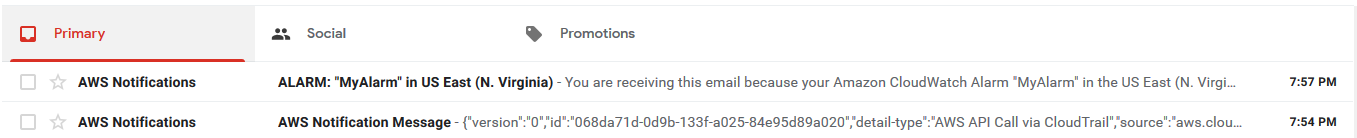
The differences between CloudWatch Events and metric filters

I am typing this mini essay out to help me understand their differences better and to understand what to use and when for the exam. I also feel like anyone from ACloudGuru is probably a little confused about this topic as it is not explained very well by Ryan. The cloud opened up a whole new space for security teams and that was automation. Automating security incidents is a big deal as often the hardest thing when dealing with an incident is actually noticing it. Both these functions in AWS deal with automation.

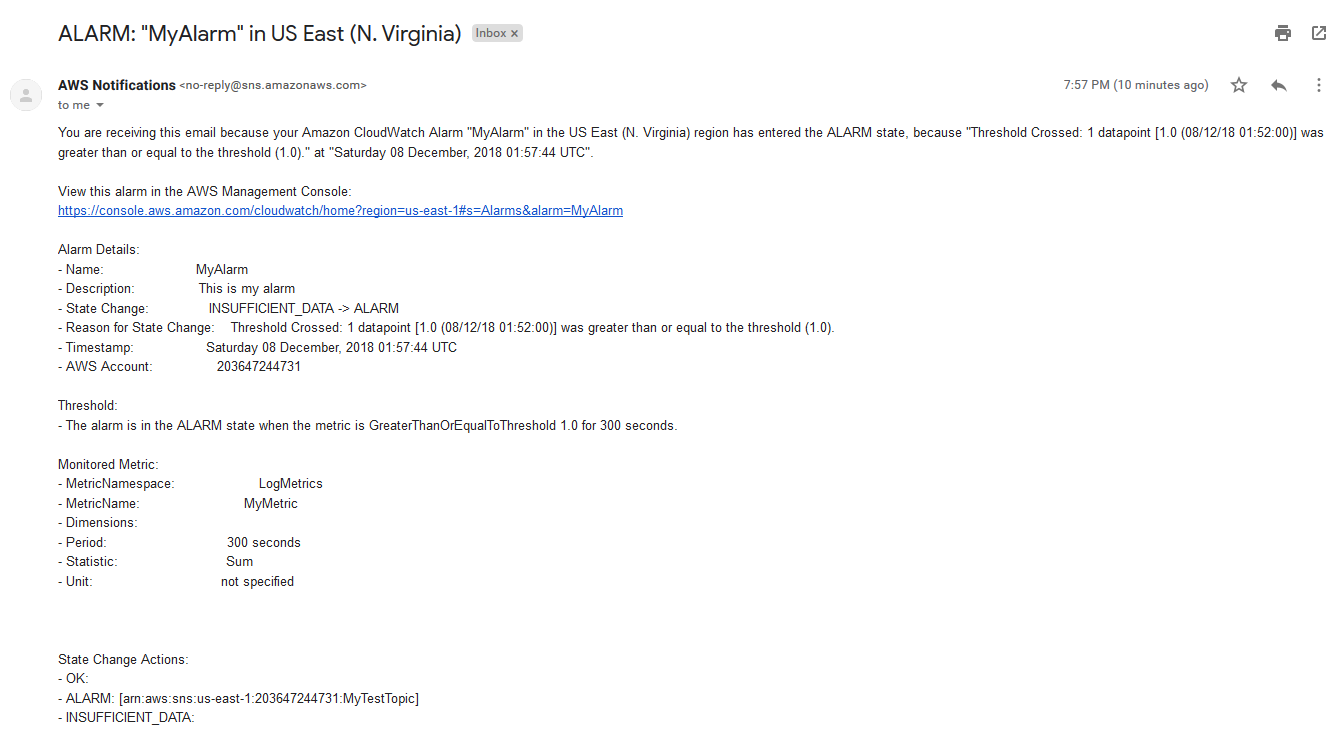
So what are their differences? Well let’s start with what they are first. Metric filters are place on log groups in CloudWatch Logs and they are a way to place metrics based on certain actions you are looking for. CloudWatch Logs can receive logs on just about any service so this is a handy tool to have. CloudWatch Events is the newer of the two and way better. There are so much more responses you can deploy when using the event feature that it almost, and I can’t stress the almost enough, makes metric filters useless.

Metric filters are considered legacy. They are near-real-time receiving notifications 15 minutes after an event at the latest. That is not too bad until you realize with CloudWatch   
Events you essential get notification immediately. Take this for example, in my account I have both a CloudWatch Event and a metric filter configured to detect the same thing. These rules both trigger when I or anyone disables a CloudTrail Trail in my account. So I disabled my CloudTrail and these are the emails I got.

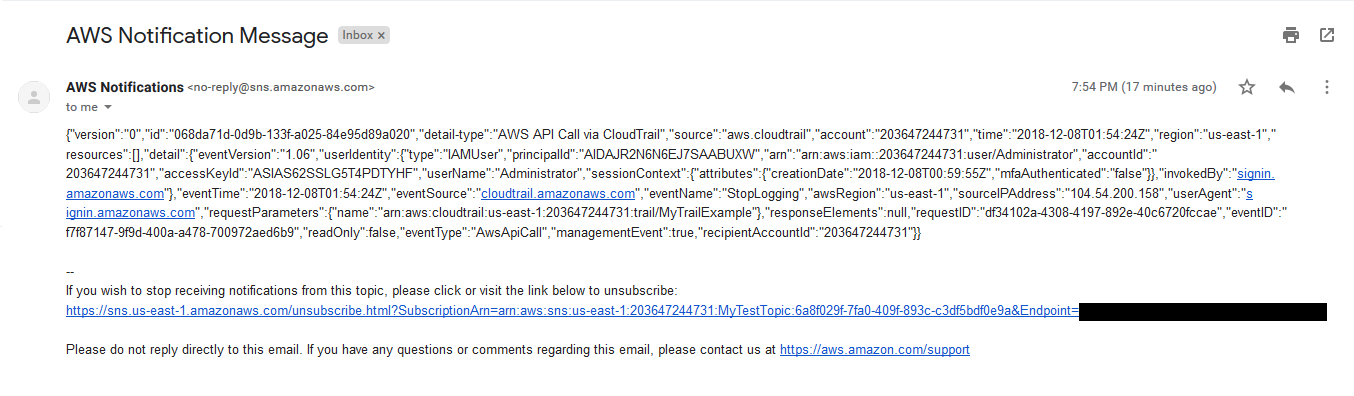


Now honestly I waited for like 15 minutes and got impatient so I did the whole process again. So obviously 3 minutes isn’t a lot as the top email comes from the metric filter alarm and the CloudWatch Event email is on the bottom. Keep in mind that I did the event at 7:54 right as I got my first email.

Next I would like to point out the contents of both emails. The metric filter does not give you much, besides informing you on the alarm you setup. On the other hand the CloudWatch Event will give you the exact API call that triggered the rule. This email will contain things like who made the change allowing for immediate answers.



This is the email based on the metric filter. As you can see not of information about the event. It just tells you what alarm got triggered and why. This email isn’t really useful unless you properly name your notifications obvious things like CloudTrail disabled.

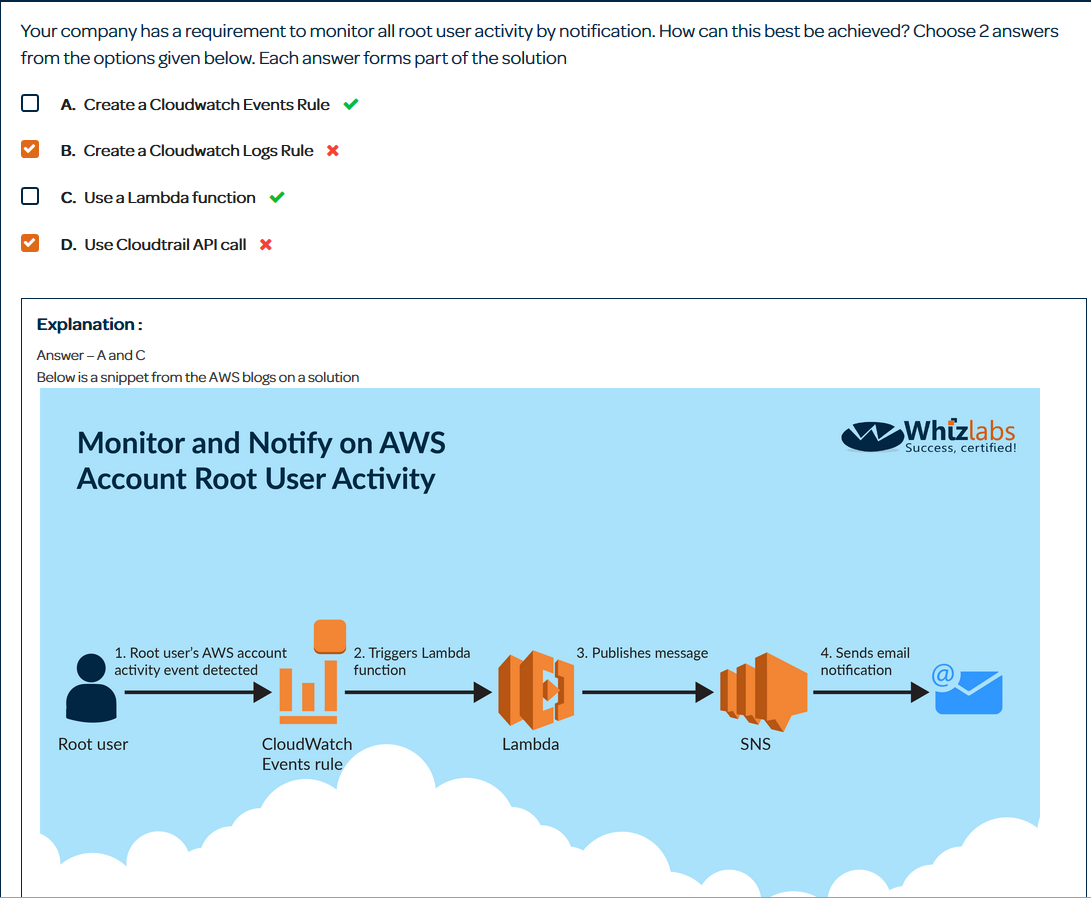


This second email based on the CloudWatch Event trigger contains the exact event that triggered the rule. Obviously it is in messy JSON, but if you did hard enough or put it in a text editor you can find good information. For example you can see the exact username of the person who did the event.

Ok so far CloudWatch Events looks better, but not by much. Well that is about to change. The main reason to use Events over filters are the amount of different services that can respond to a rule being triggered. With metric filters you have 3 options, you do an SNS email, an Auto-Scaling group, and certain EC2 actions. With CloudWatch Events there are countless options. Some of the more important ones include Lambda for automatic remediation of the event with functions, and things like system manager run command to automate commands to a fleet of instances. You can also choose to run CloudWatch events on a schedule.

So why would you use metric filters ever? A few reasons, because of CloudWatch Logs being able to receive logs from EC2 instances, and on premise servers you can use metric filters on application or system logs. Another reason you might want to use metric filters are for broader events happening in AWS. It is a little easier to configure metric filters so if you want to get an email every time your root user logs in you should consider using metric filters. The email is broad, but so is that event.

For the most part be careful on the exam and read what the question is asking for. In real life you almost always go for CloudWatch Events, but it’s probably a 50/50 on the test. Here are a few sample questions I’ve gotten from practice tests on whiz labs and Linux Academy.



I would like to point out this question because as you can tell I got it wrong. Be careful for questions like this one as in the question it states “how can you monitor all root user activity by notification”. If it was asking to watch root user logins the correct answer would be metric filters.

