

Introduction

This activity provides you with the opportunity to get hands-on experience solving a real-world scenario where we want to automate the creation of VPC Flow Logs whenever we create a new VPC.

We'll accomplish this with a CloudWatch rule and a Lambda function.

Log in to the AWS Console using the credentials provided on the hands-on lab page.

Solution

Navigate to the **CloudTrail** service from the AWS Console.

Click on **Trails**.

Click on the name of the Trail that was created for you. Verify that logging is turned on in the top-right of this window. We can also verify where the logs are being stored by scrolling down to the *CloudWatch Logs* section and noting the *Log Group* value.

To view these logs, open a new tab for the **CloudWatch** service.

Click **Logs**. Here we can see the CloudTrail and VPC Flow Logs.

We need to create a rule. Click on **Rules** in the left sidebar.

1. Click **Create rule**
   * **Service Name**: EC2
   * **Event Type**: AWS API Call via CloudTrail
2. Select **Specific operation(s)**
3. In the field directly below that, provide "CreateVpc"
4. In the window on the right, click **Add target**
   * Click into the *Function* field and select the Lambda function
5. Click **Configure details**
   * **Name**: createvpc
6. Click **Create rule**

Let's take a look at the Lambda function. Open the **Lambda** service.

Click on the function name that is provided for you.

From this page, note the settings and code in each section.

Now that we know exactly what is going on under the hood, let's see it in action. We want to create a new VPC which will trigger our workflow to enable Flow Logs.

Open the **VPC** service. Click **Create VPC**.

1. Click **Select**
2. **Name**: myvpc
3. Click **Create VPC**
4. Click **OK**

After a few minutes, refresh the page and then select the checkbox next to your new VPC name in the list. Click the **Flow Logs**tab. We should now see that Flow Logs are enabled and a CloudWatch Log Group is listed in this tab.