Accessing Internet from Lambda in a VPC (Assessment Version)

**SAL-TF-300-NWAIAL-1 - Version 1.0.0**

© 2024 Amazon Web Services, Inc. or its affiliates. All rights reserved. This work may not be reproduced or redistributed, in whole or in part, without prior written permission from Amazon Web Services, Inc. Commercial copying, lending, or selling is prohibited. All trademarks are the property of their owners.

Note: Do not include any personal, identifying, or confidential information into the lab environment. Information entered may be visible to others.

Corrections, feedback, or other questions? Contact us at [*AWS Training and Certification*](https://support.aws.amazon.com/#/contacts/aws-training).

**Lab overview**

This lab demonstrates the concept of granting a AWS Lambda function access to the internet while the function is attached to an Amazon Virtual Private Cloud (Amazon VPC).

AnyCompany needs to fetch data from a public website and hence uses a Lambda function to pull the data required for their application.

As a member of the cloud team at AnyCompany, you have been assigned to check a Lambda function configuration. The Lambda function is attached to a VPC and it must be able to access the internet when invoked. A junior member of your team already implemented the solution but it seems it was misconfigured.

Your task is to troubleshoot the issue and fix the configuration to allow the Lambda function to access the internet when invoked.

OBJECTIVES

By the end of this lab, you will be able to do the following:

* Test the Lambda function connectivity to the internet and verify the issue.
* Identify the issues in the existing configuration and remediate the configuration to allow the Lambda function to access the internet via the VPC.
* Learn the configuration required for a Lambda function attached to a VPC to access the internet.

TECHNICAL KNOWLEDGE PREREQUISITES

To successfully complete this lab, you should have a basic knowledge of:

* Navigating through the AWS Management Console.
* Amazon Virtual Private Cloud (Amazon VPC).
* AWS Lambda.

DURATION

This lab requires approximately *60* minutes to complete.

ICON KEY

Various icons are used throughout this lab to call attention to different types of instructions and notes. The following list explains the purpose for each icon:

* **Expected output:** A sample output that you can use to verify the output of a command or edited file.
* **Note:** A hint, tip, or important guidance.
* **Knowledge check:** An opportunity to check your knowledge and test what you have learned.
* **Hint:** A hint to a question or challenge.
* **Answer:** An answer to a question or challenge.
* **Task complete:** A conclusion or summary point in the lab.
* **Consider:** A moment to pause to consider how you might apply a concept in your own environment or to initiate a conversation about the topic at hand.

**Start lab**

1. To launch the lab, at the top of the page, choose **Start lab**.

**Caution:** You must wait for the provisioned AWS services to be ready before you can continue.

1. To open the lab, choose **Open Console**.

You are automatically signed in to the AWS Management Console in a new web browser tab.

**WARNING:** **Do not change the Region unless instructed.**

COMMON SIGN-IN ERRORS

**Error: You must first sign out**



If you see the message, **You must first log out before logging into a different AWS account:**

* Choose the **click here** link.
* Close your **Amazon Web Services Sign In** web browser tab and return to your initial lab page.
* Choose **Open Console** again.

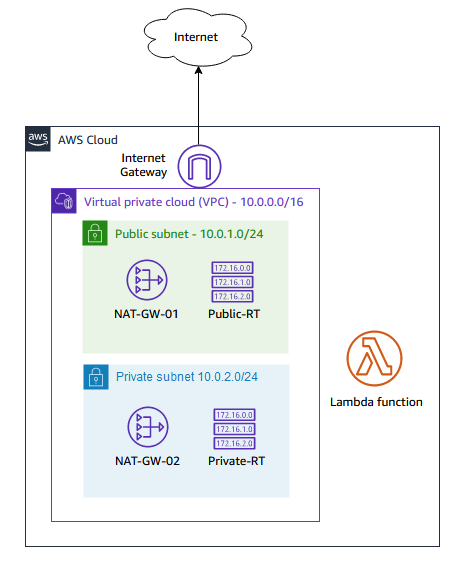
**Error: Choosing Start Lab has no effect**

In some cases, certain pop-up or script blocker web browser extensions might prevent the **Start Lab** button from working as intended. If you experience an issue starting the lab:

* Add the lab domain name to your pop-up or script blocker’s allow list or turn it off.
* Refresh the page and try again.

LAB ENVIRONMENT

The following diagram shows the lab scenario:



*Image description: The following list details the major resources in the lab:*

* *A VPC with one public subnet and one private subnet.*
* *An internet gateway attached to the VPC and provides access to the internet.*
* *Two NAT gateways (one in the public subnet and the other in the private subnet).*
* *Route tables for public and private subnets.*
* *A Lambda function with a simple code to access the internet and return a success if access is permitted. Otherwise, the function times out.*

AWS SERVICES NOT USED IN THIS LAB

AWS service capabilities used in this lab are limited to what the lab requires. Expect errors when accessing other services or performing actions beyond those provided in this lab guide.

**Task 1: Testing the Lambda function**

In this task, you test the Lambda function connectivity to the internet to verify the reported issue. You test the connectivity by creating a test event and invoking the Lambda function.

1. At the top of the AWS Management Console, in the search bar, search for and choose

Lambda

.

1. In the **Functions** page, choose the **Internet-Lambda-Function** link.
2. In the **Code** tab, you can examine the function code.

Simply, the function makes a call to a URL in the internet. If a response is received, it returns a *Success* message alongside the response data. Otherwise, the function times out after 3 seconds and returns a *Fail* message.

To test the function, you need to create a test event. The test event can be used to invoke the function and also pass parameters in the invocation. However, for the Lambda function you have, no input parameters are required as the function is only attempting to access a URL in the internet.

1. To create a test event, choose the **Test** button.
2. In the **Configure test event** popup window, configure the following:

* For **Test event action**, select **Create new event**.
* For **Event name**, enter

test-event

.

1. Leave all other fields as default and choose **Save**.

A message banner indicates that the test event was successfully saved.

Now you can test the function.

1. To test the function, choose the **Test** button.

**Expected output:** Output has been truncated.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\* EXAMPLE OUTPUT \*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Test Event Name

test-event

Response

{

"errorMessage": "2023-06-14T04:51:59.445Z aa215846-825f-4bac-bcd7-60c058710695 Task timed out after 3.01 seconds"

}

Function Logs

START RequestId: aa215846-825f-4bac-bcd7-60c058710695 Version: $LATEST

2023-06-14T04:51:59.445Z aa215846-825f-4bac-bcd7-60c058710695 Task timed out after 3.01 seconds

The function is invoked and the output of the invocation is displayed in the *Execution results* tab in the *Code source* pane.

Note that the function timed out after 3 seconds which is the timeout value configured for the function. This indicates that the function fails to access the internet.

**Task complete:** You tested the Lambda function and verified that the function cannot access the internet by running a test event.

**Task 2: Troubleshooting and remediating the issue**

In this task, you identify the issues in the existing configuration and remediate the configuration to allow the Lambda function to access the internet via the VPC.

Now that have you confirmed that the Lambda function cannot access the internet in the previous task, you need to identify the issues and remediate them.

You can navigate through the AWS Management Console of the Lambda function and any other service you need to understand why the current configuration and determine how to remediate it.

**Consider:** Here are few things to consider when you attempt remediating the issue:

* Do not attempt to change the Lambda function code as it has nothing to do with the issue.
* The solution requires that the Lambda function must be attached to the *Lab VPC*.
* You have the required AWS Identity and Access Management (IAM) permissions to remediate the issue.
* You have the permissions to use the Reachability Analyzer for troubleshooting.
* When adding Network ACL Rules, create them in increments of 100. For example: 100, 200.

DO IT YOURSELF

**Hint:** Here are some references to assist you in solving the issue:

* [Configuring a Lambda function to access resources in a VPC](https://docs.aws.amazon.com/lambda/latest/dg/configuration-vpc.html).
* [How do I give internet access to a Lambda function that’s connected to an Amazon VPC?](https://repost.aws/knowledge-center/internet-access-lambda-function).

SOLUTION

Expand the *Detailed instructions* section below for the full solution.

**Detailed instructions**

VERIFYING THE SOLUTION

Now, verify that you resolved all the issues and the Lambda function has access to the internet. Simply test the function by running the test event you created in the previous task.

1. At the top of the AWS Management Console, in the search bar, search for and choose

Lambda

.

1. In the **Functions** page, choose the **Internet-Lambda-Function** link.
2. To test the function, choose **Test**.

If the Lambda function can access the internet successfully, it should return the following output in the *Execution results* tab in the *Code source* pane.

**Expected output:** Output has been truncated.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\* EXAMPLE OUTPUT \*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Test Event Name

test-event

Response

"Success"

Function Logs

START RequestId: 736b2081-635a-432c-a4c4-8f8698632978 Version: $LATEST

data: {'args': {}, 'headers': {'Accept-Encoding': 'identity', 'Host': 'httpbin.org', 'User-Agent': 'Python-urllib/3.9', 'X-Amzn-Trace-Id': 'Root=1-647d65a6-01fda0cc038e178d262eeaad'}, 'origin': '35.163.250.201', 'url': 'https://httpbin.org/get'}

END RequestId: 736b2081-635a-432c-a4c4-8f8698632978

Observe that the *Response* is *Success* and the *Function Logs* returns the response data details from the requested URL.

**Note:** If your Lambda function output is still indicating that the function timed out, it means you still have not resolved all the issues in the configuration.

Also, examine in your Lambda execution results the value for the *origin* key. This represents the IP address making the outbound call to the internet. Compare this value with the value of *NATGateway01IPAddress* listed to the left of these instructions. The two values are the same. So the Lambda function in your scenario is always making outbound calls to the internet using the IP address of the NAT gateway in the public subnet.

This is very important if you need to have your Lambda function make outbound calls to the internet using the same public IP. If this call is targeting a 3rd party API, the 3rd party might want to allow only this IP address.

If you do not attach your Lambda function to a VPC, it is deployed in an AWS managed VPC. It can access the internet but it uses a different public IP for each outbound call.

**Consider:**

Here is a quick summary of the requirements for a Lambda function attached to a VPC to access the internet:

* The Lambda function must be attached to the VPC via a *Private subnet*.
* The private subnet where the Lambda is attached, must have a route to the internet via a NAT gateway.
* Any network access control list (network ACL) in the path of traffic must allow the required traffic in the correct directions.
* The security group of the Lambda function attachment must allow the required traffic in the correct direction.

**Task complete:** You identified the issues in the existing configuration and remediated the configuration to allow the Lambda function to access the internet via the VPC.

**Conclusion**

You have successfully done the following:

* Tested the Lambda function connectivity to the internet and verified the issue.
* Identified the issues in the existing configuration and remediated the configuration to allow the Lambda function to access the internet via the VPC.
* Learned the configuration required for a Lambda function attached to a VPC to access the internet.

**End lab**

Follow these steps to close the console and end your lab.

1. Return to the **AWS Management Console**.
2. At the upper-right corner of the page, choose **AWSLabsUser**, and then choose **Sign out**.
3. Choose **End lab** and then confirm that you want to end your lab.

For more information about AWS Training and Certification, see [*https://aws.amazon.com/training/*](https://aws.amazon.com/training/).

*Your feedback is welcome and appreciated.*  
If you would like to share any feedback, suggestions, or corrections, please provide the details in our [*AWS Training and Certification Contact Form*](https://support.aws.amazon.com/#/contacts/aws-training).