ElasticSearch & Kibana
Search Tools

Usage instructions:

1. Launch the product via 1-click. **Please wait until** the instance passes **all** status checks and is running. You can connect using your Amazon private key and '**ubuntu**' login via your SSH client.

To update software, use: **sudo apt-get update**

Elasticsearch

Testing Elasticsearch, run

curl -X GET "localhost:9200"

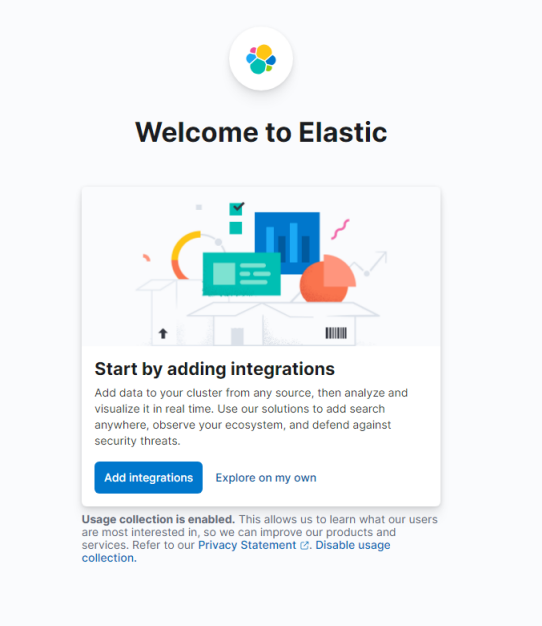
You can access using browser

http://yourinstanePublicIPaddress:9200

If you want to make configuration changes to Elasticsearch

sudo nano /etc/elasticsearch/elasticsearch.yml

sudo systemctl restart elasticsearch



Kibana

Accessing Kibana Dashboard, open a web browser

http://yourinstanePublicIPaddress:5601

If you want to make configuration changes to Kibana

sudo nano /etc/kibana/kibana.yml

sudo systemctl restart kibana

See: https://www.elastic.co/guide/en/kibana/current/introduction.html

Filebeat

Verify Elasticsearch Reception of Data, run

Replace “yourinstanceIPaddress” with you actual IP address

curl -XGET http://yourinstanceIPaddress:9200/_cat/indices?v

You can access in browser also:

http://yourinstanceIPaddress:9200/_cat/indices?v

If you want to make configuration changes to Filebeat

sudo nano /etc/filebeat/filebeat.yml

See: https://www.elastic.co/guide/en/beats/filebeat/current/directory-layout.html

Logstash

If you want to make configuration changes to Logstash

sudo systemctl start logstash.service
sudo systemctl status logstash.service

To test your Logstash installation, run the most basic Logstash pipeline

sudo -u logstash /usr/share/logstash/bin/logstash --path.settings /etc/logstash -t

See: https://www.elastic.co/guide/en/logstash/current/pipeline.html

AWS Data

- Data Encryption Configuration: This solution does not encrypt data within the running instance.
- User Credentials are stored: /root/.ssh/authorized_keys & /home/ubuntu/.ssh/authorized_keys
- Monitor the health:
    - Navigate to your Amazon EC2 console and verify that you're in the correct region.
    - Choose Instance and select your launched instance.
    - Select the server to display your metadata page and choose the Status checks tab at the bottom of the page to review if your status checks passed or failed.

Extra Information: (Optional)

Allocate Elastic IP

To ensure that your instance **keeps its IP during restarts** that might happen, configure an Elastic IP. From the EC2 console:

1. Select ELASTIC IPs.
2. Click on the ALLOCATE ELASTIC IP ADDRESS.
3. Select the default (Amazon pool of IPv4 addresses) and click on ALLOCATE.
4. From the ACTIONS pull down, select ASSOCIATE ELASTIC IP ADDRESS.
5. In the box that comes up, note down the Elastic IP Address, which will be needed when you configure your DNS.
6. In the search box under INSTANCE, click and find your INSTANCE ID and then click ASSOCIATE.
7. Your instance now has an elastic IP associated with it.
8. For additional help: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/elastic-ip-addresses-eip.html