Description
AWSLambdaBasicExecutionRole-42f42348-5466-4ef1-8e89-f40d60b49373	Customer managed	Permissions policy (1)	
AWSLambdaBasicExecutionRole-49133761-9b2d-4e39-b654-ebb451958aef	Customer managed	Permissions policy (1)	
AWSLambdaBasicExecutionRole-5624f107-40b8-4748-a077-7a15b003eb49	Customer managed	Permissions policy (1)	
AWSLambdaBasicExecutionRole-610364a1-2a4a-4d7f-bea0-41c3ee3d1568	Customer managed	Permissions policy (1)	
AWSLambdaBasicExecutionRole-66a86e90-f305-4b6d-bd54-1385ecfc9310	Customer managed	Permissions policy (1)	
AWSLambdaBasicExecutionRole-6a4a0034-6942-46c2-b5ef-de54b41c189e	Customer managed	Permissions policy (1)	
AWSLambdaBasicExecutionRole-6d235368-12c9-45ae-84af-48b37411bd33	Customer managed	Permissions policy (1)	
AWSLambdaBasicExecutionRole-f605f3a1-7aa0-4509-a86a-9f688b5b0710	Customer managed	Permissions policy (1)	
AWSLambdaSQSPollerExecutionRole-f7d2efa5-b1df-43cb-9e2a-4f25a287102a	Customer managed	Permissions policy (1)	
EC2ReadOnlyCustom	Customer managed	Permissions policy (1)	Provides read-only access
new_user_deny_policies	Customer managed	Permissions policy (1)	this policy denied stopping
S3-List-Read	Customer managed	Permissions policy (1)	S3 List Read Allowed
start-stop-instances-policy	Customer managed	Permissions policy (1)	start-stop-instances-policy
AdministratorAccess	AWS managed - job function	Permissions policy (6)	Provides full access to AW
PowerUserAccess	AWS managed - job function	None	Provides full access to AW

Step 1  
Specify permissionsSpecify permissions Info

Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

Step 2  
Review and create

## Policy editor

```
1 | {
2 |     "Version": "2012-10-17",
3 |     "Statement": [
4 |         {
5 |             "Effect": "Allow",
6 |             "Action": [
7 |                 "logs:CreateLogGroup",
8 |                 "logs:CreateLogStream",
9 |                 "logs:PutLogEvents"
10 |             ],
11 |             "Resource": "arn:aws:logs:*:*"
12 |         },
13 |         {
14 |             "Action": [
15 |                 "elastictranscoder:*",
16 |                 "s3:)"
17 |             ],
18 |             "Effect": "Allow",
19 |             "Resource": "*"
20 |         }
21 |     ]
}
```

Paste policy json code here

Visual    **JSON**    Actions ▾

## Edit statement

```
```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogGroup",
                "logs:CreateLogStream",
                "logs:PutLogEvents"
            ],
            "Resource": "arn:aws:logs:*:*"
        },
        {
            "Action": [
                "elastictranscoder:*",
                "s3:)"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}```
```

Cancel    **Next**

Step 2

Review and create

### Policy details

#### Policy name

Enter a meaningful name to identify this policy.

transcoder-policy

Maximum 128 characters. Use alphanumeric and '+-=\_,@-\_` characters.

#### Description - optional

Add a short explanation for this policy.

transcoder-policy

Maximum 1,000 characters. Use alphanumeric and '+-=\_,@-\_` characters.

### Permissions defined in this policy Info

Edit

Permissions in the policy document specify which actions are allowed or denied.

Search

Allow (3 of 385 services)

Show remaining 382 services

Service	Access level	Resource	Request condition
S3	Full access	All resources	None
Elastic Transcoder	Full access	All resources	None
CloudWatch Logs	Limited: Write	region   string like   All	None

#### 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 tag

You can add up to 50 more tags.



Cancel

Previous

Create policy

Console Home EC2 IAM RDS DynamoDB ElastiCache VPC CloudFormation S3 Elastic Kubernetes Service EFS Route 53 Elastic Beanstalk CloudWatch Lambda API Gateway CloudFront Amazon EventBridge

## Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users
- Roles
- Policies
- Identity providers
- Account settings

Access reports

- Access analyzer
- Archive rules
- Analyzers
- Settings
- Credential report
- Organization activity

IAM > Policies

### Policies (1/1142) Info

A policy is an object in AWS that defines permissions.

Filter policies by property or policy name and press enter.

"transcoder" X Clear filters 5 matches

Policy name	Type	Used as
transcoder-policy	Customer managed	None
AmazonElasticTranscoderRole	AWS managed	None
AmazonElasticTranscoder_FullAccess	AWS managed	None
AmazonElasticTranscoder_ReadOnlyAccess	AWS managed	None
AmazonElasticTranscoder_JobsSubmitter	AWS managed	None

## Identity and Access Management (IAM)

Search IAM

Dashboard

## Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

IAM &gt; Roles

Roles (38) 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.

Search



C

Delete

Create role

&lt; 1 2 &gt;

 Role name

Trusted entities

Last activity

 AWSCloud9SSMAccessRoleAWS Service: cloud9, [and 1 more...](#)

13 days ago

 AWSDataLifecycleManagerDefaultRole

AWS Service: dlm

-

 AWSServiceRoleForAmazonElasticFileSystem

AWS Service: elasticfilesystem/service

20 days ago

Create role

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

Lambda



Cancel

Next

Choose a use case for the specified service.

## Use case

 Lambda

Allows Lambda functions to call AWS services on your behalf.

## Add permissions Info

### Permissions policies (1/895) Info

Choose one or more policies to attach to your new role.



Filter by Type

<input type="checkbox"/> Policy name	Type	Description
<input type="checkbox"/> <a href="#">AmazonElasticTranscoder_FullAccess</a>	AWS managed	Grants users full access to Elastic Transco...
<input type="checkbox"/> <a href="#">AmazonElasticTranscoder_JobsSubmitter</a>	AWS managed	Grants users permission to change preset...
<input type="checkbox"/> <a href="#">AmazonElasticTranscoder_ReadOnlyAccess</a>	AWS managed	Grants users read-only access to Elastic T...
<input type="checkbox"/> <a href="#">AmazonElasticTranscoderRole</a>	AWS managed	Default policy for the Amazon Elastic Tra...
<input checked="" type="checkbox"/> <a href="#">transcoder-policy</a>	Customer managed	transcoder-policy



### ► Set permissions boundary - optional

[Cancel](#) [Previous](#) **Next**

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 alphanumeric and '+,-,\_,@,\_' 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            "lambda.amazonaws.com"
12          ]
13        }
14      }
15    ]
16  ]
```

**Step 2: Add permissions**

Permissions policy summary

Policy name	Type	Attached as
<a href="#">transcoder-policy</a>	Customer managed	Permissions policy

**Step 3: Add tags**

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.

[Cancel](#) [Previous](#) [Create role](#)

**Identity and Access Management (IAM)**

Search IAM

Dashboard

Access management

User groups

Users

**Roles**

IAM > Roles

**Roles (1/39) [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.

Search: transcoder- X 1 match

<input checked="" type="checkbox"/> Role name	▲ Trusted entities	Last activity
<a href="#">transcoder-role</a>	AWS Service: lambda	-

**Roles Anywhere [Info](#)**

Authenticate your non-AWS workloads and centrally manage access to AWS services

5-) Create Lambda Function and Trigger for  
S3 source-bucket

RDS DynamoDB ElastiCache VPC CloudFormation S3 Elastic Kubernetes Service EFS Route 53 Elastic Beanstalk CloudWatch Lambda API Gateway CloudFront Amazon EventBridge Cloud9 Simple Notification Service Simple Queue Service

### Create function Info

AWS Serverless Application Repository applications have moved to [Create application](#).

Author from scratch  
Start with a simple Hello World example.

Use a blueprint  
Build a Lambda application from sample code and configuration presets for common use cases.

Container image  
Select a container image to deploy for your function.

#### Basic information

Function name Info  
Enter a name that describes the purpose of your function.

Use only letters, numbers, hyphens, or underscores with no spaces.

Runtime Info  
Choose the language to use to write your function. Note that the console code editor supports only Node.js, Python, and Ruby.  
 ▼

Architecture Info  
Choose the instruction set architecture you want for your function code.  
 x86\_64  
 arm64

#### Permissions Info

By default, Lambda will create an execution role with permissions to upload logs to Amazon CloudWatch Logs. You can customize this default role later when adding triggers.

**▼ Change default execution role**

Execution role  
Choose a role that defines the permissions of your function. To create a custom role, go to the [IAM console](#).  
 Create a new role with basic Lambda permissions  
 Use an existing role  
 Create a new role from AWS policy templates

Existing role  
Choose an existing role that you've created to be used with this Lambda function. The role must have permission to upload logs to Amazon CloudWatch Logs.  
 ▼   
View the transcoder-role role [on the IAM console](#).

**► Advanced settings**

 ▼

Cancel

AWS Lambda

Dashboard

Applications

Functions

transcoder\_lambda\_function

Additional resources

Code signing configurations

Layers

Replicas

Related AWS resources

Step Functions state machines

Function overview Info

transcoder\_lambda\_function

Layers (0)

+ Add trigger

+ Add destination

Code Test Monitor Configuration Aliases Versions

Code source Info

File Edit Find View Go Tools Window Test Deploy

Go to Anything (Ctrl-P)

Environment Environment Vari +

lambda\_function Environment Vari +

transcoder\_lambda\_function

lambda\_function.py

```
1 import json
2
3 def lambda_handler(event, context):
4     # TODO implement
5     return {
6         'statusCode': 200,
7         'body': json.dumps('Hello from Lambda!')
8     }
9
```

This screenshot shows the AWS Lambda Function Overview page for the 'transcoder\_lambda\_function'. The left sidebar lists various AWS services like Dashboard, Applications, and Functions, with 'transcoder\_lambda\_function' selected. The main panel displays the function's name, a placeholder for triggers and destinations, and a code editor tab. The code editor shows a simple Python lambda function that returns a JSON response with a status code of 200 and a body message.

```

python
from datetime import datetime
import json
import urllib.parse
import os
import boto3

PIPELINE_ID = os.environ['PIPELINE_ID']

transcoder = boto3.client('elastictranscoder')
s3 = boto3.resource('s3')

def lambda_handler(event, context):
    print("Received event: " + json.dumps(event))

    # Get the object from the event
    key = urllib.parse.unquote_plus(
        event['Records'][0]['s3']['object']['key'], encoding='utf-8')

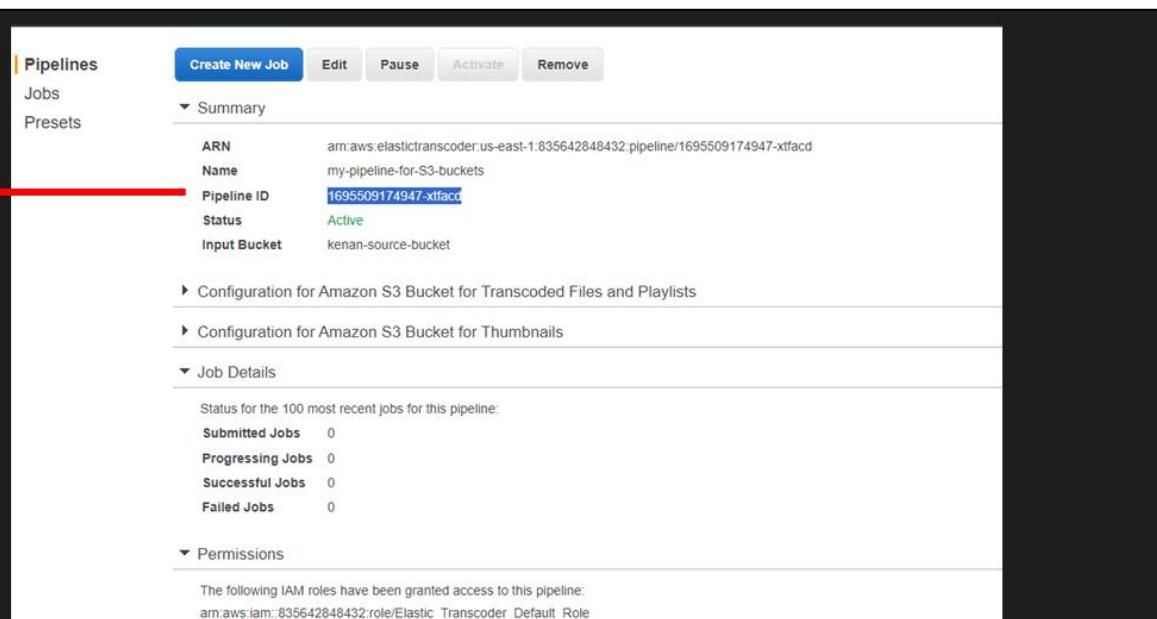
    filename = os.path.splitext(key)[0] # filename w/o extension

    # Create a job
    job = transcoder.create_job(
        PipelineId=PIPELINE_ID,
        Input={
            'Key': key
        },
        Outputs=[
            {
                'Key': filename + '-1080p.mp4',
                'ThumbnailPattern': filename + '-{resolution}-{count}',
                'PresetId': '135162000001-000001' # Generic 1080p
            },
            {
                'Key': filename + '-720p.mp4',
                'ThumbnailPattern': filename + '-{resolution}-{count}',
                'PresetId': '135162000001-000010' # Generic 720p
            }
        ]
    )

    print("start time={}".format(datetime.now().strftime("%H:%M:%S.%f")[:-3]))
    print("job={}".format(job))
    job_id = job['Job']['Id']

    # Wait for the job to complete
    waiter = transcoder.get_waiter('job_complete')
    waiter.wait(Id=job_id)
    end_time = datetime.now().strftime("%H:%M:%S.%f")[:-3]
    print("end time={}".format(end_time))

```



Pipelines Create New Preset Copy Remove

Presets Filter:

	Name	ID
<input checked="" type="checkbox"/>	System preset: Generic 1080p	135162000001-000001
<input type="checkbox"/>	System preset: Generic 720p	135162000001-000010
<input type="checkbox"/>	System preset: Generic 480p 16:9	135162000001-000020
<input type="checkbox"/>	System preset: Generic 480p 4:3	135162000001-000030

AWS Lambda

Code Test Monitor Configuration Aliases Versions

Code source Info

File Edit Find View Go Tools Window Test Deploy Changes not deployed

Go to Anything (Ctrl-P)

Environment Vari

lambda\_function Environment

transcoder\_lambda\_ Environment

lambda\_function.py

```
from datetime import datetime
import json
import urllib.parse
import os
import boto3

PIPELINE_ID = os.environ['PIPELINE_ID']

transcoder = boto3.client('elastictranscoder')
s3 = boto3.resource('s3')

def lambda_handler(event, context):
    print("Received event: " + json.dumps(event))

    # Get the object from the event
    key = urllib.parse.unquote_plus(
        event['Records'][0]['s3']['object']['key'], encoding='utf-8')

    filename = os.path.splitext(key)[0] # filename w/o extension

    # Create a job
    job = transcoder.create_job(
        PipelineId=PIPELINE_ID,
        Input={
            'Key': key
        },
        Outputs=[
            {
                'Key': filename + '-1080p.mp4',
                'ThumbnailPattern': filename + '-{resolution}-{count}',
                'PresetId': '135162000001-00001' # Generic 1080p
            },
            {
                'Key': filename + '-720p.mp4',
                'ThumbnailPattern': filename + '-{resolution}-{count}',
                'PresetId': '135162000001-00010' # Generic 720p
            }
        ]
    )
```

AWS Lambda X

[Lambda](#) > [Functions](#) > transcoder\_lambda\_function

## transcoder\_lambda\_function

**Function overview** [Info](#)

 [+ Add trigger](#)

 transcoder_lambda_function
 Layers (0)

[+ Add destination](#)

**Additional resources**

- Code signing configurations
- Layers
- Replicas

**Related AWS resources**

- Step Functions state machines

AWS Lambda

Lambda > Add trigger

## Add trigger

**Trigger configuration** [Info](#)

**S3** aws asynchronous storage

**Bucket**  
Please select the S3 bucket that serves as the event source. The bucket must be in the same region as the function.  
 [X](#) [C](#)  
Bucket region: us-east-1

**Event types**  
Select the events that you want to have trigger the Lambda function. You can optionally set up a prefix or suffix for an event. However, for each bucket, individual events cannot have multiple configurations with overlapping prefixes or suffixes that could match the same object key.

All object create events [X](#)

**Prefix - optional**  
Enter a single optional prefix to limit the notifications to objects with keys that start with matching characters.

**Suffix - optional**  
Enter a single optional suffix to limit the notifications to objects with keys that end with matching characters.

**Recursive invocation**  
If your function writes objects to an S3 bucket, ensure that you are using different S3 buckets for input and output. Writing to the same bucket increases the risk of creating a recursive invocation, which can result in increased Lambda usage and increased costs. [Learn more](#)

I acknowledge that using the same S3 bucket for both input and output is not recommended and that this configuration can cause recursive invocations, increased Lambda usage, and increased costs.

Lambda will add the necessary permissions for AWS S3 to invoke your Lambda function from this trigger. [Learn more](#)

[Cancel](#) [Add](#)

Console Home EC2 IAM RDS DynamoDB ElastiCache VPC CloudFormation S3 Elastic Kubernetes Service EFS Route 53 Elastic Beanstalk

## AWS Lambda

Dashboard Applications Functions **transcoder\_lambda\_function** Additional resources Code signing configurations Layers Replicas Related AWS resources Step Functions state machines

### Function overview

transcoder\_lambda\_function

S3

Layers (0)

+ Add destination

+ Add trigger

Code Test Monitor Configuration Aliases Versions

### Code source

File Edit Find View Go Tools Window Test Deploy

Go to Anything (Ctrl-P)

Environment

lambda\_function Environment Vari

transcoder\_lambda\_

lambda\_function.py

```
from datetime import datetime
import json
import urllib.parse
import os
import boto3
PIPELINE_ID = os.environ['PIPELINE_ID']
transcoder = boto3.client('elastictranscoder')
s3 = boto3.resource('s3')
```

**AWS Lambda** X

Dashboard  
Applications  
Functions  
**transcoder\_lambda\_function**  
Additional resources  
Code signing configurations  
Layers  
Replicas  
Related AWS resources  
Step Functions state machines

**transcoder\_lambda\_function**

Layers (0)

S3

+ Add trigger

+ Add destination

Description  
-  
Last modified  
5 minutes ago  
Function ARN  
arn:aws:lambda:us-east-1:83564284  
a\_function  
Function URL [Info](#)

Code Test Monitor Configuration Aliases Versions

General configuration  
Triggers  
Permissions  
Destinations  
Function URL  
**Environment variables**  
Tags  
VPC

**Environment variables**

Key	Value
No environment variables	

No environment variables associated with this function.

Edit

[Dashboard](#)[Applications](#)[Functions](#)[transcoder\\_lambda\\_function](#)**▼ Additional resources**[Code signing configurations](#)[Layers](#)[Replicas](#)**▼ Related AWS resources**[Step Functions state machines](#)

## Environment variables

You can define environment variables as key-value pairs that are accessible from your function code. These are useful to store configuration settings without the need to change function code. [Learn more](#)

**Key**

PIPELINE\_ID

**Value**

1695509174947-xtfacd

[Remove](#)[Add environment variable](#)[Encryption configuration](#)[Cancel](#)[Save](#)

```
2  
3 PIPELINE_ID = os.environ['PIPELINE_ID']  
4  
5 transcoder = boto3.client('elastictranscoder')  
6 s3 = boto3.resource('s3')  
7
```

**Pipelines**  
Jobs  
Presets[Create New Job](#)[Edit](#)[Pause](#)[Activate](#)[Remove](#)**▼ Summary**

ARN	arn:aws:elasti...:pipeline/1695509174947-...
Name	my-pipeline-for-S3-buckets
Pipeline ID	1695509174947-xtfacd
Status	Active
Input Bucket	kenan-source-bucket

[Configuration for Amazon S3 Bucket for Transcoded Files and Playlists](#)

▼ Function overview [Info](#)

 transcoder\_lambda\_function

 Layers (0)

 S3

+ Add trigger

+ Add destination

Description -

Last modified 23 seconds

Function ARN arn:aws:lambda:us-east-1:123456789012:function:transcoder\_lambda\_function

Function URL -

Code Test Monitor Configuration Aliases Versions



**Environment variables (1)**

The environment variables below are encrypted at rest with the default Lambda service key.

Key	Value
PIPELINE_ID	1695509174947-xtfacd

General configuration

Triggers

Permissions

Destinations

Function URL

Environment variables

Tags

# Testing

Amazon S3

Buckets

Access Points

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

AWS Organizations settings

Feature spotlight

AWS Marketplace for S3

Amazon S3 > Buckets > kenan-source-bucket > Upload

## Upload

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, 15.6 MB)

All files and folders in this table will be uploaded.

	Name	Folder	Type	Size
<input type="checkbox"/>	Aerial.mp4	-	video/mp4	15.6 MB

Add files Add folder

Find by name

Destination

Destination: s3://kenan-source-bucket

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

Triggered SNS Email Notifications

Transcoder-SNS-Topic Amazon Elastic Transcoder has finished transcoding job 1695511597196-femwcn. - { "state": "COMPLETED", "version": "2012-09-25", "jobId": "1695511597196-femwcn", "pipeline...}

Transcoder-SNS-Topic Amazon Elastic Transcoder has scheduled job 1695511597196-femwcn for transcoding. - { "state": "PROGRESSING", "version": "2012-09-25", "jobId": "1695511597196-femwcn", "...}

kenan-transcoded-bucket Info[Objects](#) [Properties](#) [Permissions](#) [Metrics](#) [Management](#) [Access Points](#)

## Objects (2)

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](#)

     [Open](#)     Find objects by prefix

&lt; 1 &gt;

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input checked="" type="checkbox"/>	<a href="#">Aerial-1080p.mp4</a>	mp4	September 24, 2023, 02:26:48 (UTC+03:00)	7.3 MB	Standard
<input type="checkbox"/>	<a href="#">Aerial-720p.mp4</a>	mp4	September 24, 2023, 02:26:47 (UTC+03:00)	3.3 MB	Standard

## Objects (2)

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](#)

     [Open](#)     Find objects by prefix

&lt; 1 &gt;

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	<a href="#">Aerial-1080p.mp4</a>	mp4	September 24, 2023, 02:26:48 (UTC+03:00)	7.3 MB	Standard
<input checked="" type="checkbox"/>	<a href="#">Aerial-720p.mp4</a>	mp4	September 24, 2023, 02:26:47 (UTC+03:00)	3.3 MB	Standard