logs & custom & server logs

(A)

Rainbow

PAGE:
DATE: / /

* Logs *

Go to IAM
click on Roles
click on create role
select AWS service
select EC2 in Common use cases.
→ click on Next.
Q search cloud Watch.
select cloud-watch-log-full-access
→ click on Next.
Give the name as role-logs
Scroll Down and click on
→ create role.

Go to EC2
click on launch Instance
select AMI
Select t2.micro
click Next add storage
click Next Add tags
click Next configure security Group HTTP & SSH
Review and launch Instance.

Now Go to Instances
select Instance
click on Action
click on security
click on Modify IAM Role
choose IAM role as role-logs
→ click on save

Rainbow
PAGE
DATE : / /

Go to Instances
Select Instance
Click on :connect
copy last command from ssh client
Open Moboxterm paste command
and connect to the Instance.
Use sudo su -
Use cd /
Use yum install awslogs -y
Use cd /etc/awslogs
Use ls -lte

We have to do changes in two files
they are ① awslogs.conf ② awscli.conf

Use vi awscli.conf

Now I am using ohio region so in region
I have used as us-east-2 so make
changes accordingly and save file.

Use vi awslogs.conf

Go in the last

Make Changes Like This

```
[application-1]
datetime_format = %b %d %H:%M:%S
file = /mnt/app.log
buffer_duration = 5000
log_stream_name = {instance_id}
initial_position = start_of_file
log_group_name = application
```

Save file

Use service awslogsd start
~~service awslogsd restart~~

Use cd /mnt
touch app.log
echo "Hii" > app.log
echo "Hello" >> app.log

Use service awslogsd restart

Now Go to cloud Watch
click on Log Groups
application is our log group name
click on application
click on log steeam name which appear in blue colour you can see your logs.

Local log file / custom

Use echo "third message" >> app.log

Now refresh ~~cloud~~ log events in cloud Watch so that we can see our latest log

Rainbow

PAGE :
DATE : / /

To configure our HTTP server logs with cloud front.

Use yum install httpd -y
service httpd start

Use cd /etc/httpd/logs
ls -lte
{ error_log
access_log }

We will these two files & have ~~two~~ to configure into our cloud front logs.

Use cd /etc/awslogs
vi awslogs.conf
paste code and save file.

Insert Below Code in last of awslogs.conf file and save

```
[server-access-logs]
datetime_format = %b %d %H:%M:%S
file = /etc/httpd/logs/access_log
buffer_duration = 5000
log_stream_name = {instance_id}
initial_position = start_of_file
log_group_name = http-server-access-logs

[server-error-logs]
datetime_format = %b %d %H:%M:%S
file = /etc/httpd/logs/error_log
buffer_duration = 5000
log_stream_name = {instance_id}
initial_position = start_of_file
log_group_name = http-server-error-logs
```

Use service awslogsd restart

GO to cloud Front
click on log Group

we can see our server access and error log groups.

Metric filters

172.31.36.19

Rainbow

PAGE:
DATE: / /

Now we have to filter logs on ~~metric~~ ~~Basis~~ Pattern Basis. They are like:

ERROR
INFO
RUN
OK

Now go to log group
~~click on metric filters~~
Click on Actions
Click on Create metric filters

In filters pattern insert ERROR

in Test Pattern
Select our instance id for select log data to test.

Click on test Pattern

Click on next

Enter filter name as error-metric

In metric details
metric namespace - error-metric
metric name - error-metric
metric value - 1
unit - none
click on next
click on create metric filters.

Rainbow (F)

PAGE:
DATE: / /

Now Go to metric filters
Click on create Alarm

In metric
namespace — error-metric
Metric name — error-metric
Statistics — Sum
Period — 1 minute

In Conditions
Threshold Type — Static
When error-metric is — Greater threshold
define threshold value — 2
Click on next

In Notification
Alarm state trigger — In Alarm
Select an SNS Topic — Choose Existing
Send notification to — SNS-Topic-1
Click on next

In Name & Description.
Alarm Name — error-metric-Alarm
description — —"—
Click on next

Review it & click on create Alarm

Rainbow

PAGE:
DATE: / /

Now Go to Mobaxterm

use cd /mnt
use ls -lte

we will se app.log file

Now use
5 times
echo "ERROR : this is essos" >> app.log
echo "ERROR : this is essos >> app.log

Now wait for 2 min

Go to ~~CW~~ Cloudwatch
click on All Alarms.

Check state of our alarm which is changed from ok to In Alarm.

Check our email Inbox also

we will get an email notification as in our logs we have an ERROR pattern that crossed its threshold limit.