Prashant Lakhera
Feb 16, 2019 · 3 min read · Listen

100 Days of DevOps — Day 6-CloudWatch Logs(Metric Filters)

Check the updated 101 Days of DevOps Course

Course Registration link: https://www.101daysofdevops.com/register/

Course Link: https://www.101daysofdevops.com/courses/101-days-of-devops/

YouTube link: https://www.youtube.com/user/laprashant/videos

Welcome to Day 6 of 100 Days of DevOps, So far

Day 1(CloudWatch) https://medium.com/devopslinks/100-days-of-devops-day-1-introduction-to-cloudwatch-metrics-b04be36307a8

Day 2(SNS) https://medium.com/@devopslearning/100-days-of-devops-day-2-introduction-to-simple-notification-service-sns-97137b2f1f1e

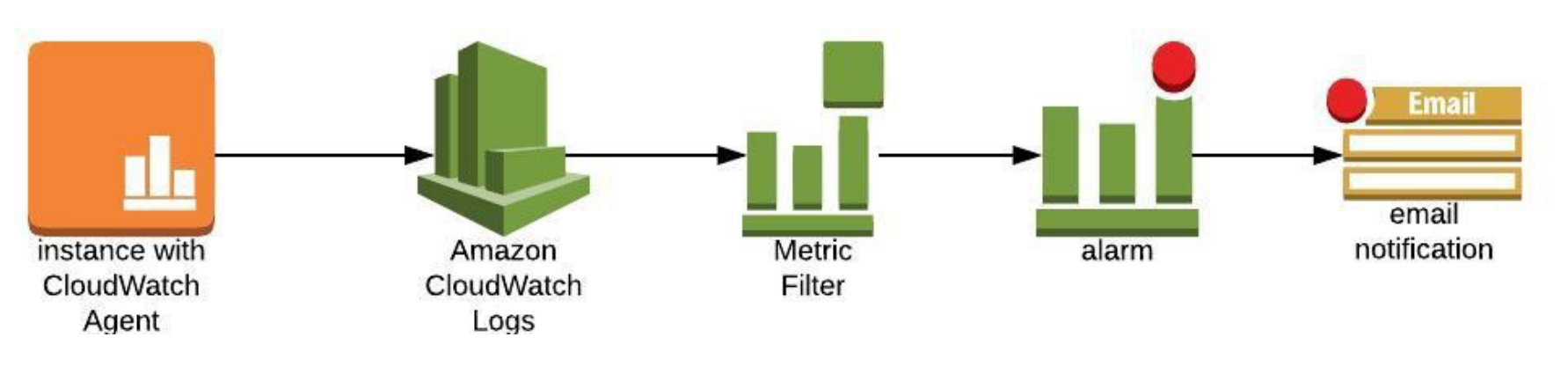
Day 3(CloudTrail) https://medium.com/@devopslearning/100-days-of-devops-day-3-introduction-to-cloudtrail-5ce923f44584

Day 4(CloudWatch Agent) https://medium.com/@devopslearning/100-days-of-devops-day-4-cloudwatch-log-agent-installation-centos7-d11054fffdf4

Day 5(CloudWatch with Slack) https://medium.com/@devopslearning/100-days-of-devops-day-5-cloudwatch-to-slack-notification-d2d84a192bf2

Problem: *I want to deploy a simple monitoring system when any unauthorized trying to access my servers I will notify via SNS.*

Solution: *This can be achieved using CloudWatch Metric Filter in combination with SNS.*

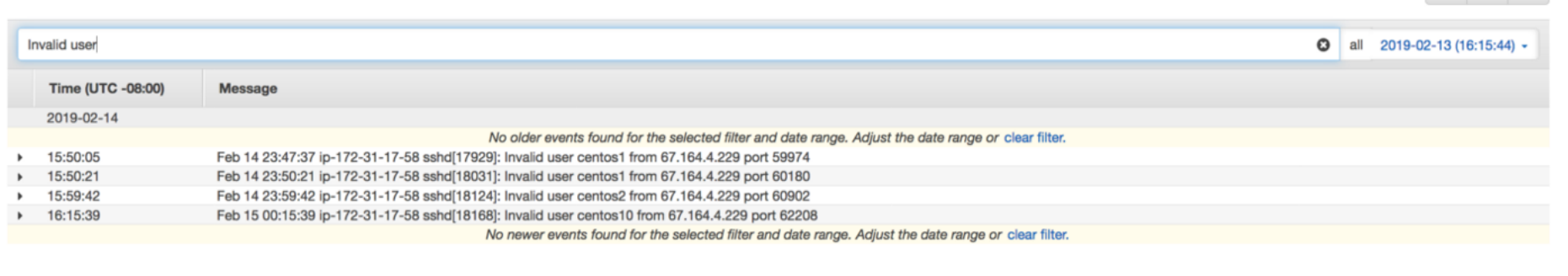


Step1

- *Install CloudWatch Agent(Make sure you are pushing /var/log/messages and /var/log/secure logs from your instance to CloudWatch log group)*

100 Days of DevOps — Day 4(CloudWatch log agent Installation — Centos7)
Welcome to Day 4 of 100 Days of DevOps, On the first day we discussed CloudWatch…
medium.com

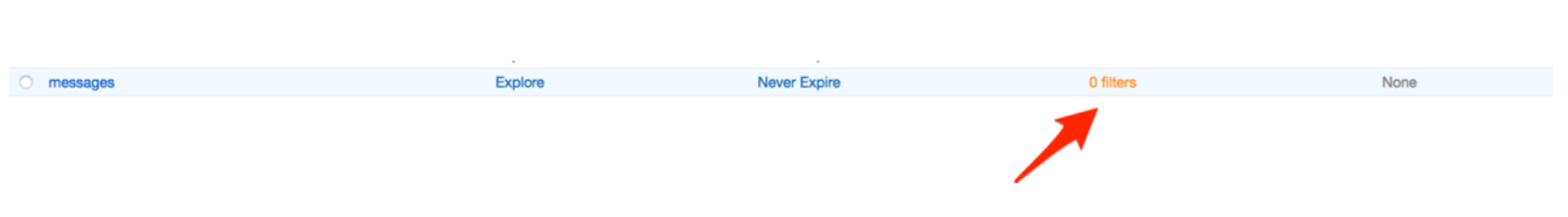
- *At the same time, go to CloudWatch Logs and search for Invalid user string*

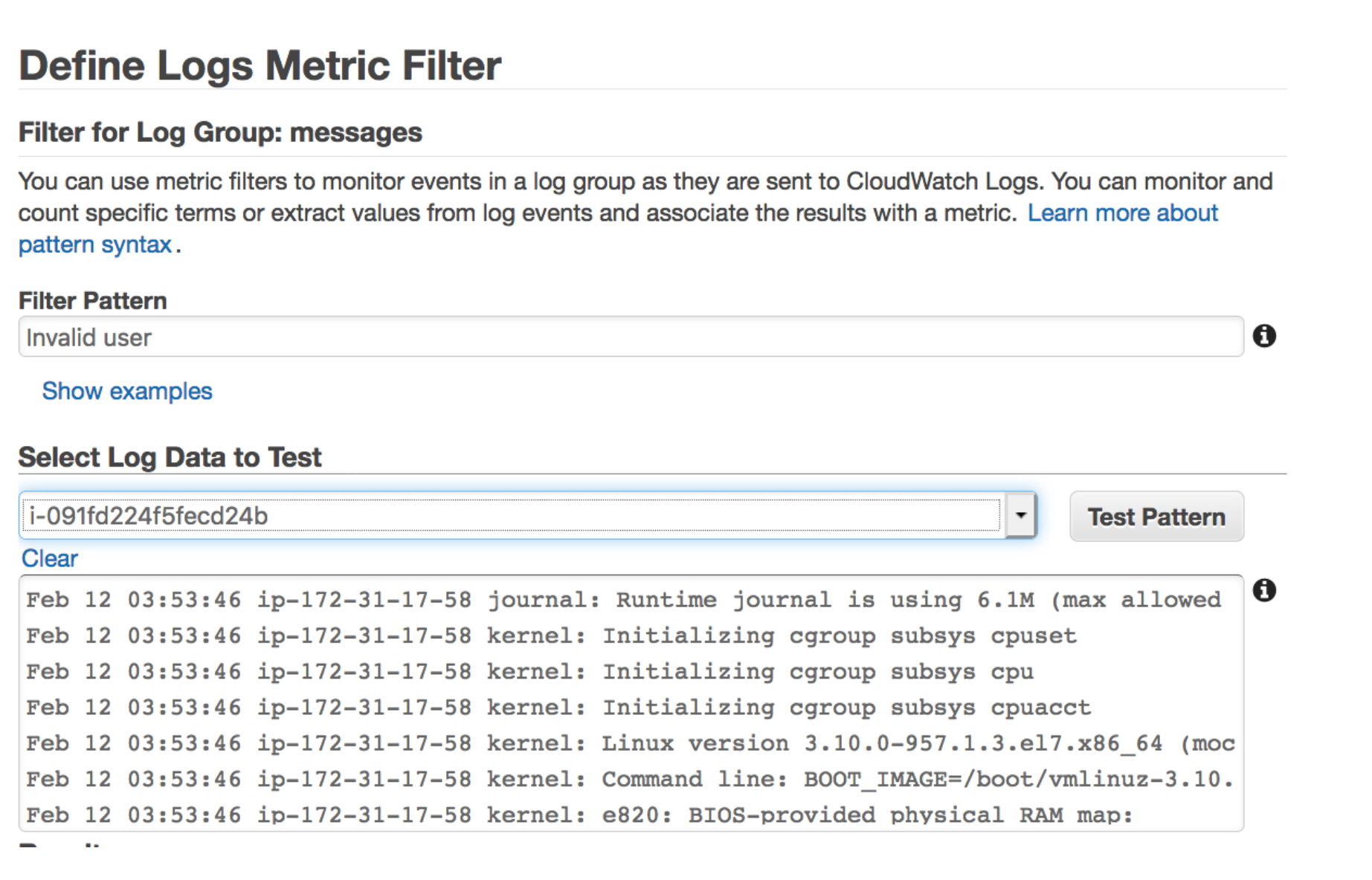


Step2

- *Go to*

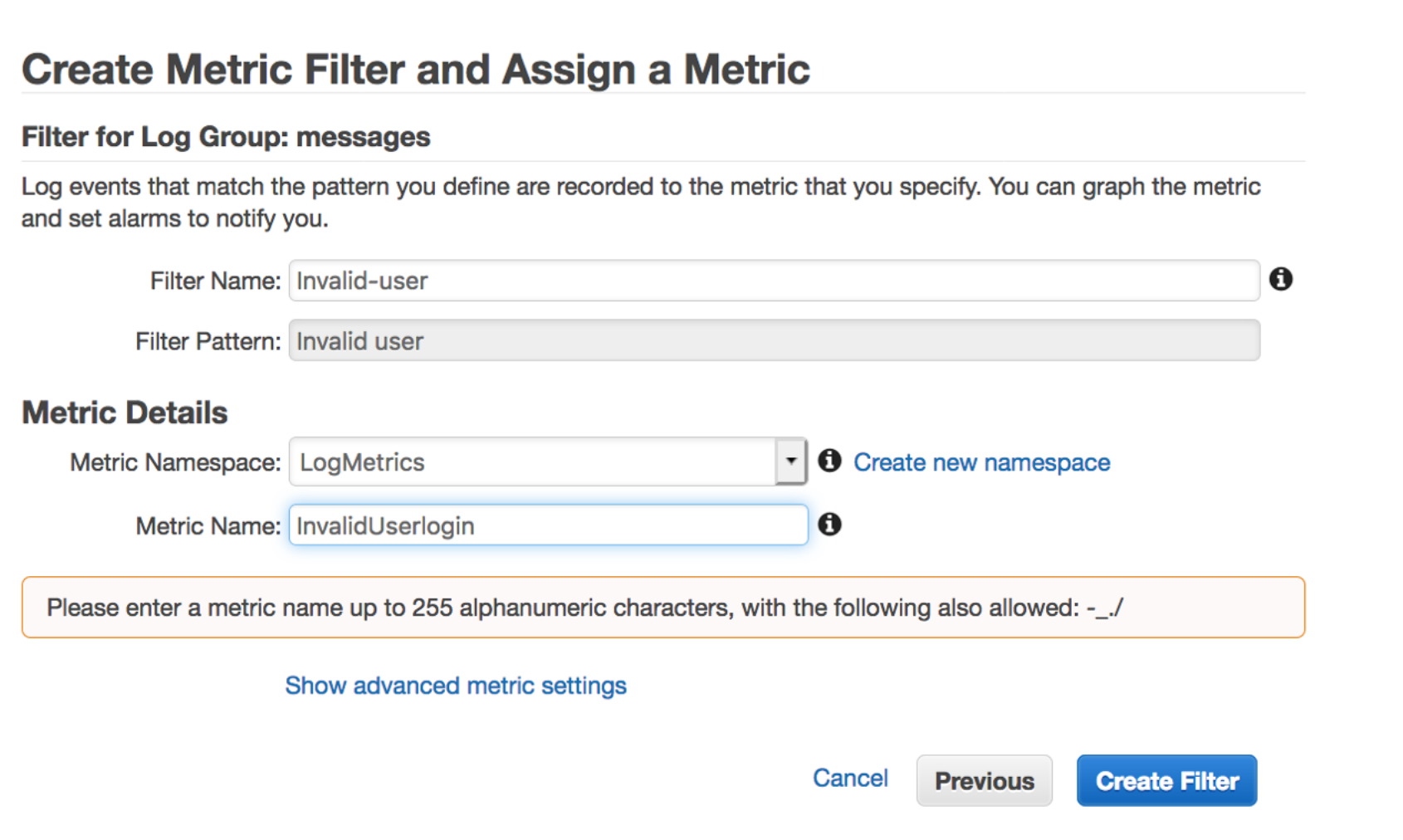
```
Management & Governance --> CloudWatch --> Logs --> messages --> 0 fileters --> Add Metric Filter
```



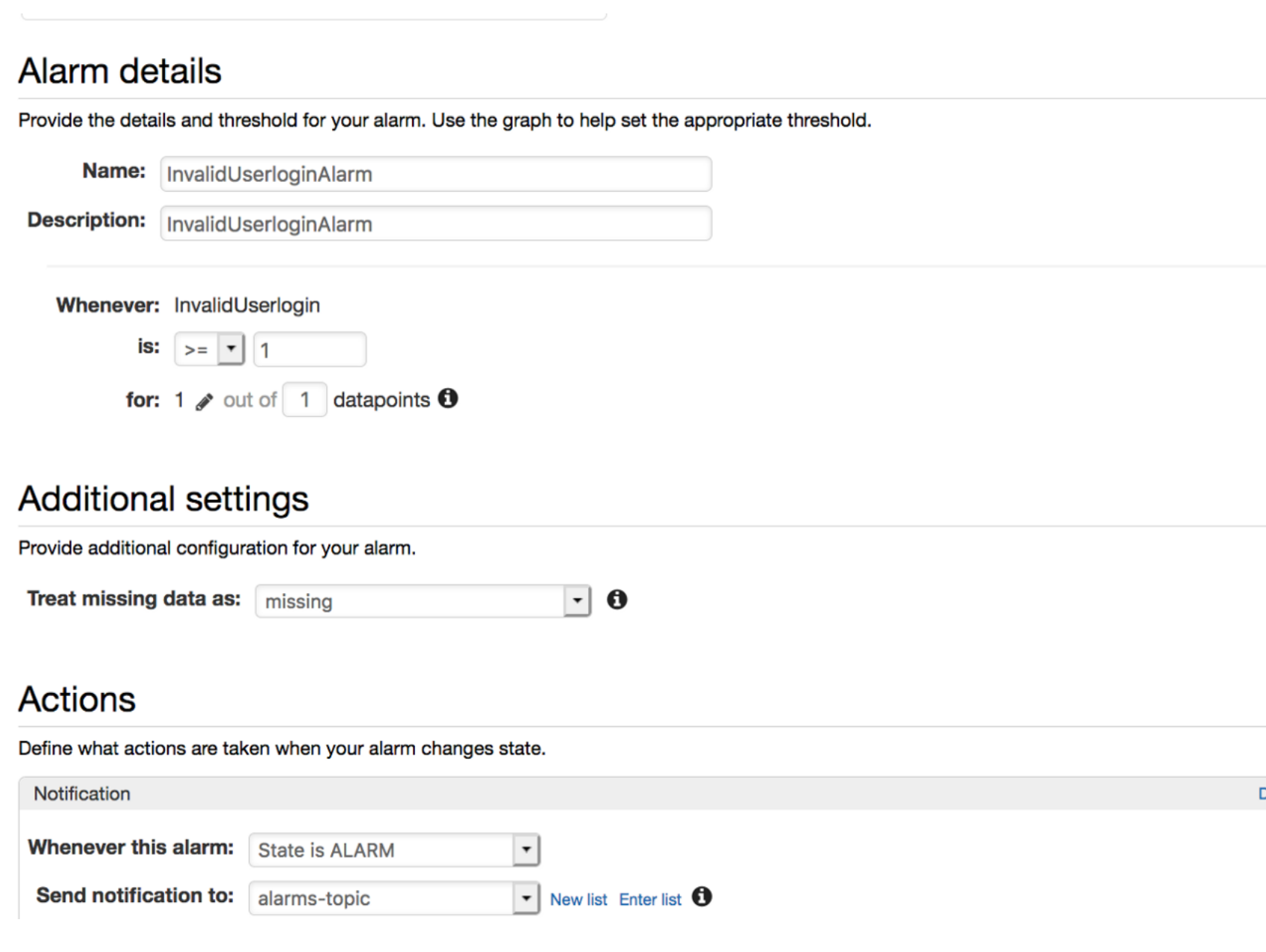



```
* Filter Pattern : Type Invalid user
* Select Log Data to Test: Select the right instance
```

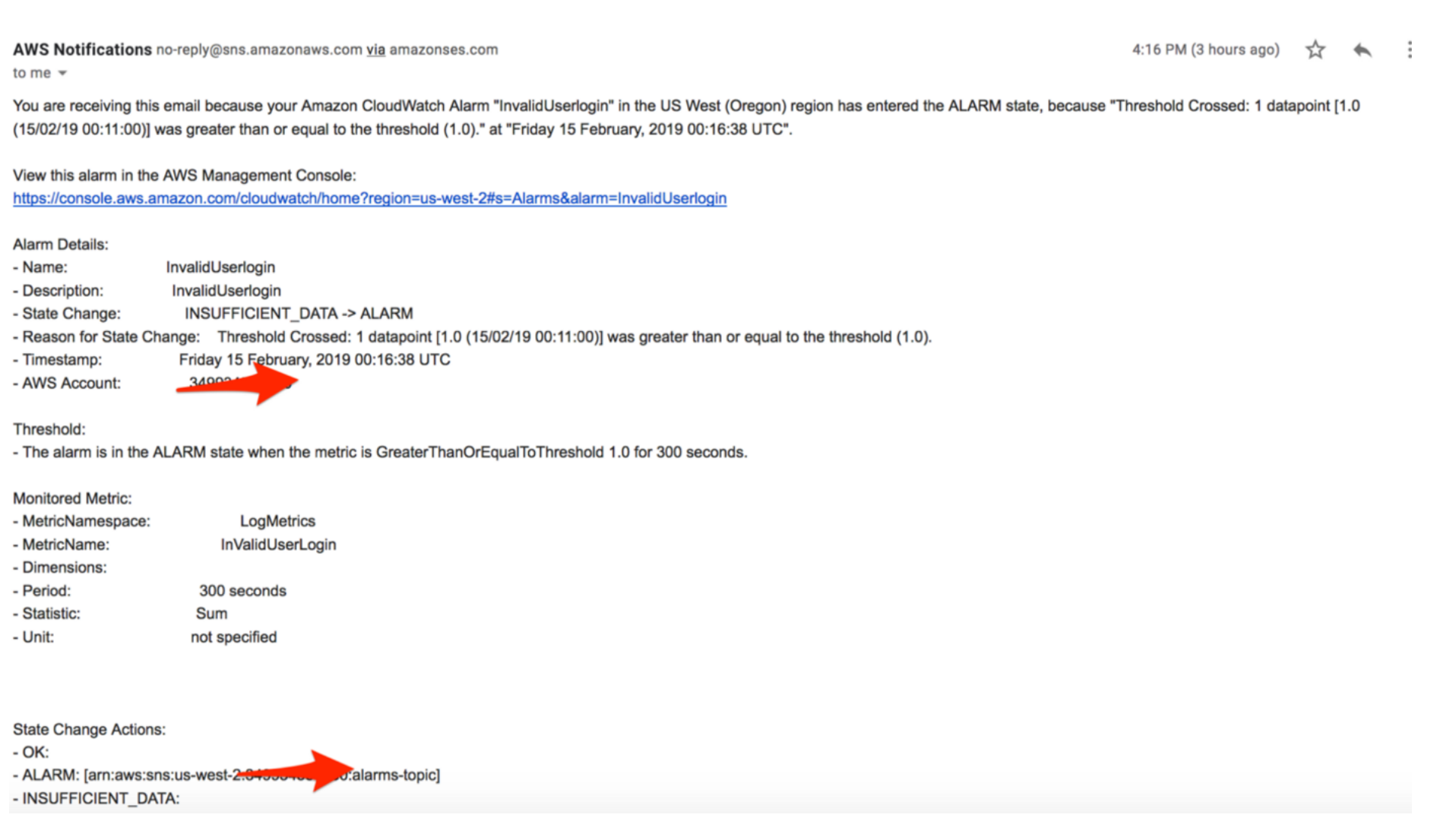
- *Keep everything default and give your metric some name(Metric Name: InvalidUserlogin)*



- *In the next screen, click on Create Alarm*




```
* Give your alarm Name and Description
* Set the threshold, for demo I am setting up as 1
* Select the SNS topic
```



- *Your simple notification system against un-authorized user is up and running.*

Looking forward from you guys to join this journey and spend a minimum an hour every day for the next 100 days on DevOps work and post your progress using any of the below medium.

- *Twitter: @100daysofdevops OR @lakhera2015*
- *Facebook: https://www.facebook.com/groups/795382630808645/*
- *Medium: https://medium.com/@devopslearning*
- *Slack: https://devops-myworld.slack.com/messages/CF41EFG49/*
- *GitHub Link:https://github.com/100daysofdevops*

Reference

100 Days of DevOps — Day 0
D-day is just one day away and finally, this is a continuation of the post(I posted a month earlier)
medium.com