

Security Development Lab

Access Information - F5 VPN & SSH

SSH with AD credentials (Enrolled through AWS - Check with Kathir & Team to create accounts in proxy ldap and also enroll for F5 VPN access)

```
ssh mahajag@10.7.20.148 / default password
```

Add in /etc/hosts

10.7.20.148 awsnlsec001.amwaternp.net

Name	Endpoint	Username	Password
Kibana	http://awsnlsec001.amwaternp.net/app/kibana	-	-
Elastic Search	http://awsnlsec001.amwaternp.net:19200/_search?q=Rao%20Sanjay		
ES Indices	http://awsnlsec001.amwaternp.net:19200/_cat/indices		

app base - installation

```
[root@awsnlsec001 ~]# cd /apporchid/solutions/awsecurity/
[root@awsnlsec001 awsecurity]# ls -l
total 20
drwxr-xr-x. 5 mahajag root 4096 Mar 16 16:13 apps
drwxr-xr-x. 3 mahajag root 4096 Mar 16 15:04 data
drwxr-xr-x. 2 mahajag root 4096 Mar 19 04:37 javaapps
-rw-r--r--. 1 mahajag root  695 Mar 16 15:04 README.txt
drwxr-xr-x. 2 mahajag root 4096 Mar 16 15:04 softwares
```

```
[root@awsnlsec001 awsecurity]# du --si . --max-depth=3
252M    ./softwares
787k    ./data/14MAR2018/orig
17k     ./data/14MAR2018/cfglogstash
1.6M    ./data/14MAR2018
1.6M    ./data
879M    ./apps/elasticsearch-6.2.2/data
369k    ./apps/elasticsearch-6.2.2/bin
9.1M    ./apps/elasticsearch-6.2.2/modules
24M     ./apps/elasticsearch-6.2.2/lib
91M     ./apps/elasticsearch-6.2.2/plugins
8.8M    ./apps/elasticsearch-6.2.2/logs
41k     ./apps/elasticsearch-6.2.2/config
```

1.1G	./apps/elasticsearch-6.2.2
4.1k	./apps/logstash-6.2.2/data
177k	./apps/logstash-6.2.2/bin
115k	./apps/logstash-6.2.2/tools
2.3M	./apps/logstash-6.2.2/modules
508k	./apps/logstash-6.2.2/lib
4.1k	./apps/logstash-6.2.2/logs
33k	./apps/logstash-6.2.2/config_vpn
33k	./apps/logstash-6.2.2/config_lenel
242M	./apps/logstash-6.2.2/vendor
35M	./apps/logstash-6.2.2/logstash-core
33k	./apps/logstash-6.2.2/config
21k	./apps/logstash-6.2.2/logstash-core-plugin-api
33k	./apps/logstash-6.2.2/config_myaccess
279M	./apps/logstash-6.2.2
69M	./apps/kibana-6.2.2-linux-x86_64/data
17k	./apps/kibana-6.2.2-linux-x86_64/bin
382M	./apps/kibana-6.2.2-linux-x86_64/node_modules
25M	./apps/kibana-6.2.2-linux-x86_64/optimize
62k	./apps/kibana-6.2.2-linux-x86_64/webpackShims
539M	./apps/kibana-6.2.2-linux-x86_64/plugins
54M	./apps/kibana-6.2.2-linux-x86_64/node
22M	./apps/kibana-6.2.2-linux-x86_64/src
13k	./apps/kibana-6.2.2-linux-x86_64/config
2.9M	./apps/kibana-6.2.2-linux-x86_64/ui_framework
1.1G	./apps/kibana-6.2.2-linux-x86_64
2.4G	./apps

```
4.1k    ./javaapps
2.7G    .
```

configurations

Directory contains logstash configuration -

```
[mahajag@awsnlsec001 awsecurity]$ ls -l ./data/14MAR2018/cfglogstash/
total 12
-rw-r--r--. 1 mahajag root 587 Mar 16 16:37 lenel.conf
-rw-r--r--. 1 mahajag root 462 Mar 16 16:37 myaccess.conf
-rw-r--r--. 1 mahajag root 700 Mar 16 16:37 vpn.conf
```

Ingest - data

Directory contains data available for processing on last week -

```
[mahajag@awsnlsec001 14MAR2018]$ ls -l /apporchid/solutions/awsecurity/data/14MAR2018
total 772
drwxr-xr-x. 2 mahajag root 4096 Mar 19 03:54 cfglogstash
-rwxr-xr-x. 1 mahajag root 1002 Mar 19 03:54 ingest.sh
-rw-r--r--. 1 mahajag root 230 Mar 19 03:54 myaccess.csv
drwxr-xr-x. 2 mahajag root 4096 Mar 19 03:54 orig
-rw-r--r--. 1 mahajag root 195237 Mar 19 03:54 VPN_radius_authentications_2018-13-03_07-10.csv
-rw-r--r--. 1 mahajag root 574515 Mar 16 16:17 Woodcrest report 3 days.txt
```

Monit Environment

```
[mahajag@awsnlsec001 ~]$ sudo monit status
The Monit daemon 5.14 uptime: 0m
```

```
System 'awsnlsec001.amwaternp.net'
  status                               Running
  monitoring status                     Monitored
  load average                          [0.00] [0.01] [0.05]
  cpu                                   0.1%us 0.0%sy 0.0%wa
  memory usage                          5.3 GB [18.2%]
  swap usage                            0 B [0.0%]
  data collected                        Mon, 19 Mar 2018 03:57:36
```

```
[mahajag@awsnlsec001 ~]$
```

Few additional CLI for managing services - e.g. status, observe, ingest, relaunch

status - informs whether services stack is RUNNING or STOPPED

observe - tails necessary logs and insight on environment

ingest - in case data is corruptly ingested, this will clear indexes in ES and re-ingest data from beginning

relaunch - relaunch services, this does not empty indexes content but just restarts all java apps.

For example -

```
[mahajag@awsnlsec001 ~]$ status
RUNNING
[mahajag@awsnlsec001 ~]$ observe
```

```
[mahajag@awsnlsec001 ~]$ ingest
[mahajag@awsnlsec001 ~]$ relaunch
```

Accessing Elastic Search Query console

Download elasticsearch-head chrome extension and try adding <http://10.7.20.148:19200/> endpoint to access query console.

The screenshot shows the Elasticsearch Head Chrome extension interface. The browser address bar displays 'Elasticsearch Head' and the URL 'chrome-extension://ffmkiejmecalpfloofpjologoblkegm/elasticsearch-head/index.html'. The main header shows 'Elasticsearch' with a 'Connect' button and the status 'cluster health: yellow (33 of 48)'. Below the header, there are tabs for 'Overview', 'Indices', 'Browser', 'Structured Query [+]', and 'Any Request [+]'.

The 'Cluster Overview' section is active, showing a 'Sort Cluster' dropdown, 'Sort Indices', 'View Aliases', and an 'Index Filter' input field. A 'Refresh' button is on the right. The main content area displays a table of indices and their shard distribution across nodes.

Index	Size	Docs	Shard 0	Shard 1	Shard 2	Shard 3	Shard 4	Shard 5	Shard 6	Shard 7	Shard 8
awsecurity_vpn	size: 870ki (870ki)	docs: 860 (860)	0	1	2						
awsecurity_myaccess	size: 31.9ki (31.9ki)	docs: 4 (4)	0	1	2	3	4				
awsecurity_lenel	size: 3.18Mi (3.18Mi)	docs: 5,019 (5,019)	0	1	2						
.watches	size: 75.3ki (75.3ki)	docs: 6 (6)	0	1	2						
.watcher-history-7-2018.03.19	size: 4.51Mi (4.51Mi)	docs: 4,016 (4,016)	0	1	2						
.watcher-history-7-2018.03.18	size: 12.7Mi (12.7Mi)	docs: 11,512 (11,512)	0	1	2						
.watcher-history-7-2018.03.17	size: 12.7Mi (12.7Mi)	docs: 11,520 (11,520)	0	1	2						

Below the index table, there is a section for 'Unassigned' shards, showing a grid of numbers (0, 1, 2, 3, 4) in boxes. A star icon and the text 'xUJiS6P' are visible next to the 'Unassigned' section.

We're using Apache HTTPD configuration to allow access for internal services with reverse proxy as following -

Apache HTTPD configuration

```
Listen 80
Listen 15601
Listen 19200

<VirtualHost *:19200>
    ProxyPreserveHost On
    ProxyPass "/" "http://localhost:9200/"
    ProxyPassReverse "/" "http://10.7.20.148:19200/"
    ServerName dev.awsecurity.com
</VirtualHost>

<VirtualHost *:15601>
    ProxyPreserveHost On
    ProxyPass "/" "http://localhost:5601/"
    ProxyPassReverse "/" "http://10.7.20.148:15601/"
    ServerName dev.awsecurity.com
</VirtualHost>

<VirtualHost *:*>
    ProxyPreserveHost On
    ProxyPass "/" "http://localhost:5601/"
    ProxyPassReverse "/" "http://10.7.20.148/"
    ServerName dev.awsecurity.com
</VirtualHost>
```