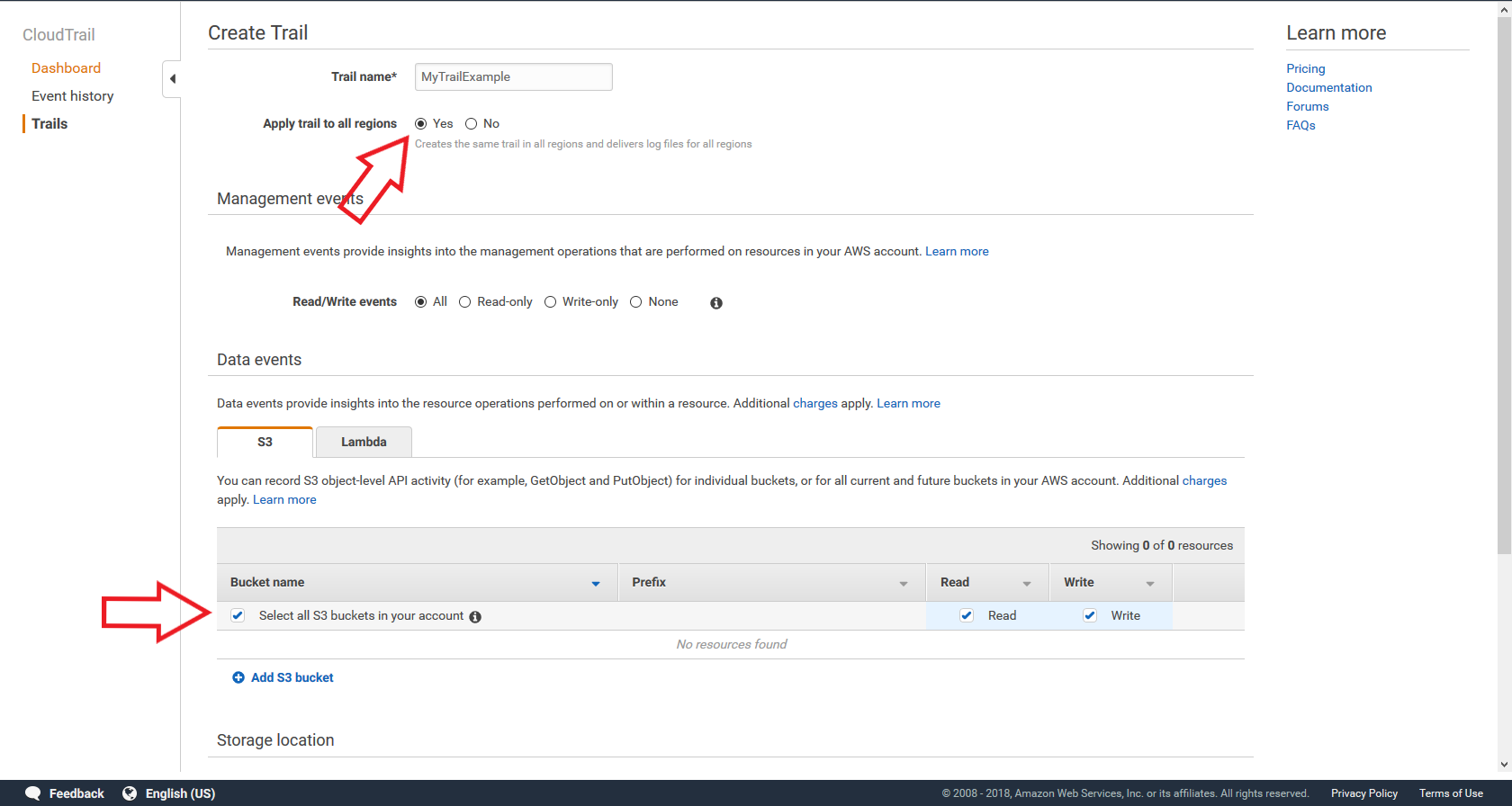
VPC Flow Logs Documentation

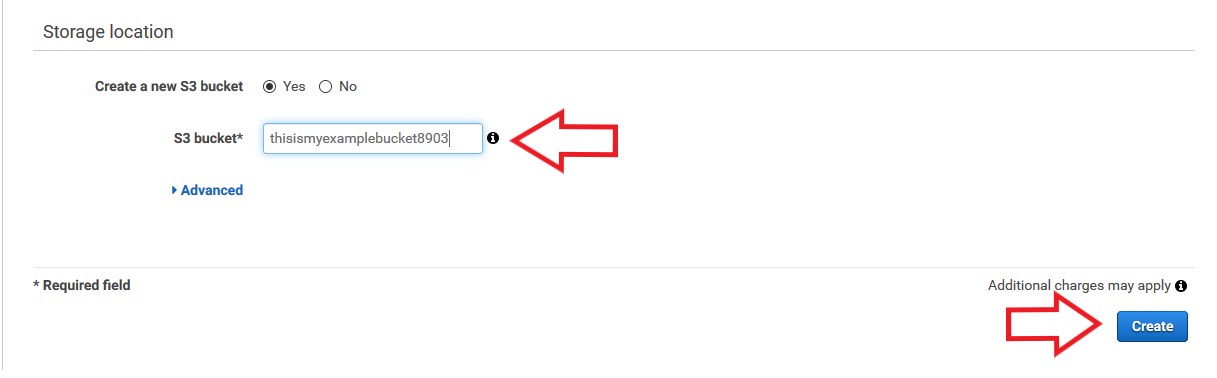
VPC Flow Logs capture IP traffic metadata in and out of your VPC. After a security incident happens looking at your VPC Flow Logs are often the biggest role when determining when an incident happened. Having them enabled is a best practice and does not cost much money at all. The point of this automation task is to enable VPC Flow Logs anytime someone create a new VPC. Maybe that VPC is being used for testing, or even that new VPC might be part of an EC2 has been hacked investigation. Best practices for determining how an instance might have been hacked is to take a snapshot of the instances, delete it, create a forensic VPC, launch a new instance from the snapshot, and then accessing that instance from an isolated desktop. This means best practice is to make a new VPC. If we setup this automation we will not need to remember to enable VPC Flow Logs which could come important during the investigation. Your company may also have a policy stating that VPC Flow Logs must be enabled at all times.

**Step 1 Setting Up a Trail:**

Sign into your AWS account and go to CloudTrail. Click on view trails and locate the blue create trail button. Name the trail whatever you want, make sure that apply trail to all regions is set to yes, and enable data events for S3 and Lambda.

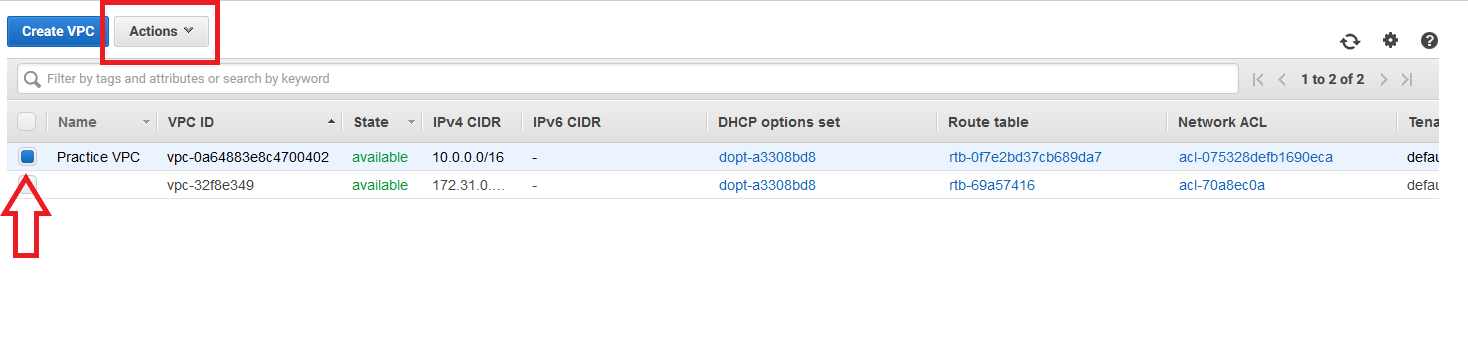


Next scroll down to storage location and either create a new S3 bucket or choose one already in your account. Then click create and your trail will be created.

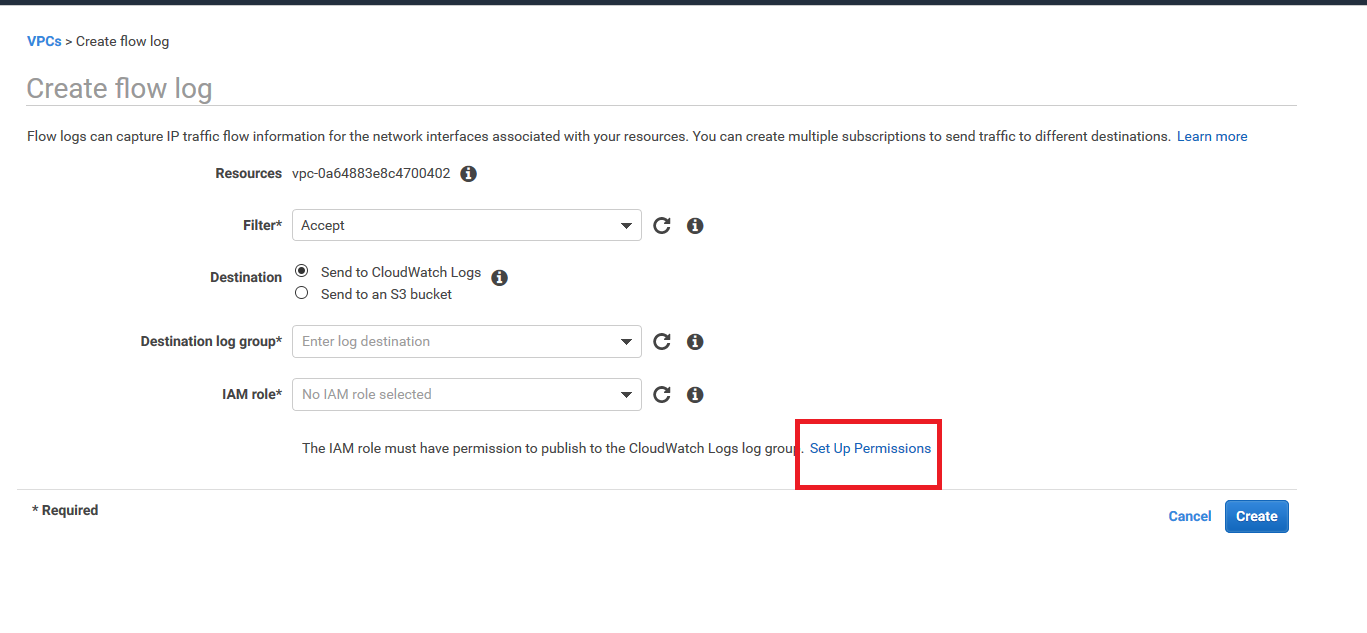


**Step 2 Create VPC Flow Log Role and Log Group:**

VPC Flow Logs need a role to log to CloudWatch Logs. That role needs to contain CreateLogGroup, CreateLogStream, DescribeLogGroups, DescribeLogStreams, and PutLogEvents in a role policy document. To create this role go to VPC’s and select a specific VPC. Click on actions and select create flow log.

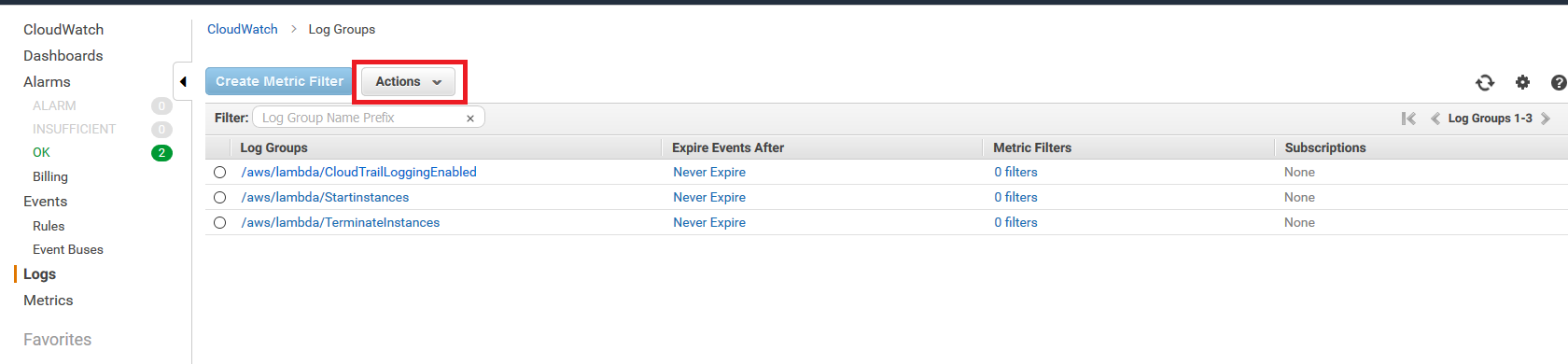


Once in the setting up flow logs page you will see a setup role permissions at the bottom. Click on that and it shall create an IAM role for VPC Flow Logs automatically for you. This is important as the Lambda function will need to reference that role and assign it to all newly create Flow Logs.

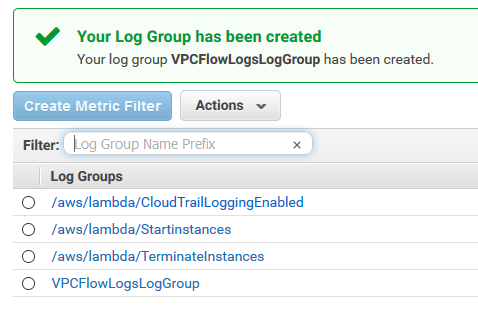


Click on set up permissions and just click allow.

Next we need to set up the destination log group that the Lambda function will reference. Go to CloudWatch Logs. Once in CloudWatch Logs select actions and click create new log group.

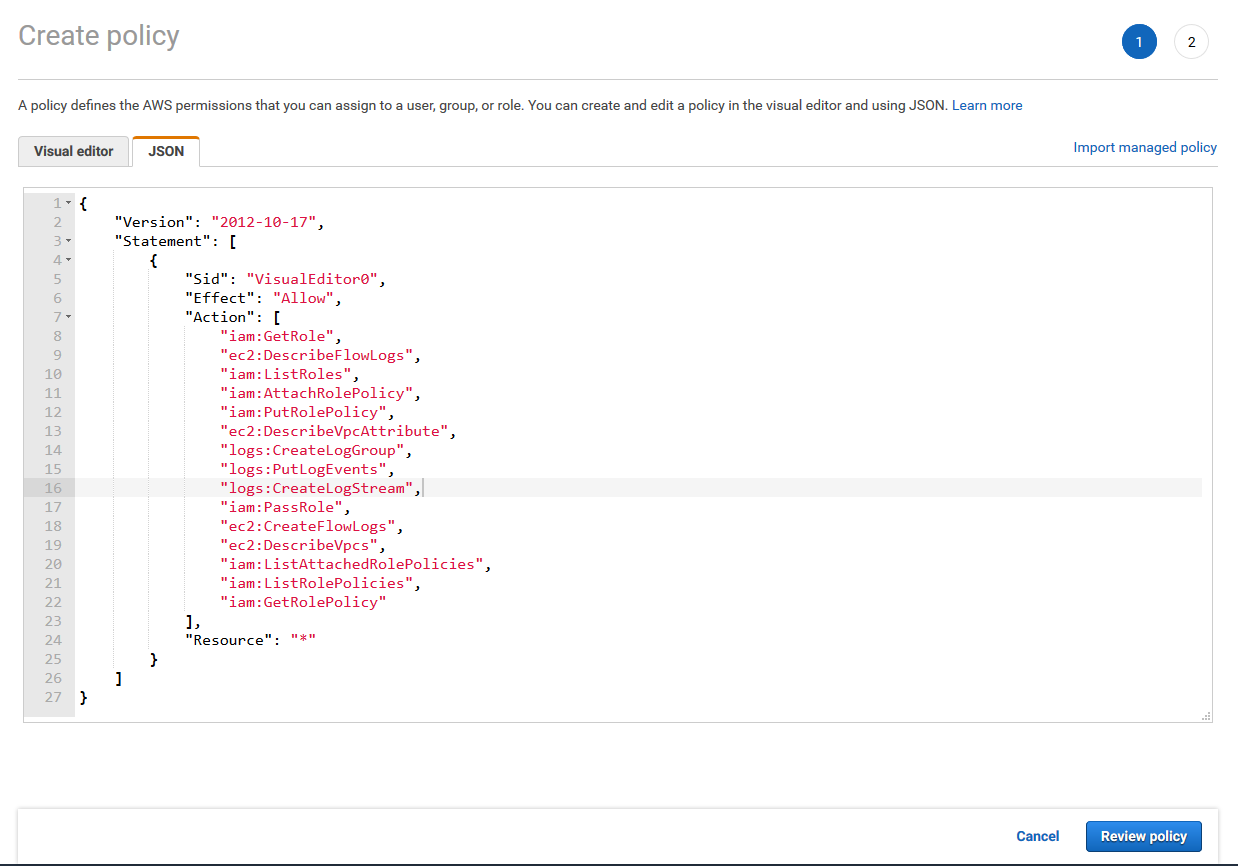


It will ask you to name your new log group and then click create.

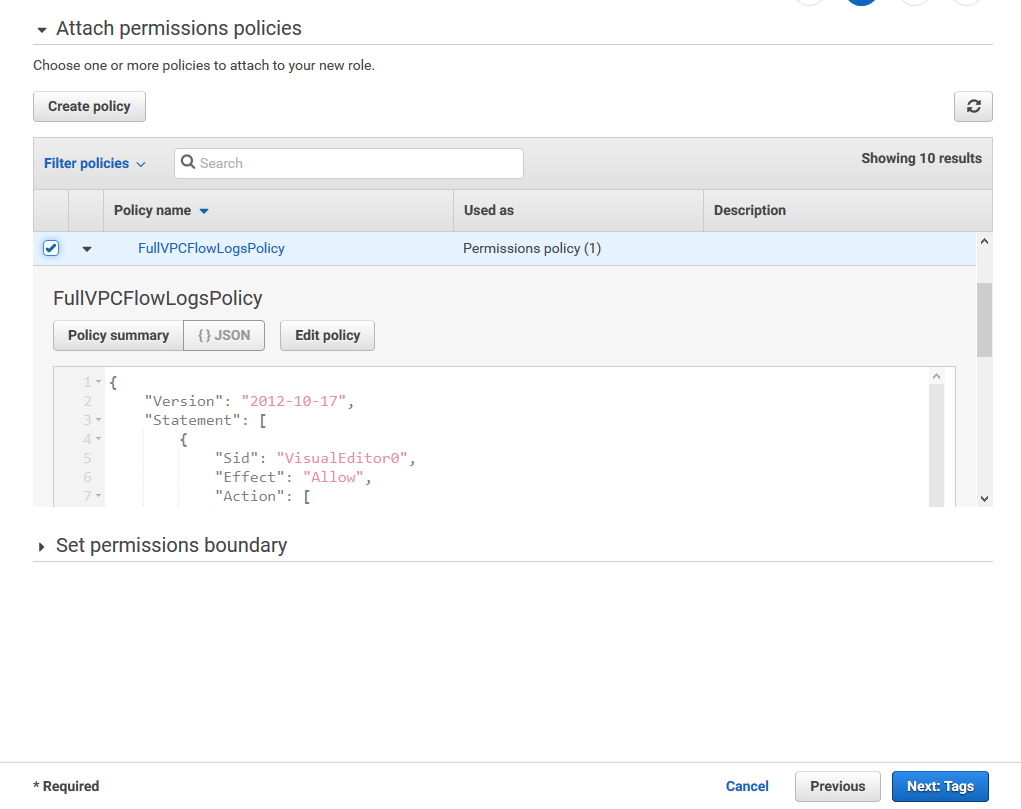


**Step 3 Create Role for Lambda Function:**

Go to IAM and select policies. You can either create 3 separate policies like I did, or you can go into my GitHub repository and locate the combined IAM policy needed for the Lambda function. It needs 3 parts, the ability to log to CloudWatch Logs, the ability to create VPC Flow Logs, and lastly the ability to pass the role into VPC Flow Logs. Go to create role, choose Lambda, and click next permissions. Click create policy and go to the JSON tab where you can copy and paste your own code. Locate my file with the code and copy and paste.



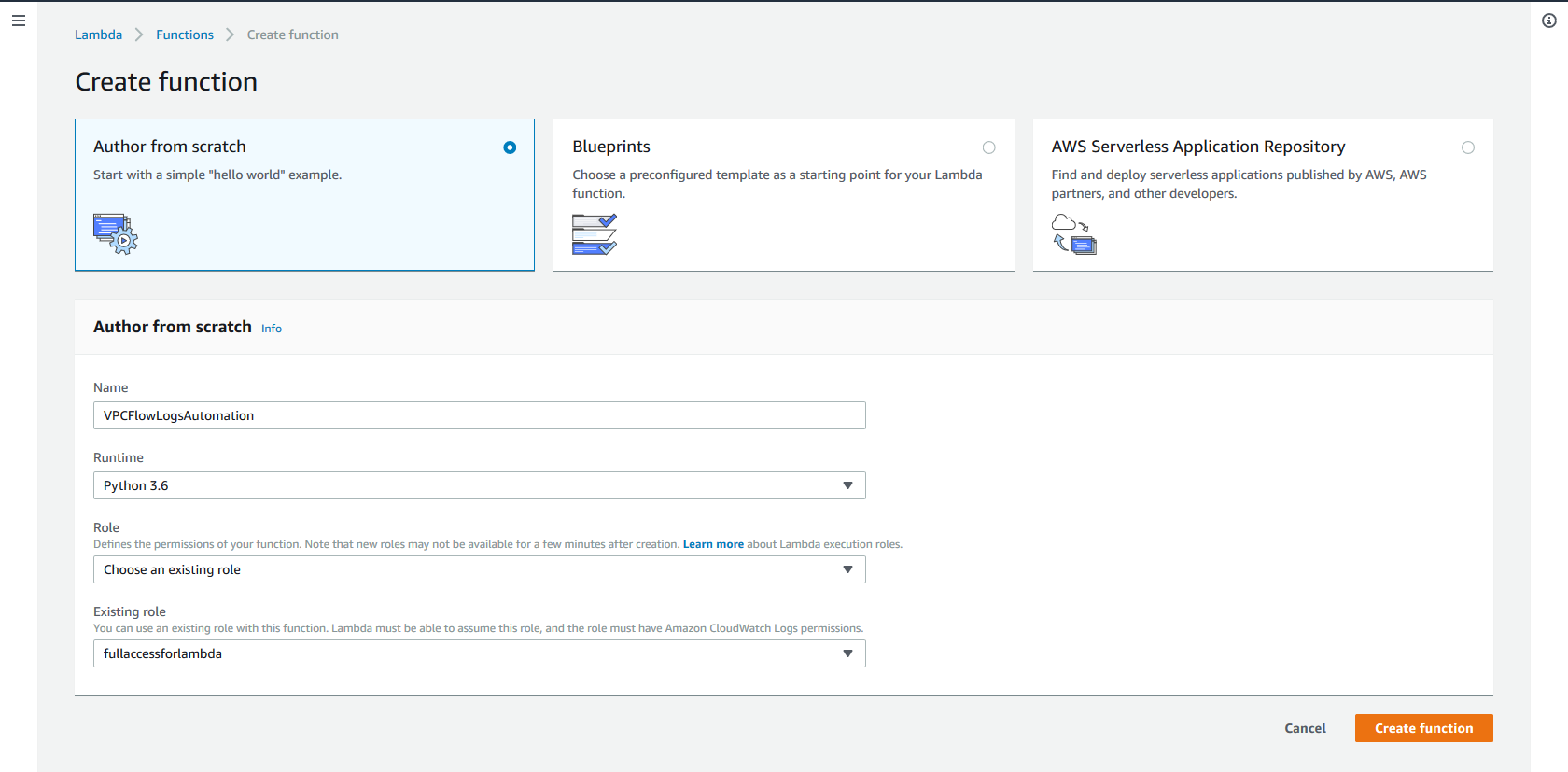
Click review policy and name it and then create the policy. After created locate that policy in the console and attach it to the Lambda role.



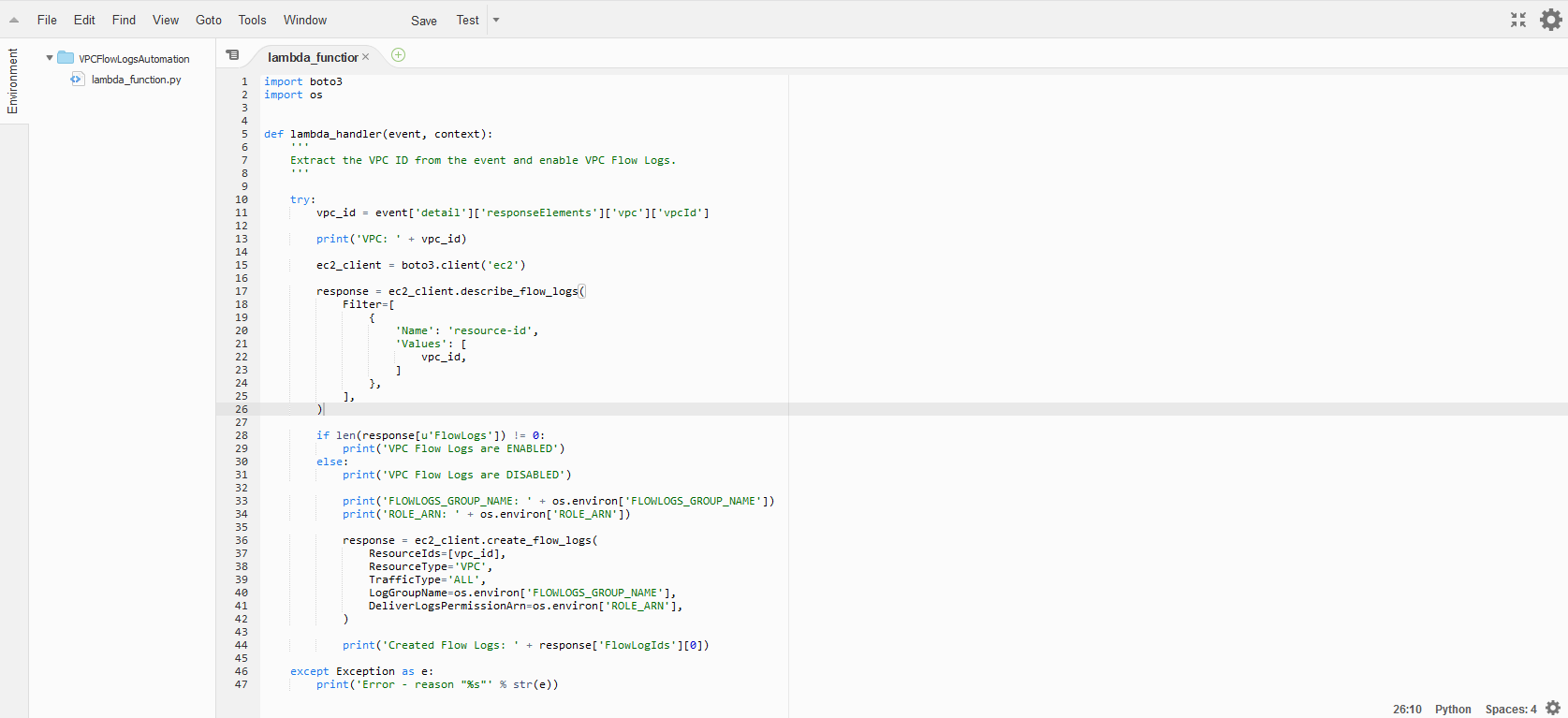
Go to next tags, next review, name the role, and then click create.

**Step 4 Create Lambda Function:**

Go to Lambda in the console and click create new function. Make sure to choose author from scratch, python 3.6, and a Lambda role that allows appropriate permissions. While making the original function I am just trying to get it to work so I chose a Role with full access to everything. I will be going back and granting that role least privilege in the near future.

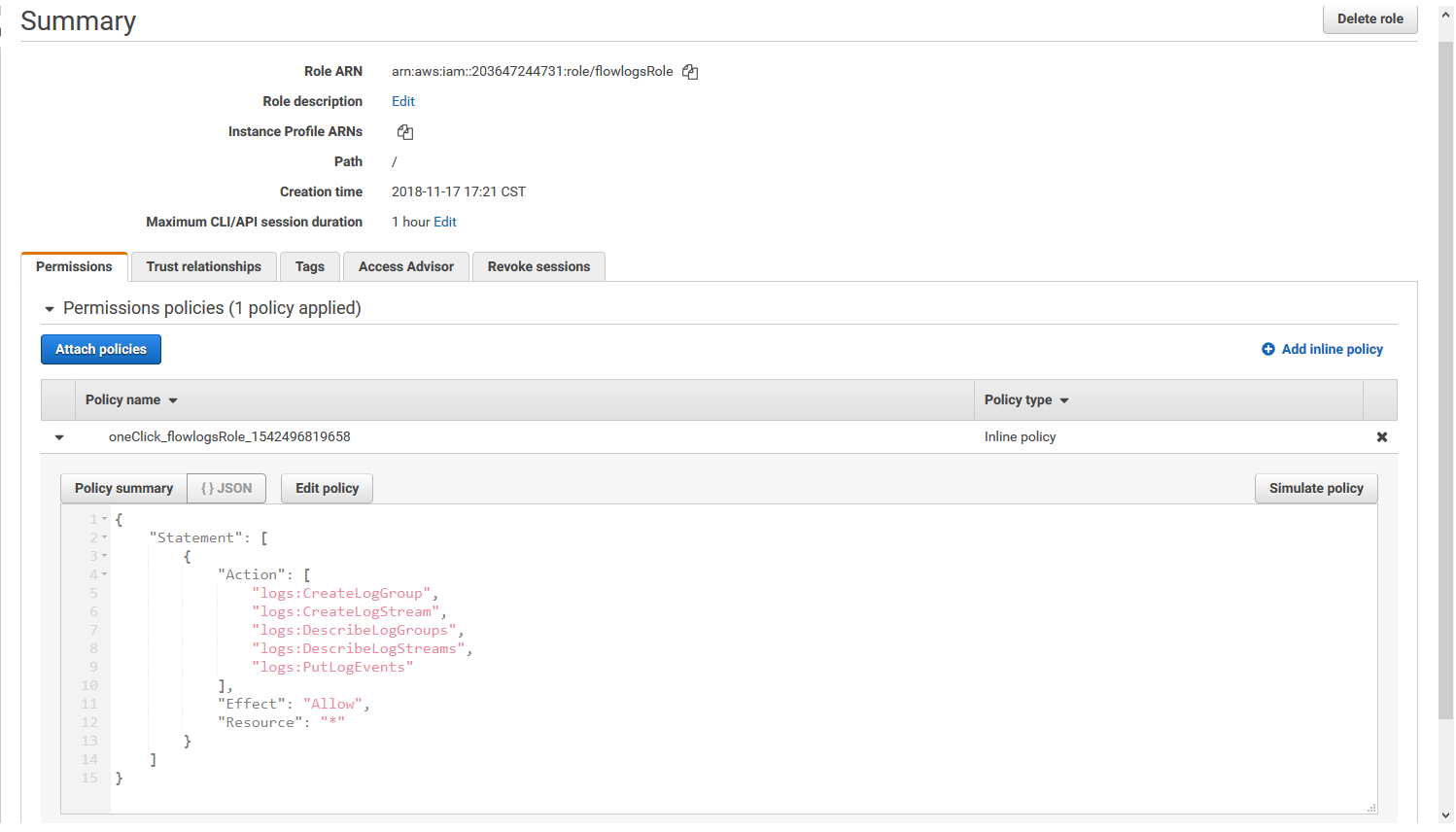


And click create function. Located in my GitHub repository is the code for this function. Copy and paste it into the box and make sure the last line is indented correctly because every time I copy and paste the final line gets indented wrongly.

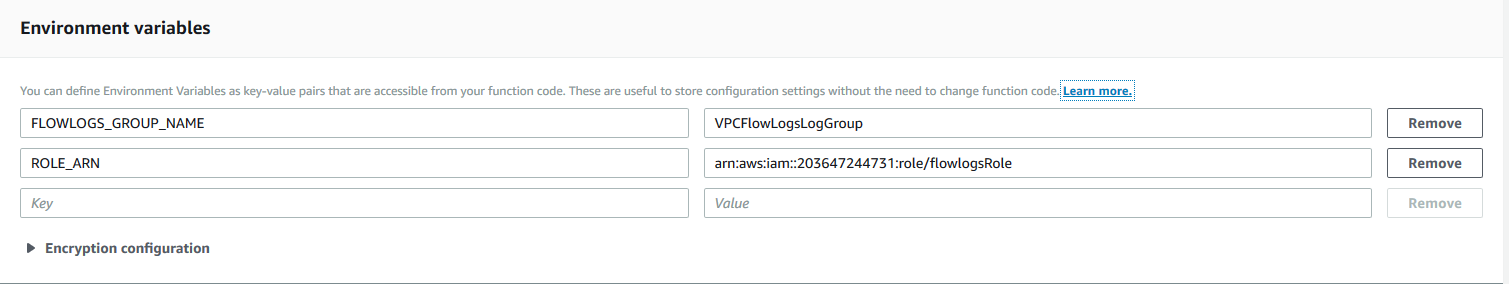


The function should be scripted like so. Notice how the final line is double indented, if this is not that case when you copy and paste from Git make sure to indent it manually. Now an important part of this Lambda function is environment variables. Here was use them to define the log group and role that the function should use while setting up the VPC Flow Logs. As shown below I have 2 variables one is stating the log group I made and the other is defining the Role ARN to use so that the VPC Flow Logs can be set up correctly.

Getting the role ARN is easy. Go back to IAM and locate roles. Locate the role you created for the VPC Flow Logs. That will bring you to a summery section of the role and you shall see the ARN at the top.



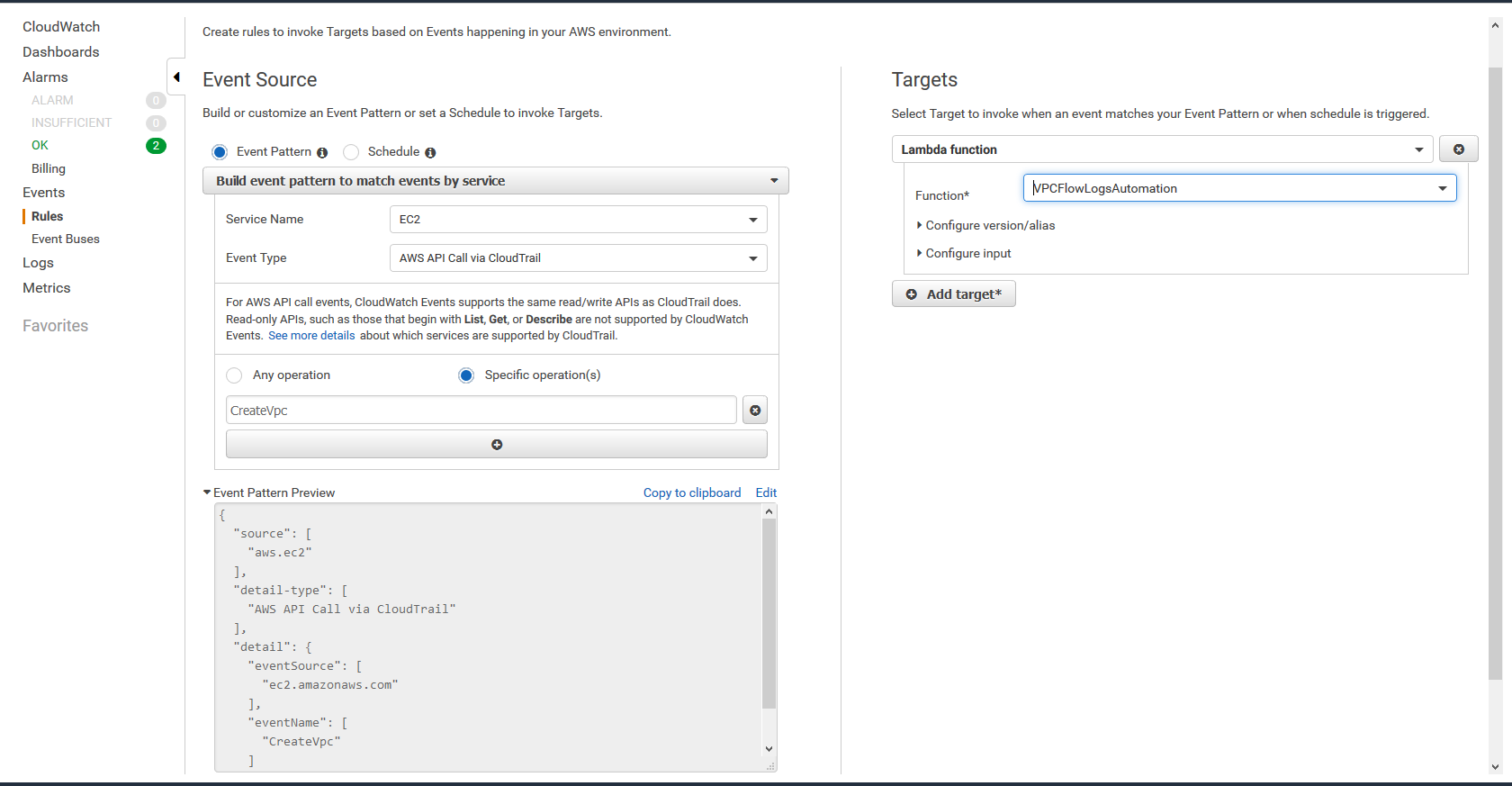
Keep in mind that for the environment variables make sure that the left side matches mine, and the right side matches the log group, and role ARN you created.



Make sure to use your own log group name and role ARN otherwise it will not work. Without defining these your function will not have the appropriate resources to create VPC Flow Logs thus causing them to fail.

**Step 5 Setting up the CloudWatch Event:**

Go to CloudWatch and locate the rules tab. Select create rule. This is based on an event pattern so make sure that is selected. For service name locate EC2 and for event type make sure it is AWS API Call via CloudTrail. We want this to trigger on the specific operation of a VPC creating so select specific operations. Make sure in that the event triggers based on the CreateVpc API. The caps are important so double check that. Next add a target and select the Lambda function you created earlier.



Select configure details, name the rule, and give it a description. Then click create rule.

**Step 6 Testing:**

Test the rule out by creating a new VPC. This is a near real time event so you need to wait at the most 15 minutes as the event is based off of CloudTrail.