

## Steps to enable cross account SQS-Lambda trigger

### Consumer Account (Lambda)

1. Create a lambda service role using the below assume role policy document

MINGW64: c:/workspace/aws

```
{
  "Version": "2012-10-17",
  "Id": "crossaccount-role",
  "Statement": [
    {
      "Sid": "AllowCrossAccountSQSToTriggerLambda",
      "Effect": "Allow",
      "Principal": {
        "Service": "lambda.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

```
$ aws iam create-role --role-name crossaccount-role --assume-role-policy-document file://po.json
{
  "Role": {
    "Path": "/",
    "RoleName": "crossaccount-role",
    "RoleId": "AROAZC4FS75Q63HTBCZS2",
    "Arn": "arn:aws:iam::[REDACTED]:role/crossaccount-role",
    "CreateDate": "2020-09-11T03:32:32+00:00",
    "AssumeRolePolicyDocument": {
      "Version": "2012-10-17",
      "Id": "crossaccount-role",
      "Statement": [
        {
          "Sid": "AllowCrossAccountSQSToTriggerLambda",
          "Effect": "Allow",
          "Principal": {
            "Service": "lambda.amazonaws.com"
          },
          "Action": "sts:AssumeRole"
        }
      ]
    }
  }
}
```

2. Attach two more AWS managed policies to the above role

- a. AWSLambdaFullAccess
- b. AWSLambdaSQSQueueExecutionRole

Roles > crossaccount-role

### Summary Delete role

Role ARN	arn:aws:iam::[redacted]:role/crossaccount-role
Role description	<a href="#">Edit</a>
Instance Profile ARNs	
Path	/
Creation time	2020-09-10 23:32 EDT
Last activity	2020-09-11 00:18 EDT (Today)
Maximum session duration	1 hour <a href="#">Edit</a>

Permissions

Trust relationships

Tags

Access Advisor

Revoke sessions

▼ Permissions policies (2 policies applied)

[Attach policies](#) + Add inline policy

Policy name ▼	Policy type ▼	
▶  AWSLambdaFullAccess	AWS managed policy	✕
▶  AWSLambdaSQSQueueExecutionRole	AWS managed policy	✕
▶ Permissions boundary (not set)		

3. Create a Lambda function using this role

4. Create an event source mapping between This lambda and SQS queue

```
vivek@DESKTOP-9VVV7IB MINGW64 /c/workspace/aws
$ aws lambda create-event-source-mapping --event-source-arn arn:aws:sqs:us-east-1:162[redacted]:cross-q --function-name arn:aws:lambda:us-east-1:624[redacted]:function:corss-function
{
  "UUID": "72dfff4f-5384-4bb0-83ca-803d3ab4bfa7",
  "BatchSize": 10,
  "EventSourceArn": "arn:aws:sqs:us-east-1:162[redacted]:cross-q",
  "FunctionArn": "arn:aws:lambda:us-east-1:624[redacted]:function:corss-function",
  "LastModified": "2020-09-11T00:13:36.834000-04:00",
  "State": "Creating",
  "StateTransitionReason": "USER_INITIATED"
}
vivek@DESKTOP-9VVV7IB MINGW64 /c/workspace/aws
```

## Producer Account (SQS)

1. Modify the queue policy to give the above role permission to perform following actions

```
"Action": [
    "SQS:ReceiveMessage",
    "SQS:DeleteMessage",
    "SQS:GetQueueAttributes"
],
```

