Create function Info

Choose one of the following options to create your function.

- 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
Enter a name that describes the purpose of your function.

myFunctionName

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.

Node.js 20.x

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

Role creation might take a few minutes. Please do not delete the role or edit the trust or permissions policies in this role.

Lambda will create an execution role named <myFunctionName>-role-ed369oob, with permission to upload logs to Amazon CloudWatch Logs.

▼ Advanced settings

Enable Code signing Info

Use code signing configurations to ensure that the code has been signed by an approved source and has not been altered since signing.

Enable function URL Info

Use function URLs to assign HTTP(S) endpoints to your Lambda function.

Auth type

Choose the auth type for your function URL. Learn more

- AWS_IAM
  Only authenticated IAM users and roles can make requests to your function URL.
- NONE
  Lambda won't perform IAM authentication on requests to your function URL. The URL endpoint will be public unless you implement your own authorization logic in your function.

Function URL permissions

When you choose auth type **NONE**, Lambda automatically creates the following resource-based policy and attaches it to your function. This policy makes your function public to anyone with the function URL. You can edit the policy later. To limit access to authenticated IAM users and roles, choose auth type **AWS_IAM**.

View policy statement

Invoke mode

Choose how your function returns responses. Learn more

- BUFFERED (default)
  The invocation results are available when the payload is complete. Response payload max size: 6 MB
- RESPONSE_STREAM
  Stream the invocation results. Streaming responses incurs additional costs. Refer to the documentation for payload size limitations. Learn more

Configure cross-origin resource sharing (CORS)

Use CORS to allow access to your function URL from any origin. You can also use CORS to control access for specific HTTP headers and methods in requests to your function URL. By default, all origins are allowed. You can edit this after creating the function. Learn more

Enable tags Info

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources, track your AWS costs, and enforce attribute-based access control.

Enable VPC Info

Connect your function to a VPC to access private resources during invocation.

VPC

Choose a VPC for your function to access.

vpc-0bc8e676704b47e83 (172.31.0.0/16)

Allow IPv6 traffic for dual-stack subnets

You can allow outbound IPv6 traffic to subnets that have both IPv4 and IPv6 CIDR blocks.

Subnets

Select the VPC subnets for Lambda to use to set up your VPC configuration.

Choose subnets

subnet-0f368396dc18bc45d (172.31.0.0/20) us-east-2a
Name: us-east-2a

▲We recommend that you choose at least 2 subnets for Lambda to run your functions in high availability mode.

Security groups

Choose the VPC security groups for Lambda to use to set up your VPC configuration. The table below shows the inbound and outbound rules for the security groups that you choose.

Choose security groups

sg-0f14fdee92b13303d (default)
default VPC security group

Inbound rules **Outbound rules**

1

Security group ID	Protocol	Ports	Source
sg-0f14fdee92b13303d	All	All	sg-0f14fdee92b13303d

Cancel **Create function**