The Amazon EC2 instances in your Elastic Beanstalk environment generate logs that you can view to troubleshoot issues with your application or configuration files. Logs created by the web server, application server, Elastic Beanstalk platform scripts, and AWS CloudFormation are stored locally on individual instances.

STEPS TO CONFIGURE:

* Create an centos7 EC2 instance (WebServer = web01)
* It should have web files (index.html) running
* SSH to the instance
* sudo –i
* cd /var/log/httpd/
* ls
* cat access\_log
* tail –f access\_log
* We would create an S3 Bucket to be used to archive the logs out of the system
* Login to your AWS account
* search for S3 service
* Bucket Name = wave-web-logs-321
* select same region of the instance
* click on create Bucket

Bucket name = wave-web-logs-321

select same region

scroll down and click on create

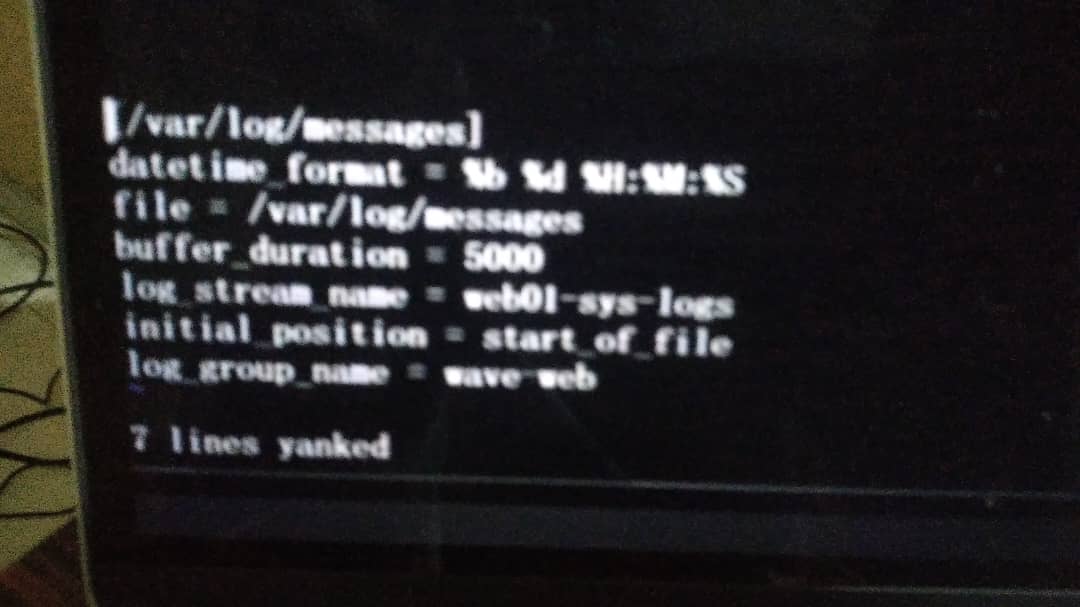
* Return back to your GitBash
* tar czvf wave-web01-httpdlogs19122020.tar.gz \*
* ls
* mkdir /tmp/logs-wave
* mv wave-web01-httpdlogs19122020.tar.gz /tmp/logs-wave/
* ls
* cat /dev/null > access\_log
* cat /dev/null > error\_log
* cat access\_log
* i would use AWS CLI to move
* ls /tmp/webtrash
* ls –ltr /tmp/logs-wave/
* yum install awscli –y
* ls
* aws s3 help
* we need to create a I-AM-USER
* aws s3 ls (It should give an error, becos i haven’t run aws configure)
* aws configure
* Go to your AWS account in the browser and click on services at the top left pan
* search for Iam and click on Add user
* user name = s3-log-admin
* check programmatic access and click on next
* click on Attach existing policies directly tab
* search for Amazon s3 full Access and check it
* click on next and then click on create user
* download the .csv file and copy the access and secret
* return to your GitBash and paste both access and secret keys
* give the region where the s3 Bucket is
* output format = json
* aws s3 ls (to show a list of all buckets in the s3)
* **aws s3 cp /tmp/logs-wave/wave-web01-httpdlogs19122020.tar.gz s3://wave-web-logs-321/**

**OR:**

**aws s3 sync /tmp/logs-wave/ s3://wave-web-logs-321/**

* rm –rf /tmp/logs-wave/\*
* Cloud watch logs is used to stream live Logs, and access given to the developers to stream (analize, set alarms on the metric, create metrics from the logs, send logs to elastic search and s3 Buckets for archiving)
* click on services and search for roles (this is an alternative way to I am User to gain access)
* click on create roles

1. type of trusted entity = AWS service
2. use cases = EC2
3. click on next and search forAmazon s3 full Access and cloud watch logs full Access
4. click on next
5. role name = log-admin-role
6. click on create role
7. Return to GitBash to remove credentials
8. cd
9. rm –rf .aws/credentials
10. Let’s attach the role we created, go to your running instances on AWS account
11. check the box to select your instance wave-web01
12. click on action button on the top right pane
13. scroll down to Security and click on modify IAM role
14. click on the drop down arrow and select the IAM role created (log-admin-role)
15. click on save
16. Return back to your GitBash
17. aws s3 ls
18. We would install cloud watch logs agent
19. curl <https://s3.amazonaws.com/aws-cloudwatch/downloads/latest/awslogs-agent-setup.py> -O (check the documentation guide for cloud watch logs)
20. ls
21. python awslogs-agent-setup.py - -region us-east-2
22. during the installation it will ask for AWS CLI keys, there is no need since we have attached the IAM user roles to the instance
23. Hit enter until you reach path of log file to upload = hit enter to accept the default path shown
24. Destination log group name = wave-web
25. Enter choice [1] = web01-sys-logs
26. Enter log stream name = web01-sys-logs
27. Timestamp format = hit enter for default
28. initial position of upload = hit enter for default
29. More log files to configure = No (these would be done through configuration)
30. Take note of the configuration file save path location
31. service awslogs status
32. ls /var/log/messages
33. If everything is configured properly you should see it in the cloud watch logs
34. click on service tab and search for cloud watch logs
35. in the left pane, search for log groups and click it
36. you should see the log group name (wave-web)
37. click on it and scroll down to see the log stream
38. we want to send the access\_log
39. ls /var/log/httpd/access\_log
40. vi /var/awslogs/etc/awslogs.conf
41. scroll down to the last 7 lines and copy them



1. leave a line and paste the copied 7 lines beneath
2. edit the line:

file = /var/log/httpd/access\_log

log\_stream\_name = web01-httpd-access

log\_group\_name = wave-web

1. :wq
2. service awslogs restart
3. If you wish to export data to Amazon S3 OR: Create Elasticsearch or Lambda

Go to your log stream under log groups

click to check the log stream created and click on the actions button

1. click on Matric filters tab if you wish to create matric and set an Alarm against suspicious IP hacking (Video at point 18.00min)

Generating Logs from Load Balancers:

1. Go to Load Balancer under service
2. click on create and select classic load balancer

* Load balancer name = wave-elb
* select your VPC
* HTTP / 80 and HTTP / 80
* create security group

SG-Name = wave-elb-sg

Description = wave-elb-sg

* Health check

ping protocol = HTTP

ping port = 80

ping path = /index.html

response timeout = 5secs

interval = 30secs

unhealthy = 2

healthy = 2

click next

* Add Instance (select the instance you want to attach the load balancer to)
* click on next
* click on preview and create
* click to check on the created load balancer
* click on the Description tab
* scroll down to attributes section and click on configure access logs button
* click to check on enable access logs
* interval = 5mins
* s3 location = paste the name of your s3 buckets (wave-web-logs-321)/the name of the directory / folder in your s3 (elb-wave)
* To create the directory in s3, open Amazon s3 and click on your s3 name
* under Objects tab, click on create folder
* folder name = elb-wave
* click on create folder
* Under the Permissions Tab, click on Edit Bucket policy
* Read the steps here:

<https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/enable-access-logs.html#attach-bucket-policy>

* copy the code in the link above into Notepad++ and edit it with all infos
* save it with a Jason extension (s3-policy.json)
* Go to Edit Bucket policy and paste the edited codes there
* click on save changes
* click on the Description tab
* scroll down to attributes section and click on configure access logs button
  + - * click to check on enable access logs
      * interval = 5mins
      * s3 location = paste the name of your s3 buckets (wave-web-logs-321)/the name of the directory / folder in your s3 (elb-wave)
* To check if it is generating text files
* Go to the s3 Bucket and click on Objects Tab
* click on elb-wave, you should see a text log file
* if you wait for 5mins, you should be able to see the elb-access-log file
* ~~When you click on save, it will show an error becos we haven’t configure the IAM or Roles permission for S3~~