ELK Stack (Elasticsearch, Logstash & Kibana)

Version:	1.0.0
Created by:	cloudimg

Table of Contents

1.) Overview

This document is provided as a user guide for the ELK stack product offering on the AWS Marketplace. Please reach out to support@cloudimg.co.uk if any issues are encountered following this user guide for the chosen product offering.

cloudimg
(+44) 02045382725
3rd Floor 86-90 Paul Street London EC2A 4NE
support@cloudimg.co.uk
https://cloudimg.co.uk

2.)Access & Security

Please update the security group of the target instance to allow the below ports and protocols for access and connectivity.

Protocol	Type	Port	Description
SSH	TCP	22	SSH connectivity
TCP	TCP	9200	Elasticsearch API calls over HTTP
TCP	TCP	5601	Kibana Dashboard

3.)System Requirements

The minimum system requirements for the chosen product offering can be found below

Minimum CPU	Minimum RAM	Required Disk Space
1	1 GB	20 GB

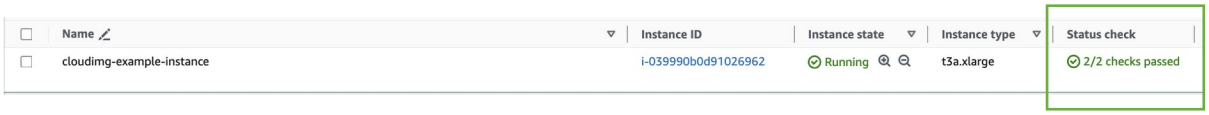
4.) Connecting to the Instance

Once launched in the Amazon EC2 Service, please connect to the instance via an SSH client using the **ec2-user** with the key pair associated at launch. Once connected as the **ec2-user** user, you will be able to sudo to the **root** user by issuing the below command.

Switch to the root user.

```
sudo su -
```

NOTE: Please allow the EC2 Instance to reach 2/2 successful status checks to ensure you will be able to connect successfully with the ec2-key pair assigned at launch. Upon attempting to SSH to early you may receive errors such as below, this is expected with an early SSH connection. Allow the EC2 instance to reach 2/2 status checks and you will be able successfully connect with the ec2-key pair assigned at launch as the ec2-user.



Example errors you may receive with an early SSH connection.

```
Permission denied (publickey,gssapi-keyex,gssapi-with-mic).

ec2-user@your-instance-ip's password:
```


cloudimg
(+44) 02045382725
3rd Floor 86-90 Paul Street London EC2A 4NE
support@cloudimg.co.uk
https://cloudimg.co.uk

5.) On Startup

An OS package update script has been configured to run on boot to ensure the image is fully up to date at first use. You can disable this feature by removing the script from /stage/scripts/ and deleting the entry in crontab for the root user.

Disable the OS update script from running on reboot

```
rm -f /stage/scripts/initial_boot_update.sh

crontab -e

#DELETE THE BELOW LINE. SAVE AND EXIT THE FILE.
@reboot /stage/scripts/initial_boot_update.sh
```

6.) Filesystem Configuration

Please see below for a screenshot of the server disk configuration and specific mount point mappings for software locations.

```
Filesystem      Size  Used Avail Use% Mounted on
devtmpfs        1.9G     0  1.9G   0% /dev
tmpfs           2.0G     0  2.0G   0% /dev/shm
tmpfs           2.0G  8.5M  1.9G   1% /run
tmpfs           2.0G     0  2.0G   0% /sys/fs/cgroup
/dev/nvme0n1p2   38G  6.0G   30G  17% /
/dev/nvme0n1p1  2.0G  121M  1.7G   7% /boot
tmpfs           391M     0  391M   0% /run/user/1002
/dev/nvme1n1    9.8G   80M  9.2G   1% /var/lib/elasticsearch
tmpfs           391M     0  391M   0% /run/user/0
```

Mount Point	Description
/boot	Operating System Kernel files
/var/lib/elasticsearch	Elasticsearch installation directory

7.) Server Components

Please see below for a list of installed server components and their respective installation paths. The below versions are subject to change on initial boot based on the initial_boot_update.sh script finding new versions of the software in the systems package repositories.

Component	Software Home
Java	/bin/java
Elasticsearch	/var/lib/elasticsearch
Logstash	/etc/logstash
Kibana	/etc/kibana

8.) Scripts and Log Files

The below table provides a breakdown of any scripts & log files created to enhance the useability of the chosen offering.

Script/Log	Path	Description
Initial_boot_update.sh	/stage/scripts	Update the Operating System with the latest updates available.
Initial_boot_update.log	/stage/scripts	Provides output for initial_boot_update.sh
elastic_password.log	/stage/scripts	Elastic user credentials
kibana_password.log	/stage/scripts	Kibana system user credentials

9.) Using System Components

Instructions can be found below for using each component of the server build mentioned in section 7 of this user guide document.

Java

Java has been preinstalled on the instance and the below command can be used to verify the version currently installed.

```
java -version
```

Elasticsearch

The Elasticsearch service has been configured to start on boot. You can stop, start and check the status of the service via the below commands.

```
#START THE ELASTICSEARCH SERVICE
systemctl start elasticsearch

#STOP THE ELASTICSEARCH SERVICE
systemctl stop elasticsearch

#CHECK THE STATUS OF THE ELASTICSEARCH SERVICE
systemctl status elasticsearch
```

You can also run the below command once the service is running to ensure a successful startup of the service has taken place. Please run the below as the root user. Enter the password value highlighted in **RED** from the randomly generated value located in the /stage/scripts/elastic_password.log file

```
curl --cacert /etc/elasticsearch/certs/http_ca.crt -u elastic http://localhost:9200
```

EXAMPLE EXPECTED OUTPUT

```
Enter host password for user 'elastic': ENTER PASSWORD AT PROMPT
{
  "name" : "ip-172-31-89-117.ec2.internal",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "wdyXEmS-TEearSUr0MEhPA",
  "version" : {
    "number" : "8.6.1",
    "build_flavor" : "default",
    "build_type" : "rpm",
    "build_hash" : "180c9830da956993e59e2cd70eb32b5e383ea42c",
    "build_date" : "2023-01-24T21:35:11.506992272Z",
    "build_snapshot" : false,
```

```
    "lucene_version" : "9.4.2",
    "minimum_wire_compatibility_version" : "7.17.0",
    "minimum_index_compatibility_version" : "7.0.0"
  },
  "tagline" : "You Know, for Search"
}
```

Kibana

The Kibana service has been configured to start on boot. You can stop, start and check the status of the service via the below commands.

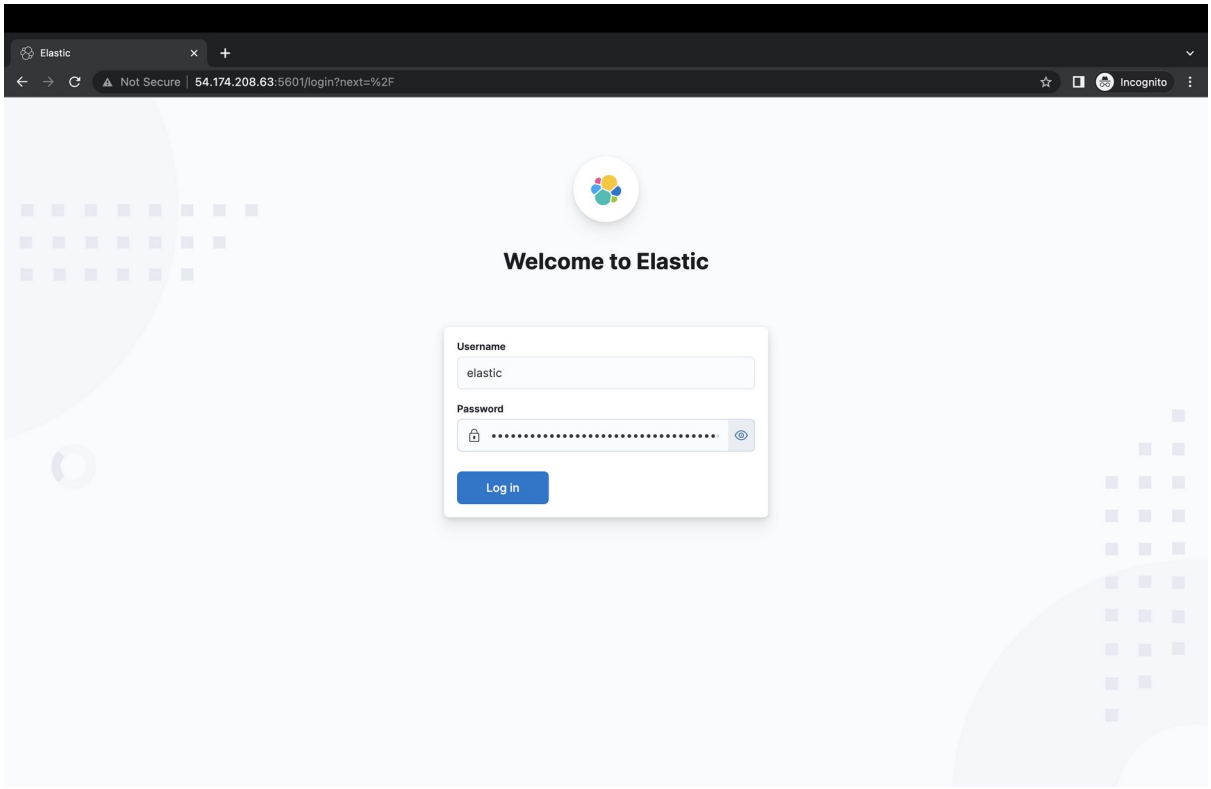
```
#START THE KIBANA SERVICE
systemctl start kibana

#STOP THE KIBANA SERVICE
systemctl stop kibana

#CHECK THE STATUS OF THE KIBANA SERVICE
systemctl status kibana
```

Once the service has been started, the Kibana dashboard will be available from the below URL. Please exchange the values between <> to match that of your instance.

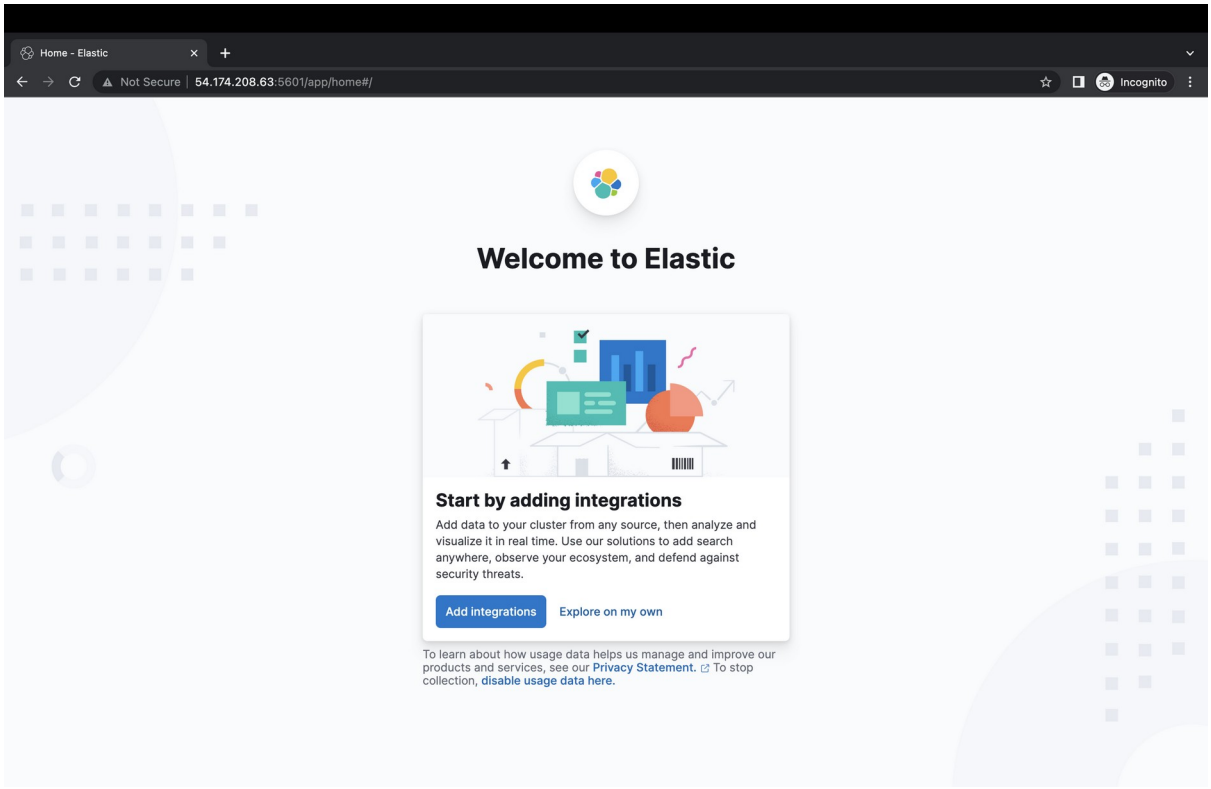
<PUBLIC/PRIVATEIP>:5601



Username = elastic

Password = REFER TO THE RANDOMLY GENERATED VALUE AVAILABNLE IN /stage/scripts/elastic_password.log

Click Log In



You may now use the ELK stack based on your requirements.

cloudimg
(+44) 02045382725
3rd Floor 86-90 Paul Street London EC2A 4NE
support@cloudimg.co.uk
https://cloudimg.co.uk