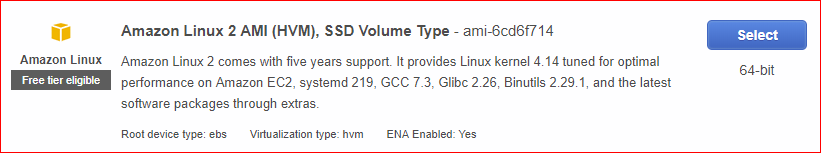
**ACIT 3640 – VPC Flow Logs**

This is the [AWS documentation for VCP Flow Logs](https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/flow-logs.html).

**Part 1**: Publishing Flow Logs to Amazon S3

We are going to use an S3 bucket to store the logs. Start by creating an Amazon Linux 2 AMI instance. Make sure you are in Oregon zone.



Install Apache on the instance as part of the bootstrap process (in step3, Advanced Details)

#!/bin/bash

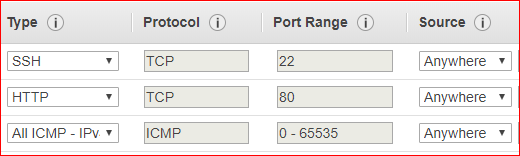
sudo yum update –y

sudo yum install -y httpd

sudo service httpd start

sudo chkconfig httpd on

Your security group should open inbound ports 22, 80 and ICMP-IPv4.



Review and launch your instance.

Create an S3 bucket. Remember: S3 buckets are globally unique. You may need to add your A00 number to your bucket name.



Accept all the defaults and create s3 bucket.

Important: After you create the S3 bucket, log out of your AWS account and log back in. If you don’t do this, you will not be able to create the Network Interface for the flow log.

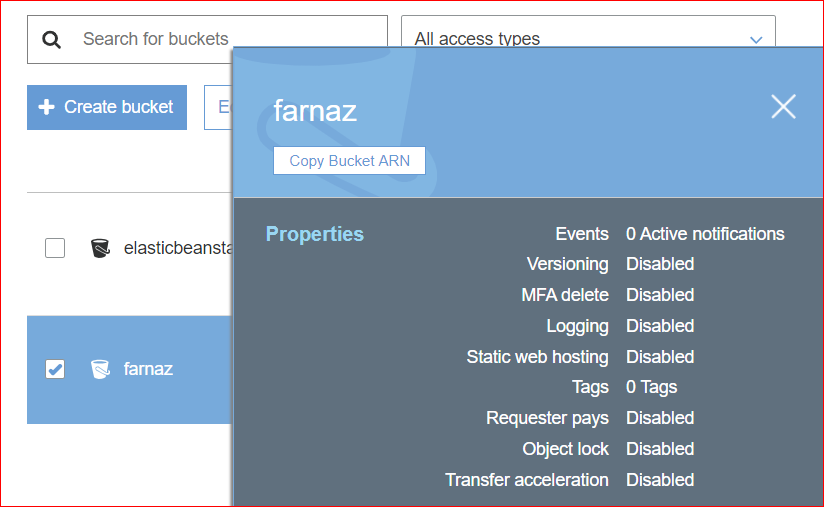
In EC2 navigation pane, choose Network Interface.

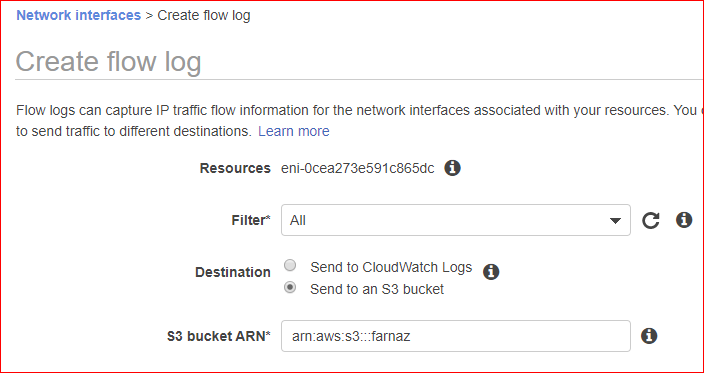
Select the Network Interface that the Instance ID matches the Instance ID of the Linux instance. Choose action, create flow log.

For Filter, specify the type of IP traffic data to log. Choose All.

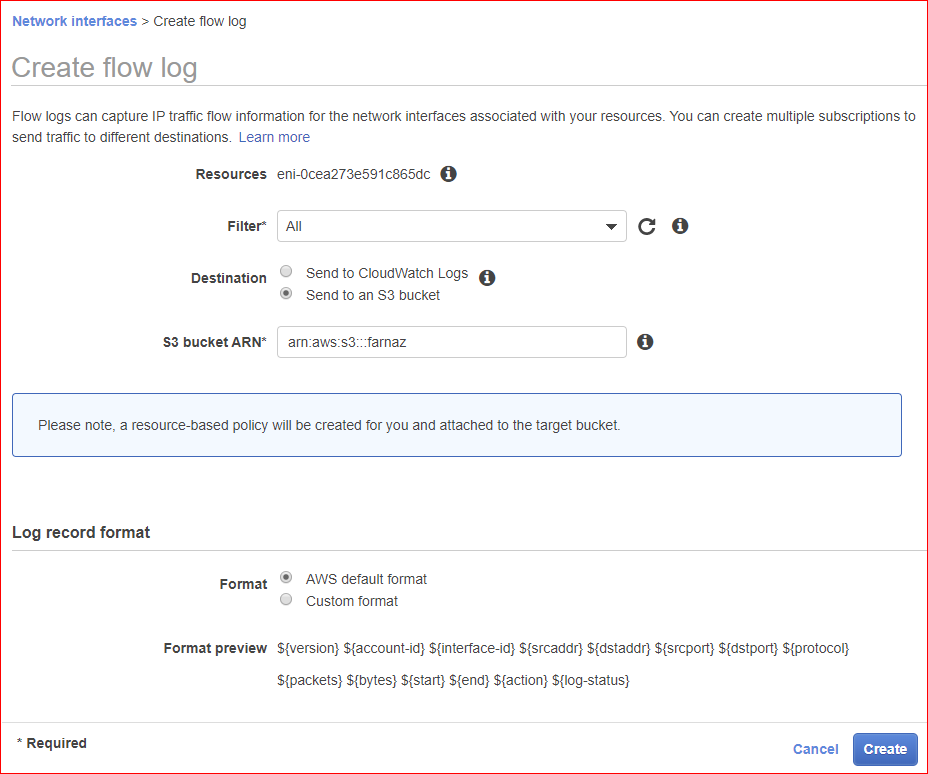
For Destination, choose Send to an Amazon S3 bucket.

Note: When creating the flow log, you will enter the S3 Bucket ARN, not the name of the bucket. Click the “Copy Bucket ARN” button.





For Format, specify the format for the flow log record. To use the default flow log record format, choose AWS default format, and click Create.

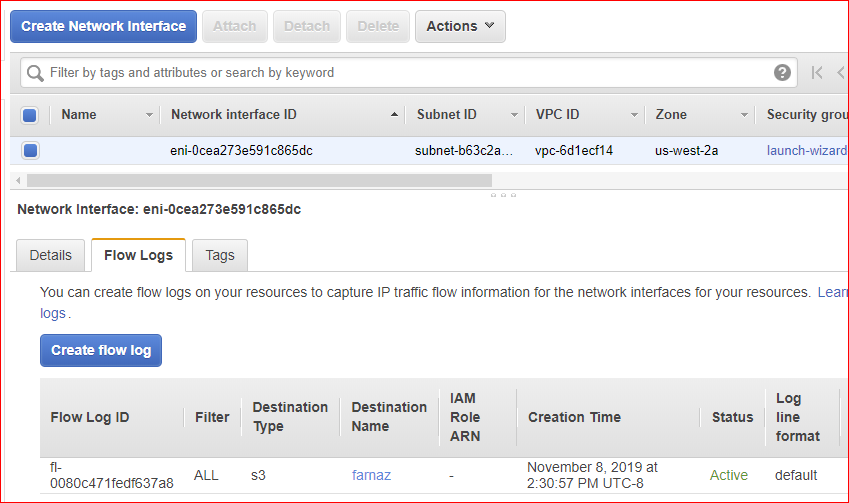


Go to S3 bucket. Click on the Permissions tab of your S3 bucket. Then click on the Bucket Policy. This is what my Bucket Policy looks like:

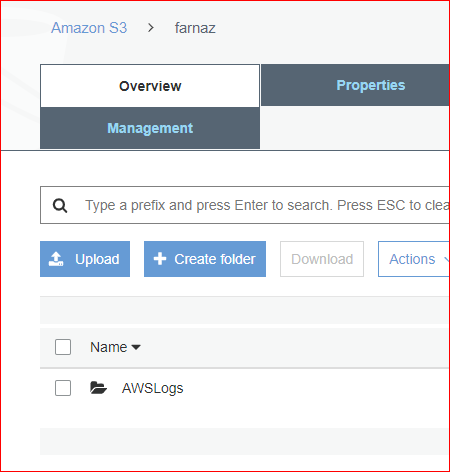


Next, we have to generate activity on the instance. Based on the inbound ports that are open, how do we do that? You must generate activity to the instance in order for logs to be created in your S3 bucket!

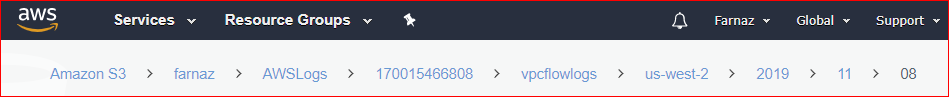
Once you have generated data to the instance, you can access the flow logs from the Network Interface by clicking on the Destination Name hyperlink:

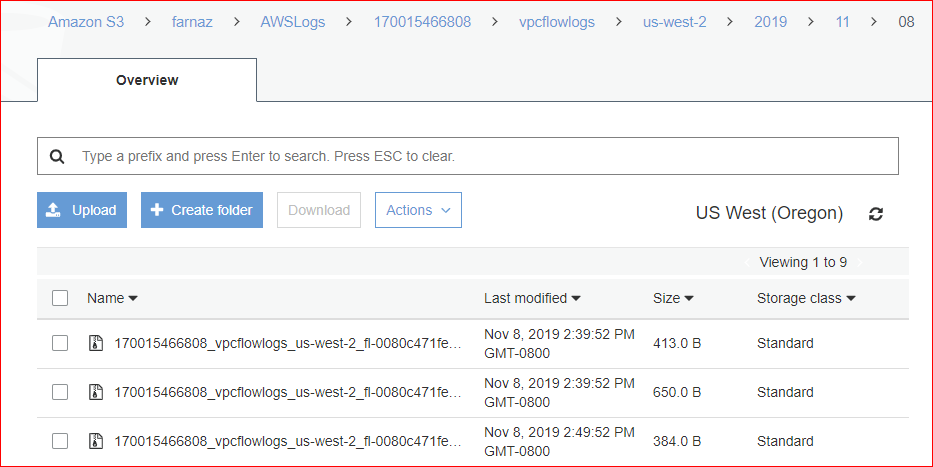


Your S3 bucket should show an AWSLogs folder.



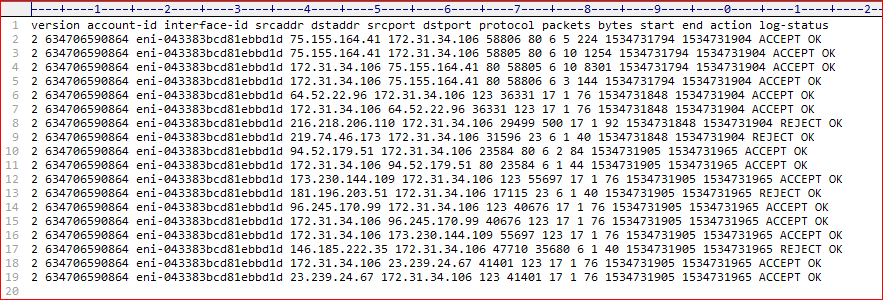
Drill down through the folders. Notice that the final three folders are year, month and day. Note: These folders will only appear after you have generated traffic to your instance! It takes 5 – 10 minutes for the logs to appear. Have patience! Don’t ask your instructor for help until you have waited at least 15 minutes.



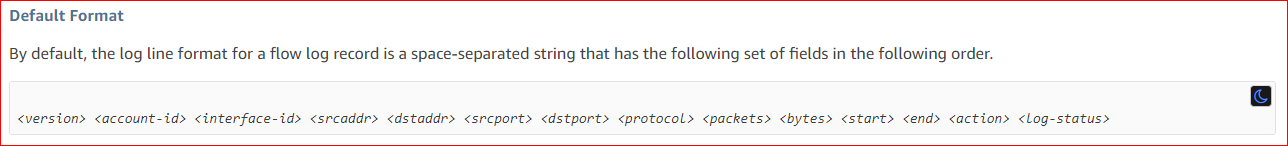


In the day folder, are raw data logs. Notice they are compressed files. They have a file extension of “gz.” This is a Linux zip file.

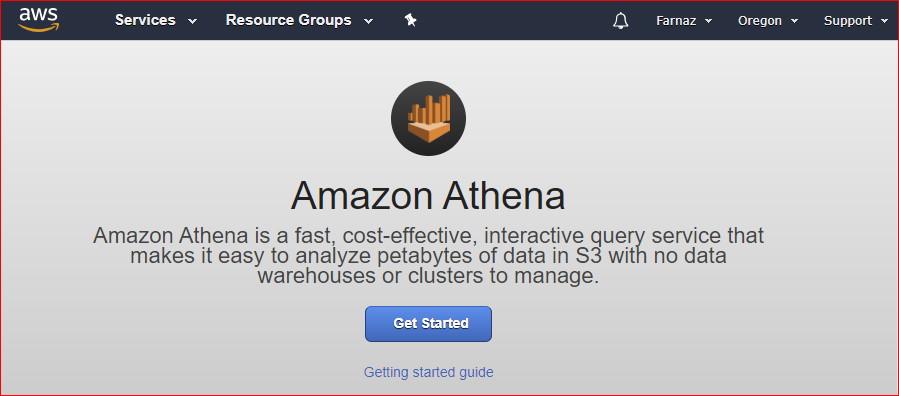
Download one of the raw log files. Because it is a compressed file, you must unzip (decompress) the file. Open the uncompressed file. You should see data that looks like this:



This should match the [online documentation.](https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html#flow-log-records) See the section Flow Log Records.



Next, we want to analyze the flow logs using Athena. What is [Athena](https://aws.amazon.com/athena/)? Find Athena through the AWS Services console.



Copy and paste the following DDL statement into text editor and from text editor to the Athena console.

CREATE EXTERNAL TABLE IF NOT EXISTS vpc\_flow\_logs (

version int,

account string,

interfaceid string,

sourceaddress string,

destinationaddress string,

sourceport int,

destinationport int,

protocol int,

numpackets int,

numbytes bigint,

starttime int,

endtime int,

action string,

logstatus string

)

PARTITIONED BY (dt string)

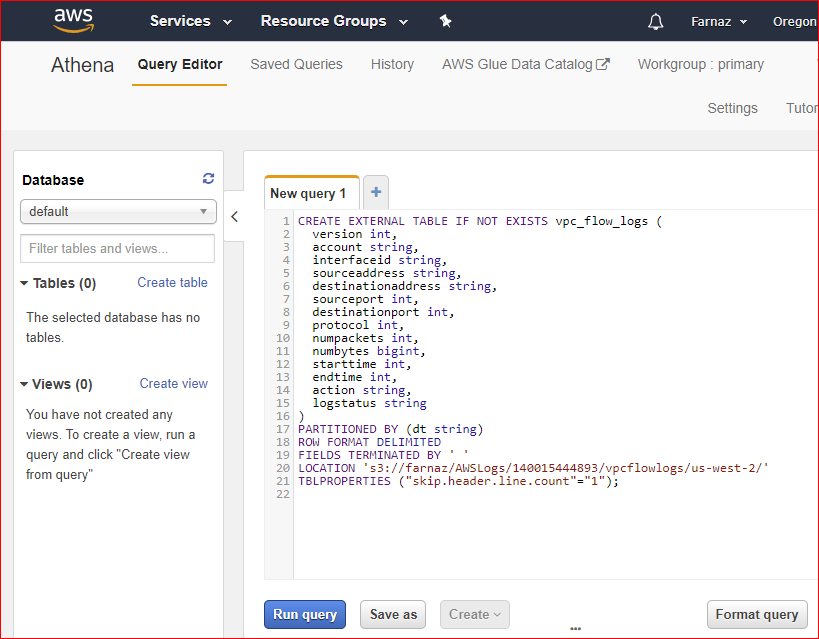
ROW FORMAT DELIMITED

FIELDS TERMINATED BY ' '

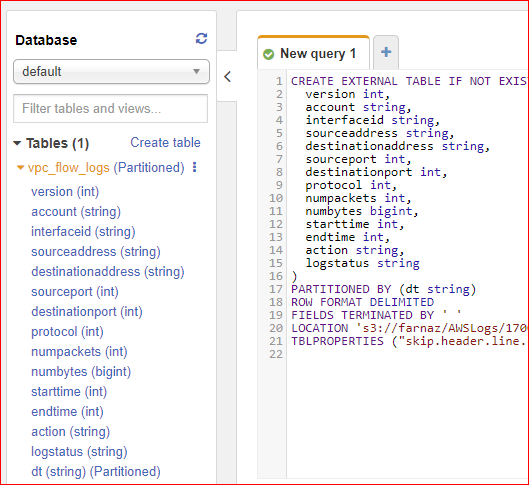
LOCATION 's3://your\_log\_bucket/AWSLogs/subscribe\_account\_id/vpcflowlogs/region\_code/'

TBLPROPERTIES ("skip.header.line.count"="1");

You need to enter your bucket name, account id and region. This is a screen shot of my Athena query. Look at the second last line where I specify my S3 bucket location.



After you run this query, you should see your table on the left. Athena registers the vpc\_flow\_logs table making the data in it ready for you to issue queries.



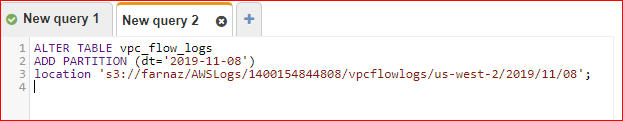
Create partitions to be able to read the data. Following query creates a single partition for a specified date.

ALTER TABLE vpc\_flow\_logs

ADD PARTITION (dt='YYYY-MM-dd')

location 's3://your\_log\_bucket/AWSLogs/account\_id/vpcflowlogs/region\_code/YYYY/MM/dd';

Make sure you enter the correct year, month and day from your S3 bucket subfolders.



The following query lists all of the TCP connections and uses the newly created date partition column, dt, to extract from it the day of the week for which these events occurred. This query uses Date and Time Functions and Operators. It converts values in the dt String column to timestamp with the date function from\_iso8601\_timestamp(string), and extracts the day of the week from timestamp with day\_of\_week.

SELECT day\_of\_week(from\_iso8601\_timestamp(dt)) AS

day,

dt,

interfaceid,

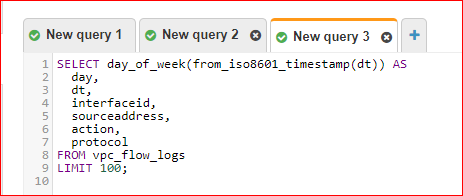
sourceaddress,

action,

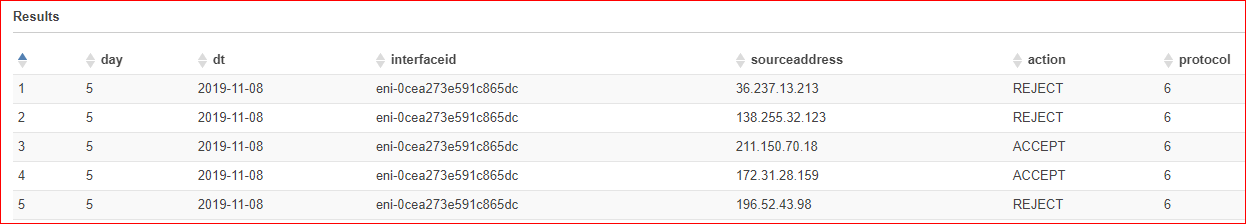
protocol

FROM vpc\_flow\_logs

LIMIT 100;



This is the data I got when I ran the query. You should have similar results:



Note: The protocol column is *not* the same as *ports.* Protocol “1” is an ICMP protocol and “6” is a TCP protocol. (See [here.](https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml))

Change your query to display the destination port for HTTP. (Hint: you may use WHERE destinationport = 80)

Lab Deliverable

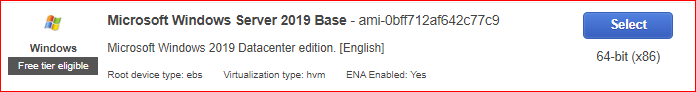
Take a screenshots of your query results, as shown above, and show it to your instructor when you finished all parts of the labs. Screen shot should include your account name on top of the page.

**Part 2:** publish flow logs to Cloud Watch logs

In this part of the lab, you will create a new instance and [publish flow logs to CloudWatch logs](https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/flow-logs-cwl.html).

On the web page, do the section labelled “Creating a Flow Logs Role.” I called my role “Flow-Logs-Role.”

1. Launch a Microsoft Windows Server 2019 Base instance.

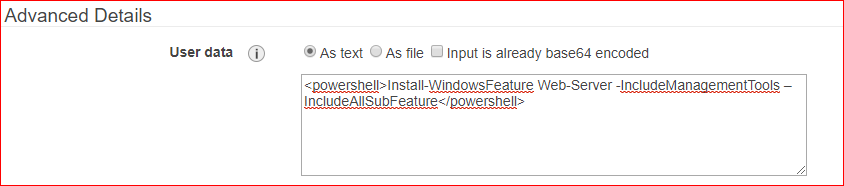


1. Bootstrap IIS, the Windows web server:

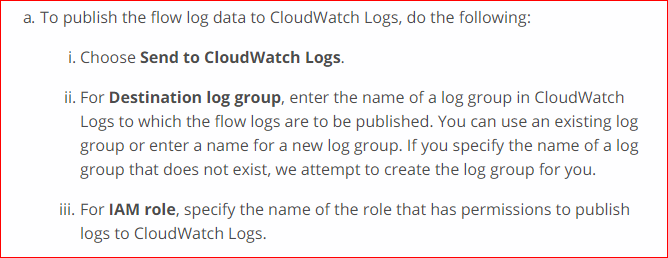
<powershell>Install-WindowsFeature Web-Server -IncludeManagementTools

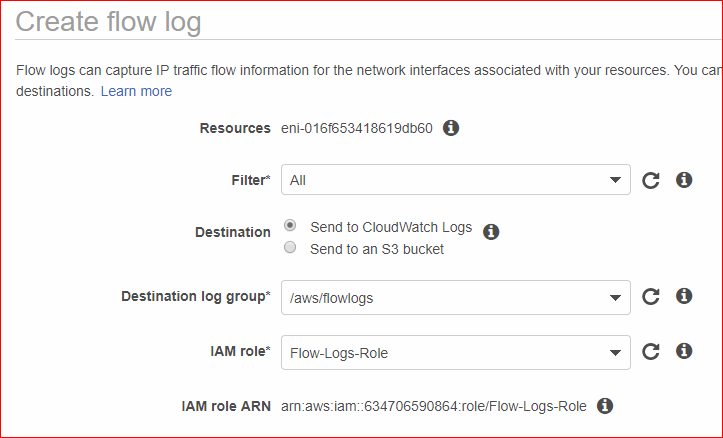
–IncludeAllSubFeature</powershell>

Note: You may want to *type this command in by hand*. There is a single hyphen in front both IncludeManagementToos and IncludeAllSubFeature. There is a single space between those two parameters.

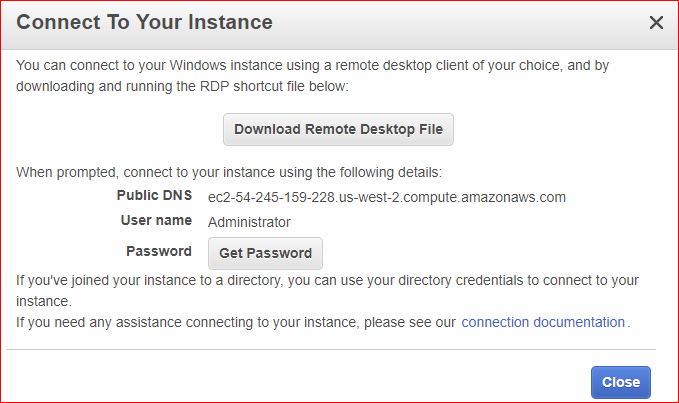


1. Open the following inbound ports: 3389 (RDP) and 80 source: Anywhere. Use your key pair and launch the instance. Name it as “Windows Server”.
2. Create a flow log and attach it to the Windows instance: In EC2 navigation pane, choose Network Interface. Select the Network Interface that the Instance ID matches the Instance ID of the windows instance. Choose action, create flow log.

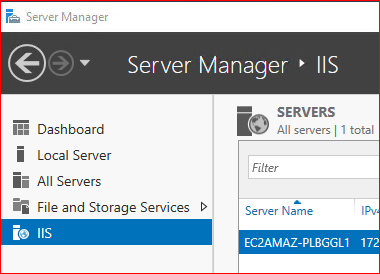




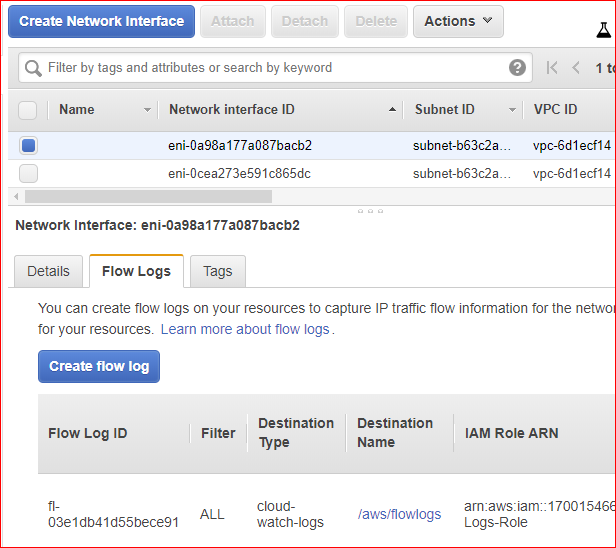
1. Let’s start by RDP into the instance.
2. Get the Windows password. This may take a few minutes before you can get it.



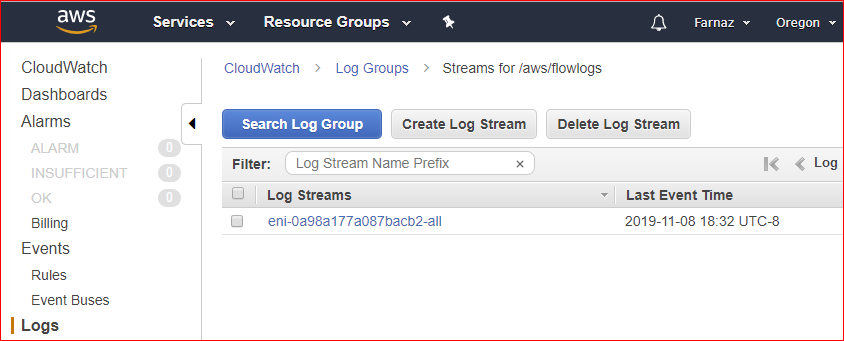
1. Verify that IIS is installed. If not, you will have to install it manually.



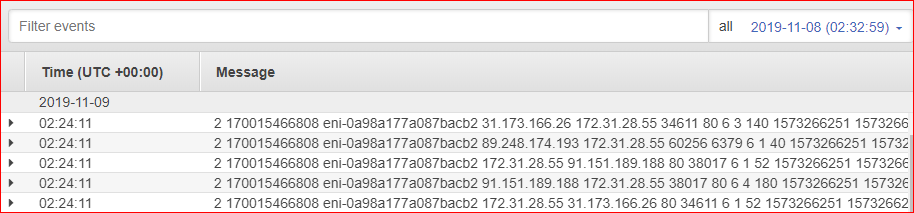
1. Generate traffic to this instance. Do it the same way you did it for the Linux instance. Wait for 2-3 minutes.
2. Check the CloudWatch logs. Click on the Destination Name link under Network Interfaces, Flow Logs.



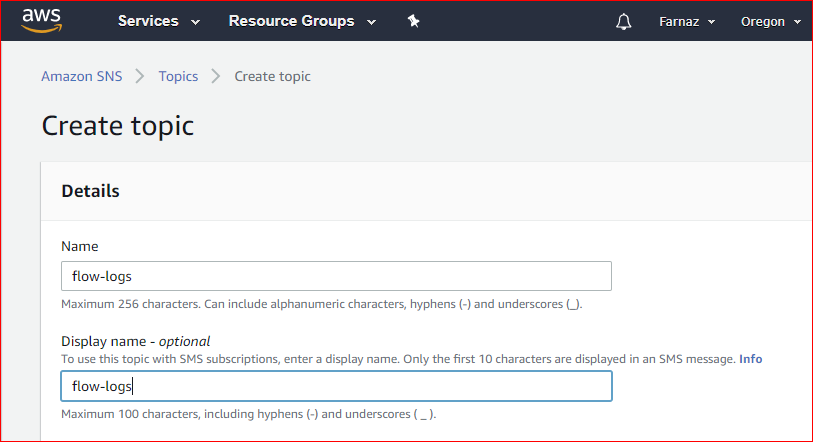
1. You should see some CloudWatch logs.



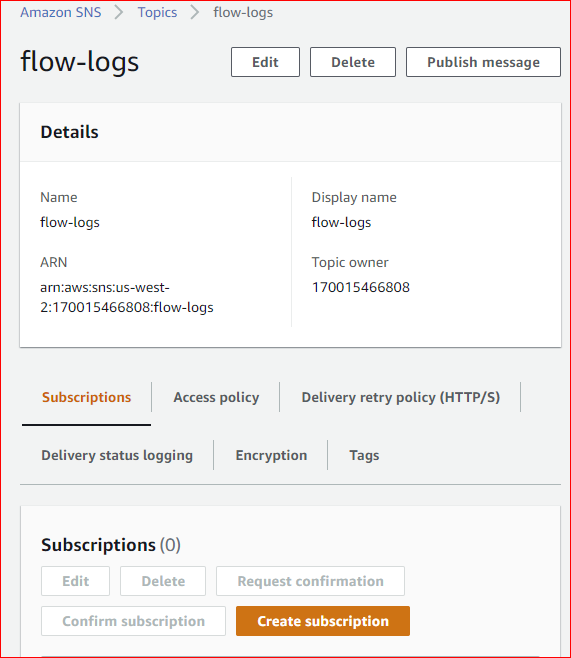
1. Click on the Log Streams. Examine the source IP addresses and TCP protocols.



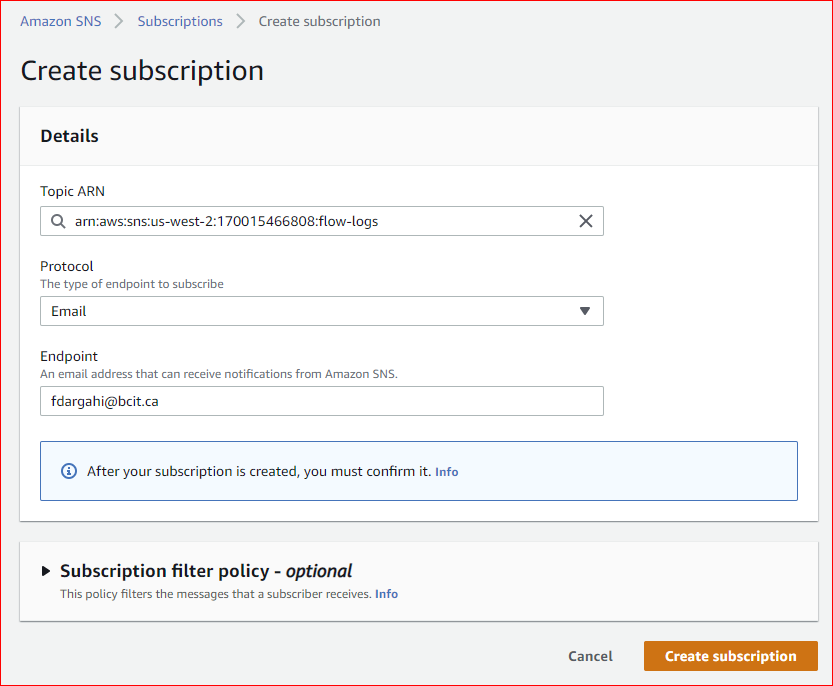
1. Before you create a CloudWatch Alarm, create an SNS topic.



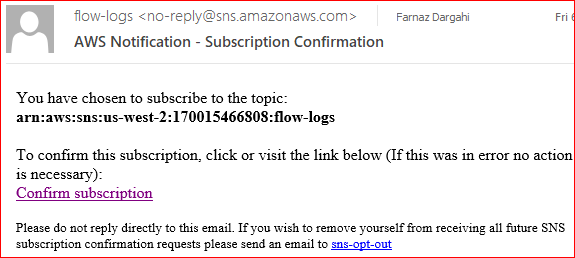
1. After creating topic, choose your topic and click create subscribe to subscribe to your topic.



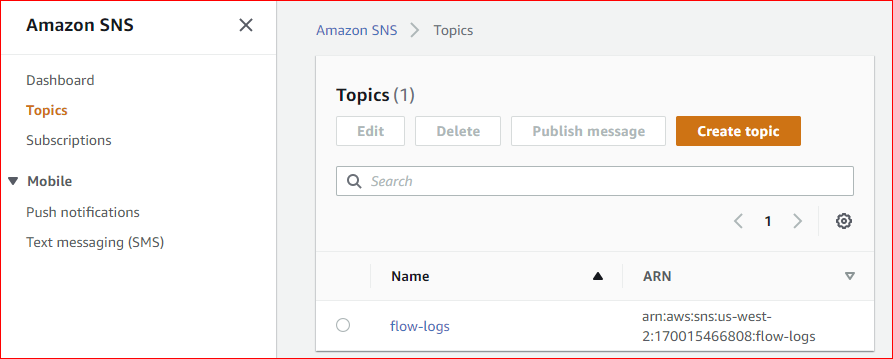
1. Enter your email address and create subscription.



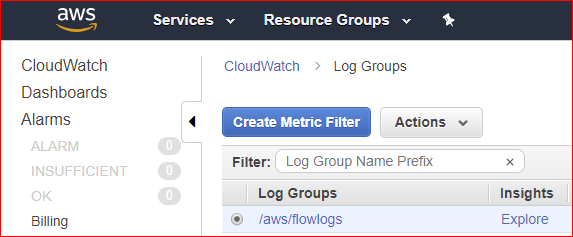
1. Go to your email and confirm the subscription.



1. Copy the ARN for the SNS topic into your clipboard. You will enter the ARN when you set up the alarm.

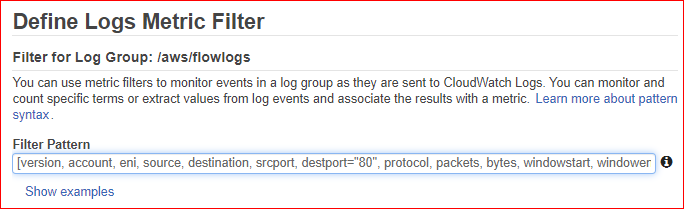


1. Now we want to create an alarm that alerts you if there have been one or more attempts to connect to your instance over TCP port 80 (HTTP) within a 5 minutes time period. First, you must create a metric filter that matches the pattern of the traffic for which to create the alarm. Then, you can create an alarm for the metric filter.
2. Go to cloud watch page. In the navigation pane, choose Logs. Select your log group and click on Create Metric Filter.

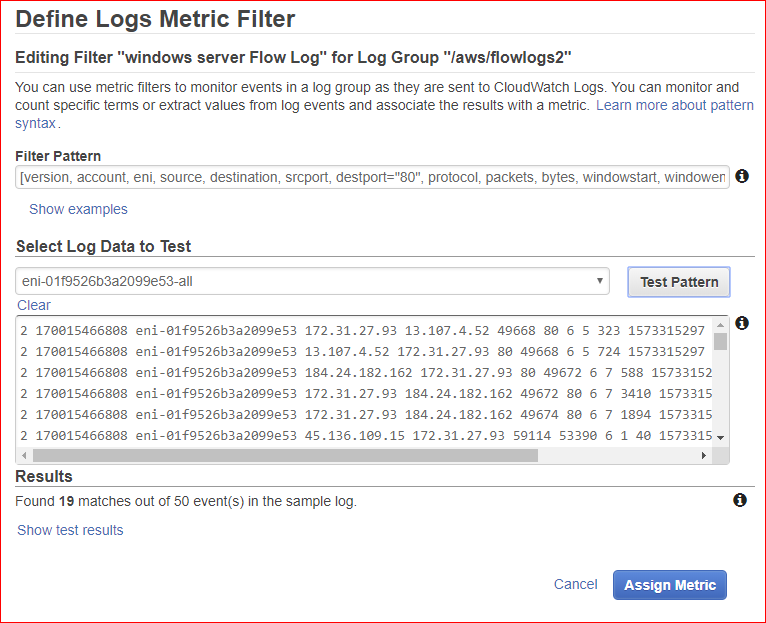


1. For the Filter Pattern, enter the following:

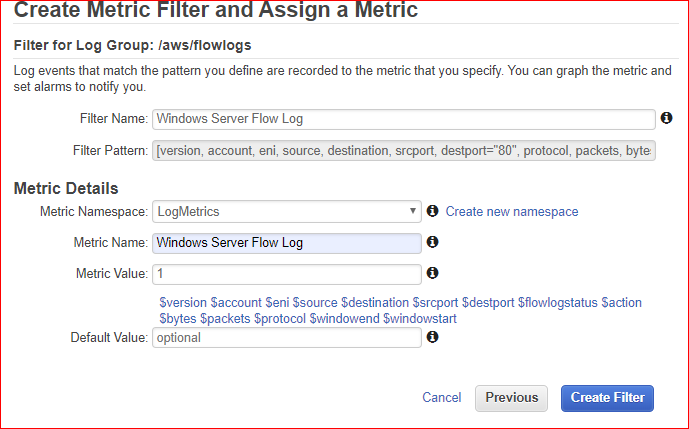
[version, account, eni, source, destination, srcport, destport="80", protocol, packets, bytes, windowstart, windowend, action, flowlogstatus]



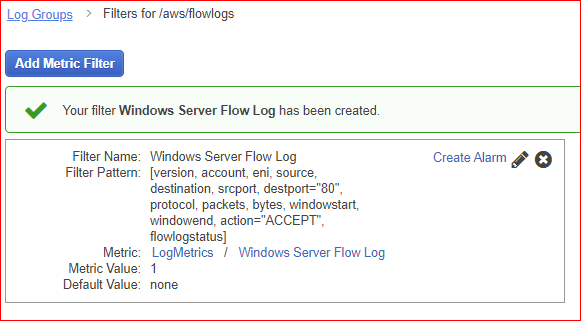
1. You can test the pattern. If you have generated HTTP traffic to the web page, you should see some results. If not, generate traffic to the web page. When you click Test Pattern, you should see some matches. I have 19 matches. Do *not* click the blue Clear link.



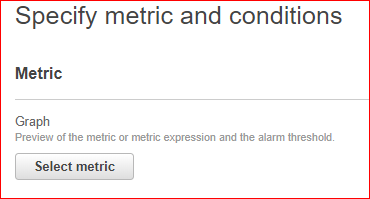
1. Click on Assign Metric.
2. Provide a metric namespace and name, and ensure that the metric value is set to 1. When you're done, choose Create Filter.



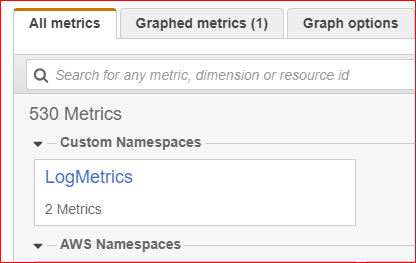
1. When you get to this screen, in the navigation pane, choose Alarms, Create Alarm.

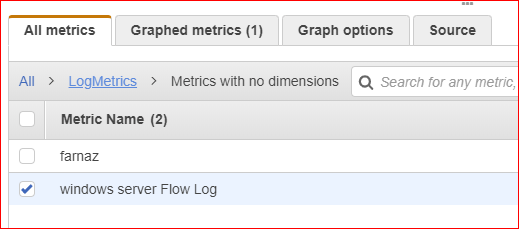


1. From the “Specify metric and conditions” screen, click on “Select metric.”

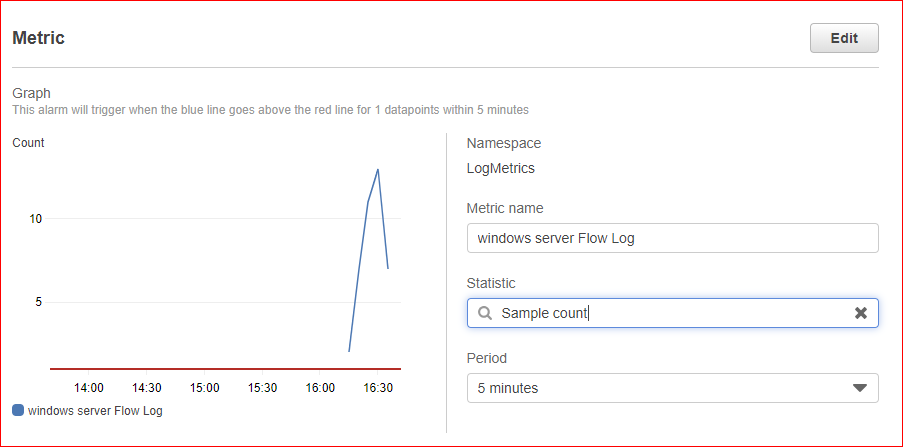


1. Under “All metrics,” you should see a custom namespace called “LogMetrics.” It can take up to 10 minutes for Custom Namespace to display in the console. Select the metric you created above. (I have two. You may only have one.)

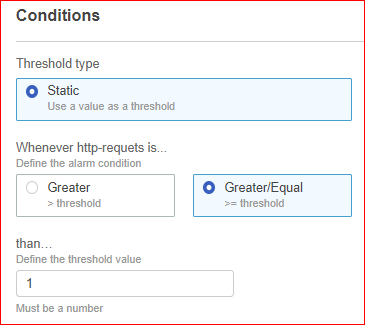




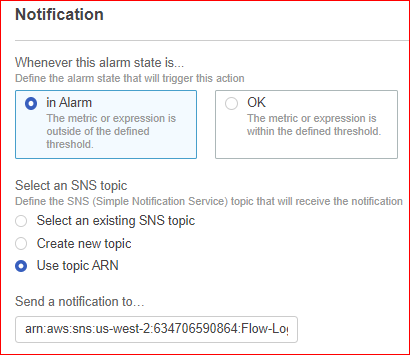
1. Set Statistic to “Sample count” and Period to “5 minutes.”

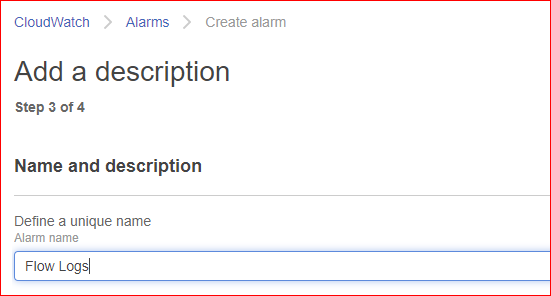


1. Select Static, Greater/Equal and enter a value of “1” in the “Define the threshold value” field.

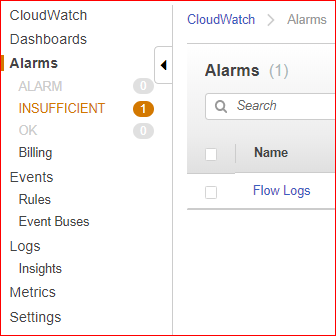


1. Select “In Alarm” and enter the ARN for the SNS topic in the “Send a notification to…” field

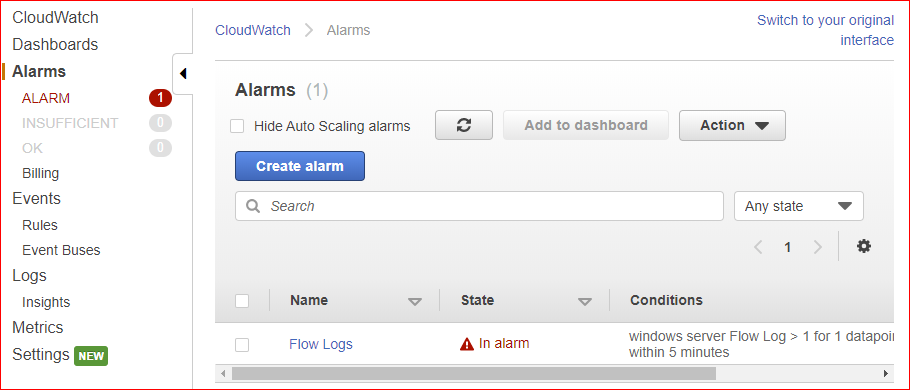


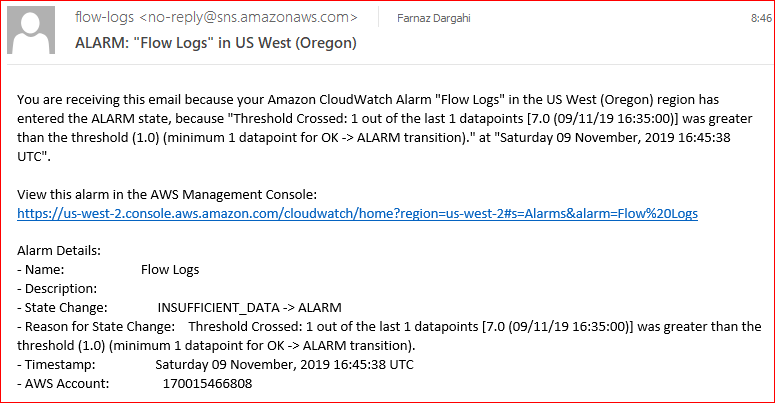


1. Click Create alarm.
2. You should see this screen with the orange INSUFFICENT showing.



1. Generate traffic to your web site. Wait about 5 minutes. An ALARM should be triggered and you should receive an alarm email.





Lab Deliverable

Show your instructor the email you received.

Clean Up

1. Delete your Athena table.
2. Delete your S3 bucket.
3. Terminate your EC2 instances.
4. Delete your Alarm in cloud watch.
5. What happened to the Network Interface?