AWS setting up Route 53 DNS Query Logs

DNS Query Logs can be enabled on Route 53 hosted zones and sent to CloudWatch Logs. Route 53 uses common DNS return codes in the log and includes the edge locations involved.

**DNS Query Logs** can help you determine when there is a DNS problem in an application.

**2 Things to know:**

1. The entity in which you used to register a domain and whom holds authority on that domain. Basically the company in which can alter that domain.
2. The company or organization who manages the DNS resolvers for the domain. This can also be referred to as where the name servers point to. This can be you, or the company who holds authority on the domain.

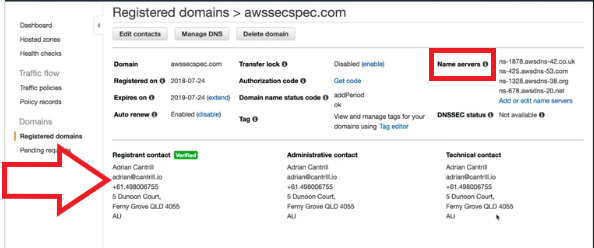
In order to run query logging in AWS, you do not need AWS to be the register for the domain (1), but you do need them to be the name servers or the resolvers of that domain (2).

The 2 limitations are first the sentence stated above and you also cannot log if you are using a Route 53 private hosted zone. In other words the hosted zone must be internet facing.

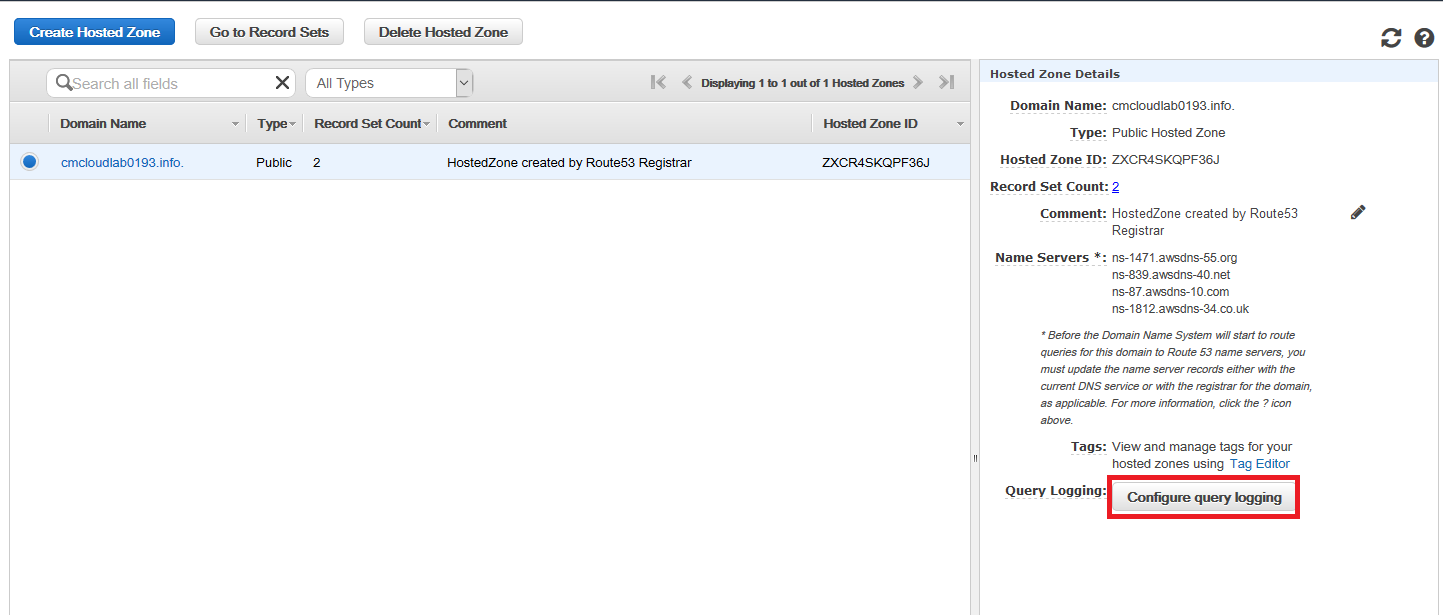
**Setting it up:**

**Step 1:**

First things first you need your own Route 53 hosted zone. As this cost money I do not have one so this documentation will be based on a Linux Academy lab. They give you limited access so I will pull pictures from their video too. For example this first picture comes from the video. He emphasizes what I stated at the top about what you need to setup query logging, and he even says it might come up on the exam. That is why I have this picture. The red box highlights the name servers, and as stated above, if these do not point to Route 53 you will not be able to do query logging. Also notice the red arrow displays the entity in which you used to register the domain with. Like I said up top, this does not need to be AWS.

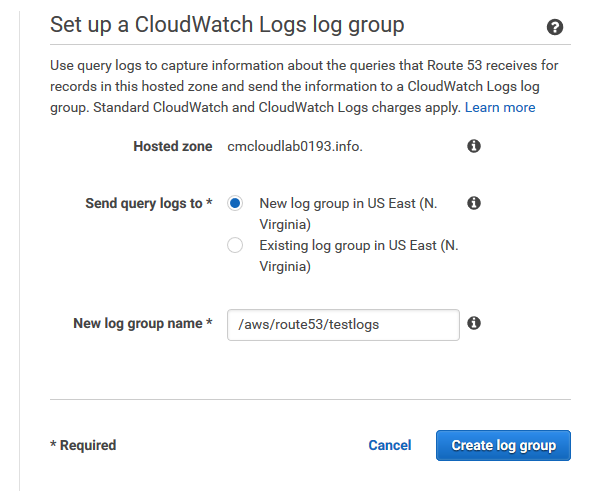


Navigate to your hosted zones by clicking the hosted zone button. Select the domain you want to log and click configure query logging.



**Step 2:**

When you are setting it up you are asked to create a new log group. Name it what you want and click create log group.



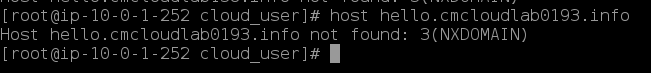
Next you are asked to configure a resource policy. It will automatically give you a valid policy you just need to supply your log group name. Then select create query log config.

**Step 3:**

Lastly you just need to test it out. One thing to note is when you first configure it with no traffic you will only get one log stream as shown below.



So to test it out we are going to do the host command with our domain name. After we do the host command you will see a second stream pop up which is a stream displaying the edge location involved. So we run the command below.



After a few minutes we get another stream.

