**Creating an AWS Lambda Function for a Custom Config Rule**

1. Sign in to the AWS Management Console and open the AWS Lambda console at

<https://console.aws.amazon.com/lambda/>.

1. In the AWS Lambda console, choose **Create a Lambda function.**
2. Choose Use a blueprint. In the search bar, type config-rule-change-triggered. Select the blueprint
   1. in the filter results and choose Configure.
   2. On the Configure triggers page, choose Next.
   3. On the Basic information page, complete the following steps:
      1. For Function name, type InstanceTypeCheck.

b. For Execution role, choose Create new role from AWS Policy templates.

c. For Runtime, keep Node.js.

d. For Role name, type name.

e. For Policy templates, choose AWS Config Rules permission.

f. For Lambda function code function, keep the preconfigured code. The Node.js code for your

function is provided in the code editor. For this procedure, you do not need to change the code.

g. Verify the details and choose Create function. The AWS Lambda console displays your function.

7. To verify that your function is set up correctly, test it with the following steps:

a. Choose Test from the menu below Function overview and then choose Configure test event.

b. For Template, choose AWS Config Configuration Item Change Notification.

c. For Name, type a name.

d. Choose Test. AWS Lambda tests your function with the example event. If your function is

working as expected, an error message similar to the following appears under Execution result:

{

"errorType": "InvalidResultTokenException,"

"errorMessage": "Result Token provided is invalid",

. . .

The InvalidResultTokenException is expected because your function runs successfully

only when it receives a result token from AWS Config. The result token identifies the AWS Config

rule and the event that caused the evaluation, and the result token associates an evaluation

with a rule. This exception indicates that your function has the permission it needs to send

results to AWS Config. Otherwise, the following error message appears: not authorized to

perform: config:PutEvaluations. If this error occurs, update the role that you assigned

to your function to allow the config:PutEvaluations action, and test your function again.

**Creating a Custom Rule**

1. Open the AWS Config console at https://console.aws.amazon.com/config/.

2. In the AWS Management Console menu, verify that the region selector is set to the same region in

which you created the AWS Lambda function for your custom rule.

3. On the Rules page, choose Add rule.

4. On the Specify rule type page, choose Create custom rule.

5. On the Configure rule page, complete the following steps:

a. For Name, type InstanceTypesAreT2micro.

b. For Description, type Evaluates whether EC2 instances are the t2.micro type.

c. For AWS Lambda function ARN, specify the ARN that AWS Lambda assigned to your function.

Note

The ARN that you specify in this step must not include the $LATEST qualifier. You

can specify an ARN without a version qualifier or with any qualifier besides $LATEST.

AWS Lambda supports function versioning, and each version is assigned an ARN with a

qualifier. AWS Lambda uses the $LATEST qualifier for the latest version.

d. For Trigger type, choose When configuration changes.

e. For Scope of changes, choose Resources.

f. For Resources, choose AWS EC2 Instance from the Resource Type dropdown list.

g. In the Parameters section, you must specify the rule parameter that your AWS Lambda

function evaluates and the desired value. The function for this procedure evaluates the

desiredInstanceType parameter.

For Key, type desiredInstanceType. For Value, type t2.micro.

6. Choose Next. On the Review and create page, verify the details about your rule, and choose Add

rule function. Your new rule displays on the Rulespage.

Compliance will display Evaluating... until AWS Config receives evaluation results from your AWS

Lambda function. If the rule and the function are working as expected, a summary of the results

appears after several minutes. For example, a result of 2 noncompliant resource(s) indicates that 2

of your instances are not t2.micro instances, and a result of Compliant indicates that all instances

are t2.micro. You can update the results with the refresh button.

If the rule or function is not working as expected, you might see one of the following for

Compliance:

• No results reported - AWS Config evaluated your resources against the rule. The rule did not

apply to the AWS resources in its scope, the specified resources were deleted, or the evaluation

results were deleted. To get evaluation results, update the rule, change its scope, or choose Reevaluate.

Verify that the scope includes AWS EC2 Instance for Resources, and try again.

• No resources in scope - AWS Config cannot evaluate your recorded AWS resources against this

rule because none of your resources are within the rule’s scope. To get evaluation results, edit the

rule and change its scope, or add resources for AWS Config to record by using the Settings page.

Verify that AWS Config is recording EC2 instances.

• Evaluations failed - For information that can help you determine the problem, choose the rule

name to open its details page and see the error message.

If your rule works correctly and AWS Config provides evaluation results, you can learn which conditions

affect the compliance status of your rule. You can learn which resources, if any, are noncompliant, and

why. For more information, see Viewing Configuration Compliance (p. 100).

Developing a Custom Rule for AWS Config

Complete the following procedure to create a custom rule. To create a custom rule, you first create an

AWS Lambda function, which contains the evaluation logic for the rule. Then you associate the function

with a custom rule that you create in AWS Config.

Important

As a security best practice when allowing AWS Config permission to invoke your Lambda

function, we strongly recommend that you restrict access in the resource-based policy

for Lambda with sourceARN and/or sourceAccountId in the invoke request. For more

information, see Security best practice for AWS Lambda resource-based policy (p. 200).

**Delete Configuration**

* No option is provided from AWS Console to delete Configuration
* We need to execute below command from AWS CLI to delete configuration
  + aws configservice delete-configuration-recorder --configuration-recorder-name default