Amazon Transcribe: Developer Guide
Copyright © 2017 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.
# Table of Contents

- What Is Amazon Transcribe? ............................................................... 1
- Are You a First-time User of Amazon Transcribe? .......................... 1
- How It Works .................................................................................. 2
  - Speech Input ................................................................................. 2
  - Output JSON ............................................................................... 2
- Getting Started ............................................................................. 4
  - Step 1: Set Up an Account .......................................................... 4
  - Sign up for AWS ................................................................. 4
  - Create an IAM User ............................................................. 5
  - Next Step .................................................................................. 5
  - Step 2: Set Up the AWS CLI ..................................................... 5
  - Next Step .................................................................................. 5
  - Step 3: Getting Started (Console) ........................................... 6
  - Create a Transcription Job ....................................................... 6
  - View a Transcription Job ......................................................... 7
  - Step 4: Getting Started (AWS CLI) ......................................... 11
- Authentication and Access Control for Amazon Transcribe .......... 14
  - Authentication .......................................................................... 14
  - Access Control ......................................................................... 15
  - Overview of Managing Access ............................................... 15
  - Managing Access to Actions ..................................................... 16
  - Specifying Policy Elements: Resources, Actions, Effects, and Principals 16
  - Specifying Conditions in a Policy ........................................... 17
- Using Identity-based Polices (IAM Policies) for Amazon Transcribe 17
  - Permissions Required to Use the Amazon Transcribe Console 18
  - Permissions Required for Audio Transcription 18
  - Permissions Required for Amazon S3 Encryption Keys ............... 19
- Amazon Transcribe API Permissions Reference ......................... 19
- Beta Guidelines and Limits ............................................................ 20
  - Guidelines ................................................................................. 20
  - Limits ....................................................................................... 20
- Document History ......................................................................... 21
- API Reference .............................................................................. 22
  - Actions ..................................................................................... 22
    - GetTranscriptionJob .......................................................... 23
    - ListTranscriptionJobs ......................................................... 25
    - StartTranscriptionJob ......................................................... 28
  - Data Types ................................................................................. 30
    - Media .................................................................................... 31
    - Transcript .............................................................................. 32
    - TranscriptionJob .................................................................. 33
    - TranscriptionJobSummary .................................................. 35
  - Common Errors ......................................................................... 36
  - Common Parameters ............................................................... 37
- AWS Glossary ............................................................................... 40
What Is Amazon Transcribe?

Amazon Transcribe provides transcription services for your audio files. It uses advanced machine learning technologies to recognize spoken words and transcribe them into text. Use Amazon Transcribe to create new products based on understanding the content of audio files. For example, you can:

- Transcribe the audio track from a video to create closed captioning for the video.
- Transcribe dictation to text. For example, use Amazon Transcribe to transcribe medical and legal dictation.
- Transcribe customer call recordings for analysis. Transcribe a customer service recording and then send the transcription to Amazon Comprehend to get keyword, topic, or sentiment information.

You can use Amazon Transcribe with other AWS services to create other applications. For example, you can use Amazon Transcribe to convert voice to text, send the text to Amazon Translate to translate the text into another language, and send the translated text to Amazon Polly to speak the translated text.

Are You a First-time User of Amazon Transcribe?

If you are a first-time user, we recommend that you read the following sections in order:

1. How Amazon Transcribe Works (p. 2) – Introduces Amazon Transcribe.
2. Getting Started with Amazon Transcribe (p. 4) – Explains how to set up your AWS account and test Amazon Transcribe.
3. API Reference (p. 22) – Contains reference documentation for Amazon Transcribe operations.
How Amazon Transcribe Works

This is prerelease documentation for a service in preview release. It is subject to change.

Amazon Transcribe analyzes audio files containing speech and then uses advanced machine learning techniques to transcribe the voice data into text. You can then use the transcription as you would any text document.

Amazon Transcribe has three operations:

- **StartTranscriptionJob (p. 28)** – Starts an asynchronous job to transcribe the speech in an audio file to text.
- **ListTranscriptionJobs (p. 25)** – Returns a list of speech recognition jobs that have been started. You can specify the status of the jobs that you want the operation to return. For example, you can get a list of all pending jobs, or a list of completed jobs.
- **GetTranscriptionJob (p. 23)** – Returns the result of a speech recognition job. The response contains a link to a JSON file containing the results.

Speech Input

Input to an Amazon Transcribe transcription job comes from an object stored in an Amazon S3 bucket. The input file must be:

- In FLAC, MP3, MP4 or WAV file format
- Less than 2 hours in length

You must specify the language, format, and sampling rate of the input file.

For best results,

- Use a lossless format, such as FLAC or WAV with PCM 16-bit encoding.
- The sample rate should be 8000 Hz for low-fidelity audio and 16000 Hz for high-fidelity audio.

You must give Amazon Transcribe permission to access the Amazon S3 bucket that contains your input file. For more information about the required permissions, see Permissions Required for Audio Transcription (p. 18).

Output JSON

When Amazon Transcribe completes a transcription job, it creates a JSON file containing the results and puts the file in an S3 bucket. The file is identified by a user-specific URI. You use the URI to get the results.

The following is the JSON file for a short audio file:

```
{
```
"jobName":"job ID",
"accountId":"account ID",
"results": {
  "transcripts": [
    {
      "transcript":"that's no answer",
      "confidence":1.0
    }
  ],
  "items": [
    {
      "start_time":"0.180",
      "end_time":"0.470",
      "alternatives": [
        {
          "confidence":0.84,
          "word":"that's"
        }
      ]
    },
    {
      "start_time":"0.470",
      "end_time":"0.710",
      "alternatives": [
        {
          "confidence":0.99,
          "word":"no"
        }
      ]
    },
    {
      "start_time":"0.710",
      "end_time":"1.080",
      "alternatives": [
        {
          "confidence":0.874,
          "word":"answer"
        }
      ]
    }
  ],
  "status":"COMPLETED"
}
Getting Started with Amazon Transcribe

This is prerelease documentation for a service in preview release. It is subject to change.

To get started using Amazon Transcribe, set up an AWS account and create an AWS Identity and Access Management (IAM) user. To use the AWS Command Line Interface (AWS CLI), download and configure it.

Topics
• Step 1: Set up an AWS Account and Create an Administrator User (p. 4)
• Step 2: Set up the AWS Command Line Interface (AWS CLI) (p. 5)
• Step 3: Getting Started (Console) (p. 6)
• Step 4: Getting Started (AWS Command Line Interface) (p. 11)

Step 1: Set up an AWS Account and Create an Administrator User

Before you use Amazon Transcribe for the first time, complete the following tasks:
1. Sign up for AWS (p. 4)
2. Create an IAM User (p. 5)

Sign up for AWS

When you sign up for Amazon Web Services (AWS), your AWS account is automatically signed up for all AWS services, including Amazon Transcribe. You are charged only for the services that you use.

With Amazon Transcribe, you pay only for the resources that you use. If you are a new AWS customer, you can get started with Amazon Transcribe for free. For more information, see AWS Free Usage Tier.

If you already have an AWS account, skip to the next section.

To create an AWS account
1. Open https://aws.amazon.com/, and then choose Create an AWS Account.
   
   Note
   This might be unavailable in your browser if you previously signed into the AWS Management Console. In that case, choose Sign in to a different account, and then choose Create a new AWS account.

2. Follow the online instructions.
Part of the sign-up procedure involves receiving a phone call and entering a PIN using the phone keypad.

Record your AWS account ID because you'll need it for the next task.

Create an IAM User

Services in AWS, such as Amazon Transcribe, require that you provide credentials when you access them. This allows the service to determine whether you have permissions to access the service's resources.

We strongly recommend that you access AWS using AWS Identity and Access Management (IAM), not the credentials for your AWS account. To use IAM to access AWS, create an IAM user, add the user to an IAM group with administrative permissions, and then grant administrative permissions to the IAM user. You can then access AWS using a special URL and the IAM user's credentials.

The Getting Started exercises in this guide assume that you have a user with administrator privileges, adminuser.

To create an administrator user and sign in to the console

1. Create an administrator user called adminuser in your AWS account. For instructions, see Creating Your First IAM User and Administrators Group in the IAM User Guide.
2. Sign in to the AWS Management Console using a special URL. For more information, see How Users Sign In to Your Account in the IAM User Guide.

For more information about IAM, see the following:

• AWS Identity and Access Management (IAM)
• Getting Started
• IAM User Guide

Next Step

Step 2: Set up the AWS Command Line Interface (AWS CLI) (p. 5)

Step 2: Set up the AWS Command Line Interface (AWS CLI)

You don't need the AWS CLI to perform the steps in the Getting Started exercises. However, some of the other exercises in this guide do require it. If you prefer, you can skip this step and go to Step 3: Getting Started (Console) (p. 6), and set up the AWS CLI later.

To set up the AWS CLI

1. Download and configure the AWS CLI. For instructions, see the following topics in the AWS Command Line Interface User Guide:
   • Getting Set Up with the AWS Command Line Interface
• Configuring the AWS Command Line Interface

2. In the AWS CLI config file, add a named profile for the administrator user:

   ```
   [profile adminuser]
   aws_access_key_id = adminuser access key ID
   aws_secret_access_key = adminuser secret access key
   region = aws-region
   ```

   You use this profile when executing the AWS CLI commands. For more information about named profiles, see Named Profiles in the AWS Command Line Interface User Guide. For a list of AWS Regions, see Regions and Endpoints in the Amazon Web Services General Reference.

3. Verify the setup by typing the following help command at the command prompt:

   ```
   aws help
   ```

Next Step

Step 3: Getting Started (Console) (p. 6)

Step 3: Getting Started (Console)

The easiest way to get started with Amazon Transcribe is to submit a job using the console to transcribe an audio file. If you haven't reviewed the concepts and terminology in How Amazon Transcribe Works (p. 2), we recommend that you do that before proceeding.

Topics

• Create a Transcription Job (p. 6)
• View a Transcription Job (p. 7)

Create a Transcription Job

Use the Amazon Transcribe console to create a transcription job for your audio files.

1. Provide the following information:

   • **Transcription job name**—A name for the job. The name must be unique within your AWS account.
   • **S3 input URL**—The S3 location of your input audio file. You must grant Amazon Transcribe permission to access the bucket. For more information, see Permissions Required for Audio Transcription (p. 18).
   • **Language**—Choose the language of your input file. Amazon Transcribe can transcribe English and Spanish audio files.
   • **Format**—The format of the audio file. For best results you should use a lossless format such as FLAC or WAV with PCM 16-bit encoding.
   • **Media sampling rate (Hz)**—Optional. The bit sampling rate of the audio file. Amazon Transcribe accepts sample rates between 8000 Hz and 48000 Hz. For best results, you should use 8000 Hz for low-fidelity audio and 16000 for high-fidelity audio.

   The following shows the Create Transcription Job filled out for a sample job.
2. Choose Create to submit the job for processing.

View a Transcription Job

Completed transcription jobs are displayed in a list that contains a brief description of the job. The Availability column shows the remaining time that the job results will be kept on the server. Jobs are kept for 90 days and then deleted from the system.
Select a job in the list to see information about the job.

The information page about the transcription job has three sections. The **Detail** section provides details about the transcription job, including the name, information about when the job will be deleted from the server, and the input and output URLs. The output URL is where you can download the output from your transcription job.

The **Output** section contains the transcription of the audio submitted to Amazon Transcribe. You can download the transcription by choosing the **Download transcription** button.
The Code samples section contains the JSON input for the StartTranscriptionJob (p. 28) operation and the output from the GetTranscriptionJob (p. 23) operation.
Code Samples

Audio conversion

JSON Request

```
{
    "TranscriptionJobName": "\[Name\]",
    "LanguageCode": "en-US",
    "MediaSampleRateHertz": 8000,
    "MediaFormat": "wav",
    "Media": {
        "MediaFileUri": "https://\[Uri\]answer2.wav"
    }
}
```

JSON Response

```
{
    "TranscriptionJob": {
        "TranscriptionJobName": "\[Name\]",
        "TranscriptionJobStatus": "COMPLETED",
        "LanguageCode": "en-US",
        "MediaSampleRateHertz": 8000,
        "MediaFormat": "wav",
        "Media": {
            "MediaFileUri": "https://\[Uri\]answer2.wav?X-Amz-SecurityToken=\[Token\]"
        }
    }
}
```
Step 4: Getting Started (AWS Command Line Interface)

In the following exercise, you use the AWS Command Line Interface (AWS CLI) to transcribe speech into text. To complete this exercise, you need to:

- Have a text editor.
- Be familiar with the AWS CLI. For more information, see Step 2: Set up the AWS Command Line Interface (AWS CLI) (p. 5).
- Have a speech file in .WAV or .MP4 format that is stored in an S3 bucket that has the proper permissions. For more information about required permissions, see Permissions Required for Audio Transcription (p. 18).

To transcribe text, you have to provide the input parameters in a JSON file.

To transcribe text

1. Copy your input speech to an S3 bucket. This example assumes that the file is in an S3 bucket named test-transcribe and that the filename is Answer2.wav.

2. Create a JSON file named test-start-command.json that contains the input parameters for the StartTranscriptionJob (p. 28) operation.

```json
{
   "TranscriptionJobName": "request ID",
   "LanguageCode": "en-US",
   "MediaFormat": "wav",
   "Media": {
      "MediaFileUri": "https://S3 endpoint/test-transcribe/answer2.wav"
   }
}
```

3. In the AWS CLI, run the following command. The example is formatted for Unix, Linux, and macOS. For Windows, replace the backslash (\) Unix continuation character at the end of each line with a caret (^).

```
aws transcribe start-transcription-job
  --endpoint-url endpoint \
  --region region \
  --cli-input-json file://test-start-command.json
```

Amazon Transcribe responds with the following:

```json
{
   "TranscriptionJob": {
      "TranscriptionJobName": "request ID",
      "LanguageCode": "en-US",
      "TranscriptionJobStatus": "IN_PROGRESS",
      "Media": {
         "MediaFileUri": "https://S3 endpoint/test-transcribe/answer2.wav"
      },
      "CreationTime": "timestamp",
      "MediaFormat": "wav"
   }
}
```
To list transcription jobs

- Run the following command:

```bash
aws transcribe list-transcription-jobs \
   --endpoint-url endpoint \ 
   --region region \ 
   --status IN_PROGRESS
```

Amazon Transcribe responds with the following:

```json
{
   "Status": "IN_PROGRESS",
   "TranscriptionJobSummaries": [
      {
         "TranscriptionJobName": "request ID",
         "LanguageCode": "en-US",
         "CreationTime": timestamp,
         "TranscriptionJobStatus": "IN_PROGRESS"
      }
   ]
}
```

To get the results of a transcription job

1. When the job has the status COMPLETED, get the results of the job. Type the following command:

```bash
aws transcribe get-transcription-job-results \
   --endpoint-url endpoint \ 
   --region endpoint \ 
   --request-id "DocTest-01"
```

Amazon Transcribe responds with the following:

```json
{
   "TranscriptionJob": {
      "TranscriptionJobName": "request ID",
      "LanguageCode": "en-US",
      "TranscriptionJobStatus": "COMPLETED",
      "Media": {
         "MediaFileUri": "input URI"
      },
      "CreationTime": timestamp,
      "CompletionTime": timestamp,
      "Transcript": {
         "TranscriptFileUri": "output URI"
      }
   }
}
```

2. Use the output URI to get the transcribed text from the audio file. The following is the output from transcribing a short audio clip:

```json
{
   "jobName": "job ID",
   "accountId": "account ID",
   "results": {
      "transcripts": ["transcribed text"]
   }
}
```
"transcript":"that's no answer",
"confidence":1.0
],
"items":[
{
"start_time":"0.180",
"end_time":"0.470",
"alternatives":[
{
"confidence":0.84,
"word":"that's"
}
],
{
"start_time":"0.470",
"end_time":"0.710",
"alternatives":[
{
"confidence":0.99,
"word":"no"
}
],
{
"start_time":"0.710",
"end_time":"1.080",
"alternatives":[
{
"confidence":0.87,
"word":"answer"
}
]
},
"status":"COMPLETED"}
Authentication and Access Control for Amazon Transcribe

This is prerelease documentation for a service in preview release. It is subject to change.

Access to Amazon Transcribe requires credentials that AWS can use to authenticate your requests. Those credentials must have permissions to access Amazon Transcribe actions. The following sections provide details on how you can use AWS Identity and Access Management (IAM) and Amazon Transcribe to help secure your resources by controlling who can access them.

- Authentication (p. 14)
- Access Control (p. 15)

Authentication

You can access AWS as any of the following types of identities:

- **AWS account root user** – When you first create an AWS account, you begin with a single sign-in identity that has complete access to all AWS services and resources in the account. This identity is called the AWS account root user and is accessed by signing in with the email address and password that you used to create the account. We strongly recommend that you do not use the root user for your everyday tasks, even the administrative ones. Instead, adhere to the best practice of using the root user only to create your first IAM user. Then securely lock away the root user credentials and use them to perform only a few account and service management tasks.

- **IAM user** – An IAM user is an identity within your AWS account that has specific custom permissions (for example, permissions to create in Amazon Transcribe). You can use an IAM user name and password to sign in to secure AWS webpages like the AWS Management Console, AWS Discussion Forums, or the AWS Support Center.

In addition to a user name and password, you can also generate access keys for each user. You can use these keys when you access AWS services programmatically, either through one of the several SDKs or by using the AWS Command Line Interface (CLI). The SDK and CLI tools use the access keys to cryptographically sign your request. If you don’t use AWS tools, you must sign the request yourself. Amazon Transcribe supports Signature Version 4, a protocol for authenticating inbound API requests. For more information about authenticating requests, see Signature Version 4 Signing Process in the AWS General Reference.

- **IAM role** – An IAM role is an IAM identity that you can create in your account that has specific permissions. It is similar to an IAM user, but it is not associated with a specific person. An IAM role enables you to obtain temporary access keys that can be used to access AWS services and resources. IAM roles with temporary credentials are useful in the following situations:
• **Federated user access** – Instead of creating an IAM user, you can use existing user identities from AWS Directory Service, your enterprise user directory, or a web identity provider. These are known as federated users. AWS assigns a role to a federated user when access is requested through an identity provider. For more information about federated users, see Federated Users and Roles in the IAM User Guide.

• **AWS service access** – You can use an IAM role in your account to grant an AWS service permissions to access your account’s resources. For example, you can create a role that allows Amazon Redshift to access an Amazon S3 bucket on your behalf and then load data from that bucket into an Amazon Redshift cluster. For more information, see Creating a Role to Delegate Permissions to an AWS Service in the IAM User Guide.

• **Applications running on Amazon EC2** – You can use an IAM role to manage temporary credentials for applications that are running on an EC2 instance and making AWS API requests. This is preferable to storing access keys within the EC2 instance. To assign an AWS role to an EC2 instance and make it available to all of its applications, you create an instance profile that is attached to the instance. An instance profile contains the role and enables programs that are running on the EC2 instance to get temporary credentials. For more information, see Using an IAM Role to Grant Permissions to Applications Running on Amazon EC2 Instances in the IAM User Guide.

Access Control

You must have valid credentials to authenticate your requests. The credentials must have permissions to call an Amazon Transcribe action.

The following sections describe how to manage permissions for Amazon Transcribe. We recommend that you read the overview first.

• Overview of Managing Access Permissions to Amazon Transcribe Resources (p. 15)
• Using Identity-based Policies (IAM Policies) for Amazon Transcribe (p. 17)

Overview of Managing Access Permissions to Amazon Transcribe Resources

Permissions to access an action are governed by permissions policies. An account administrator can attach permissions policies to IAM identities (that is, users, groups, and roles) to manage access to actions.

**Note**

An account administrator (or administrator user) is a user with administrator privileges. For more information, see IAM Best Practices in the IAM User Guide.

When granting permissions, you decide who is getting the permissions and the actions they get permissions for.

**Topics**

• Managing Access to Actions (p. 16)
• Specifying Policy Elements: Resources, Actions, Effects, and Principals (p. 16)
• Specifying Conditions in a Policy (p. 17)
Managing Access to Actions

A permissions policy describes who has access to what. The following section explains the options for creating permissions policies.

Note
This section discusses using IAM in the context of Amazon Transcribe. It doesn't provide detailed information about the IAM service. For complete IAM documentation, see What Is IAM? in the IAM User Guide. For information about IAM policy syntax and descriptions, see AWS IAM Policy Reference in the IAM User Guide.

Policies attached to an IAM identity are referred to as identity-based policies (IAM polices) and policies attached to a resource are referred to as resource-based policies. Amazon Transcribe supports only identity-based policies.

Identity-Based Policies (IAM Policies)

You can attach policies to IAM identities. For example, you can do the following:

- **Attach a permissions policy to a user or a group in your account** – To grant a user or a group of users permissions to call an Amazon Transcribe action, you can attach a permissions policy to a user or group that the user belongs to.
- **Attach a permissions policy to a role (grant cross-account permissions)** – To grant cross-account permissions, you can attach an identity-based permissions policy to an IAM role. For example, the administrator in Account A can create a role to grant cross-account permissions to another AWS account (for example, Account B) or an AWS service as follows:
  1. Account A administrator creates an IAM role and attaches a permissions policy to the role that grants permissions on resources in Account A.
  2. Account A administrator attaches a trust policy to the role identifying Account B as the principal who can assume the role.
  3. Account B administrator can then delegate permissions to assume the role to any users in Account B. Doing this allows users in Account B to create or access resources in Account A. If you want to grant an AWS service permissions to assume the role, the principal in the trust policy can be an AWS service principal.

For more information about using IAM to delegate permissions, see Access Management in the IAM User Guide.

For more information about using identity-based policies with Amazon Transcribe, see Using Identity-based Policies (IAM Policies) for Amazon Transcribe (p. 17). For more information about users, groups, roles, and permissions, see Identities (Users, Groups, and Roles) in the IAM User Guide.

Resource-Based Policies

Other services, such as AWS Lambda, support resource-based permissions policies. For example, you can attach a policy to an S3 bucket to manage access permissions to that bucket. Amazon Transcribe doesn’t support resource-based policies.

Specifying Policy Elements: Resources, Actions, Effects, and Principals

Amazon Transcribe defines a set of API operations (see Actions (p. 22)). To grant permissions for these API operations, Amazon Transcribe defines a set of actions that you can specify in a policy.
The following are the most basic policy elements:

- **Resource** – In a policy, you use an Amazon Resource Name (ARN) to identify the resource to which the policy applies. For Amazon Transcribe, the resource is always "*".

- **Action** – You use action keywords to identify operations that you want to allow or deny. For example, depending on the specified Effect, ASH:Translate either allows or denies the user permissions to perform the Amazon Transcribe Translate operation.

- **Effect** – You specify the effect of the action that occurs when the user requests the specific action —this can be either allow or deny. If you don't explicitly grant access to (allow) a resource, access is implicitly denied. You can also explicitly deny access to a resource. You might do this to make sure that a user cannot access the resource, even if a different policy grants access.

- **Principal** – In identity-based policies (IAM policies), the user that the policy is attached to is the implicit principal.

To learn more about IAM policy syntax and descriptions, see AWS IAM Policy Reference in the IAM User Guide.

For a table of Amazon Transcribe API actions, see Amazon Transcribe API Permissions: Actions, Resources, and Conditions Reference (p. 19).

### Specifying Conditions in a Policy

When you grant permissions, you use the IAM policy language to specify the conditions under which a policy should take effect. For example, you might want a policy to be applied only after a specific date. For more information about specifying conditions in a policy language, see **Condition** in the IAM User Guide.

AWS provides a set of predefined condition keys for all AWS services that support IAM for access control. For example, you can use the `aws:userid` condition key to require a specific AWS ID when requesting an action. For more information and a complete list of AWS-wide keys, see Available Keys for Conditions in the IAM User Guide.

**Note**
Condition keys are case sensitive.

Amazon Transcribe does not provide additional condition keys.

### Using Identity-based Polices (IAM Policies) for Amazon Transcribe

This topic provides examples of identity-based policies that demonstrate how an account administrator can attach permissions policies to IAM identities (users, groups, and roles) and thereby grant permissions to perform Amazon Transcribe actions.

**Important**
Before you proceed, we recommend that you review Overview of Managing Access Permissions to Amazon Transcribe Resources (p. 15).

The following is the permissions policy required to use the Amazon Transcribe StartTranscriptionJob action:

```json
{
    "Version": "2012-10-17",
    "Statement": [
```
The policy has one statement that grants permission to use the `StartTranscriptionJob` action. The policy doesn't specify the `Principal` element because you don't specify the principal who gets the permission in an identity-based policy. When you attach a policy to a user, the user is the implicit principal. When you attach a permissions policy to an IAM role, the principal identified in the role's trust policy gets the permissions.

For a table of Amazon Transcribe API actions and the resources that they apply to, see [Amazon Transcribe API Permissions: Actions, Resources, and Conditions Reference](#).

**Permissions Required to Use the Amazon Transcribe Console**

To use the Amazon Transcribe console, you need to grant permissions for the actions shown in the following policy:

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": ["transcribe:*"],
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

The policy enables the user to call all of the Amazon Transcribe operations.

**Permissions Required for Audio Transcription**

To use the Amazon Transcribe `StartTranscriptionJob` operation, you must grant Amazon Transcribe access to the Amazon S3 bucket that contains your input speech. You do this by creating permissions for the Amazon Transcribe service principal in the bucket.

The following is the permission policy:

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "transcribe.amazonaws.com"
            },
            "Action": ["transcribe:StartTranscriptionJob"],
            "Resource": "*"
        }
    ]
}
```
Permissions Required for Amazon S3 Encryption Keys

If you are using an AWS Key Management Service key to encrypt an Amazon S3 bucket, you need to include the following in the AWS KMS key policy to allow Amazon Transcribe access to the contents of the bucket. For more information about allowing access to customer master keys, see Allowing External AWS Accounts to Access a CMK in the AWS KMS Developer Guide.

```
{  
  "Sid": "Allow-Transcribe",  
  "Effect": "Allow",  
  "Principal": {  
    "Service": "transcribe.amazonaws.com"  
  },  
  "Action": [  
    "kms:Encrypt",  
    "kms:Decrypt",  
    "kms:ReEncrypt*",  
    "kms:GenerateDataKey*",  
    "kms:DescribeKey"  
  ],  
  "Resource": "*"  
}
```

Amazon Transcribe API Permissions: Actions, Resources, and Conditions Reference

Use the following table as a reference when setting up Access Control (p. 15) and writing a permissions policy that you can attach to an IAM identity (an identity-based policy). The list includes each Amazon Transcribe API operation, the corresponding action for which you can grant permissions to perform the action, and the AWS resource for which you can grant the permissions. You specify the actions in the policy’s `Action` field, and you specify the resource value in the policy’s `Resource` field.

To express conditions in your Amazon Transcribe policies, you can use AWS-wide condition keys. For a complete list of AWS-wide keys, see Available Keys in the IAM User Guide.

**Note**

To specify an action, use the `transcribe:` prefix followed by the API operation name, for example, `transcribe:StartTranscriptionJob`. 
Beta Guidelines and Limits

This is prerelease documentation for a service in preview release. It is subject to change.

Guidelines

Amazon Transcribe is available in the following region:

<table>
<thead>
<tr>
<th>Region Name</th>
<th>Region</th>
<th>Endpoint</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>US East (N. Virginia)</td>
<td>us-east-1</td>
<td><a href="https://transcribe.us-east-1.amazonaws.com">https://transcribe.us-east-1.amazonaws.com</a></td>
<td>HTTPS</td>
</tr>
</tbody>
</table>

For best results:
- Use a lossless format, such as FLAC or WAV with PCM 16-bit encoding.
- The sample rate should be 8000 Hz for low-fidelity audio and 16000 Hz for high-fidelity audio.

Limits

The beta release of Amazon Transcribe has the following limitations:
- The maximum audio file length is 2 hours.
Document History for Amazon Transcribe

The following table describes the documentation history for Amazon Transcribe.

- **Latest documentation update:** November 29, 2017

<table>
<thead>
<tr>
<th>Change</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>New guide</td>
<td>This is the first release of the <em>Amazon Transcribe Developer Guide</em>.</td>
<td>November 29, 2017</td>
</tr>
</tbody>
</table>
API Reference

This section contains the API Reference documentation.

Actions

The following actions are supported:

- GetTranscriptionJob (p. 23)
- ListTranscriptionJobs (p. 25)
- StartTranscriptionJob (p. 28)
GetTranscriptionJob

Returns information about a transcription job. To see the status of the job, check the Status field. If the status is COMPLETE, the job is finished and you can find the results at the location specified in the TranscriptionFileUri field.

Request Syntax

```json
{
    "TranscriptionJobName": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 37).

The request accepts the following data in JSON format.

**TranscriptionJobName (p. 23)**

The name of the job.

- Type: String
- Pattern: ^[0-9a-zA-Z._-]+$
- Required: Yes

Response Syntax

```json
{
    "TranscriptionJob": {
        "CompletionTime": number,
        "CreationTime": number,
        "FailureReason": "string",
        "LanguageCode": "string",
        "Media": {
            "MediaFileUri": "string"
        },
        "MediaFormat": "string",
        "MediaSampleRateHertz": number,
        "Transcript": {
            "TranscriptFileUri": "string"
        },
        "TranscriptionJobName": "string",
        "TranscriptionJobStatus": "string"
    }
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.
TranscriptionJob (p. 23)

An object that contains the results of the transcription job.

Type: TranscriptionJob (p. 33) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 36).

BadRequestException

There is a problem with one of the input fields. Check the S3 bucket name, make sure that the job name is not a duplicate, and confirm that you are using the correct file format. Then resend your request.

HTTP Status Code: 400

InternalFailureException

There was an internal error. Check the error message and try your request again.

HTTP Status Code: 500

LimitExceededException

Either you have sent too many requests or your input file is longer than 2 hours. Wait before you resend your request, or use a smaller file and resend the request.

HTTP Status Code: 400

NotFoundException

We can't find the requested job. Check the job name and try your request again.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V2
ListTranscriptionJobs

Lists transcription jobs with the specified status.

Request Syntax

```json
{
   "MaxResults": number,
   "NextToken": "string",
   "Status": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 37).

The request accepts the following data in JSON format.

MaxResults (p. 25)

The maximum number of jobs to return in the response.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 100.

Required: No

NextToken (p. 25)

If the result of the previous request to ListTranscriptionJobs was truncated, include the NextToken to fetch the next set of jobs.

Type: String

Length Constraints: Maximum length of 8192.

Required: No

Status (p. 25)

When specified, returns only transcription jobs with the specified status.

Type: String

Valid Values: IN_PROGRESS | FAILED | COMPLETED

Required: Yes

Response Syntax

```json
{
   "NextToken": "string",
   "Status": "string",
   "TranscriptionJobSummaries": [
   { "CompletionTime": number,
```
Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

**NextToken (p. 25)**

The ListTranscriptionJobs operation returns a page of jobs at a time. The size of the page is set by the MaxResults parameter. If there are more jobs in the list than the page size, Amazon Transcribe returns the NextPage token. Include the token in the next request to the ListTranscriptionJobs operation to return in the next page of jobs.

Type: String
Length Constraints: Maximum length of 8192.

**Status (p. 25)**

The requested status of the jobs returned.

Type: String

Valid Values: IN_PROGRESS | FAILED | COMPLETED

**TranscriptionJobSummaries (p. 25)**

A list of objects containing summary information for a transcription job.

Type: Array of TranscriptionJobSummary (p. 35) objects

**Errors**

For information about the errors that are common to all actions, see Common Errors (p. 36).

**BadRequestException**

There is a problem with one of the input fields. Check the S3 bucket name, make sure that the job name is not a duplicate, and confirm that you are using the correct file format. Then resend your request.

HTTP Status Code: 400

**InternalFailureException**

There was an internal error. Check the error message and try your request again.

HTTP Status Code: 500

**LimitExceededException**

Either you have sent too many requests or your input file is longer than 2 hours. Wait before you resend your request, or use a smaller file and resend the request.
HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V2
StartTranscribeDeveloperGuide
StartTranscriptionJob

Starts an asynchronous job to transcribe speech to text.

Request Syntax

```json
{
    "LanguageCode": "string",
    "Media": {
        "MediaFileUri": "string"
    },
    "MediaFormat": "string",
    "MediaSampleRateHertz": number,
    "TranscriptionJobName": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 37).

The request accepts the following data in JSON format.

**LanguageCode (p. 28)**

The language code for the language used in the input media file.

- **Type:** String
- **Valid Values:** en-US | es-US
- **Required:** Yes

**Media (p. 28)**

An object that describes the input media for a transcription job.

- **Type:** Media (p. 31) object
- **Required:** Yes

**MediaFormat (p. 28)**

The format of the input media file.

- **Type:** String
- **Valid Values:** mp3 | mp4 | wav | flac
- **Required:** Yes

**MediaSampleRateHertz (p. 28)**

The sample rate, in Hertz, of the audio track in the input media file.

- **Type:** Integer
- **Valid Range:** Minimum value of 8000. Maximum value of 48000.
- **Required:** No

**TranscriptionJobName (p. 28)**

The name of the job. The name must be unique within an AWS account.
Type: String


Pattern: ^[0-9a-zA-Z._-]+$

Required: Yes

Response Syntax

```json
{
  "TranscriptionJob": {
    "CompletionTime": number,
    "CreationTime": number,
    "FailureReason": "string",
    "LanguageCode": "string",
    "Media": {
      "MediaFileUri": "string"
    },
    "MediaFormat": "string",
    "MediaSampleRateHertz": number,
    "Transcript": {
      "TranscriptFileUri": "string"
    },
    "TranscriptionJobName": "string",
    "TranscriptionJobStatus": "string"
  }
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

TranscriptionJob (p. 29)

An object containing details of the asynchronous transcription job.

Type: TranscriptionJob (p. 33) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 36).

**BadRequestException**

There is a problem with one of the input fields. Check the S3 bucket name, make sure that the job name is not a duplicate, and confirm that you are using the correct file format. Then resend your request.

HTTP Status Code: 400

**ConflictException**

The JobName field is a duplicate of a previously entered job name. Resend your request with a different name.

HTTP Status Code: 400
**InternalFailureException**

There was an internal error. Check the error message and try your request again.

HTTP Status Code: 500

**LimitExceeded Exception**

Either you have sent too many requests or your input file is longer than 2 hours. Wait before you resend your request, or use a smaller file and resend the request.

HTTP Status Code: 400

**See Also**

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V2

**Data Types**

The following data types are supported:

- Media (p. 31)
- Transcript (p. 32)
- TranscriptionJob (p. 33)
- TranscriptionJobSummary (p. 35)
Media

Describes the input media file in a transcription request.

Contents

MediaFileUri

The S3 location of the input media file. The URI must be in the same region as the API endpoint that you are calling. The general form is:

https://<aws-region>.amazonaws.com/<bucket-name>/<keyprefix>/<objectkey>

For example:

https://s3-us-east-1.amazonaws.com/examplebucket/example.mp4
https://s3-us-east-1.amazonaws.com/examplebucket/mediadocs/example.mp4

For more information about S3 object names, see Object Keys in the Amazon S3 Developer Guide.

Type: String


Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for Ruby V2
Transcript

Describes the output of a transcription job.

Contents

TranscriptFileUri

The S3 location where the transcription result is stored. Use this URI to access the results of the transcription job.

Type: String


Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for Ruby V2
TranscriptionJob

Describes an asynchronous transcription job that was created with the StartTranscriptionJob operation.

Contents

CompletionTime

Timestamp of the date and time that the job completed.

Type: Timestamp

Required: No

CreationTime

Timestamp of the date and time that the job was created.

Type: Timestamp

Required: No

FailureReason

If the TranscriptionJobStatus field is FAILED, this field contains information about why the job failed.

Type: String

Required: No

LanguageCode

The language code for the input speech.

Type: String

Valid Values: en-US | es-US

Required: No

Media

An object that describes the input media for a transcription job.

Type: Media (p. 31) object

Required: No

MediaFormat

The format of the input media file.

Type: String

Valid Values: mp3 | mp4 | wav | flac

Required: No

MediaSampleRateHertz

The sample rate, in Hertz, of the audio track in the input media file.

Type: Integer

Required: No

**Transcript**

An object that describes the output of the transcription job.

Type: Transcript (p. 32) object

Required: No

**TranscriptionJobName**

A name to identify the transcription job.

Type: String


Pattern: ^[0-9a-zA-Z._-]+$

Required: No

**TranscriptionJobStatus**

The identifier assigned to the job when it was created.

Type: String

Valid Values: IN_PROGRESS | FAILED | COMPLETED

Required: No

**See Also**

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for Ruby V2
TranscriptionJobSummary

Provides a summary of information about a transcription job.

Contents

CompletionTime

Timestamp of the date and time that the job completed.

Type: Timestamp

Required: No

CreationTime

Timestamp of the date and time that the job was created.

Type: Timestamp

Required: No

FailureReason

If the TranscriptionJobStatus field is FAILED, this field contains a description of the error.

Type: String

Required: No

LanguageCode

The language code for the input speech.

Type: String

Valid Values: en-US | es-US

Required: No

TranscriptionJobName

The name assigned to the transcription job when it was created.

Type: String


Pattern: ^[0-9a-zA-Z._-]+$

Required: No

TranscriptionJobStatus

The status of the transcription job. When the status is COMPLETED, use the GetTranscriptionJob operation to get the results of the transcription.

Type: String

Valid Values: IN_PROGRESS | FAILED | COMPLETED

Required: No
Common Errors

This section lists the errors common to the API actions of all AWS services. For errors specific to an API action for this service, see the topic for that API action.

AccessDeniedException
You do not have sufficient access to perform this action.
HTTP Status Code: 400

IncompleteSignature
The request signature does not conform to AWS standards.
HTTP Status Code: 400

InternalFailure
The request processing has failed because of an unknown error, exception or failure.
HTTP Status Code: 500

InvalidAction
The action or operation requested is invalid. Verify that the action is typed correctly.
HTTP Status Code: 400

InvalidClientTokenId
The X.509 certificate or AWS access key ID provided does not exist in our records.
HTTP Status Code: 403

InvalidParameterCombination
Parameters that must not be used together were used together.
HTTP Status Code: 400

InvalidParameterValue
An invalid or out-of-range value was supplied for the input parameter.
HTTP Status Code: 400

InvalidQueryParameter
The AWS query string is malformed or does not adhere to AWS standards.
HTTP Status Code: 400
MalformedQueryString
The query string contains a syntax error.
HTTP Status Code: 404

MissingAction
The request is missing an action or a required parameter.
HTTP Status Code: 400

MissingAuthenticationToken
The request must contain either a valid (registered) AWS access key ID or X.509 certificate.
HTTP Status Code: 403

MissingParameter
A required parameter for the specified action is not supplied.
HTTP Status Code: 400

OptInRequired
The AWS access key ID needs a subscription for the service.
HTTP Status Code: 403

RequestExpired
The request reached the service more than 15 minutes after the date stamp on the request or more than 15 minutes after the request expiration date (such as for pre-signed URLs), or the date stamp on the request is more than 15 minutes in the future.
HTTP Status Code: 400

ServiceUnavailable
The request has failed due to a temporary failure of the server.
HTTP Status Code: 503

ThrottlingException
The request was denied due to request throttling.
HTTP Status Code: 400

ValidationError
The input fails to satisfy the constraints specified by an AWS service.
HTTP Status Code: 400

Common Parameters
The following list contains the parameters that all actions use for signing Signature Version 4 requests with a query string. Any action-specific parameters are listed in the topic for that action. For more information about Signature Version 4, see Signature Version 4 Signing Process in the Amazon Web Services General Reference.

Action
The action to be performed.
Type: string
Required: Yes
**Version**

The API version that the request is written for, expressed in the format YYYY-MM-DD.

Type: string
Required: Yes

**X-Amz-Algorithm**

The hash algorithm that you used to create the request signature.

Condition: Specify this parameter when you include authentication information in a query string instead of in the HTTP authorization header.

Type: string
Valid Values: AWS4-HMAC-SHA256

Required: Conditional

**X-Amz-Credential**

The credential scope value, which is a string that includes your access key, the date, the region you are targeting, the service you are requesting, and a termination string ("aws4_request"). The value is expressed in the following format: access_key/YYYYMMDD/region/service/aws4_request. For more information, see Task 2: Create a String to Sign for Signature Version 4 in the Amazon Web Services General Reference.

Condition: Specify this parameter when you include authentication information in a query string instead of in the HTTP authorization header.

Type: string

Required: Conditional

**X-Amz-Date**

The date that is used to create the signature. The format must be ISO 8601 basic format ("YYYYMMDD'T'HHMMSS'Z'"). For example, the following date time is a valid X-Amz-Date value: 20120325T120000Z.

Condition: X-Amz-Date is optional for all requests; it can be used to override the date used for signing requests. If the Date header is specified in the ISO 8601 basic format, X-Amz-Date is not required. When X-Amz-Date is used, it always overrides the value of the Date header. For more information, see Handling Dates in Signature Version 4 in the Amazon Web Services General Reference.

Type: string

Required: Conditional

**X-Amz-Security-Token**

The temporary security token that was obtained through a call to AWS Security Token Service (AWS STS). For a list of services that support temporary security credentials from AWS Security Token Service, go to AWS Services That Work with IAM in the IAM User Guide.

Condition: If you're using temporary security credentials from the AWS Security Token Service, you must include the security token.
Type: string
Required: Conditional
**X-Amz-Signature**

Specifies the hex-encoded signature that was calculated from the string to sign and the derived signing key.

Condition: Specify this parameter when you include authentication information in a query string instead of in the HTTP authorization header.

Type: string
Required: Conditional
**X-Amz-SignedHeaders**

Specifies all the HTTP headers that were included as part of the canonical request. For more information about specifying signed headers, see [Task 1: Create a Canonical Request For Signature Version 4](https://docs.aws.amazon.com/AmazonS3/latest/API/AmazonS3PaginationResponses.html) in the *Amazon Web Services General Reference*.

Condition: Specify this parameter when you include authentication information in a query string instead of in the HTTP authorization header.

Type: string
Required: Conditional
AWS Glossary

For the latest AWS terminology, see the AWS Glossary in the AWS General Reference.