Defining Lambda function permissions with an execution role

Archived: 2026-04-05 15:48:42 UTC

A Lambda function's execution role is an AWS Identity and Access Management (IAM) role that grants the function permission to access AWS services and resources. For example, you might create an execution role that has permission to send logs to Amazon CloudWatch and upload trace data to AWS X-Ray. This page provides information on how to create, view, and manage a Lambda function's execution role.

Lambda automatically assumes your execution role when you invoke your function. You should avoid manually calling `sts:AssumeRole` to assume the execution role in your function code. If your use case requires that the role assumes itself, you must include the role itself as a trusted principal in your role's trust policy. For more information on how to modify a role trust policy, see Modifying a role trust policy (console) in the IAM User Guide.

In order for Lambda to properly assume your execution role, the role's trust policy must specify the Lambda service principal (`lambda.amazonaws.com`) as a trusted service.

Topics

Creating an execution role in the IAM console

By default, Lambda creates an execution role with minimal permissions when you create a function in the Lambda console. Specifically, this execution role includes the `AWSLambdaBasicExecutionRole` managed policy, which gives your function basic permissions to log events to Amazon CloudWatch Logs. You can select **Create default role** in the **Permissions** section.

You can choose an existing role by selecting **Use another role** in the **Permissions** section. If your Lambda function needs additional permissions to perform tasks such as updating entries in an Amazon DynamoDB database in response to events, you can create a custom execution role with the necessary permissions. To do this, select **Use another role** in the **Permissions** section, which opens a drawer where you can customize your permissions.

To configure an execution role from Console

1. Enter a **role name** in the Role details section.
2. In the **Policy** section, select **Use existing policy**.
3. Select the AWS managed policies that you want to attach to your role. For example, if your function needs to access DynamoDB, select the **AWSLambdaDynamoDBExecutionRole** managed policy.
4. Choose **Create role**.

Alternatively, when you create a function in the Lambda console, you can attach any execution role that you previously created to the function. If you want to attach a new execution role to an existing function, follow the steps in Updating a function's execution role.

Creating and managing roles with the AWS CLI

To create an execution role with the AWS Command Line Interface (AWS CLI), use the **create-role** command. When using this command, you can specify the trust policy inline. A role's trust policy gives the specified principals permission to assume the role. In the following example, you grant the Lambda service principal permission to assume your role. Note that requirements for escaping quotes in the JSON string may vary depending on your shell.

```
aws iam create-role \
--role-name lambda-ex \
--assume-role-policy-document '{"Version": "2012-10-17","Statement": [{ "Effect": "Allow", "Principal": {"Service": "lambd
```

You can also define the trust policy for the role using a separate JSON file. In the following example, `trust-policy.json` is a file in the current directory.

Example trust-policy.json

```
{
"Version":"2012-10-17",
"Statement": [
  {
    "Effect": "Allow",
    "Principal": {
      "Service": "lambda.amazonaws.com"
    },
    "Action": "sts:AssumeRole"
  }
]
}
```

```
aws iam create-role \
--role-name lambda-ex \
--assume-role-policy-document file://trust-policy.json
```

To add permissions to the role, use the **attach-policy-to-role** command. The following command adds the `AWSLambdaBasicExecutionRole` managed policy to the `lambda-ex` execution role.

```
aws iam attach-role-policy --role-name lambda-ex --policy-arn arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutior
```

After you create your execution role, attach it to your function. When you create a function in the Lambda console, you can attach any execution role that you previously created to the function. If you want to attach a new execution role to an existing function, follow the steps in Updating a function's execution role.

Grant least privilege access to your Lambda execution role

When you first create an IAM role for your Lambda function during the development phase, you might sometimes grant permissions beyond what is required. Before publishing your function in the production environment, as a best practice, adjust the policy to include only the required permissions. For more information, see Apply least-privilege permissions in the *IAM User Guide*.

Use IAM Access Analyzer to help identify the required permissions for the IAM execution role policy. IAM Access Analyzer reviews your AWS CloudTrail logs over the date range that you specify and generates a policy template with only the permissions that the function used during that time. You can use the template to create a managed policy with fine-grained permissions, and then attach it to the IAM role. That way, you grant only the permissions that the role needs to interact with AWS resources for your specific use case.

For more information, see Generate policies based on access activity in the *IAM User Guide*.
