AWS Shield Engagement Lambda

The Configuration Guide

First published November 24, 2017

Last updated August 31, 2023

Notices

Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) represents current AWS product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from AWS and its affiliates, suppliers or licensors. AWS products or services are provided “as is” without warranties, representations, or conditions of any kind, whether express or implied. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

Contents

Abstract 4
Creating permissions for AWS Shield Engagement Lambda 5
Creating the IAM policy 5
Creating the IAM role 5
Set up the AWS Shield Engagement Lambda function 7
Testing the Lambda function 8
Using the AWS Shield Engagement Lambda function 9
Appendix 10
IAM policy 10

Abstract

The AWS Shield Engagement Lambda function is an AWS Lambda function that allows any AWS customer who is subscribed to Business Support or Enterprise Support to rapidly engage AWS Support during a Distributed Denial of Service (DDoS) attack that has impacted the availability of an application. Invoking this function will automatically create a support case. If you are subscribed to AWS Shield Advanced it will also proactively notify the AWS Shield Response Team (SRT) of the new support case.

Benefits of using the AWS Shield Engagement Lambda function include:

- **Faster case creation:** Your case is created with AWS Support seconds after engaging the function. There is no need to log into the AWS Management Console or type a manual reply.
- **Standardized engagement:** The support case will include a pre-composed message that tells the AWS Support engineer that you require immediate assistance with a DDoS attack. If you are subscribed to AWS Shield Advanced, the message also includes a request for a SRT escalation.
- **Faster escalation for AWS Shield Advanced cases:** After the AWS support case is opened, the case ID is sent to SRT in the form of an Amazon SNS message. This allows SRT engineers to engage proactively without waiting for a support engineer to commence escalation.

You can use the AWS Shield Engagement Lambda with any event source supported by AWS Lambda. For more information about Lambda event sources, see Supported Event Sources. Please be aware that misuse of this function may lead to this feature being disabled.

Following this guide will help you to set up an IAM role for Lambda, then the Lambda itself.

Creating permissions for AWS Shield Engagement Lambda

The AWS Shield Engagement Lambda requires permissions to perform tasks such as creating a support case. The following steps show how to create the required IAM role and policy.

Creating the IAM policy

1. Go to the AWS Management Console of an account that is subscribed to AWS Shield Advanced and Business or Enterprise Support where you would like to keep your Lambda function.
2. In the navigation search bar, enter `IAM` then select it.
3. Choose **Policies** then **Create policy**.
4. Instead of using the visual configuration, choose **JSON**, then replace the default text with the template provided in the Appendix labeled IAM policy.
5. Choose **Next**.
6. For the policy name, enter: `AWS_Shield_Engagement_Lambda_Policy`
7. Choose **Create policy**.

At the top of the page, you should see a banner saying:
Policy AWS_Shield_Engagement_Lambda_Policy created.

Creating the IAM role

If you just created the IAM policy and are still in the IAM console, skip to step 3.

1. Go to the AWS Management Console of an account that is subscribed to AWS Shield Advanced and Business or Enterprise Support where you would like to keep your Lambda function.
2. In the navigation search bar, enter `IAM`, then select it.
3. Choose **Roles** and then **Create role**. Provide the following configuration information:
    a. Trusted entity type: **AWS Service**
    b. User case: **Lambda**

c. Choose **Next**.

d. In the policies search field, enter the name `AWS_Shield_Engagement_Lambda_Policy` and press Enter.

e. Select the check box next to the policy, then choose **Next**.

f. For the **Role name**, enter: `AWS_Shield_Engagement_Lambda_Role`

g. Choose **Create role**.

At the top of the page, you should see a banner saying:
Role AWS_Shield_Engagement_Lambda_Role created.

You can now create the AWS Shield Engagement Lambda function itself.

Set up the AWS Shield Engagement Lambda function

If the required IAM role has not yet been created, perform the steps in the previous section before continuing.

1. Go to the AWS Management Console of an account that is subscribed to AWS Shield Advanced and Business or Enterprise Support where you would like to keep your Lambda function.
2. Select the `US East (N. Virginia)` Region from the navigation bar.
3. In the navigation search bar, enter `Lambda`, then select it.
4. Choose **Functions,** then **Create function**.
    a. Choose **Author from scratch**.
    b. For **Function name**, enter `AWS_Shield_Engagement_Lambda`
    c. The **Runtime** should be Python 3, for example, **Python 3.11**
    d. Architecture: **x86_64**
    e. Under **Permissions**, choose **Change default execution role**.
    f. For **Execution role**, choose **Use an existing role**.
    g. In the **Existing role** field, search for **AWS_Shield_Engagement_Lambda_Role** and select it.
    h. Choose **Create function**.
5. In the **Code** > **Code source** section, there will be some default code. Replace that code with the code from here.
6. Choose **Deploy**.
7. Under **Configuration** > **General configuration**, choose **Edit.**
8. Update the **Timeout** to 10 seconds, then choose **Save**.

Testing the Lambda function

You can test your function by pressing the **Test** button and looking for a new case in the AWS Support Center. Immediately close the case that was created during your test. After you have completed your testing, change the test variable to `off`. Any further runs of the Lambda function will be treated as an urgent request for assistance.

1. Choose **Test.**

   This opens a window to create a test event. Only provide an **Event name**, then choose **Save.**

2. Choose **Test** again. This runs the configured test event and shows an **Execution results** window. This opens a low severity support case. Resolve it by following these steps:

   a. In the navigation search bar, enter `Support`, then select it.

   b. Choose **Your support cases,** then select the most recent case which would have a **Subject** of **Immediate SRT assistance with DDoS attack**.

   c. Choose **Resolve case**.

Now that we know the support flow works, the Lambda *test mode* needs to be disabled.

1. Navigate back to the Lambda function, and under **Code source**, choose **lambda_function**.

2. Within the code, there is a line which looks like this:
   ```
   "test": "on", # Should be set to "off" when in production
   ```
   Change it to be:
   ```
   "test": "off", # Should be set to "off" when in production
   ```

3. Choose **Deploy.**

The Lambda function is now ready to be used to notify the AWS DDoS Response Team (DRT) of DDoS events.

Using the AWS Shield Engagement Lambda function

If your application is impacted by a DDoS attack, execute the Lambda function. An AWS Support case will open automatically. If you are subscribed to AWS Shield Advanced, you will receive a reply asking you to join an Amazon Chime call. You can install Amazon Chime in advance to take advantage of its chat and screen sharing features when communicating with SRT.

If you are not subscribed to AWS Shield Advanced, AWS Support will follow the instructions provided in the `txt` files referenced in the `standardSubject` and `standardMessage` variables. For example, you might include instructions to call you at a particular telephone number.

If you require any assistance with the AWS Shield Engagement Lambda, let us know by opening a case in the AWS Support Center under the **AWS Shield** service to let us know.

Appendix

IAM policy

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogGroup",
                "logs:CreateLogStream",
                "logs:PutLogEvents"
            ],
            "Resource": "arn:aws:logs:*:*:*"
        },
        {
            "Action": [
                "sns:Publish"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:sns:us-east-1:832974201822:*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "support:*"
            ],
            "Resource": "*"
        }
    ]
}
```