



6. If the *eventSource* value from the log record is from any of the Unauthorized Regions, then the Lambda function opens a ticket on ServiceNow.

## How to Deploy Lambda Function:

### CloudTrail:

1. In AWS CloudTrail Console, turn on the trail by specifying “bucket\_name” in the region for CloudTrail to save logs.
2. Perform the above step for all the non-us regions and specify the same “bucket\_name” to save the logs.

### IAM Role:

1. Login to AWS IAM Console.
2. Create a managed policy and attach it to the IAM role. In this step, you modify an existing AWS Managed Policy, save it using a different name, and then attach the permissions policy to an IAM role that you create.
  - A. Choose **Policies** and then choose **Create Policy**.
  - B. Select **Copy an AWS Managed Policy**.
  - C. Search for **AWSLambdaExecute** and select it.
  - D. Copy the following policy in the **Policy Document**. Make sure you specify the bucket name.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "logs:*"
      ],
      "Resource": "arn:aws:logs:*:*:*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject"
      ],
      "Resource": "arn:aws:s3:::bucket_name/*"
    }
  ]
}
```

3. Note the Policy Name.
4. Create an IAM role and then attach the permissions policy to the role.
  - A. In AWS IAM Console, click **Roles** and then **Create New Role**.
  - B. In **Role Name**, use a unique role name and click **Next Step** (for example, lambda-cloudtrail-execution-role)
  - C. In **Selece Role Type**, expand **AWS Service Roles** and then choose **AWS Lambda**.
  - D. In **Attach Policy**, choose the policy created in previous step.
  - E. Click **Next Step** to review the role and then click **Create Role**.

## Lambda:

1. Create a Lambda function deployment package and upload it.

```
$ cd monitoring-aws-activity-in-unauthorized-regions/
```

```
$ zip -r temp.zip *
```

```
$ aws lambda create-function \  
--region us-west-2 \  
--function-name cloudtrail-non-us-regions \  
--zip-file fileb://temp.zip \  
--role execution-role-arn \  
--handler lambda_function.lambda_handler \  
--runtime python2.7 \  
--timeout 10 \  
--memory-size 1024
```

2. To update the lambda function use:

```
$ aws lambda update-function-code --function-name=cloudtrail-non-us-regions --zip-file  
fileb://temp.zip
```

**NOTE:** Specify username and password in the ServiceNowConstants.py file before creating and uploading the deployment package.

3. Configure Amazon S3 to publish events.

- A. In AWS Lambda Console, select **Functions** and select the function which is just created.
- B. Choose **Triggers** and then choose **Add Trigger**.
- C. Search for “S3” and then select the **Bucket** (“bucket\_name” in our example), **Event type** as “**Object Created (All)**” and **Submit**.

## References:

[1] <http://docs.aws.amazon.com/lambda/latest/dg/with-cloudtrail.html>