VPC Flow Logs

VPC flow logs is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC. Flow log data is stored using Amazon CloudWatch Logs. After you've created a flow log, you can view and retrieve its data in Amazon CloudWatch Logs.

So it is a way of storing all the network traffic that's going on in your VPC.

***To complete this lesson, you must first create your own custom VPC. (Or if you have not deleted the VPC that you created previously, then you can use that one to complete the lesson)

Step 1) Create a log group

Click Services

Then click CloudWatch under Management & Governance

Click Logs in the left margin

Click Let's get Started (may differ depending on interface)

Click the Create Log Group Button (may differ depending on interface)

Log Group Name: OurNewCustomVPCFlowLogs ←give it a specific name like so

Click Create log group

Step 2) Create Flow Log and IAM role

Now that we have created our log group, click services and click VPC

Click Your VPCs in the left margin

Select OurNewCustomVPC and click actions and click create flow log

Filter*: All

Destination: Send to CloudWatch Logs ←Select Send to CloudWatch Logs

Destination log group*: OurNewCustomVPCFlowLogs ← select the flow log that we just created

IAM role*: ← We have yet to create a role, therefore Click **Setup Permissions**

Upon clicking Setup Permissions, a new tab will open up where we will create a new IAM role

Role Description: Provides creation and write access to AWS CloudWatch groups.

IAM Role: Create a new IAM Role.

Role Name: OurNewCustomVPCFlowLogsRole ← give it a specific name like so

(In order to view the policy document click view policy document)

Click Allow

Now return to the browser tab where we were creating our flow log and select the IAM role that we just created. The page should now look as follows:

Filter*: All

Destination: Send to CloudWatch Logs

Destination log group*: OurNewCustomVPCFlowLogs

IAM role*: OurNewCustomVPCFlowLogsRole ←Select the Role that we just created

Then click the create button at the bottom of the screen

(Our flow log has now been created)

All of our IP traffic is being sent to my CloudWatch logs group

Step 3) Create webpage on our web server so that we can test our Flow Log

(To test our flow log we will create a webpage on our web server that is located in our public subnet...If you have already created a webpage on your web server then you can skip this step)

Click Services

Click EC2

Select WebServerInPublicSubnet ← this is the name we gave our webserver in the **Build A Custom VPC in AWS** lesson. You may have named your webserver something different.

Click Connect

Select the connection method: ✓EC2 instance (browser-based SSH connection)

Once you are connected type the following

sudo su (and hit enter)

clear (and hit enter)

yum update -y (and hit enter)

service httpd status (and hit enter)

yum install httpd -y (and hit enter) ←this will install httpd clear (and hit enter)

chkconfig httpd on (and hit enter)

service httpd start and hit enter ←that will start our service

cd /var/www/html (and hit enter) ←be advised there is a space between cd and /

type ls (and hit enter) ← this is a lower case L not an upper case i

nano index.html (and hit enter)

At the nano screen type the following:

<html><h1>Is your instance running? Well then you had better go catch it!<h1></html>

Then exit by hitting ctrl + x

Then type Y and hit enter ← this will save the index.html file you created

Back at the terminal window type the following:

ls (and hit enter)

cat index.html (and hit enter)

Now lets go to our browser and open up a new url tab. Paste in the IPv4 address for your web server (To find the IPv4 address just go to the AWS console and click Services, click EC2, select the web server instance, and scroll down to the description tab, and copy the IPv4 Public IP)

Hit the refesh button several times. This will log some activity.

Step 4) Check your flow log activity

Go to the AWS console and click CloudWatch

Click Log groups in the left margin and click on OurNewCustomVPCFlowLogs and select a log stream and click search all. This will display the IP traffic activity to our web server. Mission Complete. Below are important concepts pertaining to VPC flow logs.

★VPC Flow Logs Cheat Sheet

-VPC Flow Logs monitor the in and out traffic of your Network Interfaces within your VPC

-You can turn on Flow Logs at the VPC, Subnet or Network Interface level

-VPC Flow Logs **cannot be tagged** like other AWS resources

-You **cannot change the configuration** of a flow log **after it's created**

-You **cannot enable** flow logs for VPCs which are peered with your VPC **unless it is in the same account**

-VPC Flow Logs can be delivered to **S3** or **CloudWatch Logs**

-VPC Flow Logs contains the source and destination **IP addresses** (not hostnames)

-Some instance traffic is **NOT monitored:**

> -Instance traffic generated by contacting the AWS DNS servers
>
> -Windows license activation traffic from instances
>
> -Traffic to and from the instance metadata address (169.254.169.254)
>
> -DHCP Traffic
>
> -Any traffic to the reserved IP address of the default VPC router