



Prashant Lakhera

Feb 16, 2019 · 3 min read · Listen



Get started

Sign in

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>

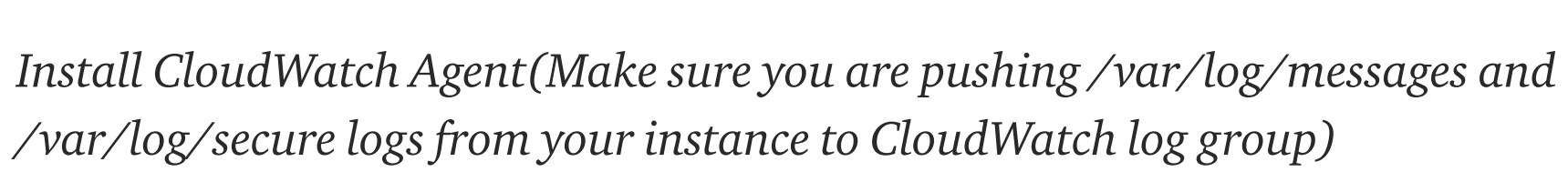
Day 3(CloudTrail) <https://medium.com/@devopslearning/100-days-of-devops-day-3-introduction-to-cloudtrail-5ce923f44584>

Day 4(CloudWatch Agent) <https://medium.com/@devopslearning/100-days-of-devops-day-4-cloudwatch-log-agent-installation-centos7-d11054fffd4>

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

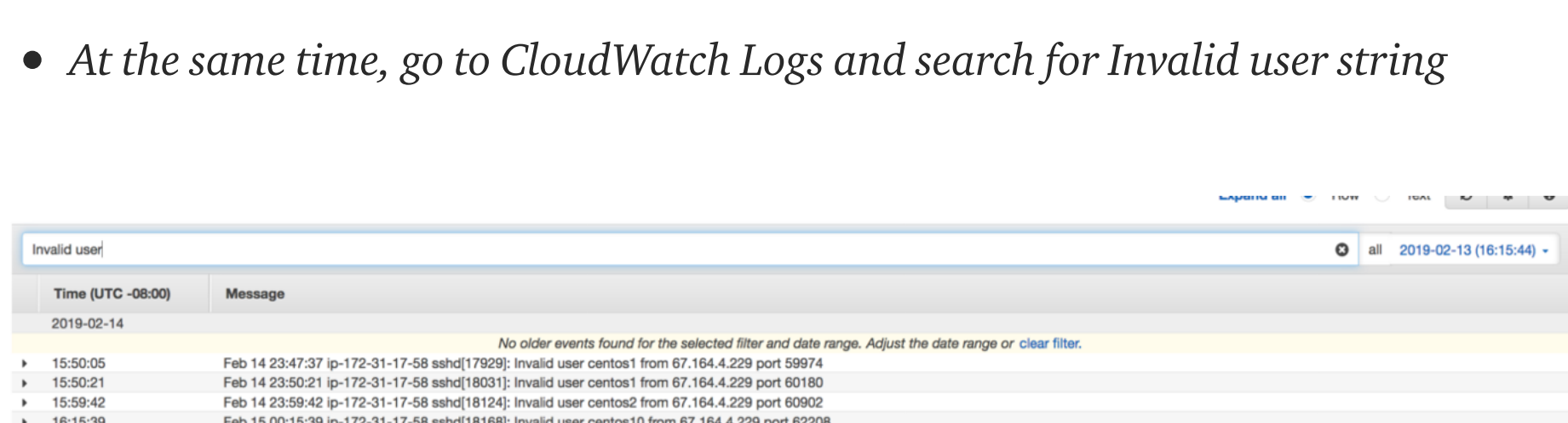
Problem: I want to deploy a simple monitoring system when any unauthorized trying to access my servers I will notify via SNS.

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)



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

Step2

- Go to

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



Define Logs Metric Filter

Filter for Log Group: messages

You can use metric filters to monitor events in a log group as they are sent to CloudWatch Logs. You can monitor and count specific terms or extract values from log events and associate the results with a metric. [Learn more about pattern syntax.](#)

Filter Pattern

Invalid user

Show examples

Select Log Data to Test

[-]091fd224f5fec24b

Feb 12 03:53:46 ip-172-31-17-58 journal: Runtime journal is using 6.1M (max allowed
Feb 12 03:53:46 ip-172-31-17-58 kernel: Initializing cgroup subways cpuset
Feb 12 03:53:46 ip-172-31-17-58 kernel: Initializing cgroup subways cpu
Feb 12 03:53:46 ip-172-31-17-58 kernel: Initializing cgroup subways cpucct
Feb 12 03:53:46 ip-172-31-17-58 kernel: Linux version 3.10.0-957.1.3.el7.x86_64 (moc
Feb 12 03:53:46 ip-172-31-17-58 kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-3.10.
Feb 12 03:53:46 ip-172-31-17-58 kernel: e820: BIOS-provided physical RAM map:

- * 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)

Create Metric Filter and Assign a Metric

Filter for Log Group: messages

Log events that match the pattern you define are recorded to the metric that you specify. You can graph the metric and set alarms to notify you.

Filter Name: Invalid-user

Filter Pattern: Invalid user

Metric Details

Metric Namespace: LogMetrics

Metric Name: InvalidUserlogin

Please enter a metric name up to 255 alphanumeric characters, with the following also allowed: ~/_

Show advanced metric settings

Cancel Previous Create Filter

- In the next screen, click on Create Alarm

Alarm details

Provide the details and threshold for your alarm. Use the graph to help set the appropriate threshold.

Name: InvalidUserloginAlarm

Description: InvalidUserloginAlarm

Whenever: InvalidUserlogin

ist: >= 1

for: 1 out of 1 datapoints

Additional settings

Treat missing data as: missing

Actions

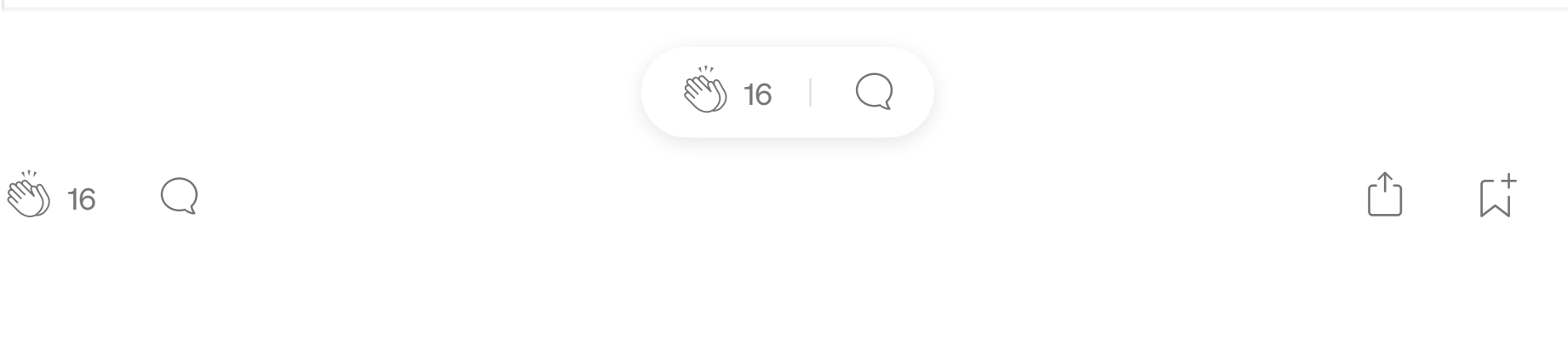
Define what actions are taken when your alarm changes state.

Notification

Whenever this alarm: State is ALARM

Send notification to: alarms-topic

- * 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.

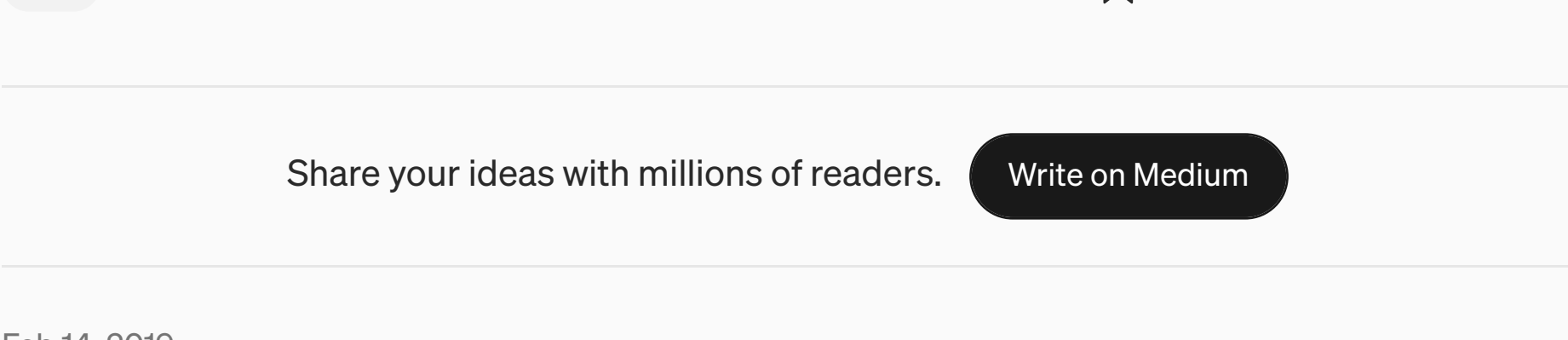
- Twitter: @100daysofdevops OR @lakhera2015
- Facebook: <https://www.facebook.com/groups/795382630808645/>

- Medium: <https://medium.com/@devopslearning>

- Slack: <https://devops-myworld.slack.com/messages/CF41EFG49/>

- GitHub Link:<https://github.com/100daysofdevops>

Reference



Get an email whenever Prashant Lakhera publishes.

Your email

Subscribe

By signing up, you will create a Medium account if you don't already have one. Review our [Privacy Policy](#) for more information about our privacy practices.

More from Prashant Lakhera

AWS Community Builder, Ex-Redhat, Author, Blogger, YouTuber, RHCA, RHCCS, RHCE, Docker Certified,4XAWS, CCNA, MCP, Certified Jenkins, Terraform Certified, 1XGCP

Feb 15, 2019

100 Days of DevOps — Day 5-(CloudWatch to Slack Notification)

Check the updated 101 Days of DevOps Course Course Registration link: <https://www.101daysofdevops.com/register/> Course Link:...

AWS 6 min read

Share your ideas with millions of readers.

Write on Medium

Feb 14, 2019

100 Days of DevOps — Day 4(CloudWatch log agent Installation — Centos7)

Check the updated 101 Days of DevOps Course Course Registration link: <https://www.101daysofdevops.com/register/> Course Link:...

AWS 8 min read

Feb 13, 2019

100 Days of DevOps -Day 3(Introduction to CloudTrail)

Check the updated 101 Days of DevOps Course Course Registration link: <https://www.101daysofdevops.com/register/> Course Link:...

AWS 7 min read

Feb 12, 2019

100 Days of DevOps — Day 2 -Introduction to Simple Notification Service(SNS)

Check the updated 101 Days of DevOps Course Course Registration link: <https://www.101daysofdevops.com/register/> Course Link:...

AWS 4 min read

Published in FAUN Publication · Feb 11, 2019

100 Days of DevOps — Day 1(Introduction to CloudWatch Metrics)

Check the updated 101 Days of DevOps Course Course Registration link: <https://www.101daysofdevops.com/register/> Course Link:...

AWS 7 min read

Love podcasts or audiobooks? Learn on the go with our new app.

Try Knowable

Search



Prashant Lakhera

4.6K Followers

AWS Community Builder, Ex-Redhat, Author, Blogger, YouTuber, RHCA, RHCCS, RHCE, Docker Certified,4XAWS, CCNA, MCP, Certified Jenkins, Terraform Certified, 1XGCP

Follow

More from Medium

Kashawn Shifflett

How to install NGINX on CentOS 8

Courtney Gatlin

Create a CI/CD pipeline with AWS & GitHub

Sujit Patel

Easy Steps to Create AWS VPC with Terraform

Narendra Reddy

AWS—10

Help Status Writers Blog Careers

Privacy Terms About Knowable