CloudFront logs with AWS Elasticsearch Service

AWS Elastic Search

Kibana

S3

(Log Bucket)

**S3:**

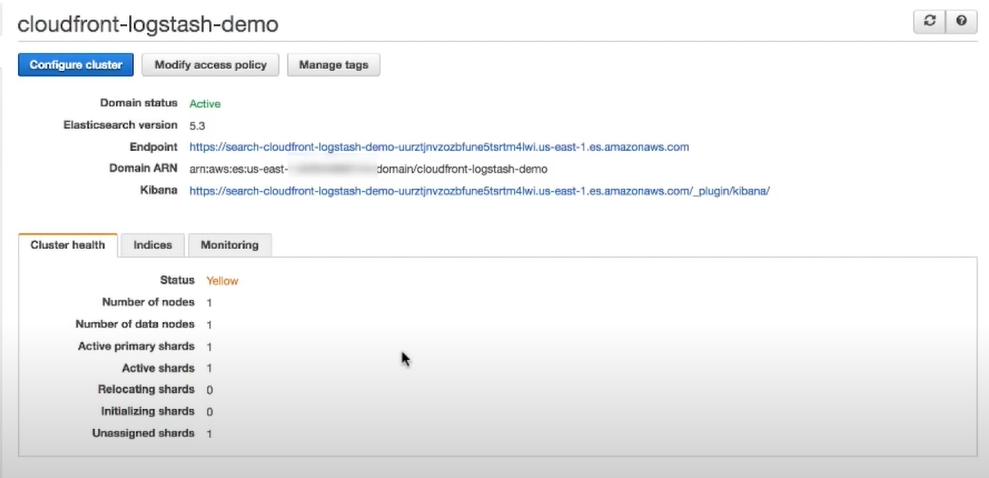
* Create bucket for logs.
* Cloud Front > edit distribution > enable logging > choose the s3 bucket to put logs

**Log Stash:**

* Open CLI and SSH in to EC2 instance.
* Download Log stash from Log stash site: $ wget “link”
* Extract files: $ tar xvf “file name”
* Install logstash plugin for elastic search: $ bin/plugin install logstash-output-amazon\_es
* Create or edit config file (template which describes what logstash has to do)
* After doing this, Log stash will start putting logs from S3 into the Elastic Search Domain**.**

**Elastic Search:**

* Create Elastic Search Domain



**Kibana:**

* Elastic Search Domain will provide ARN for Kibana.
* You can modify access policy as per your requirement